TRENDnet®

User's Guide

TEW-692GR
1.01

Manual abstract:

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. 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. 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. 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. 2 Europe EU Declaration of Conformity This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC: EN60950-1:2006+A11: 2009 Safety of Information Technology Equipment EN 62311:2008 Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public EN 300 328 V1.7.1: (2006-10) Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.

2 of the R&TTE Directive EN 301 489-1 V1.8.1: (2008-04) Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements - - EN 301 489-17 V2.1.1:(2009-05) Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems This device is a 2.

4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies. In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services. This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France. 3 TRENDnet tímto prohlasuje, ze tento TEW-692GR je ve shod se základními Cesky [Czech] pozadavky a dalsími píslusnými ustanoveními smrnice 1999/5/ES. Dansk [Danish] Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-692GR overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. Hiermit erklärt TRENDnet, dass sich das Gerät TEW-692GR in Deutsch [German] Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet. Käesolevaga kinnitab TRENDnet seadme TEW-692GR vastavust direktiivi Eesti [Estonian] 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. Hereby, TRENDnet, declares that this TEW-692GR is in compliance with the English essential requirements and other relevant provisions of Directive 1999/5/EC.

Por medio de la presente TRENDnet declara que el TEW-692GR cumple con los Español [Spanish] requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. TRENDnet TEW-692GR [Greek] 1999/5/. Français Par la présente TRENDnet déclare que l'appareil TEW-692GR est conforme aux [French] exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Con la presente TRENDnet dichiara che questo TEW-692GR è conforme ai Italiano [Italian] requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. Ar so TRENDnet deklar, ka TEW-692GR atbilst Direktvas 1999/5/EK Latviski [Latvian] btiskajm prasbm un citiem ar to saisttajiem noteikumiem. Siuo TRENDnet deklaruoja, kad sis TEW-692GR atitinka esminius reikalavimus Lietuvi [Lithuanian] ir kitas 1999/5/EB Direktyvos nuostatas. 4 Nederlands [Dutch] Malti [Maltese] Magyar [Hungarian] Polski [Polish] Português [Portuguese] Slovensko [Slovenian] Slovensky [Slovak] Suomi [Finnish] Svenska [Swedish] Hierbij verklaart TRENDnet dat het toestel TEW-692GR in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Hawnhekk, TRENDnet, jiddikjara li dan TEW-692GR jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC. Alulírott, TRENDnet nyilatkozom, hogy a TEW-692GR megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak. Niniejszym TRENDnet owiadcza, e TEW-692GR jest zgodny z zasadniczymi wymogami oraz pozostalymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

TRENDnet declara que este TEW-692GR está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE. TRENDnet izjavlja, da je ta TEW-692GR v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolocili direktive 1999/5/ES. TRENDnet týmto vyhlasuje, ze TEW-692GR spa základné poziadavky a vsetky príslusné ustanovenia Smernice 1999/5/ES. TRENDnet vakuuttaa täten että TEW-692GR tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. Härmed intygar TRENDnet att denna TEW-692GR står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

European Union Notice: Radio products with the CE marking comply with the R&TTE Directive (1999/5/EC), the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community. Compliance with these directives implies conformity to the following European Norms: EN 60950 Product Safety EN 300 328 Technical requirement for radio equipment EN 301 489-1/-17 General EMC requirements for radio equipment Trademark recognition All product names used in this manual are the properties of their respective owners and are acknowledged. 5 Contents

.....
.....
....

....
.....
.....
....

....
.....
.....
....

....
.....
.....
....

... 42 Special Applications ....
.....
.....
....

....
.....
.....
....

....
.....
.....
....

...... 43 10/100/1000Mbps Auto-MDIX LAN ports 1 x 10/100/1000Mbps WAN port (Internet) Wi-Fi Protected Setup (WPS) button On/off power switch (EU Version) LED status indicators Compliant with IEEE 802.11n/b/g/a standards High-speed data rates of up to 450 Mbps using both 2.4 GHz and 5 GHz bands Enable/disable wireless functionality with the WLAN on/off toggle switch Compatible with most popular cable/DSL Internet Service Providers using Dynamic/Static IP, PPPoE, L2TP, and PPTP connection Advanced firewall protection with Network Address Translation (NAT) support Advanced wireless security of up to WPA2-RADIUS DMZ support Wi-Fi Multimedia (WMM) Quality of Service (QoS) data prioritization Support for up to four virtual wireless networks (SSIDs) per wireless band Gaming Port Controls: supports opening multiple ports or a range of ports Internet Access Control with MAC, URL, Service Type, and IP Range filtering Internet Access Control Rule Scheduling: schedule access to websites, online video games, Internet cameras and more for specific times through the week One touch wireless connection to wireless clients using the WPS button Easy setup via Web browser using the latest versions of Internet Explorer, FireFox, Safari, and Chrome Virtual server and Application Level Gateway (ALG) services for special Internet applications Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications Coverage up to 100 meters (330 ft.) indoor and 300 meters (980 ft.

) outdoor (depends on the environment) 3- year limited warranty 9 Overview NETWORK DIAGRAM: FRONT PANEL LEDS · · · · · · · · · · PWR WAN LAN1 LAN2 LAN3 LAN4 Wireless Wireless WPS Reserve REAR PANEL · · · · · · · DC-IN POWER SWITCH(EU) WAN LAN1 LAN2 LAN3 LAN4 10 WIRELESS PERFORMANCE CONSIDERATIONS There are a number of factors that can impact the range of wireless devices. 1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose. 2.

Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them. 3. Building materials can have a large impact on your wireless signal.

In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal. 4. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices. 5. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors. 6. Any device operating on the 2.

4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices. If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment. 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 TEW-639GR and other network devices to a minimum - each wall or ceiling can reduce your wireless products range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized. 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. 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. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise.*

2 3 4 11 Using the Configuration Menu Whenever you want to configure your TEW-692GR, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the TEW-692GR. The TEW-692GR's default IP Address is http://192.168.10.1 · · Open the Web browser. Type in the IP Address of the Router (http://192.168.10.1) If you have changed the default IP Address assigned to the TEW-692GR, make sure to enter the correct IP Address. · · · Select admin in the User Name field.

Default password is admin. Click OK. 12 Setup Wizard Setup Wizard is an easy way to set up the TEW-692GRstep by step. The Wizard will guide user's to set up the TEW-692GR in just few steps. To setup the router's internet connection settings, click Launch Internet Connection Setup Wizard' and follow Wizard to complete your setting.

Once the internet connection setup is completed, click "Launch Wireless Security Setup Wizard" to configure the router's wireless settings. 13 Network WAN SETTING There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and Russia PPTP. If you are unsure of your connection method, please contact your Internet Service Provider. WAN Connection Type There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and Russia PPTP. If you are unsure of your connection method, please contact your Internet Service Provider.

Static: Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings. You must enter the IP address, Subnet Mask, Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all of this information. DHCP:A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server.

Host Name: Some ISP's may check your computer's Host Name. The Host Name identifies your system to the ISP's server. 14 PPPoE: Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet.

Reconnect Mode: Typically PPPoE connections are not always on. The router allows you to set the reconnection mode. The settings are: Always on: A connection to the Internet is always maintained. On demand: A connection to the Internet is made as needed. Manual: You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet. Maximum Idle Time: Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes. L2TP:L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet. L2TP Server IP Address: The ISP provides this parameter, if necessary.

The value may be the same as the Gateway IP Address. Reconnect Mode: Typically PPPoE connections are not always on. The router allows you to set the reconnection mode. The settings are: Always on: A connection to the Internet is always maintained. On demand: A connection to the Internet is made as needed. Manual: You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet. Maximum Idle Time: Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes. WAN Interface IP Type Static: If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields for WAN Interface IP Setting: IP Address, Subnet Mask , Default Gateway.

Dynamic: If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option. PPTP: PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet. PPTP Server IP Address: The ISP provides this parameter, if necessary.

The value may be the same as the Gateway IP Address. 15 Reconnect Mode: Typically PPPoE connections are not always on. The router allows you to set the reconnection mode. The settings are: Always on: A connection to the Internet is always maintained. On demand: A connection to the Internet is made as needed.

Manual: You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet. Maximum Idle Time: Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes. WAN Interface IP Type Static: If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields for WAN Interface IP Setting: IP Address, Subnet Mask , Default Gateway, and optional for DNS Server Dynamic: If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option. Russia PPTP:The Russia PPTP can configure IP address on the WAN interface and establish PPTP to get IP address, subnet mask, default gateway and DNS for ANOTHER logical IP interface on WAN port. So the physical WAN port will have 2 logical IP interfaces and can communicate with internal ISP's network resources and also communicate with Internet through PPTP tunnel. It is specified by Russia Cobrina ISP, user can configure it the same as the normal PPTP and PPTP server IP Address can use the domain name string. WAN MTU Setting:The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets.

Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer. t modes. MAC Address Clone: Each networking device has it's own unique MAC address defined by the hardware manufacturer. Some ISP's may check your computer's MAC address. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address.

This router has a different MAC address than the computer or router that initially connected to the ISP. If you need to change the MAC address of the rounter's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the router using that computer and click the Clone Your PC's 16 MAC Address button. The WAN interface will then use the MAC address of the network adapter in your computer.

LAN 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. 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 192.168.10.

1. This means that addresses 192.168.10.2 to 192.168.10.254 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, 192.168.10.1. 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 17 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. 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 reserve 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. QOS QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications.

18 Upload Bandwidth: Limit bandwidth of upload manually with 'User Defined' or set the bandwidth limit via drop-down menu (between 64Mbits ~ 230Mbits) per device on network. DHCP CLIENT LIST This section displays all connected LAN devices currently receiving IP address from the router. 19 Wireless 2.4GHz BASIC 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 wireless mode. If you have some devices that use a different transmission mode, choose the appropriate wireless mode. The TEW-692GR supports 2.4GHz wireless networks.

There are many different configuration options available to choose from. Use the drop down list to select the wireless mode. Note: One wireless mode can be selected can select at any one time. This means that you can only select one of the operating frequency at a time. Wireless Mode options: 2.4GHz 802.11b/g mixed mode - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access the 20 TEW-692GRat 11Mbps for wireless b, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.

4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time. 2.4GHz 802.11 n only This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless n client devices to connect and access the TEW-692GRup to 450Mbps. Although the wireless n operates in the 2.4GHz frequency, this mode will only permit wireless n client devices to work and will exclude any other wireless mode and devices that are not wireless n only. 2.4 GHz 802.11b/g/n mixed mode - This wireless mode works in the 2.*

4GHz frequency range and will only allow the use of wireless g client devices to connect and access the TEW-692GRat 11Mbps for wireless b, 54Mbps for wireless g and up to 450Mbps for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.*

*Maximum wireless signal rates are referenced from IEEE 802.

11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions. @@This name is also referred to as the SSID. @@@@@@@@@@@@@@@@A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. @@You can add up to four additional devices in the spaces provided.

@@ 21 (Note: WDS supports wireless g/n modes. @@@@Channel BandWidth: Set channel width of wireless radio. @@Long Guard Interval, 800 nsec Short Guard Interval, 400 nsec MCS: Fix MCS rate for HT rate (0-15). The Modulation and Coding Scheme (MCS) is a value that determines the modulation, coding and number of spatial channels. 22 ADVANCED 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. @@@@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. 23 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. TX Power: Allows the wireless Router to deliver better throughput in the same period and environment in order to increase speed. Higher power output delivers better throughput SECURITY 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 24 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. 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. WPA/WPA2 mixed environment: For those WPA2 stations, they will use AES for unicast. For those WPA stations, they will use TKIP for unicast. But for multicast all WPA and WPA2 stations have to use the same key, and that will be TKIP, because WPA station only knows about TKIP, WPA2 is new standard, so it is defined to backward support TKIP on multicast.

25 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. The rule of thumb: In mixed mode, multicast key has to be TKIP, but unicast key can be different per stations. In WPA or WPA2 only mode, unicast and multicast key can be only AES for WPA2, and TKIP for WPA. (AES means the unicast and multicast key are all AES.

TKIP/AES means multicast is TKIP.

But unicast can be AES or TKIP, which depends on the peer.) WPS 26 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. PBC Settings: The push button method can be used to allow wireless clients to connect to the router without entering/remember any encryption keys.

The user can use the PBC method by pressing the WPS button on the side of the router or select the PBC option under Wireless/WPS settings page and hit Apply. STATION LIST All the wireless clients connecting to the router will be shown here, you could monitor your network and prevent any unauthorized wireless connection easily. 27 Wireless 5GHz BASIC 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 wireless mode. If you have some devices that use a different transmission mode, choose the appropriate wireless mode. The TEW-692GRsupports 5GHz wireless networks. There are many different configuration options available to choose from. Use the drop down list to select the wireless mode. Note: One wireless mode can be selected can select at any one time. This means that you can only select one of the operating frequencies at a time. 28 Wireless Mode options: 5GHz 802.11a only mode - This wireless mode works in the 5GHz frequency range and will allow wireless a client to connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router at 54Mbps for wireless a only mode. Although the wireless a operates in the 5GHz frequency, this mode will only permit wireless a client devices to work and will exclude any other wireless mode and devices that are not wireless a only.

5GHz 802.11a/n mixed mode - This wireless mode works in the 5GHz frequency range and will only allow the use of wireless a/n dual band client devices to connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router up to 450Mbps*. Dual band wireless client devices that support both wireless a/n can connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router up to 450Mbps. Wireless a client devices can connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router but, will only connect up to 54Mbps, (this due to the legacy limitation of wireless a technology for that standard). Although the wireless a/n operate in the same 5GHz frequency, this mode will only permit wireless a/n client devices to work and will exclude any other wireless mode and devices that are not wireless a/n. (note: wireless b/g/n will not be able to connect at the same time to the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router with 5GHz wireless a/n mode enable). @@This name is also referred to as the SSID. @@@@@@This name is also referred to as the SSID. @@@@@@@@@@@@@@@@@@@You can add up to four additional devices in the spaces provided. @@@@(Note: WDS supports wireless g/n modes.

@@@@Channel BandWidth: Set channel width of wireless radio. @@@@Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds. @@@@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. TX Burst: Allows the wireless Router to deliver better throughput in the same period and environment in order to increase speed. 31 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. SECURITY 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 32 (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. 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. WPA/WPA2 mixed environment: For those WPA2 stations, they will use AES for unicast. For those WPA stations, they will use TKIP for unicast. But for multicast all WPA and WPA2 stations have to use the same key, and that will be TKIP, because WPA station only knows about TKIP, WPA2 is new standard, so it is defined to backward support TKIP on multicast. 33 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. The rule of thumb: In mixed mode, multicast key has to be TKIP, but unicast key can be different per stations. In WPA or WPA2 only mode, unicast and multicast key can be only AES for WPA2, and TKIP for WPA. (AES means the unicast and multicast key are all AES.

TKIP/AES means multicast is TKIP. But unicast can be AES or TKIP, which depends on the peer.) 34 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.

35 PBC Settings: The push button method can be used to allow wireless clients to connect to the router without entering/remember any encryption keys. The user can use the PBC method by pressing the WPS button on the side of the router or select the PBC option under Wireless/WPS settings page and hit Apply. STATION LIST All the wireless clients connecting to the router will be shown here, you could monitor your network and prevent any unauthorized wireless connection easily. 36 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. 37 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 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. DMZ IP Address Specify the LAN IP address of the LAN computer that you want to have unrestricted Internet communication. 38 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.

168.10.50. 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. 39 ROUTING 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. 40 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.

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. 41 ALG ALG (Application level gateway): It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, SIP, RTSP, file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria. 42 SPECIAL APPLICATIONS 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. 43 GAMING 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 192.168.10.50. 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. 44 INBOUND FILTER 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.) 45 SCHEDULE 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. 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. 46 ADVANCED NETWORK UPnP: By default, the UPnP feature is enabled. Universal Plug and Play (UPnP) is a set of networking protocols for primarily residential networks without enterprise class devices that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. WAN Ping: By default, the WAN Ping Respond feature is disabled. Enable WAN Ping Respond will reply information of router to outside network.

47 Administrator MANAGEMENT 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. 48 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.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. UPLOAD FIRMWARE Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the router. 49 SETTING MANAGEMENT Export Settings: This option allows you to export and then save the router's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade. Import Settings: Use this option to restore previously saved router configuration settings. Load Factory Defaults: This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost.

If you want to save your router configuration settings, use the Export Settings option above. System Reboot: This restarts the router. It is useful for restarting when you are not near the device. 50 TIME 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. 51 STATUS The section displays the current status of the router. 52 Help Help section provides web-based explanations on each configurable field. 53 Appendix 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 SETTTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.