

# T-Mobile @Home



HiPort+™  
User Guide

<b>Chapter 1: Product Overview</b>	<b>2</b>
Front Panel . . . . .	2
Back Panel . . . . .	2
<b>Chapter 2: Wireless Security Checklist</b>	<b>3</b>
General Network Security Guidelines . . . . .	3
Additional Security Tips . . . . .	3
<b>Chapter 3: Installation</b>	<b>4</b>
SIM Card Installation . . . . .	4
SIM Card Removal . . . . .	4
Connections . . . . .	5
Table or Wall Mount Instructions . . . . .	6
<b>Chapter 4: Configuration</b>	<b>7</b>
How to Access the Web-Based Utility . . . . .	7
Setup > Basic Setup . . . . .	7
Setup > DDNS . . . . .	10
Setup > MAC (Address) Clone . . . . .	11
Setup > Advanced Routing . . . . .	12
Wireless > Basic Wireless Settings . . . . .	13
Wireless > Wireless Security . . . . .	13
Wireless > Wireless MAC Filter . . . . .	15
Wireless > Advanced Wireless Settings . . . . .	16
Security > Firewall . . . . .	17
Security > VPN . . . . .	17
Access Restrictions > Internet Access . . . . .	18
Applications & Gaming > Port Range Forward . . . . .	19
Applications & Gaming > Port Triggering . . . . .	19
Applications & Gaming > DMZ . . . . .	20
Applications and Gaming > QoS . . . . .	20
Administration > Management . . . . .	21
Administration > Log . . . . .	22
Administration > Diagnostics . . . . .	23
Administration > Factory Defaults . . . . .	23
Administration > Firmware Upgrade . . . . .	24
Administration > Config Management . . . . .	24
Status > Router . . . . .	25
Status > Local Network . . . . .	25
Status > Wireless . . . . .	26
Status > Voice . . . . .	27
<b>Appendix A: Troubleshooting</b>	<b>28</b>
<b>Appendix B: Specifications</b>	<b>29</b>

<b>Appendix C: Warranty Information</b>	<b>30</b>
Limited Warranty . . . . .	.30
<b>Appendix D: Regulatory Information</b>	<b>32</b>
FCC Statement . . . . .	.32
Industry Canada Statement . . . . .	.32
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) . . . . .	.33
<b>Appendix E: Software Licensing Agreement</b>	<b>37</b>
Software in Linksys Products . . . . .	.37
Software Licenses . . . . .	.37

# About This Guide

## Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:



**NOTE:** This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.



**WARNING:** This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.



**WEB:** This globe icon indicates a noteworthy website address or e-mail address.

## Online Resources

Most web browsers allow you to enter the web address without adding the http:// in front of the address. This User Guide will refer to websites without including http:// in front of the address. Some older web browsers may require you to add it.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

## Copyright and Trademarks

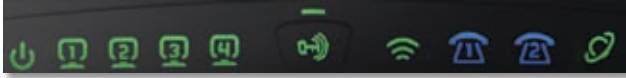



Linksys, Cisco and the Cisco Logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2008 Cisco Systems, Inc. All rights reserved.


# Chapter 1: Product Overview


## Front Panel


The HiPort +™ LEDs are located on the front panel.





- 

**Power** (Green/Amber) The Power LED lights up green and will stay on while the HiPort+ is powered on. When the HiPort+ 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. This LED flashes amber when the HiPort+ is doing a firmware upgrade. This LED alternately flashes green and amber if a SIM card is not installed or if SIM card registration fails. This LED lights up amber if 911 Emergency Calling has not been registered.
- 

**Ethernet 1-4** (Green) These LEDs serves two purposes. If the LED is continuously lit, the HiPort+ is successfully connected to a device. A flashing LED indicates network activity.
- 

**Pairing** (Green/Amber) This LED lights up green when wireless security is enabled. The LED flashes amber when pairing is in progress.
- 


**Wireless** (Green) The Wireless LED lights up when the wireless feature is enabled. If the LED is flashing, the HiPort+ is actively sending or receiving data over the network.
- 

**Phone 1-2** (Blue) This LED lights up blue when a SIM card is correctly installed and registered. This LED flashes blue if the HiPort+ has received voice mail.
- 


**Internet** (Green) The Internet LED lights up when there is a connection made through the Internet port. The LED flashes when there is traffic.


## Back Panel





- 

**Reset** The Reset button serves two purposes. You can restore its factory default settings or reboot the HiPort.

  - To restore the factory default settings, press the **Reset** button for approximately five seconds, using a pin or straightened paper clip ( factory defaults can also be restored via the *Administration > Factory Defaults* screen of the HiPort+'s web-based utility).
  - To reboot the HiPort+, press and release the **Reset** button quickly using a pin or straightened paper clip.
- 

**Internet** Use this port to connect the HiPort+ to your broadband Internet connection.
- 

**Ethernet 1-4** Use these ports to connect the HiPort+ to your networked PCs and other Ethernet network devices.
- 

**Phone 1-2** Use these ports to connect phones to the HiPort+.
- 

**Power** Use this port to connect the power adapter.



**IMPORTANT:** Resetting the HiPort+ will erase all of your settings (Internet connection and other settings) and replace them with the factory defaults. Do not reset the HiPort+ if you want to retain these settings.

## 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 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.

### 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 Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

### 2. 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 unauthorized changes, customize the device's password so it will be hard to guess.

### 3. 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.

### 4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. Currently, devices that are Wi-Fi certified are required to support WPA2, but are not required to support WEP.

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.

## 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 passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications 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 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.com/security](http://www.linksys.com/security)

## Chapter 3: Installation

### SIM Card Installation

To install the SIM card, follow these steps:

1. Before connecting the HiPort+, turn it over. Insert a coin into the the SIM card cover slot.
2. Press on the coin and the cover will open.



Open SIM Card Cover

3. Slide a SIM card into a slot, with the "T" facing up.



Place SIM Card into Slot

4. Press the SIM card securely into the slot.



SIM Card Inserted



SIM Card Cover Closed.

5. Slide the cover back into place.

If you have an additional SIM card, insert it the same way into the second slot.

### SIM Card Removal

To remove, follow steps 1 and 2 to open the cover, then pull out the SIM card.



Open SIM Card Cover

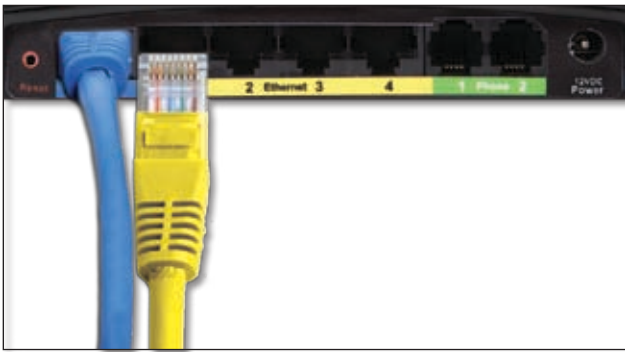
## Connections

1. Power down your network devices.
2. Locate an optimum location for the HiPort+. Connect a standard Ethernet network cable to the HiPort+'s Internet port. Then, connect the other end of the Ethernet cable to your cable or DSL broadband modem.



Connecting the Internet Connection

3. Connect the included Ethernet cable to the HiPort+'s Ethernet port. Then connect the other end to your network PC's or your Router's numbered ports using standard Ethernet network cabling.



Connecting the Ethernet Connection

4. Connect a standard RJ-11 phone cable to the HiPort+'s Phone port. This port should correspond to the SIM slot into which the SIM card was installed. Then connect the other end to a telephone. If you have a second telephone, you can connect it through the HiPort+'s other phone port.



Connecting the RJ-11 cable



**IMPORTANT:** Do not connect the Phone port to a telephone wall jack. Make sure you only connect a telephone to the Phone port. Otherwise, the Router or the telephone wiring in your home or office may be damaged.

5. Connect the AC power adapter to the HiPort+'s Power port and the other end into an electrical outlet. Only use the power adapter supplied with the HiPort+. Use of a different adapter may damage the product.



Connecting the Power Adapter



## Table or Wall Mount Instructions




### Horizontal Placement

The HiPort+ can be placed on a level surface near an electrical outlet.

### Wall-Mounting Placement

The HiPort+ has two wall-mount slots on its bottom panel. The distance between the slots is 123 mm (2.36 inches).

Two screws are needed to mount the HiPort+.

Suggested Mounting Hardware		
		
4-5 mm	1-1.5 mm	2.5-3.0 mm

†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 HiPort+. 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 123 mm (4.84 inches) apart.
3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed.
4. Maneuver the HiPort+ so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the HiPort+ down until the screws fit snugly into the wall-mount slots.



Wall Mount Slots

## Chapter 4: Configuration

For details on connecting the HiPort+, please refer to the *Installation* chapter. This chapter will describe each screen of the web-based utility and each screen's key functions. The web-based utility can be accessed via your web browser through use of a computer connected to the HiPort+. Most users only need to configure the following screens:

- **Basic Setup** On the *Setup > Basic Setup* screen, enter the Internet connection settings provided by your Internet Service Provider (ISP). If you do not have this information, you can call your ISP to request the settings. When you have the setup information, then you can configure the HiPort+.
- **Management** On the *Administration > Management* screen, change the local router access password from the default value (**admin**). Enter a new password in the *Password* and *Re-enter to confirm* fields.

There are six main tabs: Setup, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Sub tabs vary depending upon the main tab selection.

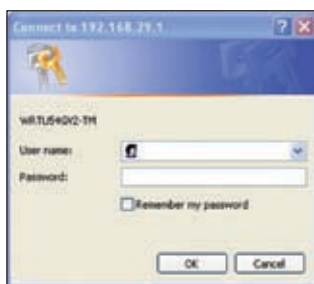
### How to Access the Web-Based Utility

To access the web-based utility of the HiPort+, launch your web browser, and enter the HiPort+'s default IP address, **192.168.29.1**, in the *Address* field. Press the **Enter** key.



Internet Explorer Address Bar

A screen will appear asking you for your User name and Password. Enter **admin** in the *User Name* field. Enter **admin** in the *Password* field. Then click **OK**.

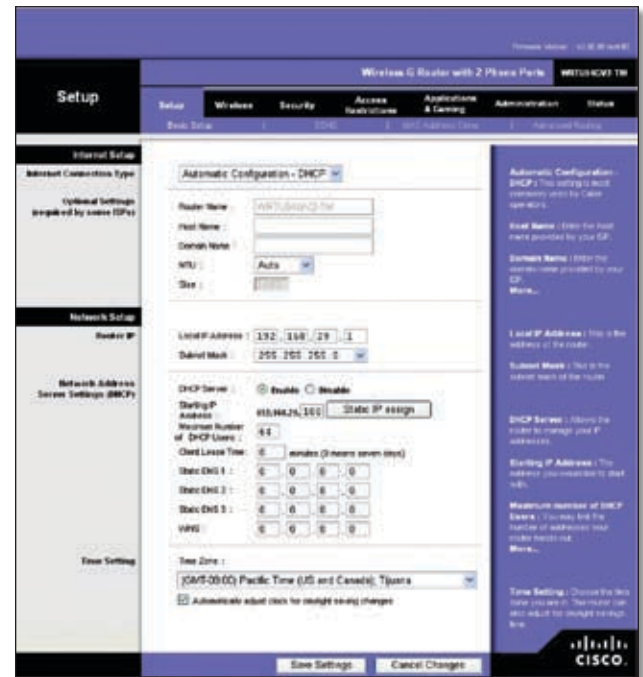


Login Screen

Make the necessary changes through the Utility. When you have finished making changes to a screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

### Setup > Basic Setup

The *Basic Setup* screen is the first screen you see when you access the web-based utility.



Setup > Basic Setup

### Internet Setup

The Internet Setup section configures the HiPort+ for your Internet connection type. This information can be obtained from your ISP.

#### Internet Connection Type

The HiPort+ supports two connection types: Automatic Configuration - DHCP and Static IP. Each *Basic Setup* screen and the available features will differ depending on what kind of connection type you select.

#### Internet Connection Type

Select the type of Internet connection your ISP provides from the drop-down menu. The available types are:

- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP

#### Automatic Configuration - DHCP

By default, the HiPort+'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. (This option usually applies to cable connections.)



Internet Connection Type > Automatic Configuration - DHCP

### Static IP

If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.

Internet Connection Type > Static IP

**IP Address** This is the HiPort+'s IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to enter here.

**Subnet Mask** This is the HiPort+'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 Gateway Address, which is the ISP server's IP address.

**DNS** Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

### PPPoE

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**.

Internet Connection Type > PPPoE

**User Name and Password** Enter the User Name and Password provided by your ISP.

**Service Name (optional)** If provided by your ISP, enter the Service Name.

**Connect on Demand: Max Idle Time** You can configure the HiPort+ 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 HiPort+ 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 HiPort+ will periodically check your Internet connection. If you are disconnected, then the HiPort+ 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 HiPort+ to check the Internet connection. The default Redial Period is **30** seconds.

### PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.

Internet Connection Type > PPTP

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**. Then configure the following:

**Internet IP Address** This is the HiPort+'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 HiPort+'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 Gateway Address, which is the ISP server's IP address.

**DNS** Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

**Server IP Address** Your ISP will provide you with the Server IP Address.

**User Name and Password** Enter the User Name and Password provided by your ISP.

**Connect on Demand: Max Idle Time** You can configure the HiPort+ 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 HiPort+ 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 HiPort+ will periodically check your Internet connection. If you are disconnected, then the HiPort+ will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default value is **30** seconds.

## L2TP

L2TP is a service that applies to connections in Israel only.

Internet Connection Type > L2TP

**Server IP Address** This is the IP address of the L2TP Server. Your ISP will provide you with the IP Address you need to specify here.

**User Name and Password** Enter the User Name and Password provided by your ISP.

**Connect on Demand: Max Idle Time** You can configure the HiPort+ 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 HiPort+ 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

## Optional Settings

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.

Optional Settings

**Router Name** Some ISPs require these names as identification. You may have to check with your ISP to see if your Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

**Host Name and Domain Name** Some ISPs require these names as identification. You may have to check with your ISP to see if your Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

**MTU** The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. To manually set a value, select **Manual** and enter the value desired in the *Size* field. You should leave this value in the 1200 to 1500 range. The default is **Auto**, which allows the HiPort+ to select the best MTU for your Internet connection.

## Network Setup

The Network Setup section allows you to change the settings on the network connected to the HiPort+'s Ethernet ports. Wireless Setup is performed through the Wireless tab.

### Router IP

The HiPort+'s Local IP Address and Subnet Mask are shown here. In most cases, you should keep the defaults.

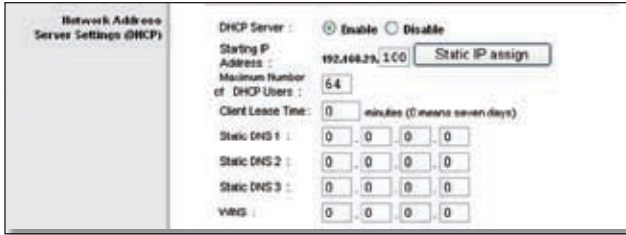
Local IP Address

**Local IP Address** The default value is **192.168.29.1**.

**Subnet Mask** The default value is **255.255.255.0**.

### DHCP Server Setting

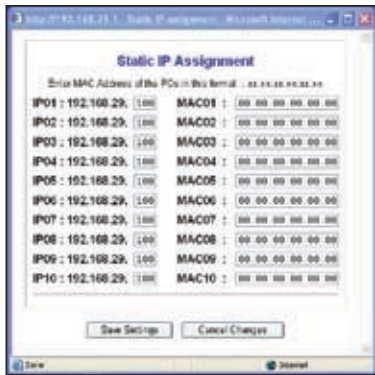
The HiPort+ can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the HiPort+ enabled as a DHCP server.



DHCP Server Setting

**DHCP Server** DHCP is enabled by factory default. If you already have a DHCP server on your network, set the HiPort+'s DHCP option to **Disable**. If you disable DHCP, remember to assign a static IP address to the HiPort+ on your computer.

While DHCP is enabled, if you want to assign a static IP address to a client, click **Static IP assign**, then enter the desired static IP address and the client's MAC address. Click **Save Settings** to save or **Cancel Changes** to cancel.



Static IP Assignment

**Starting IP Address** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the HiPort+ is 192.168.29.1, the Start IP Address must be 192.168.29.2 or greater, but smaller than 192.168.29.254. The default Start IP Address is **192.168.29.100**.

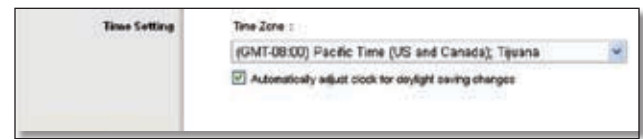
**Maximum Number of DHCP Users** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **64**.

**Client Lease Time** The Client Lease Time is the amount of time a network user will be allowed connection to the HiPort+ with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. 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. You can enter up to three DNS Server IP Addresses here. The HiPort+ will use these for quicker access to functioning DNS servers.

**WINS** The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

## Time Setting



Time Setting

**Time Zone** Select the time zone in which your network functions. If you want the HiPort+ to automatically adjust the clock for daylight savings, then select the check box.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## Setup > DDNS

The HiPort+ 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 HiPort+.

Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com. If you do not want to use this feature, keep the default setting, Disable.

## DDNS

### DDNS Service

If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. 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.



Setup &gt; DDNS &gt; DynDNS.org

### DynDNS.org

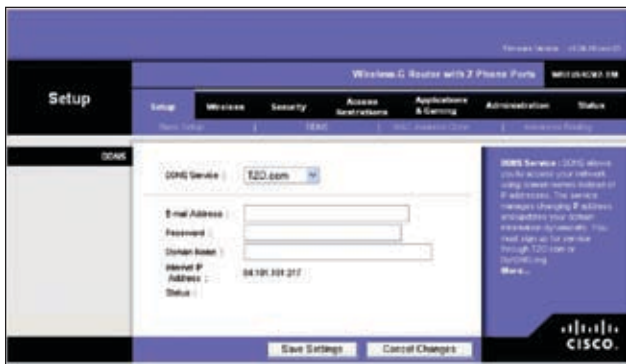
**User Name** Enter the user name from DynDNS.org.

**Password** Enter the password associated with the user name.

**Host Name** Enter the appropriate host name. The proper format is name.dyndns.org

**Internet IP Address** The current Internet IP address is displayed here.

**Status** The status of the DDNS service connection is displayed here.



Setup &gt; DDNS &gt; TZO.com

### TZO.com

**E-mail Address** Enter the e-mail address used to register with TZO.com.

**Password** Enter your TZO.com password.

**Domain Name** Enter your TZO.com domain name.

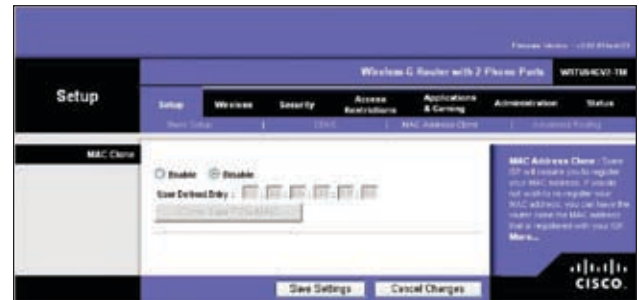
**Internet IP Address** The current Internet IP address is displayed here.

**Status** The status of the DDNS service connection is displayed here.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. For more information, click **Help**.

## Setup > MAC (Address) Clone

Every computer hardware device, including the network adapter of your computer has a unique code called a MAC address. Some Internet Service Providers (ISPs) require you to register this address with them 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 HiPort+'s with the MAC Clone feature.



Setup &gt; MAC Clone

### MAC Clone

**Enable/Disable** To enable MAC Address cloning, select **Enable**.

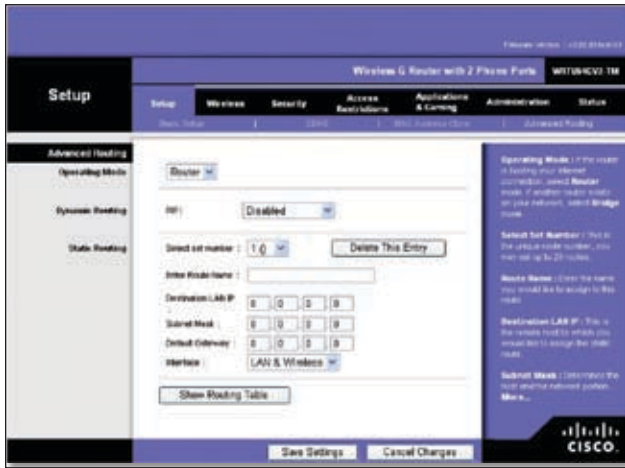
**User Defined Entry** Enter the MAC Address registered with your ISP here.

**Clone Your PC's MAC** Clicking this button will 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.

## Setup > Advanced Routing

The *Advanced Routing* screen allows you to configure the dynamic and static routing settings.



Setup > Advanced Routing > Router



Setup > Advanced Routing > Bridge

## Advanced Routing

### Operating Mode

If this HiPort+ is hosting your network's connection to the Internet, select **Router**. If another router exists on your network, select **Bridge**.

### Dynamic Routing

**RIP** This feature enables the HiPort+ to automatically adjust to physical changes in the network's layout and exchange routing tables with the other routers. The HiPort+ determines the network packets' route based on the fewest number of hops between the source and the destination.

**Disabled** This option disables the dynamic routing feature for all data transmissions.

**LAN & Wireless** This option enables dynamic routing for the LAN connection.

**WAN (Internet)** This option enables dynamic routing for the WAN side.

**Both** This option enables dynamic routing for the WAN and LAN connections.

### Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Use this feature to set up a static route between the HiPort+ and another network (you can have up to 20 static routes). To create a static route, alter the following settings:

**Select Set Number** Select the number of the static route from the drop-down menu.

**Delete This Entry** To delete a route, select its number from the drop-down menu, and click this button.

**Enter Route Name** Enter a name for the static route, using a maximum of 25 alphanumeric characters.

**Destination LAN IP** The Destination LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route.

**Subnet Mask** The Subnet Mask determines which portion of a Destination 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 HiPort+ and the remote network or host.

**Interface** Select LAN or WAN (Internet), depending on the location of the final destination.

**Show Routing Table** Click **Show Routing Table** to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this screen.

Destination LAN IP	Subnet Mask	Gateway	Interface
64.831.161.0	255.255.255.0	0.0.0.0	WAN (Internet)
192.168.24.0	255.255.255.0	0.0.0.0	LAN & Wireless
223.0.0.0	223.0.0.0	0.0.0.0	LAN & Wireless
0.0.0.0	0.0.0.0	64.831.161.1	WAN (Internet)

Advanced Routing > Routing Table

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## Wireless > Basic Wireless Settings

The basic settings for wireless networking are set on this screen.



Wireless > Basic Wireless Settings

### Wireless Network

**Wireless Network Mode** From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, Mixed. If you have only 802.11g devices, select G-Only. If you have only 802.11b devices, select B-Only. If you do not have any 802.11g and 802.11b devices in your network, select Disable..

**Wireless 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 keyboard characters. Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name.

**Wireless Channel** Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

**Wireless SSID Broadcast** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the HiPort+. To broadcast the HiPort+'s SSID, keep the default setting, Enable. If you do not want to broadcast the HiPort+'s SSID, then select Disable.

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

## Wireless > Wireless Security

The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the HiPort+: 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. WPA2 is a more advanced, more secure version of WPA. WEP stands for Wired Equivalent Privacy, and RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the HiPort+, refer to "Chapter 2: Wireless Security."

### Wireless Security

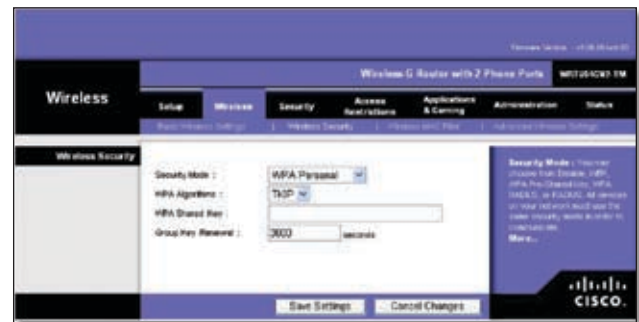
#### Security Mode

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

#### WPA Personal



**NOTE:** If you are using WPA, always remember that each device in your wireless network **MUST** use the same WPA method and shared key, or else the network will not function properly.



Security Mode > WPA Personal

**WPA Algorithm** WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**WPA Shared Key** Enter the key shared by the HiPort+ and your other network devices. It must have 8-63 characters.

**Group Key Renewal** Enter a Key Renewal period, which tells the HiPort+ how often it should change the encryption keys. The default Group Key Renewal period is **3600** seconds.

#### WPA Enterprise

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS



server is connected to the HiPort+.)



Security Mode > WPA Enterprise

**WPA Algorithm** WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**RADIUS Server Address** Enter the IP Address of the RADIUS server.

**RADIUS Port** Enter the port number of the RADIUS server. The default value is **1812**.

**Shared Key** Enter the key shared between the HiPort+ and the server.

**Key Renewal Timeout** Enter a Key Renewal Timeout period, which instructs the HiPort+ how often it should change the encryption keys. The default Key Renewal Timeout period is **3600** seconds.

### WPA2 Personal



Security Mode > WPA2 Personal

**WPA Algorithm** WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. The default selection is **AES**.

**WPA Shared Key** Enter a WPA Shared Key of 8-63 characters.

**Group Key Renewal** Enter a Group Key Renewal period, which instructs the HiPort+ how often it should change the encryption keys. The default Group Key Renewal period is **3600** seconds.

### WPA2 Enterprise

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the HiPort+.)



Security Mode > WPA2 Enterprise

**WPA Algorithm** WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. The default selection is **AES**.

**RADIUS Server Address** Enter the IP Address of the RADIUS server.

**RADIUS Port** Enter the port number of the RADIUS server. The default value is **1812**.

**Shared Key** Enter the key shared between the HiPort+ and the server.

**Key Renewal Timeout** Enter a Key Renewal Timeout period, which instructs the HiPort+ how often it should change the encryption keys. The default Key Renewal Timeout period is **3600** seconds.

### RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the HiPort+.)



Security Mode > RADIUS



**IMPORTANT:** If you are using WEP encryption, always remember that each device in your wireless network **MUST** use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

**RADIUS Server Address** Enter the IP Address of the RADIUS server.

**RADIUS Port** Enter the port number of the RADIUS server. The default value is **1812**.

**Shared Key** Enter the key shared between the HiPort+ and the server.

**Default Transmit Key** Select a Default Transmit Key (choose which Key to use). The default is **1**.

**WEP Encryption** Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

**Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

**Key 1-4** If you did not enter a Passphrase, enter the WEP key(s) manually.

## WEP

WEP is a basic encryption method, which is not as secure as WPA.



Security Mode > WEP

**Default Transmit Key** Select a Default Transmit Key (choose which Key to use). The default is **1**.

**WEP Encryption** Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

**Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

**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 access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.



Wireless > Wireless MAC Filter

## Wireless MAC Filter

**Wireless MAC Filter** To filter wireless users by MAC Address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC Address, keep the default setting, **Disable**.

**Prevent** Select this to block wireless access by MAC Address. This button is selected by default.

**Permit Only** Select this to allow wireless access by MAC Address. This button is not selected by default.

**Edit MAC Filter List** Click this to open the *MAC Address Filter List* screen. On this screen, you can list users, by MAC Address, to whom you wish to provide or block access. For easy reference, click **Wireless Client MAC List** to display a list of network users by MAC Address.



MAC Address Filter List

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

## Wireless > Advanced Wireless Settings

This *Wireless > Advanced Wireless Settings* screen is used to set up the HiPort+'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

**Authentication Type** 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.

**Basic Rate** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the HiPort+ can transmit. The HiPort+ will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The HiPort+ will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the HiPort+ can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the HiPort+ can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the HiPort+'s rate of data transmission, configure the Transmission Rate setting.

**Transmission Rate** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the HiPort+ automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the HiPort+ and a wireless client. The default value is **Auto**.

**CTS Protection Mode** CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able to transmit to the HiPort+ in an environment with heavy 802.11b traffic. This function boosts the HiPort+'s ability to catch all Wireless-G transmissions but will severely decrease performance.

**Beacon Interval** The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the HiPort+ to synchronize the wireless network.

**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 HiPort+ has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its client 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 HiPort+ 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**.

**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 HiPort+ but not with each other. To use this function, select **On**. AP Isolation is turned **Off** by default.

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

## Security > Firewall

The *Firewall* screen offers a firewall and filters that block specific Internet data types.



Security > Firewall

### Firewall

**Firewall Protection** A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network. Select **Enable** to use a firewall, or **Disable** to disable it.

### Block WAN Requests

**Block Anonymous Internet Requests** When enabled, this feature keeps your network from being “pinged,” or detected, by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network. This filter is enabled by default. Select **Disable** 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 HiPort+ will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enable** to filter multicasting, or **Disable** to disable this feature.

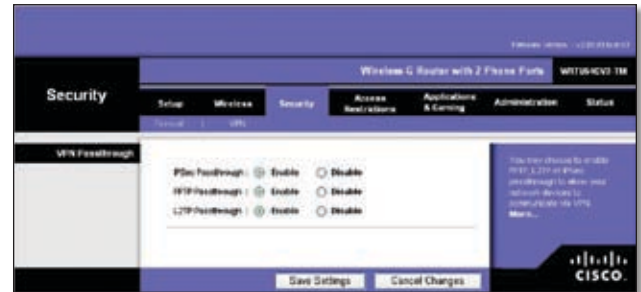
**Filter Internet NAT Redirection** This feature uses port forwarding to block access to local servers from local networked computers. Select **Enable** to filter Internet NAT redirection, or **Disable** to disable this feature.

**Filter IDENT (Port 113)** This feature keeps port 113 from being scanned by devices outside of your local network. Select **Enable** to filter port 113, or **Disable** to disable this feature.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## Security > VPN

The *VPN Passthrough* screen allows you to allow VPN tunnels using IPsec, L2TP, or PPTP protocols to pass through the HiPort+.



Security > VPN

### VPN Passthrough

**IPSec Passthrough** IPsec (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click **Enable**. To disable IPSec Passthrough, click **Disable**.

**PPTP Passthrough** PPTP (Point-to-Point Tunneling Protocol) Passthrough allows the Point-to-Point (PPP) to be tunneled through an IP network. To allow PPTP Passthrough, click **Enable**. To disable PPTP Passthrough, click **Disable**.

**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 HiPort+, click **Enable**. To disable L2TP Passthrough, click **Disable**.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## 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, websites, and inbound traffic during specific days and times.



Access Restrictions > Internet Access

## Internet Access

**Internet Access Policy** Internet access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down 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**.

On the *Summary* screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, click the Enabled check box. To delete a policy, click its Delete button. 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**.

**Status** Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click **Enable**.

To create a policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click **Enable**.
3. Enter a Policy Name in the field provided.
4. Click **Edit List of PCs** to select which PCs will be

affected by the policy. The *List of PCs* screen will appear. 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.

5. After making your changes, click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes.



Internet Access Policy > List of PCs

6. Click 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.
7. 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**.
8. You can block websites with specific URL addresses. Enter each URL in a separate field next to *Website Blocking by URL Address*.
9. You can also block websites using specific keywords. Enter each keyword in a separate field next to *Website Blocking by Keyword*. You can filter access to various services accessed over the Internet, such as FTP or Telnet. (You can block up to two applications per policy.)
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. Then click **Add**.  
To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click **Modify**.  
To delete a service, select it from the Application list. Then click **Delete**.

Click **Save Settings** to save the policy's settings. To cancel the policy's settings, click **Cancel Changes**. Help information is available on the right side of the screen.

## Applications & Gaming > Port Range Forward

Port range forwarding sets 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 HiPort+ 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).

If you need to forward all ports to one PC, click the *DMZ* tab.



Applications & Gaming > Port Range Forward

### Port Range Forward

To add an application, complete the following fields:

**Application Name** Enter the name of the application.

**Start to End Port** Enter the number or range of port(s) used by the server or Internet application. Check with the Internet application documentation for more information.

**Protocol** Select the protocol **TCP** or **UDP**, or select **Both**.

**IP Address** Enter the IP address of the server that you want the Internet users to be able to access.

**Enable** Click the **Enable** check box to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## Applications & Gaming > Port Triggering

This screen instructs the HiPort+ to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the HiPort+, so that when the requested data returns through the HiPort+, the data is sent to the proper computer by way of IP address and port mapping rules.



Applications & Gaming > Port Range Triggering

### Port Triggering

To add an application, complete the following fields:

**Application** Enter the name of the application.

**Triggered Range** Enter the starting and ending port numbers of the triggered port range. Check with the Internet application documentation for the port number(s) needed.

**Forwarded Range** Enter the starting and ending port numbers of the forwarded port range. Check with the Internet application documentation for the port number(s) needed.

**Enable** Click the **Enable** check box to enable the applications you have defined. This is disabled (unchecked) by default.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## Applications & Gaming > DMZ

The DMZ screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding 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.

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.



Applications & Gaming > DMZ

## DMZ

This feature completely exposes a designated computer to the Internet. To use this feature, select **Enable**. To disable DMZ hosting, select **Disable**.

**DMZ Host IP Address** Complete the IP address in the field provided.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## 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.

There are three types of QoS available: Device Priority, Ethernet Port Priority, and Application Priority.

### QoS

**Enable/Disable** To enable QoS, select **Enable**. Otherwise, select **Disable**. QoS is disabled by default.

**Uplink Bandwidth** Displays the outgoing bandwidth that applications can utilize.



Applications & Gaming > QoS

## Wired QoS

### Device Priority

Enter the name of your network device in the *Device name* field, enter its MAC Address, and then select its priority from the drop-down menu.

### Ethernet Port Priority

Ethernet Port Priority QoS allows you to prioritize performance for the HiPort+'s four ports, LAN Ports 1-4. For each port, select the priority and flow control setting.

**Priority** Select **High** or **Low** in the Priority column. The HiPort+'s four ports have been assigned low priority by default.

**Flow Control** If you want the HiPort+ to control the transmission of data between network devices, select **Enabled**. To disable this feature, select **Disabled**. Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports LAN ports 1-4 are in your network. This feature is enabled by default.

### Application Priority

Application Priority QoS manages information as it is transmitted and received. Depending on the settings of the QoS screen, this feature will assign information a high or low priority for the applications that you specify.

**Optimize Gaming Applications** Select this to automatically allow common game application ports to have a higher priority. These games include, but are not limited to: *Counter-Strike*, *Half-Life*, *Age of Empires*, *EverQuest*, *Quake2/Quake3*, and *Diablo II*. The default setting is unselected.

**Application Name** Enter the name you wish to give the application in the *Application Name* field.

**Priority** You can assign priority to the application from the drop down menu. The options are **Low**, **Medium**, **High** and **Highest**. The default is **Low**.

**Specific Port #** Enter the port number for the application.

### Wireless QoS

**WMM Support** Wi-Fi Multimedia (WMM), formerly known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance certified feature, based on the IEEE 802.11e standard. This feature provides QoS to wireless networks. It is especially suitable for voice, music and video applications; for example, Voice over IP (VoIP), video streaming, and interactive gaming. If you have other devices on your wireless network that support WMM, keep the default, **Enable**.

**No Acknowledgement** This feature prevents the HiPort+ from re-sending data if an error occurs. To use this feature, select **Enable**. Otherwise keep the default setting, **Disable**.

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

## Administration > Management

When you click the **Administration** tab, you will see the Management screen. This screen allows you to change the HiPort+'s access settings and configure the UPnP (Universal Plug and Play) features. You can also back up and restore the HiPort+'s configuration file.

### Management



Administration > Management

### Router Password

#### Local Router Access

To ensure the HiPort+'s security, you will be asked for your password when you access the HiPort+'s web-based utility. The default password is **admin**.

**Password and Re-enter to Confirm** It is recommended that you change the default password to one of your choice. Enter a new HiPort+ password and then enter it again in the *Re-enter to Confirm* field.

#### Web Access

**Access Server** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**.

**Wireless Access Web** If you are using the HiPort+ in a public domain where you are giving wireless access to your guests, you can disable wireless access to the HiPort+'s web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Keep the default, **Enable**, to enable wireless access to the HiPort+'s web-based utility, or select **Disable** to disable wireless access to the utility.



## Remote Router Access

**Remote Management** To permit remote access of the HiPort+, from outside the local network, select **Enable**. Otherwise, keep the default setting, **Disable**.

**Management Port** Enter the port number that will be open to outside access.

**Use HTTPS** HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. To enable HTTPS, select the check box.



**NOTE:** When you are in a remote location and wish to manage the HiPort+, enter `http://<Internet IP Address>:port` or `https://<Internet IP Address>:port`, depending on whether you use HTTP or HTTPS. Enter the HiPort+'s specific Internet IP address in place of `<Internet IP Address>`, and enter the Administration Port number in place of the word `port`.

## UPnP

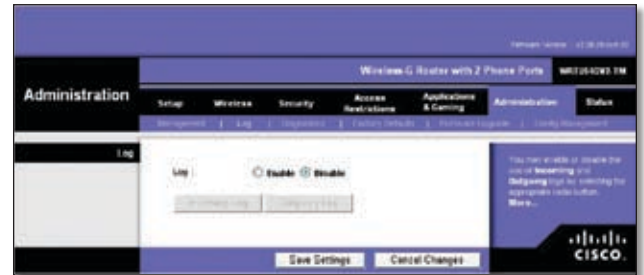
Universal Plug and Play (UPnP) allows Windows 2000, XP and Vista to automatically configure the HiPort+ for various Internet applications, such as gaming and video conferencing.

**UPnP** If you want to use UPnP, keep the default setting, **Enable**. Otherwise, select **Disable**.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is available on the right side of the screen.

## Administration > Log

When you click the Administration tab, you will see the *Log* screen. It provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.



Administration > Log

## Log

**Log** To access activity logs, select **Enable**. With logging enabled, you can choose to view temporary logs. Click **Disable** to disable this function.

**Incoming Log** The Incoming Log will display a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic.



Log > Incoming Log

**Outgoing Log** The Outgoing Log will display a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic.



Log > Outgoing Log

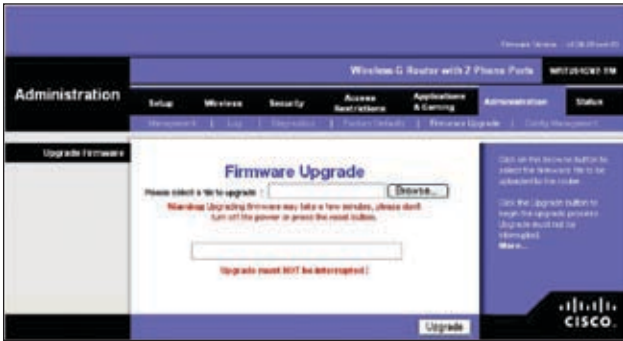
Click **Refresh** to update the log.

When you have finished making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. Help information is



## Administration > Firmware Upgrade

The *Firmware Upgrade* screen allows you to upgrade the HiPort+'s firmware. Do not upgrade the firmware unless you are experiencing problems with the HiPort+ or the new firmware has a feature you want to use.



Administration > Firmware Upgrade

Before upgrading the firmware, download the HiPort+'s firmware upgrade file from the Linksys Website, [www.linksys.com](http://www.linksys.com). Then extract the file.

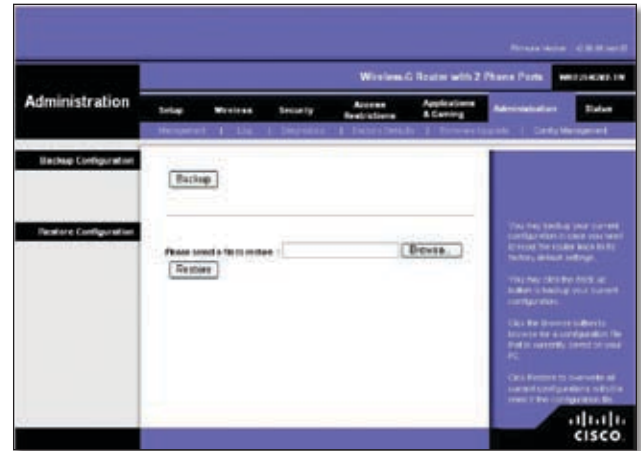
### Upgrade Firmware

**Please Select a File to Upgrade** In the field provided, enter the name of the extracted firmware upgrade file, or click **Browse** to locate the file.

**Upgrade** After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Help information is shown on the right-hand side of the screen.

## Administration > Config Management



Administration > Config Management

### Backup Configuration

Click this button to backup the current configuration settings of the HiPort+.

### Restore Configuration

Click this option to overwrite the current configuration settings with the configuration settings from the specified file.

**Please select a file to restore** In the field provided, enter the name of the backup file, or click **Browse** to search for the file.

## Status > Router

The *Router* screen displays information about the HiPort+ and its current settings. The on-screen information will vary depending on the Internet Connection Type selected on the Setup screen.



Status > Router

## Router Information

**Firmware Version** This is the version number of the HiPort+'s current firmware.

**Current Time** This shows the time set on the HiPort+.

**MAC Address** This is the HiPort+'s MAC address, as seen by your ISP.

**Router Name** If required by your ISP, this was entered on the Basic Setup screen.

**Domain Name** If required by your ISP, this was entered on the Basic Setup screen.

## Internet

### Configuration Type

**Login Type** This indicates the type of Internet connection you are using.

For dial-up style connections such as PPPoE or PPTP, there is a **Connect** button to click if there is no connection and you want to establish an Internet connection.

**IP Address** The HiPort+'s Internet IP address is displayed here.

**Subnet Mask and Default Gateway** The HiPort+'s Subnet Mask and Default Gateway address are displayed here for DHCP and static IP connections.

**DNS1-3** Shown here are the DNS (Domain Name System) IP addresses currently used by the HiPort+.

**MTU** Shown here is the MTU (Maximum Transmission Unit) setting for the HiPort+.

**DHCP Release** Available for a DHCP connection, click this button to release the current IP address of the device connected to the HiPort+'s Internet port.

**DHCP Renew** Available for a DHCP connection, click this button to replace the current IP address—of the device connected to the HiPort+'s Internet port—with a new IP address.

Click **Refresh** to update the on-screen information. Help information is available on the right side of the screen.

## Status > Local Network

The Local Network screen displays information about the local network.



Status > Local Network

## Local Network

**MAC Address** The MAC Address of the HiPort+'s local interface is displayed here.

**IP Address** This shows the HiPort+'s IP address, as it appears on your local network.

**Subnet Mask** The HiPort+'s Subnet Mask is shown here.

**DHCP Server** The status of the HiPort+'s DHCP server function is displayed here.

**Start IP Address** For the range of IP addresses used by devices on your local network, the beginning IP address is shown here.

**End IP Address** For the range of IP addresses used by devices on your local network, the ending IP address is shown here.