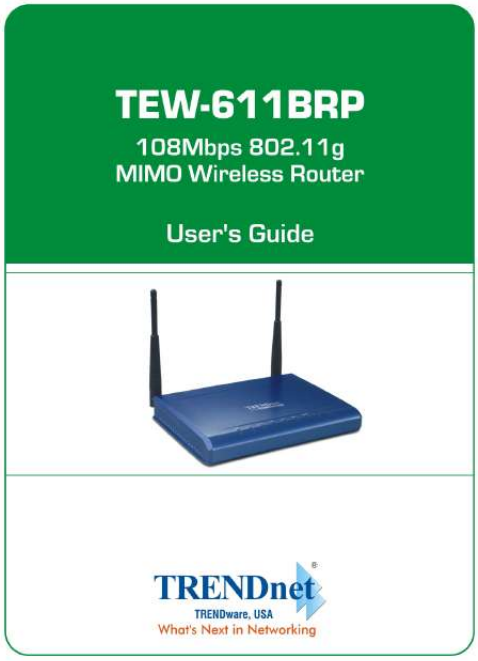

Manual abstract:

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. 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 2005 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-611BRP .

.....
.....

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

.....
65 3 Getting Started with the TEW-611BRP Congratulations on purchasing the TEW-611BRP! This manual provides information for setting up and configuring the TEW-611BRP. 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-611BRP 108Mbps 11g MIMO Wireless Router Power Adapter (5V DC, 2A) CD-ROM with Software and Manual Quick Installation Guide Cat.5 Ethernet Cable 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. 6 Introduction The TEW-611BRP MIMO Wireless Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places. Unlike most routers, the TEW-611BRP provides data transfers at up to 108 Mbps (compared to the standard 54Mbps) when used with other Super G MIMO products. The 802.11g standard is backwards compatible with 802.11b products.

This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11g's speed when you mix 802.11b and 802.11g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11b network. You may choose to slowly change your network by gradually replacing the 802.11b devices with 802.11g devices.
Features Wi-Fi Compliant with IEEE 802.11g and IEEE 802.11b Standards 4 x 10/100Mbps Auto-MDIX LAN Port and 1 x 10/100Mbps WAN Port (Internet) Supports Cable/DSL Modems with Dynamic IP, Static IP, PPPoE, PPTP, L2TP or BigPong Connection Types Supports Super G Technology with Data Rate up to 108Mbps (8X Faster) Enhance Wireless Coverage up to 800% More Coverage with MIMO Technology DHCP Server Feature Allocates up to 252 Client IP Addresses and up to 64 Reservations Supports 64/128-bit WEP(Hex), WPA/WPA2 & WPA-PSK/WPA2-PSK Encryptions 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 Static DHCP Client, Static Routing (RIP v1 Announcer) and Dynamic DNS (8 Verified Services) 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 Compliant with Windows 95/98/NT/2000/XP/2003 Server, Linux and Mac OS 7 Hardware Overview Real Panel DC-IN The DC power input connector is a single jack socket to supply power to the TEW-611BRP. Please use the Power Adapter provided on the TEW-611BRP package. Auto-MDIX LAN Ports These ports automatically sense the cable type when connecting to Ethernet-enabled computers.
Auto-MDIX WAN Port This is the connection for the Ethernet cable to the Cable or DSL modem WLAN Slide Switch Turn ON/OFF of wireless function. Reset Button Pressing the reset button restores the router to its original factory default settings. 8 LEDs POWER LED A solid light indicates a proper connection to the power supply. LAN1~LAN4 LED A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This 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. 9 Installation Considerations The TEW-611BRP MIMO 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-611BRP 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-611BRP Wireless Broadband Router (WAN port). Ethernet LAN ports of the TEW-611BRP are Auto-MDIX and will work with both Straight-Through and Cross-Over cable. 10 Using the Configuration Menu Whenever you want to configure your TEW-611BRP, you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the TEW-611BRP. The TEW-611BRP's default IP Address is http://192.168.0.1 Open the Web browser. Type in the IP Address of the Router (http://192. 168.0.1). If you have changed the default IP Address assigned to the TEW-611BRP, make sure to enter the correct IP Address. Type admin in the User Name field. Leave the Password blank. Click Login In. 11 Basic The Basic tab provides the following configuration options: Wizard, WAN, LAN, DHCP, and Wireless. Basic_Wizard Internet Connection Setup Wizard This wizard guides you through the following basic router setup steps: · · · Set your Password Select your Time Zone Configure your Internet Connection 12 Wireless Security Setup Wizard This wizard guides you through the following steps for setting up security for your wireless network: · · Name your Wireless Network Secure your Wireless Network Basic_WAN The WAN (Wide Area Network) section is where you configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond.

If you are unsure of your connection method, please contact your Internet Service Provider. Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled. 13 Static WAN Mode 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 WAN Mode A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the Internet. Host Name: Some ISP's may check your computer's Host Name. The Host Name identifies your system to the ISP's server.

This way they know your computer is eligible to receive an IP address. In other words, they know that you are paying for their service. Enable BigPond: Check this option to connect to the internet through Telstra BigPond Cable Broadband in Australia. Telstra BigPond provides the values for 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. WAN Port Speed: Normally, this is set to "auto". If you have trouble connecting to the WAN, try the other settings.

Respond to WAN Ping: If you leave this option unchecked, you are causing the public WAN 15 IP address of the router not to respond to ping commands. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid. WAN Ping Inbound Filter: Select a filter that controls access as needed for WAN pings. 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. MAC Cloning Enabled: Some ISP's may check your computer's MAC address. Each networking device has it's own unique MAC address defined by the hardware manufacturer. 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. Your new Wireless router has a different MAC address than the computer or router that initially connected to the ISP. To resolve this problem, the Wireless router has a special feature that allows you to clone (that is, replace the router's MAC address with) another MAC address.

MAC Address: If you have enabled MAC Cloning, you can 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 Wireless router using that computer and click the Clone Your PC's MAC Address button. The WAN port will then use the MAC address of the network adapter in your computer. 16 Basic_LAN 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. RIP Announcement. Used with multiple routers to broadcast routing information. Router Metric. The metric or cost of the routes advertised in RIP announcements.

17 Basic_DHCP 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 Wireless 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. 18 DHCP IP Address Range These two values (from and to) define a range of 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 Wireless router, by default, has a static IP address of 192.168.0.1. This means that addresses 192.168.0.2 to 192.168.0.
254 (from 2 to 254) can be made available for allocation by the DHCP Server. Example: Your Wireless router uses 192.168.0.1 for the IP address. You've assigned a computer that you want to designate as a Web server with a static IP address of 192.168.0.3. You've assigned another computer that you want to designate as an FTP server with a static IP address of 192.
168.0.4. Therefore the starting IP address for your DHCP IP address range needs to be 5 or greater. Example: Suppose you configure the DHCP Server to manage addresses From 100 To 199. This means that 3 to 99 and 200 to 254 are 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 192.168.0.

100. 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. 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.
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 19 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. Add/Edit Static DHCP Client 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 if a device has a static IP address except that it must still request an IP address from the Wireless router. The Wireless router will provide the device the same IP address every time. Static DHCP is 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. MAC Address: To input the MAC address of your system, enter it in manually or connect to the Wireless 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 Wireless 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 98SE 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 Wireless router. Select the Ethernet button and the Ethernet ID will be listed. This is the same as the MAC address. Windows 2000 Windows XP Mac OS X Computer Name: You can assign a name for each computer that is given a static IP address. This may help you keep track of which computers are assigned this way. Example: Game Server Static DHCP Client List This shows clients that you have specified to have static DHCP address. 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 Static DHCP Client" section is activated for editing. 20 Basic_Wireless The wireless section is used to configure the wireless settings for your Wireless router.
Please note that changes made on this section may also need to be duplicated on your Wireless Client. To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security.
WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server. Enable Wireless Radio This option turns off and on the wireless connection feature of the router.

When you set this option, the following parameters are displayed. 21 Wireless Network Name When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below).
This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Visibility Status The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network. Auto Channel Select If you select this option, the router automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the router uses the channel that you specify with the following Channel option. Channel A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients.

Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network. Transmission Rate By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. 802.11 Mode If all of your devices can connect in 802.11g Mode, you can change the mode to 802.11g only. If you have some devices that are 802.11b, leave the setting at Mixed.
Super GTM Mode Super G Turbo Modes must use channel 6 for communication. For Super G with Static Turbo, 802.11g Mode must be set to 802.11g. For proper operation, RTS threshold and Fragmentation Threshold on the Advanced -> Advanced Wireless screen should both be set to their default values. Super G without Turbo: Performance enhancing features such as Packet Bursting, Fast Frames, and Compression. Super G with Static Turbo: This mode is not backwards compatible with non-Turbo (legacy) devices. This mode should only be enabled when all devices on the wireless network are Static Turbo enabled. Super G with Dynamic Turbo: This mode is backwards compatible with non-Turbo (legacy) devices. This mode should be enabled when some devices on the wireless network are not Turbo enabled but support other Super G features mentioned above.
22 WEP A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

Four keys can be defined so that you can change keys easily. A default key is selected for use on the network. 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.) 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 23 to generate session keys that are unique for each wireless client. Example: Wireless Networking technology enables ubiquitous communication 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. 24 Advanced The Advanced tab provides the following configuration options: Virtual Server, Special Applications, Gaming, Traffic Shaping, Routing, Access Control, WEB Filter, MAC Address Filter, Firewall, Inbound Filter, Advanced Wireless and Schedules.

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 192.168.0.50 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: 192.168.0.50 3. Enter the Private Port as [80] 4. Enter the Public Port as [8888] 25 5. Select the Protocol - 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 192.168.0.

50. Add/Edit Virtual Server In this section you can add an entry to the Vertual Servers List below or edit an existing entry. Enable Entries in the list can be either active (enabled) or inactive (disabled). Name Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the "Select Virtual Server" list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server. IP Address The IP address of the system on your internal network that will provide the virtual service, for example 192.168.0.50. Protocol Select the protocol used by the service. 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. Save Saves the new or edited virtual server entry in the following list. When finished updating the 26 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. Note: 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. Advanced_Special Applications 27 Application Level Gateway (ALG) Configurations 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 network using PPTP protocol. IPSec VPN Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system adminstrator of your corporate network whether your VPN client supports NAT traversal. 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 Messenger Supports use of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) on LAN computers. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled. 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. NetMeeting Allows 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 28 192.168.0.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened. AOL Use this ALG if you are experiencing frequent disconnects from the AOL server due to inactivity.

MMS Allows Windows Media Player, using MMS protocol, to receive streaming media from the internet. L2TP Allows multiple machines on the LAN to connect to their corporate network using the L2TP protocol. Add/Edit Special Applications Rule The Special Application section 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. Special Applications rules apply to all computers on your internal network. 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.

You can also select from a 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. [6500-6700] Trigger Protocol Select the outbound protocol used by your application. [Both] Input Port Range Enter the port range that you want to open up to Internet traffic.
[6000-6200] Input Protocol Select the protocol used by the Internet traffic coming back into the router through the opened port range. [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. Save 29 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.
With this Special 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. 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. 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). The Gaming 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. This feature allows you to enter ports in various formats: Range (50-100) Individual (80, 68, 888) Mixed (1020-5000, 689) 30 Edit/Add Game Rule Here you can add entries to the Game Rules List below, or edit existing entries. Example: You are hosting an online game server that is running on a PC with a Private IP Address of 192.168.0.50. This game requires that you open multiple ports (6159-6180, 99) on the router so Internet users can connect. Enable Each entry in Game Rules List can be active (enabled) or inactive (disabled) Name Give the Gaming 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 game server, for example 192.168.0.50. TCP Ports To Open / UDP Ports To Open Enter the TCP ports to open. [6159-6180, 99] / Enter the UDP ports to open. [6159-6180, 99] Inbound Filter Select a filter that controls access as needed for this game 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. 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. With 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.
0.50. 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_Traffic Shaping The Traffic ShapingTM feature helps improve your network gaming performance by prioritizing applications. By default, the Traffic Shaping settings are disabled. 32 Traffic Shaping Setup Enable Traffic Shaping This option is disabled by default. Enable it 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. 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. 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, 1.5Mbits/284Kbits. For this example, you would enter "284". Alternatively you can test your uplink speed with a service such as www.dslreports.com.
@@@@@@@@@@@@@@@@Priority The priority of the message flow is entered here. @@Protocol The protocol used by the messages.
@@@@@@@@@@@@@@@@@@@@@@@@Enable: Specifies whether the entry will be enabled or disabled. 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.
@@@@Metric: The relative cost of using this route. 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, and you will see the following configuration sections. Note: Once you enabled the Access Control, you would need to have a rule for all the devices on the network. For example, every device on the LAN that needs to access the internet must have an Access Control rule permits it to access the Internet. Device that do not have the rule cannot access the Internet. 36 Add/Edit Access Control Rule Access Control Rules specify what a LAN device is allowed to access.

Here you can add entries to the Access Control Rules List or edit existing entries. Enable Each entry in Access Control Rules List can be active (enabled) or inactive (disabled) Policy Name Create a name for this access control policy (rule) that is meaningful to you. Typically this would be a system name or user name; for example "Casey's PC". Address Type Select the type of address on which you want to base the rule. IP Address: Enter the IP Address of the machine that you want the access control rule to apply to. Make sure that the device on the LAN either has a static IP address (that is, one that is not in the DHCP range) or is in the Static DHCP Client List (see Basic -> DHCP). Machine Address: Enter the MAC Address of the machine that you want the access control rule to apply to. If you want to enter the MAC Address of the computer you are using, click the Copy Your PC's MAC Address button. Others: If you want to restrict access for all devices that do not have an explicit rule configured for them, then select "Others" for the Address Type. Schedule Select a schedule of the times when you want the policy to apply.
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. Apply Web Filter With this option enabled, the specified system will only have access to the Web sites listed in the Web Filter section. Log Internet Access If this option is enabled, all of the Web sites visited by the specified machine will be logged. Filter Ports By clicking the Filter Ports >> button you can specify that the rule prohibits access to specific IP addresses and ports. Save Saves the new or edited access control rule in the following list.
Repeat the process, creating an Access Control Rule for each of the devices on your LAN that needs access to the Internet. When finished updating the Access Control Rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. 37 Access Control Rules List This section shows the current access control rules. Rules 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 Access Control Rule" section is activated for editing.
Advanced_WEB Filter The Web Filter section is where you add the Web sites to be used for Access Control. 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. The Allowed Web Site List is used for systems that have the Web filter option enabled in Access Control. Enable Entries in the Allowed Web Site List can be activated or deactivated with this checkbox. New entries are activated by default. Web Site Enter the URL (address) of the Web Site that you want to allow; for example: google.com. Do not enter the http:// preceding the URL. Enter the most inclusive domain; for example, enter dlink.com and access will be permitted to both www.

dlink.com and support.dlink.com. Note: 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 38 doubleclick.net. 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. 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. 39 Note: 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. 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 Enable SPI SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol.

When SPI is enabled, the extra state information will be reported on the Status -> Active Sessions page. Enable DMZ 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.
Note: 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 IP address of the computer on the LAN 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 -> DHCP page so that the IP address of the DMZ machine does not change. 41 Advanced_Inbound Filter The Inbound Filter option is an advanced method of controlling data received from the Internet.
With this feature you can configure inbound data filtering rules that control data based on IP Address. 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. 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. 42 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 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.) Advanced_Advanced Wireless 43 Fragmentation Threshold This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance. 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.
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. 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. 802.11d Enable Enables 802.
11d operation. 802.11d is a wireless specification for operation in additional regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains (countries). The current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement adds the requirements and definitions necessary to allow 802.11 WLAN equipment to operate in markets not served by the current standard.

Enable this option if you are operating in one of these "additional regulatory domains". 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. 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. 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. 44 Advanced_Schedules Schedules can be created for use with enforcing rules.
For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm. 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 triggered only by the start time. 45 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 used for email events. Save Saves the new or edited Schedule Rule in the following list. When finished updating the Schedule Rules, you must still click the button at the top of the page to make the changes effective and permanent. Schedule Rules List The section shows the currently defined Schedule Rules.

A Schedule 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 Schedule Rule" section is activated for editing. 46 Tools The Tools tab provides the following configuration options: Admin, Time, Syslog, Email, System, Firmware and Dynamic DNS. Tools_Admin The Admin option is used to set a password for access to the Web-based management. By default there is no password configured.

It is highly recommended that you create a password to keep your new router secure. 47 Admin Password Enter a password for the user "admin", who will have full access to the Web-based management interface. User Password Enter a password for the user "user", who will have read-only access to the Web-based management interface. Router Name The name of the router can be changed here. Enable Remote Management Enabling Remote Management allows you to manage the router from anywhere on the Internet. Disabling Remote Management allows you to manage the router only from computers on your LAN. Remote Admin Port The port that you will use to address the management interface from the Internet. For example, if you specify port 1080 here, then, to access the router from the Internet, you would use a URL of the form: http://my.domain.com:1080/.

Remote Admin Inbound Filter Select a filter that controls access as needed for this admin port. 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. Admin Idle Timeout The amount of time before the administration session (either remote or local) is closed when there is no activity. Save Configuration This option allows you to save the router's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

Restore Configuration from File Use this option to load previously saved router configuration settings. Save Configuration To Wireless Network Setup Wizard If your PC's operating system is Windows XP Service Pack 2 (SP2) or later and you are using Windows Internet Explorer (IE) as your browser, you can use this option to save key parts of the router's current wireless security settings to your PC with Windows Connect Now (WCN) technology. The settings will then be available to propagate to other wireless devices. WCN ActiveX Control The WCN ActiveX Control provides the necessary WCN link between the router and your PC via the browser. The browser will attempt to download the WCN ActiveX Control, if it is not already available on your PC.

For this action to succeed, the WAN connection must be established, and the browser's internet security setting must be Medium or lower (select Tools 48 -> Internet Options -> Security -> Custom Level -> Medium). Click the Save to Windows Connect Now button, and the WCN technology will capture the wireless network settings from your router and save them on your PC. Note that WCN only saves a few of the wireless security settings. When you use WCN to propagate settings to other wireless devices, you may have to make additional settings manually on those devices. Note that, in Microsoft's current implementation of WCN, you cannot save the wireless settings if a profile of the same name already exists. To work around this limitation, either delete the existing profile or change the SSID when you change the wireless settings; then, when you save the new settings, a new profile will be created. Tools_Time The Time Configuration option allows you to configure, update, and maintain the correct time on the router's internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight saving can also be configured to automatically adjust the time when needed. 49 Time Configuration Time Zone Select your local time zone from pull down menu.

Daylight Saving Enable Check this option if your location observes daylight saving time. Daylight Saving Offset Select the time offset, if your location observes daylight saving time. DST Start and DST End Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun" and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM." Automatic Time Configuration Enable NTP Server Select this option if you want the router's clock synchronized 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. NTP Server 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, or you can click the Copy Your Computer's Time Settings button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.) Note: If the router loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the router, or you must enable the NTP Server option. 50 Tools_Syslog This section allows you to archive your log files to a Syslog Server.

Enable Logging to Syslog Server Enable this option if you have a syslog server currently running on the LAN and wish to send log messages to it. Enabling this option causes the following parameter to be displayed. Syslog Server IP Address Enter the LAN IP address of the Syslog Server. 51 Tools_Email The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address. Enable Enable Email Notification When this option is enabled, router activity logs or firmware upgrade notifications can be emailed to a designated email address, and the following parameters are displayed.

Email Settings From Email Address This email address will appear as the sender when you receive a log file or firmware upgrade notification via email. To Email Address Enter the email address where you want the email sent. 52 SMTP Server Address Enter the SMTP server address for sending email. Enable Authentication If your SMTP server requires authentication, select this option. Account Name Enter your account for sending email. Password Enter the password associated with the account. Verify Password Re-type the password associated with the account. Email Log When Full or on Schedule On Log Full Select this option if you want logs to be sent by email when the log is full.