



X-ROUTER

TRANSFORMABLE ROUTER SERIES

User Manual

X-108NX

English Version 2.0.7

CONTENT

CHAPTER1	INTRODUCTION.....	1
1.1	BENEFITS	1
1.2	PACKAGE CONTENT	2
CHAPTER2	HARDWARE INSTALLATION.....	5
2.1	PANEL LAYOUT	5
2.1.1	Front LEDs.....	5
2.1.2	Side Panel.....	6
2.1.3	Rear Panel	6
2.2	PROCEDURE FOR HARDWARE INSTALLATION.....	7
2.2.1	Power On.....	7
2.2.2	Setup LAN Connection.....	7
2.2.3	Setup WAN Connection.....	7
CHAPTER3	NETWORK SETTINGS FOR YOUR PC	8
3.1	FOR WINDOWS XP USERS.....	8
3.2	FOR WINDOWS 2000 USERS	10
3.3	FOR WINDOWS 98/ME USERS	12
3.1	FOR WINDOWS7 USERS	14
CHAPTER4	ACCESSING TO AXIMCom X-ROUTER	16
4.1	START-UP AND LOG-IN	16
CHAPTER5	BASIC SETTINGS.....	17
5.1	WAN SETUP	17
5.1.1	DHCP (automatic IP address assignment)	19
5.1.2	Static (Fixed IP address assignment)	20
5.1.3	PPPoE (connected by username/password)	21
5.1.4	Mobile WAN (connected by information related to what your ISP needs)	22
5.1.5	Windows Mobile / Google Android Phones / iPhone	24
5.1.6	HSPA+ Super Speed.....	25
5.2	WAN DETECT	27
5.3	LAN SETUP	28
5.4	ROUTING SETUP	29
5.4.1	Routing Settings	29
5.4.2	Add Routing Rule	30
5.4.3	Example	31
5.5	DHCP SERVER SETUP.....	32
5.6	DDNS SETUP	33
5.7	MAC ADDRESS CLONE SETUP	35

CHAPTER6	WIRELESS SETTINGS	36
6.1	BASIC SETUP	36
6.1.1	Settings.....	36
6.1.2	SSID Settings.....	38
6.1.3	WEP	40
6.1.4	WPA Pre-shared Key / WPA2 Pre-shared Key	40
6.1.5	WPA / WPA2.....	42
6.2	ADVANCED SETUP	43
6.3	WDS SETUP	45
6.4	UNIVERSAL REPEATER SETUP	46
CHAPTER7	SECURITY SETTINGS	47
7.1	FIREWALL SETUP	47
7.2	ACCESS CONTROL LIST (ACL) SETUP	49
7.2.1	ACL Settings	49
7.3	MAC ACCESS CONTROL SETUP	52
7.4	OpenDNS SETUP	54
7.4.1	OpenDNS Settings	54
7.5	WEB FILTERING SETUP	55
7.5.1	Added Web Filtering Rules.....	56
7.6	VPN / PPTP SETUP	57
7.6.1	VPN / PPTP Settings	57
7.6.2	Add VPN / PPTP Rule.....	59
CHAPTER8	INTELLIGENT DYNAMIC BANDWIDTH MANAGEMENT	60
8.1	iDBM SETUP	60
8.1.1	iDBM Settings.....	60
8.1.2	Add SBM Rules	63
8.1.3	Add DBM Rule.....	66
8.2	THROUGHPUT OPTIMIZER	67
8.3	TurboNAT SETUP	68
8.4	SESSION MANAGER.....	69
CHAPTER9	APPLICATIONS SETTINGS.....	70
9.1	PORT RANGE FORWARD SETUP	70
9.1.1	Port Range Forward Settings	71
9.1.2	Add Port Range Forwarding Rule	72
9.2	STREAMING/VPN PASS-THROUGH	73
9.3	UPnP/NAT-PMP SETUP	74
CHAPTER10	STORAGE FUNCTION SETTINGS	75
10.1	STORAGE DEVICE	75
10.1.1	USB Storage Device Installation	75

10.1.2 Storage Formatting	77
10.1.3 Ejecting of the Storage Device	78
10.2 FTP SERVER.....	79
10.3 SAMBA SERVER.....	80
CHAPTER11 ADMIN	81
11.1 MANAGEMENT.....	81
11.2 SYSTEM UTILITIES.....	83
11.3 TIME SETUP	85
CHAPTER12 STATUS	86
12.1 ROUTER INFORMATION	86
12.2 USER/DHCP	88
12.3 USER/ CURRENT	89
12.4 LOG	90

CHAPTER1 INTRODUCTION

AXIMCom's X series Router is a new design for users that have multiple requirements. The X-Router combined different aspect of features in a single box, such as 3G/4G sharing and storage functions.

AXIMCom aims to give the users the most cost effective and best performance products. The X-Router, says Transformable Router, can be changed into different working mode anytime and anywhere. In 3G/4G mode, simply connecting a 3G/4G modem, you can create a mobile broadband for a group of users and devices to share. Since the mobile broadband is shared, the 'cost per user/device' is then consequently reduced. In storage mode, simply connecting a USB storage device, you can create a mini network file sharing system to share the files by the X-Router. Furthermore, AXIMCom's X-Router Series also supports 802.11n technology, so you can enjoy the fastest and farthest wireless coverage! The higher-end models to be released will equipped with more switch modes such as Radio Station, VPN Server, Print Server, etc, and will let users to choose which is needed by them.

1.1 BENEFITS

- **System Mode Switch**

AXIMCom's X series router allows user to change its working mode anytime and anywhere. User can operate the Router met their user scenarios.

- **True Mobile Broadband Sharing (Support 3G/4G + 802.11n + xDSL/cable modem)**

AXIMCom X-Router working in 3G/4G mode supports multiple broadband technologies, including 3G/4G, 802.11n and xDSL/cable modem. You can create a mobile broadband using a 3G/4G modem or switch to fixed line connection using xDSL/cable modem. It also supports the latest 802.11n technology, offering a true mobile broadband sharing solution!

- **Complete 3G/4G Modem Support**

AXIMCom's X-Router provides complete support for all major 3G/4G USB modems. Simply use your existing 3G/4G modem and service provider to create a mobile broadband sharing environment. (Find our compatibility at the end of the user manual.)

- **Energy Saving**

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

- **3G/4G APN and PIN Code Support**

AXIMCom X-Router supports 3G/4G APN and PIN code in order to prevent unauthorized access to your

X-Router and increase the security levels of your mobile broadband.

- **Universal Repeater**

With the use of the Universal Repeater function, AXIMCom X-Router 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.

- **Session Manager**

AXIMCom X-Router supports up to 50000 fast recycling sessions in order to guarantee stable network connection and to accommodate more users/applications in the network. (Session numbers vary between models.)

- **Gigabit Ethernet supported (Applied to X-108NX and X-116NX Only)**

The X-Router equipped with Gigabit Ethernet as well as 950Mbps NAT throughput features which really met the requirements for Gigabit environment.

- **iDBM - Intelligent Bandwidth Management (Applied to X-108NX and X-116NX Only)**

Enabled with AXIMCom's patent-pending iDBM technology, AXIMCom X-Router's two highest level models, 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.

- **TurboNAT (Applied to X-108NX and X-116NX Only)**

Embedded with the TurboNAT Engine, AXIMCom X-Router's two premium models are able to increase NAT throughput to 950Mbps.

- **MRTG Monitoring (Applied to X-108NX and X-116NX Only)**

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.

- **PPTP Server**

With PPTP server enabled, this function provides a secured data connection in the most convenient way for the X108NX and X-116NX.

1.2 PACKAGE CONTENT

- **One AXIMCom X-Router**
- **One User Manual CD**
- **One Quick Installation Guide**
- **One Power Adaptor**
- **Two Dipole Antenna**

CHAPTER2 HARDWARE INSTALLATION

2.1 PANEL LAYOUT

2.1.1 Front LEDs

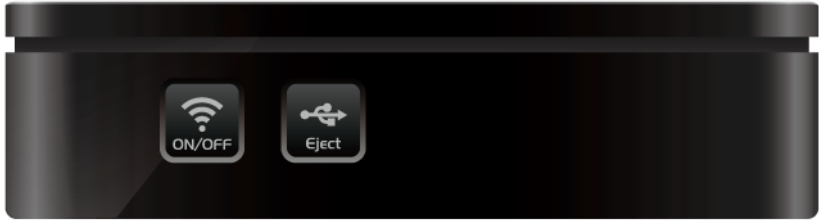


LED	Function	Color	Status	Description
WAN 	WAN Activity	Green/ Red	On	The WAN port is linked
			Off	The LAN port is not linked
			Blinking	Data is being transmitted via the LAN port
(LAN) 1-4 	LAN Activity	Green/ Red	On	The LAN port is linked
			Off	The LAN port is not linked
			Blinking	Data is being transmitted via the LAN port
WLAN 	Wireless Activity	Green	On	Wireless connection is enabled
			Off	Wireless connection is disabled
Status 	Router status indication	Green	On	USB device is working.
			Off	No USB device is detected.
			Fast Blinking	USB device is being initialized or is being ejecting
			Slow Blinking	System is booting up and will turn off after booting. Please contact AXIMCom if the LED is continuous in this status.
Power 	Power Indication	Green	On	Power is on
			Off	Power is off

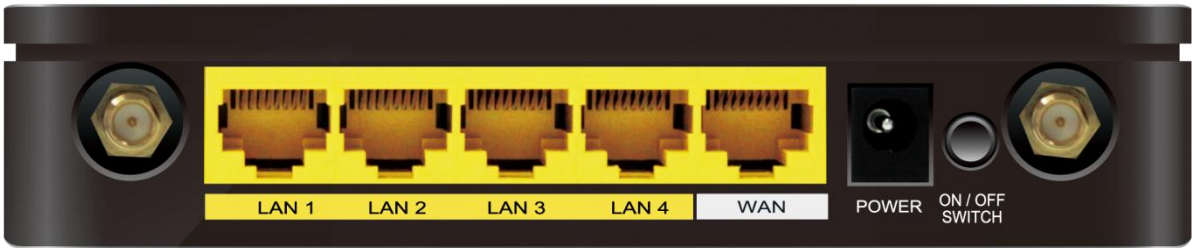
***The Red LED of WAN and LAN ports are enabled when links to the device that has gigabit ability.

Port	Description
USB	The port for connecting your USB 3G/4G modem or USB storage device

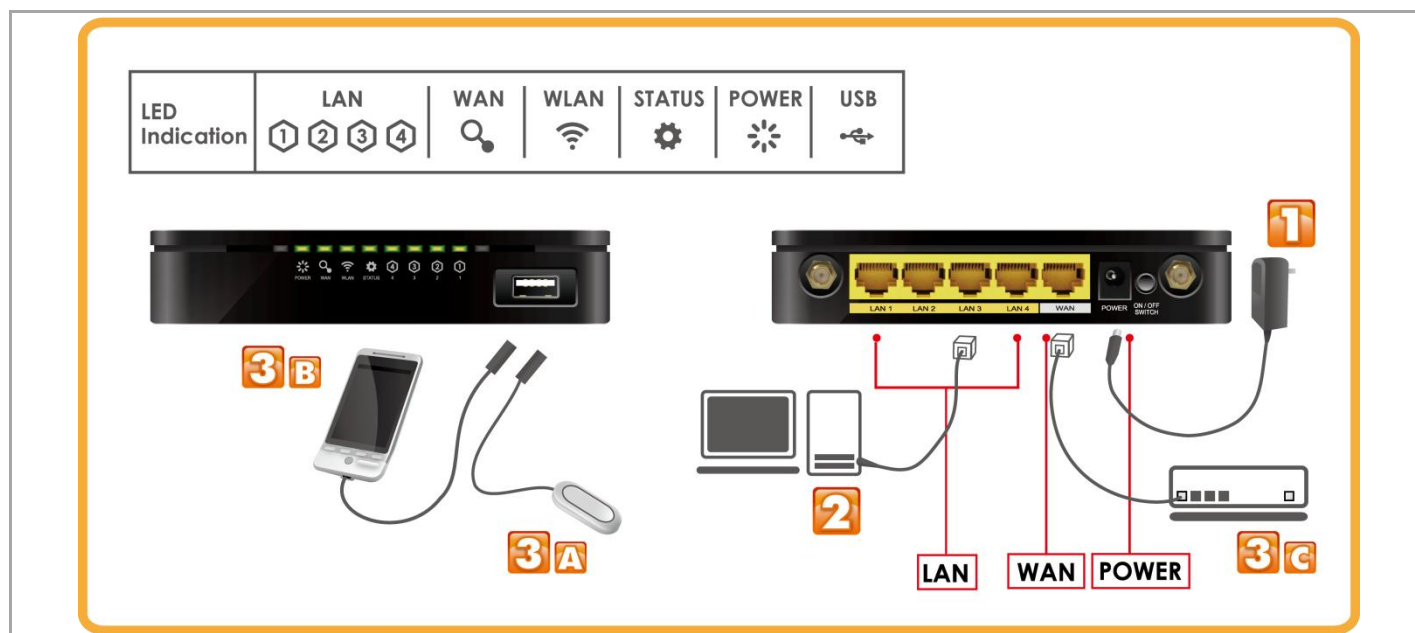
2.1.2Side Panel

	
Buttons/Port	Description
WLAN On/Off	The button for turn on/off the wireless radio.
EJECT	The button for ejecting the USB 3G/4G modem safely, not for WPS setting.
Reset	The Reset button is on the bottom of the router. Press the button for 3 seconds, AXIMCom X-Router will restore all the setting values to factory default and restart automatically.

2.1.3Rear Panel

	
Ports/Button	Description
Power	Power inlet
WAN	The port for connecting your xDSL or Cable Modem
LAN	The ports for connecting your computers, printer or other devices for making a wired connection
On/Off	Press the button to switch On/Off the power

2.2 PROCEDURE FOR HARDWARE INSTALLATION



2.2.1 Power On

Take the provided power adapter. Plug one end into the X-Router's DC power port and the other end into a power outlet. Switching on the On/Off switch, the X-Router will enter the working mode as soon as its STATUS LED light is 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 the X-Router's LAN ports.

2.2.3 Setup WAN Connection

Choose how to connect AXIMCom X- Router to the Internet. Choose one way below to connect your X-Router to the Internet.

A.B. Connecting via mobile Internet: please plug the 3G/4G USB modem or connect mobile phone into the router' s USB port.

C. Connecting via ADSL, VDSL or cable modem: take another Ethernet cable. Plug one end into your modem's LAN port and the other end into the router's WAN port.

Please note that 3G/4G connection mode (AB) is not supported in the storage mode.

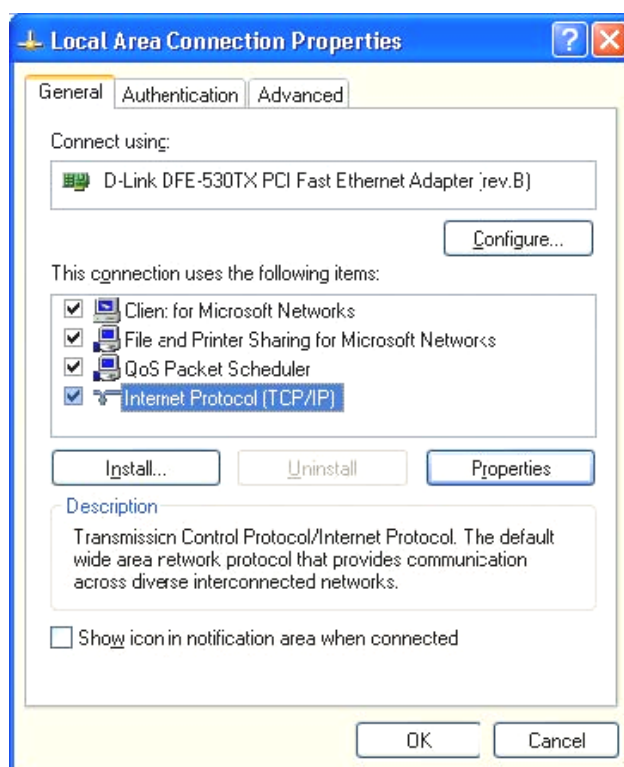
CHAPTER3 NETWORK SETTINGS FOR YOUR PC

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

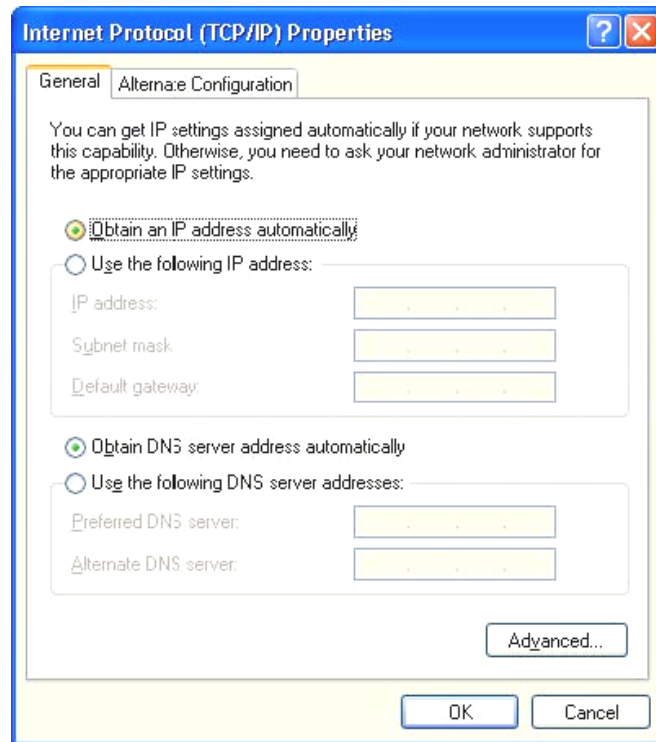
* DHCP is recommended due to its relative ease in configuration.

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 X-Router 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

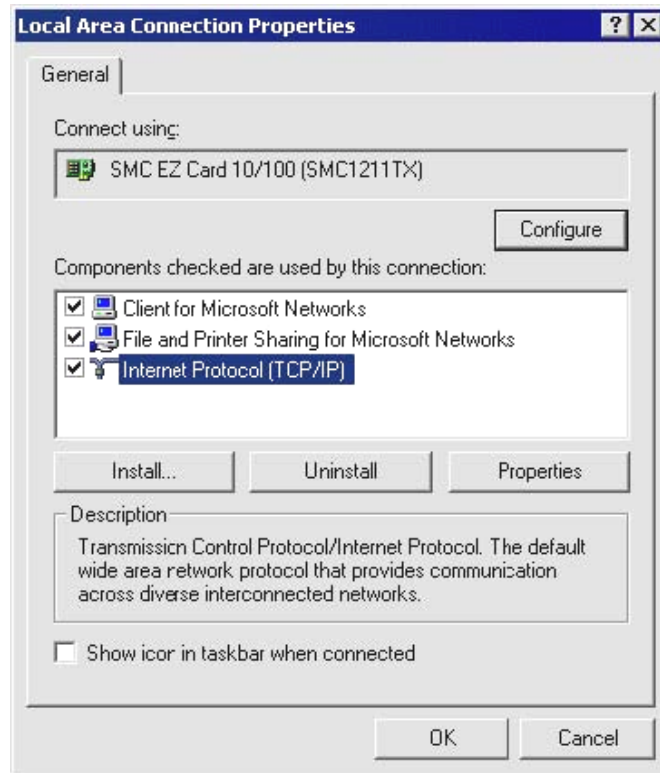
Now select Use the following DNS server addresses and enter the following.

Preferred DNS server: 192.168.1.1. Then click OK.

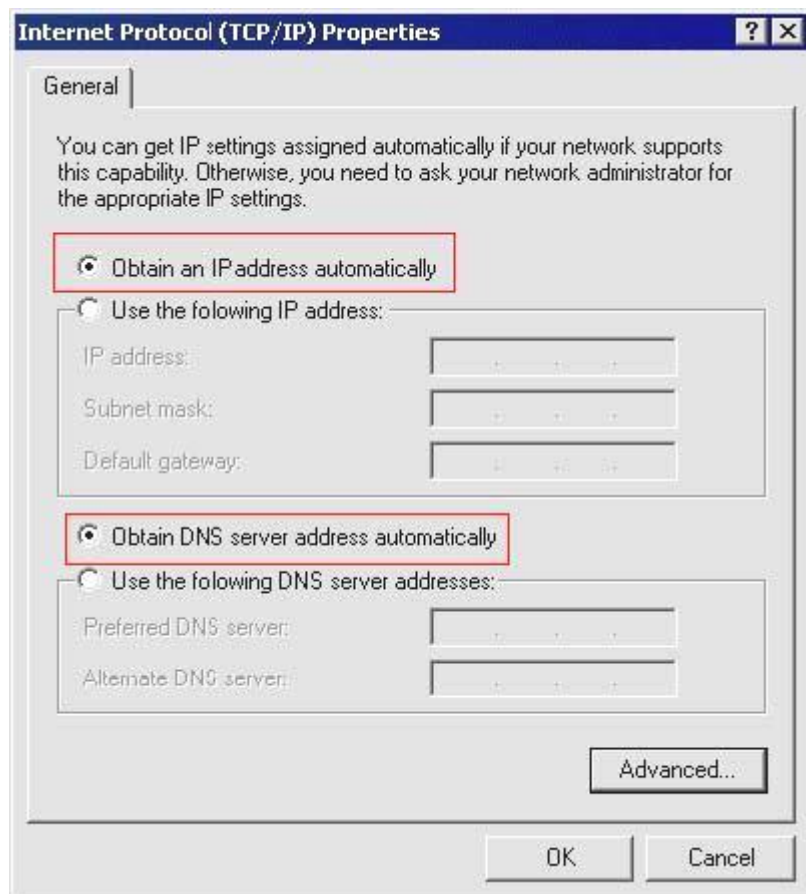
6. You have now finished the network settings for your computer. Please go to Chapter 4 to continue.

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 X-Router 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

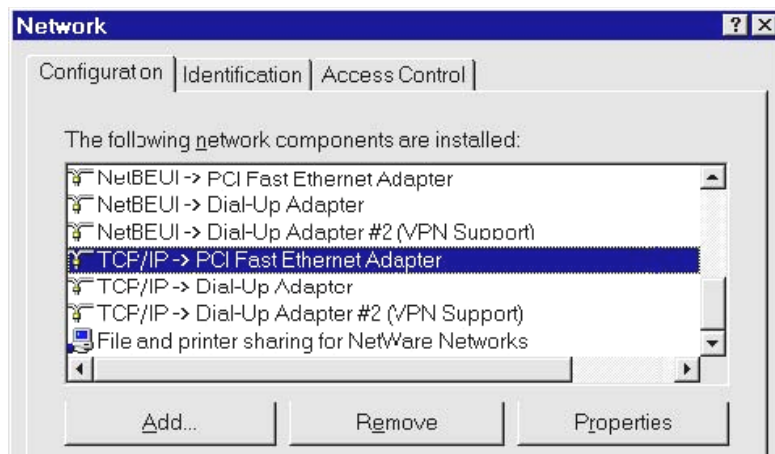
Now select Use the following DNS server addresses and enter the following. Preferred DNS server: 192.168.1.1

Then click OK.

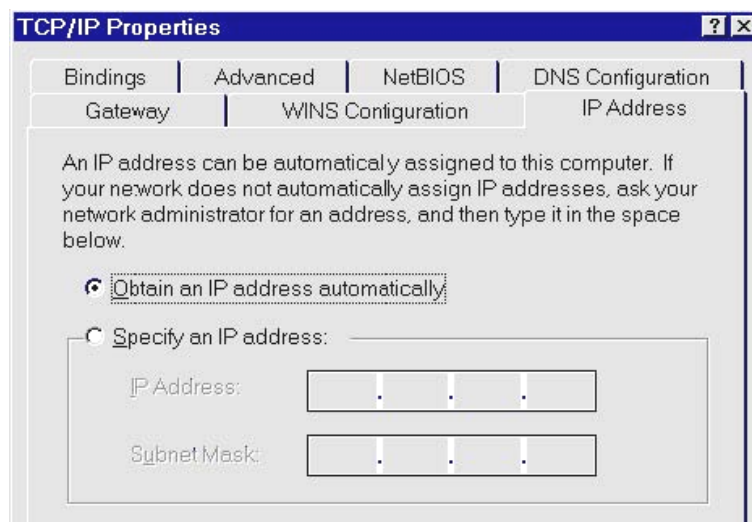
6. You have now finished the network settings of your computer. Please go to Chapter 4 to continue.

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 X-Router will now assign an IP address to your computer.

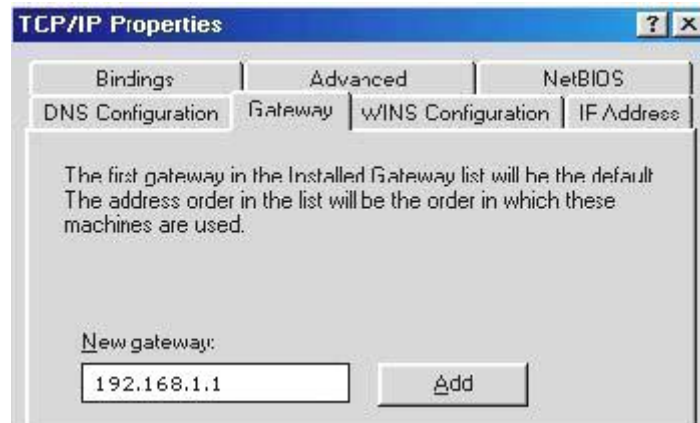
- To use Static IP

Select Specify an IP address and enter the followings.

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

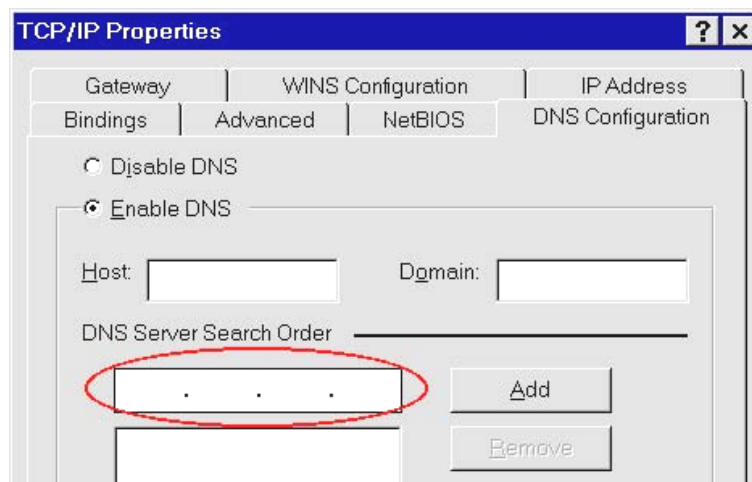
Subnet mask: 255.255.255.0

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.

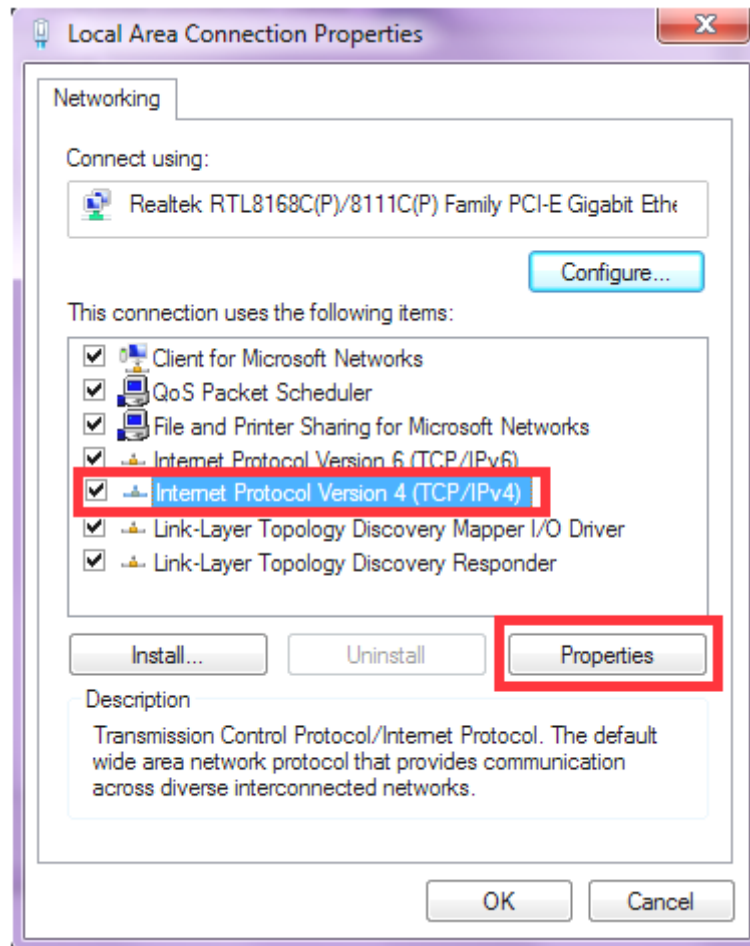


Enter 192.168.1.1 in *DNS Server Search Order* and click *Add*. Then click *OK*.

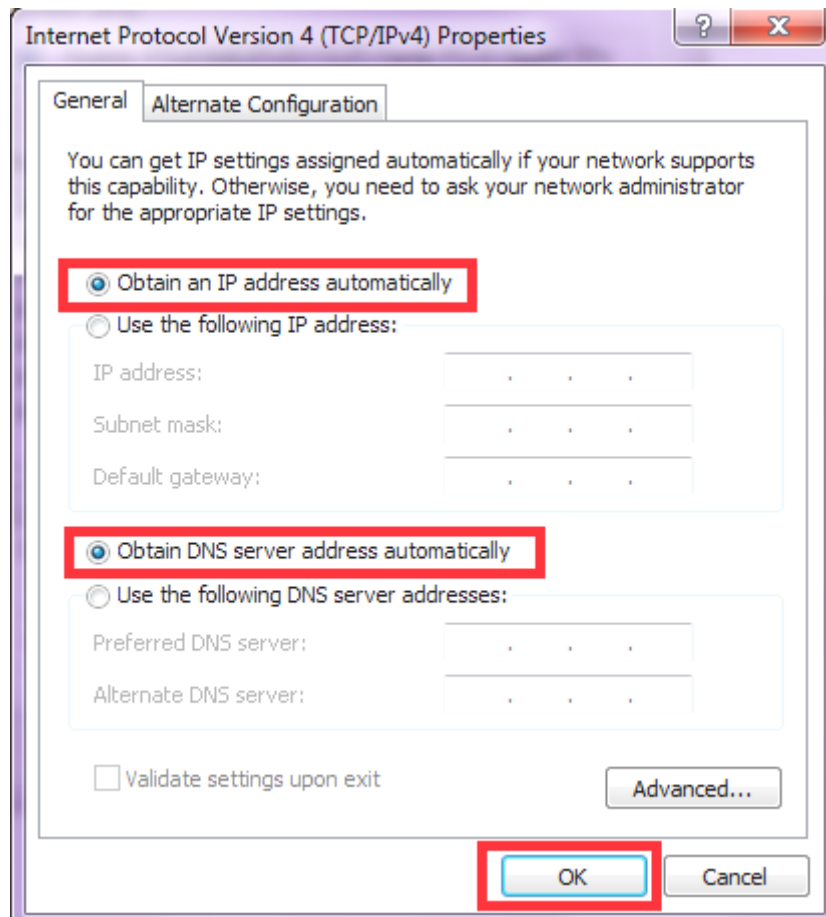
5. You have now finished the network settings of your computer. Please go to Chapter 4 to continue.

3.1 FOR WINDOWS7 USERS

1. Select Start > Control Panel > Network and Internet> Network and Sharing Center >Change Adapter Settings
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.



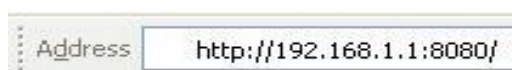
5. Enable DHCP or Static IP:

CHAPTER4 ACCESSING TO AXIMCom X-ROUTER

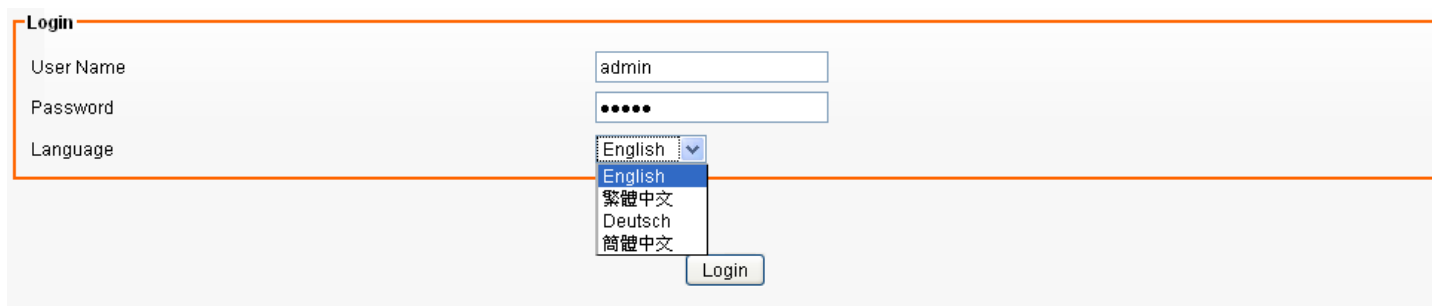
For Windows XP/2000 users, your computer should have obtained an IP address after configuring the network settings on your computer. Now you need to configure your AXIMCom X- Router.

4.1 START-UP AND LOG-IN

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



When you successfully connect to the configuration interface for AXIMCom X-Router, the login screen will pop up.

A screenshot of the AXIMCom X-Router login interface. It features a 'Login' title at the top left. Below it are three input fields: 'User Name' with the value 'admin', 'Password' with masked characters '•••••', and 'Language' with a dropdown menu. The dropdown menu is open, showing options: 'English' (selected), 'English', '繁體中文', 'Deutsch', and '簡體中文'. A 'Login' button is located at the bottom right of the form area.

Enter your username as [admin], your password as [admin] and select the preferred language. You will now see the start page of AXIMCom X-Router.

CHAPTER5 BASIC SETTINGS

5.1 WAN SETUP

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

Setup - WAN

WAN 1

WAN	☒ Enable ☐ Disable
Connection Type	3G/4G Mobile Internet ▼
Modem Brand	Auto ▼
Modem Model	Auto ▼
APN Type	☒ Service Provider ☐ Manual
Location	Taiwan ▼
Service Provider	Chunghwa Telecom ▼
Access Point Name (APN)	internet
Personal Identification Number (PIN)	
Authentication	CHAP (Auto) ▼
User Name	
Password	
Dial Number	*99#
Connection Mode	Auto ▼
PPP Connection Type	☐ Keep Alive ☐ On Demand
Max Idle Time	20 Seconds (60~3600)
PPP Echo Interval	1492 Seconds (3 ~ 50)
PPP Retry Threshold	20 Time(s) (3 ~ 50)
Mobile WAN MTU	*99***1# Bytes (592-1492)
TurboLink (Enable it might increase your 3G data charge)	☐ Enable ☐ Disable

Save SettingsCancel Changes

2. WAN Settings:

AXIMCom X-Router supports six connection types: DHCP, Static, PPPoE, 3G/4G Mobile WAN, Windows Mobile/Google Android phones/iPhone and HSPA+ Super Speed. Please ensure which connection type should be used, and select your internet connection type from the pull-down menu.

WAN 1

WAN

Connection Type

Modem Brand

Modem Model

APN Type

Location

☒ Enable ☐ Disable

3G/4G Mobile Internet

DHCP

Static IP

PPPoE

3G/4G Mobile Internet

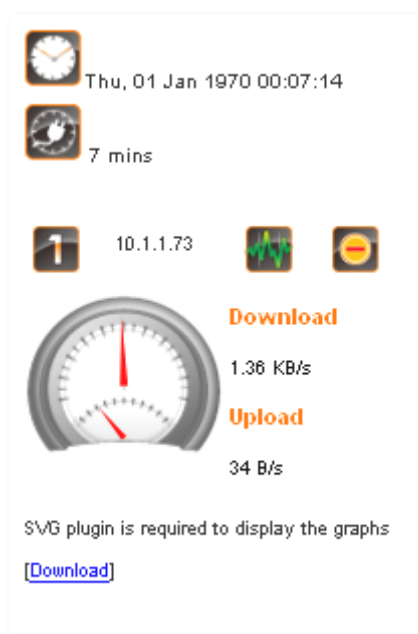
Windows Mobile / Google Android Phones

HSPA+ Super Speed

Taiwan

Whatever WAN connection type you have chosen, the Router will get a WAN IP and this IP will be shown in the setting page as bellow.

If "Not Connected" shows up in the setting, you should check the WAN settings again to get correct connection



5.1.1DHCP (automatic IP address assignment)

The IP address is automatically assigned to you by your ISP. You will see the following screen when you choose DHCP.

Setup - WAN

WAN 1

WAN

☒ Enable ☐ Disable

Connection Type

DHCP

Host Name

MTU

1500

Bytes

Bigpond Login

☐ Enable ☒ Disable

Bigpond Login Server

New South Wales (61.9.192.13)

Bigpond Login User Name

Bigpond Login Password

WAN	Select Enable/Disable 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.
MTU	Maximum Transmission Unit
Bigpond Login	If you are using "Bigpond" system, please enable this item
Bigpond Login Server	Please choose the Bigpond server.
Bigpond Login User Name	Please enter your User Name provided by Bigpond
Bigpond Login Password	Please enter your Password provided by Bigpond

5.1.2Static (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

10.1.1.25

Netmask

255.255.255.0

Gateway

10.1.1.254

Static DNS 1

10.1.1.254

Static DNS 2

MTU

1500

Bytes

Save Settings

Cancel Changes

WAN	Select Enable / Disable 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.
MTU	Maximum Transmission Unit

5.1.3 PPPoE (connected by username/password)

If your ISP provides the username and password, please enter the information accordingly.

WAN 1

WAN

Connection Type

Authentication

User Name

Password

PPP Connection Type

Max Idle Time

PPP Echo Interval

PPP Retry Threshold

PPP MTU

MTU

☒ Enable ☐ Disable

PPPoE

CHAP (Auto)

.....

☒ Always Connected ☐ On Demand

300 Seconds (60~3600)

20 Seconds (3 ~ 50)

20 Time(s) (3 ~ 50)

1492 Bytes (592-1492)

1500 Bytes (600~1500)

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	PPPoE Keep Alive will maintain the PPPoE dial up connection.
PPPoE Echo Interval	PPPoE echo will ensure whether the link is still up or not (default interval 20 seconds)
PPPoE Retry Threshold	When PPPoE echo retry exceeds PPPoE Retry Threshold (default 20 times), the dial up connection would be recognized as down.
PPPoE MTU	PPPoE maximum transmission unit: up to 1492 bytes (PPPoE's header is 8 bytes)(This value should be less than MTU value at least 8 bytes).
MTU	Physical Device Maximum Transmission Unit

5.1.4 Mobile WAN (connected by information related to what your ISP needs)

Please enter the APN, PIN code, user name, and password provided by your ISP. (Please note that some information might not be needed.)

Please note that this function is not supported in storage mode.

Setup - WAN

WAN 1

WAN	☒ Enable ☐ Disable
Connection Type	3G/4G Mobile Internet
Modem Brand	Auto
Modem Model	Auto
APN Type	☒ Service Provider ☐ Manual
Location	Taiwan
Service Provider	Chunghwa Telecom
Access Point Name (APN)	internet
Personal Identification Number (PIN)	
Authentication	CHAP (Auto)
User Name	
Password	
Dial Number	*99#
Connection Mode	Auto
PPP Connection Type	☐ Keep Alive ☐ On Demand
Max Idle Time	20 Seconds (60~3600)
PPP Echo Interval	1492 Seconds (3 ~ 50)
PPP Retry Threshold	20 Time(s) (3 ~ 50)
Mobile WAN MTU	*99***1# Bytes (592-1492)
TurboLink (Enable it might increase your 3G data charge)	☐ Enable ☐ Disable

Save Settings

Cancel Changes

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	Mobile WAN
Modem Brand	Choose the modem brand you use. You can keep it as Auto for automatic detection.
Modem Model	Choose the modem model you use. You can keep it as Auto for automatic detection.
APN Type	Choose By Service Provider for specifying the ISP you use, or otherwise choose Custom to assign desired APN.
Location	Choose your location.
Service Provider	Choose your service provider and the Access Point Name (APN) will be automatically assigned.
Access Point Name (APN)	Enter APN string offered by the ISP if you select Custom for APN Type (keep it empty if your ISP doesn't need it).
Personal Identification Number (PIN)	Enter PIN code offered by the ISP (keep it empty if your ISP doesn't need it).
User Name	The user name offered by the ISP (keep it empty if your ISP doesn't need it).
Password	The password offered by the ISP (keep it empty if your ISP doesn't need it).
Dial Number	Enter Dial Number offered by the ISP (default *99***1#).
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	PPPoE Keep Alive will maintain the PPPoE dial up connection.
PPPoE Echo Interval	PPPoE echo will ensure whether the link is still up or not (default interval 20 seconds)
PPPoE Retry Threshold	When PPPoE echo retry exceeds PPPoE Retry Threshold (default 20 times), the dial up connection would be recognized as down.
PPPoE MTU	PPPoE maximum transmission unit: up to 1492 bytes (PPPoE's header is 8 bytes).

5.1.5 Windows Mobile / Google Android Phones / iPhone

If you want to share your 3G/3.5G network via your Windows Mobile phone, Google Android Phones or iPhone, you have to choose this WAN connection type in the AXIMCom X-Router.

After connecting your phone and the Router with USB, you need to enable "Internet Sharing" or "Mobile Network Sharing" function in your Windows Mobile phone, Google Android Phones or iPhone

Please note that this function is not supported in storage mode.

WAN 1

WAN

☒ Enable ☐ Disable

Connection Type

Windows Mobile / Google Android Phones ▼

Host Name

MTU

Bytes

TurboLink (Enable it might increase your 3G data charge)

☐ Enable ☒ Disable

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	Windows Mobile / Google Android Phones
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.
MTU	Maximum transmission unit
TurboLink	Enable "TurboLink" to improve the connection speed and stability. (Please note that TurboLink function might increase your 3G data charge)

5.1.6 HSPA+ Super Speed

If you using HSPA+ super speed modem, please choose this WAN connection type. Please enter the APN, PIN code, user name, and password provided by your ISP. (Please note that some information might not be needed.)

Please note that this function is not supported in storage mode.

WAN 1

WAN	☒ Enable ☐ Disable
Connection Type	HSPA+ Super Speed
Modem Brand	Auto
Modem Model	Auto
APN Type	☒ Service Provider ☐ Manual
Location	Taiwan
Service Provider	Chunghwa Telecom
Access Point Name (APN)	internet
Personal Identification Number (PIN)	
Connection Mode	Auto
WAN MTU	1500 Bytes
Bigpond Login	☐ Enable ☒ Disable
Bigpond Login Server	New South Wales (61.9.192.13)
Bigpond Login User Name	
Bigpond Login Password	
TurboLink (Enable it might increase your 3G data charge)	☐ Enable ☐ Disable

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	HSPA+ Super Speed
Modem Brand	Choose the modem brand you use. You can keep it as Auto for automatic detection.
Modem Model	Choose the modem model you use. You can keep it as Auto for automatic detection.
APN Type	Choose By Service Provider for specifying the ISP you use, or otherwise choose Custom to assign desired APN.
Location	Choose your location. If not available in the list, please choose [custom] and enter setting values(APN, PIN) manually
Service Provider	Choose your service provider and the Access Point Name (APN) will be automatically assigned.
Access Point Name (APN)	Choose By Service Provider for specifying the ISP you use, or otherwise choose Custom to assign desired APN.
Personal Identification Number (PIN)	Please enter PIN code
Connection Mode	Choose your connection mode, Please choose AUTO mode.
WAN MTU	Maximum transmission unit
Bigpond Login	If you are using "Bigpond" system, please enable this item
Bigpond Login Server	Please choose the Bigpond server.
Bigpond Login User Name	Please enter your User Name provided by Bigpond
Bigpond Login Password	Please enter your Password provided by Bigpond
TurboLink	Enable "TurboLink" to improve the connection speed and stability. (Please note that TurboLink function might increase your 3G data charge)

5.2 WAN DETECT

There are stability issues when use 3G network. Sometime the 3G data card is connected with the 3G station but the data cannot be sent or received.

In this case, users can use the WAN Detect function to continuously ping a host, and get re-connected to the 3G station when detection fail is occurred.

Please note that this function is not supported in storage mode

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

Setup - WAN Detect

WAN Detect - WAN 1

External Connection Detection ☐ Enable ☒ Disable

Detection Host (IP address or domain name)

Detection Interval 60 Seconds

Connection Detection Threshold Time(s)(1~32)

2. Configure the basic settings of Load Balance following the instructions below.

External Connection Detection	Choose Enable/Disable to enable/disable connection detection.
Detection Host	Enter the IP address or domain name of the host to be detected.
Detection Interval	Detection Interval is 60 seconds
Connection Detection Threshold	The system will generate a PING packet to detect whether the connection is still connected. If the Host is not response for this threshold value, the system is considered to be WAN lost.

5.3 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.

5.4 ROUTING SETUP

5.4.1 Routing Settings

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

Setup - Routing

Routing

Routing

☒ Enable ☐ Disable

Routing Rule

Rule Name	Enable	Internal IP Range	External IP Range	Protocol	Service Port Range	External Interface	Routing Type	Gateway
SMTP	✖	From: To:	From: To:	TCP	From:25 To:25	WAN1	default	
AddDeleteModifyUpDown								

SaveCancel

- 2. Configure Security Settings following the instructions below.

Routing	Choose Enable/Disable to enable/disable routing policy.
---------	---

5.4.2 Add Routing Rule

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

Sequence Number: 2

Rule Name:

Enable: ☒

Internal IP Range: From: To:

External IP Range: From: To:

Protocol: *

Service Port Range: From: To:

External Interface: WAN1

Routing Gateway: Default Gateway

Gateway IP Address:

Confirm Cancel Changes

2. Configure the Routing rule following the instructions below.

Sequence Number	This defines the sequence of the Routing rules. If a packet fits the conditions set by the Routing rules, the packet will then be sorted according to the first Routing rule from the top of the list.
Rule Name	Name of the Routing rule.
Enable	Enable/Disable this Routing 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.
External Interface	Please select which External Interface (WAN1 or LAN1) you want for a packet to go through, if the packet fits the condition of this ACL rule.
Routing Gateway	Please select which Gateway(Default or Static) you want to route to.
Gateway IP Address	Please enter the Gateway IP Address if you choose Static Gateway in the Routing Gateway menu.

5.4.3Example

User has one ADSL line and one T1 line with two X-Router in use. Now administrator wants to the traffic of web browsing go through the cost effective ADSL line, who can follow the following settings below.

First, one should connect the two X-Router at the LAN side.

Router#1:

WAN: T1

IP: 192.168.1.1

Router#2:

WAN: ADSL2

IP: 192.168.1.254

Rule Name	HTTP outgoing routing
Enable	Enable
Internal IP Range	Blank (applied to all)
External IP Range	Blank (applied to all)
Protocol	TCP
Service Port Range	80:80 (HTTP Port:80)
External Interface	LAN1
Routing Gateway	Static
Gateway IP Address	192.168.1.254

5.5 DHCP SERVER SETUP

AXIMCom X-Router provides DHCP server service in order to offer IP addresses to the computers within a LAN.

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

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 Enable/Disable 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 1 Hour, 3 Hours, 6 Hours, 1 Day, 3 Days, or 7 Days.
Domain	Please enter the domain name.

5.6 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 X-Router.
2. Click on [Setup] – [DDNS] tab. You will see the following screen.

Setup - DDNS

Dynamic Domain Name Service - WAN 1

DDNS Service	☒ Enable ☐ Disable
DDNS Type	DynDNS.org ▼
User Name	
Password	
Host Name	
Action	Update

3. Configure your DDNS following the instructions listed below.

DDNS Service	Select Enable to enable DDNS service. Select Disable 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

5.7 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 X-Router using the pre-registered MAC address.

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

Setup - MAC Address Clone

MAC Address Clone - WAN 1

Clone WAN MAC

☒ Enable ☐ Disable

MAC Address

Save Settings

Cancel Changes

- 2. 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 Enable. If your ISP does not enforce access control, please select Disable.
MAC Address	If the PC you use to configure AXIMCom X-Router is the device which has the right MAC address to access the internet, press Get Current PC MAC Address button. Or you can type in the MAC Address which has been granted access by your ISP.

CHAPTER6 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	☒ 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 ▼

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/g/n or mixed use.
Transmission Power	Select the transmission power class from 10%, 25%, 50%, 75%, and 100%.
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

The screenshot displays the 'Wireless - Basic' configuration interface. It is divided into three main sections, each outlined with an orange border:

- WLAN 1**: Contains settings for the primary wireless connection.
 - Wireless Connection: Radio buttons for 'Enable' (selected) and 'Disable'.
 - Wireless Mode: A dropdown menu set to 'B/G/N Mixed'.
 - Transmission Power: A dropdown menu set to '100%'.
 - Wireless Channel: A dropdown menu set to 'Channel 6 [2.437GHz]'.
 - Wireless Isolation Between SSIDs: Radio buttons for 'Enable' and 'Disable' (selected).
- WLAN 1 - SSID 1**: Contains settings for the first SSID.
 - Wireless SSID: Radio buttons for 'Enable' (selected) and 'Disable'.
 - Wireless SSID Name: A text input field containing 'AXIMCom1'.
 - Wireless SSID Broadcasting: Radio buttons for 'Enable' (selected) and 'Disable'.
 - Wi-Fi Multimedia (WMM): Radio buttons for 'Enable' (selected) and 'Disable'.
 - Wireless Isolation: Radio buttons for 'Enable' and 'Disable' (selected).
 - Security Mode: A dropdown menu currently showing 'Disable', with a list of options expanded below it.
- WLAN 1 - SSID 2**: Contains settings for the second SSID.
 - Wireless SSID: This section is partially visible at the bottom of the screen.

The expanded dropdown for 'Security Mode' lists the following options: Disable, WEP, WPA PSK (Pre-Shared Key), WPA (Radius), WPA2 PSK (Pre-Shared Key), and WPA2 (Radius).

2. Configure SSID settings following the instructions below.

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

6.1.3 WEP

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	WEP
Key Index	1
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	AXIMCom1
Wireless SSID Broadcasting	☒ Enable ☐ Disable
Wi-Fi Multimedia (WMM)	☒ Enable ☐ Disable
Wireless Isolation	☐ Enable ☒ Disable
Security Mode	WPA PSK (Pre-Shared Key)
Key	
Encryption Method	AES

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

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.

6.1.5WPA / WPA2

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

WPA (Radius) ▼

Radius Server IP Address

Radius Server Port

1812

Radius Key

AES ▼

Encryption Method

Disable ▼

Rekey Method

3600

Rekey Time Interval

5000

Rekey Packet Interval

(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	2346	Bytes (256 ~ 2346)
RTS	2347	Seconds (1 ~ 2347)
DTim	1	(1 ~ 255)
Beacon Interval	100	Milliseconds (20 ~ 1024)
Header Preamble	Long ▼	
TxMode	None ▼	
MPDU	4 ▼	Microseconds
MSDU Aggregate	☐ Enable ☒ Disable	
Tx Burst	☒ Enable ☐ Disable	
Packet Aggregate	☐ Enable ☒ Disable	
HT Control Field	☐ Enable ☒ Disable	
Reverse Direction Grant	☐ Enable ☒ Disable	
Link Adapt	☐ Enable ☒ Disable	
Short Guard Interval(GI)	☒ Enable ☐ Disable	
Operation Mode	Mixed Mode ▼	
HT Band Width	20/40 ▼	MHz
Block Ack Setup Automatically	☒ Enable ☐ Disable	
Block Ack Window Size	64	x16 Bits (1 ~ 64)
Reject Block Ack	☐ Enable ☒ Disable	
MCS	Auto ▼	

Save Settings

Cancel Changes

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 Long or Short header preamble.
TxMode	Choose different transmission mode.
MPDU	MPDU data length. The transmission rate is increase when you choose a larger number, but usually the max value will be 4 in the wireless card
MSDU Aggregate	A kind of packet aggregation method, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
Tx Burst	Some 802.11g wireless card can supported this mode, and the transmission rate can be increased when enable this function.
Packet Aggregate	An aggregation method like A-MSDU, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
HT Control Field	Choose Enable/Disable. It is useful when you need to debug the wireless network
Reverse Direction Grant	Choose Enable/Disable. The response time can be shorter when enable this function.
Link Adapt	Choose Enable/Disable. The function is use to dynamically change the modulation and encode mechanism between wireless devices.
Short Guard Interval (SGI)	Choose Enable/Disable. Short GI can improve some transmission rate, but with less immunity when interference exist.
Operation Mode	Choose Mixed mode or Greenfield. You may choose Greenfield mode to increase the transmission rate when you using 802.11n wireless network only.
HT Band Width	Using HT20MHz or HT20/40MHz
Block Ack Setup Automatically	Choose Enable/Disable. If your Wifi Card supported Block Ack mechanism, it can improve the data transmission efficiency when enable this function.
Block Ack Window Size	Specify a Block Ack window size
Reject Block Ack	Choose Enable to reject the request of BA from other Wireless device
MCS	Select transmission (connection) speed.

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)
Disabled
Repeater (AP Enabled)
Bridge (AP Disabled)

WDS 1

WDS MAC Address

Security Mode

Disable

WDS 2

WDS MAC Address

Security Mode

Disable

WDS 3

WDS MAC Address

Security Mode

Disable

WDS 4

WDS MAC Address

Security Mode

Disable

- 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.

Please note that this function is not supported when enable Hardware NAT function. The configuration can be set on [Bandwidth-TurboNAT].

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

WLAN 1

Universal Repeater Enable

☐Enable ☒Disable

Target SSID

Target BSSID (MAC)

Wireless Channel

Channel 6 [2.437GHz]

Site Survey

Security Mode

Disable

- 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.
Site Survey	Click the tab to use site survey choosing the Target SSID
Security Mode	Choose the security mode the target AP uses, and enter the key if needed.

CHAPTER7 SECURITY SETTINGS

7.1 FIREWALL SETUP

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

Security - Firewall

Firewall Protection

SPI Firewall Protection

☒ Enable ☐ Disable

TCP SYN DoS Protection

☒ Enable ☐ Disable

ICMP Broadcasting Protection

☒ Enable ☐ Disable

ICMP Redirect Protection

☒ Enable ☐ Disable

Save Settings

Cancel Changes

2. Configure Security Settings following the instructions below.

SPI Firewall Protection	Select Enable to enable SPI Firewall Protection. Select Disable to disable SPI Firewall Protection.
TCP SYN DoS Protection	Check to enable TCP SYN DoS Protection. Uncheck to disable TCP SYN DoS Protection. 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. AXIMCom X-Router 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 X-Router is still able to serve normal traffic while it is under such an attack.

ICMP Broadcasting Protection	Check to enable ICMP Broadcasting Protection. Uncheck to disable ICMP Broadcasting Protection. ICMP broadcasting attack is a type of DoS attacks. A flood of ICMP broadcasting packets is generated and sent to a server (like AXIMCom X-Router). Consequently, this server will suffer from a huge amount of interruptions and consumption of computing resources. AXIMCom X-Router is able to stop responding to ICMP broadcasting echo packets in order to avoid a potential ICMP broadcasting DoS attack.
ICMP Redirect Protection	Check to enable ICMP Redirect Protection. Uncheck to disable ICMP Redirect Protection. 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.

7.2 ACCESS CONTROL LIST (ACL) SETUP

7.2.1 ACL Settings

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

Please do not change the parameters unless you wish to customize it by yourself.

Security - Access Control

Access Control List (ACL)
Access Control ☒ Enable ☐ Disable
Default Access Control Action ☒ ALLOW ☐ DENY

Access Control List (ACL) Rule

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

- 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)

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

- 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 °

5. Example: 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.*/24.

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

7.3 MAC ACCESS CONTROL SETUP

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

MAC Access Control

MAC Access Control

☒ Enable ☐ Disable

Default MAC Access Control Action

☒ ALLOW ☐ DENY

MAC Access Control Rule

Rule Enable

Action

ACL Enable

Static DHCP Enable

IP

Add

Delete

Modify

Up

Down

Save Settings

Cancel Changes

2. Configure ACL Settings following the instructions below.

MAC Access Control	Choose Enable/Disable to enable/disable MAC access Control
Default MAC Access Control Action	The default ACL action of the ACL rules. When you add the individual rules, it can be viewed as exceptions and take effects relating to the default action. If the action of the adding rule is the same as the default action, then this rule will not work.

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

Sequence Number

1

Rule Name

MAC

Action

ALLOW

ACL Enable

☒

Static ARP Enable

☒

Static DHCP Enable

☒

IP

Confirm

Cancel Changes

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

4. Example: Bind IP to a MAC

If users need to bind a IP to a specified MAC (network device), one can follow the settings as below.

Sequence Number	User1
Rule Name	Enable
MAC	00:33:44:55:66:77
Action	Allow Access
ACL Enable	Enable
Static ARP Enable	Enable
Static DHCP Enable	Enable
IP	192.168.1.100

7.4 OpenDNS SETUP

7.4.1 OpenDNS Settings

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

Security - OpenDNS

The screenshot displays the 'Security - OpenDNS' configuration page. It features two identical sections for 'OpenDNS - WAN 1' and 'OpenDNS - WAN 2'. Each section contains the following fields and options:

- OpenDNS Service:** Radio buttons for 'Enable' and 'Disable'. In the image, 'Disable' is selected.
- OpenDNS Username:** A text input field.
- OpenDNS Password:** A text input field.
- DNS Query Redirection to OpenDNS DNS Servers:** Radio buttons for 'Enable' and 'Disable'. In the image, 'Disable' is selected.
- OpenDNS Label:** A text input field.

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'.

2. Configure OpenDNS Settings following the instructions below.

OpenDNS Service	Choose Enable/Disable to enable/disable OpenDNS
OpenDNS Username	Enter OpenDNS user name.
OpenDNS Password	Enter OpenDNS password.
DNS Query Redirection to OpenDNS DNS Servers	Choose Enable/Disable to enable/disable the data flow redirect to the OpenDNS Server. Users can get advanced content filtering function through the setting
OpenDNS Label	Enter the OpenDNS Label

7.5 WEB FILTERING SETUP

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

Security - Web Filtering

Web Filtering

Web Filtering

☐ Enable ☒ Disable

Web Content Filtering

Activex Filtering

☐ Enable ☒ Disable

Java/JavaScript Filtering

☐ Enable ☒ Disable

Proxy Filtering

☐ Enable ☒ Disable

Web Filtering Rule

Rule Enable

Filter Keyword

Filter Type

Action

Add

Delete

Modify

Up

Down

Save Settings

Cancel Changes

2. Configure Web Filtering Settings following the instructions below.

Web Filtering	Choose Enable/Disable to enable/disable Web Filtering
Activex Filtering	Choose Enable/Disable to enable/disable Activex Filtering
Java/JavaScript Filtering	Choose Enable/Disable to enable/disable Java/JavaScript Filtering
Proxy Filtering	Choose Enable/Disable to enable/disable Proxy Filtering

7.5.1Added Web Filtering Rules

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

Sequence Number1

Rule Enable☐

Filter Keywordweb-page-name

Filter Typeurl

ActionDENY

ConfirmCancel Changes

2. Configure Web Filtering Settings following the instructions below

Sequence Number	This defines the sequence (priority) of all the Web Filtering rules.
Rule Enable	Choose Enable/Disable to enable/disable Web Filtering rule
Filter Keyword	Enter the Keyword
Filter Type	Choose URL or Sever
Action	Select ALLOW / DENY °

3. Example: Block a URL with Keyword

If one need to block Facebook related web page, can follow the settings as below

Sequence Number1

Rule Enable☒

Filter Keywordfacebook

Filter Typeurl

ActionDENY

ConfirmCancel Changes

7.6 VPN / PPTP SETUP

7.6.1 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
Add	Delete	Modify
Up	Down	

2. Configure PPTP Settings following the instructions below.

PPTP	Choose Enable/Disable 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 Enable/Disable to enable/disable Auto DNS.
DNS	Enter DNS server if you choose Disable for Auto DNS.
CHAP Enable	Choose Enable/Disable to enable/disable CHAP for VPN authentication.
MSCHAP Enable	Choose Enable/Disable to enable/disable MSCHAP for VPN authentication.
MSCHAP2 Enable	Choose Enable/Disable to enable/disable MSCHAP2 for VPN authentication.
MPP128 Enable	Choose Enable/Disable to enable/disable MPP128 encryption.
Proxy ARP Enable	Choose Enable/Disable to enable/disable Proxy ARP.
NAT Enable	Choose Enable/Disable to enable/disable NAT.

7.6.2 Add VPN / PPTP Rule

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

Sequence Number

Rule Enable ☒

User Name

Password

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

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

CHAPTER8 INTELLIGENT DYNAMIC BANDWIDTH MANAGEMENT

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 [Bandwidth] – [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 3072.0/768.0 Kbps

Static Bandwidth Management (SBM)

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

Add Delete Modify Up Down

Dynamic Bandwidth Management (DBM)

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

DBM Available Bandwidth
WAN 1 3072.0/768.0 Kbps

Rule Name	Rule Enable	DBM IP
DBM		From:192.168.1.20

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.

3. Advanced Setting Example

A user subscribed 10M/2Mbps bandwidth from ISP. After performing some speed test, the user found that the actual bandwidth is about 1135KByte/sec downloading and 200KByte/s uploading. We change the dimension in Kbps as follows,

Download Speed: $1135\text{KB/s} \times 8 = 9080\text{Kbp/s}$

Upload Speed: $200\text{KB/s} \times 8 = 1600\text{Kbp/s}$

The settings can be done as below,

Bandwidth Type (Download/Upload)	Select custom °
Download Bandwidth	Enter the value to 9080 °
Upload Bandwidth	Enter the value to 1600 °
Reserved Buffering Bandwidth	User can firstly set the value about 10% and adjust this value later. If your network is very stable, you could lower this value.

8.1.2 Add SBM Rules

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

Sequence Number: 1

Rule Name:

Rule Enable: ☒

Internal IP Address:

Protocol: *

Service Port Range: From: To:

Available Bandwidth: WAN1: 3072.0/768.0 Kbps

Bandwidth Allocation: By Ratio

Ratio: %

Utilize Bandwidth More Than Guaranteed: ☐

Confirm Cancel Changes

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	By Ratio or By Bandwidth
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 confirming this SBM rule to be able to utilize the whole bandwidth when the bandwidth is idle.

3. Advanced Setting Example1

If a user needs to reserve some bandwidth for a specified application, such as VoIP, one can have the following configuration to reserve a 25Kbps/25Kbps bandwidth for VoIP application.

Sequence Number	1
Rule Name	VoIP
Rule Enable	☒
Internal IP Address	192.168.1.101
Protocol	*
Service Port Range	From: To:
External Interface	WAN1
Available Bandwidth	
WAN1:	3661.4/921.6 Kbps
WAN2:	1536.0/192.0 Kbps
Bandwidth Allocation	By Bandwidth
Download	25 Kbps
Upload	25 Kbps
Utilize Bandwidth More Than Guaranteed	☐

Confirm Cancel Changes

Rule Name	VoIP
Rule Enable	Check the box to enable this rule
Internal IP Address	Enter the IP address of the VoIP machine
Protocol	Select * will apply this rule for both TCP and UDP protocols
External Interface	Choose the WAN interface you want to use
Service Port Range	Enter the service port number that used by VoIP
Bandwidth Allocation	Allocating the bandwidth by fixed value assignment or ratio
Download	Enter the reserved download rate to 25 Kbps
Upload	Enter the reserved upload rate to 25 Kbps
Utilize Bandwidth More Than Guaranteed	Uncheck this box to reserve a fixed rate for this application; You may also check this box allowing this application use the rest(free) bandwidth when it consume more bandwidth.

4. Advanced Setting Example 2

In the case users need to guarantee a PC or a network device for a specified bandwidth and allow the user to use rest bandwidth up to some values, one may follow the settings as below.

In this case, the PC with IP address-192.168.1.1 will be guaranteed for 100Kbps/20Kbps bandwidth. Additionally, this PC can use up to 150Kbps/30Kbps if there is still any free bandwidth existed.

The screenshot shows a configuration window for a bandwidth rule. The fields are as follows:

Sequence Number	2
Rule Name	IP1_Rate
Rule Enable	☒
Internal IP Address	192.168.1.100
Protocol	*
Service Port Range	From: To:
External Interface	WAN1
Available Bandwidth	
WAN1:	3586.4/901.6 Kbps
WAN2:	1536.0/192.0 Kbps
Bandwidth Allocation	By Bandwidth
Download	100 Kbps
Upload	20 Kbps
Utilize Bandwidth More Than Guaranteed	☒
Use Maximal Download	150 Kbps
Use Maximal Upload	30 Kbps

Buttons: Confirm, Cancel Changes

Rule Name	IP1_Rate
Rule Enable	Check this box to enable this rule
Internal IP Address	Enter the IP address this rule to be applied to.
Protocol	* (Applied to both TCP and UDP)
External Interface	Select the external WAN Interface to be applied to.
Service Port Range	Applied to all port range if left this field blank
Bandwidth Allocation	Allocating the bandwidth by fixed value assignment or ratio
Download	Enter the download guaranteed value to 100 Kbps °
Upload	Enter the upload guaranteed value to 25 Kbps °
Utilize Bandwidth More Than Guaranteed	Check this box to allow the usage of free bandwidth
Use Maximal Download	Enter the limited download value to 150Kbps
Use Maximal Upload	Enter the limited upload value to 30Kbps

8.1.3 Add DBM Rule

It is very simple to set-up a DBM rule, users only need to set the IPs to be controlled in the DBM IP ranges.

After assignment of the DBM IPs, the AXIMCom's Router will dynamically control the bandwidth by equality and priority methods

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

Sequence Number

2

Rule Name

Rule Enable

☒

Internal IP Range

From: To:

Confirm

Cancel Changes

- 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.

- 3. DBMSetting Example

The maximum DBM IPs is 32 in the X-108NX. The user may set the DHCP releasing range from 192.168.2.30 to 192.168.1.45 and set those IP as DBM IP accordingly. In this manner, all user access through this router will be controlled by DBM system without any other complicated settings.

Sequence Number

2

Rule Name

SEC_A

Rule Enable

☒

Internal IP Range

From: 192.168.2.30 To: 192.168.2.45

Confirm

Cancel Changes

8.2 THROUGHPUT OPTIMIZER

AXIMCom 3G/4G X-Router built in iDBM 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 [Bandwidth] – [Throughput Optimizer] tab. You will see the following screen.

Please do not change the parameters unless you wish to customize it by yourself.

Bandwidth - Throughput Optimizer

Throughput Optimizer

Throughput Optimizer ☒ 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

2. Configure Throughput Optimizer Settings following the instructions below

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

8.3 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 X-Router to fulfill the higher speed network and to reserve the system performance for other features such as ACL and VPN servers.

In order to meet the Gigabit Ethernet requirement, AXIMCom's GbE X-Routers are supported with Hardware NAT mode. The NAT throughput can be up to 950Mbps, hence supports the Gigabit Ethernet WAN usage.

- 1. Click on [Bandwidth] – [TurboNAT] tab. You will see the following screen.

Hardware NAT

Hardware NAT

☒ Enable ☐ Disable

TurboNAT

TurboNAT

☒ Enable ☐ Disable

Save Settings

Cancel Changes

- 2. Configure [TurboNAT] Settings following the instructions below

Hardware NAT	Select Enable/Disable to enable/disable Hardware NAT
TurboNAT	Select Enable/Disable to enable/disable TurboNAT.

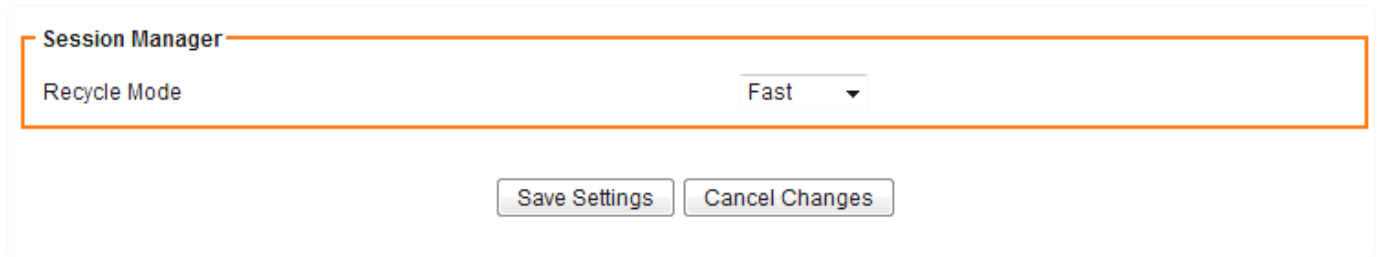
Please note that, when enable the Hardware NAT mode, some of the management features will be disabled automatically, such as iDBM, Universal Repeater and WDS functions.

8.4 SESSION MANAGER

Session manager will automatically recycle old/dead sessions to get better connection efficiency. Users can choose the recycle rate to optimize the connection efficiency especially in the application of P2P download.

1. Click on [Bandwidth] – [Session Manager] tab. You will see the following screen.

Bandwidth - Session Manager



Session Manager

Recycle Mode Fast ▼

Save Settings Cancel Changes

2. Configure [Session Manager] Settings following the instructions below

Recycle Mode	Select Fast/Regular/Slow recycle rate
--------------	---------------------------------------

CHAPTER9 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's Router 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's Router 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:

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
-----------------	---

9.1.2Add Port Range Forwarding Rule

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

Sequence Number

9

Rule Name

Rule Enable

☐

External Interface

WAN1

Protocol

TCP

External Port Range

From: To:

Internal IP

Internal Port Range

From: To:

Confirm

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 1st 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 PASS-THROUGH

You can enhance your media streaming quality by enabling RTSP, MSS, 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

[Save Settings](#) [Cancel Changes](#)

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

RTSP	Select Enable/Disable to enable/disable RTSP
MMS	Select Enable/Disable to enable/disable MMS

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

H.323	Select Enable/Disable to enable/disable H.323
-------	---

4. Configure [VPN] Settings following the instructions below

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

9.3 UPnP/NAT-PMP SETUP

- 1. Click on [Applications] – [UPnP / NAT-PMP] tab. You will see the following screen.

Applications - UPnP / NAT-PMP

UPnP

UPnP

NAT-PMP

UPnP Port

☒ Enable ☐ Disable

☐ Enable ☒ Disable

5555

Save Settings

Cancel Changes

- 2. Configure [UPnP] Settings following the instructions below

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

CHAPTER10 STORAGE FUNCTION SETTINGS

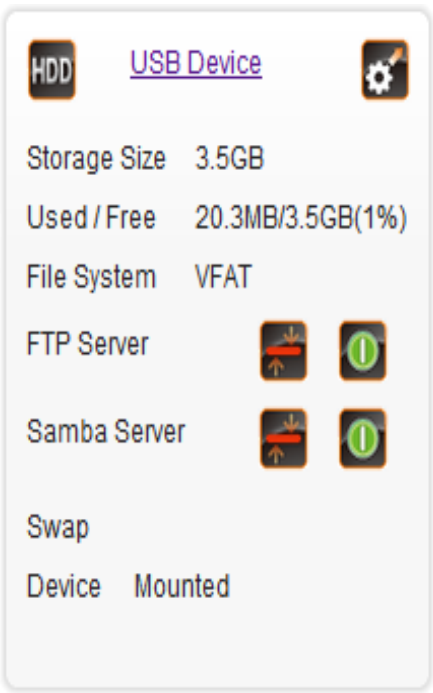
The X-Router can be operated in storage mode. User can insert an external USB storage device to enable the storage relevant function such as FTP Server, SAMBA Sever.

Please note that the setting in this chapter is not available in 3G/4G Router mode

10.1 STORAGE DEVICE

10.1.1 USB Storage Device Installation

There is a widget window shown in the setting page to indicate the information of the USB storage device.



Please refer to the following table to check your USB storage device is installed properly.

Storage Size	Indicate the capacity of your storage device
Used/Free	Indicate the current usage of the storage
File System	Current file system of your storage device. FAT and EXT3 file system can be supported in the X series router
FTP Server	Indicate the FTP Server is active or not. You may click right small button to enable/disable the service.
Samba Server	Indicate the Samba Server is active or not. You may click right small button to enable/disable the service.
Swap	Indicate the usage of the Swap file in the system
Device	Indicate the storage device is unknown, Un-mounted or Mounted

If your storage device is successfully installed in the X-Router, you will see the device information like the picture above. If the [Device] field shows unknown, you may need to format your storage device to get it worked with the X-Router.

10.1.2 Storage Formatting

1. Click on [Storage]-[Storage Device], you will see the following page.

Storage - Storage Management

Storage Device

Language

Traditional Chinese

Swap File Size

64MB

Format

File System Type

FAT

Format USB HDD

Format

Save Settings

Cancel Changes

2. Perform [Format] operation according to the instructions below

File System Type	Select the type of file system you want to use in the storage. You may choose FAT or EXT3 that supported by the system FAT file system support up to 2TB storage device and 4GB for single file. EXT3 file system support up to 8TB storage device and the single file can be bigger than 4GB.
Format	***Note: You will get lost all the data in the storage after formatting the device. Press the button to start formatting your storage device. Please note that do not detach your device during formatting. During the formatting process, the router function is suspended and the USB status LED will blink. Please be patient, especially for the large capacity device, and wait for the completion of the process.

Please note that the Windows system cannot access the EXT3 file system directly. If user wants to get access to EXT3 file system in the Windows O.S., the additional tools is needed.

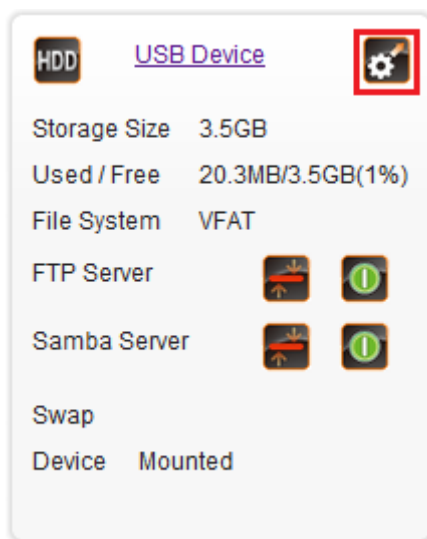
10.1.3 Ejecting of the Storage Device

When user need to remove your USB storage device, please follow the safely remove process or the data or file system in your storage can be crashed.

1. Method 1

Simply click on the remove button in the setting, the system will automatically stop all relevant service for you. After the system successfully removing you device, a [Unmounted] will show up in the [Device] field of the widget

User may un-plug the USB device this time.



2. Method 2

User can directly press the [EJECT] push button on the side of housing about 3 seconds to remove without entering the setting page. When user press the [EJECT] button, you will see the USB status LED is blinking. After the LED light is turned off, user may un-plug the USB storage device.

10.2 FTP SERVER

1. Click on [Storage]-[FTP Server], you will see the following page.

Storage - FTP Server

FTP Server

☒ Enable ☐ Disable

FTP Server Port

FTP Bandwidth

KB/s

FTP Server External Access

☐ Enable ☒ Disable

User Rule

Rule Enable

User Name

Password

Per Session Upload (KB/s)

Per Session Download (KB/s)

✓

admin

adminpassword

50

100

Add

Delete

Modify

Up

Down

Save Settings

Cancel Changes

2. User may set the FTP Server according to the instructions below

FTP Server	Check / Un-check the box to enable/disable the FTP Server
FTP Server Port	FTP service port. The default port number is 21.
FTP Bandwidth	Set the bandwidth limitation of the FTP service
FTP Server External Access	Check the enable box to allow the outside users to use this service
User Rule	Click [add] to add a new user using this service.

10.3 SAMBA SERVER

1. Click on [Storage]-[Samba Server], you will see the following page.

Storage - Samba Server

Samba Server

Samba Server

☒ Enable

☐ Disable

Samba Server Share Name

share

Samba Server Allow Guest

☒ Enable

☐ Disable

Samba Server Read Only

☐ Enable

☒ Disable

Samba Server External Access

☐ Enable

☒ Disable

Language

Traditional Chinese

▼

Samba Password

.....

Re-type Password

.....

(Default user name is admin, default password is admin)

Save Settings

Cancel Changes

2. User may set the Samba Server according to the instructions below

Samba Server	Check / Un-check the box to enable/disable the Samba Server
Samba Server Share Name	Enter the name of the directory that you want to Share
Samba Server Allow Guest	Check the enable box will allow the guest user access the share directory without using password.
Samba Server Read Only	Check the enable box to set the share directory as read only.
Samba Server External Access	Check the enable box to allow the outside users to use this service
Language	Select the correct language in order to display the file name correctly.
Samba Password	Password for login in to the Samba Sharing directory.

CHAPTER11 ADMIN

11.1 MANAGEMENT

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

Admin - Management

Mode Switch

Mode Router

Administration Interface

Language English

Administrator Password

Re-type Password

Remote Management ☐ Enable ☒ Disable

Management Port HTTP 8080

Reboot

Reboot Reboot Router

Configuration

Configuration Export Export

Default Configuration Restore Default

Configuration Import

瀏覽... Import

Firmware

Firmware Upgrade

Upgrade

瀏覽...

Save Settings

Cancel Changes

2. Configure [Mode Switch] Settings based on the instructions listed below

Mode	Select the operation mode as Router mode or NAS mode. After you saving the settings, the router will reboot and enter the working mode which you have selected.
------	--

3. 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 Enable to enable Remote Management. Select Disable to disable Remote Management If the remote management is enabled, users who are not in the LAN can connect to AXIMCom X-Router and configure it from the Internet.
Management Port	HTTP port which users can connect to. (default port is 8080)

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

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

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

Firmware Upgrade	Click Browse and Upgrade to upgrade the firmware.
------------------	---

11.2 SYSTEM UTILITIES

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

Admin - System Utilities

Ping

Interface

*

Target Host

Number of Packets

4

Packets (1 ~ 10)

Ping

Ping

ARPing (Within the same broadcasting domain)

Interface

WAN1

Target Host

Number of Packets

4

Packets (1 ~ 10)

ARPing

ARPing

Trace Route

Interface

*

Target Host

Hop Count

4

Counts (1 ~ 15)

Trace route

Trace Route

Save Settings

Cancel Changes

2. Using the [ping] tool based on the instructions listed below

Interface	Select the interface that use to ping to, ie. LAN, WAN.
Target Host	Enter the IP address to ping to
Number of Packets	Specify the number of the ICMP packets to send out
Ping	Press the tab to start the "ping" actions

3. Using the [ARPing] tool based on the instructions listed below

Interface	Select the interface that use to ARPing to, ie. LAN, WAN.
Target Host	Enter the MAC address to ARPing to
Number of Packets	Specify the number of the ARP request packets to send out
ARPing	Press the tab to start the "ARPing" actions

4. Using the [Trace Route] tool based on the instructions listed below

Interface	Select the interface that use to ARPing to, ie. WAN1, WAN2.
Target Host	Enter the destination IP address / domain name to trace
Hop Count	Specify the Hop number you need to trace
Trace route	Press the tab to start the "Trace Route" actions

11.3 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

Automatic

Time Server IP Address

Time Zone

UTC+08:00 Taiwan, China, Hong Kong, Western Australia, Singapore

Periodic Synchronization

☒ Enable ☐ Disable

Synchronization Interval

Every Day

Action

Update

Save Settings

Cancel Changes

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

Time Synchronization	Select Enable/Disable 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 Enable/Disable to enable/disable Periodic Synchronization
Synchronization interval	Select from Every Hour, Every 6 Hours, Every 12 Hours, Every Day, and Every Week.

CHAPTER12 STATUS

You can access and view all the system information regarding AXIMCom's Router from here.

12.1 ROUTER INFORMATION

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

Status - Router

Router Information

Model Name	AXIMCom Product
Firmware Version	2.0.0 (M.1)
License	Unauthorized(4)
Current Time	Mon, 08 Jun 2009 19:56:54
Running Time	5 hours, 20 mins

WAN 1

MAC Address	00:0C:43:30:52:77
Connection Type	pppoe
IP Address	118.166.47.8
Subnet Mask	32
Gateway	61.217.32.254

LAN 1

MAC Address	00:0C:43:30:52:10
IP Address	192.168.1.1
Subnet Mask	24
DHCP Service	Enabled

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 X-Router 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

12.2 USER/DHCP

1. Click on [Status] – [DHCP] 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
maede-ibook-g4	192.168.1.21	00:11:24:cd:21:1e	19:11:48
eeehp	192.168.1.23	00:1b:24:37:0a:e3	21:39:49

Refresh

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

12.3 USER/ CURRENT

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

Status - User

ARP Table (11 users)

IP Address	MAC Address	ARP Type
10.1.1.78	00:13:49:22:e3:35	Unknown
10.1.1.77	00:13:e8:35:2d:f7	Dynamic
10.1.1.66	00:1d:e0:00:e1:ab	Dynamic
10.1.1.72	00:22:43:5d:4b:02	Unknown
10.1.1.61	00:06:4f:89:34:b2	Unknown
10.1.1.79	00:06:4f:6e:5f:34	Dynamic
10.1.1.67	00:13:ce:69:c1:1d	Unknown
10.1.1.55	00:0f:66:fd:01:6b	Dynamic
10.1.1.62	00:15:00:11:6e:71	Dynamic
10.1.1.202	00:1f:d0:97:84:94	Dynamic
10.1.1.80	00:13:49:22:e3:35	Dynamic

Refresh

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

12.4 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