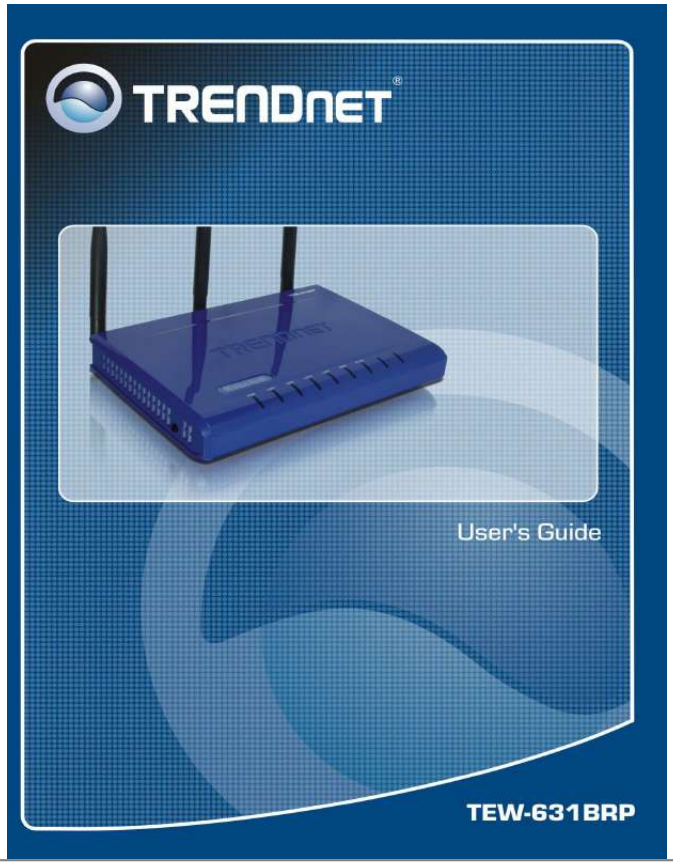

Manual abstract:

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. 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. TRENDnet declares that TEW-631BRP (FCC ID: S9ZTEW631BRP) is limited in CH1~CH11 for 2.

4 GHz by specified firmware controlled in U.S.A. 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. 2 Table of Contents Getting Started with the TEW-631BRP Package Contents Minimum System Requirements Wireless LAN Networking Introduction Features Hardware Overview Rear Panel LEDs Installation Considerations Getting Started Using the Configuration Menu Basic Advanced Tools Status Glossary 4 5 5 6 9 9 10 10 11 12 12 13 14 24 55 69 80 Note: Always run the CD and follow the steps in the Quick Installation Guide to setup your router. If you still have problems after doing so then proceed to the User's Guide to install the router with web-based configuration. 3 Getting Started with the TEW-631BRP Congratulations on purchasing the TEW-631BRP! This manual provides information for setting up and configuring the TEW-631BRP. 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 AND TIPS, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVERLOOKED. 4 Package Contents TEW-631BRP 11n(Draft) Wireless Router CAT-5 Ethernet Cable Power Adapter User's Guide CD-ROM Multi-Language 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. 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 5 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. Transmission Rate (Transfer Rate) The TEW-631BRP 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 TEW-631BRP to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the TEW-631BRP 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 TEW-631BRP 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.

6 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. 7 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 8 Introduction The TEW-631BRP 11n (Draft) Wireless Router is a high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places. Unlike most routers, the TEW-631BRP 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.

Features Wi-Fi Compliant with IEEE 802.11n (draft) and IEEEE 802.11b/g Standards 2.412 to 2.484GHz frequency band operation Compliant with IEEE 802.3 & 3u 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 or BigPond Connection Types Firewall features Network Address Translation (NAT), and Stateful Packet Inspection (SPI) protects against Dos attacks Traffic Control with Virtual Server (max 64 configurable servers) and DMZ UPnP (Universal Plug & Play) and ALGs Support for Internet applications such as Email, FTP, Gaming, Remote Desktop, Net Meeting, Telnet, and more Provides Additional Security of Enable/Disable SSID, Internet Access Control (Services, URL and MAC Filtering) Supports Multiple and Concurrent 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(for 11b/g), WPA/WPA2, and WPA-PSK/WPA2-PSK Compliant with Windows 98/NT/2000/XP/2003 Server/Vista, Linux and Mac OS Support 4 x 10/100Mbps Auto-MDIX LAN Port and 1 x 10/100Mbps WAN Port (Internet) 3 External Fixed Antennas to support high speed performance and great coverage 9 Hardware Overview Real Panel DC-IN The DC power input connector is a single jack socket to supply power to the TEW-631BRP. Please use the Power Adapter provided on the TEW-631BRP package.

Reset Button Pressing the reset button restores the router to its original factory default settings. WLAN Slide Switch To turn wireless function ON/OFF Auto MDI/MDIX WAN Port This is the connection for the Ethernet cable to the Cable or DSL modem Auto MDI/MDIX LAN Ports These ports automatically sense the cable type when connecting to Ethernet-enabled computers. 10 LEDs PWR/SYS LED Solid lights indicate a proper connection to the power supply, and indicate the system ready or not. LAN LEDs Solid lights indicate connections to Ethernet-enabled computers on ports 1-4. LED blinks during data transmission.

WAN LED A solid light indicates connection on the WAN port. This LED blinks during data transmission. WLAN LED A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission. WPS Button Enable the PBC WPS configuration.

The router and the client adapters both require to have WPS support to use this feature . 11 Installation Considerations The TEW-631BRP 11n (Draft) Wireless 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 TEW-631BRP 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. 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 Getting Started For a typical wireless setup at home, please do the following: 1. 2. 3. 4. You will need broadband Internet access (a Cable or DSL-subscriber line into your home or office) Consult with your Cable or DSL provider for proper installation of the modem. Connect the Cable or DSL modem to the TEW-631BRP Wireless Broadband Router (WAN port).

Ethernet LAN ports of the TEW-631BRP are Auto-MDIX and will work with both Straight-Through and Cross-Over cable. 12 Using the Configuration Menu Whenever you want to configure your TEW-631BRP, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the TEW-631BRP. The TEW-631BRP'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-631BRP, m 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 16 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. Example: 64-bit hexadecimal keys are exactly 10 characters in length.

(12345678FA is a valid string of 10 characters for 64-bit encryption.) 128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.) 64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.) 128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.) Note that, if you enter fewer characters in the WEP key than required, the remainder of the key is automatically padded with zeros. 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 "WPA or WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. The strongest cipher that the client supports will be used. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

If the clients support the AES cipher, it will be used across the wireless network to ensure best security.
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.
Example: Wireless Networking technology enables ubiquitous communication 17 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. MAC Address Authentication: If this is selected, the user must connect from the same computer whenever logging into the wireless network. Advanced: Optional Backup RADIUS Server This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server.

The second RADIUS server is consulted only when the primary server is not available or not responding. The fields Second RADIUS Server IP Address, RADIUS Server Port, Second RADIUS server Shared Secret, Second MAC Address Authentication provide the corresponding parameters for the second RADIUS Server. 18 Basic_Network Settings Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again. WAN Port Mode This option controls how the device reacts to traffic on the WAN connector. In this case the Term "port" refers to the Ethernet connectors on the device. Router Mode Select this option if the WAN port is connected to the Internet, the device functions as a NAT router. Bridge Mode Select this option if the device is connected to a local network downstream from another router. In this mode, the device functions as a bridge between the network on its WAN port and the 19 Devices on its LAN port and those connected wirelessly.
The Router IP Address field below must be set to the IP address of this device. The Gateway must be set to the IP address of the upstream router. Both addresses must be within the LAN subnet as specified by Subnet Mask. Router Settings These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section.
The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network. IP Address The IP address of your router on the local area network. Your local area network settings are based on the address assigned here. For example, 192.
168.0.1. Subnet Mask The subnet mask of your router on the local area network. Local Domain Name This entry is optional. Enter a domain name for the local network. The router's DHCP server will give this domain name to the computers on the wireless LAN. So, for example, if you enter mynetwork.net here, and you have a wireless laptop with a name of chris, that laptop will be known as chris.mynetwork.

net. Note, however, if the router's settings specify "DHCP (Dynamic)" Address, and the router's DHCP server assigns a domain name to the AP, that domain name will override any name you enter here. DNS Relay When DNS Relay is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server. RIP (Routing Information Protocol) Used to broadcast routing information among routers. Enable RIP Enable RIP if required by the ISP, if the LAN has multiple routers, or if the LAN has auto-IP devices. RIP Operating mode This router supports both version 2 and version 1 of the RIP specification. V1.
Use if none of the routers supports Version 2. V2 Broadcast. Use if some routers are capable of Version 2, but some are only capable of Version 1. V2 Multicast. Use if this is the only router on the LAN or if all the routers support Version 2.
20 Router Metric The additional cost of routing a packet through this router. The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes. Act as default router Make this router the preferred destination for packets that are not otherwise destined. Allow RIP updates from WAN For security, disable this option unless required by the ISP.
RIP Password RIP Version 2 supports the use of a password to limit access to routers through the RIP protocol. If the ISP or other LAN router requires a RIP password, enter the password here. 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 (from and to) 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 (see Static DHCP Client below), 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. Example: Your router uses 192.168.
10.1 for the IP address. You've assigned a computer that you want to designate as a Web server with a static IP address of 192.168.10.
3. You've assigned another computer that you want to designate as an FTP server with a static IP address of 192.168.10.4. Therefore the starting IP address for your DHCP IP address range needs to be 192.168.10.5 or greater. 21 Example: Suppose you configure the DHCP Server to manage addresses From 192.

168.10.101 To 192.168.10.200. This means that 192.168.10.2 to 192.
168.10.100 and 192.168.10.
201 to 192.168.10.254 is NOT managed by the DHCP Server. Computers or devices that use addresses from these ranges are to be manually configured. Suppose you have a web server computer that has a manually configured address of 192.168.10.150. Because this falls within the "managed range" be sure to create a reservation for this address and match it to the relevant computer (see Static DHCP Client below). 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.

22 Always Broadcast If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN. 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. As an alternative, you can locate a MAC address in a specific operating system by following the steps below: Windows 98 Windows Me Go to the Start menu, select Run, type in winipcfg, and hit Enter. A popup window will be displayed. Select the appropriate adapter from the pull-down menu and you will see the Adapter Address.
This is the MAC address of the device. Go to your Start menu, select Programs, select Accessories, and select Command Prompt. At the command prompt type ipconfig /all and hit Enter. The physical address displayed for the adapter connecting to the router is the MAC address. Go to the Apple Menu, select System Preferences, select Network, and select the Ethernet Adapter connecting to the router. Select the Ethernet button and the Ethernet ID will be listed. This is the same as the MAC address. Windows 2000 Windows XP Windows Vista Mac OS X 23 DHCP Reservations List This shows clients that you have specified to have reserved DHCP addresses. An entry can be changed by clicking the Edit icon, or 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.

Number of Dynamic DHCP Clients In this section you can see what LAN devices are currently leasing IP addresses. Revoke The Revoke option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed. Clicking Revoke cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network. Reserve The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List. 24 Advanced The Advanced tab provides the following configuration options: Virtual Server, Special Applications, Gaming, StreamEngine, Routing, Access Control, WEB Filter, MAC Address Filter, Firewall, Inbound Filter, Advanced Wireless and Advanced Network. Advanced_Virtual Server The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port. Example: You are hosting a Web Server on a PC that has LAN IP Address of 192.
168.10.50 and your ISP is blocking Port 80. 1. Name the Virtual Server (for example: Web Server) 2.
Enter the IP Address of the machine on your LAN (for example: 192.168.10.50 3. Enter the Private Port as [80] 4.
Enter the Public Port as [8888] 25 5. Select the Protocol (for example TCP). 6. Ensure the schedule is set to Always 7. Click Save to add the settings to the Virtual Servers List 8. Repeat these steps for each Virtual Server Rule you wish to add. After the list is complete, click Save Settings at the top of the page.

With this Virtual Server entry, all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 192.168.10.

50. Virtual Server Parameters 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. Inbound Filter Select a filter that controls access as needed for this virtual server.

If you do not see the filter you need in the list of filters, go to the Advanced Inbound Filter screen and create a new filter. 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, go to the Tools Schedules screen and create a new schedule.

Add/Edit Virtual Server In this section you can add an entry to the Virtual Servers List below or edit an existing entry. Enable 26 Entries in the list can be either active (enabled) or inactive (disabled).

Save Saves the new or edited virtual server entry in the following list. When finished updating the virtual server entries, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. Virtual Servers List The section shows the currently defined virtual servers. A Virtual Server can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Virtual Server" section is activated for editing. You might have trouble accessing a virtual server using its public identity (WAN-side IP-address of the gateway or its dynamic DNS name) from a machine on the LAN. Your requests may not be looped back or you may be redirected to the "Forbidden" page. This will happen if you have an Access Control Rule configured for this LAN machine. The requests from the LAN machine will not be looped back if Internet access is blocked at the time of access. To work around this problem, access the LAN machine using its LAN-side identity.

Requests may be redirected to the "Forbidden" page if web access for the LAN machine is restricted by an Access Control Rule. Add the WAN-side identity (WAN-side IP-address of the router or its dynamic DNS name) on the Advanced Web Filter screen to work around this problem. 27 Advanced_Special Applications An application rule is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. An application rule applies to all computers on your internal network. Parameters for an Application Rule Example: You need to configure your router to allow a software application running on any computer on your network to connect to a web-based server or another user on the Internet. 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. Application Instead of entering a name for the Special Application rule, you can select from this list of common applications, and the remaining configuration values will be filled in accordingly. Trigger Port Range Enter the outgoing port range used by your application (for example 6500-6700). Trigger Protocol Select the outbound protocol used by your application (for example Both).

28 Input Port Range Enter the port range that you want to open up to Internet traffic (for example 6000-6200). Input Protocol Select the protocol used by the Internet traffic coming back into the router through the opened port range (for example Both). Schedule Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools Schedules screen and create a new schedule. With the above example application rule enabled, the router will open up a range of ports from 6000-6200 for incoming traffic from the Internet, whenever any computer on the internal network opens up an application that sends data to the Internet using a port in the range of 6500-6700.

Add/Edit Special Applications Rule This section is where you define and edit Special Applications Rules. Save Saves the new or edited Special Applications Rule in the following list. When finished updating the special applications rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. Special Applications Rules List The section shows the currently defined special applications rules. A special applications rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon.

When you click the Edit icon, the item is highlighted, and the "Edit Special Applications Rule" section is activated for editing. 29 Advanced_Gaming Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. You can enter ports in various formats: Range (50-100) Individual (80, 68, 888) Mixed (1020-5000, 689) Example: Suppose you are hosting an online game server that is running on a PC with a private IP Address of 192.168.10.50. This game requires that you open multiple ports (6159-6180, 99) on the router so Internet users can connect. 30 Port Forwarding Fields 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. 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. If you do not see the filter you need in the list of filters, go to the Advanced Inbound Filter screen and create a new filter.

Schedule Select a schedule for the times when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools Schedules screen and create a new schedule. With the above example values filled in and this Gaming Rule enabled, all TCP and UDP traffic on ports 6159 through 6180 and port 99 is passed through the router and redirected to the Internal Private IP Address of your Game Server at 192.168.10.

50. Edit/Add Game Rule Here you can add entries to the Game Rules List below, or edit existing entries. Enable Each entry in Game Rules List can be active (enabled) or inactive (disabled) Save Saves the new or edited Game Rule in the following list. When finished updating the game rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. Game Rules List The section shows the currently defined game rules. A game rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Game Rule" section is activated for editing. 31 Advanced_StreamEngine The StreamEngine feature helps improve your network gaming performance by prioritizing the data flows of network applications. StreamEngine Setup Enable StreamEngine Enable this option for better performance and experience with online games and other interactive applications, such as VoIP. Automatic Classification This option is enabled by default so that your router will automatically determine which programs should have network priority. 32 Dynamic Fragmentation This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets. Automatic Uplink Speed When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example). Measured Uplink Speed This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network.

Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections. Manual Uplink Speed If Automatic Uplink Speed is disabled, this options allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISPs often specify speed as a downlink/uplink pair; for example, 1.5Mbps/284kbps. For this example, you would enter "284". Alternatively you can test your uplink speed with a service such as www.dslreports.com. Note however that sites such as DSL Reports, because they do not consider as many network protocol overheads, will generally note speeds slightly lower than the Measured Uplink Speed or the ISP rated speed. Connection Type By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the WAN settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results. Detected xDSL or Frame Relay Network When Connection Type is set to Auto-detect, the automatically detected connection type is displayed here.

StreamEngine Rules A StreamEngine Rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate, and specific StreamEngine Rules will not be required. Conflicting rules are not permitted. Conflicting rules are those that share any combination of source address/port, destination address/port, and protocol. Rejecting conflicting rules ensures that every flow defined in a rule receives the expected priority and avoids indeterminate prioritization that could reduce QoS effectiveness.

33 Name Create a name for the rule that is meaningful to you. Priority The priority of the message flow is entered here -- 1 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent). Priority 0 is reserved. Flows that are not prioritized by any rule receive lowest priority. Protocol The protocol used by the messages. The common choices can be selected from the drop-down menu. To specify any other protocol, enter its protocol number (as assigned by the IANA) in the Protocol box. Source IP Range The rule applies to a flow of messages whose LAN-side IP address falls within the range set here. Source Port Range The rule applies to a flow of messages whose LAN-side port number is within the range set here. Destination IP Range The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.

Destination Port Range The rule applies to a flow of messages whose WAN-side port number is within the range set here. Add/Edit StreamEngine Rule Enable Each entry in StreamEngine Rules List can be active (enabled) or inactive (disabled) Save Saves the new or edited StreamEngine Rule in the following list. When finished updating the StreamEngine rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. StreamEngine Rules List The section shows the currently defined StreamEngine rules. A StreamEngine rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit StreamEngine Rule" section is activated for editing. 34 Advanced_Routing Add/Edit Route Adds a new route to the IP routing table or edits an existing route. Enable: Specifies whether the entry will be enabled or disabled. Destination IP: The IP address of packets that will take this route. Netmask: One bits in the mask specify which bits of the IP address must match.

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.

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

Save: Saves the new or edited route in the following list. When finished updating the routing table, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. 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 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. 35 Advanced_Access Control The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games. Enable By default, the Access Control feature is disabled. If you need Access Control, check this option.

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. Policy Wizard The Policy Wizard guides you through the steps of defining each access control policy. A policy is the "Who, What, When, and How" of access control -- whose computer will be affected by the control, what internet addresses are controlled, when will the control be in effect, and how is the control implemented. You can define multiple policies. The Policy Wizard starts when you click the button below and also when you edit an existing policy. Add Policy Click this button to start creating a new access control policy. Policy Table This section shows the currently defined access control policies. A policy can be changed by clicking the Edit icon, or deleted by clicking the Delete icon.

When you click the Edit icon, the Policy Wizard starts and guides you through the process of changing a policy. You can enable or disable specific policies in the list by clicking the "Enable" checkbox. 36 Advanced_WEB Filter This section is where you add the Web sites to be used for Access Control. The Web sites listed here are used when the Web Filter option is enabled in Access Control. The Web Filter section is one of two means by which you can specify the web sites you want to allow.

Web Filter Parameters Web Site Enter the address of the web site that you want to allow; for example: trendnet.com. Do not enter the http:// preceding the address. Enter the most inclusive domain; for example, enter t and access will be permitted to both www.trendnet.

com and support.trendnet.com. Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all the web sites used to construct a page. For example, to access my.yahoo.com, you need to enable access to yahoo.com, yimg.com, and doubleclick.

net. 37 Add/Edit Web Site This is where you can add Web sites to the Allowed Web Site List or change entries in the Allowed Web Site List. Enable Entries in the Allowed Web Site List can be activated or deactivated with this checkbox. New entries are activated by default. Save Saves the new or edited Allowed Web Site in the following list. When finished updating the Allowed Web Site List, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. Allowed Web Site List The section lists the currently allowed web sites. An allowed web site can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Web Site" section is activated for editing. 38 Advanced_MAC Address Filter The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s).

It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter. Enable MAC Address Filter When this is enabled, computers are granted or denied network access depending on the mode of the filter. Misconfiguration of this feature can prevent any machine from accessing the network. In such a situation, you can regain access by activating the factory defaults button on the router itself.

Filter Settings Mode When "only allow listed machines" is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When "only deny listed machines" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network. 39 Filter Wireless Clients When this is selected, the MAC address filters will be applied to wireless network clients. Filter Wired Clients When this is selected, the MAC address filters will be applied to wired network clients. Add/Edit MAC Address In this section, you can add entries to the MAC Address List below, or edit existing entries.

Enable MAC address entries can be activated or deactivated with this checkbox. MAC Address Enter the MAC address of the desired computer or connect to the router from the desired computer and click the Copy Your PC's MAC Address button. Save Saves the new or edited MAC Address entry in the following list. When finished updating the MAC Address List, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. MAC Address List The section lists the current MAC Address filters. A MAC Address entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit MAC Address" section is activated for editing. 40 Advanced_Firewall The router provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attackers. However, some network applications cannot run with a tight firewall.

Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.

See also Virtual Server, Port Forwarding, Application Rules, and UPnP for related options. 41 Firewall Settings Enable SPI SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol. When the protocol is TCP, SPI checks that packet sequence numbers are within the valid range for the session, discarding those packets that do not have valid sequence numbers. Whether SPI is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state. NAT Endpoint Filtering The NAT Endpoint Filtering options control how the router's NAT manages incoming connection requests to ports that are already being used.

@@@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 uses 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. DMZ IP Address Specify the LAN IP address of the LAN computer that you want to have unrestricted Internet communication. If this computer obtains its address automatically using DHCP, then you may want to make a static reservation on the Basic Network Settings page so 43 that the IP address of the DMZ computer does not change. Non-UDP/TCP/ICMP LAN Sessions When a LAN application that uses a protocol other than UDP, TCP, or ICMP initiates a session to the Internet, the router's NAT can track such a session, even though it does not recognize the protocol.

This feature is useful because it enables certain applications (most importantly a single VPN connection to a remote host) without the need for an ALG. Note that this feature does not apply to the DMZ host (if one is enabled). The DMZ host always handles these kinds of sessions. Enable Enabling this option (the default setting) enables single VPN connections to a remote host. (But, for multiple VPN connections, the appropriate VPN ALG must be used.) Disabling this option, however, only disables VPN if the appropriate VPN ALG is also disabled. Application Level Gateway (ALG) Configuration Here you can enable or disable ALGs. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the PPTP ALG is to increase VPN performance. Enabling the PPTP ALG also allows incoming VPN connections to a LAN side VPN server (refer to Virtual Server). IPSec (VPN) Allows multiple VPN clients to connect to their corporate networks using IPSec. Some VPN clients support traversal of IPSec through NAT. This option may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try disabling this option. Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

Note that L2TP VPN connections typically use IPSec to secure the connection. To achieve multiple VPN pass-through in this case, the IPSec ALG must be enabled. RTSP Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol. Windows/MSN Messenger Supports use on LAN computers of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) and MSN Messenger.

The SIP ALG must also be enabled when the Windows Messenger ALG is enabled. 44 FTP Allows FTP clients and servers to transfer data across NAT. Refer to the Advanced Virtual Server page if you want to host an FTP server. H.323 (Netmeeting) Allows H.

323 (specifically Microsoft Netmeeting) clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the Advanced Virtual Server page for information on how to set up a virtual server. SIP Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off. Wake-On-LAN This feature enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable. The WOL device must be defined as such on the Advanced Virtual Server page. The LAN IP address for the virtual server is typically set to the broadcast address 192.

168.10.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened. MMS Allows Windows Media Player, using MMS protocol, to receive streaming media from the internet. 45 Advanced_Inbound Filter When you use the Virtual Server, Gaming, or Remote Administration features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN to cyber attacks from the Internet. In these cases, you can use Inbound Filters to limit that exposure by specifying the IP addresses of internet hosts that you trust to access your LAN through the ports that you have opened.

You might, for example, only allow access to a game server on your home LAN from the computers of friends whom you have invited to play the games on that server. Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features.

Each filter can be used for several functions; for example a "Game Clan" filter might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time an "Admin" filter might only allows systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used. 46 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. Source 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.

Save Saves the new or edited Inbound Filter Rule in the following list. When finished updating the Inbound Filter Rules List, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. Inbound Filter Rules List The section lists the current Inbound Filter Rules. An Inbound Filter Rule can be changed by clicking the Edit icon, or 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.) 47 Advanced_Advanced Wireless Transmit Power Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area.

By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area. Beacon Period 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. RTS Threshold This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended. Fragmentation Threshold This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance. DTIM Interval 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. 48 Short GI 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. Extra Wireless Protection Extra protection for neighboring 11b wireless networks. Turn this option off to reduce the adverse effect of legacy wireless networks on 802.11ng performance. WDS Enable When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links.

Note that WDS is incompatible with WPA -- both features cannot be used at the same time. 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. Make sure the APs are configured with same channel number. WDS AP MAC Address Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP. Enter a MAC address for each of the other APs that you want to connect with WDS. 49 Advanced_Network UPnP UPnP is short for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This router has optional UPnP capability, and can work with other UPnP devices and software. Enable UPnP If you need to use the UPnP functionality, you can enable it here. WAN Ping Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

Enable WAN Ping Respond If you leave this option unchecked, you are causing the router to ignore ping commands for the public WAN IP address of the router. WAN Port Speed Normally, this is set to "auto". If you have trouble connecting to the WAN, try the other settings. Multicast Streams The router uses the IGMP protocol to support efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients. Enable Multicast Streams This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option. 50 Advanced_ WISH WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications. WISH Enable WISH Enable this option if you want to allow WISH to prioritize your traffic. Priority Classifiers HTTP Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

51 Windows Media Center Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360. Automatic When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority. Add/Edit WISH Rule A WISH Rule identifies a specific message flow and assigns a priority to that flow.