

2.4GHz Wireless 802.11n(DRAFT) Giga Router

WRT-390L

Rev 0.7

User Manual

Federal Communication Commission Interference Statement

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

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Copyright

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Copyright 2006

Trademark recognition

All product names used in this manual are the properties of their respective owners and are acknowledged.

Table of Contents

Getting Started with the WRT-390L	3
Package Contents	
Minimum System Requirements	
Wireless LAN Networking	5
Introduction	
Features	
Hardware Overview	10
LED Indications	
Rear Panel	
Installation Considerations	
Getting Started	
Using the Configuration Menu	12
Network	
Wireless	
Advanced	
Administrator	

1. Getting Started with the WRT-390L

Congratulations on purchasing the WRT-390L! This manual provides information for setting up and configuring the WRT-390L. This manual is intended for both home users and professionals.

The following conventions are used in this manual:



THE NOTE SYMBOL INDICATES ADDITIONAL INFORMATION ON THE TOPIC AT HAND.



THE TIP SYMBOL INDICATES HELPFULL INFORMATION AND TIPS TO IMPROVE YOUR NETWORK EXPERIENCE.



THE CAUTION SYMBOL ALERTS YOU TO SITUATIONS THAT MAY DEGRADE YOUR NETWORKING EXPERIENCE OR COMPROMISE



LIKE NOTES, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVERLOOKED.

1.1 Package Contents

- WRT-390L 2.4GHz Wireless 802.11n(DRAFT) Giga Router
- CAT-5 Ethernet Cable
- Power Adapter (12V, 1A)
- CD-ROM with Manual
- Quick Installation Guide



Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.

1.2 Minimum System Requirements

- Ethernet-Based Cable or DSL Modem
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter and CD-ROM Drive
- Internet Explorer Version 6.0 or Netscape Navigator Version 7.0 and Above

2. Wireless LAN Networking

This section provides background information on wireless LAN networking technology. Consult the **Glossary** for definitions of the terminology used in this section.



THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

Transmission Rate (Transfer Rate)

The WRT-390L provides various transmission (data) rate options for you to select. In most networking scenarios, the factory default Best (automatic) setting proves the most efficient. This setting allows your WRT-390L to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the WRT-390L automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the WRT-390L gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

Types of Wireless Networks

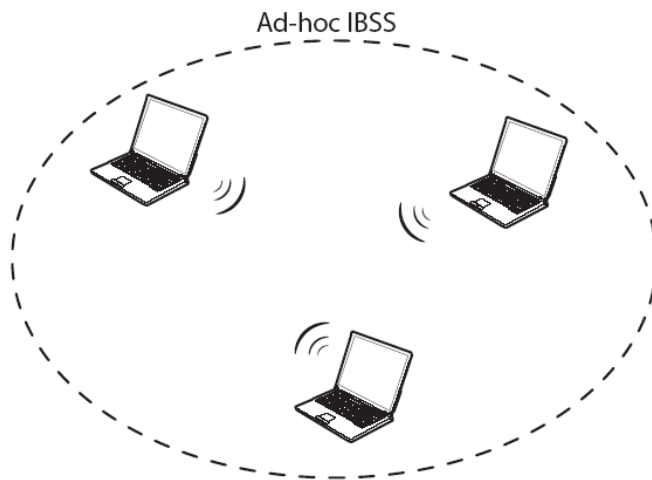
Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

AD-HOC (IBSS) NETWORK

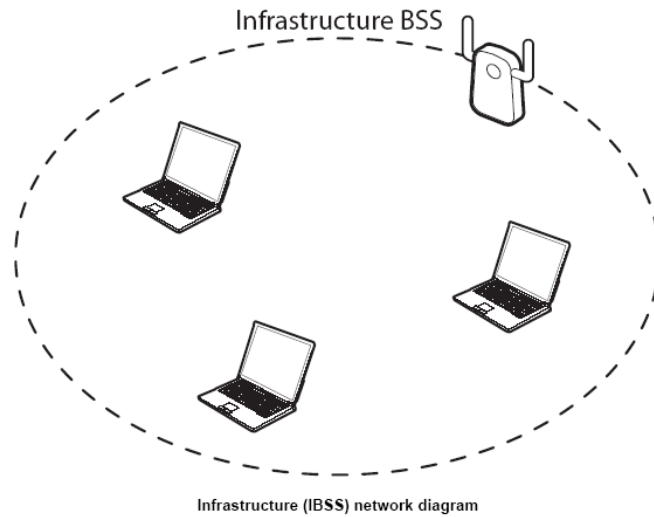
Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each station.

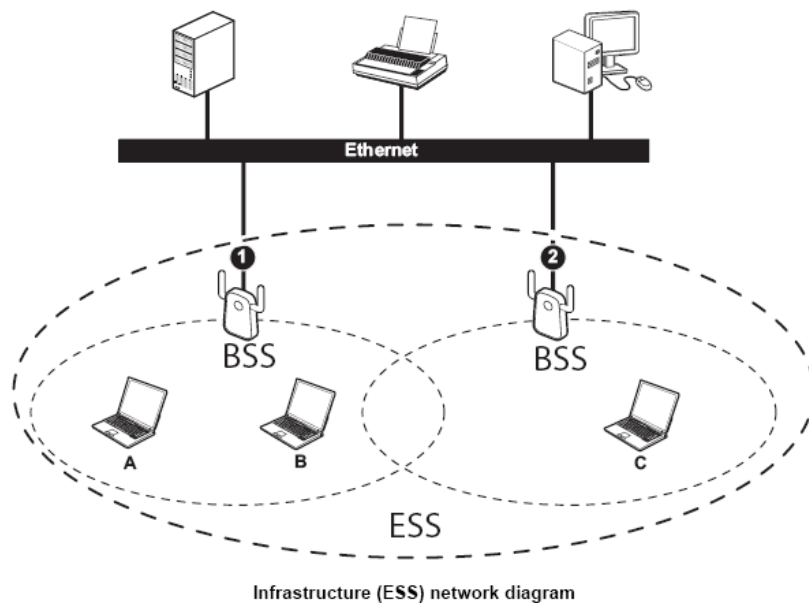


Ad-hoc (also known as peer-to-peer) network diagram

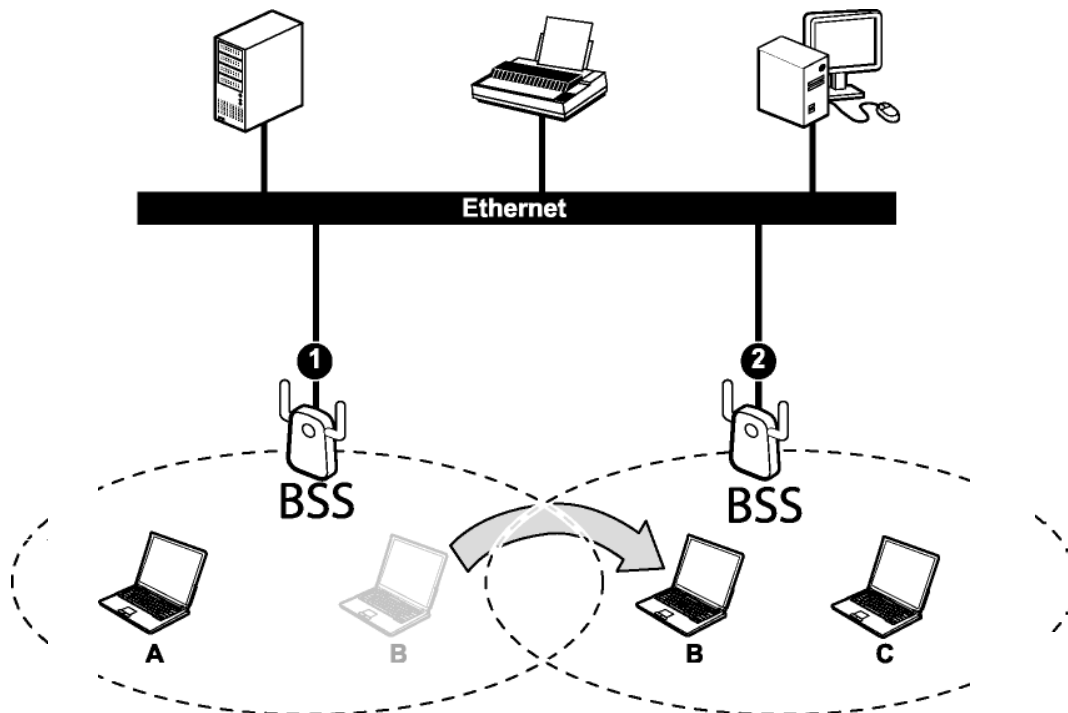
When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).



In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.



In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the WLAN client devices automatically switches to the channel used in BSS (2).



Roaming in an ESS network diagram

2.1 Introduction

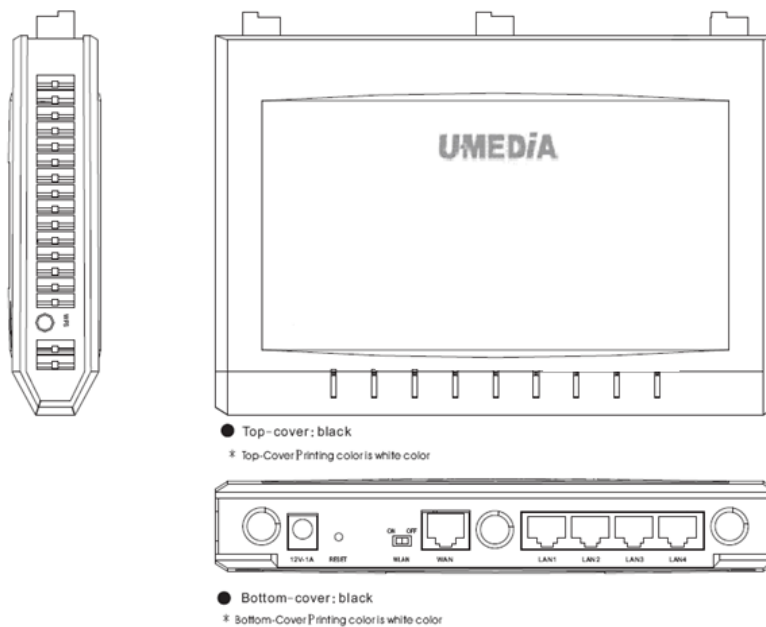
The WRT-390L 2.4GHz Wireless 802.11n(DRAFT) Giga Router is an high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

Unlike most routers, the WRT-390L provides data transfers at up to 300Mbps when using 11n (Draft) connection. This router is also back compatible with 802.11g or 11b devices. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 11n's (Draft) speed when you mix 11n (Draft) and 11b/g devices, but you will not lose the ability to communicate when you incorporate the 11n (Draft) standard into your 11b/g network. You may choose to slowly change your network by gradually replacing the 11b/g devices with 11n (Draft) devices.

2.2 Features

- Supports draft IEEE 802.11n & 11b/g 2.4GHz wireless Local Area Network (WLAN) application
- 2.412 to 2.462GHz frequency band operation
- Compliant with IEEE 802.3, 802.3u & 802.3ab standards
- Support OFDM and CCK modulation
- High-Speed up to 300Mbps Data Rate using IEEE 802.11n (draft) connection
- Supports Cable/DSL Modems with Dynamic IP, Static IP, PPPoE, PPTP, L2TP Connection Types
- Firewall features Network Address Translation (NAT)
- Traffic Control with Virtual Server and DMZ
- UPnP (Universal Plug & Play) and ALGs Support for Internet applications such as Email, FTP, Gaming, Streaming, Net Meeting, Telnet, and more
- Provides Additional Security of Enable/Disable SSID, Internet Access Control (IP/Port range blocking)
- Supports IPSec, L2TP and PPTP VPN Pass-Through Sessions
- Flash Memory for Firmware Upgrade, Save/Restore Settings
- Easy Management via Web Browser (HTTP) and Remote Management
- Supports 64/128-bit WEP, WPA/WPA2, and WPA-PSK/WPA2-PSK.
- Easy wireless setup via PBC or PIN of WiFi Protected Setup
- Work with IE6.0 and above, web browsers.
- Support 4 x 10/100/1000Mbps Auto-MDIX LAN Port and 1 x 10/100/1000Mbps WAN Port (Internet)
- Built-in 3 External Antennas to support high speed performance and great coverage

3. Hardware Overview



3.1 LED Indications: (from bottom to top)

- ◆ PWR
- ◆ WAN
- ◆ LAN1
- ◆ LAN2
- ◆ LAN3
- ◆ LAN4
- ◆ Wireless
- ◆ WPS
- ◆ Reserve
- ◆ Reserve

3.2 Rear panel: (from bottom to top)

- ◆ DC-IN
- ◆ RESET
- ◆ WAN
- ◆ LAN1
- ◆ LAN2
- ◆ LAN3
- ◆ LAN4

3.3 Installation Considerations

The WRT-390L 2.4GHz Wireless 802.11n(DRAFT) Giga Router lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- 1 Keep the number of walls and ceilings between the WRT-390L and other network devices to a minimum - each wall or ceiling can reduce your wireless product's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- 2 Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- 3 Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- 4 Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise.

3.4 Getting Started

For a typical wireless setup at home, please do the following:

1. You will need broadband Internet access (a Cable or DSL-subscriber line into your home or office)
2. Consult with your Cable or DSL provider for proper installation of the modem.
3. Connect the Cable or DSL modem to the WRT-390L Wireless Broadband Router (WAN port).
4. Ethernet LAN ports of the WRT-390L are Auto MDI/MDIX and will work with both Straight-Through and Cross-Over cable.

4. Using the Configuration Menu

Whenever you want to configure your WRT-390L, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the WRT-390L. The WRT-390L's default IP Address is <http://10.10.10.254>

- Open the Web browser.
- Type in the **IP Address** of the Router (<http://10.10.10.254>).



If you have changed the default IP Address assigned to the WRT-390L, make sure to enter the correct IP Address.

NOTE

- Select **admin** in the **User Name** field.
- Leave the **Password** blank.
- Click **Login In**.

4.1 Network

Network: Wan Setting

Network <ul style="list-style-type: none">• Wan Setting• Lan Setting• DHCP Client List Wireless Advanced Administrator	Wide Area Network (WAN) Settings <p>You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.</p>									
	WAN Connection Type									
	Connection Type <input type="text" value="STATIC"/>									
	WAN Interface IP Setting									
	<table><tr><td>IP Address</td><td><input type="text" value="192.168.100.100"/></td></tr><tr><td>Subnet Mask</td><td><input type="text" value="255.255.255.0"/></td></tr><tr><td>Default Gateway</td><td><input type="text" value="192.168.100.1"/></td></tr><tr><td>Primary DNS Server</td><td><input type="text" value="168.95.192.1"/></td></tr><tr><td>Secondary DNS Server</td><td><input type="text"/></td></tr></table>	IP Address	<input type="text" value="192.168.100.100"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>	Default Gateway	<input type="text" value="192.168.100.1"/>	Primary DNS Server	<input type="text" value="168.95.192.1"/>	Secondary DNS Server
IP Address	<input type="text" value="192.168.100.100"/>									
Subnet Mask	<input type="text" value="255.255.255.0"/>									
Default Gateway	<input type="text" value="192.168.100.1"/>									
Primary DNS Server	<input type="text" value="168.95.192.1"/>									
Secondary DNS Server	<input type="text"/>									
WAN MTU Setting										
Use Default MTU Setting <input type="text" value="Enabled"/>										
MTU Setting <input type="text" value="1500"/> (bytes) default=1500 bytes										
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>										

Network: Lan Setting

Network

- Wan Setting
- **Lan Setting**
- DHCP Client List

Wireless**Advanced****Administrator**

Local Area Network (LAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

LAN Interface Setting

IP Address	<input type="text" value="192.168.10.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
MAC Address	00:81:74:E0:02:96

DHCP Server Setting

DHCP Server	<input type="text" value="Enable"/>
DHCP Start IP	<input type="text" value="192.168.10.100"/>
DHCP End IP	<input type="text" value="192.168.10.200"/>
DHCP Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Default Gateway	<input type="text" value="192.168.10.1"/>
DHCP Lease Time	<input type="text" value="86400"/>

Add DHCP Reservation

Enable	<input type="checkbox"/>
Computer Name	<input type="text"/>
IP Address	<input type="text"/>
MAC Address	<input type="text"/> (Ex: 00:11:22:33:44:55)

DHCP Reservations List

Enable	Computer Name	IP Address	MAC Address	Edit	DEL
--------	---------------	------------	-------------	------	-----

LAN Interface Setting

IP Address

The IP address of the this device on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.0.101.

Subnet Mask

The subnet mask of the local area network.

DHCP Server Settings

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Enable DHCP Server

Once your router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically". When you set **Enable DHCP Server**, the following options are displayed.

DHCP IP Address Range

These two IP values (Start and End) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved, so that the DHCP Server knows that this specific address can only be used by a specific computer or device.

Your router, by default, has a static IP address of 192.168.0.1. This means that addresses 192.168.0.2 to 192.168.0.254 can be made available for allocation by the DHCP Server.

Subnet Mask

The subnet mask of the local area network.

Gateway

The IP address of the router on the local area network. For example, 192.168.0.1.

DHCP Lease Time

The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

Add/Edit DHCP Reservation

This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the

same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

Computer Name

You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way. Example: **Game Server**.

IP Address:

The LAN address that you want to reserve.

MAC Address

To input the MAC address of your system, enter it in manually or connect to the router's Web-Management interface from the system and click the **Copy Your PC's MAC Address** button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the router from the computer and click the **Copy Your PC's MAC Address** button to enter the MAC address.

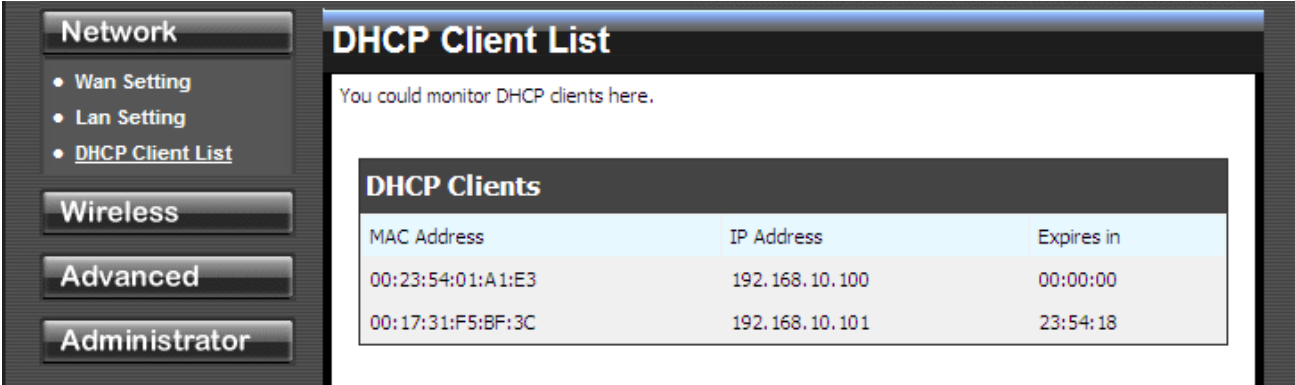
Clear

Re-initialize this area of the screen, discarding any changes you have made.

DHCP Reservations List

This shows clients that you have specified to have reserved DHCP addresses. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit DHCP Reservation" section is activated for editing.

Network: DHCP Client List



The screenshot shows a web-based network management interface. On the left is a sidebar with a 'Network' menu containing 'Wan Setting', 'Lan Setting', and 'DHCP Client List'. Below this are buttons for 'Wireless', 'Advanced', and 'Administrator'. The main content area is titled 'DHCP Client List' and contains the text 'You could monitor DHCP clients here.' followed by a table of active DHCP clients.

MAC Address	IP Address	Expires in
00:23:54:01:A1:E3	192.168.10.100	00:00:00
00:17:31:F5:BF:3C	192.168.10.101	23:54:18

DHCP Client List

In this section you can see what LAN devices are currently leasing IP addresses.

4.2 Wireless

Wireless: Basic

Network	Basic Wireless Settings
Wireless	You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.
<ul style="list-style-type: none">• Basic• Advanced• Security• WPS• Station List	
Advanced	
Administrator	

Wireless Network	
Radio On/Off	<input type="button" value="RADIO ON"/>
Wireless Mode	2.4GHz 802.11 b/g/n mixed mode ▾
Wireless Name (SSID)	TRENDnet639
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	00:81:74:E0:02:96
Frequency (Channel)	2437MHz (Channel 6) ▾

Wireless Distribution System(WDS)	
WDS	<input type="button" value="Disable"/> ▾

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input checked="" type="radio"/> 20 <input type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
MCS	Auto ▾
Reverse Direction Grant (RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10) ▾

<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
--------------------------------------	---------------------------------------

Radio On/Off

This indicates the wireless operating status. The wireless can be turned on or off by the slide switch. When the radio is on, the following parameters are in effect.

Wireless Mode

If all of the wireless devices you want to connect with this router can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Wireless Network Name (SSID)

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.

Frequency (Channel)

A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

Wireless: Advanced

Advanced Wireless	
Beacon Interval	100 ms (range 20 - 1000, default 100)
DTIM	1 (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Apply Cancel

Beacon Interval

Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

DTIM

A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Fragmentation Threshold

Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.

RTS Threshold

When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value

of 2346 bytes.

Short Preamble and Slot

Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

Wireless: Security

The screenshot displays the 'Wireless Security Setting' configuration page. On the left sidebar, the 'Wireless' menu is active, with 'Security' selected. The main panel is titled 'Wireless Security Setting' and includes the following fields:

- Select SSID:** A dropdown menu showing 'TRENDnet639'.
- Security Policy: TRENDnet639:** A dropdown menu showing 'Disable'.
- Wireless MAC Filter:** A dropdown menu showing 'Disable' and an empty text input field for the MAC address, with a hint '(Ex: 00:11:22:33:44:55)'.

At the bottom of the main panel are 'Apply' and 'Cancel' buttons.

Security Mode

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

WEP

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

WPA-Personal and WPA-Enterprise

Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ.

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

Cipher Type: The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.

WPA-Personal

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

WPA-Enterprise

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

Authentication Timeout: Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

Wireless MAC Filtering

Choose the type of MAC filtering needed.

Turn MAC Filtering Disable: When "Disable" is selected, MAC addresses are not used to control network access.

Add MAC Filtering Rule

Use this section to add MAC addresses to the list below.

MAC Address

Enter the MAC address of a computer that you want to control with MAC filtering. Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu.

Wireless: WPS

The screenshot shows the 'Wi-Fi Protected Setup' configuration page. On the left is a navigation menu with 'Network', 'Wireless', 'Advanced', and 'Administrator' sections. The 'Wireless' section is expanded, showing 'Basic', 'Advanced', 'Security', 'WPS', and 'Station List'. The main content area is titled 'Wi-Fi Protected Setup' and includes a sub-header 'WPS Config' with a 'WPS' dropdown set to 'Enable' and an 'Apply' button. Below this is a 'WPS Summary' table with the following data:

WPS Current Status	Not used
WPS Configured	No
WPS SSID	TRENDnet639
WPS Auth Mode	Open
WPS Encryp Type	None
WPS Default Key Index	1
WPS Key(ASCII)	
AP PIN	46807267

Below the summary is a 'Reset To WPS Default' button. The next section is 'WPS Action', featuring a 'WPS mode' section with radio buttons for 'PIN' (selected) and 'PBC', and a 'Client PIN' text input field with an 'Apply' button. The final section is 'WPS Status', which shows 'WSC:Not used' and a scrollable area for logs.

WPS

Enable

Enable the WPS feature.

Lock Wireless Security Settings

Locking the wireless security settings prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using WPS.

PIN Settings

A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

Current PIN

Shows the current value of the router's PIN.

Reset To WPS Default

Restore the default PIN of the router.

Generate New PIN

Create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.

Wireless: Station List

The screenshot shows a web interface with a dark grey sidebar on the left and a main content area on the right. The sidebar contains several buttons: 'Network', 'Wireless', 'Advanced', and 'Administrator'. Under the 'Wireless' button, there is a list of sub-items: 'Basic', 'Advanced', 'Security', 'WPS', and 'Station List'. The 'Station List' item is highlighted with a blue underline. The main content area has a blue header bar with the text 'Station List'. Below the header, there is a white box containing the text 'You could monitor stations which associated to this AP here.' Below this text is a table with a dark grey header row and a light blue header row. The table header row contains the text 'Wireless Network'. The light blue header row contains three columns: 'MAC Address', 'Aid', and 'PSM'. The table body is currently empty.

Network

Wireless

- Basic
- Advanced
- Security
- WPS
- Station List

Advanced

Administrator

Station List

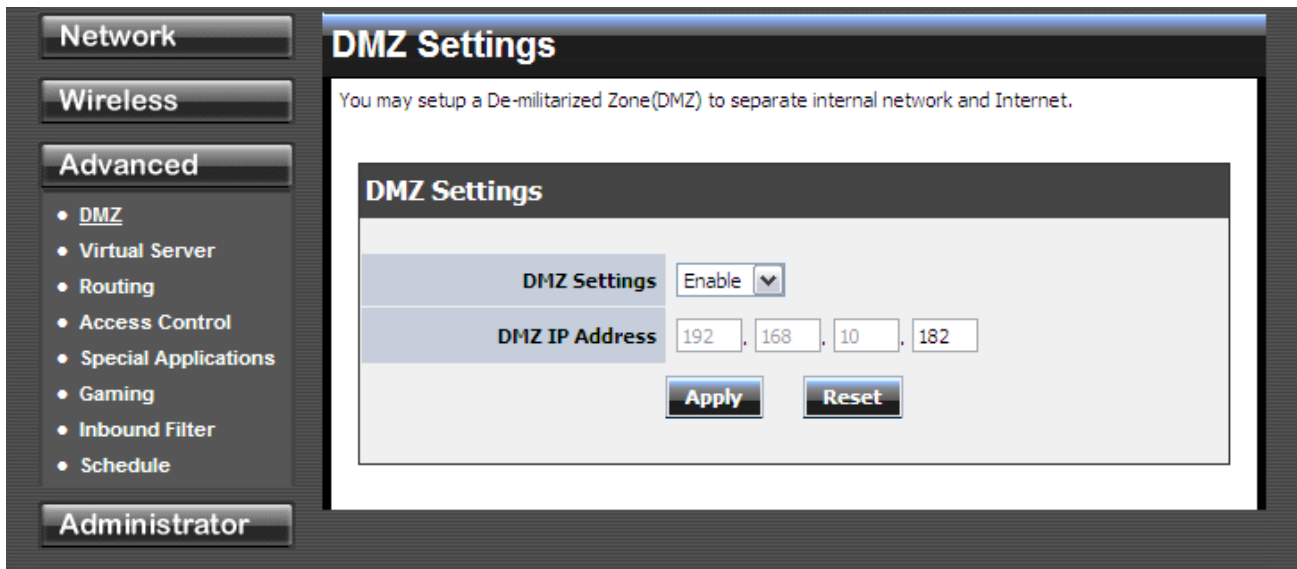
You could monitor stations which associated to this AP here.

Wireless Network

MAC Address	Aid	PSM
-------------	-----	-----

4.3 Advanced

Advanced: DMZ



DMZ Setting

DMZ means "Demilitarized Zone." If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

When a LAN host is configured as a DMZ host, it becomes the destination for all incoming packets that do not match some other incoming session or rule. If any other ingress rule is in place, that will be used instead of sending packets to the DMZ host; so, an active session, virtual server, active port trigger, or port forwarding rule will take priority over sending a packet to the DMZ host. (The DMZ policy resembles a default port forwarding rule that forwards every port that is not specifically sent anywhere else.)

The router provides only limited firewall protection for the DMZ host. The router does not forward a TCP packet that does not match an active DMZ session, unless it is a connection establishment packet (SYN). Except for this limited protection, the DMZ host is effectively "outside the firewall". Anyone considering using a DMZ host should also consider running a firewall on that DMZ host system to provide additional protection.

Packets received by the DMZ host have their IP addresses translated from the WAN-side IP address of the router to the LAN-side IP address of the DMZ host. However, port numbers are not translated; so applications on the DMZ host can depend on specific port numbers.

The DMZ capability is just one of several means for allowing incoming requests that might appear unsolicited to the NAT. In general, the DMZ host should be used only if there are no other alternatives, because it is much more exposed to cyberattacks than any other system on the LAN. Thought should be given to using other configurations instead: a virtual server, a port forwarding rule, or a port trigger. Virtual servers open one port for incoming sessions bound for a specific application (and also allow port redirection and the use of ALGs). Port forwarding is rather like a selective DMZ, where incoming traffic targeted at one or more ports is forwarded to a specific LAN host (thereby not exposing as many ports as a DMZ host). Port triggering is a special form of port forwarding, which is activated by outgoing traffic, and for which ports are

only forwarded while the trigger is active.

Few applications truly require the use of the DMZ host. Following are examples of when a DMZ host might be required:

- A host needs to support several applications that might use overlapping ingress ports such that two port forwarding rules cannot be used because they would potentially be in conflict.
- To handle incoming connections that use a protocol other than ICMP, TCP, UDP, and IGMP (also GRE and ESP, when these protocols are enabled by the PPTP and IPsec ALGs).

Enable DMZ



Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

NOTE

DMZ IP Address

Specify the LAN IP address of the LAN computer that you want to have unrestricted Internet communication.

Advanced: Virtual Server

The Virtual Server can define a single public port for redirection to an internal IP and port.

Add Virtual Server

Rule Enable	<input type="checkbox"/>
Rule Name	<input type="text"/>
IP Address	<input type="text"/>
Protocol	TCP <input type="button" value="v"/>
Public Port	<input type="text"/>
Private Port	<input type="text"/>
Inbound Filter	Allow All <input type="button" value="v"/>
Schedule	Always <input type="button" value="v"/>

Virtual Server List

Enable	Rule Name	IP Address	Protocol, Public Port/Private Port	Inbound Filter	Schedule	Edit	DEL

Add/Edit Virtual Server

Enable

Specifies whether the entry will be active or inactive.

Name

Assign a meaningful name to the virtual server, for example **Web Server**. Several well-known types of virtual server are available from the "Application Name" drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.

IP Address

The IP address of the system on your internal network that will provide the virtual service, for example **192.168.0.50**. You can select a computer from the list of DHCP clients in the "Computer Name" drop-down menu, or you can manually enter the IP address of the server computer.

Protocol

Select the protocol used by the service. The common choices -- UDP, TCP, and both UDP and TCP -- can be selected from the drop-down menu. To specify any other protocol, select "Other" from the list, then enter the corresponding protocol number (as assigned by the IANA) in the **Protocol** box.

Private Port

The port that will be used on your internal network.

Public Port

The port that will be accessed from the Internet.

Schedule

Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules.

Clear

Re-initialize this area of the screen, discarding any changes you have made.

Advanced: Routing

Static Routing Settings

The Static Routing option allows you to define fixed routes to specific destinations

Add Static Route

Destination IP Address :

Destination IP Netmask :

Gateway :

Metric :

Interface :

Static Route List

No.	IP	Netmask	Gateway	Metric	Interface
-----	----	---------	---------	--------	-----------

Routing Table

IP	Netmask	Gateway	Metric	Interface
239.255.255.250	255.255.255.255	0.0.0.0	0	LAN/WLAN
192.168.100.0	255.255.255.0	0.0.0.0	0	WAN
192.168.10.0	255.255.255.0	0.0.0.0	0	LAN/WLAN
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN/WLAN
224.0.0.0	240.0.0.0	0.0.0.0	0	LAN/WLAN
0.0.0.0	0.0.0.0	192.168.100.1	0	WAN

Add/Edit Route

Adds a new route to the IP routing table or edits an existing route.

Destination IP

The IP address of packets that will take this route.

Gateway

Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN.

Metric

The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.

Interface

Specifies the interface -- LAN or WAN -- that the IP packet must use to transit out of the router, when this route is used.

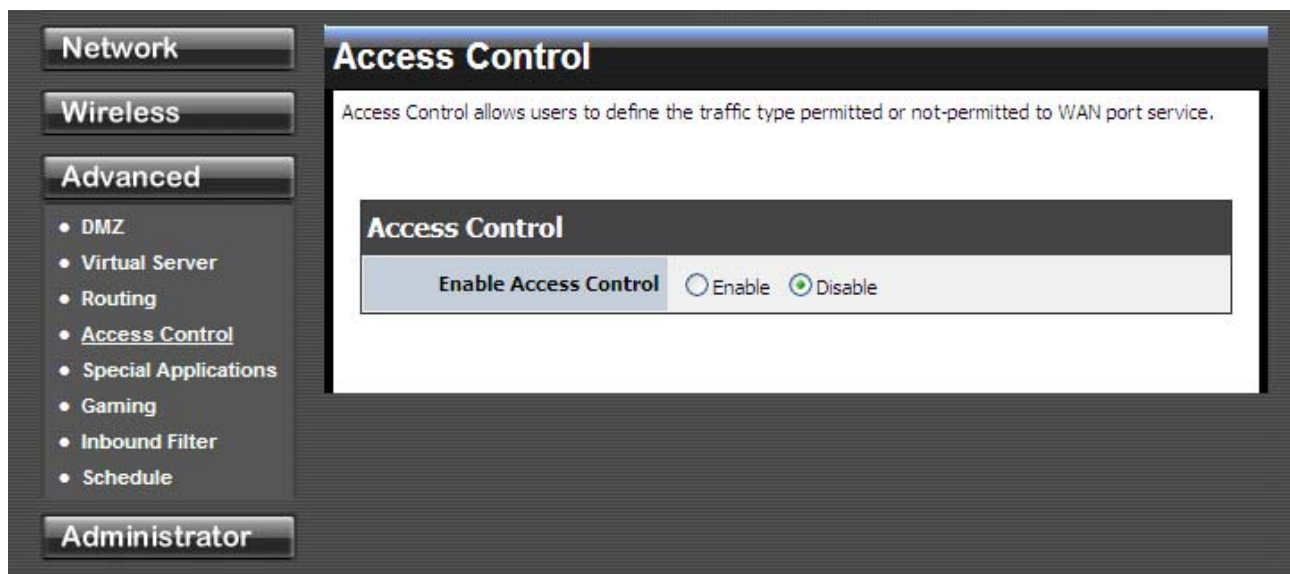
Clear

Re-initialize this area of the screen, discarding any changes you have made.

Routes List

The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Route" section is activated for editing. Click the Enable checkbox at the left to directly activate or de-activate the entry.

Advanced: Access Control



Enable

By default, the Access Control feature is disabled. If you need Access Control, check this option.

Note: When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.

Advanced: Special Applications

The screenshot shows a web-based configuration interface for a network device. On the left is a sidebar with navigation tabs: Network, Wireless, Advanced, and Administrator. The 'Advanced' tab is selected, showing a list of options: DMZ, Virtual Server, Routing, Access Control, Special Applications (highlighted), Gaming, Inbound Filter, and Schedule. The main content area is titled 'Port Trigger' and contains the following sections:

- Port Trigger Function:** A section with a 'Port Triggering' dropdown menu set to 'Enable' and an 'Apply' button.
- Add Port Trigger Rule:** A form with fields for:
 - Rule Enable:
 - Rule Name:
 - Match Protocol: TCP (dropdown)
 - Match Port:
 - Trigger Protocol: TCP (dropdown)
 - Trigger Port:
 - Schedule: Always (dropdown)Buttons for 'Add' and 'Clear' are at the bottom.
- Port Trigger Rule List:** A table with columns: En., Rule Name, Match Port Protocol/Ports, Trigger Port Protocol/Ports, Schedule, and Edit.

Add/Edit Port Trigger Rule

Enable

Specifies whether the entry will be active or inactive.

Name

Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. Alternatively, you can select from the **Application** list of common applications.

Protocol

Select the protocol used by the service. The common choices -- UDP, TCP, and both UDP and TCP -- can be selected from the drop-down menu.

Trigger Port

Enter the outgoing port range used by your application (for example **6500-6700**).

Schedule

Select a schedule for when this rule is in effect.

Clear

Re-initialize this area of the screen, discarding any changes you have made.

Port Trigger Rule List

This is a list of the defined application rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon.

Advanced: Gaming

That can open multiple ports or a range of ports in your router. The formats including Port Ranges (50-60), Individual Ports (21, 25, 80), or Mixed (3000-5000, 8080).

Add Port Range Rule

Rule Enable	<input type="checkbox"/>
Rule Name	<input type="text"/>
IP Address	<input type="text"/>
TCP Ports to Open :	<input type="text"/>
UDP Ports to Open :	<input type="text"/>
Inbound Filter	Allow All ▾
Schedule	Always ▾

Port Range Rule List

Enable	Rule Name	IP Address	TCP/UDP Ports	Inbound Filter	Schedule	Edit	Delete

Add/Edit Port Range Rule

Use this section to add a Port Range Rule to the following list or to edit a rule already in the list.

Rule Enable

Specifies whether the entry will be active or inactive.

Rule Name

Give the rule a name that is meaningful to you, for example **Game Server**. You can also select from a list of popular games, and many of the remaining configuration values will be filled in accordingly. However, you should check whether the port values have changed since this list was created, and you must fill in the IP address field.

IP Address

Enter the local network IP address of the system hosting the server, for example **192.168.0.50**. You can select a computer from the list of DHCP clients in the "Computer Name" drop-down menu, or you can manually enter the IP address of the server computer.

TCP Ports to Open

Enter the TCP ports to open (for example **6159-6180, 99**).

UDP Ports to Open

Enter the UDP ports to open (for example **6159-6180, 99**).

Inbound Filter

Select a filter that controls access as needed for this rule.

Schedule

Select a schedule for the times when this rule is in effect.

Clear

Re-initialize this area of the screen, discarding any changes you have made.

Port Range Rule List

This is a list of the defined Port Range Rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Port Forwarding Rule" section is activated for editing.

Advanced: Inbound Filter

Network

Wireless

Advanced

- DMZ
- Virtual Server
- Routing
- Access Control
- Special Applications
- Gaming
- Inbound Filter
- Schedule

Administrator

Inbound Filter

The Inbound Filter controlling data received from the Internet. In this feature you can configure inbound data filtering rules that control data based on an IP address.

Add Inbound Filter Rule

Rule Name

Rule Action Allow Deny

IP Address

Inbound Filter Rule List

Rule Name	RuleAction	IP Address	Edit	Delete
-----------	------------	------------	------	--------

Add/Edit Inbound Filter Rule

Here you can add entries to the Inbound Filter Rules List below, or edit existing entries.

Name

Enter a name for the rule that is meaningful to you.

Action

The rule can either Allow or Deny messages.

Remote IP Range

Define the ranges of Internet addresses this rule applies to. For a single IP address, enter the same address in both the **Start** and **End** boxes. Up to eight ranges can be entered. The **Enable** checkbox allows you to turn on or off specific entries in the list of ranges.

Clear

Re-initialize this area of the screen, discarding any changes you have made.

Inbound Filter Rules List

The section lists the current Inbound Filter Rules. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Inbound Filter Rule" section is activated for editing.

In addition to the filters listed here, two predefined filters are available wherever inbound filters can be applied:

Allow All

Permit any WAN user to access the related capability.

Deny All

Prevent all WAN users from accessing the related capability. (LAN users are not affected by Inbound Filter Rules.)

Advanced: Schedule

Schedule Rules
Define schedule rules for various firewall features.

Add Schedule Rule

Rule Name:

Day(s): Select Day(s) All Week

Sun Mon Tue Wed Thu Fri Sat

All Day - 24hrs:

Start Time: :

End Time: :

Schedule Rule List

Rule Name	Day(s)	Time stamp	Edit	Delete
-----------	--------	------------	------	--------

Add/Edit Schedule Rule

In this section you can add entries to the Schedule Rules List below or edit existing entries.

Name

Give the schedule a name that is meaningful to you, such as "Weekday rule".

Day(s)

Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.

All Day - 24 hrs

Select this option if you want this schedule in effect all day for the selected day(s).

Start Time

If you don't use the All Day option, then you enter the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email events are normally triggered only by the start time.

End Time

The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not normally used for email events.

Clear

Re-initialize this area of the screen, discarding any changes you have made.

Schedule Rules List

This section shows the currently defined Schedule Rules. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Schedule Rule" section is activated for editing.

4.4 Administrator

Administrator: Management

The screenshot displays the 'System Management' web interface. On the left is a navigation menu with categories: Network, Wireless, Advanced, and Administrator. Under 'Administrator', the following options are listed: Management (selected), Upload Firmware, Settings Management, Time, and Status. The main content area is titled 'System Management' and contains the following sections:

- Administrator Settings:** A form with 'Account' set to 'admin' and an empty 'Password' field. A red note indicates '(Max Length: 16 characters)'. 'Apply' and 'Cancel' buttons are present.
- Device Name Settings:** A form with 'Device Name' set to 'TEW-639GR'. 'Apply' and 'Cancel' buttons are present.
- DDNS Settings:** A form with 'Dynamic DNS Provider' set to 'None', and empty fields for 'Host Name', 'Account', and 'Password'. 'Apply' and 'Cancel' buttons are present.
- Remote Management:** A form with 'Remote Control (via WAN)' set to 'Disable' and 'Remote Port' set to '8080'. 'Apply' and 'Reset' buttons are present.

Admin Password

Enter a password for the user "admin", who will have full access to the Web-based

management interface.

Device Name

The name of the router can be changed here.

Enable Dynamic DNS

Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider. The following parameters are displayed when the option is enabled.

Dynamic DNS Provider

Select a dynamic DNS service provider from the pull-down list.

Host Name

Enter your host name, fully qualified; for example: **myhost.mydomain.net**.

Account

Enter the account provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Password

Enter the password provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Administrator: Setting Management

Network

Wireless

Advanced

Administrator

- Management
- Upload Firmware
- **Settings Management**
- Time
- Status

Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export Settings

Export

Import Settings

Settings file location

Load Factory Defaults

Load Default

System Reboot

System Reboot

Administrator: Time

The screenshot shows a web-based configuration interface for a router. On the left is a navigation menu with buttons for 'Network', 'Wireless', 'Advanced', and 'Administrator'. Under 'Administrator', there are links for 'Management', 'Upload Firmware', 'Settings Management', 'Time', and 'Status'. The main content area is titled 'Time Setting' and contains the following sections:

- Time Configuration:** A box labeled 'System Time' showing 'Sat Jan 10:31:1 2000'.
- NTP Settings:** A box labeled 'Enable NTP Server' with an unchecked checkbox.
- Date and Time Settings:** A box labeled 'Date And Time' with dropdown menus for Year (2004), Month (Jan), Day (01), Hour (01), Minute (31), and Second (00).

At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

Time Configuration

Current Router Time

Displays the time currently maintained by the router. If this is not correct, use the following options to configure the time correctly.

Time Zone

Select your local time zone from pull down menu.

Automatic Time Configuration

Enable NTP Server

Select this option if you want to synchronize the router's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.

Note that, even when NTP Server is enabled, you must still choose a time zone and set the daylight saving parameters.

NTP Server Used

Select a Network Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

Set the Date and Time Manually

If you do not have the NTP Server option in effect, you can either manually set the time for your router here.

Administrator: Status

Network

Wireless

Advanced

Administrator

- Management
- Upload Firmware
- Settings Management
- Time
- Status






Status

The device status.

System Info

Firmware Version	0.0.0.33, 6-Oct-2008
System Time	Sat Jan 1 0:31:28 2000
System Up Time	31:28

Cable Status

WAN	LAN 1	LAN 2	LAN 3	LAN 4
				

Internet Configurations

Connected Type	Static IP
WAN Network Status	Disconnected
WAN IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

LAN

MAC Address	00:81:74:E0:02:96
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

Wireless LAN

Wireless Radio	Radio On
MAC Address	00:81:74:E0:02:96
Network Name (SSID)	TRENDnet639
Channel	6
Security Mode	Disabled