

LUXUL

Simply Connected

User Guide

XWR-1750

Dual Band Wireless

AC1750 Gigabit Router



Use the XWR-1750 to:

- ▶ Deliver Next Generation 802.11ac Gigabit Wi-Fi with Speeds up to 1750Mbps
- ▶ Maximize Data Rates with Concurrent Dual-Band Technology
- ▶ Optimize VoIP, Streaming Media and Other Demanding Applications
- ▶ Create a Secure Guest Network
- ▶ Provide an Affordable High Performance Network

XWR-1750

User Guide

Model Number: XWR-1750

Dual Band Wireless AC1750 Gigabit Router

FCC ID: W59XWR1750

IC: 8584A-XWR1750

© 2015 Luxul. All Rights Reserved.

No part of this publication may be modified or adapted in any way, for any purposes without permission in writing from Luxul. The material in this manual is subject to change without notice. Luxul reserves the right to make changes to any product to improve reliability, function, or design. No license is granted, either expressly or by implication or otherwise under any Luxul intellectual property rights. An implied license only exists for equipment, circuits and subsystems contained in this or any Luxul product.

This product is covered by one or more U.S. and foreign patents.

Patents: 7,379,717, 6,606,075, 6,373,448, other patents pending

DOCUMENT CONVENTIONS

The following graphical alerts are used in this document to indicate notable situations:



NOTE: Tips, hints, or special requirements that you should take note of.



CAUTION: Care is required. Disregarding a caution can result in data loss or equipment malfunction.



WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

CONTACT LUXUL

Sales

P: 801-822-5450

E: sales@luxul.com

Technical Support

P: 801-822-5450

E: support@luxul.com

FCC COMPLIANCE

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CONTENTS

1 PRODUCT OVERVIEW	4
1.1 Product Introduction	4
1.2 Product Features	4
1.3 Product Specifications	5
1.4 Package Contents	5
2 HARDWARE DESCRIPTION AND INSTALLATION	5
2.1 Panel Layout	5
2.2 System Requirements	7
2.3 Installation Requirements	7
2.4 XWR-1750 Installation	8
2.5 Default IP Address	8
2.6 Connecting a Client Device	8
2.7 Verifying Connectivity	8
3 CONFIGURATION	9
3.1 Quick Setup	9
3.2 Status	16
3.3 Network	20
3.4 Wireless	24
3.5 Guest Network	31
3.6 Firewall/Security	33
3.7 QoS	37
3.8 VPN	39
3.9 Administration	41
3.10 Tools	48
4 REGULATORY COMPLIANCE	49
APPENDIX 1: COMMON COMMANDS	52

1 PRODUCT OVERVIEW

1.1 Product Introduction

The Luxul XWR-1750 Wireless Router is a feature rich network device designed to enhance the performance, security and reliability of a home or commercial network. It enables simple monitoring, management and control of network usage to boost efficiency, reduce network bandwidth and minimize security risks. With web-based management tools; along with advanced security, VPN, and bandwidth control features, the XWR-1750 provides the ideal foundation upon which to build your Luxul network.

1.2 Product Features

- ▶ Complies with IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n and IEEE802.11ac
- ▶ One 10/100/1000M auto-negotiating WAN interface
- ▶ Four 10/100/1000M auto-negotiating LAN interfaces
- ▶ Protocol Support for TCP/IP, UDP, VPN, DHCP, NAT, SMTP, DNS, FTP
- ▶ True QOS support to prioritize traffic by Host, Protocol and Port
- ▶ 600MHz processor and powerful NAT forwarding features support up to 39K+ concurrent sessions
- ▶ Support for Port Forwarding, DMZ hosts and ALG applications
- ▶ VPN server supports PPTP VPN clients
- ▶ PPTP VPN server function gives up to 10 users simultaneous access to the local network providing a secure connection
- ▶ Supports Dynamic Domain Name System or DDNS
- ▶ Provides system security logs and flow statistics
- ▶ Built-in DHCP server with static address lease capability

1.3 Product Specifications

Supported Protocols and Standards	IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ac TCP/IP, DHCP, ICMP, NAT, PPPoE, SNMP, HTTP, DNS, ARP
Network Media	10Base-T \oplus Cat5 or better 100Base-TX \oplus Cat5 or better 1000Base-TX: Cat5 or better (Cat6 recommended) Wireless 802.11a/b/g/n/ac adapter
Dimensions LxWxH in. (mm)	8.6"x6.2"x1.3" (218.6x156.5x33.8)
Power and Consumption	AC 110V 60Hz or 220V 50Hz Consumption:

1.4 Package Contents

The following items are included in the box:

- ▶ XWR-1750 Wireless Router
- ▶ Power Cord
- ▶ Quick Installation Guide

If any of the listed items are missing or damaged, please contact the reseller from whom you purchased for return/replacement.

2 HARDWARE DESCRIPTION AND INSTALLATION

2.1 Panel Layout

2.1.1 Front Panel



XWR-1750 Front Panel

XWR-1750

LED Indicators:

Indicator	Description		Function
 5GHz	5GHz	FLASHING	Indicates the XWR-1750 is passing 5GHz wireless data.
		ON	Indicates a 5GHz wireless network is configured and broadcasting.
		OFF	Indicates there is no 5GHz wireless network configured or the 5GHz radio is disabled.
 2.4GHz	2.4GHz	FLASHING	Indicates the XWR-1750 is passing 2.4GHz wireless data.
		ON	Indicates a 2.4GHz wireless network is configured and broadcasting.
		OFF	Indicates there is no 2.4GHz wireless network configured or the 2.4GHz radio is disabled.
1·2·3·4	1-4 LAN LED	ON	Indicates a device is connected to the Ethernet port number.
		FLASHING	Indicates data packets are being transmitted to the connected device.
	Internet LED	ON	Indicates the XWR-1750 is connected to the ISP.
		FLASHING	Indicates data packets are being transmitted to the Internet
	USB LED	ON	Indicates a USB enabled device is connected and configured.
	System LED	ON	Indicates the XWR-1750 is booting.
		FLASHING	Indicates the XWR-1750 is operating normally.
		OFF	Indicates the XWR-1750 will not boot.
	Power LED	ON	Indicates power is applied to the XWR-1750.
		OFF	Indicates power is not applied to the XWR-1750.
	Luxul LED		Unused at this time



NOTE: If additional local ports are required, it is recommended that a Luxul switch be used in conjunction with the XWR-1750.

2.1.2 Rear Panel

- ▶ Antenna: 3 RPSMA Antenna ports for connecting 2.4/5GHz wireless Antennas.
- ▶ Power: Power port used to connect the provided DC power supply.
- ▶ WAN: 1 WAN RJ-45 Ethernet Port for connecting internet feed.
- ▶ LAN: 4 LAN RJ-45 Ethernet Ports allowing for four local network connections.
- ▶ Reset Button: Used for hard reset or factory default reset. To hard reset the router, press and release the button. To reset to factory defaults, press and hold this button for 15 seconds.



CAUTION: Resetting the XWR-1750 to factory defaults will remove all custom settings



XWR-1750 Rear Panel

2.2 System Requirements

- ▶ Network Connections: 802.3 Ethernet Enabled Computer or 802.11a/b/g/n/ac Wireless Enabled Computer
- ▶ Web Browsers: Supported Web browser versions include I.E. 9, Firefox 25, Safari 5, Chrome 30, and up. The Web browser is used to configure the XWR-1750.
- ▶ Internet: Broadband Internet Service (depending on the service provider, a separate modem may be required)

2.3 Installation Requirements

- ▶ Install the XWR-1750 in a stable/safe place to avoid any possible damage
- ▶ Inspect the DC power adapter to ensure that it is correctly connected and undamaged
- ▶ To avoid electric shock, DO NOT open the XWR-1750 housing (no user serviceable parts inside). Opening the XWR-1750 will void your warranty.

XWR-1750

- ▶ It is recommended that the Grounding connection to the outlet is functioning properly and the XWR-1750 is positioned away from direct sun light
- ▶ Ensure there is sufficient space around the XWR-1750 for proper ventilation and heat dissipation. It is recommended to have at least 4-6 inches around all sides.

2.4 XWR-1750 Installation

Before installing the XWR-1750, test the Internet connection to validate that it is functioning properly. When Internet access has been confirmed, follow the steps below for Router installation.

1. Connect the Internet cable to the XWR-1750 WAN port
2. Connect one of the XWR-1750 LAN port to a switch, access point, or computer.
3. Connect DC Power Adapter
4. Establish LAN or Wireless Connection
5. Connect a Wireless device to the 2.4GHz or 5GHz Wireless SSID.



NOTE: Connect the included DC power adapter to the XWR-1750 first and then to the AC outlet.

2.5 Default IP Address

The XWR-1750 default IP address is 192.168.0.1. This address can be changed. However, for hassle free installation of other plug and play Luxul devices, it is recommended that the default IP value be maintained.

2.6 Connecting a Client Device

Connect a client device to one of the XWR-1750 LAN ports or to a switch that is connected to an XWR-1750 LAN port. Connect a wireless client device to one of the wireless SSIDs (**Luxul17502G** or **Luxul17505G**). The DHCP server on the XWR-1750 is configured by default. If your client device is set to obtain an address automatically, no further configuration is required.

2.7 Verifying Connectivity

After automatic configuration of the TCP/IP parameters, the ping command can be used to check connectivity between the XWR-1750 and the client device.

Windows Devices:

6. Select **Start >> Run**. Input **cmd** in the Run line then press enter.

- At the newly opened command interface enter the following command: ping 192.168.0.1 and press enter. If connected properly, the system should report back a result as follows: packets sent=4, packets received=4, packets lost=0. This means the device is connected with a valid IP address.

3 CONFIGURATION

This chapter introduces the configuration of the XWR-1750 Enterprise Multi-WAN Router functions via the Web-based management interface.

- ▶ Quick Setup
- ▶ Status
- ▶ Network
- ▶ Wireless
- ▶ Guest Network
- ▶ Firewall/Security
- ▶ QoS
- ▶ VPN
- ▶ Administration
- ▶ Tools

3.1 Quick Setup

The Quick Setup page allows you to configure the Primary Internet / WAN connection settings and the Local Network / LAN settings. This page is intended to get your Internet connection up and running as quick and painless as possible.

3.1.1 Connection Type DHCP

This Connection Type option will automatically pull the WAN IP, WAN Subnet Mask, WAN Gateway, WAN Primary DNS and WAN Secondary DNS from your ISP's Modem.

Select the Menu **Quick Setup** and **Connection Type DHCP** from the dropdown to view the following page:

Internet / WAN

Connection Type	<input type="checkbox"/>	<input type="text" value="DHCP"/>
Primary DNS	<input type="checkbox"/>	<input type="text" value="DNS Assigned By ISP"/>
Custom MAC Address	<input type="checkbox"/>	<input type="text"/>
Custom MTU	<input type="checkbox"/>	<input type="text" value="1500"/>

- ▶ **Internet/WAN:** Displays the WAN connection Options
 - ▶ **Connection Type:** Select the desired WAN Connection Type. When set to DHCP, the Router will pull all connection information automatically from the ISP's Modem. DHCP is the default setting.
 - ▶ **Primary DNS:** Allows you to select the checkbox and manually configure a Primary DNS Server IP Address. "DNS Assigned By ISP" is the default setting
 - ▶ **Secondary DNS:** Allows you to select the checkbox and manually configure a Secondary DNS Server IP Address. "DNS Assigned By ISP" is the default setting
 - ▶ **Custom MAC Address:** Allows you to set a Custom MAC Address which allows the Router to appear as a Computer to the ISP Modem. Some Modems will cache the MAC Address of the first device used to setup Internet Service and cannot be reset by the user. If this occurs you can clone that setup Device's MAC Address to allow the XWR-1750 to connect to the Modem.
 - ▶ **Custom MTU:** Allows you to configure a Custom MTU setting. MTU (or Maximum Transmission Unit), is the maximum packet size allowed on the network. Some ISPs (usually DSL or Fiber) will require this value to be set if the Modem is in Bridge mode.
- ▶ After making any changes to the Connection Type, you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.1.2 Connection Type PPPOE

This Connection Type option requires a Username and Password that is provided by the ISP and is typically used on Bridged DSL Modem connections. This type will automatically pull the WAN IP, WAN Subnet Mask, WAN Gateway, WAN Primary DNS and WAN Secondary DNS from the ISP's Modem once the Router is successfully Authenticated.

Select the Menu **Quick Setup** and **Connection Type PPPOE** from the dropdown to view the following page:

Internet / WAN

Connection Type 

User Name 

Password 

Max Failed Pings 

Ping Interval 

Primary DNS 

Custom MAC Address 

Custom MTU 

► **Internet/WAN:** Displays the WAN connection Options

- **Connection Type:** Select the desired WAN Connection Type. When set to PPPOE, enter a Username and Password that the ISP provides to authenticate the Router allowing it to connect. The Router will pull all connection information automatically from the ISP's Modem once it is successfully authenticated. DHCP is the default setting.
- **Username:** Allows you to enter the PPPOE Username specified by the ISP.
- **Password:** Allows you to enter the PPPOE Password specified by the ISP.
- **Max Failed Pings:** Allows you to specify the Maximum number of Failed Pings to the PPPOE Server before the Router attempts to re-authenticate to the PPOE Sever. We recommend the default value of 3 attempts unless the ISP recommends a different value.
- **Ping Interval:** Allows you to specify the number of seconds to wait between Ping attempts to the PPPOE Server. We recommend the default value of 5 seconds in order to preserve WAN resources.
- **Primary DNS:** Allows you to select the checkbox and manually configure a Primary DNS Server IP Address. "DNS Assigned By ISP" is the default setting.
- **Secondary DNS:** Allows you to select the checkbox and manually configure a Secondary DNS Server IP Address. "DNS Assigned By ISP" is the default setting.

XWR-1750

- ▶ **Custom MAC Address:** Allows you to set a Custom MAC Address which allows the Router to appear as a Computer to the ISP Modem. Some Modems will cache the MAC Address of the first device used to setup Internet Service and cannot be reset by the user. If this occurs you can clone that setup Device's MAC Address to allow the XWR-1750 to connect to the Modem.
- ▶ **Custom MTU:** Allows you to configure a Custom MTU setting. MTU (or Maximum Transmission Unit), is the maximum packet size allowed on the network. Some ISPs (usually DSL or Fiber) will require this value to be set if the Modem is in Bridge mode.
- ▶ After making any changes to the Connection Type, you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.1.3 Connection Type Static IP

This Connection Type option requires the Static IP, Netmask, Gateway, Primary DNS and Secondary DNS provided by the ISP to be entered manually. This type will never have an IP Address change on the connection and is typically used in Business or Remote Access implementations.

Select the Menu **Quick Setup** and **Connection Type Static IP** from the dropdown to view the following page:

Internet / WAN

Connection Type  Static IP ▾

Static IP: 

Netmask: 

Gateway: 

Primary DNS 

Secondary DNS 

Custom MAC Address 

Custom MTU 

- ▶ **Internet/WAN:** Displays the WAN connection Options
 - ▶ **Connection Type:** Select the desired WAN Connection Type. When set to Static IP, you must enter the IP information that the ISP provides allowing the Router to connect.

- ▶ **Static IP:** Allows you to enter the WAN connection IP Address specified by the ISP.
 - ▶ **Netmask:** Allows you to enter the WAN connection Subnet Mask specified by the ISP.
 - ▶ **Gateway:** Allows you to enter the WAN connection Gateway IP Address specified by your ISP.
 - ▶ **Primary DNS:** Allows you to manually configure the Primary DNS Server IP Address specified by the ISP or any third party DNS Server IP Address. With the Static IP Connection Type specified, this is a required field.
 - ▶ **Secondary DNS:** Allows you to manually configure the Primary DNS Server IP Address specified by the ISP or any third party DNS Server IP Address. With the Static IP Connection Type specified this is a required field.
 - ▶ **Custom MAC Address:** Allows you to set a Custom MAC Address which allows the Router to appear as a Computer to the ISP Modem. Some Modems will cache the MAC Address of the first device used to setup Internet Service and cannot be reset by the user. If this occurs you can clone that setup Device's MAC Address to allow the XWR-1750 to connect to the Modem.
 - ▶ **Custom MTU:** Allows you to configure a Custom MTU setting. MTU (or Maximum Transmission Unit), is the maximum packet size allowed on the network. Some ISPs (usually DSL or Fiber) will require this value to be set if the Modem is in Bridge mode.
- ▶ After making any changes to the Connection Type, you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.1.4 Local Network / LAN

Allows you to set the Local Network IP Address of the Router and the Subnet Mask used in the Local Network.

Select the Menu **Quick Setup** to view the following page:

Local Network / LAN

LAN IP Address	<input type="text" value="192.168.0.1"/>
LAN Subnet Mask	<input type="text" value="255.255.255.0"/>
<input type="button" value="Save"/> <input type="button" value="Reboot"/> <input type="button" value="Cancel"/>	

XWR-1750

- ▶ **Local Network / LAN:** Displays the Local Network IP Options
 - ▶ **LAN IP Address:** Allows you to configure the LAN IP of the Router, this will be used by all devices in the LAN as the Default Gateway. If you are installing other Luxul devices, we recommend keeping the default IP of 192.168.0.1.
 - ▶ **LAN Subnet Mask:** Allows you to specify the Subnet Mask to be used in the LAN. The default value of 255.255.255.0 is recommended unless specified otherwise by your Network Administrator.

3.1.5 Wireless Settings 2.4GHz Frequency

Allows you to configure the Primary 2.4GHz Wireless Network.

Select the Menu **Quick Setup** to view the following page:

Wireless Settings 2.4GHz Frequency

Operating Mode ⓘ Access Point ▾

Network Name (SSID) ⓘ LuxulXen6002G

Security Mode ⓘ Open ▾

Channel ⓘ 6 ▾

- ▶ **Wireless Settings 2.4GHz Frequency:** Displays the 2.4GHz Wireless Network settings.
 - ▶ **Operating Mode:** Allows you to select the Operating Mode of the SSID. Access Point is the default setting.
 - ▶ **Network Name (SSID):** Allows you to specify the Network Name (SSID) used to identify the Wireless Network to client devices.
 - ▶ **Security Mode:** Allows you to set the desired Security Mode used to connect to the SSID, the supported modes include 64bit/128bit WEP, WPA, WPA2 and WPA/WPA2 Mixed. Open is the default setting, we strongly recommend adding Security to any SSID.
 - ▶ **WEP Key:** When selecting WEP Security a new option will appear WEP Key. This allows you to set the WEP Key, it can consist of Numbers 0-9 and Letters A-F. For 64bit WEP enter 10 hexadecimal digits (0-9 and A-F) or 5 regular characters. For 128bit WEP enter 26 hexadecimal digits (0-9 and A-F) or 13 regular characters.
 - ▶ **Encryption:** When selecting WPA or WPA2 security two new options will appear the first is Encryption. This allows you to set the Encryption type used by WPA/WPA2 the options include AES, TKIP&AES and TKIP. AES is the default and recommended setting.

- ▶ **WPA Passphrase:** When selecting WPA or WPA2 security two new options will appear the second is WPA Passphrase. This allows you to set the Passphrase used to connect to the SSID. WPA Passphrases must be a minimum of 8 to a maximum of 63 Characters and can contain Letters (capitol and lowercase), Numbers, Special Characters and Spaces.
- ▶ **Channel:** Allows you to specify the Channel used by the 2.4GHz Radio in the Router, the supported Channels include 1-11 (non-overlapping channels are 1, 6 and 11). 6 is the default setting.

3.1.6 Wireless Settings 5GHz Frequency

Allows you to configure the Primary 5GHz Wireless Network.

Select the Menu **Quick Setup** to view the following page:

Wireless Settings 5GHz Frequency

Operating Mode ⓘ Access Point ▾

Network Name (SSID) ⓘ LuxulXen6005G

Security Mode ⓘ Open ▾

Channel ⓘ 153 ▾

Save Reboot Cancel

- ▶ **Wireless Settings 5GHz Frequency:** Displays the 5GHz Wireless Network settings.
 - ▶ **Operating Mode:** Allows you to select the Operating Mode of the SSID. Access Point is the default setting.
 - ▶ **Network Name (SSID):** Allows you to specify the Network Name (SSID) used to identify the Wireless Network to client devices.
 - ▶ **Security Mode:** Allows you to set the desired Security Mode used to connect to the SSID, the supported modes include 64bit/128bit WEP, WPA, WPA2 and WPA/WPA2 Mixed. Open is the default setting, we strongly recommend adding Security to any SSID.
 - ▶ **WEP Key:** When selecting WEP Security a new option will appear WEP Key. This allows you to set the WEP Key, it can consist of Numbers 0-9 and Letters A-F. For 64bit WEP enter 10 hexadecimal digits (0-9 and A-F) or 5 regular characters. For 128bit WEP enter 26 hexadecimal digits (0-9 and A-F) or 13 regular characters.

- ▶ **Encryption:** When selecting WPA or WPA2 security two new options will appear the first is Encryption. This allows you to set the Encryption type used by WPA/WPA2 the options include AES, TKIP&AES and TKIP. AES is the default and recommended setting.
- ▶ **WPA Passphrase:** When selecting WPA or WPA2 security two new options will appear the second is WPA Passphrase. This allows you to set the Passphrase used to connect to the SSID. WPA Passphrases must be a minimum of 8 to a maximum of 63 Characters and can contain Letters (capitol and lowercase), Numbers, Special Characters and Spaces.
- ▶ **Channel:** Allows you to specify the Channel used by the 5GHz Radio in the Router, the supported Channels will change depending on the Wireless Mode 802.11ac+n+g offers 40 and 153. While 802.11a offers 36, 40, 44, 48, 149, 153, 157, 161 and 165 (the available options are non-overlapping channels) 153 is the default setting.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to the Internet / WAN and/or Local Network / LAN you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.2 Status

There are three submenus in the Status menu; Overview, Connected Clients and Wireless Connections. Click a submenu to view and/or modify the corresponding settings.

3.2.1 Overview

This page displays the System, Internet / WAN Settings and Local Network / LAN Settings configured on the Router.

Select the menu **Status>>Overview** to display the following page:

System	
Device Name	LuxulXEN XWR-1750
Firmware Version	4.0.3
Hardware Version	v1
CPU Usage	0%
Memory Usage	31%
Uptime	0d 2h 55m
Current Date/Time	Thu May 1 19:44:05 UTC 2014
Internet / WAN Settings	
Connection Type	DHCP
IP Address	192.168.100.124
Subnet Mask	255.255.255.0
Gateway	192.168.100.1
DNS Server	192.168.100.1
Alternate DNS	208.67.222.222
MAC Address	A4:13:4E:01:D3:4B
Local Network / LAN Settings	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	A4:13:4E:01:D3:4B

- ▶ **System:** Displays the XWR-1750 System properties.
 - ▶ **Firmware Version:** Displays the Version of Firmware running on the Router.
 - ▶ **Hardware Version:** Displays the Hardware Version of the Router.
 - ▶ **CPU Usage:** Displays the percentage of CPU Cycles currently occupied.
 - ▶ **Memory Usage:** Displays the percentage of Memory currently in use.
 - ▶ **Uptime:** Displays how long it has been since the Router has rebooted.
 - ▶ **Current Date/Time:** Displays the Date/Time pulled from the NTP Servers on the Internet.
- ▶ **Internet / WAN Settings:** Displays the WAN Settings of the Router.
 - ▶ **Connection Type:** Displays the WAN Connection Type configured on the Router.
 - ▶ **IP Address:** Displays the WAN IP Address assigned to the Router.
 - ▶ **Subnet Mask:** Displays the WAN Subnet Mask assigned to the Router.
 - ▶ **Gateway:** Displays the WAN Gateway IP Address assigned to the Router.
 - ▶ **DNS Server:** Displays the Primary DNS Server IP Address assigned to the Router.
 - ▶ **Alternate DNS:** Displays the Secondary DNS Server IP Address assigned to the Router.
 - ▶ **MAC Address:** Displays the current WAN Port MAC Address assigned to the Router.
- ▶ **Local Network / LAN Settings:** Displays the current LAN Settings of the Router.

XWR-1750

- ▶ **IP Address:** Displays the LAN IP Address of the Router. This address will be the Default Gateway for all client devices in the Local Network.
- ▶ **Subnet Mask:** Displays the LAN Subnet Mask of the Router. This Mask will be the Subnet Mask for all client devices in the Local Network.
- ▶ **MAC Address:** Displays the LAN MAC Address assigned to the Router.



NOTE: If DHCP or PPPOE is the configured Connection Type and the IP Address, Subnet Mask, Gateway, DNS Server and/or Alternate DNS information is blank, no information was received from the ISP's Modem. Please check configuration and if any changes were made please verify they were Saved and the Router was Rebooted.



NOTE: If a Custom MAC Address was specified it will be displayed as the Internet / WAN Settings MAC Address.



NOTE: If you notice a missing Alternate DNS IP Address, we recommend going to Quick Setup then select the Secondary DNS checkbox and manually adding a Secondary DNS Server. You must Save and Reboot for the changes to take effect.

3.2.2 Connected Clients

This Page displays the Client Devices that have requested a DHCP Address from the XWR-1750.

Select the menu **Status»Connected Clients** to display the following page:

Connected Clients

Device Name	IP Address	MAC Address
MBoulterPC	192.168.0.101	c0:18:85:bc:ed:45

- ▶ **Connected Clients:** Displays the current DHCP Leases issued by the Router.
 - ▶ **Device Name:** Displays the Hostname reported by the device or the Hostname specified in the Static Lease (see **Network»Static Leases** for details).
 - ▶ **IP Address:** Displays the IP Address issued to the Client Device by the Router's DHCP server.
 - ▶ **MAC Address:** Displays the MAC Address of the Client Device.



NOTE: This list will be blank after the Router has been rebooted until the client devices have requested a new DHCP Address from the Router.

3.2.3 Wireless Connections

This Page displays the Client Devices that connected wirelessly to the XWR-1750.

Select the menu **Status»Wireless Connections** to display the following page:

SSID: LuxulXen17502G(Access Point)

Data Received: 4.4 MB

Data Transmitted: 8.8 MB

Clients: 1

MAC Address	Rate
C0:18:85:BC:ED:45	58 Mbps

SSID: LuxulXen17505G(Access Point)

Data Received: 0.0 B

Data Transmitted: 7.6 MB

Clients: 0

- ▶ **SSID:** Displays the SSID (Wireless Network Name) and Wireless Mode.
 - ▶ **Data Received:** Displays the amount of Data Received on this SSID in Megabytes.
 - ▶ **Data Transmitted:** Displays the amount of Data Transmitted by this SSID in Megabytes.
 - ▶ **Clients:** Displays the number of connected Wireless Client devices.
 - ▶ **MAC Address:** Displays the MAC Address of the connected Wireless Client.
 - ▶ **Rate:** Displays the maximum theoretical Data Rate the client is capable of.



NOTE: The information categories are the same for the 2.4GHz SSID and 5GHz SSID.



NOTE: The Rate value for all devices will change depending on Wireless signal quality and strength

3.3 Network

There are four submenus in the Network menu: DHCP Server, Static Leases, Dynamic DNS and Routing. Click a submenu to view and/or modify the corresponding settings.

3.3.1 DHCP Server

This page displays the DHCP Server Settings configured on the Router.

Select the menu **Network»DHCP Server** to display the following page:

DHCP

Enable DHCP Server 

DHCP Range:

Start  192.168.0.

End  192.168.0.

Lease Time (hours) 

- ▶ **DHCP:** Displays the DHCP Server settings of the Router. These settings can be viewed or modified here.
 - ▶ **Enable DHCP Server:** Allows you to Enable or Disable the Router's DHCP Server. Enabled is the default setting.
- ▶ **DHCP Range:** Displays the DHCP Pool settings of the Router. These settings can be viewed or modified here.
 - ▶ **Start:** Allows you to set the Starting IP Address of the DHCP Pool. 192.168.0.100 is the default setting.
 - ▶ **End:** Allows you to set the Ending IP Address of the DHCP Pool. 192.168.0.200 is the default setting.

- ▶ **Lease Time (hours):** Allows you to set the number of Hours the Client Device DHCP Lease is valid before requiring a DHCP Renew. 12 Hours is the default setting.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to the DHCP Server, you must click the Save button to Save your changes. Then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.3.2 Static Leases

This page displays the DHCP Static Leases configured on the Router.

Select the menu **Network»Static Leases** to display the following page:

Static Assignments

Hostname	<input type="text"/>
IP Address	<input type="text"/>
Mac Address	<input type="text" value=" : : : : :"/> <input type="button" value="Add"/>
<input type="button" value="Reboot"/>	

Hostname	IP Address	Mac Address	Modify
MBoulterPC	192.168.0.101	c0:18:85:bc:ed:45	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

- ▶ **Static Assignments:** Allows you to specify a Hostname and IP Address to be assigned to the Client Device with the specified MAC Address. This Device from this point forward will always receive this IP Address from the Router when using DHCP.
- ▶ **Hostname:** Allows you to specify a Hostname for easy identification of the Client Device.

- ▶ **IP Address:** Allows you to specify the IP Address that is assigned to the specified Client Device. The IP Address entered here can be inside or outside of the DHCP Pool configured on the Router (see **Network»DHCP Server** for details).
- ▶ **MAC Address:** Allows you to enter the MAC Address of the Client Device for which the Static Lease is being configured. This is what the Router will use to identify the Client Device and issue the Static Lease.
- ▶ **Add/Update:** Allows you to Add your Static Lease to the Static Leases table or Edit an existing Static Lease. This also Saves the Static Lease settings, allowing you to browse to another page in the Router before rebooting to apply the changes.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Static Leases Table:** Displays the Static Leases configured on the Router and allows you to Edit or Delete individual entries.
 - ▶ **Hostname:** Displays the Hostname of the Client Device.
 - ▶ **IP Address:** Displays the IP Address of the Client Device.
 - ▶ **Mac Address:** Displays the MAC Address of the Client Device.
 - ▶ **Edit:** Allows you to Edit the selected Static Lease by entering the lease information in the Static Assignments section. Simply make changes and click the Update button to Save. This requires a Reboot to apply the changes.
 - ▶ **Delete:** This button allows you to Delete the selected Static Lease and Saves the changes, allowing you to browse to any other setup page.



NOTE: After making any changes to the Static Leases you must click the Add/Update/Delete buttons to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Add/Update/Delete buttons and proceed to other pages without losing your configured changes.

3.3.3 Dynamic DNS

This page displays the Dynamic DNS Settings configured on the Router.

Select the menu **Network»Dynamic DNS** to display the following page.

Dynamic DNS

DNS: ▾

Service Provider ▾

Hostname

Username

Password

Check Interval Minutes

Force Update Interval Days

- ▶ **DNS:** Allows you to Enable or Disable Dynamic DNS support. Disabled is the default.
 - ▶ **Service Provider:** Allows you to specify the DDNS Service Provider Currently, no-ip.com, dyndns.org and freedns.afraid.org are supported.
 - ▶ **Hostname:** Allows you to enter the Dynamic DNS Hostname configured for this Router in your DDNS account. This will be only the Hostname (i.e. mydomain.dyndns.org). Do not include any headings like www. or http://.
 - ▶ **Username:** Allows you to enter the Username used to authenticate the DDNS Provider account. This is the same Username you would use to login to their Web Site.
 - ▶ **Password:** Allows you to enter the Password used when authenticate the DDNS Provider account. This is the same Password you would use to login to their Web Site.
 - ▶ **Check Interval:** Allows you to set how often in minutes the DDNS client on the Router will check for a WAN IP Address change. Ten minutes is the default setting. We do not recommend lowering this value as it can consume excess CPU resources.
 - ▶ **Force Update Interval:** Allows you to set how often in Days the DDNS client on the Router will push an Update to your DDNS Provider. Three days is the default setting. We do not recommend raising this past 30 days as all three supported Providers will age out the Hostname at 30 days.

XWR-1750

- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes; or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to Dynamic DNS you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.3.4 Routing

This page displays the Routing Table of the Router.

Select the menu **Network»Routing** to display the following page:

Active Routes

Destination IP	Subnet Mask	Gateway	Metric	Interface
default	0.0.0.0	192.168.100.1	0	eth0.4081
192.168.0.0	255.255.255.0	0.0.0.0	0	br-lan
192.168.100.0	255.255.255.0	0.0.0.0	0	eth0.4081

- ▶ **Active Routes:** Displays the Active Routes on the Router.
 - ▶ **Destination IP:** Displays the Destination IP Address or IP Range of the Route.
 - ▶ **Subnet Mask:** Displays the Subnet Mask of the Destination IP.
 - ▶ **Gateway:** Displays the Gateway to which the Router forwards the connection. 0.0.0.0 forwards to the router itself, whereas a specified IP forwards to another Network (i.e. the Internet).
 - ▶ **Metric:** Displays the number of Hops needed to connect to this Route in most cases this will be 0.
 - ▶ **Interface:** Displays the Interface of the Router used for the specified Route (i.e. eth0 specifies WAN 1 and br-lan specifies Local Network).

3.4 Wireless

There are three submenus in the Wireless menu: Settings, Profiles and WPS. Click a submenu to view and/or modify the corresponding settings.

3.4.1 Settings

This page displays the Wireless Settings configured on the Router.

Select the menu **Wireless»Settings** to display the following page:

2.4GHz Options

Wireless Radio  Enabled ▾

Wireless Mode  802.11n+g ▾

Channel Width  20MHz ▾

Channel  6 ▾

5GHz Options

Wireless Radio  Enabled ▾

Wireless Mode  802.11ac+n+a ▾

Channel Width  20/40/80MHz Auto ▾

Primary Channel  153 ▾

Save

Reboot

Cancel

- ▶ **2.4GHz Options:** Displays the 2.4GHz Wireless options active on the Router.
 - ▶ **Wireless Radio:** Allows you to Enable or Disable the 2.4GHz Wireless Radio in the Router. Enabled is the default setting.
 - ▶ **Wireless Mode:** Allows you to specify the 802.11 Wireless mode the 2.4GHz Radio will operate in, the supported modes include 802.11n+g and 802.11g. 802.11n+g is the default and recommended setting.
 - ▶ **Channel Width:** Allows you to specify the 2.4GHz Channel Width used by the Router. The supported widths include 20MHz and 20/40MHz Auto. 20MHz is the default and recommended setting.
 - ▶ **Channel:** Allows you to specify the Channel used by the 2.4GHz Radio in the Router. Supported Channels include 1-11 (non-overlapping channels are 1, 6 and 11). 6 is the default setting.



NOTE: When selecting the Channel Width option 20/40MHz, a second Channel option will appear allowing you to set if the secondary channel used by 40MHz is below or above your current Channel.

- ▶ **5GHz Options:** Displays the 5GHz Wireless options active on the Router.
 - ▶ **Wireless Radio:** Allows you to Enable or Disable the 5GHz Wireless Radio in the Router. Enabled is the default setting.
 - ▶ **Wireless Mode:** Allows you to specify the 802.11 Wireless mode to which the 5GHz Radio will operate. Supported modes include 802.11ac+n+a and 802.11a. 802.11ac+n+a is the default and recommended setting.
 - ▶ **Channel Width:** Allows you to specify the 5GHz Channel Width used by the Router. Supported widths include 20/40/80MHz Auto and 20MHz. 20/40/80MHz Auto is the default setting. When selecting the Wireless Mode 802.11a, the Channel Width is forced to 20MHz only.
 - ▶ **Channel:** Allows you to specify the Channel used by the 5GHz Radio in the Router. Supported Channels will change depending on the Wireless Mode. 802.11ac+n+g offers 40 and 153, while 802.11a offers 36, 40, 44, 48, 149, 153, 157, 161 and 165 (the available options are non-overlapping channels). 153 is the default setting.
 - ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
 - ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
 - ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to Wireless Settings you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.

3.4.2 Profiles

This menu displays the Wireless Profile options for 2.4GHz and 5GHz on the Router.

3.4.2.1 2.4GHz

This page displays the 2.4GHz Profile Settings on the Router.

Select the menu **Wireless>>Profiles>>2.4GHz** to display the following page:

Profile List

SSID:

Reboot

- ▶ **Profile List:** Displays the 2.4GHz Wireless Profiles active on the Router.
 - ▶ **SSID:** Allows you to select the Profile you would like to Edit or to Create a new Profile. Select an SSID in the dropdown list.
 - ▶ **Enable/Disable SSID:** Allows you to Enable or Disable the SSID. Enabled is the default setting.
 - ▶ **Operating Mode:** Allows you to select the Operating Mode of the SSID. Access Point is the default setting.
 - ▶ **Network Name (SSID):** Allows you to specify the Network Name (SSID) used to identify the Wireless Network to client devices.
 - ▶ **SSID Broadcast:** Allows you to Enable or Disable the SSID Broadcast. Enabled is the default setting.
 - ▶ **Security Mode:** Allows you to set the desired Security Mode used to connect to the SSID. Supported modes include 64bit/128bit WEP, WPA, WPA2 and WPA/WPA2 Mixed. Open is the default setting. We strongly recommend adding Security to all SSIDs.
 - ▶ **WEP Key:** When selecting WEP Security, a WEP key option will appear. This allows you to set the WEP Key, it can consist of Numbers 0-9 and Letters A-F. For 64bit WEP, enter 10 hexadecimal digits (0-9 and A-F) or 5 regular characters. For 128bit WEP enter 26 hexadecimal digits (0-9 and A-F) or 13 regular characters.

XWR-1750

- ▶ **Encryption:** When selecting WPA or WPA2 security, two options will appear. The first is Encryption, which allows you to set the Encryption type used by WPA/WPA2. Options include AES, TKIP&AES and TKIP. AES is the default and recommended setting.
- ▶ **WPA Passphrase:** When selecting WPA or WPA2 security, two options will appear. The second is WPA Passphrase, which allows you to set the Passphrase used to connect to the SSID. WPA Passphrases must be a minimum of 8 to a maximum of 63 Characters and can contain Letters (capitol and lowercase), Numbers, Special Characters and Spaces.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.
- ▶ **Delete:** Allows you to Delete the current SSID selected. Once you have clicked Delete, you may move to other pages in the Router setup. Delete will require a Reboot to allow the changes to take effect.



NOTE: After making any changes to a Wireless Profile you must click the Save or Delete buttons to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save or Delete button and proceed to other pages without losing your configured changes.



NOTE: WPA/WPA2 with TKIP&AES Encryption Security mode is recommended for high turnover environments like Restaurants or Hotels. This mode covers the widest range of devices.



NOTE: WEP Security is not recommended due to the Security being inherently insecure. WEP is only recommended when devices do not support WPA.

3.4.2.2 5GHz

This page displays the 5GHz Profile Settings on the Router.

Select the menu **Wireless»Profiles»5GHz** to display the following page:

Profile List

SSID:

- ▶ **Profile List:** Displays the current 5GHz Wireless Profiles active on the Router.
 - ▶ **SSID:** Allows you to select the Profile to Edit or to Create a new Profile. Select an SSID in the dropdown list.
 - ▶ **Enable/Disable SSID:** Allows you to Enable or Disable the SSID. Enabled is the default setting.
 - ▶ **Operating Mode:** Allows you to select the Operating Mode of the SSID. Access Point is the default setting.
 - ▶ **Network Name (SSID):** Allows you to specify the Network Name (SSID) used to identify the Wireless Network to client devices.
 - ▶ **SSID Broadcast:** Allows you to Enable or Disable the SSID Broadcast. Enabled is the default setting.
 - ▶ **Security Mode:** Allows you to set the desired Security Mode used to connect to the SSID. Supported modes include 64bit/128bit WEP, WPA, WPA2 and WPA/WPA2 Mixed. Open is the default setting. Adding Security to all SSIDs is recommended.
 - ▶ **WEP Key:** When selecting WEP Security a WEP key option will appear. This allows you to set the WEP Key. It can consist of Numbers 0-9 and Letters A-F. For 64bit WEP, enter 10 hexadecimal digits (0-9 and A-F) or 5 regular characters. For 128bit WEP, enter 26 hexadecimal digits (0-9 and A-F) or 13 regular characters.

XWR-1750

- ▶ **Encryption:** When selecting WPA or WPA2 security, two new options will appear. The first is Encryption, which allows you to set the Encryption type used by WPA/WPA2. Options include AES, TKIP&AES and TKIP. AES is the default and recommended setting.
- ▶ **WPA Passphrase:** When selecting WPA or WPA2 security two new options will appear. The second is WPA Passphrase, which allows you to set the Passphrase used to connect to the SSID. WPA Passphrases must be a minimum of 8 to a maximum of 63 Characters and can contain Letters (capitol and lowercase), Numbers, Special Characters and Spaces.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.
- ▶ **Delete:** Allows you to Delete the current SSID selected. Once you have clicked Delete, you may move to other pages in the Router setup. Delete will require a Reboot to allow the changes to take effect.



NOTE: After making any changes to a Wireless Profile you must click the Save or Delete buttons to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save or Delete button and proceed to other pages without losing your configured changes.



NOTE: WPA/WPA2 with TKIP&AES Encryption Security mode is recommended for high turnover environments like Restaurants or Hotels. This mode covers the widest range of devices.



NOTE: WEP Security is not recommended due to the Security being inherently insecure. WEP is only recommended when devices do not support WPA.

3.5 Guest Network

This page displays the Guest Network Settings currently configured on the Router.

Select the menu **Wireless»Guest Network** to display the following page:

Guest SSID

Enable/Disable SSID  Disabled ▾

Network Name (SSID) 

SSID Broadcast  Enabled ▾

Security Mode  Open ▾

Guest DHCP

Enable DHCP Server  Enabled ▾

DHCP Range:

Start 

End 

Lease Time (hours) 

- ▶ **Guest SSID:** Displays the current Guest Network settings active on the Router.
 - ▶ **Enable/Disable SSID:** Allows you to Enable or Disable the SSID. Disabled is the default setting.
 - ▶ **Network Name (SSID):** Allows you to specify the Network Name (SSID) used to identify the Wireless Network to client devices.
 - ▶ **SSID Broadcast:** Allows you to Enable or Disable the SSID Broadcast. Enabled is the default setting.
 - ▶ **Security Mode:** Allows you to set the desired Security Mode used to connect to the SSID. Supported modes include 64bit/128bit WEP, WPA, WPA2 and WPA/WPA2 Mixed. Open is the default setting. Adding Security to any SSIDs is recommended.
 - ▶ **WEP Key:** When selecting WEP Security a WEP key option will appear. This allows you to set the WEP Key. It can consist of Numbers 0-9 and Letters A-F. For 64bit WEP, enter 10 hexadecimal digits (0-9 and A-F) or 5 regular characters. For 128bit WEP, enter 26 hexadecimal digits (0-9 and A-F) or 13 regular characters.
 - ▶ **Encryption:** When selecting WPA or WPA2 security, two new options will appear. The first is Encryption, which allows you to set the Encryption type used by WPA/WPA2. Options include AES, TKIP&AES and TKIP. AES is the default and recommended setting.

XWR-1750

- ▶ **WPA Passphrase:** When selecting WPA or WPA2 security two new options will appear. The second is WPA Passphrase, which allows you to set the Passphrase used to connect to the SSID. WPA Passphrases must be a minimum of 8 to a maximum of 63 Characters and can contain Letters (capitol and lowercase), Numbers, Special Characters and Spaces.
- ▶ **Guest DHCP:** Displays the Guest Network DHCP Server settings of the Router.
 - ▶ **Enable DHCP Server:** Allows you to Enable or Disable the Routers DHCP Server. Enabled is the default setting.
- ▶ **DHCP Range:** Displays the DHCP Pool settings of the Router. Settings can be viewed or modified here.
 - ▶ **Start:** Allows you to set the Starting IP Address of the DHCP Pool. 192.168.10.100 is the default setting.
 - ▶ **End:** Allows you to set the Ending IP Address of the DHCP Pool. 192.168.10.200 is the default setting.
 - ▶ **Lease Time (hours):** Allows you to set the number of Hours for which the DHCP Lease issued to the Client Device is valid before requiring a DHCP Renew. 12 Hours is the default setting.
 - ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
 - ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
 - ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to the Guest Network you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.



NOTE: WPA/WPA2 with TKIP&AES Encryption Security mode is recommended for high turnover environments like Restaurants or Hotels. This mode covers the widest range of devices.



NOTE: WEP Security is not recommended due to the Security being inherently insecure. WEP is only recommended when devices do not support WPA.

3.6 Firewall/Security

There are six submenus in the Firewall/Security menu: Port Forwarding, DMZ, UPnP, IP-MAC Binding, URL Filtering and Client Filtering. Click a submenu to view and/or modify the corresponding settings.

3.6.1 Port Forwarding

This page displays the Port Forwarding Rules configured on the Router.

Select the menu **Firewall/Security>>Port Forwarding** to display the following page:

Port Forwarding

Forward Individual Ports From WAN to LAN

Application Name	Protocol	WAN Port	LAN IP	LAN Port	
<input type="text"/>	Both ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add
Application	Protocol	WAN Port	LAN IP	LAN Port	
RemoteAccess	Both	8080	192.168.0.1	80	Remove

- ▶ **Port Forwarding:** Allows you to open public Ports to allow access to the private Port of a local device. Port Forwarding opens a hole in the Firewall to the specified Local Network device. Port Forwarding relies on the security of the Local Network device as it merely allows the incoming connection to reach the Local Network device.
 - ▶ **Application Name:** Allows you specify a Name for the Port Forwarding rule for easy identification. Special characters or spaces in the Application Name are not recommended.
 - ▶ **Protocol:** Allows you to specify whether to use TCP, UPD or Both protocols to pass the Port Forwarding traffic. Both is the default and recommended setting.
 - ▶ **WAN Port:** Allows you to specify the Public Port to be opened. This Port will match the LAN Port in most configurations. The WAN Port does not need to match the LAN Port, allowing you to serve Multiple devices on the Local Network on the same Port (i.e. 80) with differing WAN Ports (i.e. you have three devices that serve over Port 80. You can set the first WAN Port to 80, the second to 81 and third to 82). The WAN Port can also be different if the LAN Port is well known (i.e. 80, 443, 59, 22, etc...) and you wish to hide it behind a less well known port (i.e. 5001).
 - ▶ **LAN IP:** IP Address of the Local Network device you are Port Forwarding too.
 - ▶ **LAN Port:** The Local Network Port served by the Local Network device, typically the same as the WAN Port.

XWR-1750

- ▶ **Add:** Click the Add button to add your Port Forwarding Rule to the Port Forwarding Table. This also Saves the Port Forwarding settings, allowing you to browse to another page in the Router before rebooting to apply the changes.
- ▶ **Port Forwarding Table:** Displays the configured Port Forwarding Rules.
 - ▶ **Application Name:** Displays the Application Name of the Rule.
 - ▶ **Protocol:** Displays the permitted Protocol of the Rule.
 - ▶ **WAN Port:** Displays the WAN Port specified on for the Rule.
 - ▶ **LAN IP:** Displays the IP Address of the Local Network device to which incoming traffic will be redirected.
 - ▶ **LAN Port:** Displays the Port of the Local Network device to which incoming traffic will be redirected.
 - ▶ **Remove:** This button allows you to Delete the selected Port Forwarding Rule and Saves the changes, allowing you to browse to any other setup page.



NOTE: After Adding a Port Forwarding Rule your settings are Saved, then you must click the Reboot button for the changes to take effect. You can click the Add button and proceed to other pages without losing your configured changes.



NOTE: Port Forwarding is inherently insecure, relying on the security of the Local Network device to which you are forwarding. With this being the case, requiring a Login to the Local device is recommended while also changing the Default Username and Password of the device.

3.6.2 DMZ

This page displays the DMZ Settings currently configured on the Router.

Select the menu **Firewall/Security»DMZ** to display the following page.

DMZ

DMZ(De-Militarized Zone)  Disabled ▾

IP Address  192.168.0.1

- ▶ **DMZ:** Displays the DMZ currently configured.
 - ▶ **DMZ (De-Militarized Zone):** Allows you to Enable or Disable the DMZ on the Router. Disabled is the default setting. Enabling the DMZ and entering a Local Device IP Address, will Disable all Incoming Firewall Rules for the specified Device.

- ▶ **IP Address:** Allows you to specify the Local Device IP Address to which all incoming traffic should be passed.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to the DMZ you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.



NOTE: DMZ is typically used for Web Server installations and all Firewall and Security resides on the device specified in the DMZ. Please consult your Network Administrator if you are asked to configuring a DMZ.

3.6.3 UPnP

This page displays the UPnP Settings currently configured on the Router.

Select the menu **Firewall/Security>>UPnP** to display the following page:

UPnP Configuration

UPnP:

Available Networks

Local Network/LAN:

Guest Network:

Current UPnP Leases

WAN Port	LAN IP	LAN Port	Protocol

- ▶ **UPnP Configuration:** Displays the UPnP (Universal Plug and Play) configuration.
 - ▶ **UPnP:** Allows you to Enable or Disable UPnP on the Router. Enabled is the default.
- ▶ **Available Networks:** Displays which Networks on the Router have UPnP Enabled.
 - ▶ **Local Network/LAN:** Allows you to enable UPnP for the configured Local Network.

XWR-1750

- ▶ **Guest Network:** Allows you to enable UPnP for the configured Guest Network.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **Cancel:** This button Cancels any changes made on this page.
- ▶ **Current UPnP Leases:** Displays the active UPnP (Universal Plug and Play) Port Leases.
- ▶ **WAN Port:** Displays the WAN Port opened by the UPnP Device Lease.
- ▶ **LAN IP:** Displays the Local Network IP Address of the UPnP Device that requested the Lease.
- ▶ **LAN Port:** Displays the LAN Port used by the UPnP Device.
- ▶ **Protocol:** Displays the Protocol (TCP/UDP/Both) set by the UPnP Device.



NOTE: After making any changes to the DMZ you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.



NOTE: UPnP is more secure than Port Forwarding as the Port is only open for a short time. Once the Port Lease expires, the UPnP Lease is Deleted. Client devices supporting UPnP initiate the Lease request. This process is not configurable by the user.

3.6.4 IP-MAC Binding (Future Release)

This page displays the IP-MAC Binding Settings currently configured on the Router.

Select the menu **Firewall/Security»IP-MAC Binding** to display the following page:

- ▶ This feature is under construction. To be notified of Firmware Releases including new features please Join our Mailing List at <http://luxul.com>.

3.6.5 URL Filtering (Future Release)

This page displays the URL Filtering Rules currently configured on the Router.

Select the menu **Firewall/Security»URL Filtering** to display the following page:

- ▶ This feature is under construction. To be notified of Firmware Releases including new features please Join our Mailing List at <http://luxul.com>.

3.6.6 Client Filtering (Future Release)

This page displays the Client Filtering Rules currently configured on the Router:

Select the menu **Firewall/Security>Client Filtering** to display the following page.

- ▶ This feature is under construction. To be notified of Firmware Releases including new features please Join our Mailing List at <http://luxul.com>.

3.7 QoS

QoS (Quality of Service) Allows you to specify at what Priority (Normal, Priority, Express or Bulk) a packet is forwarded. QoS as implemented on the Router allows you to target packets by Source Host, Protocol (TCP/UDP/All) and/or TCP Port Number.

Select the menu **QoS** to display the following page:

QoS Setup

QoS Service ⓘ Disabled ▾

Calculate Overhead ⓘ Disabled ▾

Download Speed (Mbps) ⓘ 5

Upload Speed (Mbps) ⓘ 2

Save Reboot

QoS Rules ⓘ

Service Level	Source Host	Protocol	Ports	
Normal ▾	All	All ▾	All	Add
Service Level	Source Host	Protocol	Ports	
Priority			22,53	Del
Express			5060	Del

- ▶ **QoS Setup:** Displays the QoS settings running on the Router.
 - ▶ **QoS Service:** Allows you to Enable or Disable the QoS service on the Router. Disabled is the default setting.
 - ▶ **Calculated Overhead:** Allows you to Enable or Disable the Calculated Overhead function in QoS. Disabled is the default setting. Calculated Overhead is used by the Router to manage fluctuating bandwidth supplied by the Internet connection. This function keeps the Router from overrunning the available bandwidth.
 - ▶ **Download Speed:** Allows you to specify the Download Speed in Megabits per second allowed in the QoS Rules. 5Mbps is the default setting.

XWR-1750

- ▶ **Upload Speed:** Allows you to specify the Upload Speed in Megabits per second allowed in the QoS Rules. 2Mbps is the default setting.
- ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
- ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **QoS Rules:** Allows you to configure QoS Rules.
 - ▶ **Service Level:** Allows you to specify the QoS Service Level used for this Rule. Normal is the default setting.
 - ▶ **Source Host:** Allows you to specify by IP Address to which Host(s) this Rule will apply. All is the default setting. and applies this Rule to all packets transmitted to the WAN Port.
 - ▶ **Protocol:** Allows you to specify what Protocol is targeted by this Rule: TCP, UDP or All. All is the default setting.
 - ▶ **Ports:** Allows you to specify the Port(s) targeted by this Rule. All is the default setting. You can specify multiple Ports in a single rule by separating the Port numbers with a comma (i.e. 23,53,80,443).
 - ▶ **Add:** Click the Add button to add your QoS Rule to the QoS Table. This also Saves the QoS Rule, allowing you to browse to another page in the Router before rebooting to apply the changes.
- ▶ **QoS Rules Table:** Displays the QoS Rules currently running on the Router.
 - ▶ **Service Level:** Displays the QoS Service Level used for this Rule. Normal is the default setting.
 - ▶ **Source Host:** Displays the IP Address(es) to which this Rule will apply. All is the default setting and applies this Rule to all packets transmitted to the WAN Port.
 - ▶ **Protocol:** Displays what Protocol is targeted by this Rule: TCP, UDP or All. All is the default setting.
 - ▶ **Ports:** Displays the Port(s) targeted by this Rule. All is the default setting. You can specify multiple Ports in a single rule by separating the Port numbers with a comma (i.e. 23,53,80,443).
 - ▶ **Del:** This button allows you to Delete the selected QoS Rule and Saves the changes, allowing you to browse to any other setup page. Most changes will require a Reboot to allow the changes to take effect.



NOTE: After making any changes to QoS you must click the Save/Add buttons to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save/Add buttons and proceed to other pages without losing your configured changes.



NOTE: If QoS is configured incorrectly, it may be required to Reset the Router to Default Settings. Please back up any configuration before attempting to Enable QoS.

3.8 VPN

There are three submenus in the VPN menu: PPTP Server, PPTP Users and L2TP. Click a submenu to view and/or modify the corresponding settings.

3.8.1 PPTP Server

This page displays the PPTP Server Settings configured on the Router.

Select the menu **VPN»PPTP Server** to display the following page:

PPTP Server

PPTP Server  Disabled ▾

Starting IP Address  192.168.0. 20

Ending IP Address  192.168.0. 30

- ▶ **PPTP Server:** Displays the current PPTP VPN settings of the Router.
 - ▶ **PPTP Server:** Allows you to Enable or Disable the PPTP Server on the Router. Disabled is the default setting.
 - ▶ **Starting IP Address:** Allows you to set the Starting IP Address of the DHCP Pool used by the VPN Server. 192.168.0.20 is the default setting.
 - ▶ **Ending IP Address:** Allows you to set the Ending IP Address of the DHCP Pool used by the VPN Server. 192.168.0.30 is the default setting.
 - ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot for the changes to take effect.
 - ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
 - ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to the VPN Server you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.



NOTE: The DHCP Pool used by the VPN Server must be outside the DHCP Pool used by the DHCP Server (see **Network»DHCP Server** for current settings).

3.8.2 PPTP Users

This page displays the PPTP User settings configured on the Router.

Select the menu **VPN»PPTP Users** to display the following page:

PPTP User Configuration

Username

Password

S.No.	Username	
1.	test	<input type="button" value="Remove"/>

- ▶ **PPTP Users Configuration:** Displays the PPTP User configuration options on the Router.
 - ▶ **Username:** Allows you to enter a Username for the VPN User.
 - ▶ **Password:** Allows you to enter a Password for the VPN User.
 - ▶ **Add:** Click the Add button to add your VPN User to the VPN Users Table. This also Saves the VPN User, allowing you to browse to another page in the Router before rebooting to apply the changes.
 - ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
- ▶ **PPTP Users Table:** Displays the current PPTP Users configured on the Router.
 - ▶ **S.No.:** Displays the VPN User ID number.
 - ▶ **Username:** Displays the configured VPN Username.
 - ▶ **Remove:** This button allows you to Delete the selected VPN User and Saves the changes, allowing you to browse to any other setup page. Most changes will require a Reboot to allow the changes to take effect.



NOTE: After making any changes to the VPN Users you must click the Add/Remove buttons to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Add/Remove buttons and proceed to other pages without losing your configured changes.



NOTE: If the password for the VPN User is lost or incorrect, you must Remove and re-add the User.

3.8.3 L2TP (Future Release)

This page displays the L2TP Settings configured on the Router.

Select the menu **VPN»L2TP** to display the following page:

- ▶ This feature is under construction. To be notified of Firmware Releases including new features please Join our Mailing List at <http://luxul.com>.

3.9 Administration

There are six submenus in the Administration menu: Admin Password, Firmware Update, Factory Defaults, Backup/Restore, System Log and Set Time. Click a submenu to view and/or modify the corresponding settings.

3.9.1 Admin Password

This page displays the Admin Password settings configured on the Router.

Select the menu **Administration»Admin Password** to display the following page:

Administrator Login

Password

Confirm Password

XWR-1750

- ▶ **Administrator Login:** Displays the Admin Password settings of the Router.
 - ▶ **Password:** Allows you to enter a new Admin Password for the Router.
 - ▶ **Confirm Password:** Allows you to confirm the new Admin Password for the Router.
 - ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save, you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
 - ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
 - ▶ **Cancel:** This button Cancels any changes made on this page.



NOTE: After making any changes to the Admin Password you must click the Save button to Save your changes, then you must click the Reboot button for the changes to take effect. You can click the Save button and proceed to other pages without losing your configured changes.



NOTE: If the Admin Password is lost or incorrect, you must Reset the Router to Factory Defaults and re-configure the Router. Please back up any configuration before changing the Admin Password.

3.9.2 Firmware Update

This page displays the Firmware Update of the Router.

Select the menu **Administration»Firmware Update** to display the following page:

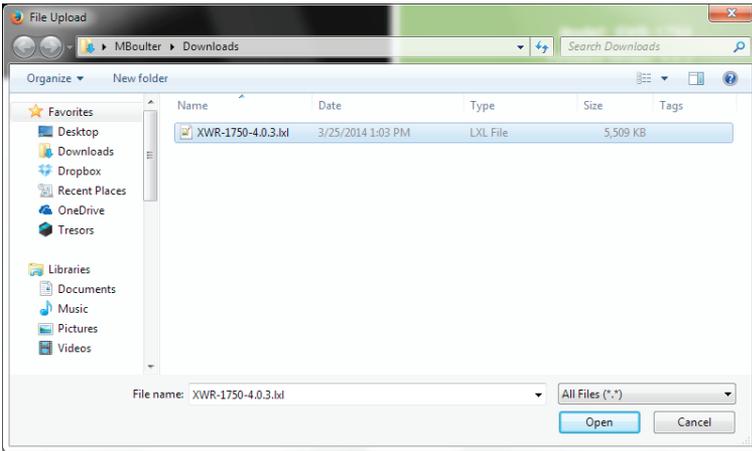
Firmware Update

Select File

XWR-1750-4.0.3.txl

Start Upgrade

- ▶ **Firmware Update:** Displays the Firmware Update actions.
 - ▶ **Select Files:** Allows you to Browse your computer for the Firmware Update file and displays the filename of the file selected. Click the Browse button to open the File Explorer of your computer. Select the Firmware file and click Open.



- ▶ **Start Upgrade:** Allows you to Start the Upgrade process. Click upgrade to begin the Upgrade process. The Router will reboot as part of the Upgrade process. Once the Upgrade is in process, the following Progress bar is displayed. Do not Power Down the Router during this process as Upgrade Failure may result.

Firmware Upgrade is in Progress. Please Wait...



NOTE: Please back up any configuration before performing a Firmware Update.

3.9.3 Factory Defaults

This page displays the Factory Defaults and WAN Acceleration Status of the Router.

Select the menu **Administration»Factory Defaults** to display the following page:

Factory Defaults

Restore Factory Defaults

Reset & Reboot

WAN Acceleration Status

WAN Acceleration



Disable ▾

Save

- ▶ **Factory Defaults:** Displays the Factory Default action.
 - ▶ **Restore Factory Defaults:** Allows you to Restore the Router to Factory settings. Click the Reset & Reboot button to perform the Restore. Do not Power Down the Router during this process as Restore failure may result.
- ▶ **WAN Acceleration Status:** Displays the current WAN Acceleration Status.
 - ▶ **WAN Acceleration:** Allows you to Enable or Disable WAN Acceleration. Enabled is the default setting. WAN Acceleration allows the Router to pass packets at near-wire speeds on Internet connections exceeding 120Mbps.
 - ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save in WAN Acceleration you do not need to reboot the Router. WAN Acceleration can take up to two minutes to become active.



NOTE: Factory Defaults will remove any custom configuration options configured on the Router. It will not remove Firmware Updates.



NOTE: If after Enabling WAN Acceleration your Internet connection becomes unstable, please Disable WAN Acceleration.

3.9.4 Backup/Restore

This page displays the Backup/Restore options of the Router.

Select the menu **Administration»Backup/Restore** to display the following page:

Backup Configuration

Save to File

Backup

Restore Configuration

Select a File

Browse...

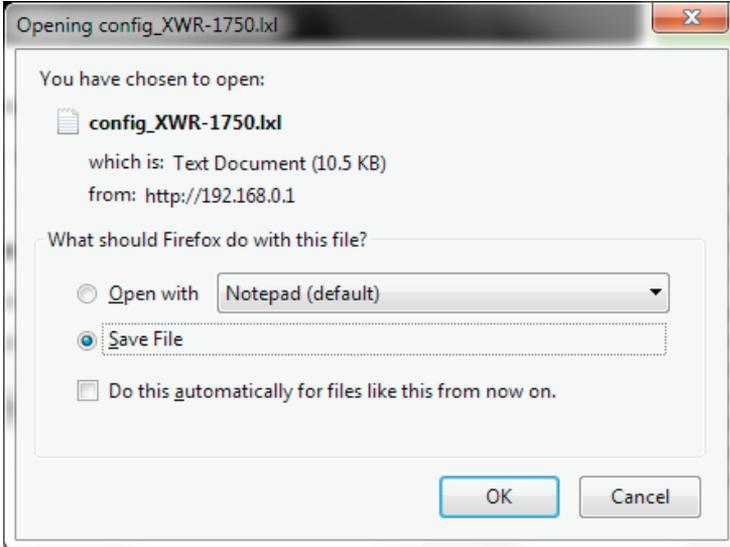
No file selected.

Upload Configuration

Restore

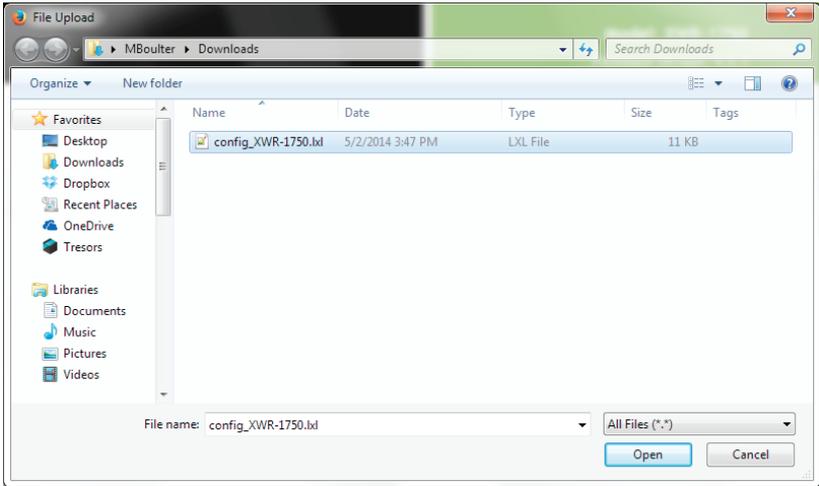
Reboot

- **Backup Configuration:** Displays the Backup action.
- **Save to File:** Allows you to Save the Router configuration to a File. Click the Backup button to open the Save File dialog box of your computer and Save the file.



XWR-1750

- ▶ **Restore Configuration:** Displays the Restore Configuration actions.
- ▶ **Select a File:** Allows you to Browse your computer for the Configuration file and displays the filename of the file selected. Click the Browse button to open the File Explorer of your computer. Select the Configuration file and click Open.



- ▶ **Restore:** Allows you to Start the Restore process. Click Restore to begin the Restore Configuration process, the Router will reboot as part of the Restore process. Once the Restore is finished, you must click the Reboot button to apply the changes.
- ▶ **Reboot:** This button is used to Reboot the Router after Configuration Restore.



NOTE: Restore Configuration will overwrite any changes made after the file was generated.

3.9.5 Systems Log

This page displays the System Log of the Router.

Select the menu **Administration»System Log** to display the following page:

System Log

Save to File

Fri Apr 18 19:36:10 2014 daemon.info dnsmasq-dhcp[1410]:
DHCPACK(br-lan) 192.168.0.101 c0:18:85:bc:ed:45 MBoulter-PC

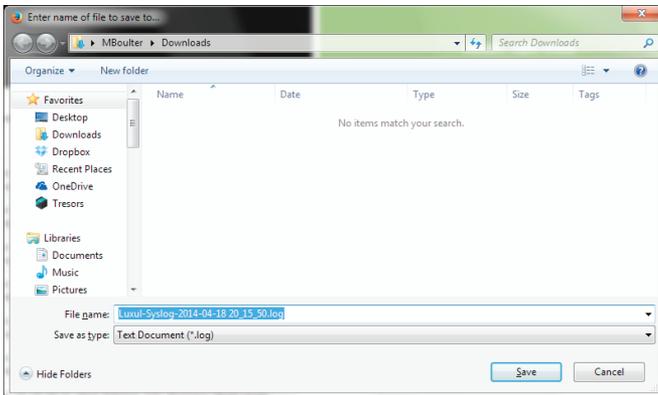
Fri Apr 18 19:37:17 2014 daemon.info dnsmasq-dhcp[1410]:
DHCPINFORM(br-lan) 192.168.0.101 c0:18:85:bc:ed:45

Fri Apr 18 19:37:17 2014 daemon.info dnsmasq-dhcp[1410]:
DHCPACK(br-lan) 192.168.0.101 c0:18:85:bc:ed:45 MBoulter-PC

Fri Apr 18 19:38:24 2014 daemon.info dnsmasq-dhcp[1410]:
DHCPINFORM(br-lan) 192.168.0.101 c0:18:85:bc:ed:45

► **System Log:** Displays the System Log entries.

- **Save to File:** Allows you to Save the System Logs to a File. Click the Save button to open the Save File dialog box of your computer and Save the file.



NOTE: A reboot of the Router will clear the System Logs if you are experiencing issues please attempt to Save the System Log prior to the reboot operation.



NOTE: System Log files are standard text files and can be viewed in all text editors. We recommend Notepad++.

3.9.5 Set Time

This page displays the Time settings of the Router.

Select the menu **Administration»Set Time** to display the following page:

Router Time Setup

Current Date/Time : Fri Apr 18 15:05:08 MDT 2014

Time Zone :

- ▶ **Router Time Setup:** Displays the Time settings of the Router.
 - ▶ **Current Date/Time:** Displays the NTP Time parameters pulled from the Internet using the current Time settings.
 - ▶ **Time Zone:** Allows you to set the Time Zone used by the Router.
 - ▶ **Save:** This button is used to Save the configuration changes made on this page. Once you have clicked Save you may move to other pages in the Router setup. Most changes will require a Reboot to allow the changes to take effect.
 - ▶ **Reboot:** This button is used to Reboot the Router after making configuration changes or can be used to Reboot the Router for any reason.
 - ▶ **Cancel:** This button Cancles any changes made on this page.

3.10 Tools

There are two submenus in the Tools menu: Iperf and USB. Click a submenu to view and/or modify the corresponding settings.

3.10.1 Iperf

This page displays the Iperf settings of the Router.

Select the menu **Tools»Iperf** to display the following page:

Iperf Server

Status Not Running

Run for

Action

- ▶ **Iperf Server:** Displays the Iperf Server Status.
 - ▶ **Status:** Displays the current Running Status of the Iperf Server.
 - ▶ **Run for:** Allows you to choose how long you would like the Iperf Server to run. One Hour is the default setting, with two and three hours available.
 - ▶ **Action:** Allows you to Start the Iperf Server. Click the Start Iperf Server button to Start the Iperf Server.



NOTE: The Iperf Server runs only for the specified time and will shut down after that period has elapsed to prevent any potential overuse of resources.

3.10.2 USB (Future Release)

This page displays the USB Settings configured on the Router.

Select the menu **Tools>>USB** to display the following page:

- ▶ This feature is under construction. To be notified of Firmware Releases including new features please Join our Mailing List at <http://luxul.com>.

4 REGULATORY COMPLIANCE

The device complies with internationally recognized standards covering human exposure to electromagnetic fields from radio devices. This equipment also complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Unauthorized antennas, modifications, or attachments could cause damage and may violate regulatory approvals. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate the equipment. The equipment version marketed in the U.S. is restricted to usage of channels 1-11 only on 2.4GHz

Health and Safety Recommendations

Warnings for the use of Wireless Devices: Please observe all warning notices with regard to the usage of wireless devices

Potentially Hazardous Atmospheres: You are reminded of the need to observe restrictions on the use of radio devices in fuel depots, chemical plants etc. and areas where the air contains chemicals or particles (such as grain, dust, or metal powders).

Safety in Hospitals: Wireless devices transmit radio frequency energy and may affect medical electrical equipment. When installed adjacent to other equipment, it is advised to verify that the adjacent equipment is not adversely affected.

RF Exposure Guidelines

Safety Information: The device complies with internationally recognized standards covering human exposure to electromagnetic fields from radio devices.

Warning: Exposure to Radio Frequency (RF) Radiation:

The radiated output of this device is below the FCC radio frequency exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during normal operation is minimized.

- ▶ The end user must avoid any extended human RF exposure directly in front of the device, up to a distance of 20cm, when unit is on.
- ▶ When servicing the equipment and selecting a location for the antennas, it is important to note that a minimum distance of 20cm is required between personnel and the device or antenna to comply with the radio frequency exposure limit.
- ▶ The antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

The following safety precautions should be observed:

- ▶ Do not touch or move the antenna while the unit is transmitting or receiving.
- ▶ Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- ▶ Do not operate the radio or attempt to transmit data unless the antenna is connected; this behavior may cause damage to the radio.

Remote and Standalone Antenna Configurations: To comply with FCC RF exposure requirements, antennas that are mounted externally at remote locations or operating near users at stand-alone desktop or similar configurations must operate with a minimum separation distance of 20 cm from all persons.

FCC Statement—Wireless FCC 2.4GHz 802.11bgn

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radio Frequency Interference Requirements—FCC

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.

Radio Transmitters (Part 15)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



Hereby, Luxul, 14203 Minuteman Drive, Suite 201, Draper, Utah, 84020, declares that this Luxul device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

For a copy of this report send a self addressed stamped envelope to:
Luxul CE, 14203 Minuteman Drive, Suite 201, Draper, Utah, 84020.

Industry Canada (RSS-Gen Issue 2)

This device complies with Industry Canada licence-exempt RSS standard(s). 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The device meets the exemption from the routine evaluation limits in section 2.5 of RSS 102 and compliance with RSS-102 RF exposure, users can obtain Canadian information on RF exposure and compliance.

Le dispositif rencontre l'exemption des limites courantes d'évaluation dans la section 2.5 de RSS 102 et la conformité à l'exposition de RSS-102 rf, utilisateurs peut obtenir l'information canadienne sur l'exposition et la conformité de rf.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Cet émetteur ne doit pas être Co-placé ou ne fonctionnant en même temps qu'aucune autre antenne ou émetteur. Cet équipement devrait être installé et actionné avec une distance minimum de 20 centimètres entre le radiateur et votre corps.

CAN ICES-03(B)/NMB-3(B)

APPENDIX 1: COMMON COMMANDS

Common Commands	Description
Cmd	Enter the command line mode of a Windows system (applicable to Windows2000 and higher).
ipconfig	Displays the IP address of any network adapters on the computer. (i.e. ipconfig /all) Must be run from the command line.
Ping	Used to test for network connectivity and device/system recognition. A device sends a packet to the target host and asks for a response. If the device receives a response from the target host, it can then see the network response time and connection status between the local device and target host. (i.e. ping 192.168.0.1) Must be run from the command line.
netstat	Displays details of active network connections including routing table and network interface information. Can also be used to count the active network connections. Must be run from the command line.
Tracert	Displays the path taken by a packet before reaching the target host and the specific time when it reached each node. Similar to the Ping command, but provides more detailed information. Displays the entire path and IP address of each node in the path and total elapsed time. Must be run from the command line.