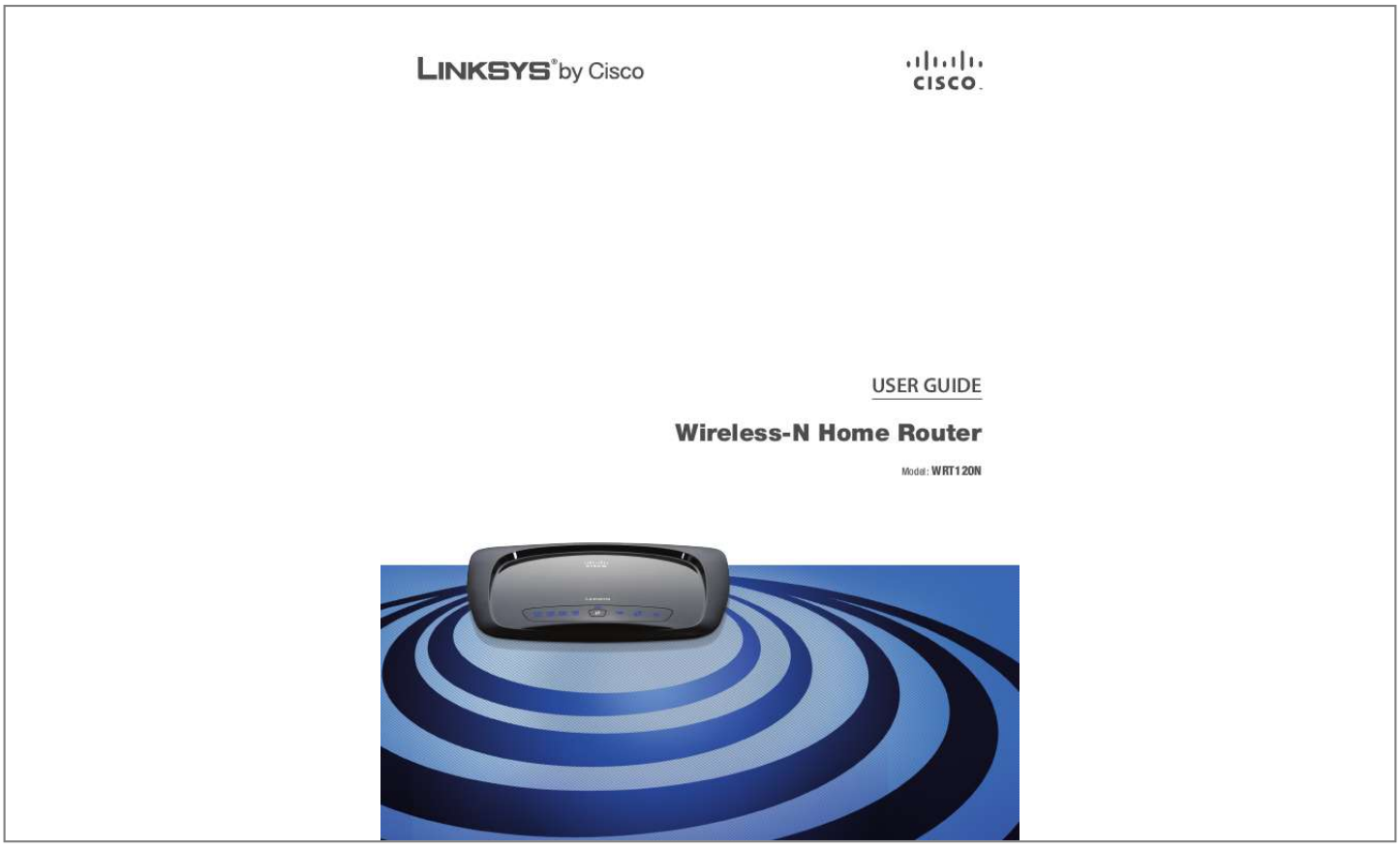

Manual abstract:

Other brands and product names are trademarks or registered trademarks of their respective holders. Wireless (Blue) The Wireless LED lights up when the wireless feature is enabled. 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. 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.

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. 1, 2, 3, 4 (Blue) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. 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.

Wi-Fi Protected Setup LED (Blue/ Amber) The LED lights up blue when wireless security is enabled. It flashes blue for two minutes during Wi-Fi Protected Setup. The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

Wait until the LED is solidly lit, or off before starting the next Wi-Fi Protected Setup session. 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. 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 browser-based utility. Power The Power port connects to the included power adapter. The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet. 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. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet. 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. Maneuver 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. Cut along the dotted line, and place on the wall to drill precise spacing. 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 cellular 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. 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 Social Security number) because this information may be available for anyone to see when browsing for wireless networks. 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. Some applications may open file sharing without your consent and/or knowledge. For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.

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 vacations). 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. 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. 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 browser-based utility. This chapter describes each web page of the utility and each page's key functions. 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 browser-based utility. To access the browser-based utility, launch the web browser on your computer, and enter the Router's default IP address, 192.

The first time you open the browser-based utility, use the default password admin. (You can set a new password from the Administration > Management screen. Select your language To use a different language, select one from the drop-down menu. The language of the browser-based utility will change five seconds after you select another language. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.
Most of this information can be obtained through your Internet Service Provider (ISP). Select the type of Internet connection your ISP provides from the drop-down menu. This allows you to change the Router's general settings. Service Name (Optional) If provided by your ISP, enter the Service Name. 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 have elapsed before your Internet connection terminates. the default Max Idle Time is 5 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. By default, the Router's Internet Connection Type is set to Automatic configuration - DHCP, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. If you are required to use a permanent IP address to connect to the Internet, select Static IP. Internet IP Address This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here. Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask. Default Gateway Your ISP will provide you with the IP address of the ISP server.
DNS 1-3 Your ISP will provide you with at least one DNS (Domain Name System) server IP address. Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE. If your ISP supports DHCP or you are connecting through a dynamic IP address, then select Obtain an IP Address Automatically.
If you are required to use a permanent IP address to connect to the Internet, then select Specify an IP Address. Specify an IP Address This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here. Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
Default Gateway Your ISP will provide you with the IP address of the ISP server. 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. DNS 1-3 Your ISP will provide you with at least one DNS (Domain Name System) server IP address. PPTP Server IP Address Your ISP will provide you with the IP address of the PPTP server. username and Password Enter the Username and Password provided by your ISP. 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 have elapsed before your Internet connection terminates. the default Max Idle Time is 5 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. Your ISP will provide you with the IP Address you need to specify here. username and Password Enter the Username and Password provided by your ISP. 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 Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time has expired, the user will be automatically assigned a new dynamic IP address, or the lease will be renewed. the default 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 computer's interaction with the Internet. If you use a WINS server, enter that server's IP Address here.
Otherwise, leave this blank. Mail Exchange (Optional) Enter the address of your mail exchange server, so e-mails 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, Disabled. to enable the feature , select Enabled. If you are not sure which setting to select, keep the default, 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, Disabled. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. Time Zone Select the time zone in which your network functions from this drop-down menu. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. 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 need to sign up for DDNS service with a DDNS service provider, www. If you do not want to use this feature, keep the default, Disabled. If your DDNS service is provided by TZO, then select TZO.

Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. 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.

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 clear your changes. 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.

Enabled/Disabled If this Router is hosting your network's connection to the Internet, keep the default, Enabled. If another router exists on your network, select Disabled. 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. Clone My PC's MAC Click this button to clone the MAC address of the computer you are using. 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. As wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

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. Default 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. 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, 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.

For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. to update the information , click Refresh. To exit this screen and return to the Advanced Routing screen, click Close. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. 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 Wireless-N network , select 40MHz only. For Wireless-G and Wireless-B networking only, keep the default, 20MHz only. If you are not sure which option to use, select Auto (20MHz or 40MHz). NOTE: If you select 40MHz only 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 40MHz only is the Channel Width setting, then this setting will be available for your primary 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.

Select any channel from the dropdown menu. If you are not sure which channel to select, keep the default, Auto. Standard Channel If 20MHz only is the Channel Width setting, then select the appropriate channel for your wireless network. If you are not sure which channel to select, then keep the default, Auto. If 40MHz only 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 be available. 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 , 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 clear your changes. Use the method that applies to the client device you are configuring. Repeat the instructions for each client device that supports Wi-Fi Protected Setup. Use this method if your client device has a Wi-Fi Protected Setup button.

Then refer back to your client device or its documentation for further instructions. 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. Then refer back to your client device or its documentation for further instructions.

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. Use this method if your client device asks for the Router's PIN number. 1. Enter the PIN number listed on this screen. 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. 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.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. Select the security method for your wireless network. If you do not want to use wireless security, keep the default, Disabled. 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. 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 option features WPA used with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router. 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. 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 option features WPA2 used with a RADIUS server.
(This should only be used when a RADIUS server is connected to the Router. Shared Secret Enter the key shared between the Router and the server. Key 1 If you did not enter a Passphrase, enter the WEP key manually. Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.
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. Key 1 If you did not enter a Passphrase, enter the WEP key manually. tX Key TX (Transmit) Key 1 is used. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. If you do not wish to filter users by MAC Address, keep the default, Disabled. 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.

AP Isolation This option 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 with each other. Frame Burst This option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, Enable. 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 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 Auto, when the Router can transmit at all standard wireless rates (1-2 Mbps, 5. 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, Auto, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. 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, Auto, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. This screen shows computers and other devices on the wireless network. the list can be sorted by Client Name , 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 01-32 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 clear your changes. 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-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, Auto.

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 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 clear your changes.
SPI Firewall Protection To use firewall protection, keep the default selection, Enabled. Filter Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. this feature is enabled by default. Deselect this option 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. 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. The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. 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. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Cookies A cookie is data stored on your computer and used by Internet sites when you interact with them. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. The VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.

Use the settings on this screen to establish an access policy (after Save Settings is clicked). To allow IPSec tunnels to pass through the Router, keep the default, Enabled. pPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, 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, Enabled. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. The policies are listed with the following information: No. To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time.
Enter a Policy Name in the field provided. You can select a computer 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 computers. After making your changes, click Save Settings to apply your changes, or click Cancel Changes to clear your changes. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the computers you listed on the Internet Access PC List 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 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 the Blocked List. 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. To IP Address For each application, enter the IP address of the computer that should receive the requests. If you assigned a static IP address to the computer, then you can look up its IP address; click DHCP Reservation on the Basic Setup screen (refer to DHCP Reservation, page 7).

enabled For each application , select Enabled to enable port forwarding. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. Click Save Settings to save the policy's settings, or click Cancel Changes to clear the changes. The Single Port Forwarding screen allows you to customize 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). The Port Range Forwarding screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized 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. 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. 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 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. Forwarded Range For each application, enter the starting and ending port numbers of the forwarded port number range. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.

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 computer that should receive the requests. If you assigned a static IP address to the computer, then you can look up its IP address; click DHCP Reservation on the Basic Setup screen (refer to DHCP Reservation, page 7). 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 clear your changes. 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. 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. Any computer 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. Triggered Range For each application, enter the starting and ending port numbers of the triggered port number range. 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. WMM Support If you have other devices that support Wi-Fi Multimedia (WMM) on your network, keep the default, Enabled. otherwise , select Disabled. 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, Disabled. By MAC address, select MAC Address and enter the MAC address in the field provided. In this section, you can set the bandwidth priority for a variety of applications and devices. there are four levels priority: High , Medium , Normal , or Low. When you set 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, Enabled. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expires 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 clear your changes. This lists the QoS entries you have created for your applications and devices. Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing. If you select Add a New Application, follow the Add a New Application instructions. You can configure the support and No Acknowledgement settings in this section.

Enter a Name Enter any name to indicate the name of the entry. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an 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. Enter a Name Enter a name for your device. MAC Address Enter the MAC address of your device. If you select Add a New Game, follow the Add a New Game instructions. 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. My Voice Device's MAC Address The MAC address of your voice device is automatically displayed. Enter a Name Enter a name for your voice device. MAC Address Enter the MAC address of your voice device.

This lists the QoS entries you have created for your applications and devices. 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 browser-based utility. You will only be able to access the utility via a wired connection if you disable the setting. Keep the default, Enabled, to allow wireless access to the utility, or select Disabled to block wireless access to the utility. 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. 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 clear your changes. Otherwise, keep the default, Disabled. Remote Upgrade If you want to be able to upgrade the Router remotely, from outside the local network, select Enabled. 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. To ensure the Router's security, you will be asked for your password when you access the Router's browser-based utility.

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. UPnP To use UPnP, keep the default, Enabled. otherwise , select Disabled. Allow Users to Configure Keep the default, Enabled, if you want to be able to make manual changes to the Router while using the UPnP feature. otherwise , select Disabled. 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, Disabled. Backup Configuration To back up the Router's configuration settings, click this button and follow the on-screen instructions. Restore Configuration To restore the Router's configuration settings, click this button and follow the on-screen instructions. Click Save the Log to save this information to a file on your computer's hard drive. Start to Reboot If you need to restart the Router, click this button. Click Save Settings to apply your changes, or click Cancel Changes to clear your changes.

The Router can keep logs of all traffic for your Internet connection.
Click Save Settings to apply your changes, or click Cancel Changes to clear your changes. The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network devices, including connection to the Internet. To monitor traffic between the network and the Internet, keep the default, Enabled. With logging enabled, you can choose to view temporary logs. View Log To view the logs, click View Log.
IP or URL Address Enter the address of the computer whose connection you wish to test. Number to Ping Enter the number of times you wish to test the connection. the default is 5. Start to Ping To run the test, click this button. NOTE: Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration settings. Restore All Settings To reset the Router's settings to the defaults, click this button and then follow the on-screen instructions. Any custom settings you have saved will be lost when the default settings are restored. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use. IP or URL Address Enter the address of the computer whose connection you wish to test.

Start to Traceroute To run the test, click this button. NOTE: The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you may have to re-enter all of your configuration settings. Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, www. Start to Upgrade After you have selected the appropriate file, click this button, and follow the on-screen instructions. WARNING: The firmware upgrade must not be interrupted; do not reboot or power off the Router during the firmware upgrade. This section shows the current network information stored in the Router. The Router screen displays information about the Router and its current settings. Router IP Address The Router's IP address, as it appears on your local network, is displayed.
Internet MAC Address The Router's MAC Address, as seen by your ISP, is displayed. Start IP Address For the range of IP addresses that can be used by devices on your local network, the starting IP address is displayed. End IP Address For the range of IP addresses that can be used by devices on your local network, the ending IP address is displayed. DHCP Clients Table Click this button to view a list of computers or other devices that are using the Router as a DHCP server. Security The wireless security method used by the Router is displayed.
To exit this screen and return to the Local Network screen, click Close. Network Name (SSID) The name of the wireless network, which is also called the SSID, is displayed. The Router does not replace your modem. You still need your cable modem in order to use the Router. Connect your cable connection to the cable modem, and then insert the setup CD into your computer.
Make sure the wireless network name or SSID is the same on both the computer and the Router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router. you need to modify the settings on the Router. Open the web browser (for example, Internet Explorer or Firefox), and enter the Router's IP address in the address field (the default IP address is 192. When prompted, enter the password to the Router (the default is admin). click the appropriate tab to change the settings. WEB: If your questions are not addressed here, refer to the Linksys website, www. Your computer cannot connect to the Internet. Follow these instructions until your computer can connect to the Internet: The Power LED should be lit and not flashing. If the Power LED is flashing, then power off all of your network devices, including the modem, Router, and computers.

Then power on each device in the following order: 1. The computer should be connected to one of the ports numbered 1-4 on the Router, and the modem must be connected to the Internet port on the Router. To use the Router, you need a cable/DSL modem and high-speed Internet connection. You cannot use the DSL service to connect manually to the Internet. After you have installed the Router, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually. The DSL telephone line does not fit into the Router's Internet port. The Router does not replace your modem. You still need your DSL modem in order to use the Router. Connect the telephone line to the DSL modem, and then insert the setup CD into your computer. click Setup and follow the on-screen instructions.
When you double-click the web browser, you are prompted for a username and password. If you want to get rid of the prompt, follow these instructions. Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers): 1. Specifications are subject to change without notice. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack.
The product may include or be bundled with third party software or service offerings. @@@@@@@@@@@@@@@@@@@@@@@@@@@@@ linksysbycisco. @@@@@@@@@@@@@@@@Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges.
Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates. This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at www. This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you. WARNING: Do not use this product near water, for example, in a wet basement or near a swimming pool. 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. This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. @@There may be a remote risk of electric shock from lightning. @@Wash hands after handling. @@Operation is subject to the following two conditions: 1. This device may not cause interference and 2. @@This device has been designed to operate with an antenna having a maximum gain of 2. 0 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. Reorient or relocate the receiving antenna Increase the separation between the equipment or devices Connect the equipment to an outlet other than the receiver's Consult a dealer or an experienced radio/TV technician for assistance This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. 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 equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
11g operation of this product in the USA is firmware-limited to channels 1 through 11. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions. Les performances dépendent de facteurs, conditions et variables multiples, en particulier de la distance par rapport au point d'accès, du volume du trafic réseau, des matériaux utilisés dans le bâtiment et du type de construction, du système d'exploitation et de la combinaison de produits sans fil utilisés, des interférences et de toute autre condition défavorable. This document contains important information for users with regards to the proper disposal and recycling of Linksys products.
Consumers are required to comply with this notice for all electronic products bearing the following symbol: European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product. This product from Cisco Systems, Inc. Or its subsidiary licensing the Software instead of Cisco Systems, Inc. ("Cisco") contains software (including firmware) originating from Cisco and its suppliers and may also contain software from the open source community. Any software originating from Cisco and its suppliers is licensed under the Cisco Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept the Cisco Software License Agreement upon installation of the software.

separate terms and features of Network Magic , a Cisco Software product , are set forth in Schedule 2 below. Any software from the open source community is licensed under the specific license terms applicable to that software made available by Cisco at www. By using the Software, you acknowledge that you have reviewed such license terms and that you agree to be bound by the terms of such licenses. Where such specific license terms entitle you to the source code of such software, that source code is available upon request at cost from Cisco for at least three years from the purchase date of this product and may also be available for download from www. If you would like a copy of the GPL or certain other open source code in this Software on a CD, Cisco will mail to you a CD with such code for $9. 99 plus the cost of shipping, upon request. The software licenses applicable to software from Cisco are made available at the Cisco public web site at: www. For your convenience of reference, a copy of the Cisco Software License Agreement and the main open source code licenses used by Cisco in its products are contained in the Schedules below. Subject to the terms and conditions of this Agreement, Cisco grants the original end user purchaser of the Software a nonexclusive license to (i) use the Software solely as embedded in, as a stand-alone application or (where authorized in the applicable documentation) for communication with such product, each solely at Cisco's discretion; (ii) if the Software is purchased separately from any Cisco Product, install the Software on personal computers within a single household or business location according to the maximum number of licenses you have purchased; and (iii) make one copy of the Software in machine-readable form and one copy of the Documentation, solely for backup purposes. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Cisco product containing the Software or complete Software product, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.
"Software" includes, and this Agreement will apply to (a) the software of Cisco or its suppliers purchased separately or provided in or with the applicable Cisco product, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to you by Cisco or an authorized reseller (whether or not for a fee), provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade. "Documentation" means all documentation and other related materials supplied by Cisco to you pursuant to this Agreement. Suitability, functionality, or legality of any sites or products to which links may be provided or third party services, and you hereby waive any claim you might have against Cisco with respect to such sites or third party software products or services.

Your correspondence or business dealings with, or participation in promotions of third parties found through the Software and any other terms, conditions, warranties, or representations associated with such dealings, are solely between you and such third party. You agree that Cisco is not responsible or liable for any loss or damage of any sort incurred as the result of any such dealings or as the result of the presence of such third party links, products or services in the Cisco Software, and Cisco may discontinue or modify the services or links offered at any time.

collection and Processing of Information. You agree that Cisco and/or its affiliates may, from time to time, collect and process information about your Cisco product and/or the Software and/or your use of either in order (i) to enable Cisco to offer you Upgrades; (ii) to provide support and assistance with your product and/or the Software; (iii) to ensure that your Cisco product and/or the Software is being used in accordance with the terms of this Agreement; (iv) to provide improvements to the way Cisco delivers technology to you and to other Cisco customers; (v) to provide reports regarding the status and health of the network, including network traffic and application usage; (vi) to enable Cisco to comply with the terms of any agreements it has with any third parties regarding your Cisco product and/or Software; and/or (vii) to enable Cisco to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Cisco and/ or its affiliates may collect and process this information provided that it does not identify you personally. You agree that Cisco has no responsibility or liability for the deletion of or failure to store any data or other information related to your Cisco product, Software or related Services. The reports feature of certain Software allows you to monitor the activity of computers running the Software in your home or small office.

You must activate this feature in order to receive reports. If you activate the reports feature, you agree to the following: (a) the Software tracks and monitors the following components and activities in your home or office: network traffic (e. g. Megabytes per hour), application usage (the foreground window is tracked and the time each application is in the foreground during active usage of the computer) and internet history. (b) For all computers on which reports feature is enabled, the above information is transmitted to servers at Cisco and/ or a third party at periodic intervals while the computer is online. This information is associated and stored with the email address supplied by you when you activated the reports feature. This information is summarized into a formal report and is emailed to the identified email address. Other than as set forth in this Agreement, you may not (i) make or distribute copies of the Software or its related Documentation, or electronically transfer the Software or Documentation from one computer to another or over a network; (ii) alter, merge, modify, adapt, decrypt or translate the Software or related Documentation, or decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form (except to the extent expressly permitted by law notwithstanding this provision); (iii) share, sell, rent, lease, or sublicense the Software or related Documentation; (iv) modify the Software or create derivative works based upon the Software; (v) if you make a backup copy of the Software and Documentation, you must reproduce all copyright notices and any other proprietary legends found on the original Software and Documentation; (vi) use the Software for management of a business network with more than 8 computers; (vii) use the Software under any circumstances for competitive evaluation, including developing competing software; (ix) to the extent permitted under applicable law, assign, sublicense or otherwise transfer the Software unless the prospective assignee, sublicensee or transferee expressly agrees to all the terms and conditions under this Agreement. The Software and Documentation contain trade secrets and/or copyrighted materials of Cisco or its suppliers. You will not disclose or make available such trade secrets or copyrighted material in any form to any third party.

In the event that you fail to comply with this Agreement, the license granted to you will automatically terminate, at which time you must immediately (i) stop using the Cisco Product in which the Software is embedded, or (ii) uninstall the Software and destroy all copies of the Software and Documentation where the Software is purchased separately. All other rights of both parties and all other provisions of this Agreement will survive this termination. ownership. The Software and Documentation are licensed and not sold to you by Cisco and the relevant third parties set forth in Schedule 3. Cisco and its licensors retain all right, title and interest, including all copyright and intellectual property rights, in and to, the Software and Documentation and all copies and portions thereof. All rights not specifically granted to you in this Agreement are reserved by Cisco and its licensors. Your use of any software product from an entity other than Cisco that may have been recommended by Cisco is governed by such software product's end user license agreement. third Party Services , Links and Advertising. Cisco may provide from within the Software links to websites or third party software products. In addition, third party services may be provided with the Software which may be subject to terms and conditions from the provider of the service.

Installing the software and changing these software settings may conflict with license agreements you have entered into with other entities, such as your Internet service provider. Error queries that are libelous, slanderous, defamatory or that may violate the intellectual property rights of others may not be processed by Cisco or its suppliers. term and Termination. You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Cisco if you fail to comply with any provision of this Agreement.

limited Warranty. Cisco additionally warrants that any media on which the Software may be provided will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of original purchase. Your exclusive remedy and Cisco's entire liability under this limited warranty will be for Cisco, at its option, to (a) replace the Software media, or (b) refund the purchase price of the Software media. eXCEPT FOR THE LIMITED WARRANTY ON MEDIA SET FORTH ABOVE AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW , ALL SOFTWARE AND SERVICES PROVIDED BY CISCO ARE PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND.