LUXUL

Simply Connected

User Guide

XBR-2300
Luxul Xen™
Enterprise Dual-WAN Router

ROUTER

Use the XBR-2300 to:

- Provide Core Functionality to Your Luxul Network
- Protect Your Network with Advanced Firewall and Security Features
- Enable VPN Access
- Optimize Network Applications with QoS

luxul.com

ENTERPRISE DUAL-WAN ROUTER

MODEL NUMBER: XBR-2300

USER GUIDE

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.

CONTENTS

1: PRODUCT OVERVIEW

1.1 Product Introduction

The Luxul XBR-2300 Enterprise Dual-WAN 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 XenSmart™ web-based management tools and dual-WAN ports; along with advanced security, VPN, and bandwidth control features, the XBR-2300 provides the ideal foundation upon which to build your Luxul network.

1.2 Product Features

- Complies with IEEE802.3, IEEE802.3u and IEEE802.3x
- Two 10/100M auto-negotiating WAN interfaces
- Three 10/100M auto-negotiating LAN interfaces
- Support for Dual-WAN Access, Automatic Load Balancing, Automatic Failover and IP Groups
- Protocol Support for TCP/IP, UDP, VPN, DHCP, NAT, SMTP, DNS, FTP
- Implements IP-MAC binding to prevent ARP attacks, ARP cheats and unauthorized access
- Special application access control over port, MAC and URL to manage network security and access
- Flexible bandwidth management and single-device limitation settings to provide bandwidth stability and optimal utilization of network resources
- 384MHz processor and powerful NAT forwarding features support up to 256 concurrent data streams and processes
- Support for Port Forwarding, DMZ hosts and ALG applications
- VPN server supports PPTP VPN clients
- PPTP VPN server function gives up to 8 groups of users simultaneous access to internet while providing a secure connection
- Supports website address classification and filters to facilitate management of domain names
- Supports Dynamic Domain Name System or DDNS
- Provides system security logs and flow statistics
- XenSmart™ Web Management

- XenConnect "Plug and Play" Compatibility
- Built-in DHCP server with static address distribution
- ARP attack prevention to provide network security and stability
- Internal firewall for management of user network access, domain name filters and MAC address filters
- 1U steel chassis

1.3 Product Specifications

Supported Protocols and Standards	▸ IEEE 802.3 10Base-T Ethernet ▸ IEEE 802.3u 100Base-TX Fast Ethernet ▸ IEEE 802.3 NWay Auto-negotiation ▸ IEEE 802.3x Flow Control ▸ TCP/IP ▸ PPPoE ▸ DHCP ▸ DNS ▸ ICMP ▸ NAT ▸ HTTP ▸ ARP
Features	▸ Number of Ports: 2 10/100BASE-T WAN; 3 10/100BASE-T LAN ▸ Auto Uplink (MDI/MDI-X) detection and configuration ▸ Load Balancing and Failover between WAN ports ▸ Quality of Service (QoS): for priority queuing and processing ▸ Built in DHCP server: Auto IP address configuration ▸ Dynamic DNS ▸ Port forwarding ▸ Syslog: Supports up to 3 Syslog and SNTP servers ▸ Virtual server: Specify protocol, port range and remote IP range ▸ UPnP: Enables discovery and control of network devices and services
Firewall and Security	▸ Stateful Packet Inspection (SPI) ▸ Network Address Translation (NAT) ▸ Block user's access of internet ▸ Block user's access of specific websites ▸ URL blocking by address or keywords ▸ IP/Port/MAC address/URL filtering
Quality of Service (QoS)	▸ Port based bandwidth control
Virtual Private Network (VPN) Support	▸ PPTP VPN server ▸ Support for 8 consecutive remote users

Management Features	▸ Remote Management through Web Based GUI ▸ System logging and status ▸ Account reporting and statistics ▸ Web based firmware and configuration updates
Interface Options	▸ RJ-45: ▹ 10 Base-T: Cat.5 UTP /STP ▹ 100 Base-TX: Cat.5 UTP /STP ▸ Cable Recognition for Straight-through or Crossover Cables
Certifications	FCC Class B, CE, RoHS
Led	▸ Per unit: Power ▸ Per port: Link/Activity
Power Consumption	5 Watts Maximum
Power Supply	Internal Switched Power, AC100-240V, 50-60Hz input
Operating Temperature	32°F to 104°F (0°C to 40°C)
Operating Humidity	10% to 95% (Relative Humidity Non-condensing)
Dimensions	W: 11.6" x D: 7" x H: 1.7" (W: 294mm x D: 178.8mm x H: 44mm)
Weight	▸ Item: 4.5 lbs (2.1Kg) ▸ Packaging: 6 lbs (2.7Kg)

1.4 Package Contents

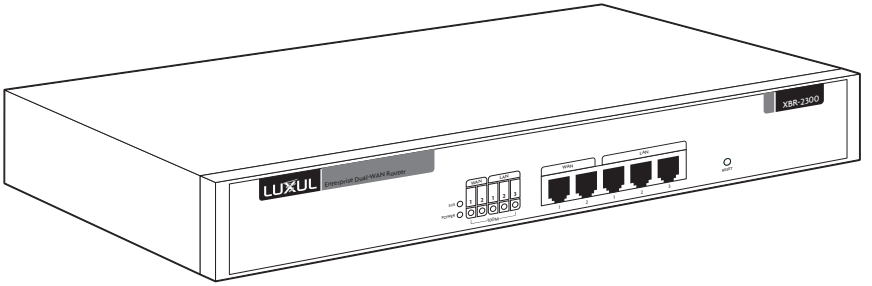
The following items should be included in the box:

- XBR-2300 Enterprise Dual-WAN Router
- Power Cord
- Two L-shaped rack mounting brackets and screws
- Four rubber pads
- Quick Installation Guide
- CD-ROM with User Documentation

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

2: HARDWARE DESCRIPTION

2.1 Front Panel



XBR-2300 Front Panel View

- **Factory Reset Button:** Used to restore factory default settings.
  - **To reset to factory defaults**, press and hold the reset button until the SYS LED turns off, approx. 10 seconds. A factory reset may take approximately a minute to complete. A successful Factory Reset is indicated by all of the Port LEDs flashing once. When the SYS LED turns on the unit is ready.

NOTE: To hard reset the router use the power switch. Turn the router off, wait 5 seconds and turn the unit back on.

CAUTION: Resetting the XBR-2300 to factory defaults will remove all custom settings.

2.2 LED Indicators

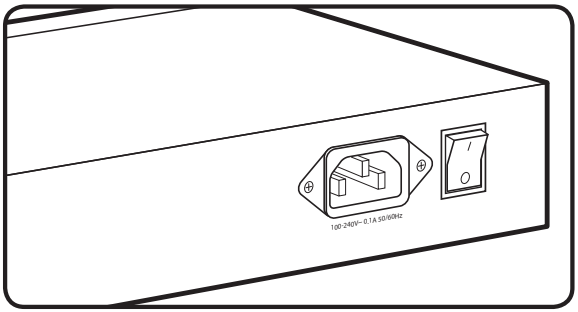
Indicator	Description	Function
POWER	Power LED	ON indicates the XBR-2300 has power.
SYSTEM	System Status LED	Flashing indicates the XBR-2300 is functioning correctly. ON indicates the XBR-2300 is booting. Off indicates the system is not functioning correctly.

Indicator	Description	Function
WAN/LAN	WAN and LAN Status LED	ON indicates the WAN/LAN port is connected correctly. Flashing indicates data packets are being transferred.
100Mbps	WAN and LAN Speed LED	On indicates the corresponding port is in 100Mbps working mode. Off indicates the corresponding port is in 10Mbps working mode

- **WAN:** 2 WAN RJ-45 Ethernet Ports for connecting up to two independent internet feeds
- **LAN:** 3 LAN RJ-45 Ethernet Ports for connecting to the local network.

NOTE: It is recommended that a Luxul switch be used in conjunction with the XBR-2300 to increase number of local ports available.

2.3 Rear Panel



XBR-2300 Rear Panel View

Power Input: Please use the included power cable

3. PREPARING FOR INSTALLATION

3.1 System Requirements

- **Ethernet Cables** to connect the XBR-2300 to Ethernet enabled devices
- **Computer** supporting TCP/IP and equipped with a Web browser. Supported Web browser versions include Microsoft IE 6.0 and up, Safari 1.0 and up or Mozilla Firefox 1.0 and up. The Web browser is used to configure the XBR-2300.

- **Power** must be AC 100-240V~ 0.1A 50/60Hz.

3.2 Before Connecting to the Network

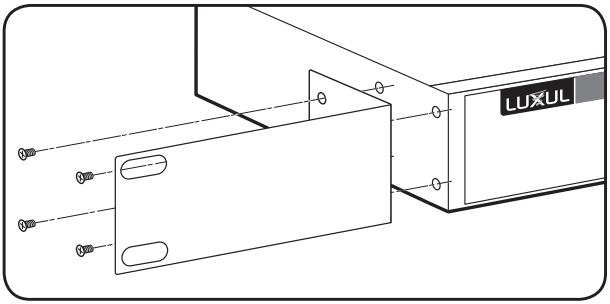
The XBR-2300 can be rack-mounted or used as a desktop switch. Before connecting to the network, please be aware of the following requirements:

- Install the XBR-2300 in a stable/safe place to avoid any possible damage
- Make sure there is adequate space around the XBR-2300 for adequate ventilation and proper heat dissipation. It is recommended to have at least 4-6 inches around all sides.
- Do not place heavy articles on the XBR-2300.
- Power outlets should be within 5 feet of the XBR-2300.
- Verify the ground connection of the outlet is functioning properly.
- Check the power cord to confirm a secure connection.
- Avoid placement in direct sunlight.
- When installing the XBR-2300 on a flat surface, attach the rubber feet to the bottom of the device to avoid scratching the surface.

4: XBR-2300 INSTALLATION

4.1 Installing the XBR-2300 in a Rack

The XBR-2300 can easily be installed in a standard 19" rack. The XBR-2300 includes two mounting ears for installing and stabilizing the switch. For attaching the mounting ears and installing the switch within a rack, please refer to the following illustration:

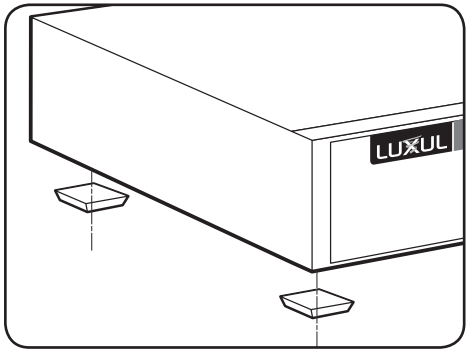


Rack-Mounting the XBR-2300

- Using the included screws, attach the mounting ears to each side of the switch,.
- Mount the switch in the rack with the LEDs facing outwards. Be sure the switch is level and properly secured within the rack.

4.2 Desktop Setup

For use as a desktop device, position and apply the included rubber feet to the bottom of the XBR-2300.



Attaching the Rubber Feet to the XBR-2300

4.3 Connecting Devices

Before installing the XBR-2300, 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. **Establish LAN Connection:** Connect one of the XBR-2300 LAN port to a switch, access point, or computer
2. **Establish WAN Connection:** Connect the Internet cable to one of the XBR-2300 WAN ports
3. **Connect AC Power:** Connect the included AC power cable to the XBR-2300 first and then to the AC outlet.

4.4 Default IP Address

The XBR-2300 default IP address is 192.168.0.1. This address can be changed. However, for hassle free installation of other XenConnect™ plug and play Luxul devices, it is recommended that the default IP value be maintained.

4.5 Connecting a Client Device

Connect the client device to one of the XBR-2300 LAN ports or to a switch that is connected to a XBR-2300 LAN port. The DHCP server on the XBR-2300 is configured by default. If your client device is set to obtain an address automatically, no further configuration is required.

4.6 Verifying Connectivity

After automatic configuration of the TCP/IP parameters, the ping command can be used to check connectivity between the XBR-2300 and the client device.

Windows Devices:

1. Select Start ›› Run input cmd in the Run line then press enter.
2. 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.

5: CONFIGURATION

This section introduces the configuration of the XBR-2300 Enterprise Dual-WAN Router functions via the XenSmart™ Web-based management interface.

5.1 Login

Parameter:	Default Value
Default IP address:	192.168.0.3
Default user name:	admin
Default password:	admin

Login to the router with the following steps:

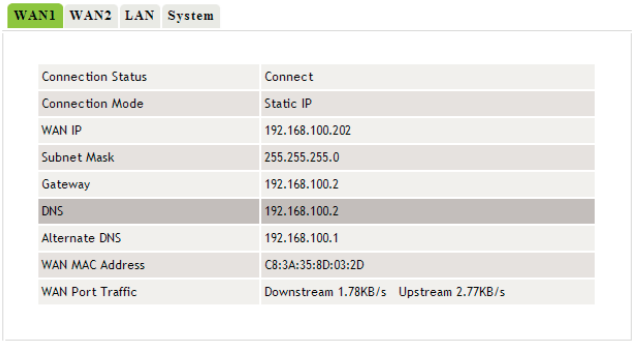
1. Plug an Ethernet cable into any of the three LAN ports of the router
2. Plug the other end into the Ethernet port of your computer
3. Power on the router
4. Check to see that the IP address of the computer is within this network segment: 192.168.0.xxx ("xxx" ranges 100~254). For example, 192.168.0.100.
5. Open the Web browser, and enter 192.168.0.1. The router login window appears, as shown below.

6. Enter the user name and password (default user name and default password are both set as “admin”), and then click “OK” to login to the switch configuration window.

5.2 Status

5.2.1 WAN1

WAN1 displays the current WAN1 Connection Status, Connection Mode, WAN IP, Subnet Mask, Gateway, DNS Server, Alternate DNS Server, WAN MAC Address, and WAN Port Traffic, and Connection Time.

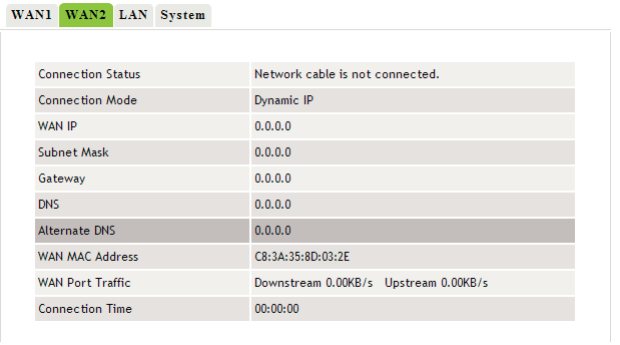


- **Connection Status:** Displays the WAN connection status
  - Disconnected: The WAN port has no connection to the Internet
  - Connecting: The WAN port is obtaining an IP address (Dynamic settings only)
  - Connected: The XBR-2300 is connected to the Internet
  - Network cable is not connected: No Cable Connected
- **Connection Mode:** Displays currently configured access mode
- **WAN IP:** IP address obtained from ISP (Dynamic only) or the Static address assigned by the ISP
- **Subnet Mask:** The subnet mask obtained from ISP (Dynamic only) or the Static Subnet Mask assigned by the ISP
- **Gateway:** The gateway obtained from ISP (Dynamic only) or the Static Gateway assigned by the ISP
- **DNS:** The DNS server obtained from ISP (Dynamic only) or the Static DNS server assigned by the ISP

- **Alternate DNS:** Alternate DNS server obtained from ISP (Dynamic only) or the Static Alternate DNS server assigned by the ISP
- **WAN MAC Address:** Displays the WAN MAC Address
- **WAN Port Traffic:** Indicates the current bandwidth being used (units are KB/s)

5.2.2 WAN2

WAN2 Status displays the current WAN2 Connection Status, Connection Mode, WAN IP, Subnet Mask, Gateway, DNS Server, Alternate DNS Server, WAN MAC Address, WAN Traffic and Connection Time.

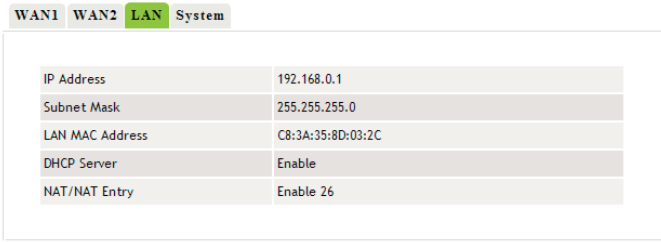


- **Connection Status:** Displays the WAN connection status
  - Disconnected: The WAN port has no connection to the Internet
  - Connecting: The WAN port is obtaining an IP address (Dynamic settings only)
  - Connected: The XBR-2300 is connected to the Internet
  - Network cable is not connected: No Cable Connected
- **Connection Mode:** Displays currently configured access mode
- **WAN IP:** IP address obtained from ISP (Dynamic only) or the Static address assigned by the ISP
- **Subnet Mask:** The subnet mask obtained from ISP (Dynamic only) or the Static Subnet Mask assigned by the ISP
- **Gateway:** The gateway obtained from ISP (Dynamic only) or the Static Gateway assigned by the ISP
- **DNS:** The DNS server obtained from ISP (Dynamic only) or the Static DNS server assigned by the ISP
- **Alternate DNS:** Alternate DNS server obtained from ISP (Dynamic only) or the Static Alternate DNS server assigned by the ISP

- **WAN MAC Address:** Displays the WAN MAC Address
- **WAN Port Traffic:** Indicates the current bandwidth being used (units are KB/s)

5.2.3 LAN

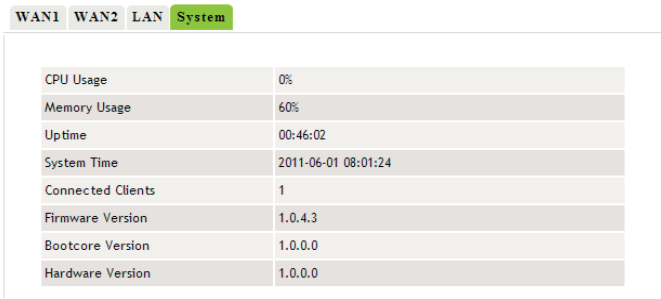
Displays the XBR-2300's IP Address, Subnet Mask, LAN MAC Address, DHCP Server status and NAT/NAT Entries.



- **IP Address:** Displays the IP address assigned to the XBR-2300. This address will be the Gateway of all other devices on the network.
- **Subnet Mask:** Displays the subnet mask assigned to the XBR-2300
- **LAN MAC Address:** Displays the LAN MAC address assigned to the XBR-2300
- **DHCP Server:** Displays the status of the DHCP server (Enabled or Disabled)
- **NAT/NAT Entry:** Displays the status of NAT (Enabled or Disabled) and the current number of NAT entries in use.

5.2.4 System

Displays the status of the XBR-2300s' CPU Usage, Memory Usage, Uptime, System time, number of Connected Clients, Firmware Version, Bootcore Version and Hardware Version.



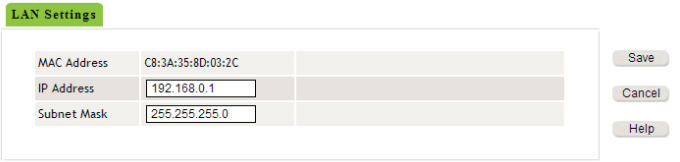
- **CPU Usage:** Displays the percentage of CPU cycles currently occupied
- **Memory Usage:** Displays the current Memory usage
- **Uptime:** Displays the current total up time since last reboot
- **System Time:** Displays the current system time
- **Connected Clients:** Displays the current number of connected devices configured by the DHCP server on the XBR-2300
- **Firmware Version:** Displays the XBR-2300 software version
- **Bootcore Version:** Displays the XBR-2300 bootcore version
- **Hardware Version:** Displays the XBR-2300 hardware version

5.3 Network

- **5.3.1 LAN Settings**
- **5.3.2 WAN Settings**
- **5.3.3 Dual-WAN Policy**
- **5.3.4 DHCP Server**
- **5.3.5 Connected Clients**
- **5.3.6 Static Leases**
- **5.3.7 DMZ**
- **5.3.8 Access Control**
- **5.3.9 Ethernet**
- **5.3.10 MAC Address**

5.3.1 LAN Settings

LAN Settings designate the IP Address and Subnet mask for the internal network.



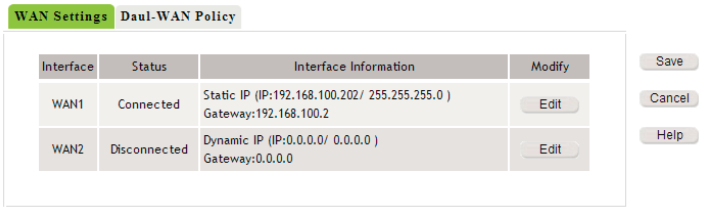
- **MAC Address:** Displays the XBR-2300 LAN MAC address
- **IP Address:** Displays the LAN IP address. The factory default IP address is 192.168.0.1
- **Subnet Mask:** Displays the LAN Subnet Mask

NOTE: 1. If the default IP address has been changed, the new IP address must be entered into the XenSmart management interface. The default gateway value of all devices connected to the LAN must be set to the new IP address in order to have Internet access.

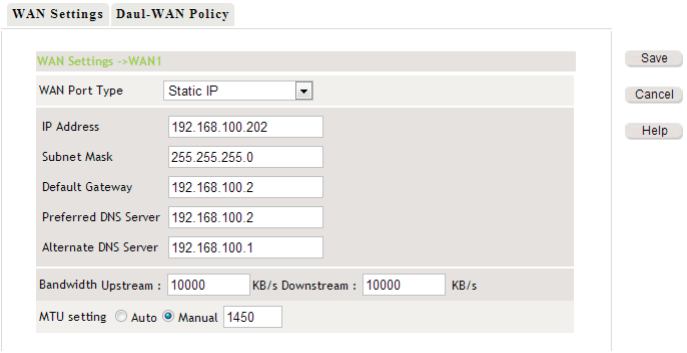
2. If your client device is set to use DHCP, the address must be re-requested. This can be done by simply unplugging and re-plugging the Ethernet cable.

5.3.2 WAN Settings

This interface displays the status of the WAN connections, as well as the port parameters.



To change the WAN interface settings, select "Edit" next to the WAN interface you would like to change. This opens up the interface shown below.



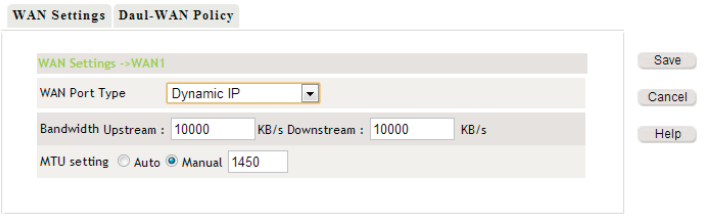
Each WAN interface supports three connection modes: Static IP, Dynamic IP and PPPoE dial-up.

- **Static IP:**
  - IP Address: Enter the Static WAN IP Address. If unknown, contact your ISP.

- Subnet Mask: Enter the Static WAN Subnet Mask. If unknown, contact your ISP.
- Default Gateway: Enter the Static Gateway that corresponds with IP and is provided by your ISP. If unknown, contact your ISP.
- Preferred DNS Server/ Alternate DNS server: Enter the DNS server IP address provided by your ISP. If unknown, contact your ISP.
- Upstream/Downstream Bandwidth (Optional): Enter the static upstream/downstream bandwidth for WAN port1. If unsure of Bandwidths, contact your ISP.
- MTU Setting: MTU (Maximum Transmission Unit) System default is 1450 bytes.

NOTE: Typically there is no need to change this. Improper MTU configuration may lead to poor network performance.

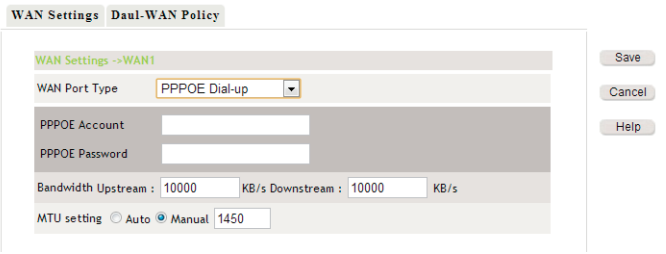
- **Dynamic IP:** If the access mode is Dynamic IP, the XBR-2300 will obtain an IP address automatically from your ISP.



- Upstream/Downstream Bandwidth (Optional): Set the static upstream/downstream bandwidth for WAN port1. If you are not sure of the Bandwidths, contact your local ISP.
- MTU: MTU (Maximum Transmission Unit). System default is 1450 bytes.

NOTE: Typically there is no need to change this. Improper MTU configuration may lead to poor network performance.

- **PPPoE:** If the access mode is PPPoE, the XBR-2300 will obtain an IP address via DSL virtual dial-up.



- PPPoE Account: Enter the PPPoE account name. If not sure of your Account Name, please contact your local ISP.
- PPPOE Password: PPPoE password provided by your ISP. If not sure of your Password, please contact your local ISP.
- Upstream/Downstream Bandwidth (Optional): Enter the PPPoE upstream/downstream bandwidth for WAN1. If not sure of your Bandwidths, please contact your ISP.
- MTU: MTU (Maximum Transmission Unit) System default is 1450 bytes.

NOTE: Typically there is no need to change this. Improper MTU configuration may lead to poor network performance.

- **PPTP:** If the connection is PPTP, your ISP should provide information to set the following parameters. PPTP can be Dynamic or Static:
  - PPTP Server IP Address: IP Address of the ISPs PPTP server. If you are not sure of the PPTP Server IP, contact your ISP.
  - User Name: Enter your PPTP user name. If not sure of your User Name, contact your ISP.
  - PPTP Password: PPTP Password provided by your ISP. If not sure of your Password, contact your ISP.
  - Address Mode: There are two modes available:
    - Dynamic IP: With Dynamic, the IP Address, Subnet Mask and Default Gateway will be automatically configured for you.
    - Static IP: With Static IP, your ISP will need to provide you with your IP Address, Subnet Mask and Default Gateway. If not sure of your IP Address, Subnet Mask and Default Gateway, contact your ISP.

NOTE: When the IP Mode is set to Dynamic, no configuration is needed for the next three settings, IP Address, Subnet Mask and Default Gateway.

  - IP Address: The IP Address assigned by your ISP.
  - Subnet Mask: The Subnet Mask assigned by your ISP.
  - Default Gateway: The Default Gateway assigned by your ISP.
  - Upstream/Downstream Bandwidth: The PPTP upstream/downstream bandwidth for WAN1. If not sure of your Bandwidths, contact your ISP.
  - MTU: MTU (Maximum Transmission Unit). System default is 1450 bytes.

NOTE: Typically there is no need to change this. Improper MTU configuration may lead to poor network performance.

- MPPE: Enables support for Microsoft's MPPE stateful encryption.

NOTE: If you experience moderate to high packet loss, do not enable this function.

- **L2TP:** If the ISP connection is L2TP, you will need to input the following parameters provided by your ISP. L2TP can be Dynamic or Static:
  - L2TP Server IP Address: IP Address of your ISPs L2TP server. If not sure of your PPTP Server IP, contact your ISP.
  - User Name: Enter your L2TP User Name. If not sure of your User Name, contact your ISP.
  - L2TP Password: L2TP password provided by your ISP. If not sure of your Password, contact your ISP.
  - Address Mode: There are two modes available:
    - Dynamic IP: With Dynamic, the IP Address, Subnet Mask and Default Gateway will be automatically configured for you.
    - Static IP: With Static IP, your ISP will need to provide you with your IP Address, Subnet Mask and Default Gateway. If not sure of your IP Address, Subnet Mask and Default Gateway, contact your ISP.

NOTE: When the IP Mode is set to Dynamic, no configuration is needed for the next three settings, IP Address, Subnet Mask and Default Gateway.

  - IP Address: The IP Address assigned by your ISP.
  - Subnet Mask: The Subnet Mask assigned by your ISP.
  - Default Gateway: The Default Gateway assigned by your ISP.
  - Upstream/Downstream Bandwidth: The PPTP upstream/downstream bandwidth for WAN1. If not sure of your Bandwidths, contact your ISP.
  - MTU: MTU (Maximum Transmission Unit). System default is 1450 bytes.

NOTE: Typically there is no need to change this. Improper MTU configuration may lead to poor network performance.

NOTE: The configuration methods for the WAN2 interface are the same as for WAN1.

5.3.3 Dual-WAN Policy

This function allows you to choose the Dual-WAN Policy that best meets your needs. Your XBR-2300 has three Active Policies: Automatic Load Balancing, for

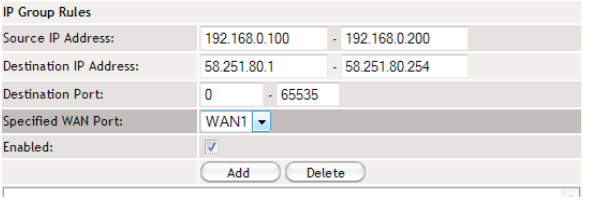
allowing each client access to the maximum available data rate; Automatic Failover, for redundant links; and IP Groups, for controlling how much bandwidth is given to each client.

- **Automatic Load Balancing:** The system searches for the WAN port with the lowest usage and automatically distributes load accordingly. This load balancing mode automatically manages flow distribution and bandwidth overlap.

NOTE: The system default mode is Automatic Load Balancing.

- **Automatic Failover:** Users can choose a WAN port (WAN1 or WAN2), as the primary connection, while making the other port a backup connection. The XBR-2300 will automatically switch to the backup connection when the primary connection has an interruption in service. This change over is subject to a short delay of approximately 40 seconds on primary connection failure.
- **IP Group:** This mode allows for the control of bandwidth provided to groups of client devices. When using this mode, specific IP address ranges are placed in groups and assigned to a particular port (WAN1 or WAN2). The source address, destination address, and destination port are all specified. All data packets included in the defined range are then processed by the selected WAN interface. All data packets that are not included in the defined range are forwarded to the other WAN interface.

Example: To designate that LAN Source IP addresses with a range of 192.168.0.100 to 192.168.0.200 pass through WAN2 and with a Destination IP Address range of 58.251.80.1 to 58.251.80.254, via ports: 0-65535, you need to fill in the corresponding source IP Addresses, Destination IP Addresses, Destination Ports, and Designate a WAN port. To activate this setting, check "Enabled" and click "Add to the corresponding list." See below for details:



NOTE: 1. All packets which not included in the configured range will be handled by WAN2.

2. If rules are configured more than once or have overlapping parameters, only the most recently configured rules will be valid.

5.3.4 DHCP Server

Settings include IP Address, Subnet Mask, Gateway and DNS Server. With DHCP Server, IP addresses are assigned automatically by the XBR-2300. Simply enable the DHCP Server to automatically configure the IP Address of all new devices on the LAN.

DHCP Server: Select this option if you want DHCP to automatically assign and configure device IP Addresses.

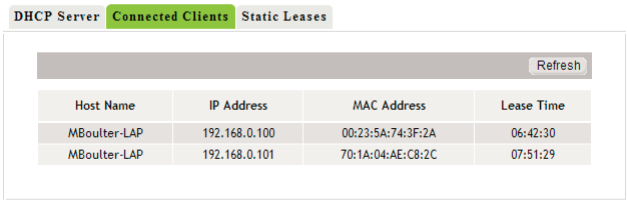
- **Starting IP Address:** The first IP Address allowed to be assigned by the DHCP Server.
- **Ending IP Address:** The last IP Address allowed to be assigned by the DHCP Server.
- **Lease Time:** The amount of time the device is guaranteed its current address. Set to 8 hours (480 minutes) by default.
- **Primary DNS Server:** First DNS Server distributed to client device during the DHCP operation.
- **Secondary DNS Server:** Second DNS Server distributed to client device during the DHCP operation.

NOTE: The only addresses available for DHCP are the addresses between the Starting and Ending IP Pool (192.168.0.100-200 by default). If you need to have more addresses available on the network, please add to the pool (192.168.0.20-254 are available in all Luxul networks).

NOTE: In order to properly utilize the DHCP Server option, the TCP/IP network connection of the device must be set to "Obtain an IP address automatically".

5.3.5 Connected Clients

The DHCP client list displays the Host Device Name, IP Address, MAC Address and Lease Time.

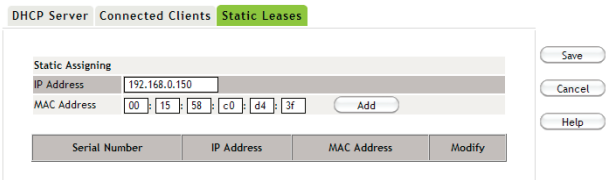


- **Host Name:** The name of the device
- **IP Address:** The IP address assigned to the device
- **MAC Address:** The MAC address of the device
- **Lease Time:** The amount of time remaining in the DHCP Lease

5.3.6 Static Leases

The DHCP Server function of the XBR-2300 supports static IP address assignment. This would be used when you need a device on the network to receive the same DHCP IP address each time it comes online.

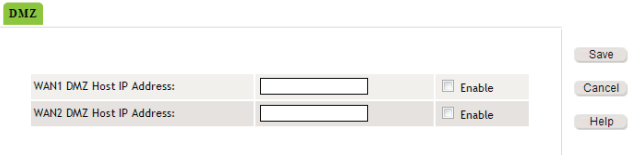
Example: The MAC address of a computer hosting your movie collection is 00:15:58:c0:d4:3f. If you want that computer to receive the IP Address 192.168.0.150 every time it comes online, you would assign this Static DHCP IP Address to that device. To do so, first enter the desired IP Address and MAC Address of the device. Then, click "Add" and "Save." The finished configuration should appear as shown in the image below.



- **IP Address:** Reserved DHCP IP Address (Static address)
- **MAC Address:** The MAC address of the device to receive the Static address
- **Add:** Adds the configured options to the Static Leases List
- **Edit:** Modifies the current configuration
- **Delete:** Deletes the current configuration

5.3.7 DMZ

In some special cases, a device on the network is required to be fully exposed to the Internet. In such cases, the device needs to be configured as a DMZ host.



WAN1 DMZ Host IP Address: Enter the IP address of the device you want to be the DMZ host mapped to WAN1

WAN2 DMZ Host IP Address: Enter the IP address of the device you wish to be the DMZ host mapped to WAN2

Save: Saves the current configuration

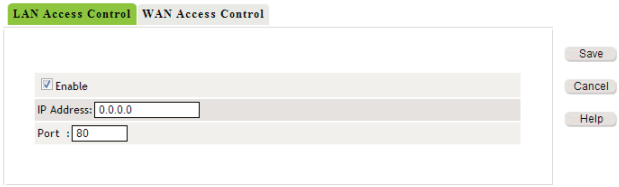
NOTE: Must "Save" each time a change is made

CAUTION: Firewall settings for all devices set as a DMZ Host will be disabled!!!

5.3.8 Access Control

Access Control determines which devices on your WAN and LAN will be allowed to open the XenSmart Web based management portal for the XBR-2300.

5.3.8.1 LAN Access Control

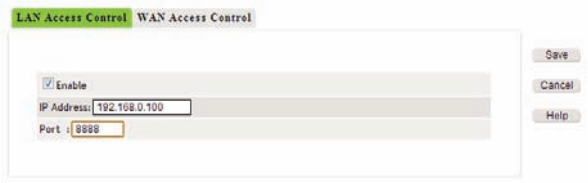


- **Enable:** Enables access to the XenSmart Web Interface
- **IP Address:** Enter the IP address of the device allowed to access the XenSmart Web interface.

NOTE: If you use the default of 0.0.0.0 all devices can connect.

- **Port:** The TCP port number to access the Web interface. The default port number for LAN traffic is 80 (http)

NOTE: When an IP address is set, no other device can log on to the XenSmart Web Interface. Example:: when the XBR-2300 default IP address is 192.168.0.1, if you only permit a client computer with the IP address of 192.168.0.100 to access the Web portal via port 8888, only that device will be allowed to connect. To access the XenSmart Web Interface, use the following address format http://192.168.0.1:8888.



5.3.8.2 WAN Access Control

By default, only LAN users can access the XenSmart Web Interface portal. This function will enable remote access and control of the XBR-2300.

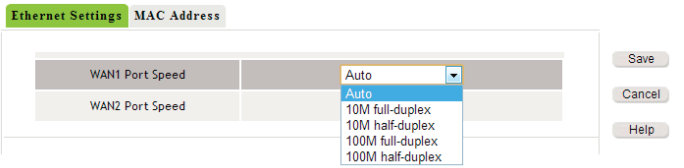
- **Enable:** Allows access to the XenSmart Web Interface via a WAN port
- **IP Address:** Enter the IP address of the remote device allowed to access the XenSmart Web interface.

NOTE: If you use the default of 0.0.0.0 all devices can connect.

- **Port:** This setting will configure a port number to provide more security. The default port is 8080.

NOTE: WAN-based Access Control to the XBR-2300 can be modified according to your needs. All WAN devices can access the XBR-2300 at the default Access Control IP Address: 0.0.0.0. If the default Access Control IP Address is changed (for example; 58.60.111.221), then only the specified client device (say 58.60.111.221) will be allowed access to the XenSmart management portal. So, if the WAN1 IP address is 58.251.88.90, to access the Web portal, the following address format would be used: http://58.251.88.90:8080 and would only function if connecting from the client device with the IP number of 58.60.111.221.

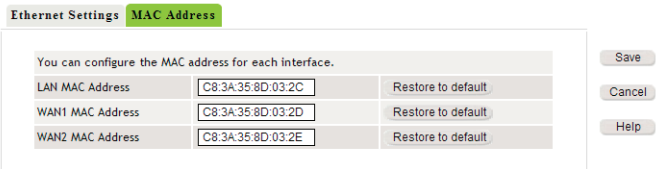
5.3.9 Ethernet Settings



Ethernet Settings: Here you can set the speed and duplex of the WAN interfaces (WAN1 and WAN2). The available options are: Auto, 10Mbps half duplex, 10Mbps full duplex, 100Mbps half duplex and 100Mbps full duplex. 100Mbps full duplex is the most common for newer devices.

5.3.10 MAC Address

MAC Address: Allows you to manually specify a MAC address for WAN1, WAN2 and/or LAN.



- **LAN MAC Address:** Use this if the specified MAC Address is to be used by the XBR-2300 in the internal network
- **WAN1 MAC Address:** Use this if the specified MAC Address is to be used by the XBR-2300 for all Internet traffic across WAN interface 1
- **WAN2 MAC Address:** Use this if the specified MAC Address to be used by the XBR-2300 for all Internet traffic across WAN interface 2
- **Restore to Default:** Resets the MAC Addresses to factory default settings

NOTE:

1. Some ISPs bind the connection to the user's computer MAC Address. In this scenario, copy the computer's MAC Address to the corresponding WAN interface MAC address field.
2. MAC Address modifications only take effect when router is rebooted.
3. Unless required by the ISP setup or other non-standard scenario, it is suggested that this function not be used.

5.4 Internet Access

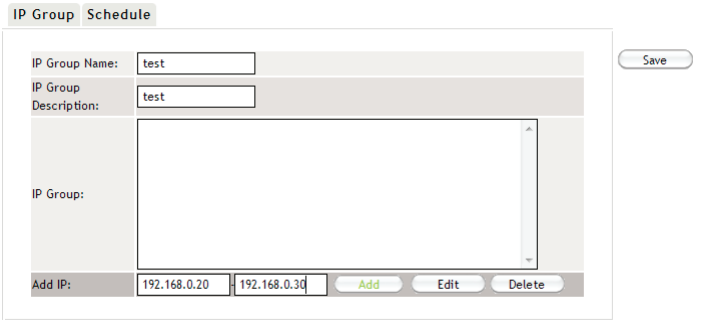
There are five submenus In the Internet Access section:

- **5.4.1 IP Groups**
- **5.4.2 Schedule**
- **5.4.3 Client Filter**
- **5.4.4 URL Filter**
- **5.4.5 Bandwidth/NAT**

5.4.1 IP Groups

Use this feature by adding an IP Group Name, a Group Description, and suitable IP Address Range. The IP Group you create can then be used to manage Internet Access of the devices using those IP addresses.

Example: Let's assume that a specific group of devices has an IP address range of 192.168.0.20 to 192.168.0.30. Click "Add IP Group" and enter the Group Name, Group Description, the IP address range and then click "Add." This will create your group. To finish configuration and save the settings, click on "Save."

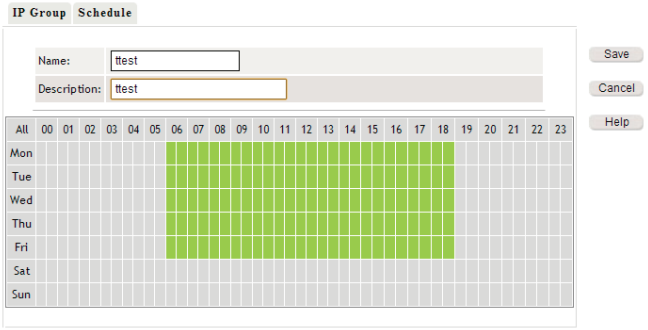


- **IP Group Name:** Unique name to identify the IP address Group
- **IP Group Description:** Description of the IP address Group
- **Add IP:** Enter the beginning and ending IP addresses of the Group
- **Add:** Creates the defined Group
- **Save**: Saves the settings

5.4.2 Schedule

This feature allows you to set Group Internet access Schedules. To use this feature, select "Add" and then select the group for which you would like to make a schedule.

Example: to enable Internet Access only during normal office hours, you might select 06:00-19:00 on the work days from Monday to Friday as a schedule. To do this, simply click "Add" and the following will appear.

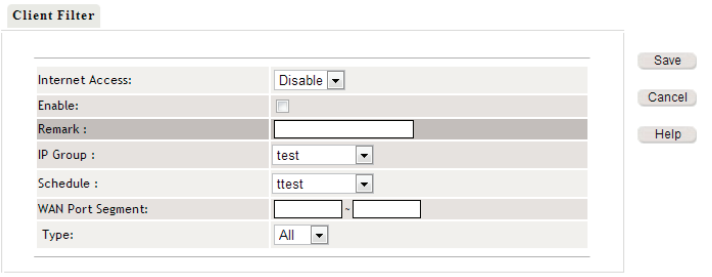


- **Name:** Name of the Schedule
- **Description:** Description of the Schedule
- **Time Range:** Simply choose the desired Time or Time Range (see image above)

- **Edit: Allows** changes to the configured Schedule
- **Delete:** Removes the configured Schedule

5.4.3 Client Filter

For control of client device behavior we can create a Client Filter that will either allow or block Internet access to an IP Group during a specified Schedule.



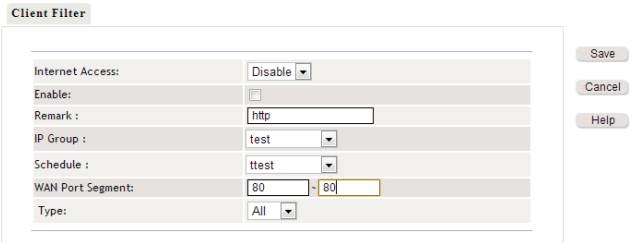
- **Internet Access:** Choose either Disable (blocks access) or Enable (allows access)
  - Disable: Blocks the traffic that meets the specified IP Group and Schedule criteria. ALL other unrestricted traffic is allowed to pass
  - Enable: Allows the traffic that meets the IP Group and Schedule criteria entered
- **Enable:** Enables or Disables the filter
- **Remark:** Description of the Rule being created
- **IP Group:** The name of the desired IP Group
- **Schedule:** The name of the desired Schedule
- **WAN Port Segment:** Enter the desired TCP/UDP port or port range (1-65535)

NOTE: Some ports are linked to a Protocol (i.e. HTTP, FTP, SMTP, etc) For a list of Ports and corresponding Protocols see http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

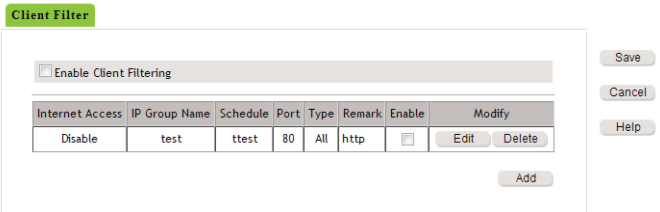
Type: Select TCP, UDP or All to block the corresponding traffic

NOTE: The configured Client Filter will only affect the devices in the range of the specified IP Group during the schedule you have selected. All other traffic will be allowed to pass.

Example: If you do not want the computers with IP addresses of 192.168.0.20 to 192.168.0.30 (IP Group=test) to visit HTTP websites from 06:00-19:00 (Schedule=ttest) Monday through Friday, you would set the Client Filter rule as follows:

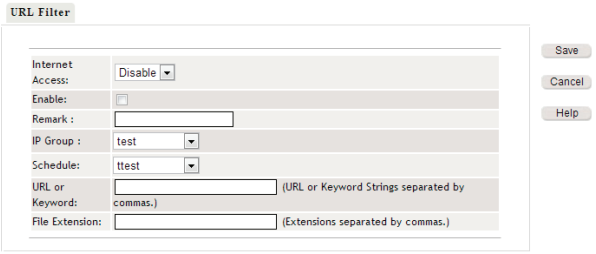


This is what the created Rule will look like after clicking on "Save"



5.3.4 URL Filter

To control visits to websites with a particular phrase or name in the URL, a URL Filter Rule can be created.

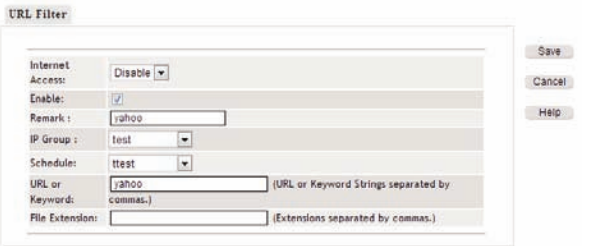


- **Internet Access:** Choose either Disable (blocks access) or Enable (allows access)
  - Disable: Blocks the traffic that meets the specified IP Group and Schedule criteria. ALL other unrestricted traffic is allowed to pass
  - Enable: Allows the traffic that meets the IP Group and Schedule criteria entered
- **Enable:** Enables or Disables the Filter
- **Remark:** Description of the Rule being created
- **IP Group:** The name of the desired IP Group

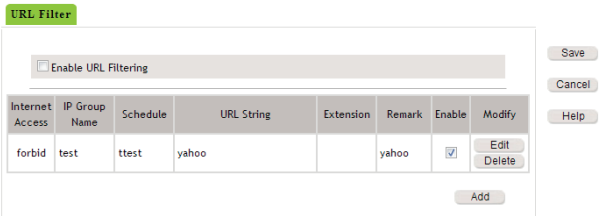
- **Schedule:** The name of the desired Schedule
- **URL String:** The String you would like to filter (i.e. test, yahoo, facebook, etc)
- **Extension:** Domains or extension suffix (i.e. .com, .biz, .org, .exe, .rar, etc.)

NOTE: The configured Client Filter will only affect the devices in the range of the specified IP Group during the schedule you have selected. All other traffic will be allowed to pass.

Example: If you do not want the computers with IP addresses of 192.168.0.20 to 192.168.0.30 (IP Group=Test) to visit HTTP websites associated with "Yahoo" from 06:00-19:00 (Schedule=work days) Monday through Friday, you would set the Client Filter rule as follows:



This is what the created Rule will look like after clicking on "Save"

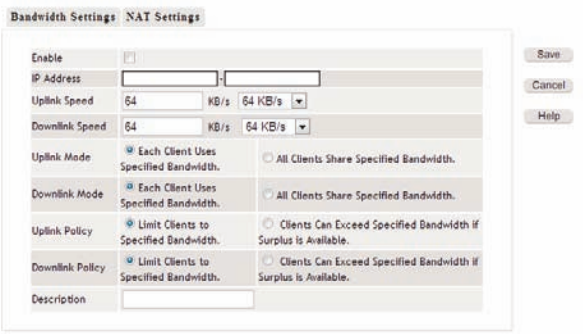


5.4.5 Bandwidth/NAT

The Bandwidth/NAT section has two submenus: Bandwidth Settings and NAT Settings. These settings allow for the control of how much Bandwidth is available to client devices, as well as which WAN IP Address is used for NAT on a specific range of devices.

5.4.5.1 Bandwidth Settings

Bandwidth Settings allows the control of bandwidth allocated to each device on the network. The XBR-2300 can control the bandwidth for up to 256 individual client devices. IP address ranges are also supported.



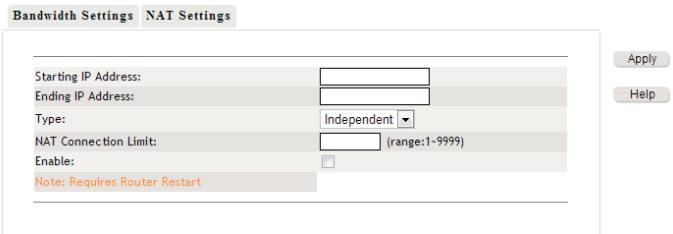
- **Enable:** Enables or Disables Bandwidth control for the specified device(s)
- **IP Address:** Sets the IP Address(es) for bandwidth controlled devices
- **Uplink Range:** Maximum upload data rate per device
- **Downlink Range:** Maximum download data rate per device
- **Uplink /Downlink Mode:** Selects whether the specified limits are to be shared by devices in the range or if each individual device is allocated this limit
- **Uplink/Downlink Policy:** Selects whether or not surplus bandwidth can be used

NOTE: if you choose "when the bandwidth has a surplus, you can use more bandwidth", the XBR-2300 will automatically manage the upload and download flow.

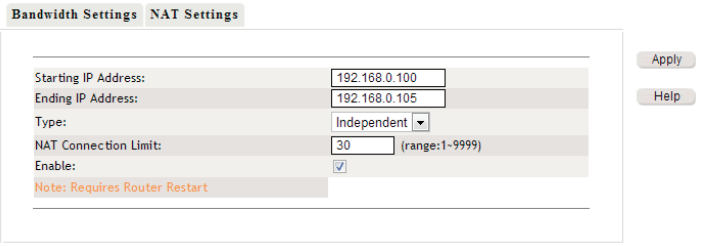
- **Description:** Name of Bandwidth Control Rule

5.4.5.2 NAT Settings

NAT Settings allow for the specification of the maximum number of NAT Table entries created by a device or group of devices on the network. This basically limits the number of websites a device can visit at any given time.



- **Starting IP Address/Ending IP Address:** Enter the IP address range you would like to control
- **Type:** Select the NAT Setting control type (Independent or Shared)
  - Independent: Takes effect on each IP address and controls the maximum NAT entries of each device
  - Shared: Takes effect on the whole IP group and controls the total entries of the devices within the IP group
- **NAT Connection Limit:** Indicates the maximum NAT entries allowed. This can be a range from 1 to 9999
- **Enable:** Enables the NAT Connection Limit function



NOTE: In order for the new NAT Settings to take effect, the XBR-2300 must be rebooted .

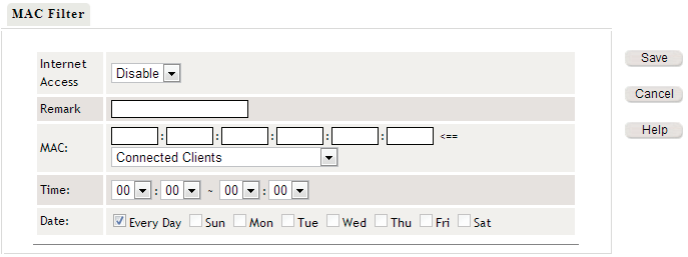
5.5 Security

The Security section consists of the following submenus:

- **5.5.1 MAC Filter**
- **5.5.2 ARP Defense**
- **5.5.3 WAN Attack Defense**
- **5.5.4 LAN Attack Defense**
- **5.5.5 IP-MAC Binding**
- **5.5.6 Attack List**

5.5.1 MAC Filter

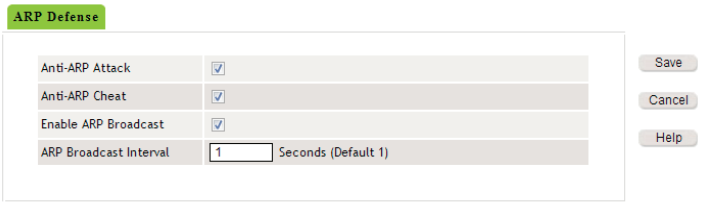
The XBR-2300 has the ability to limit Internet access by MAC Address. This function can be used to block unknown devices from accessing the Internet.



- **Internet Access:** Enable or Disable the Internet Access of a specified device
  - Disable: Blocks the MAC Address listed from connecting to the Internet
  - Enable: Allows the MAC Address listed access to the Internet
- **Remark:** Name of the MAC Address filter (user defined)
- **MAC:** The MAC Address of the device to be filtered
- **Time:** The Start and End time of the rule. The default value is 000-2400 hours
- **Day:** Selects the days of the week the filter should be in effect

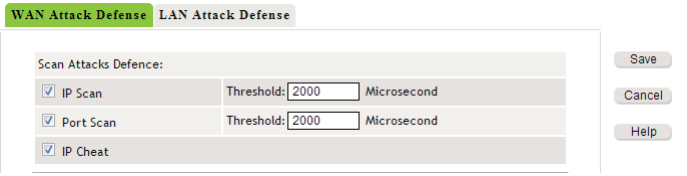
5.5.2 ARP Defense

This function helps prevent ARP attacks and cheats. To protect the network, the ARP defense is enabled by default within the XBR-2300. The default ARP broadcast interval is one second and can be set from 1-60 seconds.



5.5.3 WAN Attack Defense

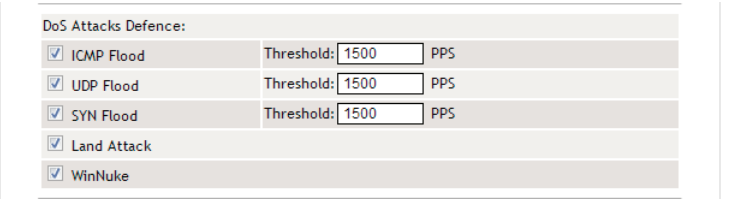
The XBR-2300 can block the following primary types of attacks: Scan Attacks, DoS Attacks, Suspicious Packets, Packets Containing IP Options and Other Attacks (i.e. Shockwave, Sasser, and other Viruses).



Scan Attacks Defense

- **IP Scan:** A source IP sends ICMP request packets to 10 different destination IP addresses within the defined time limit. The XBR-2300 drops all ICMP requests once the limit is reached
- **Port Scan:** A source IP sends TCP SYN request packets to 10 different ports of one destination address within the defined time limit. The XBR-2300 drops all request packets once the limit is reached
- **IP Cheat:** Attempts to block LAN devices using an Internet Proxy to bypass access restrictions.

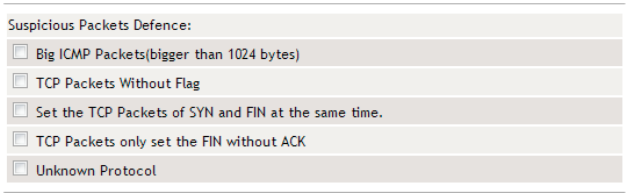
NOTE: This function takes effect on LAN ports



Denial of Service (DoS) Attacks Defense

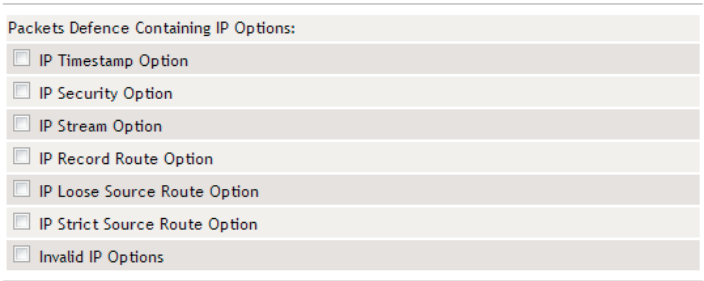
- **ICMP Flood:** If ICMP request packets exceed the specified limit, all ICMP traffic will be blocked
- **UDP Flood:** If UDP packets exceed the specified limit, all UDP traffic will be blocked
- **SYN Flood:** If TCP SYN packets targeted to a specific IP Address exceed the specified limit, all TCP SYN requests will be blocked
- **LAND Attack:** When enabled, the XBR-2300 will attempt to drop all traffic that matches the following definition: SYN packets that include the device's IP address as both the source and destination IP address

- **WinNuke:** When enabled, the XBR-2300 will attempt to drop all traffic that matches the following definition: TCP fragments (usually configured as URG NetBIOS port 139) are sent to connected devices, causing fragment overlapping



Suspicious Packets Defense

- **Big ICMP Packets:** ICMP packets should be 1024 Bytes or less. This filter drops all ICMP packets that exceed 1024 Bytes
- **TCP Packets without Flag:** All normal TCP packet have at least one configured symbol (Flag). This filter drops all TCP packets that do not have a set Flag
- **Set the TCP Packets of SYN and FIN at the Same Time:** TCP packets that have set both the SYN and FIN Flags are abnormal and considered suspicious. This filter drops all TCP packets that have set both the SYN and FIN Flags.
- **TCP Packets only Set FIN without ACK:** TCP packets that have the FIN Flag but no ACK Flag set are considered abnormal. This filter drops all TCP packets that have set the FIN Flag but are missing the ACK Flag
- **Unknown Protocol:** If the character value in protocol type of an IP packet is 135 bytes or larger, it is impossible to determine in advance whether this unknown protocol is well-intentioned or malicious (all well known protocols and most unknown protocols have character values less than 135 bytes). This filter drops all packets with 135 bytes or more in the protocol type.



Packets Containing IP Options Defense

- **IP Timestamp Option:** Checks an IP packet to see if it contains an Internet Timestamp. If enabled, all packets without an Internet Timestamp will be dropped.
- **IP Security Option:** Checks an IP packet to see if it contains a Security marker. If enabled, all packets without a Security marker will be dropped.
- **IP Stream Option:** Check an IP packet to see if it contains a Stream ID. If enabled, any packet stream without a Stream ID will be dropped.
- **IP Record Route Option:** Checks an IP packet to see if it contains a Record Route. If enabled, any packets without a Record Route will be dropped.
- **IP Loose Source Route Option:** Checks an IP packet to see if it contains a Loose Source Route. If enabled, any packets without a Loose Source Route will be dropped.
- **IP Strict Source Route Option:** Checks an IP packet to see if it contains a Strict Source Route. If enabled, any packets without a Strict Source Route will be dropped.
- **Invalid IP Options:** Checks an IP packet to see if it contains any integrity errors. If enabled, any packets containing Invalid IP Options will be dropped.

Other Attacks

- **Filter Ping from WAN Port:** If enabled, XBR-2300 will drop all ICMP packets
- **DDoS Attack Defense:** If enabled, the XBR-2300 will attempt to drop all DDoS packets (i.e. ICMP, ARP, etc)
- **Shock Waves, Sasser and Other Viruses Defense:** The XBR-2300 will block all well known virus attacks.

NOTE: This requires updating the firmware as new updates are released

5.5.4 LAN Attack Defense

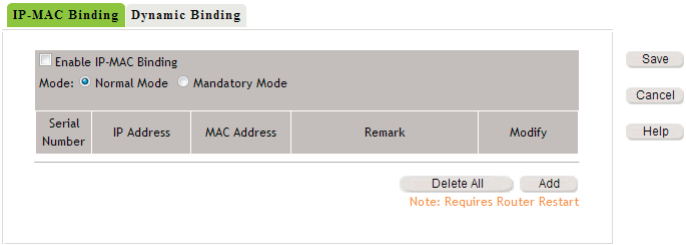
The settings options for this section are identical to WAN Attack Defense simply applied to the LAN ports of the XBR-2300. Please refer to section 3.4.3 WAN Attack Defense.

5.5.5 IP-MAC Binding

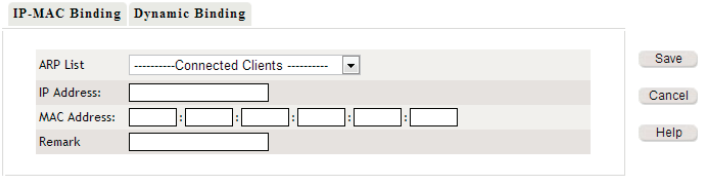
In the IP-MAC Binding section there are two submenus: IP-MAC Binding and Dynamic Binding.

5.5.5.1 IP-MAC Binding

This function Binds a specified MAC address to a specified IP Address. This is useful in networks where a device IP and the MAC address must remain linked (i.e. VoIP Phones, Servers, Secondary Routers, etc.)



- **Enable IP-MAC Binding:** Enables IP-MAC Binding function
- **Mode:** There are two optional modes: Normal Mode or Mandatory Mode
  - Normal Mode: Blocks any IP Address that does not match the bound MAC Address. IP Addresses not included in the binding list will communicate normally
  - Mandatory Mode: Only IP Addresses matching the MAC addresses on the Binding List are allowed to access the Internet. All addresses not included in the list are blocked.



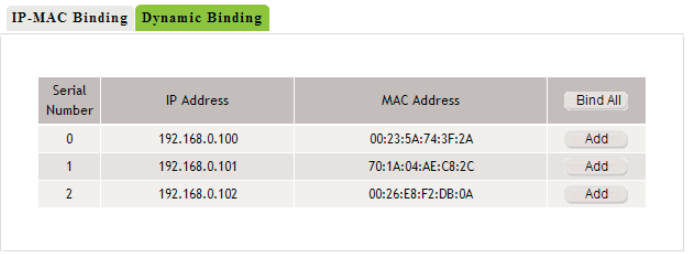
- **ARP List:** Displays the corresponding IP and MAC addresses in the ARP Table. Select Connected Clients in ARP List to manually add IP and MAC addresses.
- **IP Address:** Specifies the IP address to be Bound.
- **MAC Address:** MAC addresses to be Bound

NOTE: Once Binding is enabled, the device can only access the internet when the IP and MAC addresses on the binding list match

Remark: Name of Binding rule

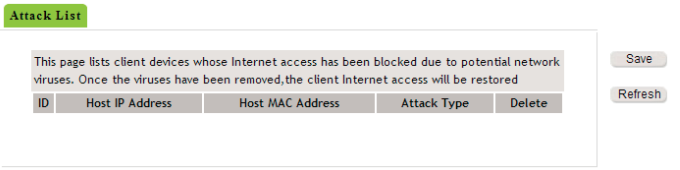
5.5.5.2 Dynamic Binding

Displays the current IP Address to MAC Address relationship for all devices using DHCP on the network. By simply clicking the "Binding" or "All Binding" buttons, you can automatically configure Binding rules for each device on the network.



5.5.6 Attack List

This page displays the devices on the network that have been detected by any LAN Attack Defense settings. The device will be denied Internet access until it is removed from the list. It is recommended that any devices appearing on this list are checked and thoroughly cleaned of any viruses before allowing them to access the Internet.



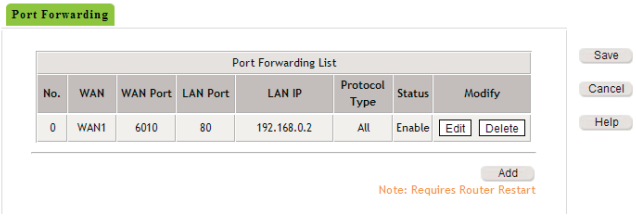
5.6 Advanced Settings

The Advanced Settings section includes:

- **5.6.1 Port Forwarding**
- **5.6.2 UPnP**
- **5.6.3 One -to -One NAT**
- **5.6.4 Dynamic DNS**
- **5.6.5 Router Table**
- **5.6.5 Static Routes**

5.6.1 Port Forwarding

Port Forwarding allows traffic that reaches the WAN port to be redirected to a LAN device. Port Forwarding allows you to setup public Web, FTP, and Email servers that physically reside on the internal LAN network.

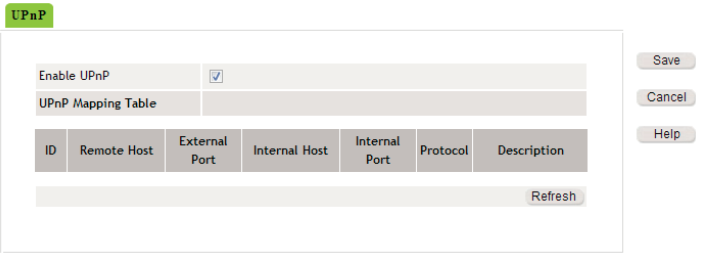


- **WAN:** Selects a WAN interface for mapping (either WAN1 or WAN2)
- **WAN Port:** Selects a TCP/UDP port to be mapped
- **Well-known Ports:** In the Well-known Ports dropdown, there are some commonly used protocol ports such as: DNS (53), FTP (21), GOPHER (70), HTTP (80), NNTP (1190), POP3 (110), PPTP (1723), SMTP (25), SOCK (1080) and TELNET (23). Any ports that are not included in the dropdown can be manually added.
- **LAN Port:** Selects the destination port on the Internal Server
- **LAN IP:** Sets the IP Address of the Internal Server to be accessed
- **Protocol:** Sets which type of traffic is forwarded: TCP, UDP or All
- **Enable:** Enables the port forwarding rule
- **Modify:** Updates the port forwarding rule

NOTE: If you set up Port Forwarding with a service port of 80, remote access to the XenSmart Web Management interface will need to be through another port such as 8080 to avoid potential conflicts.

5.6.2 UPnP

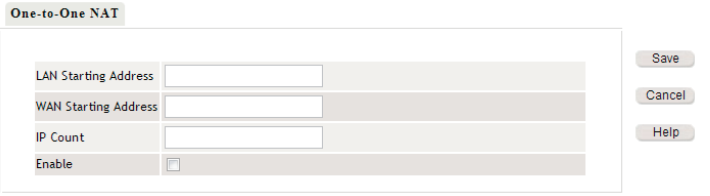
The latest Universal Plug and Play network protocol is supported by Windows XP or higher (the operating system needs to be integrated with or have Directx9.0 or higher). If UPnP is enabled, port forwarding information is automatically supplied at the request of any compatible application.



- **ID:** Displays the device UPnP ID (usually the ID of the network card)
- **Remote Host:** Description of the remote device that receives or sends data
- **External Port:** The external port number used for forwarding UPnP traffic
- **Internal Host:** Description of the internal device receiving or sending data
- **Internal Port:** The internal port number used for forwarding UPnP traffic
- **Protocol:** Displays the protocol TCP/UDP of the UPnP traffic
- **Description:** Displays the configured message of the UPnP device serving traffic

5.6.3 One-to-One NAT

Requires the IP Address of a local device to NAT behind the specified public WAN IP Address.

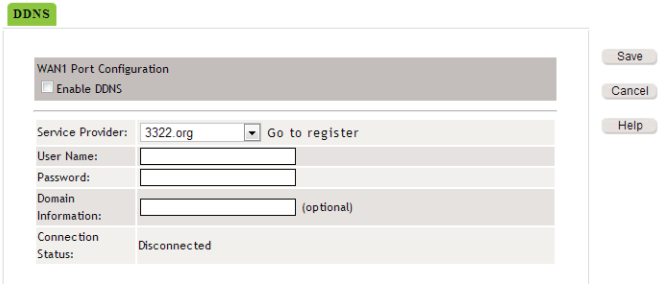


- **LAN Starting Address:** Enter the desired LAN IP Address
- **WAN Starting Address:** Enter the WAN IP Address you wish to NAT behind
- **IP Count:** Enter the number of IP Addresses immediately after the LAN Starting Address you wish to perform a One-to-One NAT
- **Enable:** Enables the configured One-to-One NAT rule

Example: If you enter 192.168.0.10 in the LAN starting IP address, 172.138.112.111 in the WAN starting IP address and 5 in the IP Count field, this means that that devices with LAN IPs 192.168.0.10—192.168.0.14 and WAN IPs: 172.138.112.111—172.138.112.115 are to use a One-to-One NAT relationship.

5.6.4 DDNS

This page allows for the setup of Dynamic DNS parameters when a connection is successfully established. Other hosts can access the XBR-2300 or a virtual server via the Domain Name configured in the DDNS account.

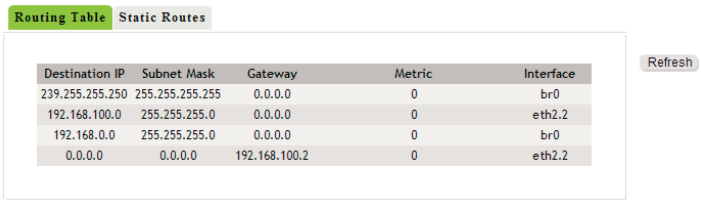


- **Enable DDNS:** Enables Dynamic DNS support
- **Service Provider:** Specifies the site providing your DDNS services (i.e. DynDNS.org)
- **User Name:** DDNS service account user name
- **Password:** DDNS service account password
- Domain Information: The Domain Name given by the DDNS service to your domain
- Connection Status: The current connection status to the DDNS server

NOTE: The configuration is identical for WAN Interfaces 1 and 2. However, each port can have a different DDNS service provider and serve a different Domain Name.

5.6.5 Routing Table

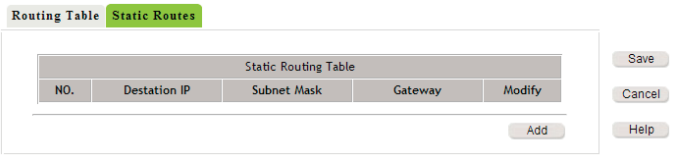
This page displays the Routing Table contents.



Destination IP	Subnet Mask	Gateway	Metric	Interface
239.255.255.250	255.255.255.255	0.0.0.0	0	br0
192.168.100.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	192.168.100.2	0	eth2.2

5.6.6 Static Routes

Static Routes can be configured on this page.



- **Destination IP:** Designated the IP Address of a destination device or destination Network.

> **NOTE:** The IP address for a device would be similar to 192.96.82.123, whereas a network would be represented by 192.96.82.0.

  - **Subnet Mask:** The subnet mask of the destination IP Address or Network
  - **Gateway:** The IP address of the XBR-2300's entry for next hop. If the traffic should be routed to the Internet, this would be the WAN Interface address. If the traffic should be routed to the internal network, this would be the LAN IP Address.

5.7 VPN

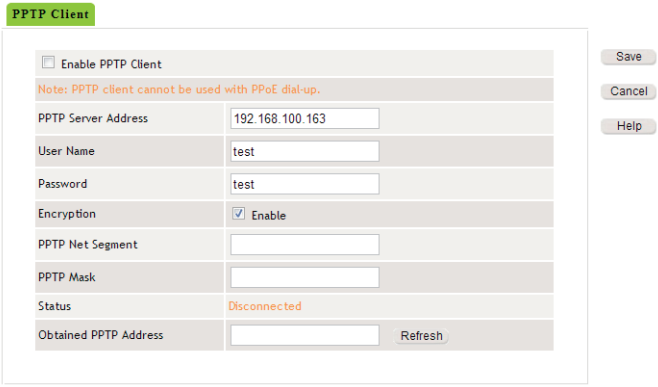
There are two submenus in the VPN section:

- **5.7.1 PPTP Client**
- **5.7.2 PPTP Server**

5.7.1 PPTP Client

PPTP Client supports the configuration of a connection between the XBR-2300 and another Router offering a VPN Server connection.

Example: A home office requires secure access to the head office. Two Routers can be configured to provide a secure link.



- **Enable PPTP Client:** Enables the VPN Client
- **PPTP Server Address:** Address of the remote device providing PPTP VPN service
- **User Name:** PPTP user name
- **Password:** PPTP password
- **Encryption:** Enables or Disables Encryption between the Client and VPN Server when authenticating.

NOTE: The configuration on the Client and Server must match to make a secure connection. If authentication errors occur, test with this setting disabled. However, it is not recommended to run the connection continuously with encryption disabled as the traffic will not be secure.

- **PPTP Net Segment:** The Network to be accessed after completing the PPTP tunnel
- **PPTP Mask:** The Network subnet mask
- **Status:** Displays the current PPTP connection status
- **Obtained PPTP Address:** Displays the IP Address of the PPTP tunnel connection

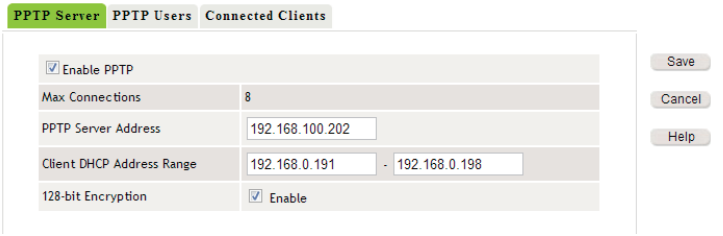
5.6.2 PPTP Server

There are three sections in the PPTP Server submenu: PPTP Server, Client Setting and Dial-in List.

5.6.2.1 PPTP Server

The PPTP server supports the connection between the PPTP Client and the VPN Router.

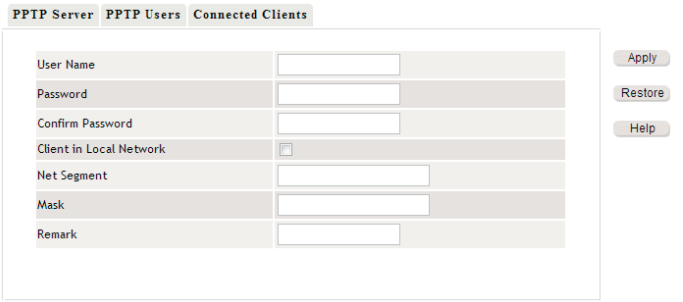
Example: You are traveling and/or working from a remote location and need access to a server at the office or on your home network. The XBR-2300's VPN Server can be configured to allow access to the internal network while providing a secure encrypted connection.



- **Enable PPTP:** Enables the PPTP VPN Server
- **Maximum Connections:** The maximum number of supported concurrent PPTP VPN connections
- **PPTP Server Address:** The address you would like the PPTP VPN server to run on. This is typically configured as WAN interface 1 or 2
- **Client DHCP Address Range:** The available internal IP Addresses available to VPN clients
- **128-bit Encryption:** Enables the PPTP VPN encryption. Both the Client and Server must have encryption enabled to create a connection. The XBR-2300 supports 128-bit data encryption

5.7.2.2 PPTP Users

This section allows the creation of accounts that can be used by the PPTP clients to connect to the server.



- **User Name:** User name to connect to the PPTP Server
- **Password:** Password to connect to the PPTP Server
- **Confirm Password:** Re-confirm the Password for connecting to the PPTP Server
- **Client is Local Network:** Select the access mode of the PPTP Client. The VPN Server can be set to allow access to a single IP or to the entire internal network

NOTE: You must choose network for the Client if the Client is another Router.

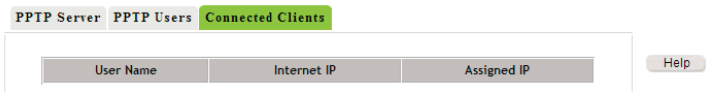
Net Segment: PPTP Client network segment

Mask: PPTP Client Subnet Mask

Remark: Displays when the Client connection is used (optional)

5.7.2.3 Connected Clients

This page shows the information of PPTP Clients that are connected.



- **User name:** User name of PPTP Client
- **Internet IP:** PPTP Client remote IP address
- **Assign IP:** Internal IP address assigned by the PPTP Server

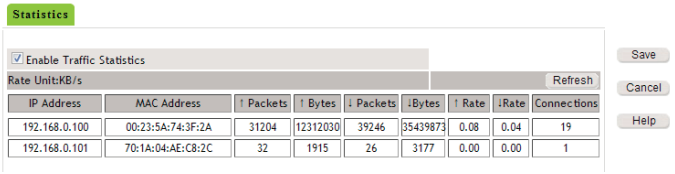
5.8 Monitor

There are three submenus in the Monitor section:

- **5.8.1 Statistics**
- **5.8.2 Logs**
- **5.8.3 Syslog**

5.8.1 Statistics

Displays traffic statistics of the XBR-2300 by connected device.



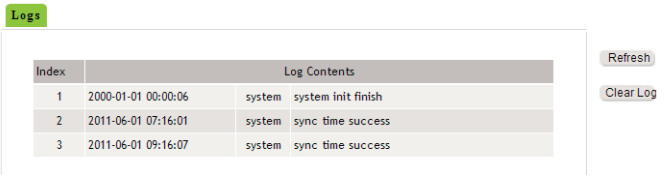
- Enable Traffic Statistics: Enables or Disables traffic statistics (Disabled by default).

NOTE: It is recommended to use Traffic Statistics only when necessary and then disable to ensure best possible network performance.

- Refresh: Refreshes the Statistics list

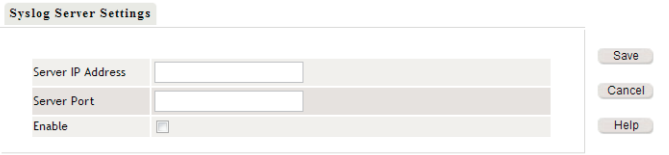
5.8.2 Logs

The Logs page shows any alerts listed by the XBR-2300 including: Restarts, Attacks, and VPN Connections.



5.8.3 Syslog

By default, the XBR-2300 will only display the most recent 256 log entries. If it is necessary to save all logs generated, the XBR-2300 can be configured to send log entries to a Log Server.



- **Server IP Address:** IP address of Log Server
- **Server Port:** Service port of Log Server
- **Enable:** Enables remote logging

5.9 System Tools

There are seven submenus in the System Tools section:

- **5.9.1 Time Settings**
- **5.9.2 Backup and Restore**
- **5.9.3 Firmware Upgrade**
- **5.9.4 Policy Upgrade**
- **5.9.5 Restore Factory Default**
- **5.9.6 Reboot**
- **5.9.7 Change Password/ Username**

5.9.1 Time Settings

This is where the Time, Date and Time Zone are set for the XBR-2300.

Time zone can be manually set by the user or GMT can be automatically obtained from the Internet. If the automatic GMT option is selected, time can only be set after the XBR-2300 has access to the Internet. Current time can also be set manually.

- **Enable Network Time:** System time is obtained automatically from the Internet
- **Update Interval:** Sets the time Adjusting Period for Daylight Savings
- **Time Zone:** Sets the Local Time Zone in which the XBR-2300 resides

5.9.2 Backup/Restore

This section allows you to Backup and Restore the XBR-2300 configuration.

- **Backup:** Click "Backup" to be given a Save Configuration dialog box
- **Restore:** Click "Browse" to select a saved Configuration file on your device

5.9.3 Firmware Upgrade

This section allows for the upgrade of the XBR-2300 Firmware. It is recommended to check regularly for any Firmware updates.

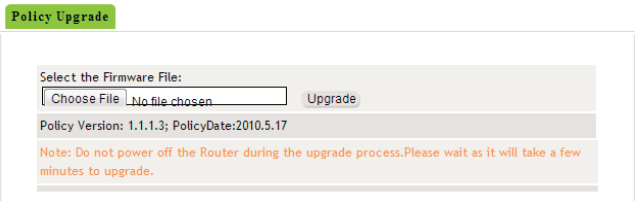
Firmware upgrading steps

1. **Browse:** To select the path of the Firmware File
2. **Upgrade:** Performs the upgrade with the selected Firmware File
3. **Router automatically reboots after being upgraded**

WARNING!: Do not shut down power to the XBR-2300 during the upgrade process or the router will be damaged. The XBR-2300 will automatically restart after a successful upgrade. The upgrade process may take several minutes to finish.

5.9.4 Policy Upgrade

Policy Upgrade updates the automatic filters on the device, creating a more secure network. It is recommended to run this Upgrade periodically to obtain new definitions.



Policy upgrading steps:

1. **Browse:** To select the current Policy File
2. **Upgrade:** Upgrades the XBR-2300 Policy File using the selected Policy File

5.8.5 Restore Defaults

This option can be used to restore the XBR-2300 to Factory Default Settings. This is useful if there are any configuration errors.

- **Default Password:** admin
- **Default IP Address:** 192.168.0.1
- **Default Subnet Mask:** 255.255.255.0

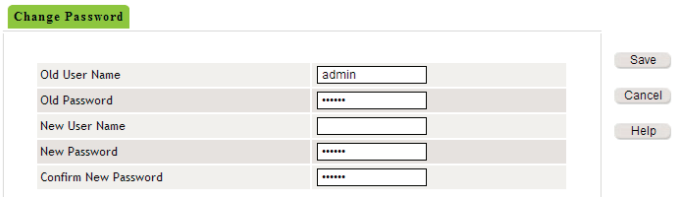
NOTE: Restore Factory Default only takes effect after the router reboots

5.9.6 Reboot

Forces a Reboot of the XBR-2300. This option is used when a configuration change requires a Reboot in order to take effect.

5.9.7 Username/Password

This Page allows you to change the Username and Password of the XBR-2300 configuration interface.



- **Old User Name:** Current User Name
- **Old Password:** Current Password
- **New User Name:** The desired new User Name
- **New Password:** The desired new Password

CAUTION: It is highly recommended that you change the default User Name and Password for security.

5.10 Logout

Logs you out of the configuration interface of the XBR-2300.

6: REGULATORY COMPLIANCE

This device is approved under the Luxul brand and designed to comply for use specifically with other approved Luxul devices. This device is designed to be compliant with rules and regulations in locations where they are sold and will be labeled as required. Any changes or modifications to Luxul equipment, not expressly approved by Luxul, could void the user's authority to operate the equipment. This Luxul device when used in conjunction with the approved Luxul Models should be professionally installed and the Radio Frequency Output Power will not exceed the maximum allowable limit for those countries that have regulatory approval.

6.1 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.

Power Supply: Use only a Luxul approved power supply output rated at 100-240VDC and minimum 0.1A. The power supply shall be Listed to UL/CSA 60950-1; and certified to IEC60950-1 and EN60950-1 with SELV outputs. The device can also be powered from a compliant POE source. Use of alternative power supply will invalidate any approval given to this device and may be dangerous.

6.2 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 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.

7: CONTACT LUXUL

For sales questions please contact our Sales Department

P: (801) 822-5450
E: sales@luxul.com

If you experience any problems, please contact Technical Support

P: (801) 822-5450
E: support@luxul.com

To check for firmware updates or download pre-configured application modules, visit luxul.com.

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 the computer. (i.e. ipconfig/all) Must be run from the command line.
Ping	Used to test for network availability and device/system recognition. 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. Must be run from the command line.
netstat	Displays details of current 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 tim. Must be run from the command line.

357 South 670 West | Suite 160 | Lindon, UT 84042
p: 801-822-5450 | f: 801-822-5460