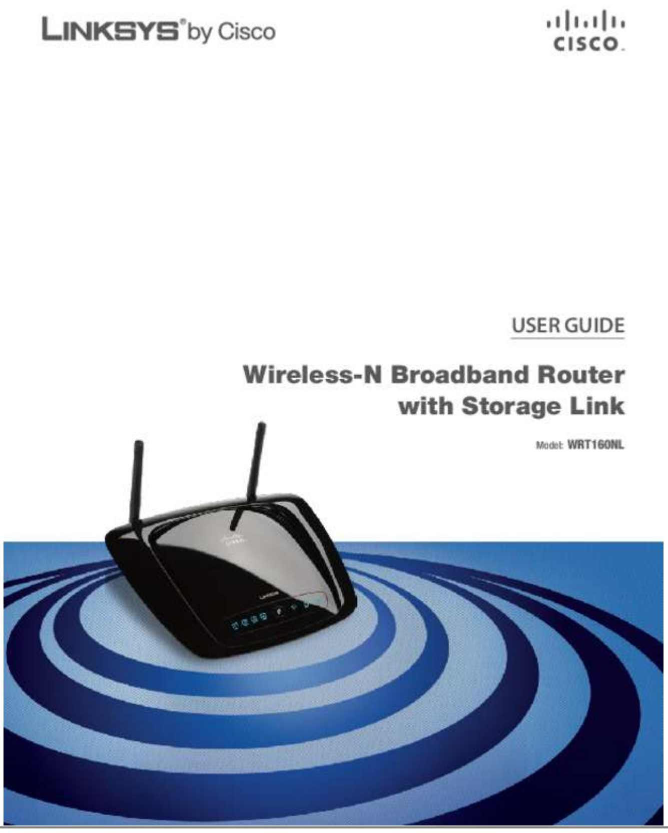

LINKSYS® by Cisco

CISCO

USER GUIDE

Wireless-N Broadband Router with Storage Link

Model: WRT160NL

Manual abstract:

If you use an older web browser, you may have to add http:// in front of the web address. Com/security Copyright and Trademarks Linksys, Cisco and the Cisco Logo are registered trademarks or trademarks of Cisco Systems, Inc. And/or its affiliates in the U. Other brands and product names are trademarks or registered trademarks of their respective holders. @@It flashes blue for two minutes during Wi-Fi Protected Setup. @@Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again. The LED flashes when a Wi-Fi Protected Setup session is active. the Router supports one session at a time. @@@@If the LED is flashing, the Router is sending or receiving data over the network.

Internet (Blue) The Internet LED lights up when there is a connection made through the Internet port. it flashes to indicate network activity over the Internet port. Power (Blue) The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit.

Chapter 1: Product Overview Thank you for choosing the Linksys by Cisco Wireless-N Broadband Router with Storage Link. The Router lets you access the Internet via a wireless connection or through one of its four switched ports. You can also use the Router to share resources such as computers, printers and files. The Router's USB port connects to a USB storage device, so you can access your portable files. (A USB hard drive may require an external power supply.

) A variety of security features help to protect your data and your privacy while you are online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall, and NAT technology. Configuring the Router is easy using the provided browser–based utility. Front Panel 1, 2, 3, 4 (Blue) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. a flashing LED indicates network activity over that port. Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network. To use Wi-Fi Protected Setup, run the Setup Wizard, or refer to Wi-Fi Protected Setup, page 11. Back Panel Antenna Ports The female R-SMA antenna ports connect to the male R-SMA connectors of the included antennas. Internet The Internet port is where you will connect your cable or DSL Internet connection.

4, 3, 2, 1 These Ethernet ports (4, 3, 2, 1) connect the Router to computers on your wired network and other Ethernet network devices. uSB Port The USB port connects to a USB storage device. If the storage device does not fit (for example, it may block port 1), then use the included USB extension cable. Power The Power port connects to the included power adapter. Wireless-N Broadband Router with Storage Link 1 Chapter 1 Product Overview Wall-Mounting Placement The Router has two wall-mount slots on its bottom panel. The distance between the slots is 152 mm (6 inches). Two screws are needed to mount the Router. 5 mm Reset The Reset button is located on the right side of the product label. There are two ways to reset the Router to its factory defaults. Either press and hold the Reset button for approximately five seconds, or restore the defaults from the Administration > Factory Defaults screen of the Router's web-based utility.

††Note: Mounting hardware illustrations are not true to scale. NOTE: Linksys is not responsible for damages incurred by insecure wall-mounting hardware. follow these instructions: 1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry and sturdy.

Also make sure the location is within reach of an electrical socket. 2. Drill two holes into the wall. Make sure the holes are 152 mm (6 inches) apart. 3. Insert a screw into each hole and leave 3 mm (0. Manoeuvre the Router so the wall-mount slots line up with the two screws. 5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots. Horizontal Placement The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical socket. 152 mm Print this page at 100% size. Cut along the dotted line, and place on the wall to drill precise spacing. Wall-Mounting Template Wireless-N Broadband Router with Storage Link 2 Chapter 2 Wireless Security Checklist Chapter 2: Wireless Security Checklist Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network.

Like signals from your mobile or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalent Privacy (WEP) offer different levels of security for wireless communication. A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment. WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA. 1. Change the default wireless network name or SSID Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network and can be up to 32 characters in length. Linksys wireless products use linksys as the default wireless network name.

You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your National Insurance number) because this information may be available for anyone to see when browsing for wireless networks. General Network Security Guidelines Wireless network security is useless if the underlying network is not secure. •Password protect all computers on the network and individually password protect sensitive files. Change the default password For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. the Linksys default password is admin.

Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorised changes, customise the device's password so it will be hard to guess. May open file sharing without your consent and/or knowledge. additional Security Tips •• Keep wireless routers , access points or gateways away from exterior walls and windows.

• Turn wireless routers, access points or gateways off when they are not being used (at night, during holidays). • Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary. WEB: For more information on wireless security, visit www. Enable MAC address filtering Linksys routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network. Wireless-N Broadband Router with Storage Link 3 Chapter 3 Advanced Configuration Chapter 3: Advanced Configuration After setting up the Router with the Setup Wizard (located on the CD-ROM), the Router will be ready for use. However, if you want to change its advanced settings, use the Router's web-based utility.

This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router. The web-based utility has these main tabs: Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration and Status. Additional tabs will be available after you click one of the main tabs. NOTE: When first installing the Router, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the web-based utility. Setup > Basic Setup Access the Web-Based Utility To access the web-based utility, launch the web browser on your computer and enter the Router's default IP address, 192. Leave the Username field blank. The first time you open the Web-based utility, use the default password admin. (You can set a new password from the Administration > Management screen.

) Click OK to continue. Language Select your language   To use a different language, select one from the drop-down menu. The language of the web-based utility will change five seconds after you select another language. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Internet Setup The Internet Setup section configures the Router to your Internet connection.

Most of this information can be obtained through your Internet Service Provider (ISP). Internet Connection Type Select the type of Internet connection your ISP provides from the drop-down menu. These are the available types: •• •• •• Login Screen •• •• Automatic Configuration - DHCP Static IP PPPoE PPTP L2TP Telstra Cable Setup > Basic Setup The first screen that appears is the Basic Setup screen. This allows you to change the Router's general settings. • Wireless-N Broadband Router with Storage Link 4 Chapter 3 Advanced Configuration Connect on Demand: Max Idle Time   You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time).

If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. to use this option , select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to elapse before your Internet connection terminates. the default Max Idle Time is 15 minutes. Keep Alive: Redial Period   If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. to use this option , select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. the default Redial Period is 30 seconds. Automatic Configuration - DHCP By default, the Router's Internet Connection Type is set to Automatic Configuratioou can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time).

If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. to use this option , select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to elapse before your Internet connection terminates. the default Max Idle Time is 15 minutes. Keep Alive: Redial Period   If you select this option, the Router will pstart with when issuing IP addresses. Because the Router's default IP address is 192. 1, the Start IP Address must be 192. Maximum Number of Users   Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. the default value is 50.

IP Address Range   Displayed here is the range of available IP addresses. Client Lease Time   The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the 7 DHCP Server Setting DHCP Server   DHCP is enabled by factory default. If you already have a DHCP server on your network or you do not want a DHCP server, then select Disabled (no other DHCP features will be available). wireless-N Broadband Router with Storage Link Chapter 3 Advanced Configuration DynDNS.

Org amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time has elapsed, the user will be automatically assigned a new dynamic IP address. The default setting is 0 minutes, which means one day. Static DNS 1-3   The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address.

If you wish to use another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers. WINS   The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank. Time Settings Time Zone   Select the time zone in which your network functions from this drop-down menu.

(You can even automatically adjust for daylight saving time). Setup > DDNS > DynDNS Username   Enter the Username for your DDNS account. Password   Enter the Password for your DDNS account.

Host Name   The is the DDNS URL assigned by the DDNS service. System   Select the DynDNS service you use: Dynamic, Static or Custom. the default selection is Dynamic. Mail Exchange (Optional)   Enter the address of your mail exchange server, so emails to your DynDNS address go to your mail server. backup MX   This feature allows the mail exchange server to be a backup. To disable this feature, keep the default setting of Disabled. to enable the feature , select Enabled. If you are not sure which setting to select, keep the default setting of Disabled. wildcard   This setting enables or disables wildcards for your host. For example, if your DDNS address is myplace.

dyndns. Org and you enable wildcards, then x. Org will work as well (x is the wildcard). If you are not sure which setting to select, keep the default setting of Disabled. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes.

Time Settings Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. setup > DDNS The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server or other server behind the Router. Before you can use this feature, you have to sign up for DDNS service with a DDNS service provider, www.

If you do not want to use this feature, keep the default setting of Disabled. If your DDNS service is provided by TZO, then select TZO. com. The features available on the DDNS screen will vary, depending on which DDNS service provider you use. Wireless-N Broadband Router with Storage Link 8 Chapter 3 Advanced Configuration Clone My PC's MAC   Click this button to clone the MAC address of the computer you are using. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. tZO. Com Setup > Advanced Routing This screen is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network.

Static Routing sets up a fixed route to another network destination. Setup > DDNS > TZO E-mail Address, TZO Key and Domain Name   Enter the settings of the account you set up with TZO. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Setup > MAC Address Clone A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature. Setup > Advanced Routing Advanced Routing NAT Enabled/Disabled   If this Router is hosting your network's connection to the Internet, keep the default setting of Enabled. If another router exists on your network, select Disabled. when the NAT setting is disabled , dynamic routing will be enabled. Dynamic Routing (RIP) Enabled/Disabled   This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s).

The Router determines the network packets' route based on the fewest number of hops between the source and the destination. When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this feature is available. MAC Address   Enter the MAC Address registered with your ISP here. Wireless-N Broadband Router with Storage Link Static Routing A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

Enter the information described below to set up a new static route. Route Entries   To set up a static route between the Router and another network, select a number from the dropdown list. click Delete This Entry to delete a static route. Enter Route Name   Enter a name for the Route here, using a maximum of 25 alphanumeric characters. Destination LAN IP   The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask   The Subnet Mask determines which portion of a Destination LAN IP address is the network portion and which portion is the host portion. Gateway   This is the IP address of the gateway device that allows for contact between the Router and the remote network or host. Interface   This interface tells you whether the Destination IP Address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet). Click Show Routing Table to view the static routes you have already set up. Basic Wireless Settings Wireless > Basic Wireless Settings (Manual Setup) Network Mode   From this drop-down menu, you can select the wireless standards running on your network. If you have Wireless-N, Wireless-G and Wireless-B devices in your network, keep the default setting of Mixed. If you have only Wireless-G and Wireless-B devices in your network, select BG-Mixed. If you have only Wireless-N devices, select Wireless-N Only. If you have only Wireless-G devices, select Wireless-G Only. If you have only Wireless-B devices, select Wireless-B Only.

If you do not have any wireless devices in your network, select Disabled. Network Name (SSID)   The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (linksys) to a unique name. channel Width   For best performance in a network using Wireless-N , Wireless-G and Wireless-B devices , select Wide - 40MHz Channel. For Wireless-G and Wireless-B networking only, keep the default setting of Standard 20MHz Channel. If you are not sure which option to use, select Auto. NOTE: If you select Wide - 40MHz Channel for the Channel Width setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary one (Standard Channel).

this will enhance Wireless-N performance. Wide Channel   If Wide - 40MHz Channel is the Channel Width setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu. If you are not sure which channel to select, keep the default setting of Auto. 10 Advanced Routing > Routing Table Routing Table For each route, the Destination LAN IP address, Subnet Mask, Gateway and Interface are displayed.

Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Wireless > Basic Wireless Settings The basic settings for wireless networking are set on this screen. There are two ways to configure the Router's wireless network(s), manual and Wi-Fi Protected Setup. Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

To use Wi-Fi Protected Setup, Wireless-N Broadband Router with Storage Link Chapter 3 Advanced Configuration Standard Channel   If Standard - 20 MHz Channel is the Channel Width setting, then this setting will be available. Select the appropriate channel for your wireless network. If you are not sure which channel to select, keep the default setting of Auto. If Wide - 40MHz Channel is the Channel Width setting, then the Standard Channel will be a secondary channel for Wireless-N (2. 4 GHz). If you selected a specific channel for the Wide Channel setting, then the Standard Channel options will vary. Select the appropriate channel for your wireless network. SSID Broadcast   When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting of Enabled. If you do not want to broadcast the Router's SSID, then select Disabled.

Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. wi-Fi Protected Setup Configured Wi-Fi Protected Setup There are three methods available. Use the method that applies to the client device you are configuring. nOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup. Method #1 Use this method if your client device has a Wi-Fi Protected Setup button. 1. Click or press the Wi-Fi Protected Setup button on the client device. 2. Click the Wi-Fi Protected Setup button on this screen. Then refer back to your client device or its documentation for further instructions. Wireless > Basic Wireless Settings (Wi-Fi Protected Setup) Wi-Fi Protected Setup > Congratulations Method #2 Use this method if your client device has a Wi-Fi Protected Setup PIN number. 1. Enter the PIN number in the field on this screen. Wireless-N Broadband Router with Storage Link 11 Chapter 3 Advanced Configuration WPA Personal NOTE: If you are using WPA, then each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.

Then refer back to your client device or its documentation for further instructions. Method #3 Use this method if your client device asks for the Router's PIN number. 1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router).

Then refer back to your client device or its documentation for further instructions. The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption and Passphrase are displayed at the bottom of the screen. NOTE: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings and then manually configure those client devices. Security Mode > WPA Personal Wireless > Wireless Security The Wireless Security screen configures the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service). These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to Chapter 2: Wireless Security Checklist, page 3. Encryption   WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys.

Key Renewal   Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. the default value is 3600 seconds. WPA2 Personal Wireless Security Security Mode Select the security method for your wireless network. If you do not want to use wireless security, keep the default setting of Disabled. Security Mode > WPA2 Personal Encryption   WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Key Renewal   Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. the default value is 3600 seconds. Wireless-N Broadband Router with Storage Link 12 Chapter 3 Advanced Configuration RADIUS Server   Enter the IP address of the server. RADIUS Port   Enter the port number of the server. the default value is 1812.

Shared Secret   Enter the key shared between the Router and the server. Key Renewal   Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. (This should only be used when a RADIUS server is connected to the Router). rADIUS This option features WEP used with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router).

IMPORTANT: If you are using WEP, then each device in your wireless network MUST use the same WEP encryption method and key, or else the network will not function properly. Security Mode > WPA Enterprise Encryption   WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. RADIUS Server   Enter the IP address of the server. RADIUS Port   Enter the port number of the server. the default value is 1812.

Shared Secret   Enter the key shared between the Router and the server. Key Renewal   Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. (This should only be used when a RADIUS server is connected to the Router). Security Mode > RADIUS RADIUS Server Enter the IP address of the server. RADIUS Port   Enter the port number of the server. the default value is 1812. Shared Secret   Enter the key shared between the Router and the server. Key 1-4   If you did not enter a Passphrase, enter the WEP key(s) manually. 13 Security Mode > WPA2 Enterprise Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Wireless-N Broadband Router with Storage Link Chapter 3 Advanced Configuration Wireless > Wireless MAC Filter Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network’s radius.

WEP WEP is a basic encryption method, which is not as secure as WPA. IMPORTANT: If you are using WEP encryption, then each device in your wireless network MUST use the same WEP encryption method and key, or else the network will not function properly.

Security Mode > WEP Encryption   Select a level of WEP encryption, 40/64 bits (10 hex digits) or 104/128 bits (26 hex digits). Key 1-4   If you did not enter a Passphrase, enter the WEP key(s) manually. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. wireless > Wireless MAC Filter Wireless MAC Filter Enabled/Disabled   To filter wireless users by MAC Address , either permitting or blocking access , select Enabled. If you do not wish to filter users by MAC Address, keep the default setting of Disabled. Access Restriction Prevent   Select this option to block wireless access by MAC Address. this button is selected by default. Permit   Select this option to allow wireless access by MAC Address.

This button is not selected by default. MAC Address Filter List Wireless Client List   Click this to open the Wireless Client List screen. Wireless-N Broadband Router with Storage Link 14 Chapter 3 Advanced Configuration with each other. The default is set to Auto, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication.

With Shared Key authentication, the sender and recipient use a WEP key for authentication. select Shared Key to only use Shared Key authentication. Basic Rate   The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. (The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

) The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is Default, when the Router can transmit at all standard wireless rates (1-2 Mbps, 5. 5 Mbps , 11 Mbps , 18 Mbps and 24Mbps). Select 1-2Mbps for use with older wireless technology. Select All, when the Router can transmit at all wireless rates. transmission Rate   The Transmission setting is available if the Network Mode is BG-Mixed , Wireless-G Only or Wireless-B Only. The rate of data transmission should be set depending on the speed of your wireless network. Select from a range of transmission speeds, or keep the default setting of Auto to have the Router automatically use the fastest possible data rate and enable the AutoFallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.

n Transmission Rate   The N Transmission setting is available if the Network Mode is Mixed or Wireless-N Only. The rate of data transmission should be set depending on the speed of your Wireless-N networking. Select from a range of transmission speeds, or keep the default setting of Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. CTS Protection Mode   The Router automatically uses CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G devices are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802. 11b traffic. This option boosts the Router's ability to catch all Wireless-N and Wireless-G transmissions but severely decreases performance. To use this option, keep the default setting of Auto. to disable this option , select Disabled. Wireless Client List Wireless Client List This screen shows computers and other devices on the wireless network.

The list can be sorted by Client Name, Interface, IP Address, MAC Address and Status. Select Save to MAC Address Filter List for any device you want to add to the MAC Address Filter List. To exit this screen and return to the Wireless MAC Filter screen, click Close. MAC 01-50   Enter the MAC addresses of the devices whose wireless access you want to block or allow. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Wireless > Advanced Wireless Settings This Advanced Wireless Settings screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance. Wireless > Advanced Wireless Settings Advanced Wireless AP Isolation   This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not Wireless-N Broadband Router with Storage Link 15 Chapter 3 Advanced Configuration Firewall SPI Firewall Protection   To use firewall protection, keep the default selection of Enabled. The Beacon Interval value indicates the frequency interval of the beacon.

A beacon is a packet broadcast by the Router to synchronise the wireless network. the default value is 100 milliseconds. DTIM Interval   This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. the default value is 1. Fragmentation Threshold   This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance.

Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346. RTS Threshold   Should you encounter inconsistent data flow, only a minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Internet Filter Filter Anonymous Internet Requests   This feature makes it more difficult for outside users to work their way into your network. this feature is selected by default.

Deselect the feature to allow anonymous Internet requests. Filter Multicast   Multicasting allows for multiple transmissions to specific recipients at the same time.

If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. select this option to filter multicasting. This feature is not selected by default.

Filter Internet NAT Redirection   This feature uses port forwarding to block access to local servers from local networked computers. Filter IDENT (Port 113)   This feature keeps port 113 from being scanned by devices outside of your local network. Web Filter Proxy   Use of WAN proxy servers may compromise the Gateway's security. Deselect the feature to allow proxy access. java   Java is a programming language for websites.

If you deny Java, you run the risk of not having access to Internet sites created using this programming language. select this option to enable Java filtering. Deselect the feature to allow Java usage. activeX   ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. select this option to enable ActiveX filtering. Deselect the feature to allow ActiveX usage. Cookies   A cookie is data stored on your computer and used by Internet sites when you interact with them. select this option to filter cookies. Deselect the feature to allow cookie usage.

Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Security > Firewall The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network. Security > Firewall Wireless-N Broadband Router with Storage Link 16 Chapter 3 Advanced Configuration Security > VPN Passthrough The VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP or L2TP protocols to pass through the Router's firewall. Security > VPN Passthrough Storage > Disk VPN Passthrough IPSec Passthrough   Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, keep the default setting of Enabled. PPTP Passthrough   Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunnelled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default setting of Enabled. L2TP Passthrough   Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default setting of Enabled. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes.

Disk Management If a formatted disk is connected to the Router, then its name is displayed. For each partition of the disk, the Partition, File System, Capacity and Free Space information are displayed. safely Remove Disk   Before physically disconnecting a disk from the Router , click Safely Remove Disk first. This prevents the possible loss of data, which may occur if you remove the disk while it is transferring data. Create Share   To create a shared folder, click this option for the appropriate partition and the Shared Folder screen appears.

proceed to Create or Edit a Shared Folder , page 18. Shared Folder Shared Disk IP Address   The IP address of the disk is displayed. Summary   To view a list of shared folders, click this option. proceed to Shared Folders Summary , page 18. For each shared folder, the Display Name, Partition and Shared Folder location are displayed.

Edit   To change the access settings of a shared folder, click this option and the Shared Folder screen appears. Storage > Disk The storage options are available when a USB storage device is connected to the USB port of the Router. If the storage device does not fit (for example, it may block port 1), then use the included USB extension cable. The Disk screen describes the disk currently attached to the Router. Use this screen to create shared folders, safely remove a disk, or format a disk (any data on the disk will be deleted during formatting). Shared folders are folders you create to manage access to the folders on the disk. By default the Router creates a shared folder called Public, which includes all of the folders on the disk. For the Public folder, the admin group has read-and-write access rights and the guest group has read-only access rights. (By default the Router creates two user groups, admin and guest.) Wireless-N Broadband Router with Storage Link 17 Chapter 3 Advanced Configuration Shared Folders Summary The Shared Folders Summary screen displays the following information: Display Name, Partition, Shared Folder and Groups with Access.

Summary To exit the Shared Folders Summary screen and return to the Disk Management screen, click Close. Format Disk Disk   To format a disk and create a new partition, select the disk you want to format and then click Format Disk. (If your disk was formatted with multiple partitions, then the formatting will delete them and create a single partition. To format the disk as FAT32, click Format and follow the on-screen instructions. Share entire Partition   Select this option if the shared folder should include the entire partition. If you do not want to share the entire partition, then select the folder you do want to share. Enter into Folder   To display sub-folders, click this button. select   Select a folder. Return to Upper Folder   To return to the previous folder, click this button. Claim Disk On the Disk Management screen, click Refresh to update the on-screen information.

Access Specify which user groups have read-and-write or readonly access to the shared folders. (To create user groups , refer to Create or Edit a Group Account , page 20.) Available Groups   To allow a group access to the shared folder, select it and then click the >> button. Groups with Access   To block a group from accessing the shared folder, select it and then click the << button. Create or Edit a Shared Folder Use this screen to add a shared folder. Wireless-N Broadband Router with Storage Link 18 Chapter 3 Advanced Configuration Scan All   To scan all media files, click this button. The database table lists the media folders with the following information: Name, Partition and Folder. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. click Close to exit the screen. Storage > Media Server The storage options are available when a USB storage device is connected to the USB port of the Router.

If the storage device does not fit (for example, it may block port 1), then use the included USB extension cable. Create a Media Folder Use this screen to add a media folder. Storage > Media Server UPnP Media Server If you have UPnP AV-enabled (or DLNA-certified) devices in your home, then you can use the Router as a media server. Examples of UPnP AV-enabled devices include a digital media adapter, a gaming console with a built-in media player, or a digital picture frame.

For example, if you have a digital media adapter that sends content to your entertainment system, then the digital media adapter can locate the Router using the UPnP AV standard. The folders you specify can then be accessed and played by the digital media adapter. Share entire Partition   Select this option if the media folder should include the entire partition. If you do not want to share the entire partition, then select the folder you do want to share. Enter into Folder   To display sub-folders, click this button. select   Select a folder.

Return to Upper Folder   To return to the previous folder, click this button. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. click Close to exit the screen. On the Media Server screen, click Save Settings to apply your changes, or click Cancel Changes to clear your changes. 19 Setup Server Name   The default server name of the Router is WRT160NL. You can change this name on the Storage > Administration screen. Database Setup Specify Folder to Scan   To add a media folder to the database of the Router's media server, click this button. Auto-scan every __   To automatically scan the media folders, select this option. Then select the appropriate interval: 2 Hours (default), 6 Hours, 12 Hours, 24 Hours, or 48 Hours. Wireless-N Broadband Router with Storage Link Chapter 3 Advanced Configuration User Management By default the Router creates two users, admin and guest. The users are listed by Username and Group. Create New User   To create a new user, click this button. Edit   To change the settings of a user account, click Modify and the User Account screen appears. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Storage > Administration The Administration screen allows you to manage the user groups and individual users who can access the shared folders.

Create or Edit a Group Account Storage > Administration Information Server Name   Enter the server name for the Router; it will be used for the disk and media server features. Use only alphanumeric characters (letters A to Z and numbers 0 to 9) in the server name. the default setting is WRT160NL. Workgroup Name   Enter the workgroup name for the Router; it should match the workgroup name of the computers on your local network. the Router's default is workgroup.

Server LAN IP Address   The local IP address of the Router is displayed. Server Internet IP Address   The Internet IP address of the Router is displayed. Group Account Group Account Group Name   Create a name for the group. description   Enter keywords to describe the group. Access   Select the appropriate level of access, read and write or read only. Click Create or Modify to apply your changes, or click Cancel to clear your changes. click Close to exit the screen. Group Management By default the Router creates two user groups, admin and guest. The groups are listed by Group Name and Access level. there are two levels of access , r & w (read-and-write) and r (read-only).

Create New Group   To create a new group of users, click this button. Edit   To change the description or access rights of a group, click Modify and the Group Account screen appears. proceed to Create or Edit a Group Account , page 20. Delete   To delete a group, click this button. Wireless-N Broadband Router with Storage Link 20 Chapter 3 Advanced Configuration Create or Edit a User Account User Account User Account Name   Create a name for the user. Full Name   Enter the actual name of the user. description   Enter keywords to describe the user. Password   Enter the password that the user will use for login Confirm Password   Enter the password again to confirm. Group Member   Select the appropriate user group. Account disabled   To temporarily disable an account, select this option.

Click Create User or Modify User to apply your changes, or click Cancel to clear your changes. click Close to exit the screen. On the Media Server screen, click Save Settings to apply your changes, or click Cancel Changes to clear your changes. access Restrictions > Internet Access Internet Access Policy Access Policy   Access can be managed by a policy. Use the settings on this screen to establish an access policy (after Save Settings is clicked).

Selecting a policy from the dropdown menu will display that policy's settings. To delete a policy, select that policy's number and click Delete This Policy. To view all the policies, click Summary. Summary The policies are listed with the following information: No. Click Save Settings to save your changes or click Cancel Changes to cancel your changes.

To return to the Internet Access Policy screen, click Close. Access Restrictions > Internet Access The Internet Access screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services and websites during specific days and times. summary Wireless-N Broadband Router with Storage Link 21 Chapter 3 Advanced Configuration the Blocked List. To remove an application from the Blocked List, select it and click the << button. 10. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the Application Name field. Enter its range in the Port Range fields. Select its protocol from the Protocol drop-down menu. Click Save Settings to save the policy's settings or click Cancel Changes to clear the changes. status   Policies are disabled by default.

To enable a policy, select the policy number from the drop-down menu and select Enabled. To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time. 1. Select a number from the Access Policy drop-down menu. 2. Enter a Policy Name in the field provided. Click Edit List to select which PCs will be affected by the policy. the List of PCs screen appears. You can select a PC by MAC address or IP address.

You can also enter a range of IP addresses if you want this policy to affect a group of PCs. After making your changes, click Save Settings to apply your changes or click Cancel Changes to clear your changes. then click Close. Applications and Gaming > Single Port Forwarding The Single Port Forwarding screen allows you to customise port services for common applications on this screen. When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers).

Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen; refer to DHCP Reservation, page 7). list of PCs 5. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen.

6. Decide which days and what times you want this policy to be enforced.

Select the individual days during which the policy will be in effect or select Everyday. Then enter a range of hours and minutes during which the policy will be in effect or select 24 Hours. 7. You can block websites with specific URL addresses. You can also block websites using specific keywords. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.) From the Applications list, select the application you want to block. Then click the >> button to move it to Wireless-N Broadband Router with Storage Link Applications and Gaming > Single Port Forwarding Single Port Forwarding Common applications are available for the first five entries. select the appropriate application.

Then enter the IP address of the server that should receive these requests. select Enabled to activate this entry. For additional applications, complete the following fields: Application Name   Enter the name you wish to give the application. Each name can be up to 12 characters. 22 Chapter 3 Advanced Configuration Port Range Forwarding To forward a port, enter the information on each line for the criteria required. Application Name   In this field, enter the name you wish to give the application. Each name can be up to 12 characters. Start-End Port   Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information. Protocol   Select the protocol(s) used for this application, TCP, UDP or Both.

To IP Address   For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address. Enabled   Select Enabled to enable port forwarding for the applications you have defined. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. External Port   Enter the external port number used by the server or Internet application.

Check with the Internet application documentation for more information. Internal Port   Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information. Protocol   Select the protocol(s) used for this application, TCP, UDP or Both. To IP Address   For each application, enter the IP address of the PC that should receive the requests.

If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address. enabled   For each application , select Enabled to enable port forwarding. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Applications and Gaming > Port Range Forwarding The Port Range Forwarding screen allows you to set up public services on your network, such as web servers, ftp servers, email servers or other specialised Internet applications. (Specialised Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding). When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen; refer to DHCP Reservation, page 7). If you need to forward all ports to one computer, click the DMZ tab. Applications & Gaming > Port Range Triggering The Port Range Triggering screen allows the Router to watch outgoing data for specific port numbers.

The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules. Applications and Gaming > Port Range Triggering Port Range Triggering Applications and Gaming > Port Range Forwarding Application Name   Enter the application name of the trigger. 23 Wireless-N Broadband Router with Storage Link Chapter 3 Advanced Configuration address in the field provided. to retrieve this information , click DHCP Client Table. Triggered Range   For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed. Forwarded Range   For each application, enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed. Enabled   Select Enabled to enable port triggering for the applications you have defined. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes.

DMZ > DHCP Client Table Applications and Gaming > DMZ The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet. DHCP Client Table The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address and Expired Time (how much time is left for the current IP address). To exit this screen and return to the DMZ screen, click Close. Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Applications and Gaming > QoS Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications such as videoconferencing. Applications and Gaming > DMZ DMZ Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function. Then configure the following settings: Source IP Address   If you want any IP address to be the source, select Any IP Address.

If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields. Destination   If you want to specify the DMZ host by IP address, select IP Address and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select MAC Address and enter the MAC Wireless-N Broadband Router with Storage Link Applications and Gaming > QoS QoS (Quality of Service) Wireless You can configure the support and No Acknowledgement settings in this section.

WMM Support If you have other devices that support Wi-Fi Multimedia (WMM) on your network, keep the default setting of Enabled. otherwise , select Disabled. 24 Chapter 3 Advanced Configuration application that uses from 1000 to 1250, you enter 10001250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used. Your new entry will appear in the Summary list.

No Acknowledgement If you want to disable the Router's Acknowledgement feature, so the Router will not re-send data if an error occurs, then select Enabled. Otherwise, keep the default setting of Disabled. Internet Access Priority In this section, you can set the bandwidth priority for a variety of applications and devices. there are four levels of priority: High , Medium , Normal or Low. When you set the priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority. Enabled/Disabled To use the QoS policies you have set, keep the default setting of Enabled. Proceed to the instructions for your selection. qoS > Online Games Games Select the appropriate game.

If you select Add a New Game, follow the Add a New Game instructions. Your new entry will appear in the Summary list. Add a New Game Summary This lists the QoS entries you have created for your applications and devices. If you select Add a New Application, follow the Add a New Application instructions. Your new entry will appear in the Summary list.

Add a New Application QoS > Add a New Game Enter a Name Enter any name to indicate the name of the entry. Port Range Enter the port range that the game will be using. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

QoS > Add a New Application Enter a Name Enter any name to indicate the name of the entry. Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an Wireless-N Broadband Router with Storage Link Click Add to save your changes. Your new entry will appear in the Summary list. 25 Chapter 3 Advanced Configuration Name This column displays the application , device or port name. Information This column displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section. qoS > MAC Address MAC Address Remove Click this button to remove an entry. Edit Click this button to make changes.

Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Enter a Name Enter a name for your device. MAC Address Enter the MAC address of your device. Your new entry will appear in the Summary list. Administration > Management The Administration > Management screen allows the network's administrator to manage specific Router functions for access and security. Your new entry will appear in the Summary list. Voice Device Administration > Management QoS > Voice Device Management Router Access To ensure the Router's security, you will be asked for your password when you access the Router's web-based utility. the default setting is admin. Router Password Enter a new password for the Router. Re-enter to confirm Enter the password again to confirm.

Enter a Name Enter a name for your voice device. MAC Address Enter the MAC address of your voice device. Your new entry will appear in the Summary list. Summary This lists the QoS entries you have created for your applications and devices. priority This column displays the bandwidth priority of High , Medium , Normal or Low.

Local Management Access Access via HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. 26 Wireless-N Broadband Router with Storage Link Chapter 3 Advanced Configuration Allow Users to Disable Internet Access Select Enabled, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default setting of Disabled. Access via Wireless If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. You will only be able to access the utility via a wired connection if you disable the setting.

Keep the default setting of Enabled, to allow wireless access to the utility or select Disabled to block wireless access to the utility. Backup and Restore Backup Configurations To back up the Router's configuration settings, click this button and follow the on-screen instructions. Restore Configurations To restore the Router's configuration settings, click this button and follow the onscreen instructions. (You must have previously backed up the Router's configuration settings). Click Save Settings to apply your changes or click Cancel Changes to cancel your changes. Remote Access Remote Management To permit remote access of the Router, from outside the local network, select Enabled. Otherwise, keep the default setting of Disabled. Access via HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. Remote Upgrade If you want to be able to upgrade the Router remotely, from outside the local network, select Enabled. (You must have the Remote Management feature enabled as well).

Otherwise, keep the default setting of Disabled. Allowed Remote IP Address If you want to be able to access the Router from any external IP address, select Any IP Address. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided. Remote Management Port Enter the port number that will be open to outside access. NOTE: When you are in a remote location and wish to manage the Router, enter http://xxx. Enter the Router's specific Internet IP address in place of xxx. Xxx and enter the Remote Management Port number in place of yyyy. Administration > Log The Router can keep logs of all traffic for your Internet connection. administration > Log Log Log To disable the Log function , select Disabled. To monitor traffic between the network and the Internet, keep the default setting of Enabled.

With logging enabled, you can choose to view temporary logs. View Log To view the logs, click View Log. UPnP Universal Plug and Play (UPnP) allows the appropriate Windows operating system to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.