10/100 16-Port VPN Router

Model: RV016
About This Guide

Icon Descriptions

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

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

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

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

Online Resources

Website addresses in this document are listed without http:// in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add http:// in front of the web address.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys</td>
<td><a href="http://www.linksys.com">www.linksys.com</a></td>
</tr>
<tr>
<td>Linksys International</td>
<td><a href="http://www.linksys.com/international">www.linksys.com/international</a></td>
</tr>
<tr>
<td>Glossary</td>
<td><a href="http://www.linksys.com/glossary">www.linksys.com/glossary</a></td>
</tr>
<tr>
<td>Network Security</td>
<td><a href="http://www.linksys.com/security">www.linksys.com/security</a></td>
</tr>
</tbody>
</table>
# Table of Contents

## Chapter 1: Introduction

1. Introduction to the Router
2. Introduction to VPNs
3. VPN Examples
   - VPN Router to VPN Router
   - Computer (using VPN client software) to VPN Router

## Chapter 2: Product Overview

1. Front Panel
2. Back Panel
3. Left Side Panel

## Chapter 3: Installation

1. Physical Installation
   - Horizontal Placement
   - Wall-Mount Placement
   - Rack-Mount Placement
2. Cable Connections

## Chapter 4: Advanced Configuration

1. Overview
2. How to Access the Web-Based Utility
3. System Summary
   - System Information
   - Configuration
   - Port Statistics
   - Network Setting Status
   - Firewall Setting Status
   - VPN Setting Status
   - Log Setting Status
4. Setup > Network
   - Network
5. Setup > Password
   - Password
6. Setup > Time
   - Time
7. Setup > DMZ Host
   - DMZ Host
8. Setup > Forwarding
   - Forwarding
9. Setup > UPnP
   - UPnP
10. Setup > One-to-One NAT
    - One-to-One NAT
### Table of Contents

- One-to-One NAT ................................................................. .18
- Setup > MAC Clone ......................................................... .18
  - MAC Clone ................................................................. .18
- Setup > DDNS ................................................................. .19
  - DDNS ........................................................................ .19
- Setup > Advanced Routing ............................................... .20
  - Advanced Routing ...................................................... .20
- DHCP > Setup ................................................................. .21
  - Setup ................................................................. .22
- DHCP > Status ............................................................... .23
  - Status ................................................................. .23
- System Management > Multi-WAN ....................................... .23
  - Load Balance ........................................................... .23
- System Management > Bandwidth Management ........................ .26
  - Bandwidth Management ............................................... .27
- System Management > SNMP ............................................ .28
- System Management > Diagnostic ....................................... .29
  - Diagnostic ............................................................. .29
- System Management > Factory Default ................................ .30
  - Factory Default ....................................................... .30
- System Management > Firmware Upgrade ................................ .30
  - Firmware Upgrade .................................................... .30
  - Restart ................................................................. .31
- System Management > Setting Backup ................................ .31
  - Import Configuration File ............................................ .31
  - Export Configuration File ........................................... .31
- Port Management > Port Setup ........................................... .31
  - Basic Per Port Config .................................................. .32
- Port Management > Port Status ........................................... .32
  - Port Status ............................................................. .32
- Firewall > General ......................................................... .33
  - General ................................................................. .33
- Firewall > Access Rules .................................................. .34
  - Access Rules ........................................................... .34
  - Add a New Access Rule ................................................ .35
- Firewall > Content Filter ................................................ .36
  - Content Filter .......................................................... .36
- ProtectLink ................................................................. .36
- VPN > Summary ............................................................. .36
  - Summary ............................................................... .36
- VPN > Gateway to Gateway ............................................... .38
  - Add a New Tunnel ....................................................... .38
- IPSec Setup ................................................................. .41
Table of Contents

VPN > Client to Gateway ........................................ 43
Add a New Tunnel ................................................. 44
IPSec Setup ......................................................... 47
VPN > VPN Client Access ........................................ 49
VPN Client Access ................................................ 50
VPN > VPN Pass Through ........................................ 50
VPN Pass Through ................................................ 51
VPN > PPTP Server ................................................ 51
PPTP Server ......................................................... 51
Connection List ..................................................... 51
Log > System Log .................................................. 51
System Log .......................................................... 52
Log > System Statistics ........................................... 53
Wizard ............................................................... 54
Basic Setup ........................................................ 54
Access Rule Setup ............................................... 58
Support .............................................................. 60
Manual ............................................................... 60
Linksys Web Site .................................................. 60
Logout ............................................................... 60

Appendix A: Troubleshooting ................................. 61

Appendix B: Linksys QuickVPN for Windows 2000, XP, or Vista ......................... 62
Introduction ........................................................ 62
Computer (using VPN client software) to VPN Router ..................................... 62
Linksys QuickVPN Instructions .................................. 62
Router Configuration ............................................. 62
Export a Client Certificate from the Router ................................................. 62
Add VPN Client Users ............................................ 63
Linksys QuickVPN Client Installation and Configuration .............................. 63
Install from the CD-ROM ......................................... 63
Download from the Internet ........................................ 64
Install the Client Certificate ........................................ 64
Use of the Linksys QuickVPN Software ....................................................... 64
Linksys QuickVPN Connection ................................... 64
Version Number of Linksys QuickVPN ....................................................... 65

Appendix C: Gateway-to-Gateway VPN Tunnel ............................................. 66
Overview ........................................................... 66
Before You Begin .................................................. 66
Configuration when the Remote Gateway Uses a Static IP Address ................. 66
Configuration of the RVL200 ...................................... 66
Configuration of the RV016 ........................................ 67
Configuration of PC 1 and PC 2 ........................................... .67
Configuration when the Remote Gateway Uses a Dynamic IP Address ........................................... .68
Configuration of the RVL200 ........................................... .68
Configuration of the RV016 ........................................... .68
Configuration of PC 1 and PC 2 ........................................... .69
Configuration when Both Gateways Use Dynamic IP Addresses ........................................... .69
Configuration of the RVL200 ........................................... .69
Configuration of the RV016 ........................................... .70
Configuration of PC 1 and PC 2 ........................................... .70

Appendix D: IPSec NAT Traversal 71
Overview .............................................................. .71
Before You Begin ......................................................... .71
Configuration of Scenario 1 ........................................... .71
  Configuration of Router A ........................................... .71
  Configuration of Router B ........................................... .72
Configuration of Scenario 2 ........................................... .73
  Configuration of the One-to-One NAT Rules ........................................... .73
  Configuration of Router B ........................................... .74
  Configuration of Router A ........................................... .74

Appendix E: Bandwidth Management 76
Overview .............................................................. .76
Creation of New Services ........................................... .76
Creation of New Bandwidth Management Rules ........................................... .77

Appendix F: Firmware Upgrade 78
Overview .............................................................. .78
How to Access the Web-Based Utility ........................................... .78
Upgrade the Firmware ........................................... .78
Alternative Firmware Upgrade Option ........................................... .78

Appendix G: Trend Micro ProtectLink Gateway Service 80
Overview .............................................................. .80
How to Access the Web-Based Utility ........................................... .80
How to Purchase, Register, or Activate the Service ........................................... .80
  System Summary ........................................... .80
  ProtectLink ........................................... .81
How to Use the Service ........................................... .81
  ProtectLink > Web Protection ........................................... .82
  ProtectLink > Email Protection ........................................... .83
  ProtectLink > License ........................................... .83

Appendix H: Specifications 85
# Table of Contents

## Appendix I: Warranty Information  
86
   Exclusions and Limitations .............................................. 86
   Obtaining Warranty Service ............................................ 86
   Technical Support ....................................................... 87

## Appendix J: Software License Agreement  
88
   Software in Linksys Products .......................................... 88
   Software Licenses ....................................................... 88
   Schedule 1 ............................................................... 88
   Linksys Software License Agreement .................................. 88
   END OF SCHEDULE 1 ..................................................... 89
   Schedule 2 ............................................................... 89
      GNU GENERAL PUBLIC LICENSE .................................... 89
   END OF SCHEDULE 2 ..................................................... 92
   Schedule 3 ............................................................... 92
      GNU LESSER GENERAL PUBLIC LICENSE .......................... 93
   END OF SCHEDULE 3 ..................................................... 97
   Schedule 4 ............................................................... 97
      OpenSSL License ...................................................... 98
      Original SSLeay License .............................................. 98
   END OF SCHEDULE 4 ..................................................... 99

## Appendix K: Regulatory Information  
100
   FCC Statement .......................................................... 100
   Safety Notices ......................................................... 100
   Battery Recycling Statement ........................................... 100
   Industry Canada Statement ............................................. 100
      Avis d’Industrie Canada ............................................... 100

## Appendix L: Contact Information  
105
Chapter 1: Introduction

Introduction to the Router

Thank you for choosing the Linksys 10/100 16-Port VPN Router. The Router lets multiple computers in your office share an Internet connection, and its 16 ports offer versatility.

Two are dedicated Internet ports that let you connect a second Internet line as a backup, or you can use both Internet ports at the same time, allowing the Router to manage bandwidth demands for maximum efficiency. Up to five of the 13, full-duplex, 10/100 local ports can be reconfigured as Internet ports, for an up to seven-port failover or load balanced redundancy. A dedicated DMZ port gives you a publicly accessible channel so you can set up a web or FTP server.

For remote connections, up to 50 remote office or traveling users can securely connect to your office network using the Router’s Virtual Private Network (VPN) capability.

Use the browser-based utility to configure settings and run convenient wizards that will help you set up the Router and its access rules.

Introduction to VPNs

A VPN is a connection between two endpoints—a VPN Router, for instance—in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

The private network is established by creating a “tunnel”. A VPN tunnel connects the two computers or networks and allows data to be transmitted over the Internet as if it were still within those networks. A VPN tunnel uses industry-standard encryption and authentication techniques to secure the data sent between the two networks.

Virtual Private Networking was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. It can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road.

There are two basic ways to create a VPN connection:

- VPN Router to VPN Router
- computer (using VPN client software) to VPN Router

The VPN Router creates a “tunnel” or channel between two endpoints, so that data transmissions between them are secure. A computer with VPN client software can be one of the two endpoints.

For an IPSec VPN tunnel, the VPN Router and any computer with the built-in IPSec Security Manager (Windows 2000 and XP) can create a VPN tunnel using IPSec (Windows Vista uses a similar utility). Other Windows operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

NOTE: The 10/100 16-Port VPN Router supports IPSec VPN client software, including the Linksys QuickVPN software. (For more information, refer to “Appendix B: Linksys QuickVPN for Windows 2000, XP, or Vista”)

For a PPTP VPN tunnel, the 10/100 16-Port VPN Router and any computer running Windows 2000 or XP can create a VPN tunnel using PPTP.

VPN Examples

The following are examples of a VPN tunnel between two VPN routers and a VPN tunnel between a computer using VPN client software and a VPN router.

VPN Router to VPN Router

For example, at home, a telecommuter uses his VPN Router for his always-on Internet connection. His Router is configured with his office’s VPN settings. When he connects to his office’s router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs use the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office’s network, as if he were physically connected.
For additional information and instructions about creating your own VPN, visit the Linksys website at www.linksys.com.
Chapter 2: Product Overview

Front Panel

- **Diag** (Orange) The Diag LED lights up when the Router is not ready for use. It turns off when the Router is ready for use.
- **System** (Green) The System LED lights up when the Router is powered on. It flashes when the Router is running a diagnostic test.
- **LAN/Act 1-13** (Green) These numbered LEDs correspond with the numbered ports (white print). The LED is solidly lit when the Router is connected to a device through the corresponding port. The LED flashes to indicate network activity over that port.

LAN/Act LEDs 9-13 and Internet/Act LEDs 3-7 represent the dual-function ports, which can be used as LAN or Internet ports. These correspond with the LAN ports 9-13 (white print) or Internet ports 3-7 (dark print) on the Router’s front panel.

- **Internet/Act 1-7** (Green) These numbered LEDs correspond with the numbered ports (dark print). The LED lights up when the Router is connected to a cable or DSL modem through the corresponding port. The LED flashes to indicate network activity over that port.

Internet/Act LEDs 1 and 2 are labeled Internet because they can be used only as Internet ports.
- **DMZ** (Orange) The DMZ LED lights up when the Router is connected to a DMZ host through the DMZ port. The LED flashes to indicate network activity over the DMZ port.

1-13 (LAN) These Ethernet ports connect the Router to wired computers and other Ethernet network devices.

LAN ports 9-13 can also be used as Internet ports.

Internet (1-7) These Ethernet ports connect the Router to Internet devices, such as cable or DSL modems.

Internet ports 3-7 can also be used as LAN ports.

- **DMZ** The DMZ port connects to a switch or public server.
- **Reset** The Reset button can be used for a warm reset or a reset to factory defaults.
  - **Warm Reset** If the Router is having problems connecting to the Internet, press and hold in the Reset button for a second using the tip of a pen. This is similar to pressing the power button on your computer to reboot it.
  - **Reset to Factory Defaults** If you are experiencing extreme problems with the Router and have tried all other troubleshooting measures, press and hold in the Reset button for 30 seconds. This will restore the factory defaults and clear all of the Router’s custom settings.

You can also reset the Router to factory defaults using the System Management > Factory Default screen of the Router’s web-based utility.

Back Panel

- **Power** The Power port connects to the AC power cord.

Left Side Panel

- **Security Slot** You can attach a lock to the security slot so the Router will be protected from theft.
Chapter 3: Installation

Physical Installation

There are three ways to place 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. The third way is to mount the Router in a standard-sized, 19-inch high rack.

Horizontal Placement

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

WARNING: Do not place excessive weight on top of the Router; too much weight could damage it.

Wall-Mount Placement

The Router has two wall-mount slots on its bottom panel. The distance between the two slots is 94 mm (3.70 inches).

Two screws are needed to mount the Router.

Suggested Mounting Hardware

<table>
<thead>
<tr>
<th>Diameter (mm)</th>
<th>Length (mm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-6</td>
<td>1.6-2</td>
</tr>
<tr>
<td>3-3.8</td>
<td></td>
</tr>
</tbody>
</table>

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

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

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.

2. Drill two holes into the wall. Make sure the holes are 94 mm (3.07 inches) apart.

3. Insert a screw into each hole and leave 2 mm (0.8 inches) below the head exposed.

4. Maneuver the Router so two of the wall-mount slots line up with the two screws.

Print this page at 100% size. Cut along the dotted line, and place on the wall to drill precise spacing.

Wall Mounting Template
Chapter 3

Installation

5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.

Rack-Mount Placement

The Router includes two brackets and eight screws for mounting on a standard-sized, 19-inch high rack. Observe the following guidelines:

- **Elevated Operating Ambient** If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

- **Reduced Air Flow** Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

- **Mechanical Loading** Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

- **Circuit Overloading** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

- **Reliable Earthing** Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

To rack-mount the Router in any standard 19-inch rack, follow these instructions.

1. Place the Router on a hard flat surface with the front panel faced towards your front side.

2. Attach a rack-mount bracket to one side of the Router with the supplied screws and secure the bracket tightly.

3. Repeat step 2 to attach the other bracket to the opposite side.

4. After the brackets are attached to the Router, use suitable screws to securely attach the brackets to any standard 19-inch rack.

Cable Connections

To connect network devices to the Router, follow these instructions:

1. Before you begin, make sure that all of your hardware is powered off, including the Router, computers, switches, and cable or DSL modem.

2. Connect one end of an Ethernet network cable to one of the numbered local ports (white print). Connect the other end to an Ethernet port on a network device, such as a computer or switch.

Repeat this step to connect more computers or other network devices to the Router.
Chapter 3

3. Connect your cable or DSL modem’s Ethernet cable to one of the Router’s Internet ports.

   Repeat this step to connect additional Internet devices to the Router’s other Internet ports.

4. If you are using the DMZ port, then connect an Ethernet cable to the DMZ port. Connect the other end to an appropriate network device, such as a public server.

5. Power on the cable or DSL modem(s). If you have a network device connected to the DMZ port, power on that network device.

6. Connect the included power cord to the Router’s Power port, and then plug the power cord into an electrical outlet.

7. The System LED on the front panel will light up as soon as the power adapter is connected properly.

8. Power on your computers and other network devices.
Chapter 4: Advanced Configuration

Overview

The Router’s web-based utility allows you to set up the Router and perform advanced configuration and troubleshooting. This chapter will explain all of the functions in this utility.

These are the main tabs of the utility: System Summary, Setup, DHCP, System Management, Port Management, Firewall, VPN, Log, Wizard, Support, and Logout. (The ProtectLink tab is available with upgraded firmware.) Additional tabs will be available after you click one of the main tabs.

How to Access the Web-Based Utility

1. For local access of the Router’s web-based utility, launch your web browser, and enter the Router’s default IP address, 192.168.1.1, in the Address field. Press the Enter key.

   ![Address Bar](image1)

   **NOTE:** If the Remote Management feature on the Firewall > General screen has been enabled, then users with administrative privileges can remotely access the web-based utility. Use http://<WAN IP address of the Router>, or use https://<WAN IP address of the Router> if you have enabled the HTTPS feature.

2. A login screen prompts you for your User name and Password. Enter admin in the User name field, and enter admin in the Password field. (You can change the Password on the Setup > Password screen.) Then click OK.

   ![Login Screen](image2)

System Summary

The first screen that appears is the System Summary screen, which displays the Router’s current status and settings. This information is read-only. Underlined text is hyperlinked to related setup pages, so if you click a hyperlink, the related setup screen will appear. On the right-hand side of this screen and all other screens of the utility is a link to the Site Map, which has links to all of the utility’s tabs. Click Site Map to view the Site Map. Then, click the desired tab.

   ![System Summary](image3)
Chapter 4

Advanced Configuration

System Information

Serial Number  Displayed here is the serial number of the Router.
Firmware version  Displayed here is the current version number of the firmware installed on the Router.
CPU  Displayed here are the type and speed of the processor installed on the Router.
DRAM  Displayed here is the size of DRAM installed on the Router's motherboard.

Flash  Displayed here is the size of flash memory installed on the Router's board.

System Up Time  This is the length of time in days, hours, and minutes that the Router has been active. The current time and date are also displayed.

Trend Micro™ ProtectLink Gateway

The optional Trend Micro ProtectLink Gateway service provides security for your network. It checks e-mail messages, filters website addresses (URLs), and blocks potentially malicious websites.

NOTE: If the Trend Micro ProtectLink Gateway options are not displayed on the System Summary screen, you can upgrade the Router’s firmware if you want to purchase and use this optional service. Refer to “Appendix F: Firmware Upgrade” for instructions.

Go buy  To purchase a license to use this service, click Go buy. You will be redirected to a list of Linksys resellers on the Linksys website. Then follow the on-screen instructions.

Register  If you already have a license, click Register. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

NOTE: To have your e-mail checked, you will need to provide the domain name and IP address of your e-mail server. If you do not know this information, contact your Internet Service Provider (ISP).

Activate  If you have registered, click Activate. You will be redirected to the Trend Micro ProtectLink Gateway website. Follow the on-screen instructions.

For more information, refer to “Appendix G: Trend Micro ProtectLink Gateway Service.”

Configuration

If you need help to configure the Router, click Setup Wizard, and follow the on-screen instructions. For additional information, refer to the “Wizard” section of this chapter.

Port Statistics

The image of the Router’s front panel displays the status of each port. If a port is disabled, it will be red; if a port is enabled, it will be black. If a port is connected, it will be green. Click any port to view the port’s Summary table in a separate window.
The Summary table shows the settings of the selected port, including Type, Interface, Link Status, Port Activity, Priority, Speed Status, Duplex Status, Auto negotiation, and VLAN.

For the selected port, the statistics table shows this information: number of packets received, number of packet bytes received, number of packets transmitted, number of packet bytes transmitted, and number of packet errors.

To update the on-screen information, click Refresh. To exit this screen, click Close.

Network Setting Status

LAN IP It shows the current LAN IP address of the Router, as seen by internal users on the network, and it hyperlinks to the LAN Setting section on the Network screen of the Setup tab.

WAN IP This shows the current WAN IP addresses of the Router, as seen by external users on the Internet and hyperlinks to the WAN Setting section on the Setup > Network screen. By default, the Router provides two WAN ports. On the Setup > Network screen, you can set up additional WAN ports.

If the port is set to Obtain an IP automatically, two buttons, Release and Renew, will be available. Click Release to release the IP address, and click Renew to update the DHCP Lease Time or get a new IP address. If the WAN port is set to PPPoE or PPTP, two buttons, Connect and Disconnect, will be available.

DMZ IP This shows the DMZ IP address, as seen by external users on the Internet and hyperlinks to the DMZ Setting section on the Setup > Network screen.

Mode It shows the Router’s Working Mode (Gateway or Router), and it hyperlinks to the Dynamic Routing section on the Setup > Advanced Routing screen.

DNS It shows all DNS server IP addresses and hyperlinks to the WAN Connection Type settings on the Setup > Network screen.

Bandwidth Management It shows the Bandwidth Management settings of the Router’s WAN port(s) and hyperlinks to the System Management > Bandwidth Management screen.

DDNS It shows the DDNS settings of the Router’s WAN port(s) and hyperlinks to the Setup > DDNS screen.

DMZ Host It shows the DMZ private IP address and hyperlinks to the Setup > DMZ Host screen. The default is Disabled.

Firewall Setting Status

SPI (Stateful Packet Inspection) It shows the status (On/Off) of the SPI setting and hyperlinks to the Firewall > General screen.

DoS (Denial of Service) It shows the status (On/Off) of the DoS setting and hyperlinks to the Firewall > General screen.

Block WAN Request It shows the status (On/Off) of the Block WAN Request setting and hyperlinks to the Firewall > General screen.

VPN Setting Status

VPN Summary It hyperlinks to the VPN > Summary screen.

Tunnel(s) Used It shows the number of VPN tunnels used.

Tunnel(s) Available It shows the number of VPN tunnels available.

Current Connected (The Group Name of GroupVPN1) users It shows the number of users. (If the GroupVPN feature is disabled, the message, “No Group VPN was defined”, is displayed.)

Current Connected (The Group Name of GroupVPN2) users It shows the number of users.

PPTP Server It shows the status of the PPTP Server feature.

Log Setting Status

It hyperlinks to the Log > System Log screen of the Log tab.

If you have not set up the e-mail server on the Log tab, the message, “E-mail cannot be sent because you have
not specified an outbound SMTP server address," will be displayed.

If you have set up the mail server but the log has not been generated due to the Log Queue Length and Log Time Threshold settings, the message, "E-mail settings have been configured," will be displayed.

If you have set up the e-mail server and the log has been sent to the e-mail server, the message, "E-mail settings have been configured and sent out normally," will be displayed.

If you have set up the e-mail server and the log cannot be sent to the e-mail server, the message, "E-mail cannot be sent out, probably use incorrect settings," will be displayed.

Setup > Network

The Network screen shows all of the Router's basic setup functions. The Router can be used in most network setups without changing any of the default values; however, you may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL or cable) carrier. The setup information is provided by your ISP.

Device IP Address and Subnet Mask  The default values are 192.168.1.1 for the Router's local IP address and 255.255.255.0 for the subnet mask.

Multiple Subnet  You can add more Class C networks to expand the network. Select this option to enable the Multiple Subnet feature. Then click Add/Edit to create or modify subnet(s). A new screen appears.

Create or Modify a Subnet

LAN IP Address  Enter the LAN IP address.

Subnet Mask  Enter the subnet mask.

For example, the current LAN settings show the Device IP Address as 192.168.1.1 and the Subnet Mask as 255.255.255.0. To add one more Class C network, enter the following:

- **LAN IP Address** 192.168.2.1
- **Subnet Mask** 255.255.255.0

Click Add to List. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Network screen.

Network

Host Name and Domain Name  Enter a host and domain name for the Router. Some 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, you can leave these fields blank.

LAN Setting

The LAN MAC address of the Router is displayed.
Chapter 4

Add One More Class C Network

If you want to modify a subnet you have created, select it and make changes. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Network** screen.

If you want to delete a subnet you have created, select it and click **Delete selected subnet**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Network** screen.

You can also divide a Class C network into four subnets. For example, the current LAN settings show the Device IP Address as 192.168.1.1 and the Subnet Mask as 255.255.255.192.

![LAN Settings Example](image)

To get the other three subnets, enter the following:

**Subnet 1**
- **LAN IP Address**: 192.168.2.65
- **Subnet Mask**: 255.255.255.192

**Subnet 2**
- **LAN IP Address**: 192.168.2.129
- **Subnet Mask**: 255.255.255.192

**Subnet 3**
- **LAN IP Address**: 192.168.2.193
- **Subnet Mask**: 255.255.255.192

Click **Add to List**. Then click **Save Settings**.

Create Three Additional Subnets

**WAN Setting**

By default, the Router allows you to simultaneously connect two broadband connections to the Router; however, you can set up as many as seven broadband connections.

From the drop-down menu, select how many WAN ports you want to use. The default is **2**. (You can also change the number of WAN ports using the **Port Management > Port Setup** screen.) Make sure the physical network configuration matches the number of WAN port settings on this screen.

If you change the number of WAN ports, click **Save Settings** to save your change. A confirmation message will appear. Then click **OK** to save the new setting.

The WAN Setting table displays the WAN port numbers in the **Interface** column and their respective connection types in the **Connection Type** column. Click **Edit** in the **Config.** column to change the WAN settings of the selected WAN port. You must save the new number of WAN ports before you can click **Edit** to change the settings of any new WAN ports.

The **Connection Type** column will display the word "Undefined" if you changed the number of WAN ports but did not click Save Settings. After you save this setting, the Connection Type column will display, “Obtain an IP automatically.” The default Connection Type of all WAN ports is **Obtain an IP automatically**.

**Edit WAN Connection**

After you clicked **Edit**, configure the WAN settings for the selected WAN port.

**Interface** The selected WAN port will be displayed.
These are the available connection types: Obtain an IP automatically, Static IP, PPPoE, PPTP, and Heart Beat Signal. Depending on which connection type you select, you will see various settings.

**Obtain an IP Automatically**

If your ISP automatically assigns an IP address, select **Obtain an IP automatically**. (Most cable modem subscribers use this connection type.) Your ISP assigns these values.

**Use the Following DNS Server Addresses** If you want to specify DNS server IP addresses, select this option.

**DNS Server (Required) 1/2** If you select Use the Following DNS Server Addresses, enter at least one DNS server IP address. Multiple DNS server IP settings are common. In most cases, the first available DNS entry is used.

**MTU** The Maximum Transmission Unit (MTU) setting specifies the largest packet size permitted for network transmission. In most cases, keep the default, Auto. To specify the MTU, select Manual, and then enter the maximum MTU size.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Back** to return to the Network screen without saving any changes.

**Static IP**

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

**Specify WAN IP Address** Enter the external IP address of the Router.

**Subnet Mask** Enter the subnet mask of the Router.

**Default Gateway Address** Enter the IP address of the default gateway.

**DNS Server (Required) 1/2** Enter at least one DNS server IP address. Multiple DNS server IP settings are common. In most cases, the first available DNS entry is used.

**MTU** The Maximum Transmission Unit (MTU) setting specifies the largest packet size permitted for network transmission. In most cases, keep the default, Auto. To specify the MTU, select Manual, and then enter the maximum MTU size.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Back** to return to the Network screen without saving any changes.

**PPPoE (Point-to-Point Protocol over Ethernet)**

Some DSL-based Internet Service Providers (ISPs) use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE, select PPPoE.

**User Name and Password** Enter your account’s User Name and Password. The maximum number of characters is 60.

**Service Name** Enter the Service Name, if provided by your ISP.

**Connect on Demand** If you select the Connect on Demand option, the connection will be disconnected after a specified period of inactivity (Max Idle Time). If you have been disconnected 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. Enter the number of minutes you want to have elapsed before your Internet access disconnects. The default Max Idle Time is 5 minutes.
Chapter 4

Advanced Configuration

Keep Alive: Redial Period If you select the Keep Alive option, the Router will keep the connection alive by sending out a few data packets periodically, so your ISP thinks that the connection is still active. This option keeps your connection active indefinitely, even when it sits idle. The default Redial Period is 30 seconds.

MTU The Maximum Transmission Unit (MTU) setting specifies the largest packet size permitted for network transmission. In most cases, keep the default, Auto. To specify the MTU, select Manual, and then enter the maximum MTU size.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the Network screen without saving any changes.

PPTP (Point-to-Point Tunneling Protocol)

Point to Point Tunneling Protocol (PPTP) is a service used in Europe, Israel, and other countries.

Specify WAN IP Address Enter the external IP address of the Router.

Subnet Mask Enter the subnet mask of the Router.

Default Gateway Address Enter the IP address of the default gateway.

User Name and Password Enter your account’s User Name and Password. The maximum number of characters is 60.

Connect on Demand If you select the Connect on Demand option, the connection will be disconnected after a specified period of inactivity (Max Idle Time). If you have been disconnected 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. Enter the number of minutes you want to have elapsed before your Internet access disconnects. The default Max Idle Time is 5 minutes.

Keep Alive If you select the Keep Alive option, the Router will keep the connection alive by sending out a few data packets periodically, so your ISP thinks that the connection is still active. This option keeps your connection active indefinitely, even when it sits idle. The default Redial Period is 30 seconds.

MTU The Maximum Transmission Unit (MTU) setting specifies the largest packet size permitted for network transmission. In most cases, keep the default, Auto. To specify the MTU, select Manual, and then enter the maximum MTU size.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the Network screen without saving any changes.

Heart Beat Signal

Heart Beat Signal is a service used in Australia only.

User Name and Password Enter your account’s User Name and Password. The maximum number of characters is 60.

Heart Beat Server Enter the IP address of the Heart Beat server.

MTU The Maximum Transmission Unit (MTU) setting specifies the largest packet size permitted for network transmission. In most cases, keep the default, Auto. To specify the MTU, select Manual, and then enter the maximum MTU size.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the Network screen without saving any changes.

DMZ Setting

The Router comes with a special DMZ port, which is used for setting up public servers. The DMZ port sits between the local network ports and the Internet port. Servers on the DMZ are publicly accessible. Use of the DMZ port is optional; it may be left unconnected.

Using the DMZ is preferred and is, if practical, a strongly recommended alternative to using public LAN servers or putting these servers on WAN ports where they are not protected and not accessible by users on the LAN.
Each of the servers on the DMZ will need a unique, public Internet IP address. The ISP you use to connect your network to the Internet should be able to provide these addresses, as well as information on setting up public Internet servers. If you plan to use the DMZ setting, contact your ISP for the static IP information.

The DMZ Setting table displays the DMZ port name in the Interface column and its IP address in the IP Address column. Click Edit in the Config. column to change the DMZ settings of the DMZ port.

Edit DMZ Connection
After you clicked Edit, configure the DMZ settings.

Interface  The DMZ port will be displayed. Static IP is automatically selected.

Specify DMZ IP Address  Enter the IP address of the computer connected to the DMZ port.
Subnet Mask  Enter the subnet mask of the computer connected to the DMZ port.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the Network screen without saving any changes.

Setup > Password

The Router’s default User Name and Password is admin, and Linksys strongly recommends that you change the Router’s password from the default to a unique password.

NOTE: The password cannot be recovered if it is lost or forgotten. If the password is lost or forgotten, you have to reset the Router to its factory default settings; this will remove all of your configuration changes.

Password

The User Name is admin; it cannot be changed.
Old Password  Enter the old password. The default is admin when you first power up the Router.
New Password  Enter a new password for the Router. Your password must have 20 or fewer characters and cannot contain any spaces.
Confirm New Password  Re-enter the new password to confirm it.

Click Save Settings to save your change, or click Cancel Changes to undo it.

Setup > Time

The Router uses the time settings to time stamp log events, automatically apply the Access Rules and Content Filter, and perform other activities for other internal purposes.

Time

To set the local time, select Set the local time using the Network Time Protocol (NTP) automatically or Set the local time Manually.

Automatic

Time Zone  Select your time zone. The default is (GMT-08:00) Pacific Time (US & Canada); Tijuana.
Daylight Saving  To use the daylight saving feature, select Enabled. Enter the Month and Day of the start date, and then enter the Month and Day of the end date.

NTP Server  Enter the URL or IP address of the NTP server. The default is time.nist.gov.

Manual

**Setup > Time > Manual**

**Hours, Minutes, Seconds**  Enter the time.
**Month, Day, Year**  Enter the date.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

**Setup > DMZ Host**

The DMZ (Demilitarized Zone) Host feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. Although Port Range Forwarding can only forward ten ranges of ports maximum, DMZ hosting forwards all the ports to one computer at the same time.

**DMZ Host**

**DMZ Private IP Address**  Enter the local IP address of the computer you want to expose. The default value of 0 deactivates the DMZ Host.

Click Save Settings to save your change, or click Cancel Changes to undo it.

**Setup > Forwarding**

The Forwarding screen allows you to set up port range forwarding and port triggering applications. Port range forwarding can be used to set up public services or other specialized Internet applications on your network, while port triggering can be used to set up triggered ranges and forwarded ranges for Internet applications.

**Forwarding**

**Port Range Forwarding**

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Router can forward those requests to computers equipped to handle the requests. If, for example, you set the port number 80 (HTTP) to be forwarded to IP address 192.168.1.2, then all HTTP requests from outside users will be forwarded to 192.168.1.2.

**NOTE:** You must disable the Router’s DHCP function to use port forwarding.

You may use this function to establish a web server or FTP server via an IP gateway. Make sure that you enter a valid IP address. (You may need to establish a static IP address in order to properly run an Internet server.) For added security, Internet users will be able to communicate with the server, but they will not actually be connected. The packets will simply be forwarded through the Router.

**Service**  Select the Service you want.

**IP Address**  Enter the IP address of the server that you want the Internet users to access.
**Enable** Select **Enable** to enable this port range forwarding entry.

If the Service you need is not listed in the menu, click **Service Management** to add the new service. The **Service Management** screen appears.

![Service Management](image)

**Service Name** Enter a name.

**Protocol** Select the protocol it uses.

**Port Range** Enter its range.

Click **Add to List**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Forwarding** screen.

If you want to modify a service you have created, select it and click **Update this service**. Make changes. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Forwarding** screen.

If you want to delete a service you have created, select it and click **Delete selected service**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Forwarding** screen.

On the **Forwarding** screen, click **Add to List**, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click **Delete selected application**.

**Port Triggering**

Port triggering 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.

Some Internet applications or games use alternate ports to communicate between the server and LAN host. When you want to use these applications, enter the triggering (outgoing) port and alternate incoming port in the Port Triggering table. Then the Router will forward the incoming packets to the LAN host.

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

**Trigger Port Range** Enter the starting and ending port numbers of the trigger port range.

**Incoming Port Range** Enter the starting and ending port numbers of the incoming port range.

Click **Add to List**, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click **Delete selected application**.

Click **Show Tables** to see the details of your entries. The Port Range Forwarding Table List appears.

![Port Range Forwarding Table List](image)

**Port Range Forwarding** Select this option to view the Port Range Forwarding entries.

**Port Triggering** Select this option to view the Port Triggering entries.

![Port Triggering Table List](image)

Click **Refresh** to update the on-screen information. Click **Close** to exit this screen and return to the **Forwarding** screen.

On the **Forwarding** screen, click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**Setup > UPnP**

Universal Plug and Play (UPnP) can be used to set up public services on your network. When the UPnP function is enabled, Windows XP or Vista can modify these entries via UPnP.
Chapter 4

Advanced Configuration

UPnP

UPnP Function  Select Yes to enable the UPnP function. Otherwise, keep the default, No.

Service  Select the Service you want.

Name or IP Address  Enter the name or IP address of the server that you want the Internet users to access.

Enable  Select Enable to enable this UPnP entry.

If the Service you need is not listed in the menu, click Service Management to add the new service. The Service Management screen appears.

Service Name  Enter a name.

Protocol  Select the protocol it uses.

External Port  Enter the external port number.

Internal Port  Enter the internal port number.

Click Add to List. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the UPnP screen.

If you want to modify a service you have created, select it and click Update this service. Make changes. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the UPnP screen.

If you want to delete a service you have created, select it and click Delete selected service. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the UPnP screen.

On the UPnP screen, click Add to List, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click Delete selected application.

Click Show Tables to see the details of your entries. The UPnP Forwarding Table List appears.

Service Management

UPnP Forwarding Table List

Click Refresh to update the on-screen information. Click Close to exit this screen and return to the UPnP screen.

On the UPnP screen, click Save Settings to save your changes, or click Cancel Changes to undo them.

Setup > One-to-One NAT

One-to-One NAT (Network Address Translation) creates a relationship that maps valid external IP addresses to internal IP addresses hidden by NAT. A device with an internal IP address may be accessed at the corresponding external valid IP address.

To create this relationship, define internal and external IP address ranges of equal length. Once the relationship is defined, the device with the first internal IP address is accessible at the first IP address in the external IP address range, and so forth.

For example, you have a Local Area Network (LAN) for which the ISP has assigned the IP address range of 209.19.28.16 to 209.19.28.31, with 209.19.28.16 used as the Wide Area Network (WAN) or NAT public IP address of the Router. The address range of 192.168.168.1 to 192.168.168.255 is used for the devices on the LAN. With One-to-One NAT, the devices with the internal IP addresses of 192.168.168.2 to 192.168.168.15 may be accessed at the corresponding external IP addresses.

NOTE: The Router’s WAN IP address should not be included in the range you specify.
One-to-One NAT

Select Enable to use the One-to-One NAT function.

Add Range

Enter the starting IP address of the internal IP address range. This is the IP address of the first device that can be accessed from the Internet.

Enter the starting IP address of the public IP address range. This IP address is provided by the ISP. (Do not include the Router’s WAN IP Address.)

Enter the number of IP addresses in the range. The range length cannot exceed the number of valid IP addresses. To map a single address, enter 1.

Click Add to List, and configure as many entries as you would like, up to a maximum of ten. To delete an entry, select it and click Delete selected range.

NOTE: One-to-One NAT affects how the firewall functions work. Access to LAN devices from the Internet is allowed unless additional Deny access rules are configured on the Firewall > Access Rules screen.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

Setup > MAC Clone

Some ISPs require that you register a MAC address, which is a 12-digit code assigned to a unique piece of hardware for identification. The MAC Clone feature “clones” your network adapter’s MAC address onto the Router, so you don’t have to call your ISP to change the registered MAC address to the Router’s MAC address.

MAC Clone

The MAC Clone table displays the number of WAN ports and MAC addresses in the MAC Address column. Click Edit in the Config. column to change the MAC Clone setting of the selected WAN port.

After you clicked Edit, configure the MAC Clone settings for the selected WAN port.

Interface The selected WAN port will be displayed.

Enable/Disable Select the status of the MAC Clone feature.

User Defined WAN MAC Address To manually clone a MAC address, select User Defined WAN MAC Address, and then enter the 12 digits of your adapter’s MAC address.

MAC Address from this PC To clone the MAC address of the computer you are currently using to configure the Router, select MAC Address from this PC.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the MAC Clone screen without saving any changes.
Setup > DDNS

Dynamic Domain Name System (DDNS) service allows you to assign a fixed domain name to a dynamic WAN IP address, so you can host your own web, FTP or other type of TCP/IP server in your LAN. The DDNS feature is disabled by default.

Before configuring DDNS, visit the website of the DDNS service you want to use: www.dyndns.org, www.3322.org, or www.oray.net. Then register a domain name.

DDNS

The DDNS table displays the number of WAN ports, their status, and Host Names. Click Edit in the Config. column to change the DDNS settings of the selected WAN port.

Edit DDNS

After you clicked Edit, configure the DDNS settings for the selected WAN port.

Interface  The selected WAN port will be displayed.

DDNS Service  The DDNS feature is disabled by default. To enable this feature, select DynDNS.org, 3322.org, or Oray.net PeanutHull DDNS.

DynDNS.org

User name  Enter your DynDNS.org account information.

Password  Enter your DynDNS.org account information.

Host Name  Enter your host name in the three Host Name fields. For example, if your host name were myhouse.dyndns.org, then myhouse would go into the first field, dyndns would go into the second field, and org would go into the last field.

Custom DNS  DynDNS.org offers a free account and a paid account, which use different authentication methods. If you have a paid account, select this option to register the paid account with the DDNS server of DynDNS.org.

Click Save Settings, and the status of the DDNS function will be updated.

Internet IP Address  The Router’s current Internet IP address is displayed. Because it is dynamic, this will change.

Status  The status of the DDNS function is displayed. If the status information indicates an error, make sure you have correctly entered the information for your account with your DDNS service.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the DDNS screen without saving any changes.

3322.org

User name  Enter your 3322.org account information.

Password  Enter your 3322.org account information.

Host Name  Enter your host name in the three Host Name fields. For example, if your host name were myhouse.3322.org, then myhouse would go into the first field, 3322 would go into the second field, and org would go into the last field.

Click Save Settings, and the status of the DDNS function will be updated.

Internet IP Address  The Router’s current Internet IP address is displayed. Because it is dynamic, this will change.
**Status**  The status of the DDNS function is displayed. If the status information indicates an error, make sure you have correctly entered the information for your account with your DDNS service.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Back** to return to the DDNS screen without saving any changes.

**Oray.net PeanutHull DDNS**

![Oray.net PeanutHull DDNS Setup Screen](image1)

**User name**  Enter your PeanutHull account information.

**Password**  Enter your PeanutHull account information.

**Host Name**  Enter your host name in the three **Host Name** fields. For example, if your host name were myhouse.oray.net, then myhouse would go into the first field, oray would go into the second field, and net would go into the last field.

Click **Save Settings**, and the status of the DDNS function will be updated.

**Internet IP Address**  The Router’s current Internet IP address is displayed. Because it is dynamic, this will change.

**Status**  The status of the DDNS function is displayed. If the status information indicates an error, make sure you have correctly entered the information for your account with your DDNS service.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Back** to return to the DDNS screen without saving any changes.

**Setup > Advanced Routing**

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

![Advanced Routing Screen](image2)

**Advanced Routing**

**Dynamic Routing**

The Router’s dynamic routing feature can be used, so the Router will automatically adjust to physical changes in the network’s layout. Using the dynamic RIP protocol, the Router calculates the most efficient route for the network’s data packets to travel between the source and the destination, based upon the shortest paths. The RIP protocol regularly broadcasts routing information to other routers on the network. It determines the route that the network packets take based on the fewest number of hops between the source and the destination.

**Working Mode**  Select **Gateway** mode if the Router is hosting your network’s connection to the Internet. Select **Router** mode if the Router exists on a network with other routers, including a separate network gateway that handles the Internet connection. In Router mode, any computer connected to the Router will not be able to connect to the Internet unless you have another router function as the gateway.

**RIP (Routing Information Protocol)**  To use dynamic routing for communication of network data, select **Enabled**. Otherwise, keep the default, **Disabled**.

**Receive RIP versions**  To use dynamic routing for reception of network data, select the protocol you want: **None**, **RIPv1**, **RIPv2**, or **Both RIPv1 and RIPv2**.

**Transmit RIP versions**  To use dynamic routing for transmission of network data, select the protocol you want: **None**, **RIPv1**, **RIPv2 - Broadcast**, or **RIPv2 - Multicast**.
Chapter 4

Advanced Configuration

Static Routing

If the Router is connected to more than one network or there are multiple routers installed on your network, it may be necessary to set up static routes. The static routing function determines the path that data follows over your network before and after it passes through the Router. You can use static routing to allow different IP domain users to access the Internet through the Router.

Static routing is a powerful feature that should be used by advanced users only. In many cases, it is better to use dynamic routing because it enables the Router to automatically adjust to physical changes in the network's layout.

**NOTE:** Static routing is an advanced feature. Create these routes with care.

To create a static route entry, enter the following information:

Destination IP  Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be 0.

Subnet Mask  Enter the subnet mask used on the destination LAN IP domain. For Class C IP domains, the subnet mask is 255.255.255.0.

Default Gateway  Enter the IP address of the router of the network, for which this static route is created. For example, if this network is connected to the local router’s LAN port through another router, use the WAN IP address of that router.

Hop Count  Enter the appropriate value (maximum is 15). This indicates the number of nodes that a data packet passes through before reaching its destination. A node is any device on the network, such as a computer or router.

Interface  Select the appropriate interface. The Interface tells you whether your network is on the LAN or WAN. If the gateway router is on a LAN port, then select LAN. If you are connecting to another network through the Internet, select the appropriate WAN port option.

Click Add to List, and configure as many entries as you would like, up to a maximum of 30. To delete an entry, select it and click Delete selected IP.

Click Show Routing Table to see the details of your entries.

DHCP > Setup

The Router can be used as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server automatically assigns available IP addresses to computers on your network. If you choose to enable the DHCP server option, all of the computers on your LAN must be set to obtain an IP address automatically from a DHCP server. (By default, Windows computers are set to obtain an IP automatically.)

If the Router’s DHCP server function is disabled, do one of the following:

- Configure the IP address, subnet mask, and DNS settings of every computer on your network. (Make sure you do not assign the same IP address to different computers.)
- Set up a stand-alone DHCP server with the Router as the default gateway.

Click Refresh to update the on-screen information. Click Close to exit this screen and return to the Advanced Routing screen.

On the Advanced Routing screen, click Save Settings to save your changes, or click Cancel Changes to undo them.
Chapter 4
Advanced Configuration

DHCP > Setup

Setup

Enable DHCP Server To use the Router as your network’s DHCP server, select Enable DHCP Server. If you already have a DHCP server on your network, remove the check mark. Then configure the Dynamic IP settings.

Dynamic IP

- **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. The range is 5-43,200 minutes. The default is 1440 minutes.

- **Dynamic IP Range Start/End** Enter a starting IP address and ending IP address to create a range of available IP addresses. The default range is 100-149. (Make sure the Router’s LAN IP address is not in this dynamic IP range.) For example, if the Router uses the default LAN IP address, 192.168.1.1, then the starting value must be 192.168.1.2 or greater.

Static IP

You can assign a static IP address to a specific device based on its MAC address.

Show unknown MAC addresses Click Show unknown MAC addresses to view all devices’ IP addresses and corresponding MAC addresses. The Unknown MAC Addresses List appears.

For each device, you can enter a descriptive name in the Name field. To add an IP address and MAC address set to the Static IP list, select Enable, and then click Apply. To add all IP addresses and MAC addresses to the Static IP list, click Select All.

To update the on-screen information, click Refresh. To exit this screen and return to the Setup screen, click Close.

Static IP Address Enter the static IP address. You can enter 0.0.0.0 if you want the Router to assign a static IP address to the device.

Name Enter a descriptive name for the device.

Enable Select Enable to assign the static IP address to this device.

Click Add to List, and configure as many entries as you would like, up to a maximum of 100. To delete an entry, select it and click Delete selected Entry.

Block MAC address on the list with wrong IP address To block traffic from devices with MAC addresses on the Static IP list but using the wrong IP addresses, select this option. It prevents users from changing device IP addresses without your permission.

Block MAC address not on the list To block traffic from devices using dynamic IP addresses, select this option. It blocks all devices with MAC addresses not listed on the Static IP list.

DNS

DNS Server 1-2 You can assign DNS server(s) to the DHCP clients so the Router will use the DNS server(s) for faster access to functioning DNS server(s). Enter the IP address of at least one DNS server.

WINS

WINS Server Windows Internet Naming Service (WINS) is a service that resolves NetBIOS names to IP addresses. WINS is assigned if the computer (DHCP client) requests one. If you do not know the IP address of the WINS server, keep the default, 0.0.0.0.
**NOTE:** To support NetBIOS for DHCP clients, the Router uses two methods.

First, when the DHCP clients receive dynamic IP addresses from the Router, it automatically includes the information of the WINS server to support NetBIOS. Second, if a user sets up a static IP address, then the IP address, subnet mask, default gateway, and DNS server settings must be configured on the Internet Protocol (TCP/IP) screen of the Windows operating system. Then the WINS IP address must be configured on the advanced TCP/IP screen. (For more information, refer to Windows Help.)

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**DHCP > Status**

On the **Status** screen, view the status information for the DHCP server and its clients.

![DHCP > Status](image)

**System Management > Multi-WAN**

For the Load Balance feature, you have a choice of Intelligent Balancer (Auto Mode) and IP Group (By Users), except for WAN1. The Router reserves at least one WAN port for non-IP Group users, so WAN1 will always be set to Intelligent Balancer (Auto Mode).

![System Management > Multi-WAN > Intelligent Balancer (Auto Mode)](image)

**Load Balance**

**Mode**

**Intelligent Balancer (Auto Mode)** Select this option if you want all WAN ports to be in Auto Mode. The Router will automatically compute the maximum bandwidth of...
all WAN ports by using Weighted Round Robin to balance the loading.

**IP Group (By Users)** Select this option to group traffic by different priority levels or classes of service (CoS). It can ensure bandwidth and higher priority for the specific IP addresses of important users, and the IP Group users don’t need to share bandwidth with lower classification users who use Intelligent Balancer mode.

If you change the Router’s Load Balance Mode, a confirmation message will appear. You have to save this change before you can change the settings of any WAN ports.

**Interface Setting**

The Interface Setting displays the number of WAN ports and their Load Balance mode in the Mode column. Click **Edit** in the Config. column to change the Load Balance settings of the selected WAN port.

**Edit Load Balance (Intelligent Balancer)**

After you clicked Edit, configure the Load Balance settings for the selected WAN port.

---

**Bandwidth**

**Interface** The selected WAN port will be displayed.

**The Max. Bandwidth provided by ISP**

**Upstream** Enter the maximum upstream bandwidth provided by your ISP. The default is **512 kbit/sec**.

**Downstream** Enter the maximum downstream bandwidth provided by your ISP. The default is **512 kbit/sec**.

**Network Service Detection**

Network Service Detection can test a WAN port’s network connectivity by pinging the Default Gateway or a specific IP address. This tool can detect the network connection status of the ISP if you have set up the DNS server in the **Setup > Network** screen. If you did not set up the DNS server, the checkbox will be grayed out, and then you cannot use the DNS lookup tool.

**Network Service Detection** Network Service Detection helps manage your connection and can report when your connection experiences problems. To use this service, select this option.

**Retry Count** Enter the number of times the Router will try to reconnect if the connection fails.

**Retry Timeout** Enter the number of times the Router will try to make a connection to your ISP before it times out.

**When Fail** Should the connection be lost, set the Router to perform one of the following actions, **Remove the Connection** or **Generate the Error Condition in the System Log**.

- **Remove the Connection** Failover will occur; the backup will be used. When the WAN port’s connectivity is restored, its traffic will also be restored.
- **Generate the Error Condition in the System Log** Failover will not occur; only an error condition will be logged.

**Default Gateway** Select this option to ping the Default Gateway.

**ISP Host** Select this option to ping the ISP Host. Then enter the IP address.

**Remote Host** Select this option to ping the Remote Host. Then enter the IP address.

**DNS Lookup Host** Select this option to ping the DNS Lookup Host. Then enter the IP address.

**Protocol Binding**

The Router supports Protocol Binding functionality. This allows you to specify the internal IP and/or Service going through the selected WAN port.

**Service** Select the Service you want.

If the Service you need is not listed in the menu, click **Service Management** to add the new service. The **Service Management** screen appears.
Service Management

**Service Name**  Enter a name. For IP Binding only, select All.

**Protocol**  Select the protocol it uses.

**Port Range**  Enter its range.

Click **Add to List**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the Multi-WAN screen.

If you want to modify a service you have created, select it and click **Update this service**. Make changes. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the Multi-WAN screen.

If you want to delete a service you have created, select it and click **Delete selected service**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the Multi-WAN screen.

**Source IP**  Enter the source IP address or range. If you need Service Binding only, then you can keep the default, which is 0.

**Destination IP**  Enter the destination IP address or range. If you need Service Binding only, then you can keep the default, which is 0.

**Enable**  Select **Enable** to use this Protocol Binding rule.

Click **Add to List**, and configure as many rules as you would like, up to a maximum of 100. To delete a rule, select it and click **Delete selected application**.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

On the **Edit Load Balance** screen, click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Back** to return to the Multi-WAN screen without saving any changes.

---

**Edit Load Balance (IP Group)**

After you clicked **Edit**, configure the Load Balance settings for the selected WAN port.

**Bandwidth**

**Interface**  The selected WAN port will be displayed.

**The Max. Bandwidth provided by ISP**

**Upstream**  Enter the maximum upstream bandwidth provided by your ISP. The default is 512 kbit/sec.

**Downstream**  Enter the maximum downstream bandwidth provided by your ISP. The default is 512 kbit/sec.

**Network Service Detection**

Network Service Detection can test a WAN port's network connectivity by pinging the Default Gateway or a specific IP address. This tool can detect the network connection status of the ISP if you have set up the DNS server in the **Setup > Network** screen. If you did not set up the DNS server, the checkbox will be grayed out, and then you cannot use the DNS lookup tool.

**Network Service Detection**  Network Service Detection helps manage your connection and can report when your connection experiences problems. To use this service, select this option.

**Retry Count**  Enter the number of times the Router will try to reconnect if the connection fails.
Retry Timeout  Enter the number of times the Router will try to make a connection to your ISP before it times out.

When Fail  Should the connection be lost, set the Router to perform one of the following actions, Remove the Connection or Generate the Error Condition in the System Log.

- Remove the Connection  Failover will occur; the backup will be used. When the WAN port's connectivity is restored, its traffic will also be restored.

- Generate the Error Condition in the System Log  Failover will not occur; only an error condition will be logged.

Default Gateway  Select this option to ping the Default Gateway.

ISP Host  Select this option to ping the ISP Host. Then enter the IP address.

Remote Host  Select this option to ping the Remote Host. Then enter the IP address.

DNS Lookup Host  Select this option to ping the DNS Lookup Host. Then enter the IP address.

IP Group

The IP Group settings allow you to specify the IP Group, as well as the Service or Destination IP going through the selected WAN port.

These settings are not available for WAN1, which always uses Intelligent Balancer (Auto Mode).

Service  Select the Service you want.

If the Service you need is not listed in the menu, click Service Management to add the new service. The Service Management screen appears.

Port Range  Enter its range.

Click Add to List. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Multi-WAN screen.

If you want to modify a service you have created, select it and click Update this service. Make changes. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Multi-WAN screen.

If you want to delete a service you have created, select it and click Delete selected service. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Multi-WAN screen.

Source IP  Enter the source IP address or range. If you only need to specify the Service, then keep the default, which is 0 to 0.

Destination IP  Enter the destination IP address or range. If you only need to specify the Service, then keep the default, which is a series of zeroes.

Enable  Select Enable to use this Protocol Binding rule.

Click Add to List, and configure as many rules as you would like, up to a maximum of 100. To delete a rule, select it and click Delete selected application.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

On the Edit Load Balance screen, click Save Settings to save your changes, or click Cancel Changes to undo them. Click Back to return to the Multi-WAN screen without saving any changes.

System Management > Bandwidth Management

Quality of Service (QoS) features let you control how the Router manages network traffic. With Bandwidth Management (Layer 3), the Router can provide better service to selected types of network traffic. There are two types of functionality available, and only one type can work at one time. Rate Control functionality is for minimum (guaranteed) bandwidth and maximum bandwidth by service or IP address, while Priority functionality is for services. Both types can control inbound or outbound traffic.
Chapter 4

Advanced Configuration

Bandwidth Management

The Maximum Bandwidth provided by ISP

**Upstream** Enter the maximum upstream bandwidth provided by your ISP. The default is 512 kbit/sec.

**Downstream** Enter the maximum downstream bandwidth provided by your ISP. The default is 512 kbit/sec.

Bandwidth Management Type

**Type** Select the type of functionality you want to use, **Rate Control** or **Priority**. Rate Control functionality is for minimum (guaranteed) bandwidth and maximum (limited) bandwidth by service or IP address, while Priority functionality is for services. Then proceed to the instructions for the type you selected.

Rate Control

**Interface** Select the appropriate WAN interface.

**Service** Select the Service you want.

If the Service you need is not listed in the menu, click **Service Management** to add the new service. The Service Management screen appears.

Service Name  Enter a name.

Protocol  Select the protocol it uses.

Port Range  Enter its range.

IP  Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, 0.

Direction  Select **Upstream** for outbound traffic, or select **Downstream** for inbound traffic.

**Min. Rate** Enter the minimum rate for the guaranteed bandwidth.

**Max. Rate** Enter the maximum rate for the maximum bandwidth.

**Enable** Select **Enable** to use this Rate Control rule.

Click **Add to List**, and configure as many rules as you would like, up to a maximum of 100. To delete a rule, select it and click **Delete selected application**.

Click **Summary** to see a summary of the Rate Control rules.
Chapter 4  
Advanced Configuration

To change a rule, click **Edit**. To update the list, click **Refresh**. To return to the **Bandwidth Management** screen, click **Close**.

On the **Bandwidth Management** screen, click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**Priority**

**Interface**  Select the appropriate WAN interface.

**Service**  Select the Service you want.

If the Service you need is not listed in the menu, click **Service Management** to add the new service. The **Service Management** screen appears.

**Service Name**  Enter a name.

**Protocol**  Select the protocol it uses.

**Port Range**  Enter its range.

Click **Add to List**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Bandwidth Management** screen.

If you want to modify a service you have created, select it and click **Update this service**. Make changes. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Bandwidth Management** screen.

If you want to delete a service you have created, select it and click **Delete selected service**. Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them. Click **Exit** to return to the **Bandwidth Management** screen.

**Direction**  Select **Upstream** for outbound traffic, or select **Downstream** for inbound traffic.

**Priority**  Select **High**, **Middle**, or **Low**. High priority services will share 30% of the total system bandwidth. Middle priority services will share 60% of the total system bandwidth. Low priority services will share 10% of the total bandwidth. The default is **Middle**.

**Enable**  Select **Enable** to use this Priority rule.

Click **Add to List**, and configure as many rules as you would like, up to a maximum of 50. To delete a rule, select it and click **Delete selected application**.

Click **Summary** to see a summary of the Priority rules. The **Summary** screen appears.

**System Management > SNMP**

SNMP, or Simple Network Management Protocol, is a network protocol that provides network administrators with the ability to monitor the status of the Router and receive notification of any critical events as they occur on the network. The Router supports SNMP v1/v2c and all relevant Management Information Base II (MIBII) groups.
The appliance replies to SNMP Get commands for MIBII via any interface and supports a custom MIB for generating trap messages.

**SNMP Enable**  SNMP is enabled by default. To disable the SNMP agent, click this option to remove the check mark.

**System Name**  Set the hostname for the Router.

**System Contact**  Enter the name of the network administrator who can be contacted with updates about the Router.

**System Location**  Enter the network administrator’s contact information: an e-mail address, telephone number, or pager number.

**Get Community Name**  Create the name for a group or community of administrators who can view SNMP data. The default is `public`. A name of no more than 64 alphanumeric characters long must be entered.

**Set Community Name**  Create the name for a group or community of administrators who can receive SNMP traps, messages regarding the Router’s status. A name of no more than 64 alphanumeric characters long must be entered.

**Trap Community Name**  Create the password that will be sent with each trap to the SNMP manager. A name of no more than 64 alphanumeric characters long must be entered.

**Send SNMP Trap to**  Enter the IP address or domain name that should receive the traps sent by the Router.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**System Management > Diagnostic**

The Router has two built-in tools, DNS Name Lookup and Ping, which are used for troubleshooting network problems.

The Internet has a service called the Domain Name Service (DNS), which allows users to enter an easily remembered host name, such as www.linksys.com, instead of numerical TCP/IP addresses to access Internet resources. The DNS Name Lookup tool will return the numerical TCP/IP address of a host name.

The ping test bounces a packet off a machine on the Internet back to the sender. This test shows if the Router is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server or other machine at the ISP’s location. If this test is successful, try pinging devices outside the ISP. This will show if the problem lies with the ISP’s connection.

**Diagnostic**

**DNS Name Lookup/Ping**  Select which tool you want to use, DNS Name Lookup or Ping. Then proceed to the appropriate instructions.

**DNS Name Lookup**

Before using this tool, make sure the IP address of the DNS server is entered on the **Setup > Network screen**; otherwise, this tool will not work.

**Look up the name**  Enter the host name, and click **Go**. (Do not add the prefix `http://` or else you will get an error message.) The Router will then query the DNS server and display the results.

**Name**  The host name is displayed.

**Address**  The URL of the host is displayed.

**Ping**

Before using this tool make sure you know the device or host’s IP address. If you do not know it, use the Router’s DNS Name Lookup tool to find the IP address.
Chapter 4  Advanced Configuration

3010/100 16-Port VPN Router

System Management > Diagnostic > Ping

Ping host or IP address  Enter the IP address of the device being pinged, and click Go. The test will take a few seconds to complete. Then the Router will display the results.

Status  The status of the ping test is displayed.

Packets  The number of packets transmitted, number of packets received, and percentage of packets lost are displayed.

Round Trip Time  The minimum, maximum, and average round trip times are displayed.

System Management > Factory Default

Use this screen to clear all of your configuration information and restore the Router to its factory default settings. Only use this feature if you wish to discard all the settings and preferences that you have configured.

Factory Default

Return to Factory Default Setting  Click Return to Factory Default Setting if you want to restore the Router to its factory default settings. After clicking the button, a confirmation screen appears. Click OK to continue.

System Management > Firmware Upgrade

You can use this feature to upgrade the Router’s firmware to the latest version.

Firmware Upgrade

Firmware Upgrade Right Now  After you have selected the extracted file, click Firmware Upgrade Right Now.

NOTE: The Router will take approximately ten minutes to upgrade its firmware. During this process, do not power off the Router or press the Reset button.

Firmware Download

Firmware Download from Linksys Web Site  If you need to download the latest version of the Router’s firmware, click Firmware Download from Linksys Web Site. The Support page of the Linksys website appears.

Follow the on-screen instructions to access the Downloads page for the 10/100 16-Port VPN Router (model number: RV016). Then download the firmware upgrade file.

Extract the file on your computer. Then follow the Firmware Upgrade instructions.

System Management > Restart

If you need to restart the Router, Linksys recommends that you use the Restart tool on this screen. When you restart
from the Restart screen, then the Router will send out your log file before it is reset.

**Restart**

**Restart Router** Click Restart Router to restart the Router. After clicking the button, a confirmation screen appears. Click OK to continue.

**Active Firmware Version** By default, the current firmware version is selected.

**Backup Firmware Version** You can restart the Router using a previous firmware version; however, all custom settings will be reset to their factory defaults. (If you want to save your custom settings before the restart, use the Setting Backup screen.) To use the previous firmware version for the restart, select Backup Firmware Version.

**System Management > Setting Backup**

This screen allows you to make a backup file of your preferences file for the Router. To save the backup file, you need to export the configuration file.

To use the backup preferences file, you need to import the configuration file that you previously exported.

**Import Configuration File**

To import a configuration file, first specify where your backup preferences file is located. Click Browse, and then select the appropriate configuration file.

**Import** After you select the file, click Import. This process may take up to a minute. Then restart the Router so that the changes will take effect.

**Export Configuration File**

**Export** To export the Router’s current configuration file, click Export.

Click Save, and then select the location where you want to store your backup preferences file. By default, this file will be called RV016.exp, but you may rename it if you wish. This process may take up to a minute.

**Port Management > Port Setup**

Configure the connection settings for each local port, such as priority, speed, and duplex. You can also enable or disable the auto-negotiation feature for all ports.
Chapter 4
Advanced Configuration

By default, the Router allows you to simultaneously connect two broadband connections to the Router; however, you can set up as many as seven broadband connections.

From the drop-down menu, select how many WAN ports you want to use. The default is 2. (You can also change the number of WAN ports using the Setup > Network screen.) Make sure the physical network configuration matches the number of WAN port settings on this screen.

If you change the number of WAN ports, click Save Settings to save your change. A confirmation message will appear. Then click OK to save the new setting.

The Basic Per Port Config. table displays the following:

**Port ID**
The port number or name is displayed.

**Interface**
The port’s interface type: LAN, WAN, or DMZ, is displayed.

**Disable**
To disable a port, select Disable.

**Priority**
For port-based QoS, select the appropriate priority level, **High** or **Normal**.

**Speed**
Select the port speed, **10M** or **100M**.

**Duplex**
Select the duplex mode, **Half** or **Full**.

**Auto Neg.**
Select Enable if you want the Router’s ports to auto-negotiate connection speeds and duplex mode; then you will not need to set up speed and duplex settings separately.

**VLAN**
For each LAN port, a VLAN (a Virtual LAN, or network within your network) can be established. Up to 13 VLANs can be established.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

**Port Management > Port Status**

Status information is displayed for the selected port.

**Port ID**
To see the status information and settings for a specific port, select its ID number or name.

**Port Status**

**Summary**
For the selected port, the Summary table displays the following:

**Type**
The port type is displayed.

**Interface**
The interface type, LAN or WAN, is displayed.

**Link Status**
The status of the connection is displayed.

**Port Activity**
The status of the port is displayed.

**Speed Status**
The speed of the port, 10 Mbps, or 100 Mbps, is displayed.

**Duplex Status**
The duplex mode is displayed, Half or Full.

**Auto negotiation**
The status of the feature is displayed.

**VLAN**
The VLAN of the port is displayed.

**Statistics**
For the selected port, the Statistics table displays the following:

**Port Receive Packet Count**
The number of packets received is displayed.

**Port Receive Packet Byte Count**
The number of packet bytes received is displayed.

**Port Transmit Packet Count**
The number of packets transmitted is displayed.

**Port Transmit Packet Byte Count**
The number of packet bytes transmitted is displayed.
Chapter 4

Advanced Configuration

Port Packet Error Count  The number of packet errors is displayed.

To update the on-screen information, click Refresh.

Firewall > General

Enable or disable a variety of firewall, security, and web features.

Firewall > General

General

Firewall  The firewall is enabled by default. If you disable it, then the SPI, DoS, and Block WAN Request features, Access Rules, and Content Filters will also be disabled, and the Remote Management feature will be enabled.

SPI (Stateful Packet Inspection)  This option is enabled by default. The Router’s firewall uses Stateful Packet Inspection to review the information that passes through the firewall. It inspects all packets based on the established connection, prior to passing the packets for processing through a higher protocol layer.

DoS (Denial of Service)  This option is enabled by default. It protects internal networks from Internet attacks, such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing, and reassembly attacks.

Block WAN Request  This option is enabled by default. Using this feature, the Router drops both unaccepted TCP request and ICMP packets from the WAN side. Hackers will not find the Router by pinging the WAN IP address.

Remote Management  This option is disabled by default. If you want to manage the Router through a WAN connection, first change the password on the Setup > Password screen (this prevents any user from accessing the Router with the default password). Then select Enable for the Remote Management setting, and enter the port number (port 80, the default, or 8080 is usually used).

NOTE: If the Remote Management feature on the Firewall > General screen has been enabled, then users with administrative privileges can remotely access the web-based utility. Use http://<WAN IP address of the Router>, or use https://<WAN IP address of the Router> if you have enabled the HTTPS feature.

HTTPS  HTTPS is a secured HTTP session. If Remote Management is enabled, HTTPS is enabled by default.

NOTE: If you disable the HTTPS feature, then you also disable the Linksys QuickVPN service on the Router.

Multicast Pass Through  This option is disabled by default. IP multicasting occurs when a single data transmission is sent to multiple recipients at the same time. Using this feature, the Router allows IP multicast packets to be forwarded to the appropriate LAN devices. Multicast Pass Through is used for Internet games, videoconferencing, and multimedia applications.

Restrict WEB Features

Block  Select the filters you want to use.

- Java  Java is a programming language for websites. If you deny Java applets, you run the risk of losing access to Internet sites created using this programming language. To block Java applets, select Java.

- Cookies  A cookie is data stored on your PC and used by Internet sites when you interact with them. To block cookies, select Cookies.

- ActiveX  ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of losing access to Internet sites created using this programming language. To block ActiveX, select ActiveX.

- Access to HTTP Proxy Servers  Use of WAN proxy servers may compromise the Router’s security. If you block access to HTTP proxy servers, then you block access to WAN proxy servers. To block access, select Access to HTTP Proxy Servers.

Don’t block Java/ActiveX/Cookies/Proxy to Trusted Domains  To keep trusted sites unblocked, select this option.

Add  Enter the domain you want to block.
Chapter 4

Advanced Configuration

To add a domain to the list, click Add to list. To remove a domain from the list, select the entry, and click the Delete selected domain.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

Firewall > Access Rules

Access rules evaluate network traffic to decide whether or not it is allowed to pass through the Router’s firewall. Access Rules look specifically at a data transmission’s source IP address, destination IP address, and IP protocol type, and you can apply each access rule according to a different schedule.

With the use of custom rules, it is possible to disable all firewall protection or block all access to the Internet, so use extreme caution when creating or deleting access rules.

The Router has the following default rules:

- All traffic from the LAN to the WAN is allowed.
- All traffic from the WAN to the LAN is denied.
- All traffic from the LAN to the DMZ is allowed.
- All traffic from the DMZ to the LAN is denied.
- All traffic from the WAN to the DMZ is allowed.
- All traffic from the DMZ to the WAN is allowed.

Custom rules can be created to override the above default rules, but there are four additional default rules that will be always active and cannot be overridden by any custom rules.

- HTTP service from the LAN to the Router is always allowed.
- DHCP service from the LAN is always allowed.
- DNS service from the LAN is always allowed.
- Ping service from the LAN to the Router is always allowed.

Access Rules

Except for the default rules, all configured access rules are listed in the Access Rules table, and you can set the priority for each custom rule.

If the Access Rules table has multiple pages, select a different page to view from the Jump to drop-down menu. If you want more or fewer entries listed per page, select a different number from the entries per page drop-down menu.

For each access rule, the Access Rules table lists the following:

- **Priority** The priority of the access rule is displayed, 1 indicating the highest priority. To change its priority, select a different priority from the drop-down menu. (When an access rule is created, the Router automatically assigns a priority; however, you can change the priority after the rule is created.) If there is a conflict between two access rules, then the higher priority rule takes precedence. The default access rules have the lowest priority.
- **Enable** The status of the access rule is displayed. To enable or disable a rule, click the Enable check box.
- **Action** The Action, Allow or Deny, is displayed.
- **Service** The Service is displayed.
- **Source Interface** The Source Interface, LAN or WAN, is displayed.
- **Source** The specific Source is displayed.
- **Destination** The specific Destination is displayed.
- **Time** The time interval to which the access rule applies is displayed.
- **Day** The days to which the access rule applies is displayed.

Click Edit to edit an access rule, or click the Trash Can icon to delete an access rule.

Click Add New Rule to add new access rules, and the Add a New Access Rule screen appears.

Click the Restore to Default Rules to restore the default rules and delete the custom access rules.
Add a New Access Rule

Services

Wizard If you need help to configure the access rules, click Wizard, and follow the on-screen instructions. For additional information, refer to the “Wizard” section of this chapter.

Action Select Allow or Deny, depending on the purpose of the access rule.

Service Select the Service you want.

If the Service you need is not listed in the menu, click Service Management to add the new service. The Service Management screen appears.

Service Name Enter a name.

Protocol Select the protocol it uses.

Port Range Enter its range.

Click Add to List. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Add a New Access Rule screen.

If you want to modify a service you have created, select it and click Update this service. Make changes. Click Save

Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Add a New Access Rule screen.

If you want to delete a service you have created, select it and click Delete selected service. Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Exit to return to the Add a New Access Rule screen.

Log The Router can keep a log tracking this type of activity. To keep a log, select Log packets match this access rule. If you do not want a log, select Do Not Log these packets.

NOTE: If the Deny Policies option is enabled on the Log > System Log screen, then the log will not include log events from the Deny access rules on the Firewall > Access Rules screen. Log events from the Deny access rules will be logged separately from Deny Policies if the option, Log packets match this rule, is selected.

If the Allow Policies option is enabled on the Log > System Log screen, then the log will include log events from the Allow access rules on the Firewall > Access Rules screen, regardless of the option, Log packets match this rule.

Source Interface Select WAN, LAN, or Any.

Source IP Select the Source IP address(es) for the access rule. If it can be any IP address, select Any. If it is one IP address, select Single and enter the IP address. If it is a range of IP addresses, select Range, and enter the starting and ending IP addresses in the fields provided.

Destination IP Select the Destination IP address(es) for the access rule. If it can be any IP address, select Any. If it is one IP address, select Single and enter the IP address. If it is a range of IP addresses, select Range, and enter the starting and ending IP addresses in the fields provided.

Scheduling

Apply this rule Decide when you want the access rule to be enforced. To specify days of the week, select 24 Hr, and then select the appropriate days.

To specify specific hours, select from, and enter the specific hours and minutes in 24-hour format. Then select the appropriate days.

The default for any new rule is to always enforce it.

Click Save Settings to save your changes, or click Cancel Changes to undo them. Click Return to return to the Access Rules screen.
Chapter 4
Advanced Configuration

Firewall > Content Filter

Use this screen to block specific domains during the designated days and times for specific devices.

**Forbidden Domains**

**Block Forbidden Domains** To block access to the websites on the Forbidden Domains list, select this option.

**Add** Enter the domain you want to block.

To add a domain to the list, click **Add to list**. To remove a domain from the list, select the entry, and click the **Delete selected domain**.

**Website Blocking by Keywords**

**Enable Website Blocking by Keywords** To block access to websites using the keywords on the Website Blocking by Keywords list, select this option.

**Add** Enter the keyword you want to block.

To add a keyword to the list, click **Add to list**. To remove a domain from the list, select the entry, and click the **Delete selected keywords**.

**Scheduling** Decide when you want the content filters rules to be enforced. To specify specific hours, select from, and enter the specific hours and minutes in 24-hour format. Then select the appropriate days.

The default is to **always** enforce it.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**NOTE:** The content filter rules will be automatically disabled if the Trend Micro ProtectLink service is activated on the Router.

**ProtectLink**

For information about the ProtectLink tab, refer to “Appendix G: Trend Micro ProtectLink Gateway Service”.

**VPN > Summary**

This screen displays general information about the Router’s VPN tunnel settings. The Router supports up to 100 tunnels.

**Summary**

**Tunnel Used** The number of VPN tunnels being used is displayed.

**Tunnel Available** The number of available VPN tunnels is displayed.

**Detail** Click **Detail** for more information.

The WAN IP addresses will be displayed.

For each VPN tunnel, the No., Name, Status, Phase 2 Enc/Auth/Grp, Local Group, Remote Group, and Remote Gateway will be displayed.
Chapter 4
Advanced Configuration

For each group VPN, the Group Name, number of Connected Tunnels, Phase 2 Encrypt/Auth/Group, Local Group, and Remote Client will be displayed.

Click Close to exit this screen and return to the Summary screen.

Tunnel Status

Add New Tunnel Click Add New Tunnel to add a VPN tunnel. The Mode Choose screen appears.

Gateway to Gateway

To create a tunnel between two VPN devices, such as two VPN Routers, click Add Now. The Gateway to Gateway screen appears. Proceed to the “VPN > Gateway to Gateway” section for instructions. Click Return to return to the Summary screen.

Client to Gateway

To create a tunnel between the VPN Router and the client using VPN client software that supports IPSec, click Add Now. The Client to Gateway screen appears. Proceed to the “VPN > Client to Gateway” section for instructions. Click Return to return to the Summary screen.

If the VPN Summary table has multiple pages, select a different page to view from the Jump to drop-down menu. If you want more or fewer entries listed per page, select a different number from the entries per page drop-down menu.

After you have added the VPN tunnel, you will see it listed in the table.

No. It shows the number of the VPN tunnel.

Name It shows the Tunnel Name that you gave the VPN tunnel.

Status This indicates the status of the VPN tunnel.

Phase 2 Enc/Auth/Grp This shows the Phase 2 Encryption type (NULL/DES/3DES/AES-128/AES-192/AES-256), Authentication method (NULL/MD5/SHA1), and DH Group number (1/2/5) that you chose in the IPSec Setup section.

If you selected Manual for the Keying Mode in the IPSec section, then only the Encryption type and Authentication method will be displayed.

Local Group This shows the IP address and subnet mask of the Local Group.

Remote Group The IP address and subnet mask of the Remote Group are displayed here.

Remote Gateway It shows the IP address of the Remote Gateway.

Tunnel Test Click Connect to verify the status of the VPN tunnel. The test result will be updated in the Status column. If the tunnel is connected, a Disconnect button will be available so you can end the connection.

Config. Click Edit to open a new screen where you can change the tunnel’s settings. Refer to the “Gateway to Gateway” or “Client to Gateway” section for more information. Click the Trash Can icon to delete all of your tunnel settings for each individual tunnel.

Tunnel Enabled The number of enabled VPN tunnels is displayed.

Tunnel Defined The number of defined VPN tunnels is displayed.

GroupVPN Status

If you do not enable the GroupVPN setting for any of your Client to Gateway tunnels, then this section will be blank.

Group Name This shows the name you entered when you created the Client to Gateway tunnel.

Connected Tunnels This shows the number of users logged into the group VPN.

Phase2 Enc/Auth/Grp This shows the Phase 2 Encryption type (NULL/DES/3DES/AES-128/AES-192/AES-256), Authentication method (NULL/MD5/SHA1), and DH Group number (1/2/5) that you chose in the IPSec Setup section.

Local Group This shows the IP address and subnet Sec Setup

Remote Client This shows the remote clients in the group VPN.

Remote Clients Status Click Detail List to display the Group Name, IP address and Connection Time of this group VPN. Click Refresh to update the on-screen information. Click Close to exit this screen and return to the Summary screen.
**Tunnel Test** Click **Connect** to verify the status of the group VPN. The test result will be updated in the Status column. If the group VPN is connected, a Disconnect button will be available so you can end the connection.

**Config.** Click **Edit** to open a new screen where you can change the tunnel’s settings. Refer to the “Client to Gateway” section for more information. Click the **Trash Can** icon to delete all of your settings for each individual group VPN.

**VPN Clients Status**

This section identifies the VPN clients currently connected to the Router.

- **No.** It shows the number of the VPN client.
- **Username** It shows the name of the VPN client.
- **Status** This indicates the status of the VPN client connection.
- **Start Time** This shows the time when the VPN client established its VPN connection to the Router.
- **End Time** This shows the time when the VPN client ended its VPN connection to the Router.
- **Duration** This shows how long the VPN connection existed.

To disconnect any VPN client, select the VPN client in the Disconnect column, and then click **Disconnect**.

**VPN > Gateway to Gateway**

Use this screen to create a new tunnel between two VPN devices.

---

**Add a New Tunnel**

- **Tunnel No** The tunnel number is automatically generated.
- **Tunnel Name** Enter a name for this VPN tunnel, such as Los Angeles Office, Chicago Branch, or New York Division. This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
- **Interface** Select the appropriate WAN port.
- **Enable** Check this box to enable a VPN tunnel. (When you create a VPN tunnel, this check box will be disabled.)

**Local Group Setup**

- **Local Security Gateway Type**

Select the type you want to use: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**. Follow the instructions for the type you want to use.

---

**NOTE:** The Local Security Gateway Type you select should match the Remote Security Gateway Type selected on the VPN device at the other end of the tunnel.
Chapter 4

Advanced Configuration

IP Only

The default is **IP Only**. Only the device with a specific IP address will be able to access the tunnel.

**IP address** The WAN (or Internet) IP address of the Router automatically appears.

**IP + Domain Name(FQDN) Authentication**

The IP address and FQDN must match the Remote Security Gateway of the remote VPN device, and they can only be used for one tunnel connection.

**Domain Name** The Fully Qualified Domain Name (FQDN) is the host name and domain name for a specific computer on the Internet. Enter the FQDN of the Router.

**IP address** The WAN (or Internet) IP address of the Router automatically appears.

**IP + E-mail Addr.(USER FQDN) Authentication**

**E-mail address** Enter the e-mail address for authentication.

**IP address** The WAN (or Internet) IP address of the Router automatically appears.

**Dynamic IP + Domain Name(FQDN) Authentication**

The Local Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the Remote Security Gateway requests to create a tunnel with the Router, the Router will work as a responder.

**Domain Name** Enter the domain name for authentication. (Once used, you cannot use it again to create a new tunnel connection.)

**Dynamic IP + E-mail Addr.(USER FQDN) Authentication**

The Local Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the Remote Security Gateway requests to create a tunnel with the Router, the Router will work as a responder.

**E-mail address** Enter the e-mail address for authentication.

**Local Security Group Type**

Select the local LAN user(s) behind the Router that can use this VPN tunnel. Select the type you want to use: **IP**, **Subnet**, or **IP Range**. Follow the instructions for the type you want to use.

**NOTE:** The Local Security Group Type you select should match the Remote Security Group Type selected on the VPN device at the other end of the tunnel.

After you have selected the Local Security Group Type, the settings available on this screen may change, depending on which selection you have made.

**IP**

Only the computer with a specific IP address will be able to access the tunnel.

**IP address** Enter the appropriate IP address. The default IP is **192.168.1.0**.

**Subnet**

The default is **Subnet**. All computers on the local subnet will be able to access the tunnel.
Local Security Group Type > Subnet

**IP address** Enter the IP address. The default is 192.168.1.0.

**Subnet Mask** Enter the subnet mask. The default is 255.255.255.0.

**IP Range**
Specify a range of IP addresses within a subnet that will be able to access the tunnel.

Remote Security Group Type > IP Range

**IP range** Enter the range of IP addresses. The default is 192.168.1.0~254.

Remote Group Setup

Before you configure the Remote Group Setup, make sure your VPN tunnel will have two different IP subnets. For example, if the local VPN Router has an IP scheme of 192.168.1.x (x being a number from 1 to 254), then the remote VPN router should have a different IP scheme, such as 192.168.2.y (y being a number from 1 to 254). Otherwise, the IP addresses will conflict, and the VPN tunnel cannot be created.

Remote Security Gateway Type

Select the type you want to use: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, or **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**. Follow the instructions for the type you want to use.

**NOTE:** The Remote Security Gateway Type you select should match the Local Security Gateway Type selected on the VPN device at the other end of the tunnel.

**IP Only**
The default is **IP Only**. Only the device with a specific IP address will be able to access the tunnel. Select **IP address** or **IP by DNS Resolved**.

**IP address** Select this option if you know the static IP address of the remote VPN device at the other end of the tunnel, and then enter the IP address.

**IP by DNS Resolved** Select this option if you do not know the static IP address of the remote VPN device but you do know its domain name. Then enter the remote VPN device’s domain name on the Internet. The Router will retrieve the IP address of the remote VPN device via its public DNS records.

**IP + Domain Name(FQDN) Authentication**
The IP address and domain name ID must match the Local Gateway of the remote VPN device, and they can only be used for one tunnel connection.

**IP + E-mail Addr.(USER FQDN) Authentication**
The IP address and e-mail ID must match the Local Gateway of the remote VPN device, and they can only be used for one tunnel connection.
Dynamic IP + Domain Name(FQDN) Authentication

The Local Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the Remote Security Gateway requests to create a tunnel with the Router, the Router will work as a responder.

The domain name must match the Local Gateway of the remote VPN device and can only be used for one tunnel connection.

Domain Name  Enter the domain name for authentication. (Once used, you cannot use it again to create a new tunnel connection.)

Dynamic IP + E-mail Addr.(USER FQDN) Authentication

The Remote Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the Remote Security Gateway requests to create a tunnel with the Router, the Router will work as a responder.

E-mail address Enter the e-mail address for authentication.

Remote Security Group Type

Select the Remote Security Group behind the Remote Gateway that can use this VPN tunnel. Select the type you want to use: IP, Subnet, or IP Range. Follow the instructions for the type you want to use.

NOTE: The Remote Security Group Type you select should match the Local Security Group Type selected on the VPN device at the other end of the tunnel.

IP

Only the computer with a specific IP address will be able to access the tunnel.

Remote Security Gateway Type > Dynamic IP + Domain Name(FQDN) Authentication

Remote Security Gateway Type > Dynamic IP + E-mail Addr.(USER FQDN) Authentication

Remote Security Gateway Type > IP

IP address  Enter the appropriate IP address.

Subnet

The default is Subnet. All computers on the remote subnet will be able to access the tunnel.

Remote Security Gateway Type > Subnet

IP address  Enter the IP address.

Subnet Mask  Enter the subnet mask. The default is 255.255.255.0.

Remote Security Gateway Type > IP Range

IP range  Enter the range of IP addresses.

IPSec Setup

In order for any encryption to occur, the two ends of a VPN tunnel must agree on the methods of encryption, decryption, and authentication. This is done by sharing a key to the encryption code. For key management, the default mode is IKE with Preshared Key.

Keying Mode  Select IKE with Preshared Key or Manual. Both ends of a VPN tunnel must use the same mode of key management. After you have selected the mode, the settings available on this screen may change, depending on the selection you have made. Follow the instructions for the mode you want to use.

IKE with Preshared Key

IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Preshared Key to authenticate the remote IKE peer.

Phase 1 DH Group  Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol used during Phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, and Group 2 is 1,024 bits. Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.
Chapter 4
Advanced Configuration

Phase 1 Encryption Select a method of encryption: DES (56-bit), 3DES (168-bit), AES-128 (128-bit), AES-192 (192-bit), or AES-256 (256-bit). The method determines the length of the key used to encrypt or decrypt ESP packets. AES-256 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

Phase 1 Authentication Select a method of authentication, MD5 or SHA. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

Phase 1 SA Life Time Configure the length of time a VPN tunnel is active in Phase 1. The default value is 28800 seconds.

Perfect Forward Secrecy If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys.

Phase 2 DH Group If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group (the key for Phase 2 will match the key in Phase 1).

There are three groups of different prime key lengths. Group 1 is 768 bits, and Group 2 is 1,024 bits. Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You do not have to use the same DH Group that you used for Phase 1.

Phase 2 Encryption Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption: NULL, DES (56-bit), 3DES (168-bit), AES-128 (128-bit), AES-192 (192-bit), or AES-256 (256-bit). It determines the length of the key used to encrypt or decrypt ESP packets. AES-256 is recommended because it is more secure. Both ends of the VPN tunnel must use the same Phase 2 Encryption setting.

Phase 2 Authentication Select a method of authentication, NULL, MD5, or SHA. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. Both ends of the VPN tunnel must use the same Phase 2 Authentication setting.

Phase 2 SA Life Time Configure the length of time a VPN tunnel is active in Phase 2. The default is 3600 seconds.

Preshared Key This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., My_@123 or 4d795f40313233. This field allows a maximum of 30 characters and/or hexadecimal values. Both ends of the VPN tunnel must use the same Preshared Key. It is strongly recommended that you change the Preshared Key periodically to maximize VPN security.

Manual

If you select Manual, you generate the key yourself, and no key negotiation is needed. Manual key management is used in small static environments or for troubleshooting purposes.

Incoming and Outgoing SPI (Security Parameter Index) SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to select the SA, under which a packet should be processed. Hexadecimal values is acceptable, and the valid range is 100–fffffff. Each tunnel must have a unique Incoming SPI and Outgoing SPI. No two tunnels share the same SPI. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.

Encryption Select a method of encryption, DES or 3DES. This determines the length of the key used to encrypt or decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

Authentication Select a method of authentication, MD5 or SHA1. The Authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

Encryption Key This field specifies a key used to encrypt and decrypt IP traffic. Enter a key of hexadecimal values. If DES is selected, the Encryption Key is 16-bit, which requires 16 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Encryption Key will be 16-bit. If 3DES is selected, the
Encryption Key is 48-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Encryption Key will be 48-bit. Make sure both ends of the VPN tunnel use the same Encryption Key.

**Authentication Key** This field specifies a key used to authenticate IP traffic. Enter a key of hexadecimal values. If MD5 is selected, the Authentication Key is 32-bit, which requires 32 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes until it has 32 hexadecimal values. If SHA is selected, the Authentication Key is 40-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes until it has 40 hexadecimal values. Make sure both ends of the VPN tunnel use the same Authentication Key.

**Advanced**

For most users, the settings on the VPN page should suffice; however, the Router provides advanced IPSec settings for advanced users using the IKE with Preshared Key mode. Click **Advanced** to view the Advanced settings.

![Advanced Settings](image)

**Aggressive Mode** There are two types of Phase 1 exchanges, Main Mode and Aggressive Mode.

Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, leave the Aggressive Mode check box unchecked (Main Mode will be used). If network speed is preferred, select **Aggressive Mode**. If you select one of the Dynamic IP types for the Remote Security Gateway Type setting, then Main Mode will be unavailable, so Aggressive Mode will be used.

**Compress (Support IP Payload Compression Protocol (IP Comp))** IP Payload Compression is a protocol that reduces the size of IP datagrams. Select this option if you want the Router to propose compression when it initiates a connection. If the responders reject this proposal, then the Router will not implement compression. When the Router works as a responder, it will always accept compression, even if compression is not enabled.

**Keep-Alive** Keep-Alive helps maintain IPSec VPN tunnel connections. If a connection is dropped and detected, it will be re-established immediately. Select this option to use this feature.

**AH Hash Algorithm** The AH (Authentication Header) protocol describes the packet format and default standards for packet structure. With the use of AH as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. Select this option to use this feature. Then select MD5 or SHA1. MD5 produces a 128-bit digest to authenticate packet data. SHA produces a 160-bit digest to authenticate packet data. Both sides of the tunnel should use the same algorithm.

**NetBIOS Broadcast** Select this option to allow NetBIOS traffic to pass through the VPN tunnel. By default, the Router blocks this traffic.

**NAT Traversal** Select this option to use this feature. Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947.

**Dead Peer Detection (DPD)** When DPD is enabled, the Router will send periodic HELLO/ACK messages to check the status of the VPN tunnel (this feature can be used only when both peers or VPN devices of the VPN tunnel use the DPD mechanism). Once a dead peer has been detected, the Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). DPD is enabled by default, and the default interval is 10 seconds.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**VPN > Client to Gateway**

Use this screen to create a new tunnel between a VPN device and a remote computer using third-party VPN client software, such as TheGreenBow or VPN Tracker.
### Add a New Tunnel

**Tunnel/Group VPN** To create a tunnel for a single VPN client, select **Tunnel**. To create a tunnel for multiple VPN clients, select **Group VPN**. The Group VPN feature facilitates setup and is not needed to individually configure remote VPN clients.

Depending on your selection, the Local Group Setup and Remote Client Setup settings will differ. Proceed to the appropriate instructions for your selection.

**Tunnel**

- **Tunnel No** The tunnel number is automatically generated.
- **Tunnel Name** Enter a name for this VPN tunnel, such as Los Angeles Office, Chicago Branch, or New York Division.

This allows you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

**Interface** Select the appropriate WAN port.

**Enable** Check this box to enable a VPN tunnel.

### Local Group Setup

**Local Security Gateway Type**

Select the type you want to use: **IP Only**, **IP + Domain Name(FQDN) Authentication**, **IP + E-mail Addr.(USER FQDN) Authentication**, **Dynamic IP + Domain Name(FQDN) Authentication**, or **Dynamic IP + E-mail Addr.(USER FQDN) Authentication**. Follow the instructions for the type you want to use.

**NOTE:** The Local Security Gateway Type you select should match the Remote Security Gateway Type selected on the VPN device at the other end of the tunnel.

**IP Only**

The default is **IP Only**. Only the device with a specific IP address will be able to access the tunnel.

**IP address** The WAN (or Internet) IP address of the Router automatically appears.

**IP + Domain Name(FQDN) Authentication** The IP address and FQDN must match the Remote Security Gateway of the remote VPN device, and they can only be used for one tunnel connection.

**Domain Name** Enter the Fully Qualified Domain Name (FQDN), which is the host name and domain name for a specific computer on the Internet.

**IP address** The WAN (or Internet) IP address of the Router automatically appears.
Chapter 4
Advanced Configuration

IP + E-mail Addr.(USER FQDN) Authentication

E-mail address Enter the e-mail address for authentication.

IP address The WAN (or Internet) IP address of the Router automatically appears.

Dynamic IP + Domain Name(FQDN) Authentication

The Local Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the Remote Security Gateway requests to create a tunnel with the Router, the Router will work as a responder.

The domain name must match the Remote Security Gateway of the remote VPN device and can only be used for one tunnel connection.

NOTE: The Local Security Group Type you select should match the Remote Security Group Type selected on the VPN device at the other end of the tunnel.

After you have selected the Local Security Group Type, the settings available on this screen may change, depending on which selection you have made.

IP

Only the computer with a specific IP address will be able to access the tunnel.

IP address Enter the appropriate IP address. The default IP is 192.168.1.0.

Subnet

The default is Subnet. All computers on the local subnet will be able to access the tunnel.

Domain Name Enter the domain name for authentication. (Once used, you cannot use it again to create a new tunnel connection.)

Dynamic IP + E-mail Addr.(USER FQDN) Authentication

The Local Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the Remote Security Gateway requests to create a tunnel with the Router, the Router will work as a responder.

E-mail address Enter the e-mail address for authentication.

Local Security Group Type

Select the local LAN user(s) behind the Router that can use this VPN tunnel. Select the type you want to use: IP, Subnet, or IP Range. Follow the instructions for the type you want to use.

Remote Client Setup

Remote Client

Select the type you want to use: IP Only, IP + Domain Name(FQDN) Authentication, IP + E-mail Addr. (USER FQDN) Authentication, Dynamic IP + Domain Name(FQDN) Authentication, or Dynamic IP + E-mail Addr.(USER FQDN) Authentication. Follow the instructions for the type you want to use.
IP Only
The default is **IP Only**. Only the computer with a specific IP address will be able to access the tunnel. Select **IP address** or **IP by DNS Resolved**.

- **Remote Client > IP Only**

**IP address** Select this option if you know the static IP address of the remote computer at the other end of the tunnel, and then enter the IP address.

**IP by DNS Resolved** Select this option if you do not know the static IP address of the remote computer but you do know its domain name. Then enter the remote computer’s domain name on the Internet. The Router will retrieve the IP address of the remote VPN device via its public DNS records.

**IP + Domain Name(FQDN) Authentication**
The IP address and domain name ID must match the Local Gateway of the remote computer, and they can only be used for one tunnel connection.

- **Remote Client > IP + Domain Name(FQDN) Authentication**

**IP address** Select this option if you know the static IP address of the remote computer at the other end of the tunnel, and then enter the IP address.

**IP by DNS Resolved** Select this option if you do not know the static IP address of the remote computer but you do know its domain name. Then enter the remote computer’s domain name on the Internet. The Router will retrieve the IP address of the remote VPN device via its public DNS records.

**Domain Name** Enter the domain name as an ID (it cannot be a real domain name on the Internet).

**IP + E-mail Addr.(USER FQDN) Authentication**
The IP address and domain name ID must match the Local Gateway of the remote computer, and they can only be used for one tunnel connection.

- **Remote Client > IP + E-mail Addr.(USER FQDN) Authentication**

**IP address** Select this option if you know the static IP address of the remote computer at the other end of the tunnel, and then enter the IP address.

**IP by DNS Resolved** Select this option if you do not know the static IP address of the remote computer but you do know its domain name. Then enter the remote computer’s domain name on the Internet. The Router will retrieve the IP address of the remote VPN device via its public DNS records.

**Domain Name** Enter the domain name for authentication. (Once used, you cannot use it again to create a new tunnel connection.)

**Dynamic IP + E-mail Addr.(USER FQDN) Authentication**
The Remote Security Gateway will be a dynamic IP address, so you do not need to enter the IP address. When the remote computer requests to create a tunnel with the Router, the Router will work as a responder.

- **Remote Client > Dynamic IP + E-mail Addr.(USER FQDN) Authentication**

**E-mail address** Enter the e-mail address for authentication.

**Group VPN**

**Group No** The group number is automatically generated. (The Router supports up to two group VPNs.)

**Group Name** Enter a name for this group VPN, such as American Sales Group or West Coast Marketing. This allows you to identify multiple group VPNs and does not have to match the name used at the other end of the tunnel.

**Interface** Select the appropriate WAN port.

**Enable** Check this box to enable a group VPN.

**Local Group Setup**

**Local Security Group Type**
Select the local LAN user(s) behind the Router that can use this VPN tunnel. Select the type you want to use: **IP**, **Subnet**, or **IP Range**. Follow the instructions for the type you want to use.
**NOTE:** The Local Security Group Type you select should match the Remote Security Group Type selected on the remote computer at the other end of the tunnel.

After you have selected the Local Security Group Type, the settings available on this screen may change, depending on which selection you have made.

**IP**

Only the computer with a specific IP address will be able to access the tunnel.

**Remote Client Setup**

**Remote Client**

Select the type you want to use: **Domain Name (FQDN)**, **E-mail Addr. (USER FQDN)**, or **Microsoft XP/2000 VPN Client**. Follow the instructions for the type you want to use.

**Domain Name (FQDN)**

The default is **Domain Name (FQDN)**.

**Domain Name** Enter the Fully Qualified Domain Name (FQDN), which is the host name and domain name for a specific computer on the Internet. When the remote computer requests to create a tunnel with the Router, the Router will work as a responder.

**E-mail Address (User FQDN)**

**E-mail address** Enter the e-mail address of the user FQDN.

**Microsoft XP/2000 VPN Client**

Dynamic IP users, such as PPPoE or DHCP users, who use the Microsoft VPN client software, can use this option. (The Microsoft VPN client software does not support Aggressive mode and FQDN or User FQDN ID options.)

**IPSec Setup**

In order for any encryption to occur, the two ends of a VPN tunnel must agree on the methods of encryption, decryption, and authentication. This is done by sharing a key to the encryption code. For key management, the default mode is **IKE with Preshared Key**.

**Keying Mode** Select **IKE with Preshared Key** or **Manual**. Both ends of a VPN tunnel must use the same mode of key management. After you have selected the mode, the settings available on this screen may change, depending on the selection you have made. Follow the instructions for the mode you want to use. (Manual mode is available for VPN tunnels only, not group VPNs.)

**IKE with Preshared Key**

IKE is an Internet Key Exchange protocol used to negotiate key material for Security Association (SA). IKE uses the Preshared Key to authenticate the remote IKE peer.

**Phase 1 DH Group** Phase 1 is used to create the SA. DH (Diffie-Hellman) is a key exchange protocol used during Phase 1 of the authentication process to establish pre-
shared keys. There are three groups of different prime key lengths. Group 1 is 768 bits, and Group 2 is 1,024 bits. Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.

**Phase 1 Encryption** Select a method of encryption: DES (56-bit), 3DES (168-bit), AES-128 (128-bit), AES-192 (192-bit), or AES-256 (256-bit). The method determines the length of the key used to encrypt or decrypt ESP packets. AES-256 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

**Phase 1 Authentication** Select a method of authentication, MD5 or SHA. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

**Phase 1 SA Life Time** Configure the length of time a VPN tunnel is active in Phase 1. The default value is 28800 seconds.

**Perfect Forward Secrecy** If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPSec keys.

**Phase 2 DH Group** If the Perfect Forward Secrecy feature is disabled, then no new keys will be generated, so you do not need to set the Phase 2 DH Group (the key for Phase 2 will match the key in Phase 1).

There are three groups of different prime key lengths. Group 1 is 768 bits, and Group 2 is 1,024 bits. Group 5 is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5. You do not have to use the same DH Group that you used for Phase 1.

**Phase 2 Encryption** Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. Select a method of encryption: NULL, DES (56-bit), 3DES (168-bit), AES-128 (128-bit), AES-192 (192-bit), or AES-256 (256-bit). It determines the length of the key used to encrypt or decrypt ESP packets. AES-256 is recommended because it is more secure. Both ends of the VPN tunnel must use the same Phase 2 Encryption setting.

**Phase 2 Authentication** Select a method of authentication, NULL, MD5, or SHA. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure. Both ends of the VPN tunnel must use the same authentication method.

**Phase 2 SA Life Time** Configure the length of time a VPN tunnel is active in Phase 2. The default is 3600 seconds.

**Preshared Key** This specifies the pre-shared key used to authenticate the remote IKE peer. Enter a key of keyboard and hexadecimal characters, e.g., My_@123 or 4d79540313233. This field allows a maximum of 30 characters and/or hexadecimal values. Both ends of the VPN tunnel must use the same Preshared Key. It is strongly recommended that you change the Preshared Key periodically to maximize VPN security.

**Manual**

If you select Manual, you generate the key yourself, and no key negotiation is needed. Manual key management is used in small static environments or for troubleshooting purposes.

**Incoming and Outgoing SPI (Security Parameter Index)** SPI is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to select the SA, under which a packet should be processed. Hexadecimal values is acceptable, and the valid range is 100–ffffffffff. Each tunnel must have a unique Incoming SPI and Outgoing SPI. No two tunnels share the same SPI. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.

**Encryption** Select a method of encryption, DES or 3DES. This determines the length of the key used to encrypt or decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same encryption method.

**Authentication** Select a method of authentication, MD5 or SHA1. The Authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure both ends of the VPN tunnel use the same authentication method.

**Encryption Key** This field specifies a key used to encrypt and decrypt IP traffic. Enter a key of hexadecimal values.
If DES is selected, the Encryption Key is 16-bit, which requires 16 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Encryption Key will be 16-bit. If 3DES is selected, the Encryption Key is 48-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Encryption Key will be automatically completed with zeroes, so the Encryption Key will be 48-bit. Make sure both ends of the VPN tunnel use the same Encryption Key.

**Authentication Key** This field specifies a key used to authenticate IP traffic. Enter a key of hexadecimal values. If MD5 is selected, the Authentication Key is 32-bit, which requires 32 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes until it has 32 hexadecimal values. If SHA is selected, the Authentication Key is 40-bit, which requires 40 hexadecimal values. If you do not enter enough hexadecimal values, then the rest of the Authentication Key will be automatically completed with zeroes until it has 40 hexadecimal values. Make sure both ends of the VPN tunnel use the same Authentication Key.

**Advanced**

For most users, the settings on the VPN page should suffice; however, the Router provides advanced IPSec settings for advanced users using the IKE with Preshared Key mode. Click **Advanced** to view the Advanced settings.

**Aggressive Mode** There are two types of Phase 1 exchanges, Main Mode and Aggressive Mode.

Aggressive Mode requires half of the main mode messages to be exchanged in Phase 1 of the SA exchange. If network security is preferred, leave the Aggressive Mode check box unchecked (Main Mode will be used). If network speed is preferred, select **Aggressive Mode**. If you select one of the Dynamic IP types for the Remote Security Gateway Type setting, then Main Mode will be unavailable, so Aggressive Mode will be used.

**Compress (Support IP Payload Compression Protocol (IP Comp))** IP Payload Compression is a protocol that reduces the size of IP datagrams. Select this option if you want the Router to propose compression when it initiates a connection. If the responders reject this proposal, then the Router will not implement compression. When the Router works as a responder, it will always accept compression, even if compression is not enabled.

**Keep-Alive** Keep-Alive helps maintain IPSec VPN tunnel connections. If a connection is dropped and detected, it will be re-established immediately. Select this option to use this feature.

**AH Hash Algorithm** The AH (Authentication Header) protocol describes the packet format and default standards for packet structure. With the use of AH as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. Select this option to use this feature. Then select **MD5** or **SHA1**. MD5 produces a 128-bit digest to authenticate packet data. SHA produces a 160-bit digest to authenticate packet data. Both sides of the tunnel should use the same algorithm.

**NetBIOS Broadcast** Select this option to allow NetBIOS traffic to pass through the VPN tunnel. By default, the Router blocks this traffic.

**NAT Traversal** Select this option to use this feature. Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947.

**Dead Peer Detection (DPD)** (This option is available for VPN tunnels only, not group VPNs.) When DPD is enabled, the Router will send periodic HELLO/ACK messages to check the status of the VPN tunnel (this feature can be used only when both peers or VPN devices of the VPN tunnel use the DPD mechanism). Once a dead peer has been detected, the Router will disconnect the tunnel so the connection can be re-established. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent). DPD is enabled by default, and the default interval is **10** seconds.

Click **Save Settings** to save your changes, or click **Cancel Changes** to undo them.

**VPN > VPN Client Access**

The VPN Client Access screen allows you to manage access for Linksys QuickVPN clients. (The Router supports up to 50 Linksys QuickVPN clients free of charge. If the Router you have only supports up to ten clients, then upgrade its firmware. Refer to “Appendix F: Firmware Upgrade” for instructions.)
VPN Client Access

For each QuickVPN client, do the following:
1. Export a client certificate.
2. Configure a user name and password.
3. Add the QuickVPN client to the list.

VPN Client Users

User Name Enter the user name.
New Password Enter the new password.
Confirm New Password Re-enter the new password.
Change Password Allowed To allow the user to change his or her password, select Yes. Otherwise, keep the default, No.
Active To activate the new user, select Active.

To add the new user to the list, click Add to list.

After a user has been added, you can change the user’s settings. Select the user from the list, and make your changes. Then click Update this user.

To delete a user, select the user from the list, and then click Delete selected users.

Certificate Management

Manage the certificate for securing communication between the Router and QuickVPN clients.

Generate New Certificate To generate a new certificate to replace the existing certificate on the Router, click Generate. After clicking the button, a confirmation screen appears. Click OK to continue.

Export Certificate for Administrator The certificate for the administrator contains the private key and should be stored in a safe place as a backup. If you reset the Router to its factory defaults, then you can import the certificate and restore it on the Router.

To save the certificate as a file, click Export for Admin. By default, the certificate file is named RV016_<MMDD>_<HHMM>.pem, which you can rename. (MMDD stands for month and day; HHMM stands for hours and minutes.) Follow the on-screen instructions to select the location where you want to store your certificate.

Export Certificate for Client The certificate for the client must be placed in the install directory of the QuickVPN client software.

To save the certificate as a file, click Export for Client. Then follow the on-screen instructions. By default, the certificate file is named RV016_<MMDD>_<HHMM>__Client.pem, which you can rename. (MMDD stands for month and day; HHMM stands for hours and minutes.) Follow the on-screen instructions to save the file in the install directory of the QuickVPN client software.

Import Certificate To specify the location of the administrator certificate, click Browse and follow the on-screen instructions. (This is the file you previously saved using the Export Certificate for Administrator option.) After you have selected the file, click Import.

Existing Certificate The filename of the current certificate is displayed.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

When you first save these settings, a message will appear, asking if you would like the Router to automatically change the LAN IP address to prevent conflicting IP addresses. To change the LAN IP address, click Yes. If an IP conflict occurs, the QuickVPN client will not connect to the Router.

VPN > VPN Pass Through

The VPN Pass Through screen allows you to enable or disable passthrough for a variety of VPN methods.

NOTE: VPN passthrough is enabled so that VPN clients on the LAN of the Router can reach the VPN server on the Internet.
Chapter 4

Advanced Configuration

VPN Pass Through

IPSec Pass Through  Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass Through is enabled by default to allow IPSec tunnels to pass through the Router.

PPTP Pass Through  Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass Through is enabled by default.

L2TP Pass Through  Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass Through is enabled by default.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

VPN > PPTP Server

The PPTP Server screen allows you to enable up to ten PPTP VPN tunnels between the Router and PPTP VPN clients. These PPTP VPN clients must be computers running PPTP client software and Windows XP or 2000.

PPTP Server

Enable PPTP Server  Select this option to allow PPTP VPN tunnels.

IP Address Range

Range Start  Enter the starting LAN IP address of the range allotted to PPTP VPN clients. The default is 192.168.1.200.

Range End  Enter the ending LAN IP address of the range allotted to PPTP VPN clients. The default is 192.168.1.209.

NOTE: The LAN IP address range for PPTP VPN clients should be outside of the normal DHCP range of the Router.

Users Setting

The Router uses this information to identify authorized PPTP VPN clients.

User Name  Enter a name for the PPTP VPN client.

New Password  Enter a password for the PPTP VPN client.

Confirm New Password  Re-enter the password.

Click Add to List, and configure as many entries as you would like, up to a maximum of five. To delete an entry, select it and click Delete selected users.

Connection List

The PPTP VPN tunnels are displayed.

User Name  It shows the name of the PPTP VPN client.

Remote Address  This shows the WAN IP address of the PPTP VPN client.

PPTP IP Address  This shows the PPTP IP address of the PPTP VPN client. When the PPTP VPN client connects to the PPTP server, it is assigned a PPTP IP address by the PPTP server, which has a pool of pre-configured IP addresses available. (With its PPTP IP address, the PPTP VPN client acts like it belongs to the LAN of the PPTP server.)

Click Refresh to update the on-screen information. Click Save Settings to save your changes, or click Cancel Changes to undo them.

Log > System Log

Configure the Router’s log settings, so you can specify how you want its activity logs handled.
System Log

Syslog

Syslog is a standard protocol used to capture information about network activity. The Router supports this protocol and can send its activity logs to an external server.

Enable Syslog  Select this option to enable the Router’s Syslog feature.

Syslog Server  In addition to the standard event log, the Router can send a detailed log to an external Syslog server. The Router’s Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP service, and number of bytes transferred. Enter the Syslog server name or IP address. Click Save Settings to save your changes, and then restart the Router for the changes to take effect.

E-mail

You may want logs or alert messages to be e-mailed to you. If so, then configure the E-mail settings.

Enable E-Mail Alert  Select this option to enable the Router’s E-Mail Alert feature.

Mail Server  If you want any log or alert information e-mailed to you, then enter the name or numerical IP address of your SMTP server. Your ISP can provide you with this information.

Send E-mail to  Enter the e-mail address that will receive your log files. If you do not want copies of the log information e-mailed to you, then leave this field blank.

Log Queue Length  You can designate the length of the log that will be e-mailed to you. The default is 50 entries, so unless you change this setting, the Router will e-mail the log to you when there are more than 50 log entries.

Log Time Threshold  You can designate how often the log will be e-mailed to you. The default is 10 minutes, so unless you change this setting, the Router will e-mail the log to you every 10 minutes.

The Router will e-mail the log every time the Log Queue Length or Log Time Threshold is reached.

Click E-mail Log Now to immediately send the log to the address in the Send E-mail to field.

Log Setting

Alert Log

Syn Flooding  Select this option if you want Syn Flooding events to trigger an alert.

IP Spoofing  Select this option if you want IP Spoofing events to trigger an alert.

Win Nuke  Select this option if you want Win Nuke events to trigger an alert.

Ping of Death  Select this option if you want Ping of Death events to trigger an alert.

Unauthorized Login Attempt  If this option is enabled, Unauthorized Login Attempt events trigger an alert. This option is enabled by default.

Output Blocking Event  (This option is available only if the Trend Micro ProtectLink service is enabled.) Select this option if you want website blocking events to trigger an alert.
Chapter 4

Advanced Configuration

General Log

System Error Messages  If this option is enabled, system error messages are included. This option is enabled by default.

Deny Policies  Select this option if you do not want to include log events from Deny rules on the Firewall > Access Rule screen. Log events from Deny rules will be logged separately from Deny Policies if the option, log packets match this rule, is selected.

Allow Policies  Select this option if you want to include log events from Allow rules on the Firewall > Access Rule screen. Log events from Allow rules will be logged whether or not the option, log packets match this rule, is selected.

Configuration Changes  If this option is enabled, configuration changes are included. This option is enabled by default.

Authorized Login  If this option is enabled, authorized login events are included. This option is enabled by default.

View System Log

To view logs, click this option. The System Log screen appears.

Current Time

The time of the Router is displayed.

Select the log you wish to view: ALL, System Log, Access Log, Firewall Log, or VPN Log. The All log displays a log of all activities. The System Log displays a list of cold and warm starts, web login successes and failures, and packet filtering policies. The Access Log displays all logins. The Firewall Log displays all activities regarding the Router’s firewall. The VPN Log shows information about VPN tunnel activity.

Time  The time of each log event is displayed. You can sort each log by time sequence.

Event-Type  The type of log event is displayed.

Message  The message associated with each log event is displayed.

To update a log, click Refresh. To clear a log, click Clear. To exit the System Log screen and return to the Log > System Log screen, click Close.

Outgoing Log Table

To view the outgoing log information, click this option.

Incoming Log Table

To view the incoming log information, click this option.

Clear Log Now

To clear your log without e-mailing it, click this option. Only use this option if you are willing to lose your log information.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

Log > System Statistics

This screen displays statistics about all of the Router’s ports (LAN and WAN ports). For each port, the following statistics are listed: Device Name, Status, IP Address, MAC Address, Subnet Mask, Default Gateway, DNS, Network Service Detection status, number of Received Packets, number of Sent Packets, number of Total Packets, number of Received Bytes, number of Sent Bytes, number of Total Bytes, number of Error Packets Received, number of Dropped Packets Received, percentage of Upstream
Bandwidth Usage, and percentage of Downstream Bandwidth Usage.

Log > System Statistics

Click Refresh to update the statistics.

Wizard

Use this tab to access two Setup Wizards, the Basic Setup Wizard and the Access Rule Setup Wizard. Run the Basic Setup Wizard to change the number of WAN ports or set up the Router for your Internet connection(s). Run the Access Rule Setup Wizard to set up the security policy for the Router.

Basic Setup

To change the number of WAN ports, proceed to the “Change Number of WAN Ports” section. To change the Router’s Internet connection settings, proceed to the “Edit Network Settings” section.

Change Number of WAN Ports

1. Click Launch Now to run the Basic Setup Wizard.
2. To change the number of WAN ports, select Set the total number of WAN ports.
   
   Click Next.
4. If you want to save your change, click **Save Settings**. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

5. A screen appears to notify you that the settings have been saved. To proceed to the *Wizard* screen, click **OK**. To proceed to the *System > Network* screen, click **Cancel**.

**Edit Network Settings**

1. Click **Launch Now** to run the Basic Setup Wizard.

2. To set up the Router for your Internet connection(s), select **Edit Network Settings**. Click **Next**.

3. Your Internet Service Provider (ISP) may require you to use a host and domain name for your Internet connection. If your ISP requires them, complete the *Host Name* and *Domain Name* fields; otherwise leave these blank. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.
5. Depending on which connection type you have selected, the appropriate screen will appear. Follow the instructions for the appropriate connection type:

**Obtain an IP automatically**

If you want to use the ISP's DNS server, select *Use DNS Server provided by ISP (default)*. If you want to designate a specific DNS server IP address, select *Use the Following DNS Server Addresses*, and enter the DNS server IP addresses you want to use (you must enter at least one).

Click *Next* to continue, and proceed to step 6. Click *Previous* if you want to return to the previous screen. Click *Exit* if you want to exit the Setup Wizard.

**Static IP**

Complete the *Static IP*, *Subnet Mask*, and *Default Gateway* fields with the settings provided by your ISP.

Click *Next* to continue. Click *Previous* if you want to return to the previous screen. Click *Exit* if you want to exit the Setup Wizard.

On the *DNS Servers* screen, enter the DNS server IP addresses you want to use (you must enter at least one).

Click *Next* to continue, and proceed to step 6. Click *Previous* if you want to return to the previous screen. Click *Exit* if you want to exit the Setup Wizard.
**PPPoE**

Complete the *User Name* and *Password* fields with the information provided by your ISP.

Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

Select **Connect on demand** or **Keep alive**. If you select the Connect on demand option, the connection will be disconnected after a specified period of inactivity (Max Idle Time). If you have been disconnected 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. Enter the number of minutes you want to have elapsed before your Internet access disconnects. The default is 5 minutes.

If you select the Keep alive option, the Router will keep the connection alive by sending out a few data packets periodically, so your ISP thinks that the connection is still active. This option keeps your connection active indefinitely, even when it sits idle. The default Redial Period is 30 seconds. The default Keepalive Interval is 30 seconds. The default Keepalive Retry Times is 5 times.

Click **Next** to continue, and proceed to step 6. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

6. To set up additional WAN ports, repeat step 5.

7. For the DMZ port, complete the *DMZ IP* and *Subnet Mask* fields with the information provided by your ISP.

Click **Next** to continue, and proceed to step 8. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.
Chapter 4

Advanced Configuration

8. If you want to save your changes, click **Save Settings**. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

9. A screen appears to notify you that the settings have been saved. To proceed to the **Wizard** screen, click **OK**. To proceed to the **System > Network** screen, click **Cancel**.

**Access Rule Setup**

1. Click **Launch Now** to run the Access Rule Setup Wizard.

2. This screen explains the Access Rules, including the Router’s Default Rules. Click **Next** to continue. Click **Exit** if you want to exit the Setup Wizard.

3. From the drop-down menu, select **Allow** or **Deny** depending on the intent of the Access Rule. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

4. Select the service you want from the **Service** pull-down menu. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.
5. For this service, you can select whether or not you want the Router to keep a log tracking this type of activity. To keep a log, select **Log packets match this rule**. If you do not want a log, select **Not log**.

Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

6. Select the Source Interface: **LAN, WAN** (number varies depending on the number of WAN ports), **DMZ**, or **Any** from the **Interface** pull-down menu.

Select the Source IP address(es) for this Access Rule. If it can be any IP address, select **Any**. If it is one IP address, select **Single** and enter the IP address. If it is a range of IP addresses, select **Range**, and enter the range of IP addresses.

Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

7. Select the Destination IP address(es) for this Access Rule. If it can be any IP address, select **Any**. If it is one IP address, select **Single** and enter the IP address. If it is a range of IP addresses, select **Range**, and enter the range of IP addresses.

Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

8. Decide when you want this Access Rule to be enforced. Select **Always** if you want the Access Rule to be always enforced, or select **Scheduling** if you want to specify when the Access Rule should be in effect.

If you selected **Always**, click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

If you selected **Scheduling**, click **Next** to continue. A new screen appears. Decide what times and which days of the week the Access Rule should be enforced. Then enter the hours and minutes in 24-hour format,
and select the appropriate days of the week. Click **Next** to continue. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

9. If you want to save your changes, click **Save Settings**. Click **Previous** if you want to return to the previous screen. Click **Exit** if you want to exit the Setup Wizard.

10. A screen appears to notify you that the settings have been saved. If you want to add another Access Rule, click **OK**, and the first screen of the Access Rule Setup Wizard will appear. If you want to exit the Access Rule Setup Wizard, click **Cancel**, and the **Firewall > Access Rules** screen will appear.

**Support**

Access a variety of resources on the Support page of the Linksys website, www.linksys.com. You must have an active Internet connection before you can visit the Linksys website.

**Manual**

If you want the latest version of this User Guide, click **On Line Manual**. The Support page of the Linksys website appears.

Follow the on-screen instructions to access the Downloads page for the 10/100 16-Port VPN Router (model number: RV016).

After downloading the user guide to your computer, open it using Adobe Reader.

**Linksy Web Site**

Click **Linksy Web Site**, and the Support page of the Linksys website appears.

**Logout**

The Logout tab is located on the upper right-hand corner of the screen. Click this tab to exit the web-based utility. (If you exit the web-based utility, you will need to re-enter your User Name and Password to log in and then manage the Router.)
Appendix A: Troubleshooting

The firmware upgrade has failed.

A firmware upgrade takes approximately ten minutes. An error may occur if you powered off the Router, pressed the Reset button, closed the System Management > Firmware Upgrade screen, or disconnected the computer from the Router during the firmware upgrade.

If the firmware upgrade failed, repeat the firmware upgrade procedure using the System Management > Firmware Upgrade screen of the web-based utility. Refer to “Appendix F: Firmware Upgrade” for details.

If the Diag LED continues to flash, the firmware image is damaged. Use the TFTP utility to upgrade the firmware. You can download the TFTP utility at www.linksys.com.

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 System LED should be green and not flashing.
- If the System 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 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, insert the setup CD into your computer, and then follow the on-screen instructions.

WEB: If your questions are not addressed here, refer to the Linksys website, www.linksys.com.
Appendix B: Linksys QuickVPN for Windows 2000, XP, or Vista

Introduction
The 10/100 16-Port VPN Router (model number: RV016) supports IPSec VPN client software, including the Linksys QuickVPN software (also known as the Linksys VPN client).

The Router supports up to 50 Linksys QuickVPN clients free of charge. If the Router you have only supports up to ten clients, then upgrade its firmware. Refer to “Appendix F: Firmware Upgrade” for instructions.

Computer (using VPN client software) to VPN Router
You can create a VPN tunnel between a computer using VPN client software and a VPN router. The following is an example of a computer-to-VPN Router VPN. In her hotel room, a traveling businesswoman connects to her Internet Service Provider (ISP). Her notebook computer has VPN client software that is configured with her office’s VPN settings. She accesses the VPN client software and connects to the VPN Router at the central office. As VPNs use the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office’s network, as if she were physically connected.

Linksys QuickVPN Instructions
This appendix has two sections. The first section explains how to do the following for each QuickVPN client, using the Router’s web-based utility:
1. Export a client certificate.
2. Configure a user name and password.
3. Add the QuickVPN client to the list.
The second section explains how to install and use Linksys QuickVPN, which works on computers running Windows 2000, XP, or Vista. (Computers using other operating systems will have to use third-party VPN software.) For Windows Vista, QuickVPN version 1.2.5 or later is required.

Router Configuration
Export a Client Certificate from the Router
1. For local access of the Router’s web-based utility, launch your web browser, and enter the Router’s default IP address, 192.168.1.1, in the Address field. Press the Enter key.

   Address Bar

   Address: http://192.168.1.1

   Login Screen

   User name: admin
   Password: admin

   OK

   Connect to 192.168.1.1

   NOTE: If the Remote Management feature on the Firewall > General screen has been enabled, then users with administrative privileges can remotely access the web-based utility. Use http://<WAN IP address of the Router>, or use https://<WAN IP address of the Router> if you have enabled the HTTPS feature.

2. A login screen prompts you for your User name and Password. Enter admin in the User name field, and enter admin in the Password field. (You can change the Password on the Setup > Password screen.) Then click OK.

   Login Screen

   Connect to 192.168.1.1
3. In the Router’s web-based utility, click the **VPN** tab.
4. Click the **VPN Client Access** tab.
5. Click **Generate** to generate a new certificate (if needed).

6. To export a client certificate, click **Export for Client** and save the certificate as a .pem file.

7. Distribute the certificate to all QuickVPN users.

### Add VPN Client Users

For each QuickVPN client, repeat steps 1-6.

For the Change Password Allowed setting, select **Yes** to allow the user to change his or her password. Otherwise, keep the default, **No**.

4. To activate the new user, select **Active**.

5. Click **Add to list**.

6. Click **Save Settings**.

**NOTE:** If the Router’s LAN IP address is the default, 192.168.1.1, then a pop-up window will appear when you first save these settings. You will be asked if you want the Router to automatically change its LAN IP address to prevent conflicting IP addresses. To allow the Router to change its LAN IP address, click **Yes**.

If there is an IP address conflict, the QuickVPN client will not be able to connect to the Router.

### Linksys QuickVPN Client Installation and Configuration

For each QuickVPN client, do the following:

1. Install Linksys QuickVPN. (Use the appropriate installation procedure, “Install from the CD” or “Download from the Internet”)

2. Install the client certificate.

### Install from the CD-ROM

1. Insert the RV016 CD-ROM into your CD-ROM drive. Click **Start** and then click **Run**. In the field provided, enter D:\VPN_Client.exe (if “D” is the letter of your CD-ROM drive).

2. The **License Agreement** screen appears. Read the agreement. Click **Yes** to accept the terms and conditions, and then the appropriate files are copied to the computer. Clicking the **Back** or **No** button will close the window, and the software will not be installed on the computer.
3. Click Finish to complete the installation. Proceed to the section, “Install the Client Certificate”.

### Download from the Internet

1. Go to [www.linksys.com](http://www.linksys.com) and select Products.
2. Click Business.
3. Click Router/VPN Solutions.
4. Click RV016.
6. Select the version number of the Router.
7. Save the zip file to your computer, and extract the .exe file.
8. Double-click the .exe file.
9. The License Agreement screen appears. Read the agreement. Click **Yes** to accept the terms and conditions, and then the appropriate files are copied to the computer. Clicking the **Back** or **No** button will close the window, and the software will not be installed on the computer.

### Install the Client Certificate

For each QuickVPN client, save the client certificate to the directory where the QuickVPN program is installed. Example: `C:\Program Files\Linksys\QuickVPN Client\`

**NOTE:** The certificate for the client must be placed in the install directory of the QuickVPN client software.

Proceed to the section, “Use of the Linksys QuickVPN Software”.

### Use of the Linksys QuickVPN Software

For each QuickVPN client, follow the instructions in the section, “Linksys QuickVPN Connection”.

### Linksys QuickVPN Connection

1. Double-click the Linksys QuickVPN software icon on your desktop or in the system tray.
2. The QuickVPN Login screen appears. Enter the following:
   - **Profile Name**  Enter a name for your profile.
   - **User Name**   Enter the User Name assigned to you.
To terminate the VPN tunnel, click Disconnect. To change your password, click Change Password. For information, click Help.

If you clicked Change Password and have permission to change your own password, the Connect Virtual Private Connection screen appears.

- **Old Password** Enter your password.
- **New Password** Enter your new password.
- **Confirm New Password** Re-enter your new password.

Click OK to save your new password. Click Cancel to cancel your change. For information, click Help.

**NOTE:** You can change your password only if you have been granted that privilege by your system administrator.

### Version Number of Linksys QuickVPN

To display the version number of Linksys QuickVPN:

1. Right-click the QuickVPN tray icon, and select About.
2. The About screen displays the QuickVPN version number.

3. Click OK to close the About screen.
Appendix C: Gateway-to-Gateway VPN Tunnel

Overview

This appendix explains how to configure an IPSec VPN tunnel between two VPN Routers, using an example. Two computers are used to test the liveliness of the tunnel.

Before You Begin

The following is a list of equipment you need:

- Two Windows desktop computers (each computer will be connected to a VPN Router)
- Two VPN Routers that are both connected to the Internet

Any VPN Routers can be deployed; however, this example uses the 4-Port SSL/IPSec VPN Router (model number: RVL200) and the 10/100 16-Port VPN Router (model number: RV016).

Configuration when the Remote Gateway Uses a Static IP Address

This example assumes the Remote Gateway is using a static IP address. If the Remote Gateway uses a dynamic IP address, refer to “Configuration when the Remote Gateway Uses a Dynamic IP Address.”

Configuration of the RVL200

Follow these instructions for the first VPN Router, designated RVL200. The other VPN Router is designated the RV016.

1. Launch the web browser for a networked computer, designated PC 1.
2. Access the web-based utility of the RVL200. (Refer to the User Guide of the RVL200 for details.)
3. Click the IPSec VPN tab.
4. Click the Gateway to Gateway tab.
5. Enter a name in the Tunnel Name field.
6. For the VPN Tunnel setting, select Enable.
7. For the Local Security Gateway Type, select IP Only. The WAN IP address (A.A.A.A) of the RVL200 will be automatically detected.
   - For the Local Security Group Type, select Subnet. Enter the RVL200’s local network settings in the IP Address and Subnet Mask fields.
8. For the Remote Security Gateway Type, select IP Only. Enter the RV016’s WAN IP address in the IP Address field.
9. For the Remote Security Group Type, select Subnet. Enter the RV016’s local network settings in the IP Address and Subnet Mask fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

Gateway-to-Gateway IPSec VPN Tunnel - Remote Gateway Using Static IP

NOTE: Each computer must have a network adapter installed.
11. In the *Preshared Key* field, enter a string for this key, for example, 13572468.

All rights reserved. Copyright © 2008 by Avaya Inc. All rights reserved. This document and any software described in it are furnished under license and may only be used, copied, duplicated, modified, reverse engineered, or distributed pursuant to the terms of that license. System software, hardware, specifications, and other product information are subject to change without notice. Avaya Inc. makes no warranty of any kind with regard to this document or the information contained herein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Avaya Inc. shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the information contained herein.

RVL200 IPSec Setup Settings

12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings** and proceed to the next section, “Configuration of the RV016.”

### Configuration of the RV016

Follow similar instructions for the RV016.

1. Launch the web browser for a networked computer, designated PC 2.
2. Access the web-based utility of the RV016. (Refer to “Chapter 4: Advanced Configuration” for details.)
3. Click the **VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the **Tunnel Name** field.
6. Select the appropriate Interface, **WAN1** or **WAN2**.
7. Select **Enable**.
8. For the Local Security Gateway Type, select **IP Only**. The WAN IP address (B.B.B.B) of the RV016 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RV016’s local network settings in the **IP Address** and **Subnet Mask** fields.

9. For the Remote Security Gateway Type, select **IP Only**. Enter the RVL200’s WAN IP address in the **IP Address** field.
10. For the Remote Security Group Type, select **Subnet**. Enter the RVL200’s local network settings in the **IP Address** and **Subnet Mask** fields.
11. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVL200.)
12. In the **Preshared Key** field, enter a string for this key, for example, 13572468.

RV016 IPSec Setup Settings

13. If you need more detailed settings, click **Advanced**. Otherwise, click **Save Settings**.

### Configuration of PC 1 and PC 2

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If they can ping each other, then the VPN tunnel is configured correctly.
Configuration when the Remote Gateway Uses a Dynamic IP Address

This example assumes the Remote Gateway is using a dynamic IP address. If the Remote Gateway uses a static IP address, refer to “Configuration when the Remote Gateway Uses a Static IP Address.”

NOTE: Each computer must have a network adapter installed.

Configuration of the RVL200

Follow these instructions for the first VPN Router, designated RVL200. The other VPN Router is designated the RV016.

1. Launch the web browser for a networked computer, designated PC 1.

2. Access the web-based utility of the RVL200. (Refer to the User Guide of the RVL200 for details.)

3. Click the IPSec VPN tab.

4. Click the Gateway to Gateway tab.

5. Enter a name in the Tunnel Name field.

6. For the VPN Tunnel setting, select Enable.

7. For the Local Security Gateway Type, select IP Only. The WAN IP address (A.A.A.A) of the RVL200 will be automatically detected.

   For the Local Security Group Type, select Subnet. Enter the RVL200’s local network settings in the IP Address and Subnet Mask fields.

8. For the Remote Security Gateway Type, select IP Only. Then select IP by DNS Resolved. Enter the RV016’s domain name in the field provided.

9. For the Remote Security Group Type, select Subnet. Enter the RV016’s local network settings in the IP Address and Subnet Mask fields.

10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

11. In the Preshared Key field, enter a string for this key, for example, 13572468.

Configuration of the RV016

Follow similar instructions for the RV016.

1. Launch the web browser for a networked computer, designated PC 2.

2. Access the web-based utility of the RV016. (Refer to “Chapter 4: Advanced Configuration” for details.)

3. Click the VPN tab.

4. Click the Gateway to Gateway tab.

5. Enter a name in the Tunnel Name field.

6. Select the appropriate Interface, WAN1 or WAN2.
7. Select **Enable**.

8. For the Local Security Gateway Type, select **IP Only**. The WAN IP address (B.B.B.B) of the RV016 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RV016’s local network settings in the **IP Address** and **Subnet Mask** fields.

9. For the Remote Security Gateway Type, select **IP Only**. Enter the RVL200’s WAN IP address in the **IP Address** field.

10. For the Remote Security Group Type, select **Subnet**. Enter the RVL200’s local network settings in the **IP Address** and **Subnet Mask** fields.

11. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVL200.)

12. In the **Preshared Key** field, enter a string for this key, for example, 13572468.

13. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings**.

### Configuration when Both Gateways Use Dynamic IP Addresses

This example assumes both Gateways are using dynamic IP addresses. If the Remote Gateway uses a static IP address, refer to “Configuration when the Remote Gateway Uses a Static IP Address.” If only the Remote Gateway uses a dynamic IP address, refer to “Configuration when the Remote Gateway Uses a Dynamic IP Address.”

#### Configuration of the RVL200

Follow these instructions for the first VPN Router, designated RVL200. The other VPN Router is designated the RV016.

1. Launch the web browser for a networked computer, designated PC 1.

2. Access the web-based utility of the RVL200. (Refer to the User Guide of the RVL200 for details.)

3. Click the **IPSec VPN** tab.

4. Click the **Gateway to Gateway** tab.

5. Enter a name in the **Tunnel Name** field.

6. For the VPN Tunnel setting, select **Enable**.

7. For the Local Security Gateway Type, select **IP Only**. The WAN IP address (A.A.A.A) of the RVL200 will be automatically detected.

   For the Local Security Group Type, select **Subnet**. Enter the RVL200’s local network settings in the **IP Address** and **Subnet Mask** fields.

### Configuration of PC 1 and PC 2

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If they can ping each other, then the VPN tunnel is configured correctly.
7. Select Enable.

8. For the Local Security Gateway Type, select IP Only. The WAN IP address (B.B.B.B) of the RV016 will be automatically detected.

For the Local Security Group Type, select Subnet. Enter the RV016’s local network settings in the IP Address and Subnet Mask fields.

9. For the Remote Security Gateway Type, select IP Only. Then select IP by DNS Resolved. Enter the RVL200’s domain name in the field provided.

10. For the Remote Security Group Type, select Subnet. Enter the RVL200’s local network settings in the IP Address and Subnet Mask fields.

11. In the Preshared Key field, enter a string for this key, for example, 13572468.

12. If you need more detailed settings, click Advanced Settings. Otherwise, click Save Settings and proceed to the next section, “Configuration of the RV016.”

**Configuration of the RV016**

Follow similar instructions for the RV016.

1. Launch the web browser for a networked computer, designated PC 2.

2. Access the web-based utility of the RV016. (Refer to “Chapter 4: Advanced Configuration” for details.)

3. Click the VPN tab.

4. Click the Gateway to Gateway tab.

5. Enter a name in the Tunnel Name field.

6. Select the appropriate Interface, WAN1 or WAN2.

13. If you need more detailed settings, click Advanced Settings. Otherwise, click Save Settings.

**Configuration of PC 1 and PC 2**

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If they can ping each other, then the VPN tunnel is configured correctly.
Appendix D: IPSec NAT Traversal

Overview

Network Address Translation (NAT) traversal is a technique developed so that data protected by IPSec can pass through a NAT. (See NAT 1 and NAT 2 in the diagram.) Since IPSec provides integrity for the entire IP datagram, any changes to the IP addressing will invalidate the data. To resolve this issue, NAT traversal appends a new IP and UDP header to the incoming datagram, ensuring that no changes are made to the incoming datagram stream.

This chapter discusses two scenarios. In the first scenario, Router A initiates IKE negotiation, while in the second scenario, Router B initiates IKE negotiation. In the second scenario, since the IKE responder is behind a NAT device, a one-to-one NAT rule is required on the NAT device.

Before You Begin

The following is a list of equipment you need:

- Two 4-Port SSL/IPSec VPN Routers (model number: RVL200), one of which is connected to the Internet
- Two 10/100 16-Port VPN Routers (model number: RV016), one of which is connected to the Internet

Configuration of Scenario 1

In this scenario, Router A is the RVL200 Initiator, while Router B is the RVL200 Responder.

Configuration of Router A

Follow these instructions for Router A.

1. Launch the web browser for a networked computer, designated PC 1.
2. Access the web-based utility of Router A. (Refer to the User Guide of the RVL200 for details.)
3. Click the **IPSec VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the **Tunnel Name** field.
6. For the VPN Tunnel setting, select **Enable**.
7. For the Local Security Gateway Type, select **IP Only**. The WAN IP address of Router A will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter Router A's local network settings in the **IP Address** and **Subnet Mask** fields.

8. For the Remote Security Gateway Type, select **IP Only**. Enter Router B's WAN IP address in the **IP Address** field.

9. For the Remote Security Group Type, select **Subnet**. Enter Router B's local network settings in the **IP Address** and **Subnet Mask** fields.

10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

11. In the **Preshared Key** field, enter a string for this key, for example, 13572468.

12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings** and proceed to the next section, “Configuration of Router B.”

**Configuration of Router B**

Follow these instructions for Router B.

1. Launch the web browser for a networked computer, designated PC 2.

2. Access the web-based utility of Router B. (Refer to the User Guide of the RVL200 for details.)

3. Click the **IPSec VPN** tab.

4. Click the **Gateway to Gateway** tab.

5. Enter a name in the **Tunnel Name** field.

6. For the VPN Tunnel setting, select **Enable**.

7. For the Local Security Gateway Type, select **IP Only**. The WAN IP address of Router B will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter Router B's local network settings in the **IP Address and Subnet Mask** fields.

8. For the Remote Security Gateway Type, select **IP Only**. Enter the WAN IP address of NAT 2 - RV016 in the **IP Address** field.

9. For the Remote Security Group Type, select **Subnet**. Enter Router A's local network settings in the **IP Address** and **Subnet Mask** fields.

10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

11. In the **Preshared Key** field, enter a string for this key, for example, 13572468.

12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings**.
Appendix D

Configuration of Scenario 2

In this scenario, Router B is the RVL200 Initiator, while Router A is the RVL200 Responder. Router B will have the Remote Security Gateway IP address set to a public IP address that is associated with the WAN IP address of Router A, which is behind the NAT. Hence the public IP address (192.168.99.1) must be mapped to the WAN IP address (192.168.11.101, a private IP address) of Router A through the two one-to-one NAT rules:

- 192.168.99.1 => 192.168.111.11 (on NAT 2)
- 192.168.111.11 => 192.168.11.101 (on NAT 1)

NOTE: Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947.

Configuration of the One-to-One NAT Rules

The one-to-one NAT rules must be configured on NAT 2 - RV016 and NAT 1 - RV016.

One-to-One NAT Rule on NAT 2 - RV016

192.168.99.1 => 192.168.111.11

Follow these instructions for the one-to-one NAT rule on NAT 2 - RV016.

1. Launch the web browser for a networked computer.
2. Access the web-based utility of NAT 2 - RV016. (Refer to “Chapter 4: Advanced Configuration” for details.)
3. Click the Setup tab.
4. Click the One-to-One NAT tab.
5. For the One-to-One NAT setting, select Enable.
6. In the Private Range Begin field, enter 99.1.
7. In the Public Range Begin field, enter 111.11.
8. In the Range Length field, enter an appropriate value. The range length cannot exceed the number of valid IP addresses. To map a single address, enter 1.
9. Click Add to List.
10. Click Save Settings.

Refer to “Chapter 4: Advanced Configuration” for more details about one-to-one NAT rules.

One-to-One NAT Rule on NAT 1 - RV016

192.168.111.11 => 192.168.11.101

Follow these instructions for the one-to-one NAT rule on NAT 1 - RV016.

1. Launch the web browser for a networked computer.
2. Access the web-based utility of NAT 1 - RV016. (Refer to “Chapter 4: Advanced Configuration” for details.)
3. Click the Setup tab.
4. Click the **One-to-One NAT** tab.
5. For the One-to-One NAT setting, select **Enable**.
6. In the **Private Range Begin** field, enter **111.11**.
7. In the **Public Range Begin** field, enter **11.101**.
8. In the **Range Length** field, enter an appropriate value. The range length cannot exceed the number of valid IP addresses. To map a single address, enter **1**.
9. Click **Add to List**.
10. Click **Save Settings**.

Refer to “Chapter 4: Advanced Configuration” for more details about one-to-one NAT rules.

**Configuration of Router B**

Set the Remote Security Gateway to IP address: **192.168.99.1**, which is the one-to-one NAT IP address used by NAT 2 - RV016.

Follow these instructions for Router B.
1. Launch the web browser for a networked computer, designated PC 2.
2. Access the web-based utility of Router B. (Refer to the User Guide of the RVL200 for details.)
3. Click the **IPSec VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the **Tunnel Name** field.
6. For the VPN Tunnel setting, select **Enable**.
7. For the Local Security Gateway Type, select **IP Only**. The WAN IP address of Router B will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter Router B’s local network settings in the **IP Address** and **Subnet Mask** fields.
8. For the Remote Security Gateway Type, select **IP Only**. Enter 192.168.99.1 in the **IP Address** field.
9. For the Remote Security Group Type, select **Subnet**. Enter Router A’s local network settings in the **IP Address** and **Subnet Mask** fields.
10. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.
11. In the **Preshared Key** field, enter a string for this key, for example, 13572468.
12. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings** and proceed to the next section, “Configuration of Router A.”

**Configuration of Router A**

Follow these instructions for Router A.
1. Launch the web browser for a networked computer, designated PC 1.
2. Access the web-based utility of Router A. (Refer to the User Guide of the RVL200 for details.)
3. Click the **IPSec VPN** tab.
4. Click the **Gateway to Gateway** tab.
5. Enter a name in the **Tunnel Name** field.
6. For the VPN Tunnel setting, select **Enable**.
7. For the Local Security Gateway Type, select **IP Only**. The WAN IP address of Router A will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter Router A’s local network settings in the **IP Address** and **Subnet Mask** fields.
8. For the Remote Security Gateway Type, select **IP Only**. Enter Router A’s WAN IP address in the **IP Address** field.

**NOTE:** This configuration is the same as the configuration of Router A in scenario 1.
Appendix D

For the Remote Security Group Type, select **Subnet**. Enter Router B’s local network settings in the **IP Address** and **Subnet Mask** fields.

In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

In the **Preshared Key** field, enter a string for this key, for example, 13572468.

If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save Settings**.
Appendix E

Bandwidth Management

Overview

This appendix explains how to ensure Quality of Service (QoS) on Vonage Voice over Internet Protocol (VoIP) phone service. This example uses Vonage; however, similar instructions will apply to other VoIP services.

Creation of New Services

Create two new services, Vonage VoIP and Vonage 2.

2. Access the Router’s web-based utility. (Refer to “Chapter 4: Advanced Configuration” for details.)
3. Click the System Management tab.
5. On the Service Management screen, enter a name, such as Vonage VoIP, in the Service Name field.
6. From the Protocol drop-down menu, select the protocol the VoIP service uses. For example, some VoIP devices use UDP.
7. Enter its SIP port range in the Port Range fields. For example, you can set the Port Range to 5060 to 5070 to make sure that all active ports are covered.
8. Click Add to List.
9. Add a second service. Enter a name, such as Vonage 2, in the Service Name field.
10. From the Protocol drop-down menu, select UDP.
11. Enter the RTP port range in the Port Range fields. These are required for both incoming and outgoing traffic. For example, you can set the Port Range to 10000 to 25000 to make sure that all active ports are covered.
12. Click Add to List.
13. Click Apply to save your changes.
Creation of New Bandwidth Management Rules

Create four new rules: Vonage VoIP (Upstream), Vonage VoIP (Downstream), Vonage 2 (Upstream), and Vonage 2 (Downstream).

1. On the Bandwidth Management screen, select **Vonage VoIP** from the Service drop-down menu.
2. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, 0.
3. From the Direction drop-down menu, select **Upstream** for outbound traffic.
4. In the Min. Rate field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
5. In the Max. Rate field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
6. Select **Enable** to enable this rule.
7. After you have set up the rule, click **Add to list**.
8. Set up a second rule for Vonage VoIP, this time for the Downstream direction.
   Select **Vonage VoIP** from the Service drop-down menu.
9. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, 0.
10. From the Direction drop-down menu, select **Downstream** for inbound traffic.
11. In the Min. Rate field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
12. In the Max. Rate field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
13. Select **Enable** to enable this rule.
14. After you have set up the rule, click **Add to list**.
15. Set up a rule for Vonage 2. Select **Vonage 2** from the Service drop-down menu.
16. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, 0.
17. From the Direction drop-down menu, select **Upstream** for outbound traffic.
18. In the Min. Rate field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
19. In the Max. Rate field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
20. Select **Enable** to enable this rule.
21. After you have set up the rule, click **Add to list**.
22. Set up a second rule for Vonage 2 (Downstream). Select **Vonage 2** from the Service drop-down menu.
23. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, 0.
24. From the Direction drop-down menu, select **Downstream** for inbound traffic.
25. In the Min. Rate field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
26. In the Max. Rate field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
27. Select **Enable** to enable this rule.
28. After you have set up the rule, click **Add to list**.
29. Click **Save Settings**.
Appendix F: Firmware Upgrade

Overview
This appendix explains how to upgrade the firmware of the Router.

How to Access the Web-Based Utility
1. For local access of the Router’s web-based utility, launch your web browser, and enter the Router’s default IP address, 192.168.1.1, in the Address field. Press the Enter key.

   ![Address Bar](http://192.168.1.1)

   **NOTE:** If the Remote Management feature on the Firewall > General screen has been enabled, then users with administrative privileges can remotely access the web-based utility. Use http://<WAN IP address of the Router>, or use https://<WAN IP address of the Router> if you have enabled the HTTPS feature.

2. A login screen prompts you for your User name and Password. Enter admin in the User name field, and enter admin in the Password field. (You can change the Password on the Setup > Password screen.) Then click OK.

   ![Login Screen](http://admin:admin@192.168.1.1)

Upgrade the Firmware
1. In the Router’s web-based utility, click the System Management tab.
2. Click the Firmware Upgrade tab.
3. In the Firmware Download section, click Firmware Download from Linksys Web Site.

   ![System Management > Firmware Upgrade](http://download.example.com)

4. The Support page of the Linksys website appears. Follow the on-screen instructions to access the Downloads page for the 10/100 16-Port VPN Router (model number: RV016).
5. Download the firmware upgrade file.
6. Extract the file on your computer.
7. In the Firmware Upgrade section of the Firmware Upgrade screen, click the Browse button to locate the extracted file.
8. After you have selected the extracted file, click Firmware Upgrade Right Now.

   **NOTE:** The Router will take approximately ten minutes to upgrade its firmware. During this process, do not power off the Router or press the Reset button.

Alternative Firmware Upgrade Option
If the web-based upgrade method fails, use the TFTP utility. Follow these instructions:
1. Use a computer on the local network of the Router. Set the computer to a static IP address. (For example, if the Router uses 192.168.1.1, then set the computer to 192.168.1.100.)
3. Select your region, and then select your country.
4. In the Enter Model Number field, enter RV016. Then click Go.
5. In the Please select version drop-down menu, select the version number of the RV016. (For more information about how to find the version number, click the image of the RV016’s bottom panel with the sticker displayed.)
6. In the Firmware section, click TFTP Utility.
7. The utility zip file will automatically open. Extract .exe file to an appropriate location on your computer.

8. Double-click the .exe file.

9. In the **Router IP** field, enter the IP address of the Router.

10. In the **Password** field, enter the password for access to the Router.

11. Click **Next**, and then follow the on-screen instructions.
Appendix G: Trend Micro ProtectLink Gateway Service

Overview

The optional Trend Micro ProtectLink Gateway service provides security for your network. It checks e-mail messages, filters website addresses (URLs), and blocks potentially malicious websites. (To purchase a license for this service, contact your Linksys reseller.)

This appendix explains how to use this service.

How to Access the Web-Based Utility

1. For local access of the Router’s web-based utility, launch your web browser, and enter the Router’s default IP address, 192.168.1.1, in the Address field. Press the Enter key.

   ![Address Bar](http://192.168.1.1)

   **NOTE:** If the Remote Management feature on the Firewall > General screen has been enabled, then users with administrative privileges can remotely access the web-based utility. Use http://<WAN IP address of the Router>, or use https://<WAN IP address of the Router> if you have enabled the HTTPS feature.

2. A login screen prompts you for your User name and Password. Enter admin in the User name field, and enter admin in the Password field. (You can change the Password on the Setup > Password screen.) Then click OK.

   ![Login Screen](http://192.168.1.1)

How to Purchase, Register, or Activate the Service

You can purchase, register, or activate the service using the System Summary or ProtectLink screen.

System Summary

Follow the instructions for the appropriate option:

- **Go buy**
- **Register**
- **Activate**

Trend Micro ProtectLink Gateway

**NOTE:** If the Trend Micro ProtectLink Gateway options are not displayed on the System Summary screen, upgrade the Router’s firmware. Refer to “Appendix F: Firmware Upgrade” for instructions.

**Go buy** To purchase a license to use this service, click Go buy. You will be redirected to a list of Linksys resellers on the Linksys website. Then follow the on-screen instructions.

**Register** If you already have a license, click Register. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.
Appendix G

**Trend Micro ProtectLink Gateway Service**

**NOTE:** To have your e-mail checked, you will need to provide the domain name and IP address of your e-mail server. If you do not know this information, contact your ISP.

**Activate** If you have registered, click **Activate**. A wizard begins. Follow the on-screen instructions.

When the wizard is complete, the **System Summary** screen will indicate that the service has been activated.

---

**ProtectLink**

Click the **ProtectLink** tab to display this screen.

---

**NOTE:** If the ProtectLink tab is not displayed, upgrade the Router’s firmware. Refer to “Appendix F: Firmware Upgrade” for instructions.

---

Follow the instructions for the appropriate option:

- I want to buy Trend Micro ProtectLink.
- I want to register online.
- I want to activate Trend Micro ProtectLink.

**I want to buy Trend Micro ProtectLink Gateway.** To purchase a license to use this service, click this link. You will be redirected to a list of Linksys resellers on the Linksys website. Then follow the on-screen instructions.

**I have purchased ProtectLink Gateway and want to register it.** If you already have a license, click this link. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

---

**NOTE:** To have your e-mail checked, you will need to provide the domain name and IP address of your e-mail server. If you do not know this information, contact your ISP.

**I have my Activation Code (AC) and want to activate ProtectLink Gateway.** If you have registered, click this link. A wizard begins. Follow the on-screen instructions.

When the wizard is complete, the Web Protection, Email Protection, and License tabs will appear.

---

**NOTE:** If you replace the Router with a new router that supports this service, click **I have my Activation Code (AC) and want to activate ProtectLink Gateway**. Then use your current activation code to transfer your license for the ProtectLink service to the new router.

---

**How to Use the Service**

Configure the service to protect your network.
ProtectLink > Web Protection

The Web Protection features are provided by the Router. Configure the website filtering settings on this screen.

Web Protection

Enable URL Filtering  To filter website addresses (URLs), select this option.

Enable Web Reputation  To block potentially malicious websites, select this option.

URL Filtering

Reset Counter The Router counts the number of attempted visits to a restricted URL. To reset the counter to zero, click Reset Counter.

For each URL category, select the appropriate Filtering option. If you want to filter a sub-category, click + to view the sub-categories for each category. Then select the appropriate Filtering option:

Business Hours  To filter this URL category during the business hours you have specified, select this option.

Leisure Hours  To filter this URL category during non-business hours, select this option.

Instances Blocked  The number of attempted visits is displayed.

Business Hour Setting

Business Days  Select the appropriate days. The default days are Mon. through Fri.

Business Times  To specify entire days, keep the default, All day (24 hours). To specify hours, select Specify business hours. For morning hours, select Morning, and then select the appropriate From and To times. For afternoon hours, select Afternoon, and then select the appropriate From and To times.

Web Reputation

Select the appropriate security level:

High  This level blocks a higher number of potentially malicious websites but also increases the risk of false positives. (A false positive is a website that can be trusted but seems potentially malicious.)

Medium  This level blocks most potentially malicious websites and does not create too many false positives. The default is Medium and is the recommended setting.

Low  This level blocks fewer potentially malicious websites and reduces the risk of false positives.

Approved URLs

You can designate up to 20 trusted URLs that will always be accessible.

Enable Approved URL list  To set up a list of always accessible URLs, select this option.

URL(s) to approve  Enter the trusted URL(s). Separate multiple URLs with semicolons (“;”).

Add  To add the URLs, click Add.

Approved URLs list  The trusted URLs are displayed. To delete a URL, click its trash can icon.

Approved Clients

You can designate up to 20 trusted clients (local IP addresses) that will always have access to filtered URLs.

Enable Approved Client list  To set up a list of trusted clients, select this option.
IP addresses/range Enter the appropriate IP addresses or ranges. Separate multiple URLs with semicolons (“;”). For a range of IP addresses, use a hyphen (“-”). Example: 10.1.1.0-10.1.1.10.

Add To add the IP addresses or ranges, click Add.

Approved Clients list The IP addresses or range of trusted clients are displayed. To delete an IP address or range, click its trash can icon.

URL Overflow Control

Specify the behavior you want if there are more URL requests than the service can handle.

Temporarily block URL requests (This is the recommended setting) If there are too many URL requests, the overflow will be held back until they can be processed. This is the default setting.

Temporarily bypass Trend Micro URL verification for requested URLs If there are too many URL requests, the overflow will be allowed without verification.

Click Save Settings to save your changes, or click Cancel Changes to undo them.

ProtectLink > Email Protection

The Email Protection features are provided by an online service called IMHS, which stands for InterScan™ Messaging Hosted Security. It checks your e-mail messages so spam, viruses, and inappropriate content are filtered out. After you have configured the IMHS settings, your e-mail messages will be checked online before appropriate messages are forwarded to your network.

https://us.imhs.trendmicro.com/linksys To set up e-mail protection, click this link. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

ProtectLink > License

The license for the Trend Micro ProtectLink Gateway service (Email Protection and Web Protection) is valid for one year from the time the activation code for Web Protection is generated. If you do not provide the necessary information to activate Email Protection during registration, please provide that information as soon as possible because Email Protection and Web Protection will expire at the same time.

NOTE: For example, if you provide the information needed for Email Protection one month after receiving the activation code for Web Protection, then you will receive only 11 months of Email Protection.

On the License screen, license information is displayed. Use this screen to renew your license, add seats, or view license information online.

License

Update Information To refresh the license information displayed on-screen, click Update Information.

License Information

View detailed license online To view license information online, click this link.

Status The status of your license, Activated or Expired, is displayed.
**Platform** The platform type, Gateway Service, is automatically displayed.

**License expires on** The date and time your license expires are displayed.

**Renew** To renew your license, click **Renew**. Then follow the on-screen instructions.

**Add Seats** Each seat allows an e-mail account to use Email Protection. To add seats to your license, click **Add Seats**. Then follow the on-screen instructions.
## Appendix H: Specifications

### Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>RV016 10/100 16-Port VPN Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>IEEE 802.3, 802.3u</td>
</tr>
<tr>
<td>Ports</td>
<td>16 10/100 RJ-45 Ports, including 2 Internet Ports, 1 DMZ Port, 8 LAN Ports, and 5 Configurable Internet/LAN Ports</td>
</tr>
<tr>
<td>Button</td>
<td>Reset</td>
</tr>
<tr>
<td>Cabling Type</td>
<td>Category 5 Ethernet</td>
</tr>
<tr>
<td>LEDs</td>
<td>Diag, System, LAN/Act 1-13, Internet/Act 1-7, DMZ</td>
</tr>
<tr>
<td>UPnP able/cert</td>
<td>Cert</td>
</tr>
<tr>
<td>Operating System</td>
<td>Linux</td>
</tr>
</tbody>
</table>

### Performance

- **NAT Throughput**: 200 Mbps
- **IPSec Throughput**: 97 Mbps

### Security

- **Firewall**: SPI Firewall
- **DoS Prevention**: Blocks Various Denial of Service Attacks
- **Access Rules**: Up to 50 Entries
- **Port Forwarding**: Up to 30 Entries
- **Port Triggering**: Up to 30 Entries
- **URL Filtering**: Static List by Domain or Keywords (included), Dynamic Filtering through Linksys/Trend Micro ProtectLink Gateway Services (optional)

### Network

- **Multi-WANs**: Support up to 7 WAN Ports with Load Balancing, Where Certain WAN Ports can be Dedicated to Specified IP Ranges and Services
- **WAN Type**: DHCP, Static IP, PPPoE, PPTP, Telstra BigPond, Dynamic DNS
- **Protocol Binding**: Protocols can be Bound to Particular WAN Port
- **DHCP**: DHCP Server, DHCP Client
- **DNS**: DNS Proxy, Dynamic DNS (DynDNS, 3322, PeanutHull)
- **NAT**: Many-to-One, One-to-One
- **DMZ**: DMZ Port, DMZ Host

### QoS

- **Port-based QoS**: Configurable per LAN Port
- **Service based QoS**: Supports Rate Control or Priority
- **Rate Control**: Upstream/Downstream Bandwidth can be Configured per Service
- **Priority**: Each Service can be Mapped to One of the 3 Priority Levels

### VPN

- **IPSec**: 100 IPSec Tunnels for Branch Office Connectivity
- **QuickVPN**: 50 QuickVPN Users for Remote Client Access
- **PPTP**: Built-in PPTP Server Supporting 10 PPTP Clients
- **Encryption**: DES, 3DES, AES-128, AES-192, AES-256
- **Authentication**: MD5, SHA1
- **IKE**: Support Internet Key Exchange
- **IPSec NAT-T**: Supported for Gateway-to-Gateway and Client-to-Gateway Tunnels
- **Dead Peer Detection**: Support for DPD
- **VPN Passthrough**: PPTP, L2TP, IPSec

### Management

- **Web-Based**: HTTPS
- **SNMP**: Supports SNMP v1 and v2c
- **Log**: Syslog, Email Alert, VPN Tunnels Status Monitor

### Environmental

- **Dimensions**: 11.00" x 1.75" x 9.50" (279.4 x 44.45 x 241.3 mm)
- **Unit Weight**: 3.25 lb (1.475 kg)
- **Power**: AC 100~240V, 50-60 Hz
- **Certifications**: FCC Class B, CE Class B
- **Operating Temp.**: 0 to 40°C (32 to 104°F)
- **Storage Temp.**: 0 to 70°C (32 to 158°F)
- **Operating Humidity**: 10 to 85% Noncondensing
- **Storage Humidity**: 5 to 90% Noncondensing

Specifications are subject to change without notice.
Appendix I: Warranty Information

Linksys warrants this Linksys hardware 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 for this product at www.linksys.com/warranty. The internet URL address and the web pages referred to herein may be updated by Linksys from time to time; the version in effect at the date of purchase shall apply.

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys’ entire liability under this limited warranty will be for Linksys, 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 Linksys product, or (c) refund the purchase price of the product less any rebates. 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 Linksys.

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 Linksys, (c) the product damage was caused by use with non-Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (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 Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS 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, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. 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 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. 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.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS 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 (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS’ 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. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to www.linksys.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 the Value Added Reseller (VAR) from whom you purchased the product or Contact Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.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 to Linksys 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 to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys’ then-current rates.

Technical Support

This limited warranty is neither a service nor a support contract. Information about Linksys’ current technical support offerings and policies (including any fees for support services) can be found at: www.linksys.com/support.

This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you. Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.
Appendix J: Software License Agreement

Software in Linksys Products

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pte Ltd. or Cisco-Linksys K.K. (“Linksys”) contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys 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 Linksys at www.linksys.com/gpl or as provided for in Schedules 2, 3, and 4 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from www.linksys.com/gpl. For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: www.linksys.com/gpl or Schedules 2, 3, or 4 below as applicable.

Software Licenses

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: www.linksys.com. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

Schedule 1

Links Systems Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. (“LINKSYS”) LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software (“You”) a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

“Software” includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, excluding technology from the open source community, and (b) any upgrades, updates, bug fixes or modified versions (“Upgrades”) or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.
Appendix J

Collection and Processing of Information. You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that your Linksys product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/or its affiliates’ collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

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 Linksys product and/or the Software to serious security threats and/or some features within your Linksys 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 or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered 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.

Open Source Software. The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at http://www.linksys.com/gpl. If you would like a copy of the GPL or other open source code in this Software on a CD, Linksys will mail to you a CD with such code for $9.99 plus the cost of shipping, upon request.

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 Linksys if you fail to comply with any provision of this Agreement.

Limited Warranty. The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

Disclaimer of Liabilities. IN NO EVENT WILL LINKSYS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

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.

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. 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.

END OF SCHEDULE 1

Schedule 2

If this Linksys product contains open source software licensed under Version 2 of the “GNU General Public License” then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at http://www.gnu.org/copyleft/gpl.html.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991
Appendix J

Software License Agreement

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 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.

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.

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.
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.

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.

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.

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

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.

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

Schedule 3

If this Linksys 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 3 apply:

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.
will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at http://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 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 (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 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 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.
Appendix J

Software License Agreement

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 3

Schedule 4

If this Linksys 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 Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 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, Ihash, 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 4
Appendix K: Regulatory Information

FCC Statement

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

Safety Notices

- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- 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.

Battery Recycling Statement

This product may contain a battery. Recycle or dispose of batteries in accordance with the battery manufacturer’s instructions and local/national disposal and recycling regulations.

Industry Canada Statement

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

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.

Avis d’Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Le fonctionnement est soumis aux conditions suivantes :
1. Ce périphérique ne doit pas causer d’interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d’entrainer un fonctionnement indésirable.

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

---

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.

Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union


Ceština (Czech) - Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk (Danish) - Miljøinformation for kunder i EU


Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/EC изисква уредите, носещи този символ върху изделиято и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от смелосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще помогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за смелосъбиране или магазина, от който сте закупили уреда.
Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidus asuveatele klientidele


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 Ξ 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 Ξ 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.

Italiano (Italian) - Informazioni relative all’ambiente per i clienti residenti nell’Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo Ξ sul prodotto e/o sull’imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche e elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l’ambiente e per la salute dell’essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda (Latvian) - Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EC ir prasība, ka aprīkojumu, kam pievienota zīme Ξ uz paša izstrādājuma vai uz tā iesainojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē, ka šī ierīce ir jāizmet atkritumos, lai tā nenonāktu kopā ar citiem elektriskajiem un elektroniskajiem ierīcēm. Šī zīme indikē, ka šī ierīce ir jāizmet atkritumos, lai tā nenonāktu kopā ar citiem elektriskajiem un elektroniskajiem ierīcēm, izmantojot ipašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un savienības jurisdikcijas pārstāvji. Jāņem vērā, ka šī ierīce ir jāizmet atkritumos, lai tā nenonāktu kopā ar citiem elektriskajiem un elektroniskajiem ierīcēm, izmantojot ipašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un savienības jurisdikcijas pārstāvji. Jāņem vērā, ka šī ierīce ir jāizmet atkritumos, lai tā nenonāktu kopā ar citiem elektriskajiem un elektroniskajiem ierīcēm, izmantojot ipašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un savienības jurisdikcijas pārstāvji. Jāņem vērā, ka šī ierīce ir jāizmet atkritumos, lai tā nenonāktu kopā ar citiem elektriskajiem un elektroniskajiem ierīcēm, izmantojot ipašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un savienības jurisdikcijas pārstāvji. Jāņem vērā, ka šī ierīce ir jāizmet atkritumos, lai tā nenonāktu kopā ar citiem elektriskajiem un elektroniskajiem ierīcēm, izmantojot ipašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un savienības jurisdikcijas pārstāvji.
Regulatory Information

Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool niet op het product of de verpakking mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze apparatuur. Apparatuur bevat elektrische en elektronische apparatuur die via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen gehandhaasd moet worden. Voor meer informatie raadpleegt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektwa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem nie był wyrzucony razem ze zwykłymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbawianie się sprzętu we właściwy sposób i jego recykling pomaga zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.
Regulatory Information

Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento elétrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudam a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Română (Romanian) - Informaţii de mediu pentru clienţii din Uniunea Europeană


Slovenčina (Slovak) - Okoljske informacije za stranke v Evropski uniji

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nemôže byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácnosti. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špeciálnych zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť pripadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obrátte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen


WEB: For additional information, please visit www.linksys.com
# Appendix L: Contact Information

<table>
<thead>
<tr>
<th>Linksys Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
</tr>
<tr>
<td>Support Site</td>
</tr>
<tr>
<td>FTP Site</td>
</tr>
<tr>
<td>Advice Line</td>
</tr>
<tr>
<td>Support</td>
</tr>
<tr>
<td>RMA (Return Merchandise Authorization)</td>
</tr>
</tbody>
</table>

**NOTE:** Details on warranty and RMA issues can be found in the Warranty section of this Guide.