

WLAN 11g Broadband Router

User Manual

V 1.0



Product Name: X-Micro WLAN 11g Broadband Router

Model Name : XWL-11GRTX

This product is in compliance with the essential requirements and other relevant provisions of the R&TTE directive 1999/5/EC.

			MAX. OU	T POWER
COUNTRY		CHANNELS	INDOOR	OUTDOOR
Spain	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
France	2400-2454 MHz	1-8	< 100 mW EIRP	< 100 mW EIRP
France	2454-2483.5 MHz	9-13	< 100 mW EIRP	< 10 mW EIRP
Italy	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
UK	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Netherlands	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Germany	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Austria	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Belgium	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Switzerland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Luxemburg	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Ireland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Portugal	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Norway	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Denmark	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Finland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Iceland	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Greece	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Lichtenstein	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
Sweden	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP

((

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal. In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

X-Micro declares that US model of XWL-11GRTX, (FCC ID: RAFRTX) is limited in CH 1~ CH 11 for 2.4G band by specific firmware controlled by the manufacturer and is not user changeable.

<u>Copyright</u>

Copyright 2007 by X-Micro Technology Corp., All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of X-Micro Technology Corp.

<u>Disclaimer</u>

X-Micro Technology Corp. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, X-Micro Technology Corp., reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or change.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Table of Contents

Т	ERMINO	DLOGYI
1	INTR	ODUCTION1
	1.1 F	PACKAGE CONTENTS
	1.2 F	PRODUCT SPECIFICATIONS
	1.3 F	PRODUCT FEATURES
	1.4 F	PANEL DESCRIPTION
2	INST	ALLATION
	2.1 F	ARDWARE INSTALLATION
	2.2 8	SOFTWARE INSTALLATION
3	SOF	TWARE CONFIGURATION
	3.1 F	PREPARE YOUR PC TO CONFIGURE THE X-MICRO WLAN 11G BROADBAND ROUTER 6
	3.2 0	CONNECT TO THE X-MICRO WLAN 11G BROADBAND ROUTER
	3.3 N	ANAGEMENT AND CONFIGURATION ON THE X-MICRO WLAN 11G BROADBAND ROUTER
	8	
	3.3.1	Status
	3.3.2	Setup Wizard 10
	I	Operation Mode10
	II	Time Zone Setting
	111	LAN Interface Setup 11
	IV	WAN Interface Setup 12
	V	Wireless Basic Settings
	VI	Wireless Security Setup
	3.3.3	Operation Mode
	3.3.4	Wireless - Basic Settings
	3.3.5	Wireless - Advanced Settings
	3.3.6	Wireless - Security Setup
	I	WEP Key Setup
	3.3.7	Wireless - Access Control
	3.3.8	WDS Settings
	I	WDS Security Setup
	П	WDS AP Table
	3.3.9	Site Survey
	3.3.1	0 LAN Interface Setup

	3.3.	11	WAN Interface Setup	25
	I	S	Static IP	26
	II	[DHCP Client	27
		IF	PPoE	29
	١٧	/ F	PPTP	31
	3.3.	12	Firewall - Port Filtering	32
	3.3.	13	Firewall - IP Filtering	33
	3.3.	14	Firewall - MAC Filtering	34
	3.3.	15	Firewall - Port Forwarding	35
	3.3.	16	Firewall – URL Filtering	37
	3.3.	17	Firewall - DMZ	37
	3.3.	18	VPN Setting	38
	I	١	/PN Setup - Edit Tunnel	40
	II	ļ	Advanced IKE Setup	42
	3.3.	19	Management - Statistics	43
	3.3.	20	Management - DDNS	44
	3.3.	21	Management - Time Zone Setting	44
	3.3.	22	Management – Denial-of-Service	45
	3.3.	23	Management - Log	46
	3.3.	24	Management - Upgrade Firmware	47
	3.3.	25	Management Save/ Reload Settings	48
	3.3.	26	Management - Password Setup	49
	3.3.	27	Management - WatchDog	49
	3.3.	28	Management - Quality of Service	50
	3.3.	29	Logout	52
4	FRE	EQL	JENTLY ASKED QUESTIONS (FAQ)	53
	4.1	Wн	AT AND HOW TO FIND MY PC'S IP AND MAC ADDRESS?	53
	4.2	Wн	AT IS WIRELESS LAN?	53
	4.3	Wн	AT ARE ISM BANDS?	53
	4.4	Ho	W DOES WIRELESS NETWORKING WORK?	53
	4.5	Wн	AT IS BSSID?	54
	4.6	Wн	AT IS ESSID?	54
	4.7	Wн	AT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE?	54
	4.8	Wн	AT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS?	55
	4.9	Wн	AT IS WEP?	55
	4.10	Wн	AT IS FRAGMENT THRESHOLD?	55
	4.11	Wн	AT IS RTS (REQUEST TO SEND) THRESHOLD?	56
	4.12	Wн	AT IS BEACON INTERVAL?	56

4.13	WHAT IS PREAMBLE TYPE?5	57
4.14	WHAT IS SSID BROADCAST?	57
4.15	WHAT IS WI-FI PROTECTED ACCESS (WPA)?5	57
4.16	WHAT IS WPA2?5	57
4.17	WHAT IS 802.1X AUTHENTICATION?	
4.18	WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)?	58
4.19	WHAT IS ADVANCED ENCRYPTION STANDARD (AES)?	58
4.20	WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)?	
4.21	WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)?	58
4.22	WHAT IS UNIVERSAL PLUG AND PLAY (UPNP)?	58
4.23	WHAT IS MAXIMUM TRANSMISSION UNIT (MTU) SIZE?	59
4.24	WHAT IS CLONE MAC ADDRESS?	
4.25	WHAT IS DDNS?	
4.26	WHAT IS NTP CLIENT?	59
4.27	WHAT IS VPN?	59
4.28	WHAT IS IPSEC?	59
4.29	WHAT IS WLAN BLOCK RELAY BETWEEN CLIENTS?	59
4.30	WHAT IS WMM?	59
4.31	WHAT IS WLAN ACK TIMOUT? ϵ	50
5.1 E	XAMPLE ONE – PPPOE ON THE WAN ϵ	51
5.2 E	XAMPLE TWO – FIXED IP ON THE WAN6	53
WWW.X-	MICRO.COM	57

Terminology

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
ССК	Complementary Code Keying
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/ Collision Detection
DDNS	Dynamic Domain Name Server
DH	Diffie-Hellman Algorithm
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MD5	Message Digest 5
NAT	Network Address Translation
NT	Network Termination
NTP	Network Time Protocol
PPTP	Point to Point Tunneling Protocol
PSD	Power Spectral Density
RF	Radio Frequency
SHA1	Secure Hash Algorithm
SNR	Signal to Noise Ratio
SSID	Service Set Identification
ТСР	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UPNP	Universal Plug and Play

VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Introduction

The X-Micro Wireless LAN Broadband Router is an affordable IEEE 802.11b/g wireless LAN broadband router solution; setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN.

This document describes the steps required for the initial IP address assign and other WLAN router configuration. The description includes the implementation of the above steps.

1.1Package contents

The package of the X-Micro WLAN 11g Broadband Router includes the following items,

- ✓ X-Micro WLAN 11g Broadband Router
- ✓ DC 7.5V Power Adapter
- ✓ Quick installation Guide
- ✓ CD-ROM
- ✓ 1.8M RJ-45 Cable Line

Product Name	X-Micro WLAN 11g Broadband Router	
Standard	802.11b/g(Wireless), 802.3(10BaseT), 802.3u(100BaseT)	
Data Transfer Rate	54Mbps(Wireless), 100Mbps(Ethernet)	
Modulation Method	CCK(802.11b), OFDM(802.11g)	
Frequency Band	2.4GHz – 2.497GJz ISM Band, DSSS	
RF Output Power	CCK< 17 dBm, OFDM< 13.5 dBm	
Receiver Sensitivity	802.11b -80 dBm@8%, 802.11g -68 dBm@5%	
Operation Range	30 to 300 meters (depend on surrounding)	
Antenna	External Antenna	
LED	Power, Active (WLAN/Ethernet)	
Security	64 bit/ 128 bit WEP, WPA, WPA2, port filtering, IP filtering, MAC	
	filtering, port forwarding and DMZ hosting	
LAN interface	One (WAN) Four (LAN) , 10/100BaseT, RJ45 connectors	
Power Consumption	7.5V DC Power Adapter	
Operating Temperature	0 ~ 50°C ambient temperature	
Storage Temperature	-20 ~ 70°C ambient temperature	
Humidity	5 to 90 % maximum (non-condensing)	
Dimension	137x96x35mm	

1.2Product Specifications

1.3 Product Features

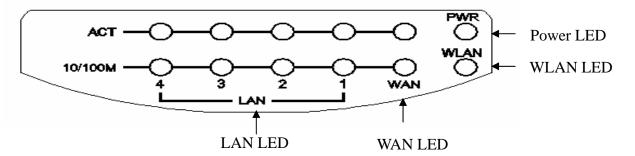
Generic Router

- Complies with IEEE 802.11b/g standard for 2.4GHz Wireless LAN.
- Supports multi-operation (bridge/gateway/WISP) modes between wireless and wired Ethernet interfaces.
- Supports 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption function to protect the wireless data transmission.
- Supports IEEE 802.1x Authentication.
- Support Wi-Fi Protected Access Authentication with Radius and Pre-Shared Key mode.
- Supports Inter-Access Point Protocol (IAPP).
- Supports Wireless Distribution System (WDS).
- Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports DHCP client for WAN interface auto IP address assignment from ISP.
- > Supports PPPoE on WAN interface.
- > Supports PPTP Client on Ethernet WAN interface.
- Supports clone MAC address function.
- Supports firewall security with port filtering, IP filtering, MAC filtering, port forwarding, trigger port, DMZ hosting and URL filtering functions.
- Supports WEB based management and configuration.
- > Supports UPnP for automatic Internet access.
- > Supports Dynamic DNS service.
- Supports NTP client service.
- > Supports Log table and remote Log service.
- Support Setup Wizard mode.
- Support DoS (Denial of Service) function.
- Support WMM function.
- Support Ping watchdog.
- Support QoS/Bandwidth Control function.

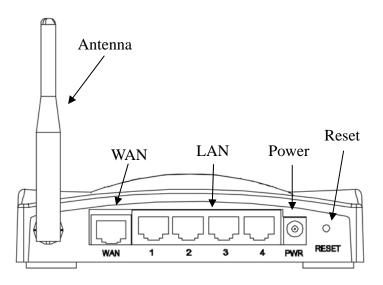
VPN Router

- Supports Virtual Private Network (VPN) connection.
- Supports IPSEC tunnel encryption(3DES/AES128) and authentication(MD5/SHA1)

1.4 Panel Description



LED Indicator	State	Description
1. Power LED	On	The X-Micro WLAN 11g Broadband Router
		is powered on.
	Off	The X-Micro WLAN 11g Broadband Router
		is powered off.
2. WLAN LED	Flashing	Data is transmitting or receiving on the
		antenna.
	Off	No data is transmitting or receiving on the
		antenna.
3. WAN LED		
ACT	Flashing	Data is transmitting or receiving on the
		WAN interface.
	Off	No data is transmitting or receiving on the
		WAN interface.
10/100M	On	Connection speed is 100Mbps on WAN
		interface.
	Off	Connection speed is 10Mbps on WAN
		interface.
4. LAN LED		
ACT	Flashing	Data is transmitting or receiving on the LAN
		interface.
	Off	No data is transmitting or receiving on the
		LAN interface.
10/100M	On	Connection speed is 100Mbps on LAN
		interface.
	Off	Connection speed is 10Mbps on LAN
		interface.



Interfaces	Description
1. Antenna	The Wireless LAN Antenna.
2. WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/
	802.3u respectively.
3. LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
4. Power	The power jack allows an external DC +7.5 V power supply connection. The external AC to DC adaptor provide adaptive power requirement to the X-Micro WLAN 11g Broadband Router.
5. Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.

2 Installation

2.1 Hardware Installation

- Step 1: Place the Wireless LAN Broadband Router to the best optimum transmission location. The best transmission location for your X-Micro WLAN 11g Broadband Router is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.
- Step 2: Connect the X-Micro WLAN 11g Broadband Router to your wired network. Connect the Ethernet WAN interface of X-Micro WLAN 11g Broadband Router by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.
- Step 3: Supply DC power to the X-Micro WLAN 11g Broadband Router. Use only the AC/DC power adapter supplied with the X-Micro WLAN 11g Broadband Router; it may occur damage by using a different type of power adapter.

The hardware installation finished.

2.2Software Installation

There are no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 3 for software configuration.

Notice: It will take about 55 seconds to complete the boot up sequence after powered on the X-Micro WLAN 11g Broadband Router; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.

3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The X-Micro WLAN 11g Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: **192.168.1.254** Default IP subnet mask: **255.255.255.0** WEB login User Name: *empty* WEB login Password: *empty*

3.1 Prepare your PC to configure the X-Micro WLAN 11g Broadband Router

For OS of Microsoft Windows 95/ 98/ Me:

- Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
 Note: Windows Me users may not see the Network control panel. If so, *select* View all Control Panel options on the left side of the window
- 2. Move mouse and double-click the right button on *Network* icon. The *Network* window will appear.
- Check the installed list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
- 4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
- Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
- 6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
- 7. Select **Specify an IP address** and type in values as following example.
 - ✓ IP Address: 192.168.1.1, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: 255.255.255.0
- 8. Click OK and reboot your PC after completes the IP parameters setting.

For OS of Microsoft Windows 2000, XP:

 Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

- Move mouse and double-click the right button on *Network and Dial-up Connections* icon. Move mouse and double-click the *Local Area Connection* icon. The *Local Area Connection* window will appear. Click *Properties* button in the *Local Area Connection* window.
- Check the installed list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
- 4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
- Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
- 6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
- 7. Select Specify an IP address and type in values as following example.
 - ✓ IP Address: 192.168.1.1, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: 255.255.255.0
- 8. Click OK to completes the IP parameters setting.

For OS of Microsoft Windows NT:

- Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
- Move mouse and double-click the right button on *Network* icon. The *Network* window will appear. Click *Protocol* tab from the *Network* window.
- Check the installed list of *Network Protocol* window. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
- 4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
- Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
- 6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
- 7. Select **Specify an IP address** and type in values as following example.
 - ✓ IP Address: 192.168.1.1, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: 255.255.255.0
- 8. Click OK to complete the IP parameters setting.
- 3.2 Connect to the X-Micro WLAN 11g Broadband Router Open a WEB browser, i.e. Microsoft Internet Explore, then enter 192.168.1.254

on the URL to connect the X-Micro WLAN 11g Broadband Router.

3.3 Management and configuration on the X-Micro WLAN 11g Broadband Router

3.3.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.

Broadband Route	or Status
Di Vauvallu Koule	i otatus
This race shows the current status a	nd some basic settings of the device.
This page shows the current status a	
System	
Uptime	Oday:Oh:23m:9s
Firmware Version	v1.4.2
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
CI 22	MyWLAN
Channel Number	11
Encryption	Disabled
DI 228	00:02:72:14:81:86
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:02:72:14:81:86
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.0.146
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.10
DNS 1	168.95.1.1
DNS 2	192.168.0.5
DNS 3	0.0.0.0
MAC Address	00:02:72:14:81:87

Screen snapshot - Status

Item

System	
Uptime	It shows the duration since X-Micro WLAN 11g Broadband Router
	is powered on.
Firmware version	It shows the firmware version of X-Micro WLAN 11g Broadband
	Router.
Wireless	
configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of this X-Micro WLAN 11g Broadband Router.
	The SSID is the unique name of X-Micro WLAN 11g Broadband
	Router and shared among its service area, so all devices
	attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the X-Micro WLAN 11g Broadband
	Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of X-Micro WLAN 11g
	Broadband Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of X-Micro WLAN
	11g Broadband Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing
	data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of X-Micro WLAN
	11g Broadband Router.
WAN configuration	
Attain IP Protocol	It shows how the X-Micro WLAN 11g Broadband Router gets the
	IP address. The IP address can be set manually to a fixed one or
	set dynamically by DHCP server or attain IP by PPPoE / PPTP
	connection.
IP Address	It shows the IP address of WAN interface of X-Micro WLAN 11g
	Broadband Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of X-Micro WLAN
	11g Broadband Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing
-	data packets.

DNS1/DNS2/DNS3	It shows the DNS server information.
MAC Address	It shows the MAC address of WAN interface of X-Micro WLAN
	11g Broadband Router.

3.3.2 Setup Wizard

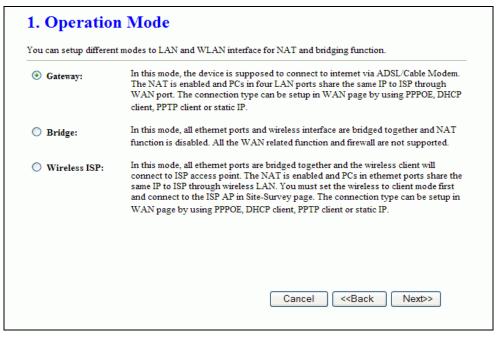
This page guides you to configure wireless broadband router for first time

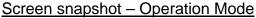
The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.					
Welcome to S	etup Wizard.				
The Wizard w	ill guide you the through	following steps.	Begin by clicking o	n Next.	
1. Setup	Operation Mode				
	e your Time Zone				
Setup	AN Interface				
	WAN Interface				
	ss LAN Setting				
6. Wirele	ss Security Setting				

Screen snapshot – Setup Wizard

I Operation Mode

This page followed by Setup Wizard page to define the operation mode.





II Time Zone Setting

This page is used to enable and configure NTP client

Enable NTP client	t update
Time Zone Select :	(GMT+08:00)Taipei
NTP server :	192.5.41.41 - North America 👻

Screen snapshot - Time Zone Settings

III LAN Interface Setup

This page is used to configure local area network IP address and subnet mask

		area network which connects to the LAN port of your addresss, subnet mask, DHCP, etc
IP Address:	192.168.1.254]
Subnet Mask:	255.255.255.0	
		1
		Cancel < <back next="">></back>

<u>Screen snapshot – LAN Interface Setup</u>

IV WAN Interface Setup

This page is used to configure WAN access type

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.		
WAN Access Type:	DHCP Client	

<u>Screen snapshot – WAN Interface Setup</u>

V Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone(Single Ethernet Client)

Band:	2.4 GHz (G)
Mode:	AP 🗸
Network Type:	Infrastructure 🗸
: D :	MyWLAN
Channel Number:	11 💌

Screen snapshot – Wireless Basic Settings

VI Wireless Security Setup

This page is used to configure wireless security

	any unauthorized		VPA by using End	ryption Keys
Encryption:	None 🗸]		

<u>Screen snapshot – Wireless Security Setup</u>

3.3.3 Operation Mode

This page is used to configure which mode wireless broadband router acts

ou can setup differen	t modes to LAN and WLAN interface for NAT and bridging function.
Sateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
O Bridge:	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
O Wireless ISP:	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Apply Change	Reset

Screen snapshot – Operation Mode

Item	Description
Gateway	Traditional gateway configuration. It always
	connects internet via ADSL/Cable Modem. LAN
	interface, WAN interface, Wireless interface, NAT
	and Firewall modules are applied to this mode

Bridge	Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported
Wireless ISP	Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface
	can do all router's functions
Apply Changes	Click the Apply Changes button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

3.3.4 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Broadband Router. Here you may change wireless encryption settings as well as wireless network parameters.

	nfigure the parameters for wireless LAN clients which may connect to e you may change wireless encryption settings as well as wireless
Disable Wireless	LAN Interface
Band:	2.4 GHz (B+G) 💌
Mode:	
Network Type:	Infrastructure 😪
SSID:	MyWLAN
Channel Number:	11 💌
Associated Clients:	Show Active Clients
Enable Mac Clor	e (Single Ethernet Client)
Enable Universal	Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Inte	rface:

Screen snapshot – Wireless Basic Settings

Item	Description
Disable Wireless LAN	Click on to disable the wireless LAN data
Interface	transmission.
Band	Click to select 2.4GHz(B) / 2.4GHz(G) /
	2.4GHz(B+G)
Mode	Click to select the WLAN AP / Client / WDS /
	AP+WDS wireless mode.
Site Survey	The Site Survey button provides tool to scan the
	wireless network. If any Access Point or IBSS is
	found, you could choose to connect it manually
	when client mode is enabled. Refer to <u>3.3.9 Site</u> Survey.
SSID	It is the wireless network name. The SSID can be 32
	bytes long.
Channel Number	Select the wireless communication channel from
	pull-down menu.
Associated Clients	Click the Show Active Clients button to open Active
	Wireless Client Table that shows the MAC address,
	transmit-packet, receive-packet and
	transmission-rate for each associated wireless client.
Enable Mac Clone	Take Laptop NIC MAC address as wireless client
(Single Ethernet Client)	MAC address. [Client Mode only]
Enable Universal Repeater Mode	Click to enable Universal Repeater Mode
SSID of Extended	Assign SSID when enables Universal Repeater
Interface	Mode.
Apply Changes	Click the <i>Apply Changes</i> button to complete the
APPly Undergeo	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.
	and providuo configuration octaing.

3.3.5 Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your X-Micro WLAN 11g Broadband Router.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○Open System ○ Shared Key ⊙ Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto 🗸
Preamble Type:	O Long Preamble ○ Short Preamble
Broadcast SSID:	
IAPP:	
802.11g Protection:	
RF Output Po we r:	⊙ 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	O Auto O Always Off Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.
Block Relay Between Clients:	O Enabled 💿 Disabled
WMM:	○ Enabled ③ Disabled
ACK Timeout:	0 (0-255) < Current: 11b: 316us / 11g: 72us >
Apply Changes Reset	

Screen snapshot – Wireless Advanced Settings

Item	Description
Authentication Type	Click to select the authentication type in Open
	System, Shared Key or Auto selection.
Fragment Threshold	Set the data packet fragmentation threshold, value
	can be written between 256 and 2346 bytes.
	Refer to 4.10 What is Fragment Threshold?
RTS Threshold	Set the RTS Threshold, value can be written
	between 0 and 2347 bytes.
	Refer to 4.11 What is RTS(Request To Send)
	Threshold?
Beacon Interval	Set the Beacon Interval, value can be written
	between 20 and 1024 ms.
	Refer to 4.12 What is Beacon Interval?
Data Rate	Select the transmission data rate from pull-down
	menu. Data rate can be auto-select, 11M, 5.5M, 2M
	or 1Mbps.
Preamble Type	Click to select the Long Preamble or Short
	Preamble support on the wireless data packet

Refer to 4.13 What is Preamble	
	A
Broadcast SSID Click to enable or disable the S	SID broadcast
function.	
Refer to 4.14 What is SSID Bro	adcast?
IAPP Click to enable or disable the IA	APP function.
Refer to 4.20 What is Inter-Acc	<u>ess Point</u>
Protocol(IAPP)?	
802.11g Protection Protect 802.11b user.	
RF Output Power To adjust transmission power le	evel.
Turbo Mode Click to Enable/Disable turbo m	node.(Only apply to
WLAN IC of Realtek).	
Block Relay Between Click Enabled/Disabled to decide	de if blocking relay
Clients packets between clients.	
WMM Click Enabled/Disabled to init V	VMM feature.
ACK Timeout Set ACK timeout value. It show	s current time in the
end.	
Apply Changes Click the Apply Changes butto	on to complete the
new configuration setting.	
Reset Click the <i>Reset</i> button to abort	change and recover
the previous configuration setting	ng.

3.3.6 Wireless - Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

ncryption: None	Set WEP Key
Use 802.1x Authentication	WEP 64bits
WPA Authentication Mode:	O Enterprise (RADIUS) 💿 Personal (Pre-Shared Key)
Pre-Shared Key Format:	Passphrase 💙
Pre-Shared Key:	
Enable Pre-Authentication	
Authentication RADIUS Server:	Port 1812 IP address Password
Note: When encryption WEP is sele	cted, you must set WEP key value.

Screen snapshot – Wireless Security Setup

Item	Description	
Encryption	Select the encryption supported over wireless	
	access. The encryption method can be None, WEP,	
	WPA(TKIP), WPA2 or WPA2 Mixed	
	Refer to <u>4.9 What is WEP?</u>	
	4.15 What is Wi-Fi Protected Access (WPA)?	
	4.16 What is WPA2(AES)?	
	4.17 What is 802.1X Authentication?	
	4.18 What is Temporal Key Integrity Protocol	
	(TKIP)? 4.19 What is Advanced Encryption Standard	
	<u>(AES)?</u>	
Use 802.1x	While Encryption is selected to be WEP.	
Authentication	Click the check box to enable IEEE 802.1x	
	authentication function.	
	Refer to 4.16 What is 802.1x Authentication?	
WPA Authentication	While Encryption is selected to be WPA.	
Mode	Click to select the WPA Authentication Mode with	
	Enterprise (RADIUS) or Personal (Pre-Shared Key).	
	Refer to 4.15 What is Wi-Fi Protected Access	
	<u>(WPA)?</u>	
Pre-Shared Key	While Encryption is selected to be WPA.	
Format	Select the Pre-shared key format from the pull-down	
	menu. The format can be Passphrase or Hex (64	
	characters). [WPA, Personal(Pre-Shared Key)	
	only]	
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared	
	Key) only]	
Enable	Click to enable Pre-Authentication. [WPA2/WPA2	
Pre-Authentication	Mixed only, Enterprise only]	
Authentication	Set the IP address, port and login password	
RADIUS Server	information of authentication RADIUS sever.	
Apply Changes	Click the Apply Changes button to complete the	
	new configuration setting.	
Reset	Click the <i>Reset</i> button to abort change and recover	
	the previous configuration setting.	

WEP Key Setup

I

This page allows you setu;	EP Key Setup p the WEP key value. You could choose use 64-bit or 128-bit as the encryption Hex as the format of input value.
	-
Key Length:	64-bit 🖌
Key Format:	Hex (10 characters) 🔽
Default Tx Key:	Key 1 🔽
Encryption Key 1:	****
Encryption Key 2:	****
Encryption Key 3:	****
Encryption Key 4:	****
Apply Changes	Close Reset

Screen snapshot – WEP Key Setup

Item	Description
Key Length	Select the WEP shared secret key length from
	pull-down menu. The length can be chose between
	64-bit and 128-bit (known as "WEP2") keys.
	The WEP key is composed of initialization vector (24
	bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from
	pull-down menu. The format can be chose between
	plant text (ASCII) and hexadecimal (HEX) code.
Default Tx Key	Set the default secret key for WEP security function.
	Value can be chose between 1 and 4.
Encryption Key 1	Secret key 1 of WEP security encryption function.
Encryption Key 2	Secret key 2 of WEP security encryption function.
Encryption Key 3	Secret key 3 of WEP security encryption function.
Encryption Key 4	Secret key 4 of WEP security encryption function.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Close	Click to close this WEP Key setup window.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

WEP encryption key (secret key) length:

Length Format	64-bit	128-bit
ASCII	5 characters	13 characters
HEX	10 hexadecimal codes	26 hexadecimal codes

3.3.7 Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.			
Wireless Access Control M	Allow Listed	•	
MAC Address:	Comment:		
Apply Changes	Reset		
Current Access Control Lis	t:		
MAC Add	ess	Comment	Select
00:02:72:81:	86:01	ST-1	

Screen snapshot – Wireless Access Control

Item	Description
Wireless Access	Click the Disabled , Allow Listed or Deny Listed of
Control Mode	drop down menu choose wireless access control mode.
	This is a security control function; only those clients
	registered in the access control list can link to this
	X-Micro WLAN 11g Broadband Router.
MAC Address	Fill in the MAC address of client to register this
	X-Micro WLAN 11g Broadband Router access
	capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the Apply Changes button to register the client to new configuration setting.

Reset	Click the Reset button to abort change and recover the previous configuration setting.
Current Access	It shows the registered clients that are allowed to
Control List	link to this X-Micro WLAN 11g Broadband Router.
Delete Selected	Click to delete the selected clients that will be access right removed from this X-Micro WLAN 11g
	Broadband Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.3.8 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.

t MAC address of other APs whic	Ethemet does. To do ch you want to	
Add WDS AP: MAC Address Comment		
Apply Changes Reset Set Security Show Statistics		
Comment	Select	
AP-1		
AP-2		
	Comment Show Statistics Comment AP-1	

Screen snapshot – WDS Setup

Item	Description
Enable WDS	Click the check box to enable wireless distribution
	system. Refer to 4.21 What is Wireless Distribution
	System (WDS)?
MAC Address	Fill in the MAC address of AP to register the wireless
	distribution system access capability.

Comment	Fill in the comment tag for the registered AP.
Apply Changes	Click the Apply Changes button to register the AP
	to new configuration setting.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.
Set Security	Click button to configure wireless security like
	WEP(64bits), WEP(128bits), WPA(TKIP),
	WPA2(AES) or None
Show Statistics	It shows the TX, RX packets, rate statistics
Delete Selected	Click to delete the selected clients that will be
	removed from the wireless distribution system.
Delete All	Click to delete all the registered APs from the
	wireless distribution system allowed list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

I WDS Security Setup

Requirement: Set [Wireless]->[Basic

Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs. Refer to <u>3.3.6 Wireless Security Setup</u>.

	the wireless security for WDS. When enabled, you must make adopted the same encryption algorithm and Key.
Encryption:	None
WEP Key Format:	ASCII (5 characters) 👻
WEP Key:	****
Pre-Shared Key Format:	Passphrase 👻
Pre-Shared Key:	

Screen snapshot - WDS Security Setup

II WDS AP Table

This page is used to show WDS statistics

his table shows the MAC address, transmission, receiption packet counters and state formation for each configured WDS AP.				
MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
00:02:72:81:86:0a	22	0	0	1
00:02:72:81:86:0b	22	14	0	1

Screen snapshot – WDS AP Table

Item	Description
MAC Address	It shows the MAC Address within WDS.
Tx Packets	It shows the statistic count of sent packets on the wireless LAN interface.
Tx Errors	It shows the statistic count of error sent packets on the Wireless LAN interface.
Rx Packets	It shows the statistic count of received packets on the wireless LAN interface.
Tx Rare (Mbps)	It shows the wireless link rate within WDS.
Refresh	Click to refresh the statistic counters on the screen.
Close	Click to close the current window.

3.3.9 Site Survey

This page is used to view or configure other APs near yours.

nanually when client mode is e	the wireless network. If any A mabled.		шоо в 100			
CII 22	CI 228	Channel	Туре	Encrypt	Signal	Select
MyWLAN	00:02:72:00:81:86	11 (B+G)	AP	no	90	0
linux-wlan	00:02:72:f1:02:ad	6 (B)	AP	no	76	0
RTL8186-VPN-GW	00:e0:4c:81:86:23	11 (B+G)	AP	no	66	0
Sales	00:02:72:04:68:92	11 (B)	AP	yes	53	0
Tekom_Office	00:02:72:00:93:fb	9 (B)	AP	yes	35	0
alex	d6:4c:fc:0d:2a:d4	1 (B)	Ad hoc	no	32	0
MyWLAN	00:02:72:85:15:99	11 (B+G)	AP	no	32	0

Screen snapshot – Wireless Site Survey

Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Туре	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Select	Click to select AP or client you'd like to connect.
Refresh	Click the <i>Refresh</i> button to re-scan site survey on
	the screen.
Connect	Click the Connect button to establish connection.

3.3.10 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your X-Micro WLAN 11g Broadband Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.

	gure the parameters for local area network which connects to the Point. Here you may change the setting for IP addresss, subnet
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server 💌
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
DNS Server:	
Domain Name:	
802.1d Spanning Tree:	Disabled 💌
Clone MAC Address:	0000000000

Screen snapshot – LAN Interface Setup

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN
	Access Point.

Subnet Mask	Fill in the subnet mask of LAN interfaces of this
	WLAN Access Point.
Default Gateway	Fill in the default gateway for LAN interfaces out
	going data packets.
DHCP	Click to select Disabled , Client or Server in
	different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to
	allocate a range of IP addresses; client with DHCP
	function set will be assigned an IP address from the
	range.
Show Client	Click to open the Active DHCP Client Table window
	that shows the active clients with their assigned IP
	address, MAC address and time expired
	information. [Server mode only]
DNS Server	information. [Server mode only] Manual setup DNS server IP address.
DNS Server Domain Name	
	Manual setup DNS server IP address.
	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients.
Domain Name	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field.
Domain Name 802.1d Spanning	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d
Domain Name 802.1d Spanning Tree	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Domain Name 802.1d Spanning Tree	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. Fill in the MAC address that is the MAC address to
Domain Name 802.1d Spanning Tree	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Refer to <u>4.24 What is Clone MAC</u>
Domain Name 802.1d Spanning Tree Clone MAC Address	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Refer to <u>4.24 What is Clone MAC</u> <u>Address?</u>
Domain Name 802.1d Spanning Tree Clone MAC Address	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Refer to <u>4.24 What is Clone MAC</u> <u>Address?</u> Click the Apply Changes button to complete the
Domain Name 802.1d Spanning Tree Clone MAC Address Apply Changes	Manual setup DNS server IP address. Assign Domain Name and dispatch to DHCP clients. It is optional field. Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. Fill in the MAC address that is the MAC address to be cloned. Refer to <u>4.24 What is Clone MAC</u> <u>Address?</u> Click the Apply Changes button to complete the new configuration setting.

3.3.11 WAN Interface Setup

This page is used to configure the parameters for wide area network that connects to the WAN port of your X-Micro WLAN 11g Broadband Router. Here you may change the access method to *Static IP*, *DHCP*, *PPPoE* or *PPTP* by click the item value of **WAN Access Type**.

I Stat	Static IP	
WAN Interfac	ce Setup	
	re the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE or PPTP by click the item value of	
WAN Access Type:	Static IP	
IP Address:	172.1.1.1	
Subnet Mask:	255.255.255.0	
Default Gateway:	172.1.1.254	
MTU Size:	1400 (1400-1500 bytes)	
DNS 1:	168.95.1.1	
DNS 2:	192.168.0.5	
DNS 3:	0.0.0.0	
Clone MAC Address:	0000000000	
Enable uPNP		
Enable Ping Acces	ss on WAN	
Enable Web Serve	r Access on WAN	
Enable IPsec pass	through on VPN connection	
Enable PPTP pass	through on VPN connection	
Enable L2TP pass	through on VPN connection	
🔲 Set TTL Value	64 (1-128)	
Apply Changes Re	6381	
<u> </u>		

Screen snapshot - WAN Interface Setup - Static IP

Item	Description
Static IP	Click to select Static IP support on WAN interface.
	There are IP address, subnet mask and default
	gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface,
	fill in the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface,
	fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface,
	fill in the default gateway for WAN interface out
	going data packets.
MTU Size	Fill in the mtu size of MTU Size. The default value is
	1400
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned. Refer to 4.24 What is Clone MAC
	Address?
Enable uPNP	Click the checkbox to enable uPNP function.
	Refer to 4.22 What is Universal Plug and Play
	<u>(uPNP)?</u>

Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable WAN Echo	Click the checkbox to enable WAN ICMP response.
Reply	
Enable IPsec pass	Click the checkbox to enable IPSec packet pass
through on VPN	through
connection	
Enable PPTP pass	Click the checkbox to enable PPTP packet pass
through on VPN	through
connection	
Enable L2TP pass	Click the checkbox to enable L2TP packet pass
through on VPN	through
connection	
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

II DHCP Client

WAN Interface Setup This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.		
WAN Access Type:	DHCP Client 🖌	
Host Name:		
MTU Size:	1400 (1400-1492 bytes)	
Attain DNS Automa	tically	
O Set DNS Manually		
DNS 1:	168.95.1.1	
DNS 2:	192.168.0.5	
DNS 3:	0.0.0	
Clone MAC Address:	0000000000	
📃 Enable uPNP		
Enable Ping Acces	s on WAN	
📃 Enable Web Serve	Access on WAN	
-	through on VPN connection	
	through on VPN connection	
Enable L2TP pass through on VPN connection		
Set TTL Value 64 (1-128)		
Apply Changes Re	set	

Screen snapshot - WAN Interface Setup - DHCP Client

Item	Description
DHCP Client	Click to select DHCP support on WAN interface for
	IP address assigned automatically from a DHCP

	server.
Host Name	Fill in the host name of Host Name. The default
	value is empty
MTU Size	Fill in the mtu size of MTU Size. The default value is
	1400
Attain DNS	Click to select getting DNS address for DHCP
Automatically	support. Please select Set DNS Manually if the
	DHCP support is selected.
Set DNS Manually	Click to select getting DNS address for DHCP
	support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned. Refer to <u>4.24 What is Clone MAC</u>
	Address?
Enable uPNP	Click the checkbox to enable uPNP function.
	Refer to 4.22 What is Universal Plug and Play
	<u>(uPNP)?</u>
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable WAN Echo	Click the checkbox to enable WAN ICMP response.
Reply	
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the providue configuration actting
	the previous configuration setting.

III F	PPPoE
-------	-------

WAN Access Type:	PPPoE 🗸
User Name:	
Password:	
Service Name:	
Connection Type:	Continuous Connect Disconnect
Idle Time:	5 (1-1000 minutes)
MTU Size:	1400 (1360-1492 bytes)
O Attain DNS Automa	atically
Set DNS Manually	
DNS 1:	168.95.1.1
DNS 2:	192.168.0.5
DNS 3:	0.0.0.0
Clone MAC Address:	0000000000
🔲 Enable uPNP	
Enable Ping Acces	s on WAN
Enable Web Serve	r Access on WAN
	through on VPN connection
	through on VPN connection
Enable L2TP pass	through on VPN connection

Screen snapshot - WAN Interface Setup - PPPoE

Item	Description
PPPoE	Click to select PPPoE support on WAN interface.
	There are user name, password, connection type
	and idle time settings need to be done.
User Name	If you select the PPPoE support on WAN interface,
	fill in the user name and password to login the
	PPPoE server.
Password	If you select the PPPoE support on WAN interface,
	fill in the user name and password to login the
	PPPoE server.
Service Name	Fill in the service name of Service Name. The
	default value is empty.
Connection Type	Select the connection type from pull-down menu.
	There are <i>Continuous</i> , <i>Connect on Demand</i> and
	<i>Manual</i> three types to select.
	Continuous connection type means to setup the
	connection through PPPoE protocol whenever this
	X-Micro WLAN 11g Broadband Router is powered
	on.
	Connect on Demand connection type means to

	setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set. <i>Manual</i> connection type means to setup the connection through the PPPoE protocol by clicking the <i>Connect</i> button manually, and clicking the <i>Disconnect</i> button manually.
Idle Time	If you select the PPPoE and Connect on Demand
	connection type, fill in the idle time for
	auto-disconnect function. Value can be between 1
	and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is
	1400. Refer to 4.23 What is Maximum Transmission
	Unit (MTU) Size?
Attain DNS	Click to select getting DNS address for PPPoE
Automatically	support. Please select Set DNS Manually if the
	PPPoE support is selected.
Set DNS Manually	Click to select getting DNS address for Static IP
	support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned. Refer to <u>4.24 What is Clone MAC</u>
	Address?
Enable uPNP	Click the checkbox to enable uPNP function.
	Refer to 4.22 What is Universal Plug and Play
	<u>(uPNP)?</u>
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable WAN Echo	Click the checkbox to enable WAN ICMP response.
Reply	
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the <i>Apply Changes</i> button to complete the
	new configuration setting.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.

IV PPTP

WAN Access Type:	PPTP 🗸
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	
MTU Size:	1400 (1400-1460 bytes)
🔲 Request MPPE Er	acryption
O Attain DNS Anton	atically
 Attain DNS Autom Set DNS Manually 	
 Attain DNS Autom Set DNS Manually DNS 1: 	
Set DNS Manually	
• Set DNS Manually DNS 1:	168.95.1.1
Set DNS Manually DNS 1: DNS 2:	168.95.1.1 192.168.0.5 0.0.0.0
• Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address:	168,95.1.1 192.168.0.5
 Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: Enable uPNP 	168.95.1.1 192.168.0.5 0.0.0.0 000000000000
Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: Enable uPNP Enable Ping Acce	168.95.1.1 192.168.0.5 0.0.0.0 000000000000
Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: Enable uPNP Enable Ping Acce Enable Web Serve	168.95.1.1 192.168.0.5 0.0.0.0 00000000000
Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: Enable uPNP Enable Ping Acce Enable Web Serve Enable IPsec pass	168.95.1.1 192.168.0.5 0.0.0.0 00000000000 ss on WAN er Access on WAN
Set DNS Manually DNS 1: DNS 2: DNS 3: Clone MAC Address: Enable uPNP Enable Ping Acce Enable Web Serve Enable IPsec pass Enable PPTP pas:	168.95.1.1 192.168.0.5 0.0.00 00000000000 ss on WAN er Access on WAN through on VPN connection

Screen snapshot – WAN Interface Setup – PPTP

Item	Description
PPTP	Allow user to make a tunnel with remote site directly
	to secure the data transmission among the
	connection. User can use embedded PPTP client
	supported by this router to make a VPN connection.
IP Address	If you select the PPTP support on WAN interface, fill
	in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill
	in the subnet mask for it.
Server IP Address	Enter the IP address of the PPTP Server.
User Name	If you select the PPTP support on WAN interface, fill
	in the user name and password to login the PPTP
	server.
Password	f you select the PPTP support on WAN interface, fill
	in the user name and password to login the PPTP
	server.
MTU Size	Fill in the mtu size of MTU Size. The default value is
	1400. Refer to 4.23 What is Maximum Transmission
	Unit (MTU) Size?
Request MPPE	Click the checkbox to enable request MPPE

Encryption	encryption.
Attain DNS	Click to select getting DNS address for PPTP
Automatically	support. Please select Set DNS Manually if the
	PPTP support is selected.
Set DNS Manually	Click to select getting DNS address for PPTP
	support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to
	be cloned. Refer to <u>4.24 What is Clone MAC</u>
	Address?
Enable uPNP	Click the checkbox to enable uPNP function.
	Refer to 4.22 What is Universal Plug and Play
	<u>(uPNP)?</u>
Enable Web Server	Click the checkbox to enable web configuration from
Access on WAN	WAN side.
Enable WAN Echo	Click the checkbox to enable WAN ICMP response.
Reply	
Set TTL value	Click to Enable and set Time to Live value.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.3.12 Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Port Filtering			
Entries in this table are used to re through the Gateway. Use of such			
Enable Port Filtering			
Port Range:	Protocol: Both 🎽 Con	ament:	
Apply Changes Re	set		
Current Filter Table:			
Port Range	Protocol	Comment	Select
20-21	TCP+UDP	FTP	
Delete Selected D	elete All Reset		

Screen snapshot - Firewall - Port Filtering

Item	Description	
Enable Port Filtering	Click to enable the port filtering security function.	
Port Range	To restrict data transmission from the local network	
Protocol	on certain ports, fill in the range of start-port and	
Comments	end-port, and the protocol, also put your comments on it.	
	The <i>Protocol</i> can be TCP, UDP or Both.	
	Comments let you know about whys to restrict data	
	from the ports.	
Apply Changes	Click the Apply Changes button to register the ports	
	to port filtering list.	
Reset	Click the <i>Reset</i> button to abort change and recover	
	the previous configuration setting.	
Delete Selected	Click to delete the selected port range that will be	
	removed from the port-filtering list.	
Delete All	Click to delete all the registered entries from the	
	port-filtering list.	
Reset	Click the <i>Reset</i> button to abort change and recover	
	the previous configuration setting.	

3.3.13 Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

IP Filtering Entries in this table are used to re through the Gateway. Use of suc			
Enable IP Filtering Loal IP Address: Apply Changes Re	Protocol: Both 🗸 Con	iment:	
Current Filter Table:			
Local IP Address	Protocol	Comment	Select
192.168.1.201	TCP+UDP	ST-1	
192.168.1.202	TCP	ST-2	
Delete Selected	elete All Reset		

Screen snapshot - Firewall - IP Filtering

Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address	To restrict data transmission from local network on
Protocol	certain IP addresses, fill in the IP address and the
Comments	protocol, also put your comments on it.
	The <i>Protocol</i> can be TCP, UDP or Both.
	Comments let you know about whys to restrict data
	from the IP address.
Apply Changes	Click the Apply Changes button to register the IP
	address to IP filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be
	removed from the IP-filtering list.
Delete All	Click to delete all the registered entries from the
	IP-filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.3.14 Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

MAC Filtering		
Entries in this table are used to restrict certain types of through the Gateway. Use of such filters can be helpful		
Enable MAC Filtering MAC Address: Comment:		
Apply Changes Reset		
Current Filter Table: MAC Address	Comment	Select
00:02:72:00:81:90	ST-1	
00:02:72:00:81:91	ST-2	
Delete Selected Delete All Rese	ət	

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address	To restrict data transmission from local network on
Comments	certain MAC addresses, fill in the MAC address and
	your comments on it.
	Comments let you know about whys to restrict data
	from the MAC address.
Apply Changes	Click the Apply Changes button to register the MAC
	address to MAC filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be
	removed from the MAC-filtering list.
Delete All	Click to delete all the registered entries from the
	MAC-filtering list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.3.15 Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwardi	ng				
Entries in this table allow y the NAT firewall. These set mail server on the private lo	ttings are only necessar	ry if you wish to host s	some sort of server like		
Enable Port Forwardin	ıg				
IP Address:	Protocol: Both 💌	Port Range:	Comment:		
Apply Changes	Reset				
Current Port Forwarding T	able:				
Local IP Address	Protocol	Port Range	Comment	Select	
192.168.1.201	TCP+UDP	20-21	FTP		
Delete Selected	Delete All	Reset			

Item	Description
Enable Port	Click to enable the Port Forwarding security
Forwarding	function.
IP Address	To forward data packets coming from WAN to a
Protocol	specific IP address that hosted in local network
Port Range	behind the NAT firewall, fill in the IP address,
Comment	protocol, port range and your comments.
	The <i>Protocol</i> can be TCP, UDP or Both.
	The <i>Port Range</i> for data transmission.
	Comments let you know about whys to allow data
	packets forward to the IP address and port number.
Apply Changes	Click the Apply Changes button to register the IP
	address and port number to Port forwarding list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected IP address and port
	number that will be removed from the
	port-forwarding list.
Delete All	Click to delete all the registered entries from the
	port-forwarding list.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.3.16 Firewall – URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.

URL Filtering		
URL filter is used to deny LAN users from accessing the internet. Block th eywords listed below.	1088 URLs which contain	
Enable URL Filtering		
URL Address: WWW.url-filter-list.com		
Apply Changes Reset		
Current Filter Table:		
URL Address	Select	
www.url-filter-list.com		
Delete Selected Delete All Reset		

Screen snapshot - Firewall - URL Filtering

Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address.

Apply Changes	Click the Apply Changes button to save settings.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.
Delete Selected	Click to delete the selected URL address that will be
	removed from the URL Filtering list.
Delete All	Click to delete all the registered entries from the
	URL Filtering list.
Reset	Click the Reset button to abort change and recover
	the previous configuration setting.

3.3.17 Firewall - DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ	
	vide Internet services without sacrificing unauthorized access to its local Z host contains devices accessible to Internet traffic, such as Web (HTTP)
servers, FTP servers, SMTP (e-mail)	
Enable DMZ	
DMZ Host IP Address: 192.168.1.2	201
Apply Changes Rese	at l

Screen snapshot - Firewall - DMZ

Item	Description
Enable DMZ	Click to enable the DMZ function.
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.
Apply Changes	Click the <i>Apply Changes</i> button to register the IP address of DMZ host.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.3.18 VPN Setting

This page is used to show VPN connection table, configure IPSEC VPN, NAT Traversal, Generate RSA Key, Show RSA Public Key.

Enable IPSEC VPN Apply Changes		Enable NAT Traversal		Generate RSA Key Show RSA Public Key			
urt	nt V	PN Connect	ion Table	:: WAN IP:19	2.168.3.254		
	ŧ	Name	Active	Local Address	Remote Address	Remote Gateway	Status
•	1	site5	Y	192.168.1.0/24	192.168.4.0/24	192.168.3.1	Connected
•	2	-	-	-	-	-	-
0	3	-	-	-	-	-	-
0	4	-	-	-	-	-	-
0	5	-	-	-	-	-	-
•	6	-	-	-	-	-	-
•	7	-	-	-	-	-	-
•	8	-	-	-	-	-	-
•	9	-	-	-	-	-	-
	10	-	-	-	-	-	-

Screen snapshot – VPN Setup

Item	Description	
Enable IPSEC VPN	Click to enable IPSEC VPN function. Refer to 4.27	
	What is VPN? and 4.28 What is IPSEC?	
Enable NAT	Click to enable NAT Traversal function.	
Traversal		
Generate RSA Key	Click to generate RSA key.	
Show RSA Public	Click to show RSA public key that we generate.	
Key		
Apply Changes	Click the Apply Changes button to enable IPSEC	
	VPN, NAT Traversal settings.	
Current VPN	It shows current WAN interface information and VPN	
Connection Table	connection table.	
Edit	Click to enter the current VPN tunnel configuration	
	page.	
Delete	Click to delete the current VPN tunnel that radio	
	button stay.	
Refresh	Click to refresh the current VPN connection table.	

I VPN Setu	VPN Setup - Edit Tunnel		
VPN Setup	VPN Setup		
🗹 Enable Tunnel 1			
Connection Name:	site5		
Auth Type:	PSK 🗸		
Local Site:	Submet Address 🗸		
Local IP Address/Network	192.168.1.0		
Local Subnet Mask	255.255.255.0		
Remote Site:	Submet Address 🗸		
Remote Secure Gateway	192.168.3.1		
Remote IP Address/Network	192.168.4.0		
Remote Subnet Mask	255.255.255.0		
Local/Peer ID:			
Local ID Type			
Local \mathbb{D}			
Remote ID Type			
Remote ID			

Screen snapshot - VPN Setup-Edit-1

Item	Description	
Enable Tunnel #	Click to enable the IPSEC VPN current tunnel.	
Connection Name	Assign the connection name tag.	
Auth Type	Click to select PSK or RSA .	
Local Site	Click to select Single Address or Subnet Address	
	VPN connection.	
Local IP	Fill in IP address or subnet address depends on	
Address/Network	which Local Site option you choose.	
Local Subnet Mask	Fill in the local subnet mask.	
Remote Site	Click to select Single Address, Subnet Address,	
	Any Address or NAT-T Any Address VPN remote	
Remote Secure	connection.	
Gateway	Fill in remote gateway IP address	
Remote IP		
Address/Network	Fill in IP address or subnet address depends on	
Remote Subnet	which Remote Site option you choose.	
Mask	Fill in remote subnet mask	
Local/Peer ID	Define IKE exchange information type	
Local ID Type	Click to select IP, DNS or E-mail as local exchange	
Local ID	type	
Remote ID Type	Fill in local ID except IP selected	
	Click to select IP, DNS or E-mail as remote	
Remote ID	exchange type	
	Fill in remote ID except IP selected	

Key Management:	
Connection Type	Responder V Connect Disconnect
ESP	3DES 🕑 (Encryption Algorithm)
	MD5 💙 (Authentication Algorithm)
PreShared Key	1234567
Remote RSA Key	
Status	Connected
Apply Changes Reset	Refresh Back

Screen snapshot – VPN Setup-Edit-2

Item	Description	
Key Management	Click to select <i>IKE</i> or <i>Manual</i> mode.	
Advanced	Click Advanced button to configure more IKE	
	settings.	
Connection Type	Click to select <i>Initiator</i> or <i>Responder</i> mode.	
Connect	Click to connect manually. [Responder mode only]	
Disconnect	Click to disconnect manually. [Responder mode	
	only].	
ESP	Click to configure 3DES, AES128 or NULL	
	encryption.	
	Click to configure <i>MD5</i> or <i>SHA1</i> authentication.	
PreShared Key	Fill in the key value. [IKE mode only]	
Remote RSA Key	Fill in the remote gateway RSA key. [IKE mode	
	only]	
Status	It shows connection status. [IKE mode only]	
SPI	Fill in Security Parameter Index value. [Manual	
	mode only]	
Encryption Key	Fill in encryption key. [Manual mode only]	
Authentication Key	Fill in authentication key. [Manual mode only]	
Apply Change	Click the Apply Changes button to save current	
	tunnel settings.	
Reset	Click the <i>Reset</i> button to abort change and recover	
	the previous configuration setting.	
Refresh	It shows the current connection status. [Manual	
	mode only]	
Back	It returns back to VPN Setup page.	

Tunnel 1	
Phase 1:	
Negotiation Mode	Main mode
Encryption Algorithm	3DES 🔽
Authenticaiton Algorithm	MD5 😽
Key Group	DH2(modp1024) 🗸
Key Life Time	3600
Phase 2:	
Active Protocol	ESP
Encryption Algorithm	3DES 🐱
Authenticaiton Algorithm	MD5 😽
Key Life Time	28800
Ecapsulation	Tunnel mode
Perfect Forward Secrecy (PFS)	ON 🗸

Screen snapshot – Advanced VPN Settings for IKE

Item	Description	
Phase 1		
Negotiation Mode	Main mode.	
Encryption Algorithm	Click to select 3DES or AES128 encryption.	
Authentication Algorithm	Click to select <i>MD5</i> or <i>SHA1</i> authentication.	
Key Group	Click to select <i>DH1(modp768)</i> , <i>DH2(modp1024)</i> or <i>DH5(modp1536)</i> key group. Default value is DH2	
Key Life Time	Fill in the key life time value by seconds.	
Phase 2		
Active Protocol	ESP.	
Encryption Algorithm	Click to select 3DES, AES128 or NULL encryption.	
Authentication Algorithm	Click to select <i>MD5</i> or <i>SHA1</i> authentication.	

Key Life Time	Fill in the key life time value by seconds.	
Encapsulation	Tunnel mode.	
Perfect Forward Secrecy (PFS)	Click to select ON or NONE .	
Ok	Click the Ok button to save current tunnel settings.	
Cancel	Click the <i>Cancel</i> button to close current window without any changes.	

3.3.19 Management - Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.

	packet counters for transm	nission and rec	eption regarding to wireless and Ethernet
etworks.			
Wireless LAN	Sent Packets	1361	
	Received Packets	25883	
Ethernet LAN	Sent Packets	1529	
	Received Packets	1269	
Ethernet WAN	Sent Packets	597	
	Received Packets	30386	

Screen snapshot – Management - Statistics

ltem	Description
Wireless LAN	It shows the statistic count of sent packets on the
Sent Packets	wireless LAN interface.
Wireless LAN	It shows the statistic count of received packets on
Received Packets	the wireless LAN interface.
Ethernet LAN	It shows the statistic count of sent packets on the
Sent Packets	Ethernet LAN interface.
Ethernet LAN	It shows the statistic count of received packets on
Received Packets	the Ethernet LAN interface.
Ethernet WAN	It shows the statistic count of sent packets on the
Sent Packets	Ethernet WAN interface.
Ethernet WAN	It shows the statistic count of received packets on
Received Packets	the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.
Ethernet WAN <i>Received Packets</i>	It shows the statistic count of received packets on the Ethernet WAN interface.

3.3.20 Management - DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.

hat (possibly everch	anging) ir-auttess.	
Enable DDNS		
Service Provider :	DynDNS 🗸	
Domain Name :	host.dyndns.org	
User Name/Email:		
Password/Key:		
	tve a 30 days free trial in create your DynDNS	<u>here</u> or manage your TZO account in <u>control panel</u> 8 account <u>here</u>

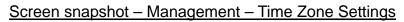
Screen snapshot – Management – DDNS

Item	Description
Enable DDNS	Click the checkbox to enable DDNS service. Refer
	to <u>4.25 What is DDNS?</u>
Service Provider	Click the drop down menu to pickup the right
	provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Apply Change	Click the Apply Changes button to save the enable
	DDNS service.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.3.21 Management - Time Zone Setting

This page is used to configure NTP client to get current time.

Time Zor	ne Setting
You can maintain	the system time by synchronizing with a public time server over the Internet.
Current Time :	Yr 2005 Mon 3 Day 16 Hr 17 Mn 57 Sec 24
Time Zone Selec	xt: (GMT+08:00)Taipei
Enable NTP	client update
NTP server :	192.5.41.41 - North America
	(Manual IP Setting)
Apply Chang	ge Reset Refresh



Item	Description
Current Time	It shows the current time.
Time Zone Select	Click the time zone in your country.
Enable NTP client	Click the checkbox to enable NTP client update.
update	Refer to 4.26 What is NTP Client?
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the Apply Changes button to save and enable
	NTP client service.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.
Refresh	Click the refresh the current time shown on the
	screen.

3.3.22 Management – Denial-of-Service

This page is used to enable and setup protection to prevent attack by hacker's program. It provides more security for users.

rvice from using that service.	eu by airexp	licit attempt by hackers to prevent legitimate use:	s or a
Enable DoS Preventicn			
Whole System Flood: SYN	0	Packets/Second	
Whole System Flood: FIN	0	Packets/Second	
Whole System Flood: UDP	0	Packets/Second	
Whole System Flood: ICMP	0	Packets/Second	
Per-Source IP Flood: SYN	0	Packets/Second	
Per-Source IP Flood: FIN	0	Packets/Second	
Per-Source IP Flood: UDP	0	Packets/Second	
Per-Source IP Flood: ICMP	0	Packets/Second	
TCP/UDP PortScan	Low	Sensitivity	
ICMP Smurf			
IP Land			
IP Spoof			
IP TearDrop			
PingOfDeath			
ICP Scan			
TCP SynWithData			
UDP Bomb			
UDP EchoChargen			
Select ALL Clear ALL			
Enable Source IP Blocking	0	Block time (sec)	
Enable Source If Blocking	Ľ	Block time (sec)	

Screen snapshot – Management – Denial-of-Service

Item	Description
Enable DoS	Click the checkbox to enable DoS prevention.
Prevention	
Whole System Flood	Enable and setup prevention in details.
/ Per-Source IP	
Flood	
Select ALL	Click the checkbox to enable all prevention items.
Clear ALL	Click the checkbox to disable all prevention items.
Apply Changes	Click the <i>Apply Changes</i> button to save above settings.

3.3.23 Management - Log

This page is used to configure the remote log server and shown the current log.

	e log server and show the system log.	
Enable Log		
🗹 system all	wireless DoS	
Enable Remote Log	Log Server IP Address:	
1 hr (1 +		
Apply Changes		
)day 00:02:18 br0: port	2(wlan0) entering disabled state	^
Oday 00:02:18 device wl	anO left promiscuous mode	
)day 00:02:18 br0: port	1(eth0) entering disabled state	
Oday OO:02:18 device et	hO left promiscuous mode	
Oday 00:02:18 device et	hO entered promiscuous mode	
Dday 00:02:18 eth0:phy	is 8305	
Oday 00:02:18 device wl	anO entered promiscuous mode	
Dday 00:02:18 br0: port	2(wlan0) entering listening state	
)day 00:02:18 br0: port	1(eth0) entering listening state	
Oday 00:02:18 entering	learning state	
)day 00:02:18 br0: port	2(wlan0) entering forwarding state	
	logy Change detected, propagating	
Jday UU:U2:18 brU: topo	1(oth0) onto ring log ming state	=
	I(e(nu)) entering reathing state	
)day 00:02:18 br0: port	1(eth0) entering forwarding state	

Screen snapshot - Management - Log

Description
Click the checkbox to enable log.
Show all log of wireless broadband router
Only show wireless log
Only show Denial-of-Service log
Click the checkbox to enable remote log service.
Input the remote log IP address
Click the Apply Changes button to save above
settings.
Click the refresh the log shown on the screen.
Clear log display screen

3.3.24 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Upgrade Fi	rmware
	upgrade the Access Point firmware to new version. Please note, do not power off the ad because it may crash the system.
Select File:	Browse
Upload Rese	

Screen snapshot – Management - Upgrade Firmware

Item	Description
Select File	Click the Browse button to select the new version of
	web firmware image file.
Upload	Click the Upload button to update the selected web
	firmware image to the X-Micro WLAN 11g
	Broadband Router.
Reset	Click the Reset button to abort change and recover the previous configuration setting.

3.3.25 Management Save/ Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.

	settings to a file or reload the settings from the file which et the current configuration to factory default.	h was saved
ave Settings to File:	Save	
oad Settings from File:	Browse	Upload
eset Settings to Default:	Reset	

<u>Screen snapshot – Management - Save/Reload Settings</u>

Item	Description
Save Settings to File	Click the Save button to download the configuration
	parameters to your personal computer.
Load Settings from	Click the Browse button to select the configuration
File	files then click the <i>Upload</i> button to update the
	selected configuration to the X-Micro WLAN 11g
	Broadband Router.
Reset Settings to	Click the <i>Reset</i> button to reset the configuration

Default parameter to factory defaults.

3.3.26 Management - Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

This page is used to set the a will disable the protection.	account to access the web server of Access Point. Empty user name and password
User Name:	
New Password:	
Confirmed Password:	

Screen snapshot - Management - Password Setup

Item	Description
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Apply Changes	Clear the <i>User Name</i> and <i>Password</i> fields to empty, means to apply no web management login control. Click the <i>Apply Changes</i> button to complete the new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover the previous configuration setting.

3.3.27 Management - WatchDog

This page is used to do watchdog function using ping command. User set IP address, interval and ping fail count conditions to decide whether router reboots or not.

Wat	WatchDog Setting	
-	g command to identify whether the router is functional or not. User has to set IP address, interval and fail count to eboot router.	
E	nable WatchDog	
Watch	WatchDog IP Address: 0.0.0.0	
Ping I	nterval: 30 (30-600 seconds)	
Ping F	ail to reboot Counter: 3 (3-30)	
App	Apply Changes Reset	

Screen snapshot - Management - WatchDog Settiing

Item	Description
Enable WatchDog	Click to enable watchdog.
WatchDog IP	IP address that is referred.
Address	
Ping Interval	Fill in the value by seconds.
Ping Fail to reboot	Fill in the value that is the threshold to reboot router
Count	when ping fails.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

3.3.28 Management - Quality of Service

This page is used to do bandwidth control by ip address. User sets total and undefined bandwidth first. Then set bandwidth by range of ip addresses.

Quality of Service
First, assign total downstream and upstream that you applied from ISP. Second, set up the specific ip address' guarantee downstream, upstream and priority and display current settings in the table.
Enable QoS
ISP Bandwidth: Download 0 KB/s Upload 0 KB/s
Undef IP Bandwidth: Download 0 KB& Upload 0 KB&
Apply Changes Reset
Bandwith Control
IP Address Range:
Guarantee Bandwidth: Download KB& Upload KB&
Priority: High 🖌
Apply Changes Reset
Current Bandwidth Control Table:
From IP Addr To IP Addr Downstream (KB/s) Priority Select
Delete Selected Delete All Reset

Screen snapshot – Management – Qaulity of Service

Item	Description
Enable QoS	Click to enable QoS.
ISP Bandwidth	
Download	Fill in the value that is the download stream from ISP
	by KB/s.
Upload	Fill in the value that is the upload stream from ISP by
	KB/s.
Undef IP Bandwidth	
Download	Define the download bandwidth that is not defined.
Upload	Define the upload bandwidth that is not defined.
Apply Changes	Click the Apply Changes button to complete the
	new configuration setting.
Reset	Click the <i>Reset</i> button to abort change and recover
	the previous configuration setting.

Item	Description
Bandwidth Control	
IP Address Range	Set start and end ip address.
Guarantee Bandwidtl	h
Download	Fill in the value by KB/s.
Upload	Fill in the value by KB/s.

Click to pick High, Medium or Low
Click the Apply Changes button to complete the
new configuration setting. It is added into Current
Bandwidth Control Table.
Click the <i>Reset</i> button to abort change and recover
the previous configuration setting.
Click to delete the selected ip addresses that will be
removed from the Current Bandwidth Control
Table.
Click to delete all the registered entries from the ip
addresses Current Bandwidth Control Table.
Click the <i>Reset</i> button to abort change and recover
the previous configuration setting.

3.3.29 Logout

This page is used to logout web management page. This item will be activated next time you login after you define user account and password.

Logout				
This page is used to log	out.			

Screen snapshot - Logout

Change setting successfully!
UK

Screen snapshot - Logout - OK

Item	Description
Apply Change	Click the Apply Change button, Then click OK
	button to logout.

4 Frequently Asked Questions (FAQ)

4.1What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
- ✓ Yype in *ipconfig /all* then press the *Enter* button.
- Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

4.2What is Wireless LAN?

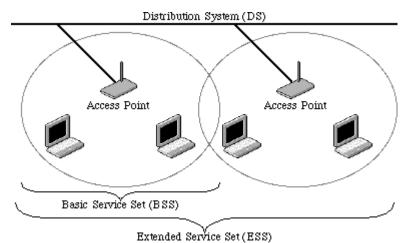
A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

4.3What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

4.4How does wireless networking work?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Independent Basic Service Set (IBSS) Example 2: wireless Ad Hoc Mode

4.5What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

4.6What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

4.7What are potential factors that may causes interference? Factors of interference:

- > Obstacles: walls, ceilings, furniture... etc.
- > Building Materials: metal door, aluminum studs.

Electrical devices: microwaves, monitors and electrical motors.
 Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, ... etc.
- ✓ Add additional WLAN Access Points if necessary.

4.8What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

4.9What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

4.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

4.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

4.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

4.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

4.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

4.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

4.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i

amendment to the 802.11 standard.

4.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

4.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

4.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

4.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

4.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

4.22 What is Universal Plug and Play (uPNP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP

devices regardless of media, operating system, programming language, and wired/wireless connection.

4.23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

4.24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients will communicate outside world through the X-Micro WLAN 11g Broadband Router, so have the cloned MAC address set on the X-Micro WLAN 11g Broadband Router will solve the issue.

4.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user own the DNS server with dynamic WAN IP address.

4.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

4.27 What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to point private link via shared or public network.

4.28 What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

4.29 What is WLAN Block Relay Between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an *Access Point* (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS

4.30 What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard.

WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

4.31 What is WLAN ACK TIMOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

5 Configuration Examples

5.1 Example One – PPPoE on the WAN

Sales division of Company ABC likes to establish a WLAN network to support mobile communication on sales' Notebook PCs. MIS engineer collects information and plans the X-Micro WLAN 11g Broadband Router implementation by the following configuration.

WAN configuration:

	PPPoE	
	User Name	H890123456
	Password	PW192867543210
LAI	N configuration	
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP Client	192.168.1.100 – 192.168.1.200
	Range	
WL	AN configuration	

AN COIIIgulallOll	
SSID	MyWLAN
Channel Number	11

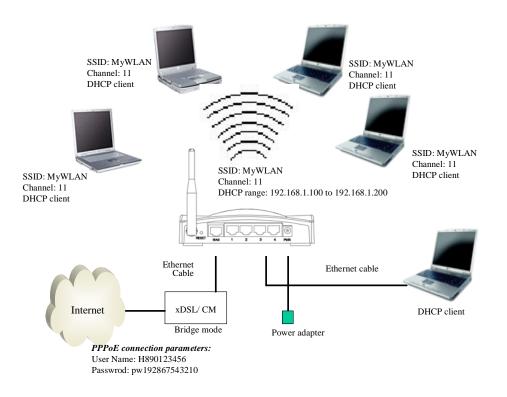


Figure 3 – Configuration Example One – PPPoE on the WAN

Configure the WAN interface:	WAN Interface This page is used to configur Point. Here you may change Access type.	e the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN
Open WAN Interface	WAN Access Type:	PPPoE 🗸
Setup page, select PPPoE	User Name: Password:	H890123456
then enter the User Name	Service Name: Connection Type:	Continuous Connect Disconnect
"H890123456" and	Idle Time: MTU Size:	5 (1-1000 minutes) 1400 (1360-1492 bytes)
Password	O Attain DNS Automat	tically
" PW192867543210 ", the	DNS 1: DNS 2:	
password is encrypted to	DNS 3: Clone MAC Address:	
display on the screen.	Enable PPTP pass	
Apply Changes Pres	ss button to c	confirm the configuration setting.

Configure the LAN interface:

Open LAN Interface Setup page, enter the IP Address "**192.168.1.254**", Subnet Mask "**255.255.255.0**", Default Gateway "**0.0.0**", enable DHCP Server, DHCP client range "**192.168.1.100**" to "**192.168.1.200**".

LAN Interfac	e Setup
	igure the parameters for local area network which connects to the Point. Here you may change the setting for IP addresss, subnet
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server 💌
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
DNS Server:	
Domain Name:	
802.1d Spanning Tree:	Disabled 💌
	0000000000

Apply Changes

Press button to confirm the configuration setting.

Configure the WLAN	
interface:	Wireless Basic Settings This page is used to configure the parameters for wireless LAN clients which may connect to
Open WLAN Interface	your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.
Setup page, enter the	Disable Wireless LAN Interface
SSID " MyWLAN ",	Band: 2.4 GHz (B+G) Mode: AP Network Type: Infrastructure
Channel Number "11".	SSID: MyWLAN
	Channel Number: 11 Associated Clients: Show Active Clients
	Enable Mac Clone (Single Ethernet Client)
	Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
	SSID of Extended Interface:
	Apply Changes Reset

Apply Changes

Press button to confirm the configuration setting.

5.2 Example Two - Fixed IP on the WAN

Company ABC likes to establish a WLAN network to support mobile communication on all employees' Notebook PCs. MIS engineer collects information and plans the X-Micro WLAN 11g Broadband Router implementation by the following configuration.

WAN configuration:

	Fixed IP	
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0
	Default Gateway	192.168.2.10
	DNS Address	168.95.1.1
LA	N configuration	
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
	Default Gateway	192.168.2.254

Range WI AN configuration

DHCP

AN configuration	
SSID	MyWLAN
Channel Number	11

Client 192.168.1.100 - 192.168.1.200

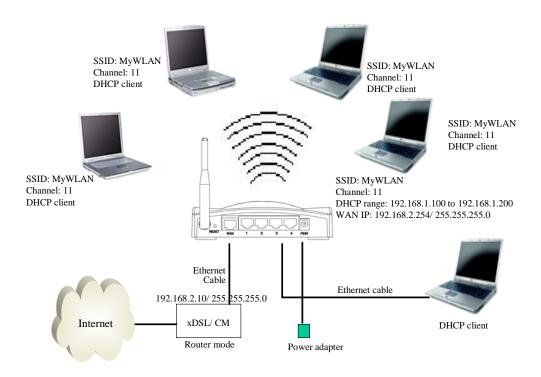


Figure 4 – Configuration Example Two – Fixed IP on the WAN

Configure the WAN	WAN Interfac	ce Setup
interface:		re the parameters for Internet network which connects to the WAN port of your Access the access method to static IP, DHCP, PPPoE or PPTP by click the item value of
Open WAN Interface	WAN Access Type:	Static IP
Setup page, select	IP Address:	192.168.2.254
Fixed IP then enter IP	Subnet Mask: Default Gateway:	255.255.255.0 192.168.2.10
	MTU Size:	1400 (1400-1500 bytes)
Address	DNS 1:	
"192.168.2.254",	DNS 2: DNS 3:	
subnet mask	Clone MAC Address:	
" 255.255.255.0 ",	Enable Web Serve	is on white x Access on WAN through on VPN connection
Default gateway	Enable PPTP pass	through on VPN connection through on VPN connection
" 192.168.2.10 ".	Apply Changes R	eset

Press

Apply Changes

button to confirm the configuration setting.

Configure the LAN interface:

Open LAN Interface Setup page, enter the IP Address "**192.168.1.254**", Subnet Mask "**255.255.255.0**", enable DHCP Server, DHCP client range "**192.168.1.100**" to "**192.168.1.200**".

Apply Changes

a	ce:	
	LAN Interface Setup	
		ure the parameters for local area network which connects to the oint. Here you may change the setting for IP addresss, subnet
	IP Address:	192.168.1.254
	Subnet Mask:	255.255.255.0
	Default Gateway:	0.0.0.0
	DHCP:	Server 💌
	DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
	DNS Server:	
	Domain Name:	

Press button to confirm the configuration setting.

Disabled 🔽

Reset

000000000000000

802.1d Spanning Tree:

Apply Changes

Clone MAC Address:

Configure the WLAN interface:

Open WLAN Interface Setup page, enter the SSID "**MyWLAN**", Channel Number "11".

	nfigure the parameters for wireless LAN clients which may connect to re you may change wireless encryption settings as well as wireless
Disable Wireless	s LAN Interface
Band:	2.4 GHz (B+G) 💌
Mode:	AP 💌
Network Type:	Infrastructure 💌
SSID:	MyWLAN
Channel Number:	11 💌
Associated Clients:	Show Active Clients
Enable Mac Clon	te (Single Ethernet Client)
📃 Enable Universal	l Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Inte	rface:

Apply Changes

Press button to confirm the configuration setting.



www.x-micro.com