User Guide

Linksys E2000 | Advanced Wireless-N Router

Contents

Chapter 1: Product Overview

Thank you for choosing the Linksys E2000 Advanced Wireless-N Router. 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 Wi-Fi Protected Access 2 (WPA2) security, a Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology.

Setup and use of the Router is easy using Cisco Connect, the software that is installed when you run the included CD. Advanced configuration of the Router is available through the provided browser-based utility.

Top

1, 2, 3, 4 (Green/Blue) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. The LED is continuously lit when the Router is connected to a device through that port. It flashes to indicates network activity over that port. Green indicates Gigabit speeds, and blue indicates 10/100 speeds.

Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use the Wi-Fi Protected Setup button to automatically configure wireless security for your wireless network(s).

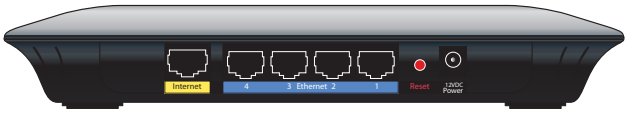
To use Wi-Fi Protected Setup, refer to **Wi-Fi Protected Setup**, **page 23**.

Wireless (Blue) The Wireless LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network.

Internet (Blue) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port.

Power (Blue) The Power LED lights up when the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, the LED flashes. When the diagnostic is complete, the LED is continuously lit.

Back



Internet Using an Ethernet cable (also called a network or Internet cable), this Gigabit port connects the Router to your Internet connection, which is typically a cable or Digital Subscriber Line (DSL) modem.

4, 3, 2, 1 Using Ethernet cables, these Gigabit Ethernet ports (4, 3, 2, 1) connect the Router to computers and other Ethernet network devices on your wired network.

Reset 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 *Administration* > *Factory Defaults* in the Router's browser-based utility.

Power The Power port connects to the included power adapter.

Placement Positions

There are two ways to physically install the Router. The first way is to place the Router horizontally on a surface. The second way is to mount the Router on a wall.

Horizontal Placement

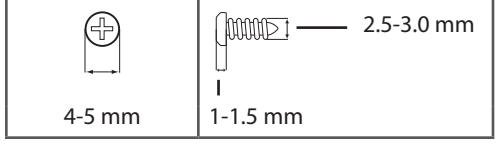
The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet.

Wall-Mounting Placement

The Router has two wall-mount slots on its bottom panel. The distance between the slots is 152 mm (6 inches).

Two screws are needed to mount the Router.

Suggested Mounting Hardware

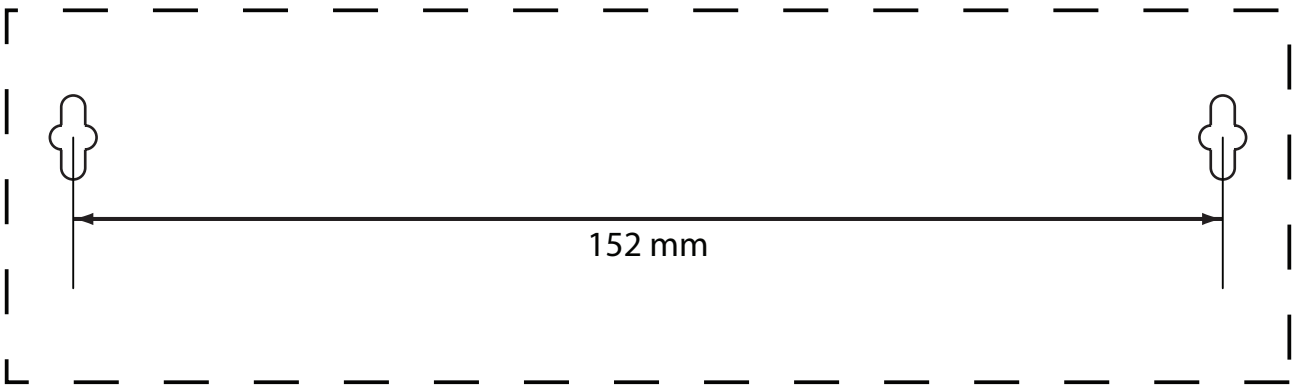


†Note: Mounting hardware illustrations are not true to scale.

NOTE: Cisco is not responsible for damages incurred by insecure wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical 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 (0.12 inches) of its head exposed.
4. 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.



Print this page at 100% size.

Cut along the dotted line, and place on the wall to drill precise spacing.

Wall Mounting Template

Chapter 2: Cisco Connect

During installation, the setup software installs Cisco Connect on your computer. Cisco Connect offers options to connect additional computers or devices to the Router and allows you to change the Router's settings.

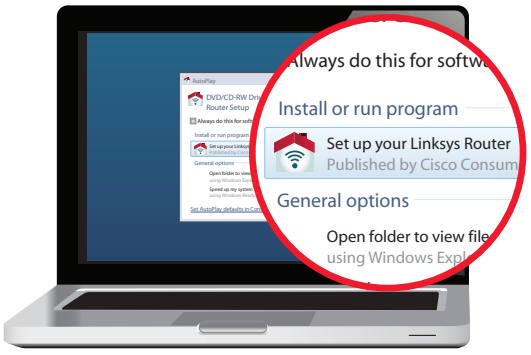
Installation

To install the Router:

1. Insert the CD into your CD-ROM drive.

Insert CD

2. Click **Set up your Linksys Router**.



Set Up Your Linksys Router

If you do not see this, access setup on the CD directly. To do so, perform the following steps for your specific operating system:

Windows 7

a. Go to **Start > Computer**.

b. Double-click your CD-ROM drive.

Windows Vista

c. Go to **Start > Computer**.

d. Double-click your CD-ROM drive.

Windows XP

a. Go to **Start > My Computer** and select your CD-ROM drive.

b. Double-click **Setup.exe**.

Mac OS X

a. Double-click the CD on your desktop.

b. Double-click **Setup**.

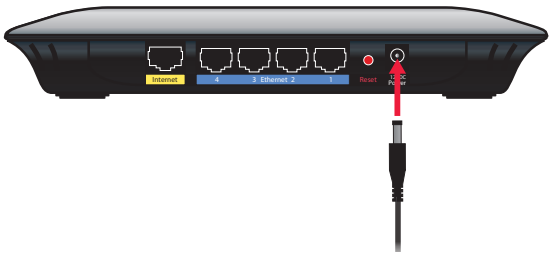
3. Read the Software End User License Agreement. To accept the agreement and continue with the installation, click **Next**.

License Agreement

4. The connection steps are displayed.

Connection Overview

a. Plug the power cord into the Power port on the back of the Router.

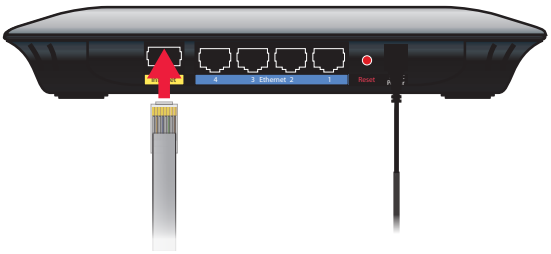


Connect to Power Port

b. Plug the power adapter into an electrical outlet.

Connect to Electrical Outlet

c. Unplug the existing Ethernet cable from your computer and plug it into the yellow port labeled **Internet** on the back of the Router. Click **Next**.



Connect Ethernet Cable

NOTE: You can view detailed connection steps by clicking Show me how in the setup software.

NOTE: If the setup software detects multiple routers, then select the serial number of your Router. The serial number is located on the left side of the product label, which is on the bottom of the Router.

5. Please wait while the setup software is setting up the Router.

Please Wait

6. The installation is complete. Click **OK**.

Installation is Complete

NOTE: If you have any problems during the installation process, refer to the Frequently Asked Questions in the setup software, or use a computer with an active Internet connection to visit **www.linksys.com/support**.

Main Menu

When Cisco Connect starts up, the main menu appears:

Main Menu

Status information is displayed in the upper right corner:

- online secure
  Your local network is secure, and your Internet connection is available.
- offline secure
  Your local network is secure; however, your Internet connection is not available. To repair your Internet connection, follow the on-screen instructions.

NOTE: A group of computers or other devices connected to a router is a local network. The router allows the networked devices to communicate with each other.

The main menu offers four options: Computers and devices, Parental controls, Guest access, and Router settings.

NOTE: To view the FAQs for more information, click **Need help?**

Local Access versus Guest Access

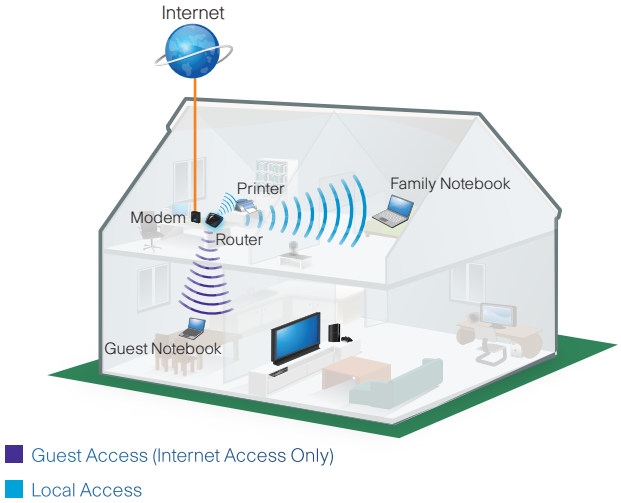
You can connect computers or devices to your Router by giving them local access (*Computers and devices* option)or guest access (*Guest access* option).

Computers and devices with local access will have access to the Internet and to other devices on your local network, including shared computers and printers that are connected to the Router. Local access can be given to a wired or wireless device. Refer to **Computers and Other Devices**, **page 9** for more information.

Guest access allows you to provide guests visiting your home with Internet access. Your guests will not have access to your other computers or personal data. Provide your guest with the guest network name and password. Guest computers must connect to your network using a wireless network connection. Refer to **Main Menu – Guest Access**, **page 8** and **Guest Access**, **page 13** for more information.

The following diagram shows a typical example of how local access and guest access are used in the same home.

Guest Access versus Local Access Diagram



Main Menu – Computers and Devices

Use this option to connect another computer or device to the Router.

There is x device(s) connected to your router The number of devices connected to the Router is displayed.

Add device To connect another computer or device to the Router, click **Add device** and go to **Computers and Other Devices**, **page 9**.

Main Menu – Parental Controls

Parental controls restrict Internet access for up to five computers. For the computers you select, you can block or limit Internet access to specific times. You can also block specific websites.

Parental controls restrictions are being applied to x device(s) The number of devices with parental controls restrictions is displayed.

Change To enable parental controls or change settings, click **Change** and go to **Parental Controls**, **page 11**.

Main Menu – Guest Access

Guest access provides Internet access only; it does not provide access to the local network and its resources. For example, the guest computer cannot print to a printer on the local network or copy files to a computer on the local network.

Guest access helps minimize exposure of your local network. To grant Internet access to friends or family, provide the guest network name and password displayed on this screen.

Guests can connect to x-guest using the password xyz When a guest wants Internet access in your home, have the guest do the following:

1. Connect to the wireless guest network, which is the name of your wireless network followed by **-guest**.
2. Open a web browser.
3. On the login screen, enter the password of your guest network. Then click **Login**.

Change To disable guest access or change settings, click **Change** and go to **Guest Access**, **page 13**.

Main Menu – Router Settings

Use this option to personalize the Router's settings.

Router name is x The name of the Router is displayed.

Change To change settings, click **Change** and go to **Router Settings**, **page 13**.

Computers and Other Devices

The *Computers and other devices* screen appears.

Computers and Other Devices

Computer Click this option to connect another computer in your home. Go to **Computer**, **page 9**.

Wireless printer Click this option to connect a wireless printer. Go to **Wireless Printer**, **page 10**.

Other devices Click this option to connect a device that is not a computer, such as a smartphone or game console. Go to **Connect Manually**, **page 10**.

Computer

You can use a USB flash drive to create an Easy Setup Key, which holds the wireless settings for the Router. Then you can use the Easy Setup Key to connect additional computers to the Router. Select the appropriate option:

Yes, I have an Easy Setup Key If you already have an Easy Setup Key, select this option. Click **Next** and go to **Connect with the Easy Setup Key**, **page 9**.

No, I don't have an Easy Setup Key — create a new one now If you want to create or update an Easy Setup Key, select this option. Click **Next** and go to **Create or Update the Easy Setup Key**, **page 10**.

I want to connect manually using my wireless settings If you want to connect manually (without an Easy Setup Key), select this option. Click **Next** and go to **Connect Manually**, **page 10**.

Do You Have an Easy Setup Key?

Connect with the Easy Setup Key

1. Insert the Easy Setup Key into an available USB port on the computer that you want to connect to the Router.

Connecting Another Computer

2. On that computer, click **Connect to your Linksys Router**. (If you do not see this, access the Easy Setup Key through Windows Explorer or the Finder, and double-click **Connect**.)

   Follow the on-screen instructions to connect that computer to the Router.

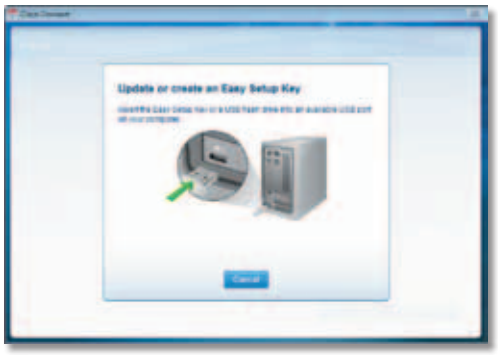
3. Come back to this computer. On the *Connecting another computer* screen, click **Next**.
4. Enter a name that will be used to identify the newly added computer. Then click **Finish**.

Name Your Device

Create or Update the Easy Setup Key

If you do not have an Easy Setup Key, then you can create one using a USB flash drive. If you already have an Easy Setup Key, then you can update it with the Router's current settings.

1. Insert the Easy Setup Key or a USB flash drive into an available USB port on your computer.

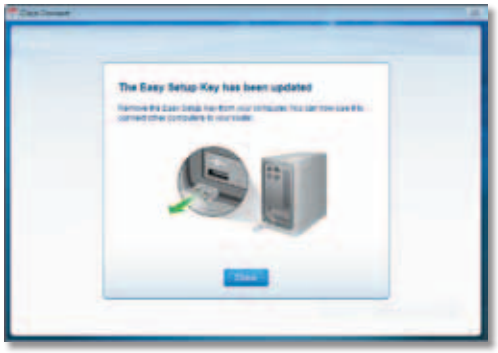


Update or Create an Easy Setup Key

2. Please wait while settings are copied to the Easy Setup Key.

Copying Files to the Easy Setup Key

3. Remove the Easy Setup Key. You can now use it to connect other computers to the Router (for more information, refer to **Connect with the Easy Setup Key**, **page 9**). Click **Close**.



Easy Setup Key Has Been Updated

Connect Manually

1. Enter the *Network name (SSID)*, *Security Key*, and *Security Type* settings on your wireless device (SSID stands for Service Set Identifier). To print this information, click **Print these settings**.

Connecting a Device

2. After your device connects, click **Next**.
3. Enter a name that will be used to identify this device. Then click **Finish**.

Name Your Device

Wireless Printer

1. Refer to your printer's documentation to learn how to connect it to a wireless printer.
2. Enter the *Network name (SSID)*, *Security Key*, and *Security Type* settings on your wireless printer. To print this information, click **Print these settings**.

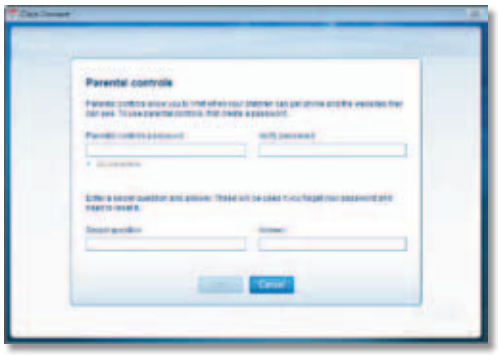
Connecting a Wireless Printer

3. Wait until your printer connects. On the *Connecting a wireless printer* screen, click **Next**.
4. Enter a name that will be used to identify this printer. Then click **Finish**.

Name Your Printer

Parental Controls

The *Parental controls* screen appears.



Parental Controls Password

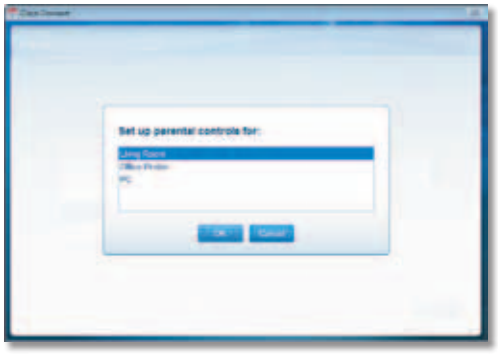
First-Time Access of Parental Controls

1. The first time you access parental controls, you will be asked to set up a parental controls password. Complete the following:

- **Parental controls password** This password protects access to parental controls. Create a password of 4-32 characters.
- **Verify password** Re-enter the password.
- **Secret question** Create a secret question and answer pair. If you forget the password, you can reset it by correctly answering the secret question. Enter your question.
- **Answer** Enter the answer to your secret question.

Click **OK** to save your settings.

2. Select the computer whose parental controls you want to set up. Then click **OK**.



Set Up Parental Controls For

3. The *Parental controls* main screen appears.

Parental Controls

You have the following options:

Restrict Internet access on The list of computer(s) you have selected for parental controls is displayed. To add, remove, or rename computers on this list, refer to **Restrict Internet Access List**, **page 12**. To set up parental controls on a computer, refer to **Set Up Parental Controls**, **page 12**.

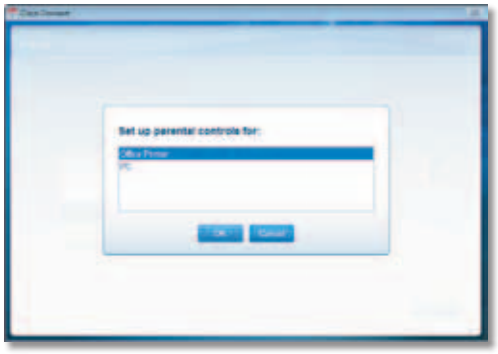
Change parental controls password Click this option to change the password that protects access to parental controls. Refer to **Change Parental Controls Password**, **page 13**.

Restrict Internet Access List

Parental Controls

Add If you want to apply parental controls to additional computers, click **Add**.

If you clicked **Add**, the *Set up parental controls for* screen appears.



Set Up Parental Controls For

Select the computer whose parental controls you want to set up. Then click **OK**.

Remove If there is a computer that should not have parental controls applied, select the computer and click **Remove**.

Rename To give a computer a new name, select the computer and click **Rename**.

If you clicked **Rename**, the *Rename the device* screen appears.

Rename the Device

Enter the new name. Then click **Rename**.

Set Up Parental Controls

To set up parental controls for a computer, follow these instructions:

1. Select the computer from the *Restrict Internet access on* list. (If the computer is not listed, click **Add** to select the computer.)

Parental Controls

2. The *Block Internet access* option offers the following:

- **Always** To always block Internet access, select this option.
- **Specific times** To block Internet access during specific days and times, select this option and set the schedule:
  - **School nights** Select the appropriate start and end times.
  - **Weekends** Select the appropriate start and end times
- **Never** To always allow Internet access, keep the default, **Never**.

3. For the *Block specific sites* option, click **Edit** to create a list of websites you want to block. By default, the list is empty.

   If you clicked **Edit**, the *Block these sites* screen appears.

Block These Sites

   a. Enter a website address on each line.

   b. Click **Save** to save your settings.

4. On the *Parental controls* screen, click **Finish** to save your settings.

NOTE: Repeat steps 1-4 to set up parental controls for different computers.

Change Parental Controls Password

If you clicked **Change parental controls password**, the *Change your parental controls password* screen appears.

Change Your Parental Controls Password

- **Old password** Enter the old password.
- **New password** Enter a new password of 4-32 characters.
- **Verify password** Re-enter the new password.

Click **Change** to save your setting.

Guest Access

The *Guest access settings* screen appears.

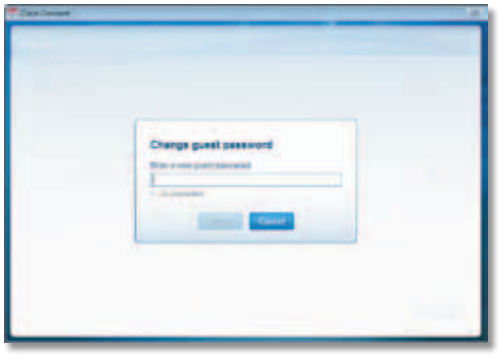
Guest Access Settings

Allow guest access By default, guest access is enabled. To disable guest access, select **no**.

Guest network name By default, the setup software sets up the name of the guest network.

Password By default, the setup software sets up the password for the guest network. To change the password, click **Change**.

If you clicked **Change**, the *Change guest password* screen appears.



Change Guest Password

- **Enter a new guest password** Enter a password of 4-32 characters.
- Click **Change** to save your setting.

Total guests allowed By default, **5** guests are allowed Internet access through the guest network. Select the appropriate number of guests allowed on your guest network; you can select up to 10 guests.

Click **Finish** to save your settings.

Router Settings

The *Router settings* screen appears.

Router Settings

Personalize

Router name The name of the Router is displayed (this is also the name of your wireless network). To change the name, click **Change** and go to **Change Router Name or Password**, **page 14**.

Password The password that protects access to the Router's settings is displayed (this also protects wireless access to your local network). To change the password, click **Change** and go to **Change Router Name or Password**, **page 14**.

Easy Setup Key

Update or create key The Easy Setup Key is a USB flash drive that holds the wireless settings for the Router. If you want to create or update an Easy Setup Key, click this option and go to **Create or Update the Easy Setup Key**, **page 10**.

Other Options

Register now to receive special offers and updates To sign up to receive special offers and updates, click this option.

Router details To view more information about the Router, click this option and go to **Router Details**, **page 14**.

Advanced settings To access settings for advanced users, click this option and go to **Advanced Settings**, **page 15**.

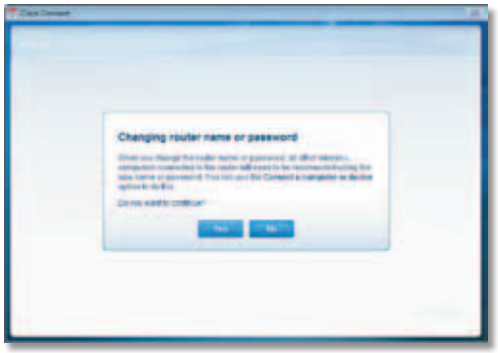
Click **Finish** to save your settings.

Change Router Name or Password

NOTE: If you change the Router name or password, you also change the name or password of your wireless network. The wireless computers or other devices connected to the Router will need to be reconnected using the new name or password (for more information, refer to **Computers and Other Devices**, **page 9**).

If you clicked **Change**, the *Changing router name or password* screen appears.

1. To change the Router name or password, click **Yes**. Otherwise, click **No**.



Changing Router Name or Password

2. Complete the following:

- **Router name** Enter a name of 1-32 characters.
- **Password** Enter a password of 8-63 characters.
- Click **Change** to save your settings.

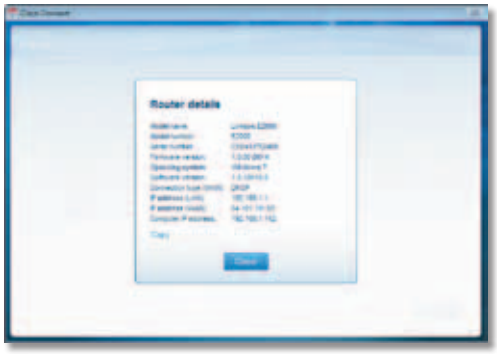
Change Router Name and Password

Router Details

The *Router details* screen appears, displaying the Model name, Model number, Serial number, Firmware version, Operating system, Software version, Connection type (WAN), IP address (LAN), IP address (WAN), and Computer IP address. (WAN stands for Wide Area Network, such as the Internet. IP stands for Internet Protocol. LAN stands for Local Area Network.)

Copy To copy the details to a text file, click **Copy** and follow these instructions:

1. Open a text editor, such as Microsoft Word or Notepad.
2. Go to **Edit > Paste**.
3. Go to **File > Save**.



Router Details

Click **Close** to return to the *Router settings* screen.

Advanced Settings

If you are an advanced user familiar with router administration, you can access the browser-based utility to use the advanced configuration settings of the Router.

Username Enter this username to access the browser-based utility.

Password Enter this password to access the browser-based utility.

Copy password To copy the password to the Clipboard, click this option.

Advanced Settings

Click **OK** to open the web browser and access the browser-based utility. For more information, refer to **How to Access the Browser-Based Utility**, **page 16**.

How to Exit Cisco Connect

To exit Cisco Connect, click **Close** on the main menu.

Main Menu

How to Access Cisco Connect

Windows

To access Cisco Connect, go to **Start > All Programs > Cisco Connect**.

Mac

To access Cisco Connect, go to **Go > Applications > Cisco Connect**.

Chapter 3: Advanced Configuration

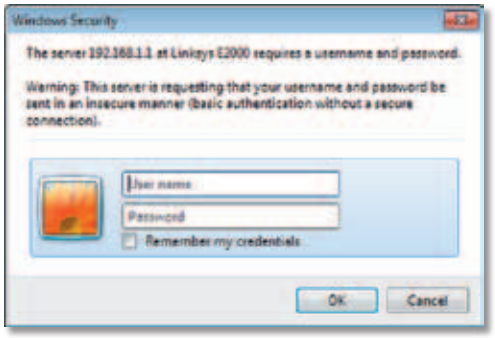
After setting up the Router with the setup software (located on the CD-ROM), the Router will be ready for use. If you would like to change its advanced settings, use the Router's browser-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router.

The browser-based utility has these main tabs: *Setup*, *Wireless*, *Security*, *Access Restrictions*, *Applications & Gaming*, *Administration*, and *Status*. Additional tabs will be available after you click one of the main tabs.

How to Access the Browser-Based Utility

To access the browser-based utility, launch the web browser on your computer, and enter the Router's default Internet Protocol (IP) address, **192.168.1.1** in the *Address* field. Then press **Enter**.

A login screen will appear. (Non-Windows 7 users will see a similar screen.) In the *User name* field, enter **admin**. Then enter the password created during the setup software. (If you did not run the setup software, then use the default password, **admin**. You can set a new password on the *Administration* > *Management* screen. Refer to **Administration > Management**, **page 33**.) Click **OK** to continue.



Login Screen

NOTE: You can also access the browser-based utility through Cisco Connect. For more information, refer to **Router Settings**, **page 13**.

Setup > Basic Setup

The first screen that appears is the *Basic Setup* screen. This allows you to change the Router's general settings.

Setup > Basic Setup

Language

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.

Internet Setup

The *Internet Setup* section configures the Router to your Internet connection. Most of this information can be obtained through your Internet Service Provider (ISP).

Internet Connection Type

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

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

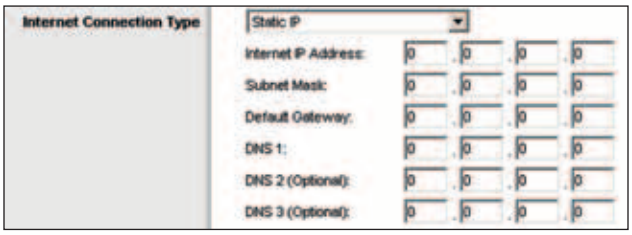
Automatic Configuration - DHCP

The default Internet Connection Type is set to **Automatic Configuration - DHCP** (Dynamic Host Configuration Protocol). Keep the default only if your ISP supports DHCP or you are connecting using 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

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 enter here.

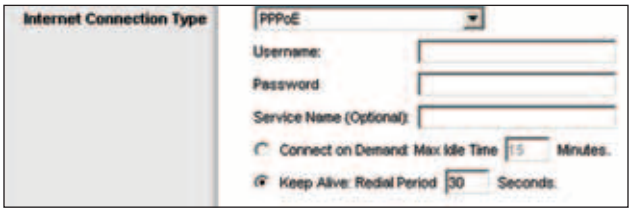
Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Gateway address, which is the ISP server's IP address.

DNS 1-3 Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

PPPoE

Some DSL-based ISPs use Point-to-Point Protocol over Ethernet (PPPoE) 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

Username and Password Enter the Username and Password provided by your ISP.

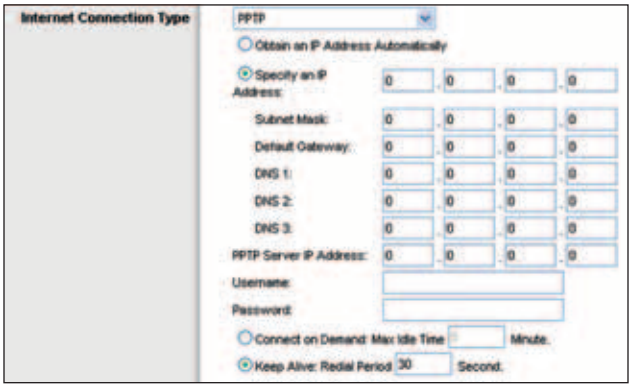
Service Name (optional) If provided by your ISP, enter the Service Name.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to elapse before your Internet connection terminates. The default 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, specify how often the Router should check the Internet connection. The default 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:

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 Gateway address, which is the ISP server's IP address.

DNS 1-3 Your ISP will provide you with at least one Domain Name System (DNS) server IP address.

PPTP Server IP Address Your ISP will provide you with the IP address of the PPTP server.

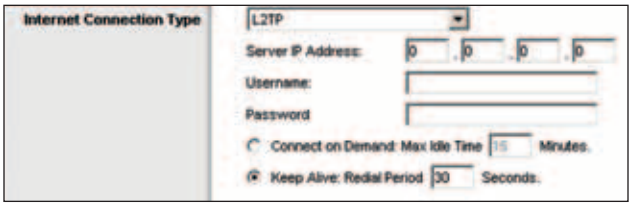
Username and Password Enter the Username and Password provided by your ISP.

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 elapse before your Internet connection terminates. The default 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, specify how often the Router should check the Internet connection. The default is **30** seconds.

L2TP

Layer 2 Tunneling Protocol (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.

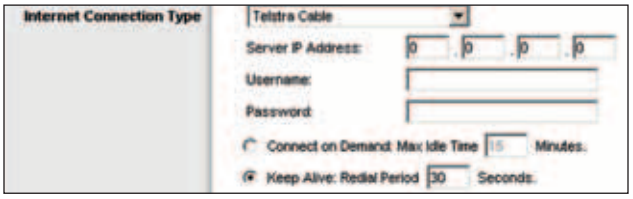
Username and Password Enter the Username and Password provided by your ISP.

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 elapse before your Internet connection terminates. The default 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, specify how often the Router should check the Internet connection. The default is **30** seconds.

Telstra Cable

Telstra Cable is a service that applies to connections in Australia only.



Internet Connection Type > Telstra Cable

Server IP Address This is the IP address of the Telstra Cable. 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 terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to elapse before your Internet connection terminates. The default 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, specify how often the Router should check the Internet connection. The default is **30** seconds.

Optional Settings

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

Optional Settings

Host Name and Domain Name These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Router select the best MTU for your Internet connection, keep the default setting, **Auto**.

Size When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet Connection Type:

- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

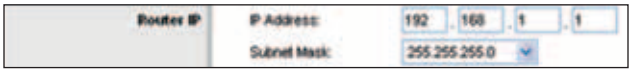
Network Setup

The *Network Setup* section configures the IP settings for your local network.

Router IP

IP Address The Router's IP address, as seen by your network, is displayed. The default Router IP address is **192.168.1.1**.

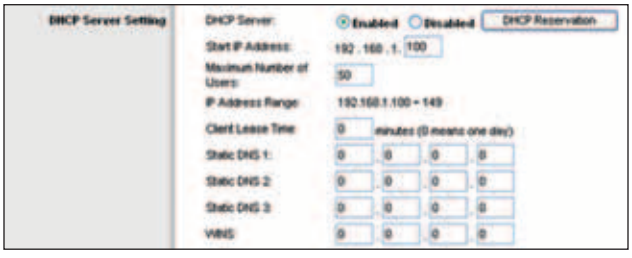
Subnet Mask The Router's Subnet Mask, as seen by your network, is displayed.



Router IP

DHCP Server Setting

The settings allow you to configure the Router's DHCP server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer or device on your network. If you choose to enable the Router's DHCP server option, make sure there is no other DHCP server on your network.



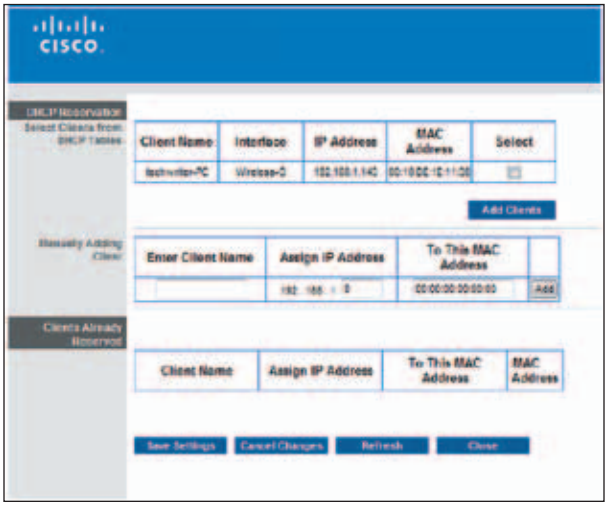
DHCP Server Setting

DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you do not want a DHCP server, then select **Disabled** (no other DHCP features will be available).

DHCP Reservation Click **DHCP Reservation** if you want to assign a fixed local IP address to a MAC address.

DHCP Reservation

You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.



DHCP Reservation

- **Select Clients from DHCP Table** Click the **Select** check box to reserve a client's IP address. Then click **Add Clients**.
- **Manually Adding Client** To manually assign an IP address, enter the client's name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Enter its MAC address in the *To This MAC Address* field. Then click **Add**.

Clients Already Reserved

A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to clear your changes. To view the most up-to-date information, click **Refresh**. To exit this screen, click **Close**.

Start IP Address The Start IP Address specifies the starting IP address for the range of addresses assigned by your Router when it functions as a DHCP server. (The first IP address assigned by the Router will be randomly selected within the range you specify.)

Because the Router's default IP address is 192.168.1.1, the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Start IP Address is **192.168.1.100**.

Maximum Number of Users Enter the maximum number of computers that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

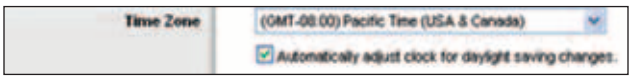
IP Address Range The range of available IP addresses is displayed.

Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, 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 Uniform Resource Locators (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.

Time Setting



Time Setting

Time Zone Select the time zone in which your network functions from this drop-down menu.

Automatically adjust clock for daylight saving changes Select this option to have the Router automatically adjust for daylight saving time.

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

Setup > DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, File Transfer Protocol (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.dyndns.org** or **www.TZO.com**. If you do not want to use this option, keep the default, **Disabled**.

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.

DynDNS.org

Setup > DDNS > DynDNS

Username Enter the Username for your DDNS account.

Password Enter the Password for your DDNS account.

Host Name The DDNS URL assigned by the DDNS service is displayed.

System Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**. The default selection is **Dynamic**.

Mail Exchange (Optional) Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server.

Backup MX This option allows the Mail eXchange (MX) 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.myplace.dyndns.org* will work as well (x is the wildcard). To disable wildcards, keep the default, **Disabled**. To enable wildcards, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

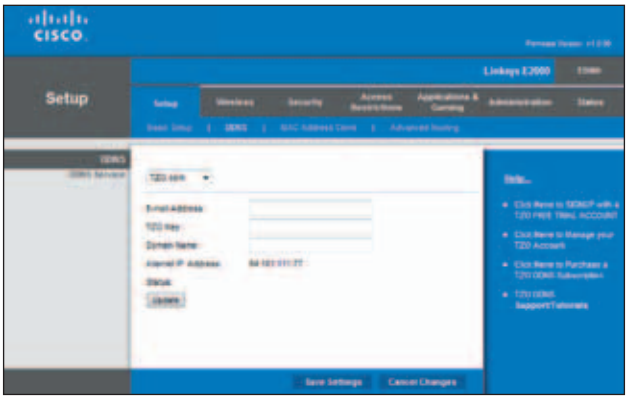
Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

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

Update To manually trigger an update, click **Update**.

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

TZO.com



Setup > DDNS > TZO

E-mail Address, TZO Key, and Domain Name Enter the settings of the account you set up with TZO.

Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

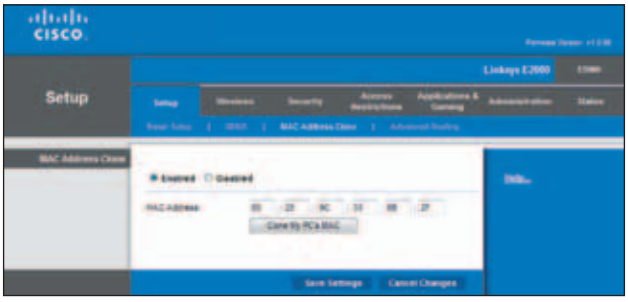
Status The status of the DDNS service connection is displayed.

Update To manually trigger an update, click **Update**.

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

Setup > MAC Address Clone

A Media Access Control (MAC) address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require you to register a MAC address in order to access the Internet. If you have your computer's MAC address registered with your ISP and you do not wish to re-register the MAC address, then you may assign the registered MAC address to the Router with the MAC Address Clone feature.



Setup > MAC Address Clone

MAC Address Clone

Enabled/Disabled To have the MAC Address cloned, select **Enabled**.

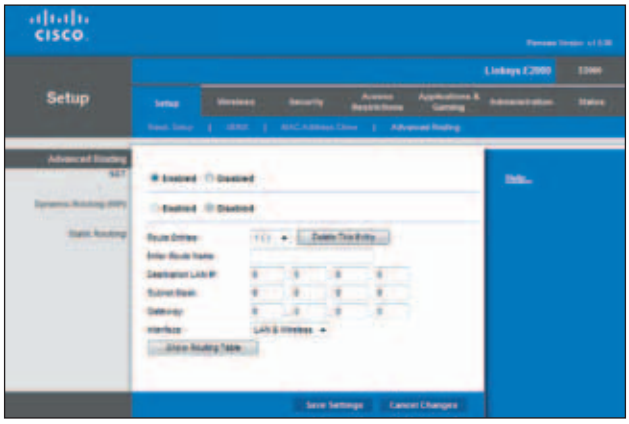
MAC Address Enter the MAC Address registered with your ISP here.

Clone My PC's MAC Click this option to clone the MAC address of the computer you are using.

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

Setup > Advanced Routing

This screen is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.



Setup > Advanced Routing

Advanced Routing

NAT

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**. When the NAT setting is disabled, dynamic routing will be enabled.

Dynamic Routing (RIP)

Dynamic routing uses the Routing Information Protocol (RIP). This option 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.

Enabled/Disabled When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this option is available. Select **Enabled** to use the Dynamic Routing option.

Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.

Route Entries To set up a static route between the Router and another network, select a number from the drop-down 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 (Local Area Network) IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Gateway This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Interface This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks) or the **WAN (Internet)**. (WAN stands for Wide Area Network.)

Click **Show Routing Table** to view the static routes you have already set up.

Advanced Routing > Routing Table

Routing Table

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.

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

Wireless > Basic Wireless Settings

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

There are two ways to configure the Router's wireless network(s), manual and Wi-Fi Protected Setup.

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

Configuration View To manually configure your wireless network, select **Manual**. Proceed to the *Manual Setup* section. To use Wi-Fi Protected Setup, select **Wi-Fi Protected Setup**. Proceed to **Wi-Fi Protected Setup, page 23**.

Manual Setup

If you set the *Configuration View* to **Manual**, the *Basic Wireless Settings* screen displays the following fields.

Wireless > Basic Wireless Settings (Manual Setup)

Wireless Band This is used to select the 2.4 GHz or 5.0 GHz band.

Network Mode From this drop-down menu, you can select the wireless standards running on your network.

- **Mixed** If you have Wireless-N, Wireless-G, and Wireless-B devices in your network, keep the default, **Mixed**.
- **BG-Mixed** If you have only Wireless-G and Wireless-B devices in your network, select **BG-Mixed**.
- **Wireless-N Only** If you have only Wireless-N devices, select **Wireless-N Only**.
- **Wireless-G Only** If you have only Wireless-G devices, select **Wireless-G Only**.
- **Wireless-B Only** If you have only Wireless-B devices, select **Wireless-B Only**.
- **Disabled** If you do not have any wireless devices in your network, select **Disabled**.

NOTE: If you are not sure which mode to use, keep the default, **Mixed**.

Network Name (SSID) The Service Set Identifier (SSID) is the network name shared by all devices in a wireless network. It is case-sensitive and must not exceed 32 keyboard characters. The default is **Ciscoxxxxx** (xxxxx are the last five digits of the Router's serial number). The serial number is located on the left side of the product label, which is on the bottom panel.

Channel Width If you are using the 2.4 GHz band, select **Auto** if you want the Router to automatically determine the proper channel width (20 MHz or 40 MHz) to use, or select **20 MHz only** (default) if you want the Router to operate in Wireless-B and Wireless-G mode only. For best performance, **Auto** is recommended.

If you are using the 5 GHz band, select **Auto** if you want the Router to automatically determine the proper channel width (20 MHz or 40 MHz) to use, select **20 MHz only** (default) if you want the Router to operate in Wireless-B and Wireless-G mode only, or select **40 MHz only** if you want the Router to operate in Wireless-N mode only. For best performance, **Auto** is recommended.

Channel Select a channel for your wireless network (from 1 to 11). If you are not sure which channel to select, then keep the default, **Auto**.

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.

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.

Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)

NOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

- **Wi-Fi Protected Setup Button** Use this method if your client device has a Wi-Fi Protected Setup button.

  a. Click or press the **Wi-Fi Protected Setup** button on the client device.

  b. Click the **Wi-Fi Protected Setup** button on the Router's *Wi-Fi Protected Setup* screen.

  The Wi-Fi Protected Setup LED flashes blue for two minutes during the Wi-Fi Protected Setup process and lights up blue when the Wi-Fi- Protected Setup process is successfully completed.

  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.

  The LED flashes amber when a Wi-Fi Protected Setup session is active, and a second session begins. The Router supports one session at a time. Wait until the LED is continuously lit or off before starting the next Wi-Fi Protected Setup session.

  c. After the client device has been configured, click **OK** on the Router's *Wi-Fi Protected Setup* screen. Then refer back to your client device or its documentation for further instructions.

- **Enter Client Device PIN on Router** Use this method if your client device has a Wi-Fi Protected Setup PIN (Personal Identification Number).

  a. Enter the PIN from the client device in the field on the Router's *Wi-Fi Protected Setup* screen.

  b. Click the **Register** button on the Router's *Wi-Fi Protected Setup* screen.

  c. After the client device has been configured, click **OK** on the Router's *Wi-Fi Protected Setup* screen. Then refer back to your client device or its documentation for further instructions.

- **Enter Router PIN on Client Device** Use this method if your client device asks for the Router's PIN.

  a. On the client device, enter the PIN listed on the Router's *Wi-Fi Protected Setup* screen. (It is also listed on the label on the bottom of the Router.)

  b. After the client device has been configured, click **OK** on the Router's *Wi-Fi Protected Setup* screen. Then refer back to your client device or its documentation for further instructions.

The Network Name (SSID), Security, Passphrase and Wireless Band 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.

Wireless > Wireless Security

The wireless security settings configure the security of your wireless network(s). The Router supports the following wireless security options: WPA/WPA2 Mixed Mode (default), WPA2 Personal, WPA Personal, WEP, and RADIUS. (WPA stands for Wi-Fi Protected Access. WEP stands for Wired Equivalent Privacy. RADIUS stands for Remote Authentication Dial-In User Service.)

The default option is **WPA/WPA2 Mixed Mode**, which allows your devices to connect using the strongest security option they support, WPA2 or WPA.

Personal Options

Security Option	Strength
WPA2 Personal	Strongest
WPA/WPA2 Mixed Mode (default)	WPA2: Strongest WPA: Strong
WPA Personal	Strong
WEP	Basic

Office Option

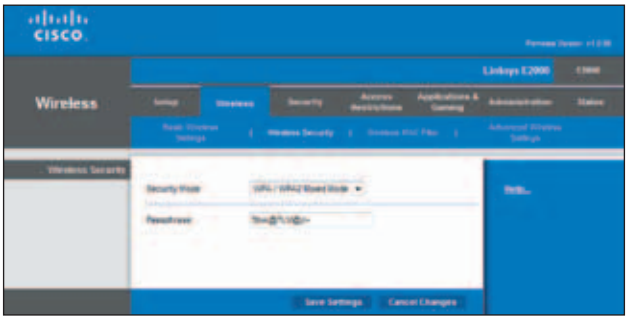
RADIUS is the security option offered for networks that use a RADIUS server for authentication.

Security Mode

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

WPA/WPA2 Mixed Mode

NOTE: If you are using WPA/WPA2 Mixed Mode, each device in your wireless network MUST use the same WPA shared key, or else the network will not function properly.

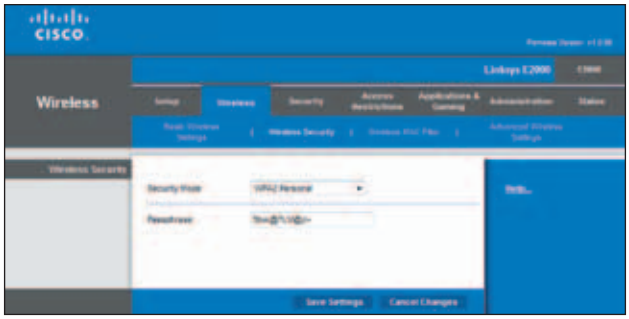


Wireless Security > WPA/WPA2 Mixed Mode

Passphrase Enter a passphrase of 8-63 characters. The default is **password**.

WPA2 Personal

NOTE: If you are using WPA2 or WPA, each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.

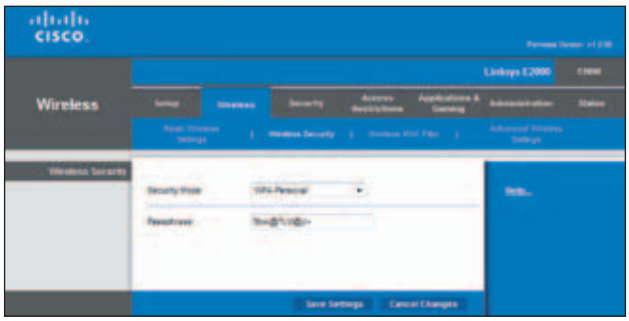


Wireless Security > WPA2 Personal

Passphrase Enter a passphrase of 8-63 characters. The default is **password**.

WPA Personal

NOTE: If you are using WPA2 or WPA, each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.



Wireless Security > WPA Personal

Passphrase Enter a Passphrase of 8-63 characters. The default is **password**.

WEP

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

NOTE: If you are using WEP encryption, 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.

Wireless Security > WEP

Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

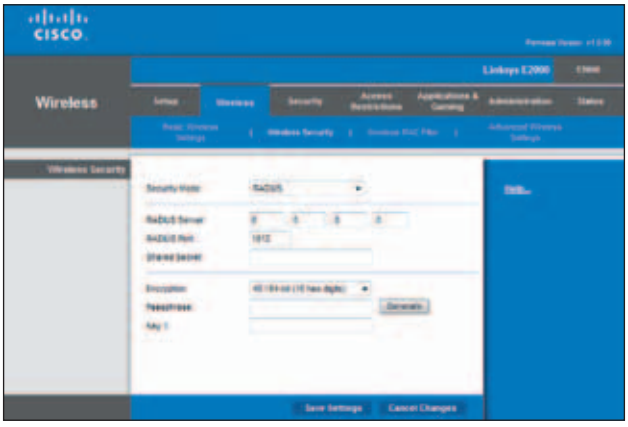
Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1 If you did not enter a Passphrase, enter the WEP key manually.

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 Router.)

NOTE: If you are using WEP encryption, 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.



Wireless Security > RADIUS

RADIUS Server Enter the IP address of the RADIUS server.

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

Shared Secret Enter the key shared between the Router and the server.

Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

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

Key 1 If you did not enter a Passphrase, enter the WEP key manually.

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

Wireless > Wireless MAC Filter

Wireless access can be filtered (restricted) by specifying the MAC addresses of the devices in your wireless network.

Wireless > Wireless MAC Filter

Wireless MAC Filter

Enabled/Disabled To filter wireless users by the MAC addresses of their computers or devices, select **Enabled**. Otherwise, keep the default, **Disabled**.

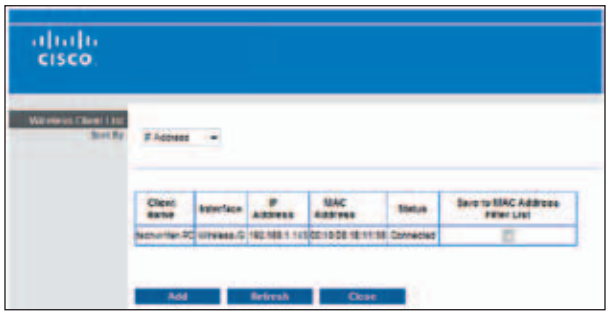
Access Restriction

Prevent PCs listed below from accessing the wireless network Select this option to block wireless access by MAC address. This option is selected by default.

Permit PCs listed below to access the wireless network Select this to option allow wireless access by MAC address. This option is disabled by default.

MAC Address Filter List

Wireless Client List Click this option to open the *Wireless Client List* screen.



Wireless Client List

Wireless Client List

This screen shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status.

Select **Save to MAC Address Filter List** for any device you want to add to the MAC Address Filter List. Then click **Add**.

To update the on-screen information, click **Refresh**. To exit this screen and return to the *Wireless MAC Filter* screen, click **Close**.

MAC 01-50 Enter the MAC addresses of the devices whose wireless access you want to control.

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

Wireless > Advanced Wireless Settings

This *Advanced Wireless Settings* screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an advanced user because incorrect settings can reduce wireless performance. In most cases, keep the default settings.

Wireless > Advanced Wireless Settings

Advanced Wireless

AP Isolation The AP (Access Point) Isolation feature 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. To use this option, select **Enabled**. AP Isolation is disabled by default.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, **Enabled**. Otherwise, select **Disabled**.

Authentication Type The Authentication Type setting is available if the Security Mode is RADIUS or WEP. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication. Select **Shared Key** to only use Shared Key authentication.

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

Transmission Rate The Transmission setting is available if the Network Mode is BG-Mixed, Wireless-G Only, or Wireless-B Only. The rate of data transmission should be set depending on the speed of your wireless network. Select from a range of transmission speeds, or keep the default, **Auto**, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.

N Transmission Rate The N Transmission setting is available if the Network Mode is Mixed or Wireless-N Only. The rate of data transmission should be set depending on the speed of your Wireless-N networking. Select from a range of transmission speeds, or keep the default, **Auto**, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.

CTS Protection Mode The Router automatically uses CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G devices are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This option boosts the Router's ability to catch all Wireless-N and Wireless-G transmissions but severely decreases performance. To use this option, keep the default, **Auto**. To disable this option, select **Disabled**.

Beacon Interval A beacon is a packet broadcast by the Router to synchronize the wireless network. The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 65,535 milliseconds. The default value is **100**.

DTIM Interval This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

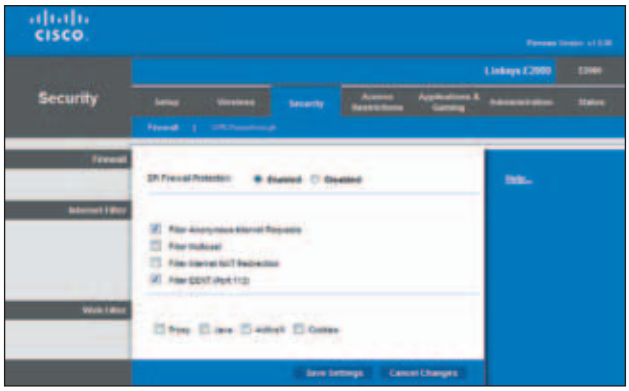
Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset Request to Send (RTS) threshold size, the RTS/CTS (Clear to Send) mechanism will not be enabled. The Router sends 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 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.

Security > Firewall

The *Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network.



Security > Firewall

Firewall

SPI Firewall Protection To use firewall protection, keep the default selection, **Enabled**. To turn off firewall protection, select **Disabled**.

Internet Filter

Filter Anonymous Internet Requests This option makes it more difficult for outside users to work their way into your network. This option is enabled by default. Disable it to allow anonymous Internet requests.

Filter Multicast The multicasting feature allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select this option to enable the filter. This option is disabled by default.

Filter Internet NAT Redirection This option is used to prevent a local computer from using a URL or Internet address to access the local server. Select this option to enable the filter. This option is disabled by default.

Filter IDENT (Port 113) The Filter IDENT (Identification) option keeps port 113 from being scanned by devices outside of your local network. This option is enabled by default. Disable it to allow port 113 to be scanned.

Web Filter

Proxy Use of WAN proxy servers may compromise the Gateway's security. Denying Proxy will disable access to any WAN proxy servers. Select this option to enable proxy filtering. Deselect the option to allow proxy access.

Java Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select this option to enable Java filtering. Deselect the option to allow Java usage.

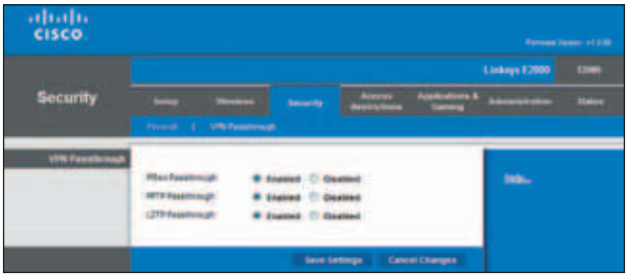
ActiveX ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select this option to enable ActiveX filtering. Deselect the option to allow ActiveX usage.

Cookies A cookie is data stored on your computer and used by Internet sites when you interact with them. Select this option to filter cookies. Deselect the option to allow cookie usage.

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

Security > VPN Passthrough

The *VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.



Security > VPN Passthrough

VPN Passthrough

IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, keep the default, **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.

Access Restrictions > Internet Access

The *Internet Access* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.

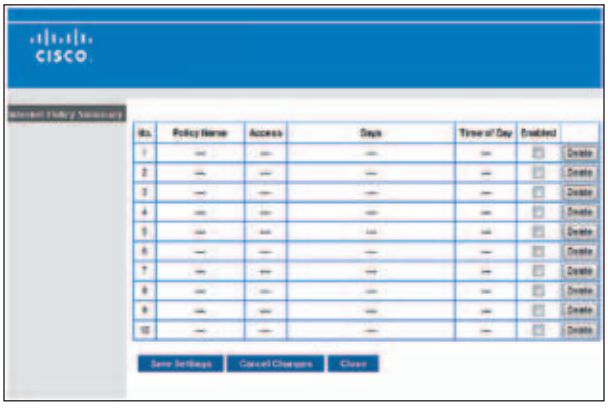
Access Restrictions > Internet Access

Internet Access Policy

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

Summary

The policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, select **Enabled**. To delete a policy, click **Delete**. Click **Save Settings** to save your changes, or click **Cancel Changes** to clear your changes. To return to the *Internet Access Policy* screen, click **Close**.

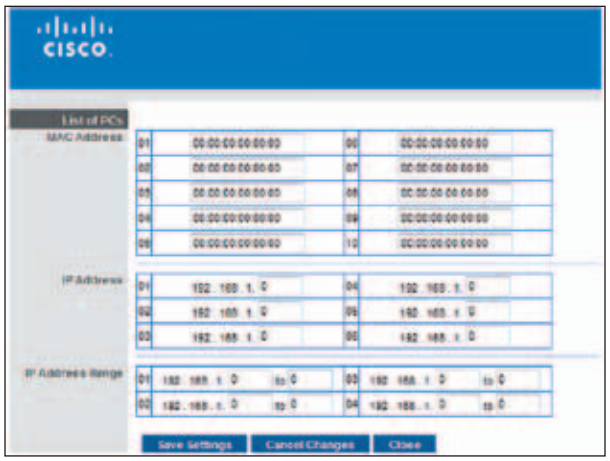


Summary

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

To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time.

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select **Enabled**.
4. Click **Edit List** to select which computers will be affected by the policy. The *List of PCs* screen appears. 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. Then click **Close**.



List of PCs

5. 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 *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. You can block websites with specific URL addresses. Enter each URL in a separate *Website Blocking by URL Address* field.
8. You can also block websites using specific keywords. Enter each keyword in a separate *Keyword* field.
9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.)

   From the Applications list, select the application you want to block. Then click the **>>** button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the **<<** button.
10. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the **Port Range** fields. Select its protocol from the *Protocol* drop-down menu. Then click **Add**.

    To modify a service, select it from the Application list. Change its Application Name, Port Range, and/or Protocol setting. Then click **Modify**.

    To delete a service, select it from the Application list. Then click **Delete**.
11. Click **Save Settings** to save the policy's settings. To cancel the policy's settings, click **Cancel Changes**.

Applications and Gaming > Single Port Forwarding

The *Single Port Forwarding* screen allows you to customize port services for various applications.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate computers (also called servers). Before using forwarding, you should assign static IP addresses to the designated computers (use the DHCP Reservation option on the *Basic Setup* screen; refer to **DHCP Reservation**, **page 19**).

Applications and Gaming > Single Port Forwarding

Single Port Forwarding

Preset applications are available for the first five entries. For each entry, complete the following:

Application Name Select the appropriate application.

To IP Address 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 static IP address; refer to **DHCP Reservation**, **page 19**.

Enabled Select **Enabled** to enable port forwarding.

You can customize entries for additional applications. For each entry, complete the following:

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 computer or Internet application. Check with the Internet application documentation for more information.

Internal Port Enter the internal port number used by the computer or Internet application. Check with the Internet application documentation for more information.

Protocol Select the protocol(s) used for this application, **TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol), or **Both**.

To IP Address 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 static IP address; refer to **DHCP Reservation**, **page 19**.

Enabled Select **Enabled** to enable port forwarding.

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

Applications and Gaming > Port Range Forwarding

The *Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, 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 computers (also called servers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation option on the *Basic Setup* screen; refer to **DHCP Reservation**, **page 19**).

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

Applications and Gaming > Port Range Forwarding

Port Range Forwarding

For each entry, complete the following.

Application Name Enter the name you wish to give the application. Each name can be up to 12 characters.

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

Protocol Select the protocol(s) used for this application, **TCP**, **UDP**, or **Both**.

To IP Address Enter the IP address of the computer running the specific application. If you assigned a static IP address to the computer, then you can look up its static IP address; refer to **DHCP Reservation**, **page 19**.

Enabled Select **Enabled** to enable port forwarding.

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

Applications & Gaming > Port Range Triggering

The *Port Range Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Applications and Gaming > Port Range Triggering

Port Range Triggering

For each entry, complete the following:

Application Name Enter the application name of the trigger.

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

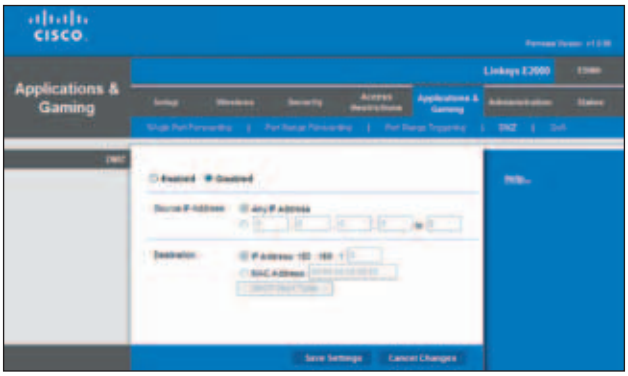
Forwarded Range Enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Enabled Select **Enabled** to enable port triggering.

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

Applications and Gaming > DMZ

The DMZ (Demilitarized Zone) feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one computer. 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.



Applications and Gaming > DMZ

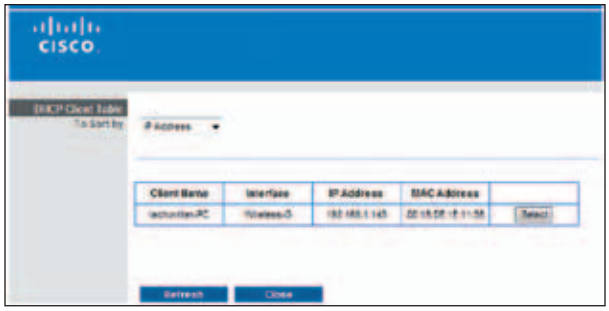
DMZ

Any computer whose port is being forwarded must have its DHCP client function disabled and have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Enabled/Disabled To disable DMZ hosting, select **Disabled**. To expose one PC, select **Enabled**. Then configure the following settings:

Source IP Address If you want any IP address to be the source, select **Any IP Address**. If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields.

Destination If you want to specify the DMZ host by IP address, select **IP Address** and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select **MAC Address** and enter the MAC address in the field provided. To retrieve this information, click **DHCP Client Table**.



DMZ > DHCP Client Table

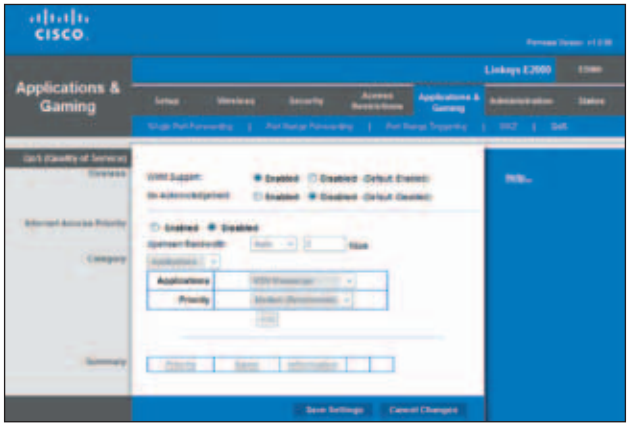
DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, and MAC Address. To select a DHCP client, click **Select**. To update the on-screen information, click **Refresh**. 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.

Applications and Gaming > QoS

Quality of Service (QoS) is a method that assigns priority to specific types of network traffic, which often are demanding, real-time applications, such as gaming, videoconferencing, video streaming, and Voice over Internet Protocol (VoIP) telephony. QoS helps to ensure optimal performance for these types of uses.



Applications and Gaming > QoS

QoS

Wireless

WMM Support Wi-Fi Multimedia (WMM) is a wireless Quality of Service feature that improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, the wireless client devices in your network must support Wireless WMM. To disable this option, select **Disabled**. Otherwise, keep the default, **Enabled**.

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**.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels of priority: High, Medium, Normal, or Low. When you set 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 set, select **Enabled**. Otherwise, keep the default, **Disabled**.

Category

You can define the Internet access priority level for as many categories as you want. The *Summary* section will display all of the priority selections that you enter. Select from the following categories:

- **Applications** Allows you to assign a priority level for a pre-defined application or one that you add.
- **Online Games** Allows you to assign a priority level for a pre-defined game or one that you add.
- **MAC Address** This option lets you prioritize network traffic based on the device that is accessing the network. For example, if you want your gaming console to have higher priority accessing the Internet than your computer, you can assign their priority levels using their respective MAC addresses.
- **Ethernet Port** This option allows you to prioritize traffic connected to a specific Ethernet port. For example, you can assign a higher priority level to the computer connected to port 1.
- **Voice Device** Voice devices require a higher priority level. You can assign a higher priority level to voice devices using their respective MAC addresses.

Summary

This lists the QoS entries you have created for your applications and devices. Refer to **Summary**, **page 33** for more information.

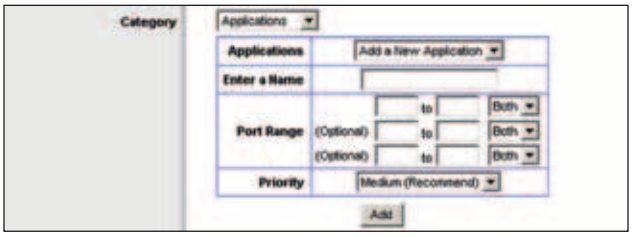
Applications

Applications Select the appropriate application. If you select Add a New Application, follow the instructions in the *Add a New Application* section.

Priority Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Add a New Application



QoS > Add a New Application

Enter a Name Enter a name for this application.

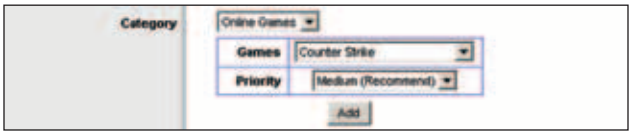
Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

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

Priority Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Online Games



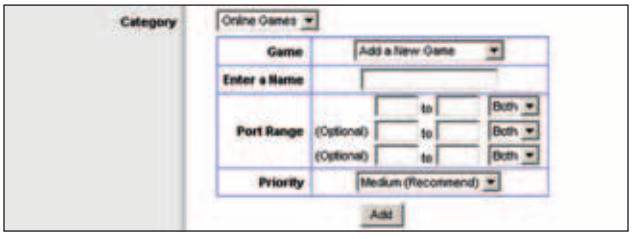
QoS > Online Games

Games Select the appropriate game. If you select Add a New Game, follow the instructions in the *Add a New Game* section.

Priority Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Add a New Game



QoS > Add a New Game

Enter a Name Enter any name to indicate the name of the entry.

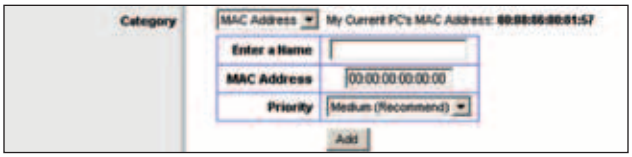
Port Range Enter the port range that the game will be using. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

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

Priority Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

MAC Address



QoS > MAC Address

The MAC address of the computer you are using is displayed.

Enter a Name Enter a name for your device.

MAC Address Enter the MAC address of your device.

Priority Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Voice Device

QoS > Voice Device

Enter a Name Enter a name for your voice device.

MAC Address Enter the MAC address of your voice device.

Priority Select the appropriate priority: **High (Recommended)**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Summary

This lists the QoS entries you have created for your applications and devices.

Priority This column displays the bandwidth priority of High, Medium, Normal, or Low.

Name This column displays the application, game, device, or port name.

Information This column displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

Remove Click this option to remove an entry.

Edit Click this option to make changes.

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

Administration > Management

The *Management* screen allows the network's administrator to manage specific Router functions for access and security.

Administration > Management

Management

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

Router Password Enter a new password for the Router.

Re-enter to confirm Enter the password again to confirm.

Web Access

Web Utility Access 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**. The default is **HTTP**.

Web Utility 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.

Remote Access

Remote Management To permit remote access of the Router from the Internet (outside the local network), select **Enabled**. Otherwise, keep the default, **Disabled**.

Web Utility Access 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**. **HTTP** is the default.

Remote Upgrade If you want to be able to upgrade the Router from the Internet (outside the local network), select **Enabled**. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default, **Disabled**.

Allowed Remote IP Address If you want to be able to access the Router from any external IP address, select **Any IP Address**. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

Remote Management Port Enter the port number that will be open to outside access. (When you remotely access the Router, you will need to enter the Router's password.)

NOTE: When you are in a remote location and wish to manage the Router, enter **http://xxx.xxx.xxx.xxx:yyyy** or **https://xxx.xxx.xxx.xxx:yyyy**, depending on whether you use HTTP or HTTPS. Enter the Router's specific Internet IP address in place of xxx.xxx.xxx.xxx, and enter the Remote Management Port number in place of yyyy.

UPnP

Universal Plug and Play (UPnP) allows the appropriate Windows operating system to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.

UPnP If you want 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 and Restore

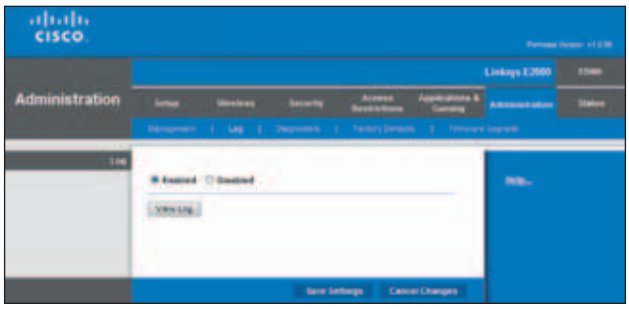
Backup Configurations To back up the Router's configuration settings, click this option and follow the on-screen instructions.

Restore Configurations To restore the Router's configuration settings, click this option and follow the on-screen instructions. (You must have previously backed up the Router's configuration settings.)

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

Administration > Log

The Router can keep logs of all traffic for your Internet connection.

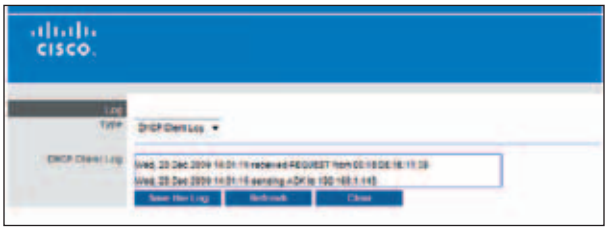


Administration > Log

Log

Log To disable the Log function, select **Disabled**. To monitor traffic between the network and the Internet, keep the default, **Enabled**. With logging enabled, you can choose to view temporary logs.

View Log To view the logs, click **View Log**.



Administration > Log > View Log

Log

- **Type** Select **Incoming Log**, **Outgoing Log**, **Security Log**, or **DHCP Client Log**.

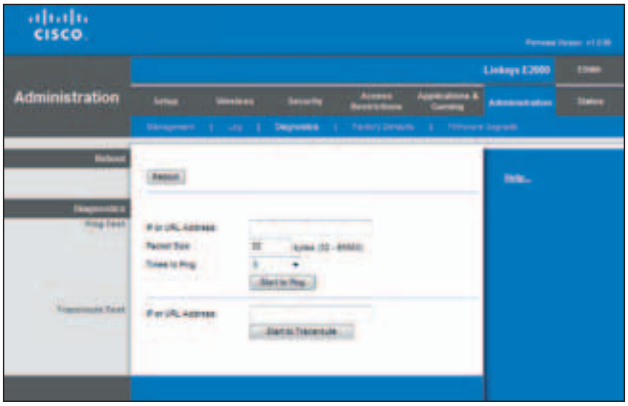
- **<Type> Log** The Incoming Log displays a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log displays a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. The Security log displays the login information for the browser-based utility. The DHCP Client Log displays the LAN DHCP server status information.

  Click **Save the Log** to save this information to a file on your computer's hard drive. Click **Refresh** to update the log. Click **Clear** to clear all the information that is displayed.

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

Administration > Diagnostics

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network devices, including connection to the Internet. This screen also allows you to reset the Router.



Administration > Diagnostics

Reboot

Reboot Click **Reboot** to reset the Router.

Diagnostics

Ping Test

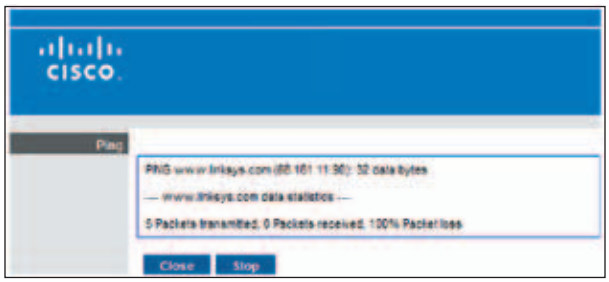
Ping checks the status of a connection.

IP or URL Address Enter the address of the computer, device, or website whose connection you wish to test.

Packet Size Enter the packet size you want to use. The default is **32** bytes.

Times 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 option. The *Ping Test* screen shows if the test is successful. Click **Close** to return to the *Diagnostics* screen. Click **Stop** to stop the test.



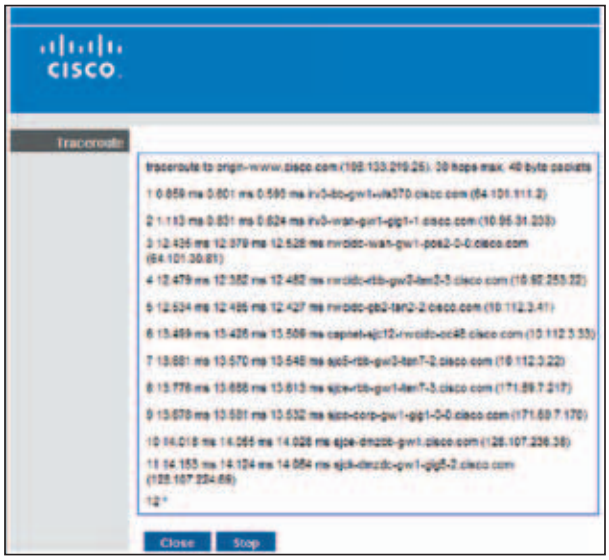
Diagnostics > Ping

Traceroute Test

Traceroute checks the performance of a connection.

IP or URL Address Enter the address of the computer, device, or website whose connection you wish to test.

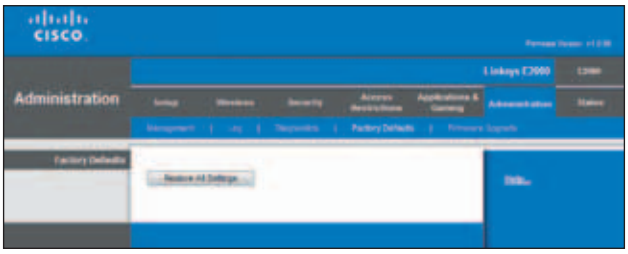
Start to Traceroute To run the test, click this option. The *Traceroute* screen shows if the test is successful. Click **Close** to return to the *Diagnostics* screen. Click **Stop** to stop the test.



Diagnostics > Traceroute

Administration > Factory Defaults

The *Factory Defaults* screen allows you to restore the Router's configuration to its factory default settings.



Administration > Factory Defaults

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.

Factory Defaults

Restore All Settings To reset the Router's settings to the defaults, click this option and then follow the on-screen instructions. Any settings you have saved will be lost when the default settings are restored.

Administration > Firmware Upgrade

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

Administration > Firmware Upgrade

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 will have to re-enter all of your configuration settings.

Firmware Upgrade

Before upgrading the firmware, download the Router's firmware upgrade file from the website, **www.linksys.com/support**.

Please select a file to upgrade the firmware Click **Browse** and select the extracted firmware upgrade file.

Start to Upgrade After you have selected the appropriate file, click this option, and follow the on-screen instructions.

WARNING: Do not interrupt the upgrade process. You should not turn off the power or press the Reset button during the upgrade process. Doing so may disable the Router.

Status > Router

The *Router* screen displays information about the Router and its current settings.

Status > Router

Router Information

Firmware Version The version number of the Router's current firmware is displayed.

Firmware Verification The unique identifier of the firmware is displayed.

Current Time This time set on the Router is displayed.

Internet MAC Address The Router's MAC Address, as seen by your ISP, is displayed.

Host Name The Host Name of the Router is displayed (if it was entered on the *Setup* > *Basic Setup* screen).

Domain Name The Domain Name of the Router is displayed (if it was entered on the *Setup* > *Basic Setup* screen).

Internet Connection

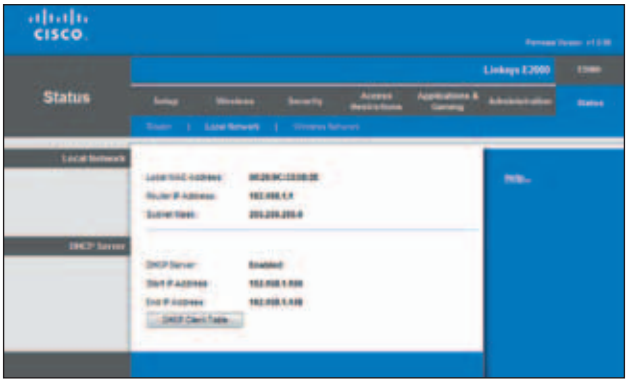
This section shows the current network information stored in the Router. The information varies depending on the Internet connection type selected on the *Setup* > *Basic Setup* screen.

For a DHCP connection, select **IP Address Release** or **IP Address Renew** as appropriate to release or renew a DHCP lease. For a PPPoE or similar connection, select **Connect** or **Disconnect** as appropriate to connect to or disconnect from the Internet.

Click **Refresh** to update the on-screen information.

Status > Local Network

The *Local Network* screen displays information about the local network.



Status > Local Network

Local Network

Local MAC Address The MAC address of the Router's local, wired interface is displayed.

Router IP Address The Router's IP address, as it appears on your local network, is displayed.

Subnet Mask The Subnet Mask of the Router is displayed.

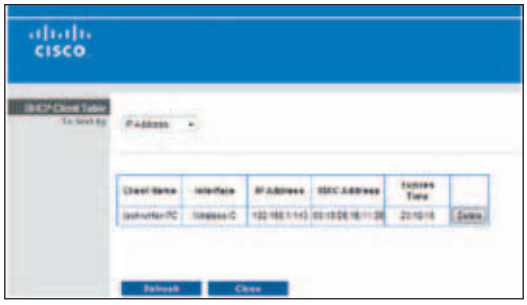
DHCP Server

DHCP Server The status of the Router's DHCP server function 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 option to view a list of computers or other devices that are using the Router as a DHCP server.



DHCP Clients Table

DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, and MAC Address. To remove a DHCP client, click **Delete**. To update the on-screen information, click **Refresh**. To exit this screen and return to the *Local Network* screen, click **Close**.

Status > Wireless Network

The *Wireless Network* screen displays information about your wireless network.

Status > Wireless Network

Wireless Network

MAC Address The MAC address of the Router's local, wireless interface is displayed.

Mode The wireless mode used by the network is displayed.

Network Name (SSID) The name of the wireless network, which is also called the SSID, is displayed.

Channel Width The Channel Width setting (selected on the *Wireless* > *Basic Wireless Settings* screen) is displayed.

Channel The Channel setting selected on the *Basic Wireless Settings* screen is displayed.

Security The wireless security method used by the Router is displayed.

SSID Broadcast The status of the SSID Broadcast option is displayed.

Appendix A: Troubleshooting

Your computer cannot connect to the Internet.

Follow these instructions until your computer can connect to the Internet:

- Make sure that the Router is powered on. 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. Cable or DSL modem
  2. Router
  3. Computer
- Check the cable connections. 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.

The modem does not have an Ethernet port.

The modem is a dial-up modem for traditional dial-up service. 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 **Set up your Linksys Router** 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. Select **Tools** > **Internet Options**.
2. Click the **Connections** tab.
3. Select **Never dial a connection**.
4. Click **OK**.

The Router does not have a coaxial port for the cable connection.

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. Click **Set up your Linksys Router** and follow the on-screen instructions.

The computer cannot connect wirelessly to the network.

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.

Router settings can be modified using the Cisco Connect software, refer to **How to Access Cisco Connect**, **page 15**. To modify the advanced settings, go to *Advanced Settings*. Refer to **Advanced Settings**, **page 15**.

You want to access the browser-based utility from Cisco Connect.

To enter the browser-based utility from Cisco Connect, follow these steps:

1. Open Cisco Connect.
2. On the main menu, click **Router settings**.
3. Click **Advanced settings**.
4. Write down the username and password that are displayed. (To help protect your password, you can copy it to the Clipboard by clicking **Copy Password**.)
5. Click **OK**.
6. Your web browser automatically opens. Enter the username and password, and then click **OK**. (If you copied the password to the Clipboard in step 4, press **Ctrl-V** to paste it into the *Password* field.)

When you try to log into the browser-based utility, your password does not work.

Your wireless security password also serves as the browser-based utility's login password. To see this password:

1. Open Cisco Connect.
2. On the main menu, click **Router settings**.
3. The *Password* is displayed on the left side of the screen.

WEB: If your questions are not addressed here, refer to our E2000 support section on the web, **www.linksys.com/support/E2000**

Appendix B: Specifications

Model Name	Linksys E2000
Description	Advanced Wireless-N Router
Model Number	E2000
Standards	802.11n, 802.11a, 802.11g, 802.11b, 802.3, 802.3u, 802.3ab
Ports	Power, Internet, and Ethernet
Buttons	Reset, Wi-Fi Protected Setup
LEDs	Ethernet (1-4), Wi-Fi Protected Setup, Wireless, Internet, Power
Cabling Type	CAT 5e
Number of Antennas	3
RF Pwr (EIRP) in dBm	17 dBm
Antenna Gain in dBi	Main Antenna*: 1.5 dBi Third Antenna: 2.2 dBi
UPnP able/cert	Able
Security Features	WEP, WPA, WPA2
Security Key Bits	Up to 128-Bit Encryption

Environmental

Dimensions	7.95" x 6.3" x 1.34" (202 x 160 x 34 mm)
Weight	10.58 oz (0.30 kg)
Power	12V
Certification	FCC, CE, IC-03, Wi-Fi
Operating Temp.	32 to 104ºF (0 to 40ºC)
Storage Temp.	-4 to 140ºF (–20 to 60ºC)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

* The Router has two main antennas.

Specifications are subject to change without notice.

Appendix C: Warranty Information

LIMITED WARRANTY

(U.S.A, Canada, Asia Pacific, Australia, New Zealand)

FOR CONSUMERS WHO ARE COVERED BY CONSUMER PROTECTION LAWS OR REGULATIONS IN THEIR COUNTRY OF PURCHASE OR, IF DIFFERENT, THEIR COUNTRY OF RESIDENCE, THE BENEFITS CONFERRED BY THIS WARRANTY ARE IN ADDITION TO ALL RIGHTS AND REMEDIES CONVEYED BY SUCH CONSUMER PROTECTION LAWS AND REGULATIONS. THIS WARRANTY DOES NOT EXCLUDE, LIMIT OR SUSPEND ANY RIGHTS OF CONSUMERS ARISING OUT OF NONCONFORMITY WITH A SALES CONTRACT. SOME COUNTRIES, STATES AND PROVINCES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES OR ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY OR CONDITION MAY LAST, SO THE LIMITATIONS OR EXCLUSIONS DESCRIBED BELOW MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY COUNTRY, STATE OR PROVINCE. THIS LIMITED WARRANTY IS GOVERNED BY AND CONSTRUED UNDER THE LAWS OF THE COUNTRY IN WHICH THE PRODUCT PURCHASE TOOK PLACE.

This warranty is provided to you by Cisco Systems, Inc. or its subsidiary instead of Cisco Systems, Inc. ("Cisco"). Cisco warrants the hardware in this Cisco product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified below:

- One (1) year for new product
- Ninety (90) days for refurbished product

Your exclusive remedy and Cisco's entire liability under this limited warranty will be for Cisco, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Cisco product, or (c) refund the actual purchase price of the product less any rebates and discounts, or (d) pay the cost of repair of the product. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Cisco.

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.

EXCLUSIONS AND LIMITATIONS

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Cisco, (c) the product damage was caused by use with non-Cisco products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Cisco does not charge a purchase price or license fee.

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 WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Cisco does not warrant that the operation of the product, software or services will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the product, software or services, or any equipment, system or network on which the product, software or services are used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED.

TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT WILL CISCO BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, LOSS OF THE ABILITY TO USE ANY THIRD PARTY PRODUCTS, SOFTWARE OR SERVICES, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, SOFTWARE OR ANY SERVICES PROVIDED IN RESPECT OF SUCH PRODUCT, SOFTWARE OR SERVICE, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY

OF SUCH DAMAGES. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT WILL CISCO'S LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose.

If you live in and have purchased the product in Australia or New Zealand, the following two (2) paragraphs will apply in place of the preceding paragraph:

To the extent permitted by law, Cisco excludes liability for any lost data, revenue or profit, loss of the ability to use any third party products, software or services, and indirect or consequential loss, whether based in statute, common law (including negligence) or otherwise, arising out of or related to the use of or inability to use the product, software, or any services provided in respect of such product, software or service, even if Cisco has been advised of the possibility of such damages and Cisco limits its liability to an amount not exceeding the amount paid by you for the product.

Part V of the Trade Practices Act (1974) (C'th of Australia), corresponding consumer protection provisions of Australian State and Territory legislation and the Consumer Guarantees Act 1993 (New Zealand) (together, "Applicable Laws") imply terms and warranties which operate to protect certain Australian and New Zealand purchasers of goods and services in various circumstances. Nothing in this warranty excludes, restricts or modifies any condition, warranty, right or remedy implied or imposed by any Applicable Laws which cannot lawfully be excluded, restricted or modified.

No Cisco employee, agent or reseller is authorized to make any verbal or written modification, extension or addition to this warranty, and Cisco expressly disclaims any such change to this warranty. If any portion of this limited warranty is found to be void or unenforceable, its remaining provisions shall remain in full force and effect.

OBTAINING WARRANTY SERVICE

If you have a question about your product or experience a problem with it, please go to **www.myciscohome.com/support** where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact Cisco Technical Support (or, if you purchased your product from a service provider, contact the service provider) for instructions on how to obtain warranty service. The telephone number for Cisco Technical Support in your area can be found by clicking the "Contact Us" link on the home page of **www.myciscohome.com**. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning. Products returned for replacement must be returned to Cisco in the same country in which the original product was purchased. 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 Cisco's then-current rates.

TECHNICAL SUPPORT

This limited warranty is neither a service nor a support contract. Information about Cisco's current technical support offerings and policies (including any fees for support services) can be found at **www.myciscohome.com/support**.

Please direct all inquiries to: Cisco, 120 Theory, Irvine, CA 92617.

Appendix D: Regulatory Information

FCC Statement

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. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 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

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.

IEEE 802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

The device for the band 5150-5250 MHz is only for indoor usage to reduce the potential for harmful interference to co-channel mobile satellite systems.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 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.

Safety Notices

WARNING: Do not use this product near water, for example, in a wet basement or near a swimming pool.

WARNING: Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

WARNING: This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003 and RSS210.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

Industry Canada Radiation Exposure Statement

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.

Restrictions in the 5 GHz Band

1. The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
2. This device has been designed to operate with an antenna having a maximum gain of 4 dBi and 3.5 dBi at 2.4 GHz and 5 GHz respectively. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Because high power radars are allocated as primary users (meaning they have priority) in 5250-5350 MHz and 5650-5850 MHz, these radars could cause interference and/or damage to licensed exempt LAN devices.

Additional requirements for the band 5600-5650 MHz: Until further notice, devices subject to this Section shall not be capable of transmitting in the band 5600-5650 MHz, so that Environment Canada weather radars operating in this band are protected.

Avis d'Industrie Canada

Cet appareil numérique de la classe B est conforme aux normes NMB-003 et RSS210 du Canada.

L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes :

1. il ne doit pas produire de brouillage et
2. il doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

Avis d'Industrie Canada concernant l'exposition aux radiofréquences

Ce matériel est conforme aux limites établies par IC en matière d'exposition aux radiofréquences dans un environnement non contrôlé. Ce matériel doit être installé et utilisé à une distance d'au moins 20 cm entre l'antenne et le corps de l'utilisateur.

L'émetteur ne doit pas être placé près d'une autre antenne ou d'un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

Restrictions dans la bande 5 GHz

1. L'appareil pour la bande de 5 150 à 5 250 MHz est conçu pour usage à l'intérieur seulement afin de réduire le potentiel d'interférences pour les systèmes mobiles par satellite qui utilisent le même canal.
2. Cet appareil est conçu pour fonctionner avec une antenne ayant un gain maximal de 4 dBi à 2,4 GHz et de 3,5 dBi à 5 GHz. Les antennes ayant un gain plus élevé sont strictement interdites par Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Du fait que les radars haute puissance ont la priorité dans les bandes 5 250-5 350 MHz et 5 650-5 850 MHz, ils pourraient causer des interférences ou endommager les périphériques réseau sans fil.

Autres restrictions pour la bande 5 600-5 650 MHz : sauf avis contraire, les périphériques concernés par cette section ne doivent pas être capables de transmettre dans la bande 5 600-5 650 MHz afin de protéger les radars d'Environnement Canada qui l'utilisent.

Wireless Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. 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.

Avis de non-responsabilité concernant les appareils sans fil

Les performances maximales pour les réseaux sans fil sont tirées des spécifications de la norme IEEE 802.11. Les performances réelles peuvent varier, notamment en fonction de la capacité du réseau sans fil, du débit de la transmission de données, de la portée et de la couverture. 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.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Cisco products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:

English - Environmental Information for Customers in the European Union

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.

Español (Spanish) - Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Français (French) - Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

WEB: For additional information, please visit **www.myciscohome.com**

Appendix E: Software End User License Agreement

Cisco Products:

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.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Cisco at **www.myciscohome.com/gpl**, or as provided for in Schedule 2 below. By using the Software, You or the entity or company that You represent ("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.myciscohome.com/gpl**. For detailed license terms and additional information on open source software in Cisco products please look at the Cisco public web site at: **www.myciscohome.com/gpl/** or Schedule 2 below as applicable. 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.

THIS SOFTWARE END USER LICENSE AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU AND CISCO. READ IT CAREFULLY BEFORE INSTALLING AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY CHECKING THE "NEXT" BOX, DOWNLOADING, INSTALLING OR USING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN DO NOT CLICK ON THE "NEXT" BUTTON AND DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. CISCO'S ACCEPTANCE IS EXPRESSLY CONDITIONED UPON YOUR AGREEMENT TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, TO THE EXCLUSION OF ALL OTHER TERMS.

In addition, if You access or otherwise use any of Cisco's web sites, You agree to all of the terms and conditions of the web sites including the "Terms of Use" located at the web site you are using, as applicable and as amended from time to time.

Software Licenses:

The software licenses applicable to software from Cisco are made available at the Cisco public web site at: **www.myciscohome.com** and **www.myciscohome.com/gpl/** respectively. 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.

Schedule 1
Cisco Software License Agreement

License. Subject to the terms and conditions of this Agreement and compliance therewith, Cisco grants You (provided You are the original end user purchaser of the Cisco product including the Software) a personal, non-commercial, nontransferable, non-sublicensable, nonexclusive license to (i) use the Software and accompanying Documentation (each as defined below) for Your personal non-commercial use only, in object code form only, and only in accordance with the accompanying Documentation; (ii) 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; (iii) 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 (iv) 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.

Service Access. Subject to the terms and conditions of this Agreement, Cisco may make available certain services through the use of the Software, as described more fully in the Software ("Services"), solely for Your own use, and not for the use or benefit of any third party. Cisco may change, suspend or discontinue the Software and Services at any time, including the availability of any feature, functionality, or content without notice or liability. Cisco may also impose limits on certain features and services or restrict Your access to parts or all of the Services without notice or liability.

"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.

"Technology" shall mean the Software and Services collectively.

License Restrictions. Other than as set forth in this Agreement, You may not, nor permit anyone else to, directly or indirectly (i) make, distribute, or, except in connection with the use of Your Cisco product, copy 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 or attempt to reduce the Software to a human-perceivable form (except to the extent expressly permitted by law notwithstanding this provision or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license); (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 Technology 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 Technology unless the prospective assignee, sublicensee or transferee expressly agrees to all the terms and conditions under this Agreement.

The Technology 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 Technology and 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 Technology is purchased separately. All other rights of both parties and all other provisions of this Agreement will survive this termination.

Ownership. The Technology and Documentation are licensed and not sold to You by Cisco and the relevant third parties set forth in Schedule 2. Cisco, its suppliers and its licensors respectively retain all right, title and interest, including all copyright and intellectual property rights, in and to, the Technology and Documentation and all copies, derivatives 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 web sites 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. Cisco makes no representations as to the quality, 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.

In addition, Cisco may collect and store detailed information regarding Your network configuration and usage for the purpose of providing You technical networking support. The information is associated with You only when You provide a unique ID number to the support representative while You are receiving help. The unique ID is generated randomly on Your computer upon installation and is completely under Your control.

EXCEPT AS OTHERWISE PROVIDED FOR IN THIS AGREEMENT, CISCO HAS NO OBLIGATION OF CONFIDENTIALITY OR (EXCEPT TO THE EXTENT REQUIRED BY THE APPLICABLE DATA PROTECTION LAWS) PRIVACY OF ANY COMMUNICATION OR INFORMATION TRANSMITTED USING THE TECHNOLOGY. Cisco will not be liable for the privacy of e-mail addresses, registration and identification information, disk space, communications, confidential or trade-secret information stored on equipment, transmitted over networks accessed by the Technology, or otherwise connected with Your use of the Technology.

Your use of Your Cisco product and/or the Technology constitutes consent by You to Cisco's and/or its affiliates' collection and use of such information and, for Canadian or European Economic Area (EEA) customers, to the transfer of such information to a location outside Canada or the EEA. Any information collected by Your Cisco product and/or the Software is done and utilized in accordance with our Privacy Policy available at **http://www.myciscohome.com/privacy**. Your election to use the Cisco product and/or Technology indicates Your acceptance and consent to Cisco's use of Your personal data in accordance with the terms of the Cisco Privacy Policy, so please review the policy carefully and check the web site above to review updates to it.

Support; Equipment. This Agreement does not entitle You to any support, upgrades, patches, enhancements, or fixes (collectively, "Support") for the Technology. Any such Support for the Technology that may be made available by Cisco, in its sole discretion, shall become part of the Technology and subject to this Agreement. You shall be responsible for obtaining and maintaining any equipment or ancillary services needed to connect to, access, or otherwise use the Technology, including, without limitation, modems, hardware, software, and long distance or local telephone service. You shall be responsible for ensuring that such equipment or ancillary services are compatible with the Technology.

Software Upgrades etc. If the Software enables You to receive Upgrades, You may elect at any time to receive these Upgrades either automatically or manually. If You elect to receive Upgrades manually or You otherwise elect not to receive or be notified of any Upgrades, You may expose Your Cisco product and/or the Software to serious security threats and/or some features within Your Cisco product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal, security or regulatory requirements or as a result of requirements to comply with the terms of any agreements Cisco has with any third parties regarding Your Cisco product and/or the Software. You will always be notified of any Upgrades being delivered to You. In addition, Cisco reserves the right to Upgrade our user interface with or without notice to You. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

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 WRITTEN LIMITED WARRANTY ON MEDIA SET FORTH ABOVE AND PROVIDED IN YOUR CISCO PRODUCT PACKAGING WITH THE PURCHASE OF THE RELEVANT CISCO PRODUCT 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. Without limiting the foregoing, Cisco does not warrant that the operation of the product, software or services will be uninterrupted, bug free or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the product, software or services, or any equipment, system or network on which the product, software or services are used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

CISCO DOES NOT AND CANNOT WARRANT THE RESULTS YOU MAY OBTAIN BY USING THE TECHNOLOGY. THIS SECTION CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT, AND THE FOREGOING DISCLAIMERS ALSO APPLY WITH RESPECT TO CISCO, THEIR DISTRIBUTORS, CONTRACTORS AND AGENTS. Further, Cisco has no special relationship with or fiduciary duty to You. You acknowledge that Cisco has no control over, and no duty to take any action regarding: which users gain access to the Technology. The Technology may contain, or enable You to access, information that some people may find

offensive or inappropriate. Cisco makes no representations concerning any content contained in or accessed through the Technology, and Cisco will not be responsible or liable for the accuracy, copyright compliance, legality or decency of material contained in or accessed through the Technology.

TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NONINFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

Disclaimer of Liabilities. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT WILL CISCO BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, SOFTWARE OR ANY SERVICES PROVIDED IN RESPECT OF SUCH PRODUCT OR SOFTWARE, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT WILL CISCO'S LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. IF YOU LIVE IN THE EUROPEAN UNION, REFERENCES TO "SPECIAL, INDIRECT, CONSEQUENTIAL, PUNITIVE OR INCIDENTAL DAMAGES" SHALL MEAN ANY LOSSES WHICH (i) WERE NOT REASONABLY FORESEEABLE BY BOTH PARTIES, AND/OR (ii) WERE KNOWN TO YOU BUT NOT TO US AND/OR (iii) WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED BY YOU SUCH AS, FOR EXAMPLE (BUT WITHOUT LIMITATION), LOSSES CAUSED BY VIRUSES, TROJANS OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO YOUR DATA. THE FOREGOING LIMITATIONS WILL APPLY WITH RESPECT TO CISCO, ITS DISTRIBUTORS, CONTRACTORS, AND AGENTS AND EVEN IF ANY WARRANTY OR REMEDY PROVIDED UNDER THIS LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. NOTHING IN THIS SECTION SHALL LIMIT THE LIABILITY OF CISCO OR ITS DISTRIBUTORS, CONTRACTORS OR AGENTS IN RELATION TO DEATH OR PERSONAL INJURIES CAUSED BY THEIR NEGLIGENCE.

Indemnity. You agree that Cisco and its distributors, partners, contractors and agents shall have no liability whatsoever for any use You make of the Technology. You shall indemnify and hold harmless Cisco and its distributors, partners, contractors and agents from any claims, damages, losses, liabilities, costs and fees (including reasonable attorney fees) arising from Your use of the Technology as well as from Your failure to comply with any term of this Agreement.

Technical Support. This limited warranty is neither a service nor a support contract. Information about Cisco's current technical support offerings and policies (including any fees for support services) can be found at **www.myciscohome.com/support**.

Export. Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

U.S. Government Users. The Software and Documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and Documentation with only those rights herein that apply to non-governmental customers. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

General Terms. This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. Each party recognizes and agrees that the warranty disclaimers and liability and remedy limitations in this Agreement are material bargained for bases of this Agreement and that they are reasonable and have been taken into account and reflected in determining the consideration to be given by each party under this Agreement and in the decision by each party to enter into this Agreement. Cisco's distributors, contractors and agents are intended third party beneficiaries under this Agreement. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere. Except as set forth in the above "License" Section or otherwise expressly provided under this Agreement, no amendment to or modification of this Agreement will be binding unless in writing and signed by Cisco and You.

Linksys, Cisco and the Cisco Logo and other trademarks contained in the Software and Documentation are trademarks or registered trademarks of Linksys, Cisco, its licensors and third parties, as the case may be. You may not remove or alter any trademark, trade names, product names, logo, copyright or other proprietary notices, legends, symbols or labels in the Software and Documentation. This Agreement does not authorize

You to use Cisco's or its licensors' names or respective trademarks.

END OF SCHEDULE 1

Schedule 2
Open Source and Third Party Licenses

Schedule 2-A

If this Cisco product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2-A will apply to that open source software. The license terms below in this Schedule 2-A are from the public web site at **http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2-A

Schedule 2-B

If this Cisco product contains open source software licensed under Version 2.1 of the "GNU Lesser General Public License" then the license terms below in this Schedule 2-B will apply to that open source software. The license terms below in this Schedule 2-B are from the public web site at **http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html**

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

   A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

   "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or

table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

   When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

    If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

    This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2-B

Schedule 2-C
OPENSSL LICENSE

If this Cisco product contains open source software licensed under the OpenSSL license:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

In addition, if this Cisco product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 2-C will apply to that open source software. The license terms below in this Schedule 2-C are from the public web site at **http://www.openssl.org/source/license.html**.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (**http://www.openssl.org/**)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

END OF SCHEDULE 2-C

www.linksys.com/support

10012110NC-AI