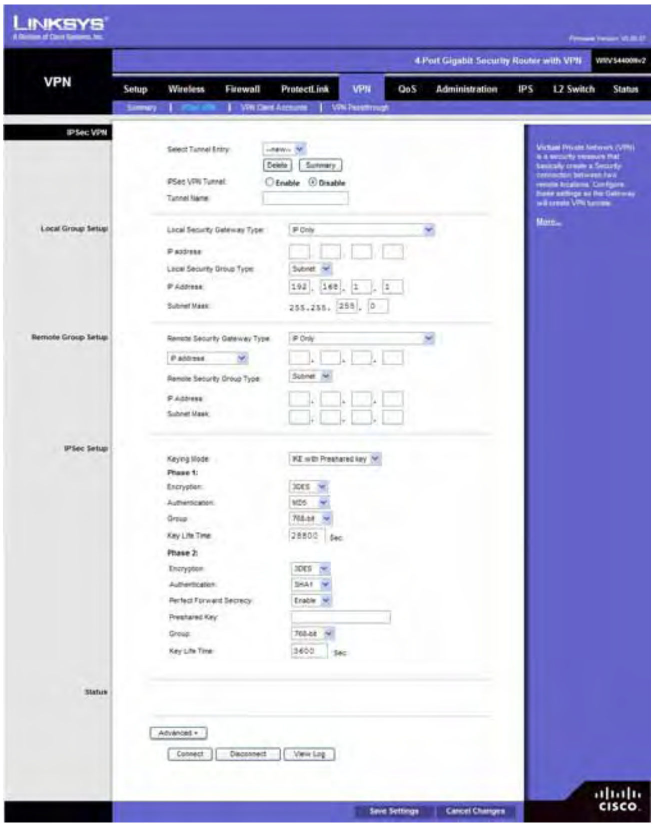
IPsec VPN

Use this screen to create VPN tunnels between the Router to the remote Router. All Linksys Routers with IPsec VPN support can be used as a remote Router (e.g. RVS4000, WRV54G, RV042). The Router supports VPN tunnels using IPsec (IP Security) technologies. You can create, delete, or modify a VPN tunnel on this page.



Select Tunnel Entry: --new--
IPSec VPN Tunnel: ○ Enable ● Disable
Tunnel Name:

Local Security Gateway Type: IP Only
IP address: . . .
Local Security Group Type: Subnet
IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255. 255 . 0

Remote Security Gateway Type: IP Only
IP address: . . .
Remote Security Group Type: Subnet
IP Address: . . .
Subnet Mask: . . .

Keying Mode: IKE with Preshared key
Phase 1:
Encryption: 3DES
Authentication: MD5
Group: 768-bit
Key Life Time: 28800 Sec
Phase 2:
Encryption: 3DES
Authentication: SHA1
Perfect Forward Secrecy: Enable
Preshared Key:
Group: 768-bit
Key Life Time: 3600 Sec

Virtual Private Network (VPN) is a security measure that basically create a Security connection between two remote locations. Configure these settings as the Gateway will create VPN tunnels.
More...

Select Tunnel Entry. Select a tunnel to configure or create a new tunnel.
Delete Button. Click this button to delete the selected tunnel.
Summary Button. Clicking this button shows the settings of all existing tunnels.
IPsec VPN Tunnel. Select **Enable** to enable this tunnel.
Tunnel Name. Enter a name for this tunnel, such as “Anaheim Office”.

Local Security Group

Local Security Gateway Type This has two settings, IP Only and IP + Domain Name (FQDN) Authentication.

- **IP Only** If this is selected, the RVS4000’s WAN IP address automatically appears in the IP Address field.
- **IP + Domain Name (FQDN) Authentication** This is the same as IP Only, but includes a domain name for greater security. Enter an arbitrary domain name in the Domain Name field. The Router’s WAN IP address automatically appears in the IP Address field.

Local Security Group Type Select the local LAN user(s) behind the router that can use this VPN tunnel. This may be a single IP address or Sub-network. Notice that the Local Security Group Type must match the other router’s Remote Security Group Type.

IP Address Enter the IP address on the local network.
Subnet Mask If the Local Security Group Type is set to Subnet, enter the mask to determine the IP addresses on the local network.

Remote Group Setup

Remote Security Gateway Type Select either **IP Only** or **IP + Domain Name (FQDN)** Authentication. The setting should match the Local Security Gateway Type for the VPN device at the other end of the tunnel.

- **IP Only** Select this to specify the remote device that will have access to the tunnel. Then either select IP Address from the drop-down menu and enter the remote gateway's WAN IP address in the IP Address field, or select IP by DNS Resolved from the dropdown menu and enter the remote gateway's domain name in the Domain Name field.
- **IP + Domain Name (FQDN) Authentication** This is the same as IP Only but includes a domain name for greater security. Enter an arbitrary domain name in the Domain Name field. Then select either IP Address or IP by DNS Resolved from the drop-down menu, and fill in the IP Address field or Domain Name field.

Remote Security Group Type Select the remote LAN user(s) behind the remote gateway who can use this VPN tunnel. This may be a single IP address or a Sub-network. Note that the Remote Security Group Type must match the other router's Local Security Group Type.
IP Address Enter the IP address on the remote network.
Subnet Mask If the Remote Security Group Type is set to Subnet, enter the mask to determine the IP addresses on the remote network.

IPSec Setup

Keying Mode. The Router supports both automatic and manual key management. When choosing automatic key management, IKE (Internet Key Exchange) protocols are used to negotiate key material for SA (Security Association). If manual key management is selected, no key negotiation is needed. Basically, manual key management is used in small static environments or for troubleshooting purpose. Notice that both sides must use the same Key Management method (both Auto or both Manual). For Manual key management, all the configurations need to match on both sides.

Phase 1

Encryption. The Encryption method determines the complexity to encrypt/decrypt ESP packets. Only 3DES is supported. Notice that both sides must use the same Encryption method.

Authentication. Authentication determines a method to authenticate the ESP packets to make sure they come from a trusted source. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.

- MD5: A one way hashing algorithm that produces a 128-bit digest.
- SHA1: A one way hashing algorithm that produces a 160-bit digest.

Group. The Diffie-Hellman (DH) group to be used for key exchange. Select the 768-bit (Group 1), 1024-bit (Group 2), or 1536-bit (Group 5) algorithm. Group 5 provides the most security, Group 1 the least.

Key Life Time. This field specifies the lifetime of the IKE generated key. If the time expires, a new key will be renegotiated automatically. The Key Lifetime may range from 1081 to 86400 seconds. The default lifetime is 28800 seconds.

Phase 2

Encryption. The Encryption method determines the complexity to encrypt/decrypt ESP packets. Only 3DES is supported. Notice that both sides must use the same Encryption method.

Authentication Algorithm. Authentication determines a method to authenticate the ESP packets to make sure they come from a trusted source. Either MD5 or SHA1 may be selected. Notice that both sides (VPN endpoints) must use the same Authentication method.

- MD5: A one way hashing algorithm that produces a 128-bit digest.
- SHA1: A one way hashing algorithm that produces a 160-bit digest.

Perfect Forward Secrecy If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. Note that both sides must have this selected.

Pre-Shared Key. IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both characters and hexadecimal values are acceptable in this field. e.g. “My_@123” or “0x4d795f40313233” Note that both sides must use the same Pre-shared Key.

Group. The Diffie-Hellman (DH) group to be used for key exchange. Select the 768-bit (Group 1), 1024-bit (Group 2), or 1536-bit (Group 5) algorithm. Group 5 provides the most security, Group 1 the least.

Key Life Time. This field specifies the lifetime of the IKE generated key. If the time expires, a new key will be renegotiated automatically. The Key Lifetime may range from 1081 to 86400 seconds. The default lifetime is 3600 seconds.

Status

Status. This field shows the connection status for the selected tunnel. The state is either connected or disconnected.

Connect button. Use this to establish a connection for the current VPN tunnel. If you have made any changes, click Save Settings to first apply your changes.

Disconnect button. Use this to break a connection for the current VPN tunnel.

View Log button. Click this to view the VPN log, which shows details of each tunnel established. You can change the Log type to show only VPN tunnel related events.

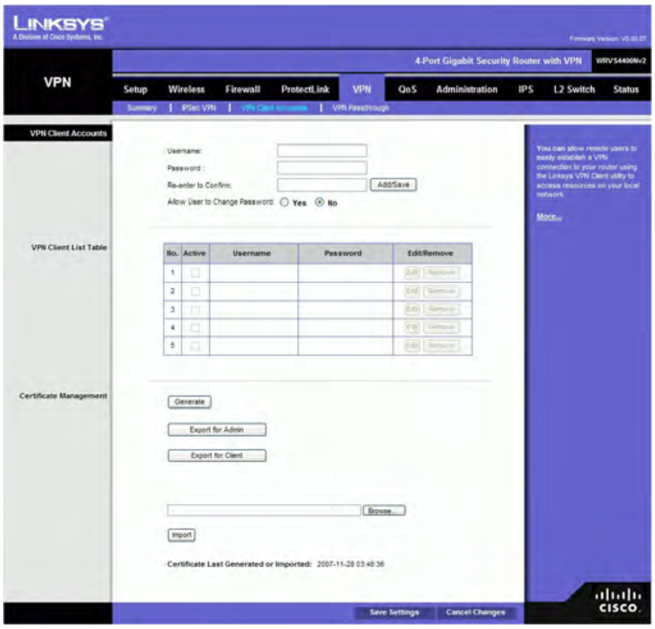
Advanced Click this button to display the following additional settings.

- **Aggressive Mode** This is used to specify the type of Phase 1 exchange, Main mode or Aggressive mode. Check the box to select Aggressive Mode or leave the box unchecked (default) to select Main 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, select Main mode.
- **NetBios Broadcasts** Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, the WRVS4000Nv2 blocks these broadcasts.

Click **Save Settings** to save the settings you have entered. Click **Cancel Changes** to cancel any changes you have entered.

VPN Client Accounts

Use this page to administer your VPN Client users. Enter the information at the top of the screen and the users you've entered will appear in the list at the bottom, showing their status. This will work with the Linksys QuickVPN client only. (The Router supports up to five Linksys QuickVPN Clients by default. Additional QuickVPN Client licenses can be purchased separately. See www.linksys.com for more information)



Username:

Password :

Re-enter to Confirm:

Allow User to Change Password: ○ Yes ● No

No.	Active	Username	Password	Edit/Remove
1	□			Edit Remove
2	□			Edit Remove
3	□			Edit Remove
4	□			Edit Remove
5	□			Edit Remove

Certificate Last Generated or Imported: 2007-11-28 03:48:36

You can allow remote users to easily establish a VPN connection to your router using the Linksys VPN Client utility to access resources on your local network.

Username. Enter the username using any combination of keyboard characters.
Password. Enter the password you would like to assign to this user.
Re-enter to Confirm. Retype the password to ensure that it has been entered correctly.
Allow User to Change Password. This option determines whether the user is allowed to change their password.

VPN Client List Table

No. Displays the user number.
Active. When checked, the designated user can connect, otherwise the VPN client account is disabled.
Username. Displays the username.
Edit button. This button is used to modify the username, password, or toggle between whether the user is
allowed to change their password.
Remove button. This button is used to delete a user account.

Certificate Management

This section allows you to manage the certificate used for securing the communication between the router and QuickVPN clients.
Generate Click this button to generate a new certificate to replace the existing certificate on the router.
Export for Admin Click this button to export the certificate for administrator. A dialog

will ask you to specify where you want to store your certificate. The default file name is “WRVS4000Nv2_Admin.pem” but you can use another name. The certificate for administrator contains the private key and needs to be stored in a safe place as a backup. If the router’s configuration is reset to the factory default, this certificate can be imported and restored on the router.

Export for Client Click this button to export the certificate for client. A dialog will ask you where you want to store your certificate. The default file name is “WRVS4000Nv2_Client.pem” but you can use another name. For QuickVPN users to securely connect to the router, this certificate needs to be placed in the install directory of the QuickVPN client.

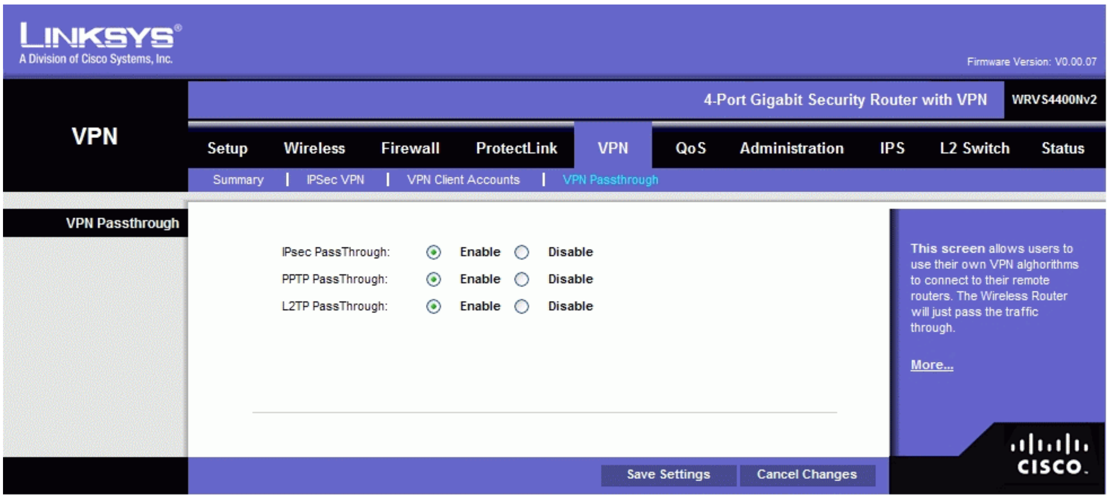
Import Click this button to import a certificate previously saved to a file using Export for Admin or Export for Client. Enter the file name in the field or click Browse to locate the file on your computer, then click Import.

Certificate Last Generated or Imported This displays the date and time when a certificate was last generated or imported.

Click **Save Setting**s to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

VPN Passthrough

This screen allows users to use their own VPN algorithms to connect to their remote Routers. The Wireless Router will just pass the traffic through.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: V0.00.07
4-Port Gigabit Security Router with VPN
WRVS4400Nv2
VPN
Setup
Wireless
Firewall
ProtectLink
VPN
QoS
Administration
IPS
L2 Switch
Status
Summary | IPSec VPN | VPN Client Accounts | VPN Passthrough
VPN Passthrough
More...
Save Settings
Cancel Changes
cisco

IPsec PassThrough: ● Enable ○ Disable

PPTP PassThrough: ● Enable ○ Disable

L2TP PassThrough: ● Enable ○ Disable

This screen allows users to use their own VPN alghorithms to connect to their remote routers. The Wireless Router will just pass the traffic through.

IPsec Passthrough. Internet Protocol Security (IPsec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPsec Passthrough is enabled by default to allow IPsec tunnels to pass through the Router. To disable IPsec Passthrough, select **Disable**.

PPTP Passthrough. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Passthrough is enabled by default. To disable PPTP Passthrough, select **Disable**.

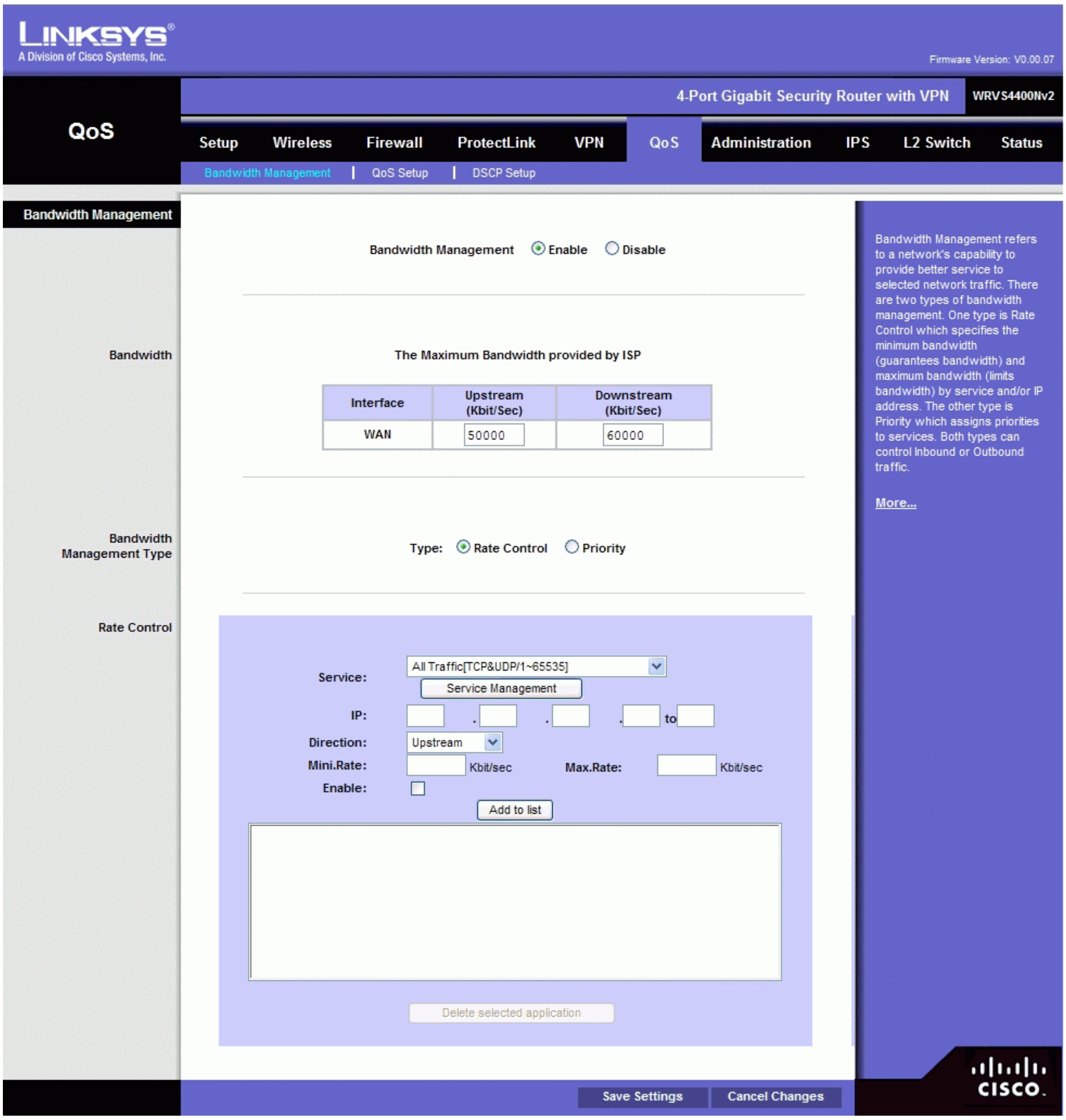
L2TP Passthrough. Layer 2 Tunneling Protocol is the similar to PPP but allows Layer 2 and the PPP session to terminate at different servers or locations. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select **Disable**.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

QoS Tab

QoS (Quality of Service) allows you to perform Bandwidth Management, by either Rate Control or Priority. You can also configure QoS Trust Mode and the DSCP settings.

Bandwidth Management



Bandwidth Management: ● Enable ○ Disable

Bandwidth

The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/Sec)	Downstream (Kbit/Sec)
WAN	50000	60000

Bandwidth Management Type

Type: ● Rate Control ○ Priority

Rate Control

Service: All Traffic[TCP&UDP/1~65535]

IP: . . . to

Direction: Upstream

Mini.Rate: Kbit/sec Max.Rate: Kbit/sec

Enable: □

Bandwidth Management refers to a network's capability to provide better service to selected network traffic. There are two types of bandwidth management. One type is Rate Control which specifies the minimum bandwidth (guarantees bandwidth) and maximum bandwidth (limits bandwidth) by service and/or IP address. The other type is Priority which assigns priorities to services. Both types can control Inbound or Outbound traffic.

More...

Bandwidth

This section lets you specify the maximum bandwidth provided by the ISP on the WAN interface, for both the upstream and downstream directions.

Bandwidth Management Type

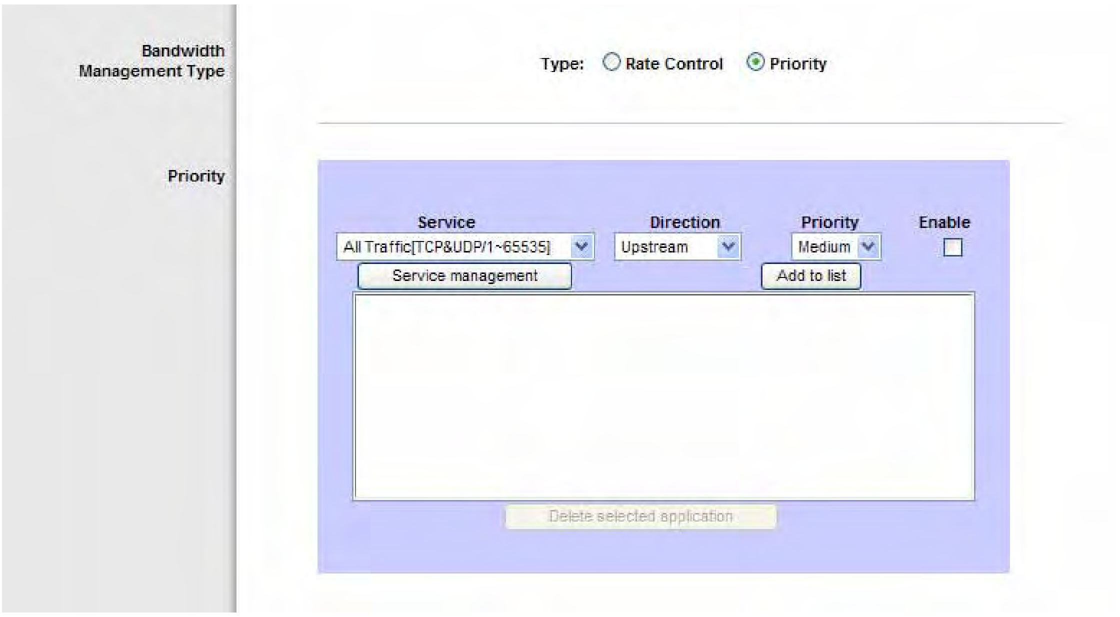
Type The desired type of bandwidth management, either **Rate Control** (default) or

Priority. Depending on your selection, the lower portion of the screen displays either the Rate Control section or the Priority section.

Rate Control

Service Select the service from the drop-down menu. If it does not contain the service you need, click Service Management to add the service.
IP Enter the IP address or IP range you need to control. The default is zero which includes all internal IP addresses.
Direction Select Upstream for outbound traffic or Downstream for inbound traffic.
Mini. Rate Enter the minimum rate for the guaranteed bandwidth.
Max. Rate Enter the maximum rate for the guaranteed bandwidth.
Enable Check this box to enable this Rate Control Rule.
Add to list After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.
Delete selected application Click this button to delete a rule from the list.

Priority



Bandwidth Management Type — Type: ○ Rate Control ● Priority

Priority

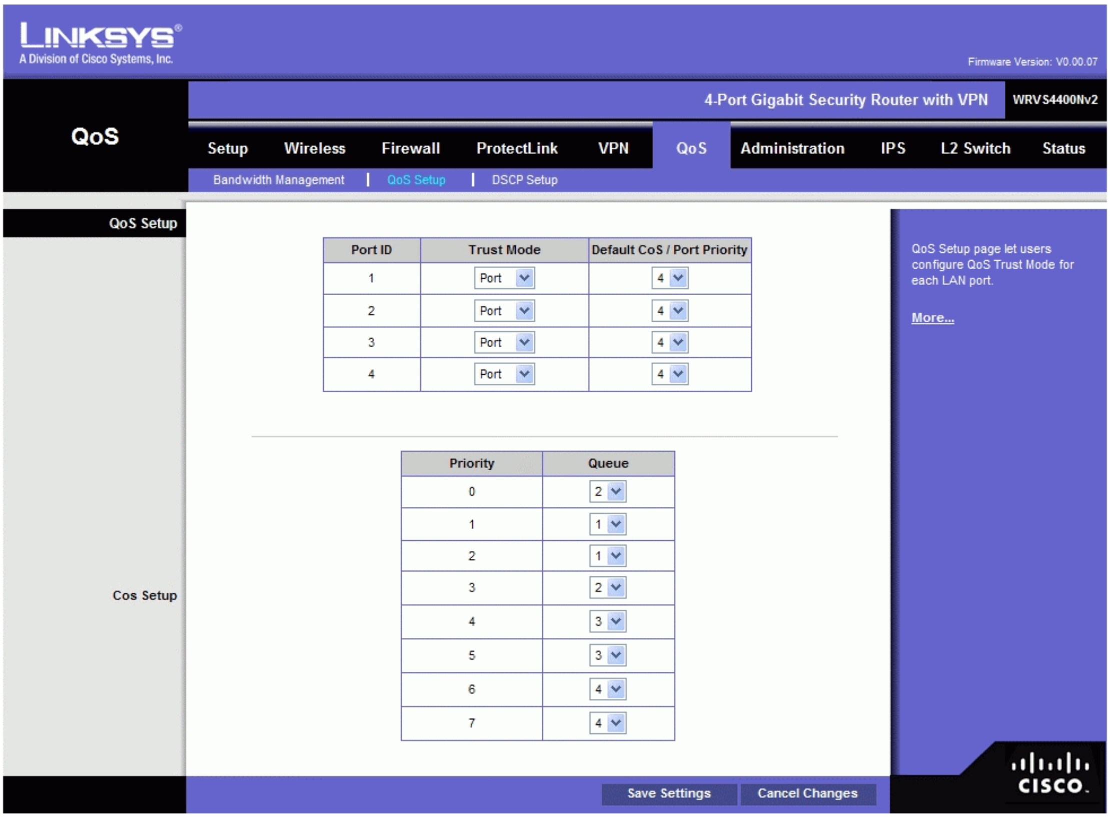
Service	Direction	Priority	Enable
All Traffic[TCP&UDP/1~65535]	Upstream	Medium	□

Service Select the service from the drop-down menu. If it does not contain the service you need, click **Service Management** to add the service.
Direction Select **Upstream** for outbound traffic or **Downstream** for inbound traffic from the drop-down menu.
Priority Select **High**, **Medium**, **Norma**l, or **Low** priority for the service. The default is **Medium**.
Enable Check this box to enable this Priority Rule.
Add to list After a rule is set up, click this button to add it to the list. The list can contain a maximum of 15 entries.
Delete selected application Click this button to delete a rule from the list.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

QoS Setup

The QoS Setup screen allows users to configure QoS Trust Mode for each LAN port.



QoS Setup page let users configure QoS Trust Mode for each LAN port.

Port ID	Trust Mode	Default CoS / Port Priority
1	Port	4
2	Port	4
3	Port	4
4	Port	4

Priority	Queue
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

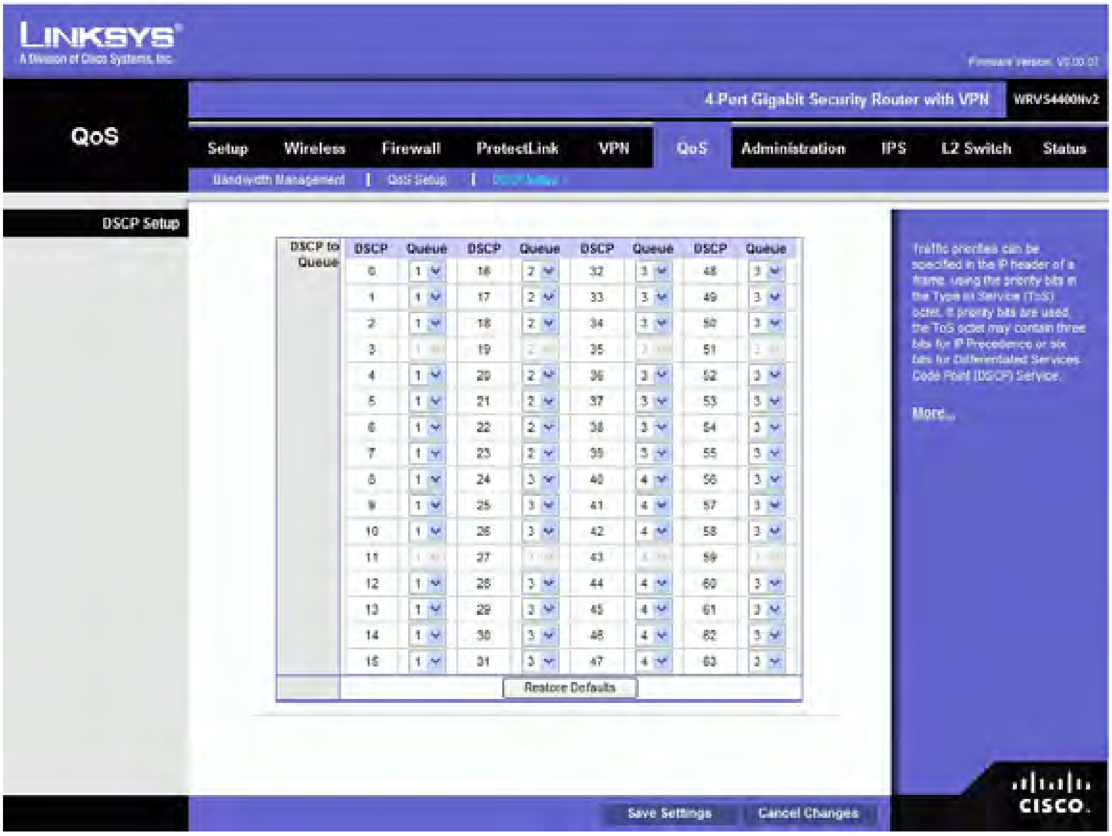
Port ID The number of the LAN port.
Trust Mode Select either **Port**, **CoS**, or **DSCP**. The default is **Port**.
Default CoS/Port Priority If Trust Mode is set to **Port**, select the port priority from **1** to **4** from the drop-down menu. If Trust Mode is set to **CoS**, select the default CoS priority from **0** to **7** from the drop-down menu.

CoS Setup

Priority The CoS priority from 0 to 7.
Queue Select the traffic forwarding queue, 1 to 4, to which the CoS priority is mapped.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

DSCP Setup



DSCP to Queue

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	1	16	2	32	3	48	3
1	1	17	2	33	3	49	3
2	1	18	2	34	3	50	3
3	1	19	2	35	3	51	3
4	1	20	2	36	3	52	3
5	1	21	2	37	3	53	3
6	1	22	2	38	3	54	3
7	1	23	2	39	3	55	3
8	1	24	3	40	4	56	3
9	1	25	3	41	4	57	3
10	1	26	3	42	4	58	3
11	1	27	3	43	4	59	3
12	1	28	3	44	4	60	3
13	1	29	3	45	4	61	3
14	1	30	3	46	4	62	3
15	1	31	3	47	4	63	3

Restore Defaults

Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) Service.

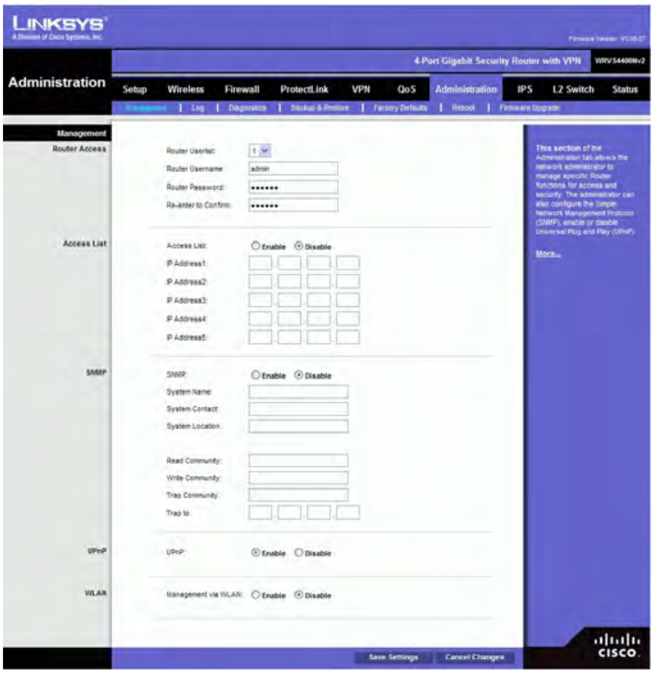
More...

DSCP The Differentiated Services Code Point value in the incoming packet.
Queue Select the traffic forwarding queue, to 4, to which the DSCP priority is mapped.
Restore Defaults Click this button to restore the default DSCP values.

Click **Save Settings** to save your settings. Click **Cancel Changes** to cancel any changes you have entered.

Management

Router Access



Router Userlist: 1
Router Username: admin
Router Password: ••••••
Re-enter to Confirm: ••••••

Access List: ○ Enable ● Disable
IP Address1: . . .
IP Address2: . . .
IP Address3: . . .
IP Address4: . . .
IP Address5: . . .

SNMP: ○ Enable ● Disable
System Name:
System Contact:
System Location:

Read Community:
Write Community:
Trap Community:
Trap to: . . .

UPnP: ● Enable ○ Disable

Management via WLAN: ○ Enable ● Disable

This section of the Administration tab allows the network administrator to manage specific Router functions for access and security. The administrator can also configure the Simple Network Management Protocol (SNMP), enable or disable Universal Plug and Play (UPnP).

Router Userlist. Select a user to configure from the drop-down menu.
Router Username. Enter the user name here.
Router Password. Enter the password.
Re-enter to Confirm. Retype the password in this field.

Access List

Access List specifies which Source IP addresses can manage the device. Default is **Disable**.

SNMP

This configures the Simple Network Management Protocol settings. Users can use management software to read or write information from or to the device.
SNMP. Select **Enable** if you wish to use SNMP. To use SNMP, you need SNMP software on your PC.
System Name Enter a suitable name. This name will be used to identify this device, and will be displayed by your SNMP software.
System Contact Enter contact information for the system.
System Location Enter the location of the system.
Read Community. Enter the SNMP community name for SNMP “Get” commands.
Write Community. Enter the SNMP community name for SNMP “Set” commands.
Trap Community Enter the SNMP community name for SNMP “Trap” commands.
Trap To. Enter the IP Address of the SNMP Manager where traps will be sent. If desired, this may be left blank.

UPnP

UPnP. Universal Plug and Play allows Windows MP and XP to automatically configure the Internet Gateway on its routing table. If you want to use UPnP, keep the default setting, **Enable**. Otherwise, select **Disable**.

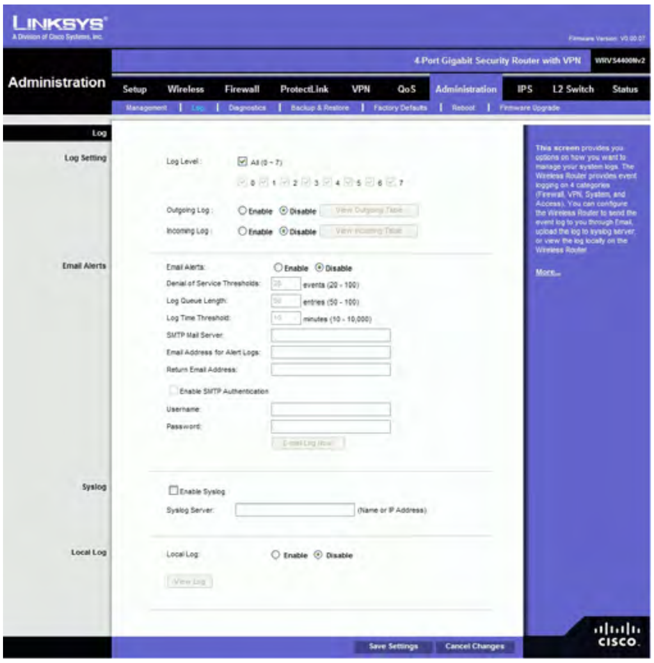
VLAN

Management via VLAN Control the access of Web based GUI from associated wireless clients. The default is **Disable**.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

Log

This screen provides you options on how you want to manage your system logs. The Wireless Router provides four categories of event logging (Firewall, VPN, System, and ACL). You can configure the Wireless Router to send the event log to you through e-mail, upload the log to syslog server, or view the log locally on the Wireless Router.



Log Setting

Log Level: ☑ All (0 ~ 7)
☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7

Outgoing Log: ○ Enable ● Disable

Incoming Log: ○ Enable ● Disable

Email Alerts

Email Alerts: ○ Enable ● Disable

Denial of Service Thresholds: 20 events (20 - 100)

Log Queue Length: 50 entries (50 - 100)

Log Time Threshold: 10 minutes (10 - 10,000)

SMTP Mail Server:

Email Address for Alert Logs:

Return Email Address:

□ Enable SMTP Authentication

Username:

Password:

Syslog

□ Enable Syslog

Syslog Server: (Name or IP Address)

Local Log

Local Log: ○ Enable ● Disable

This screen provides you options on how you want to manage your system logs. The Wireless Router provides event logging on 4 categories (Firewall, VPN, System, and Access). You can configure the Wireless Router to send the event log to you through Email, upload the log to syslog server, or view the log locally on the Wireless Router.

Log Setting

Log Level Select the log level(s) that the Router should record. Log levels and their meanings are:

Log Level

Level	Severity Name	Description
7	LOG_DEBUG	Debug-level message
6	LOG_INFO	Informational messages only
5	LOG_NOTICE	Normal but significant condition
4	LOG_WARNING	Warning conditions
3	LOG_ERR	Error conditions
2	LOG_CRIT	Critical conditions
1	LOG_ALERT	Immediate action needed
0	LOG_EMERG	System unusable

Outgoing Log Select Enable to cause all outgoing packets to be logged. You can then click **View Outgoing Table** to display information on the outgoing packets including Source IP, Destination IP, and Service/Port number.
Incoming Log Select Enable to cause all incoming packets to be logged. You can then click **View Incoming Table** to display information on incoming packets including Source

IP, Destination IP, and Service/Port number.

Email Alerts

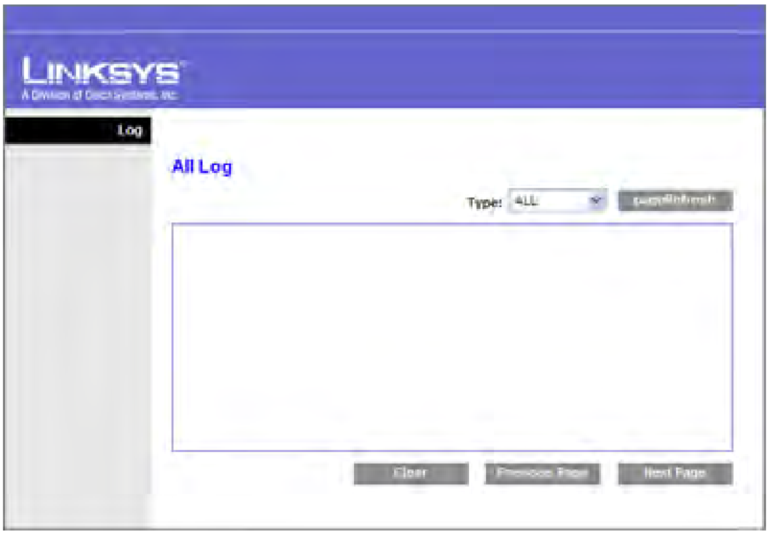
Email Alerts. If enabled, an e-mail will be sent when the number of DoS events exceeds the defined threshold or the total events number exceed 100. If enabled, the e-mail address information (below) must be provided.
Denial of Service Thresholds. Enter the number of DoS (Denial of Service) attacks which need to be blocked by the built-in Firewall before an e-mail alert is sent. The minimum value is 20, the maximum value is 100.
Log Queue Length The default is 50 entries (Router will e-mail the log if there are more than 50 entries).
Log Time Threshold The default is 10 minutes (Router will e-mail the log every 10 minutes).
SMTP Mail Server. Enter the address (domain name) or IP address of the SMTP (Simple Mail Transport Protocol) server you use for outgoing e-mails.
Email Address for Alert Logs. Enter the e-mail address the log is to be sent to.
Return Email Address. The e-mail will show this address as the sender's address.
Enable SMTP Authentication If your SMTP server requires Authentication, you can enable it here, and enter the Username and Password.
E-mail Log Now Press this button to cause the log to be e-mailed immediately.

Syslog

Enable Syslog. Select **Enable** if you want to use this feature.
Syslog Server. Enter the IP Address in the Syslog Server field when Enable Syslog is checked.

Local Log

Local Log. Enable this if you want to see the log locally on the Wireless Router.
View Log button. If **Local Log** is enabled, click **View Log** to view the event log on the Wireless Router.

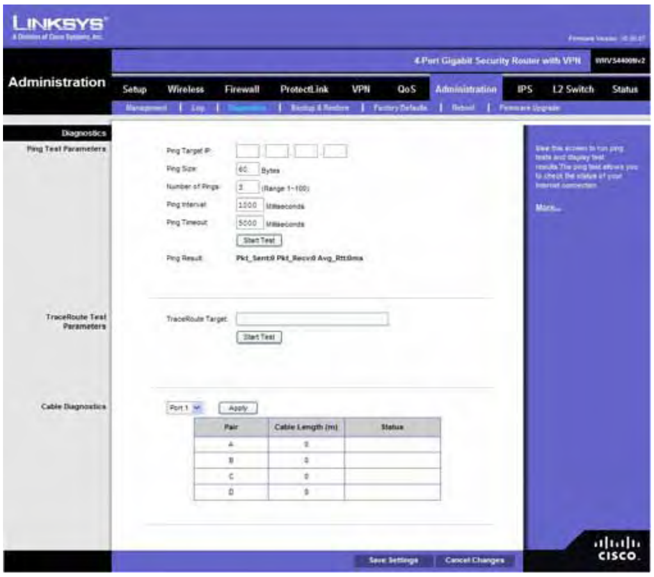


Type: ALL

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

Diagnostics

Ping Test Parameters



Ping Target IP: . . .
Ping Size: 60 Bytes
Number of Pings: 3 (Range 1~100)
Ping Interval: 1000 Milliseconds
Ping Timeout: 5000 Milliseconds
Ping Result: Pkt_Sent:0 Pkt_Recv:0 Avg_Rtt:0ms

TraceRoute Target:

Port 1

Pair	Cable Length (m)	Status
A	0	
B	0	
C	0	
D	0	

Use this screen to run ping tests and display test results. The ping test allows you to check the status of your Internet connection.

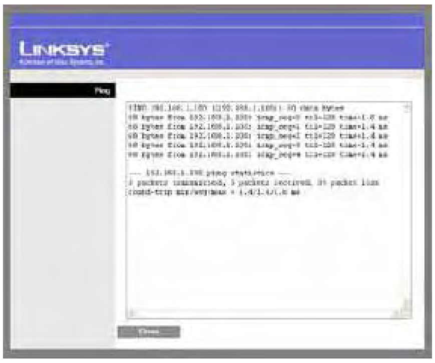
Ping Target IP. Enter the IP address or URL that you want to ping.
Ping Size. Enter the size of the packet you want to use.
Number of Pings. Enter the number of times you wish to ping the target device.
Ping Interval. Enter the time period (in milliseconds) between each ping.
Ping Timeout. Enter the desired time period (in milliseconds). If a response is not received within the defined ping period, the ping is considered to have failed.
Start Test button. Click this button to begin the test. A new screen will appear and display the test results. A summary of the PING results will be shown on the bottom of this screen.
Ping Result. It displays the Ping status.

Traceroute Test Parameters

Traceroute Target Enter the target IP address for the traceroute test.
Start Test Click this button to begin the test. A new screen will appear and display the test results.

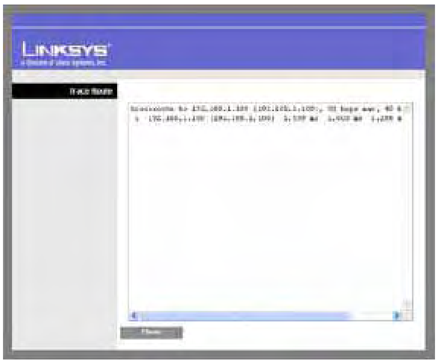
Cable Diagnostics

Port Select the port number from the drop-down menu.
Pair Identifies a specific pair (A, B, C, or D) in the cable. Each cable consists of 8 pins (4 pairs).
Cable Length Displays the length of the cable in meters.
Status Displays the status of the pair.



```
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=128 time=1.8 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=1.4 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=128 time=1.4 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=128 time=1.4 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=128 time=1.4 ms

--- 192.168.1.100 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.4/1.4/1.8 ms
```

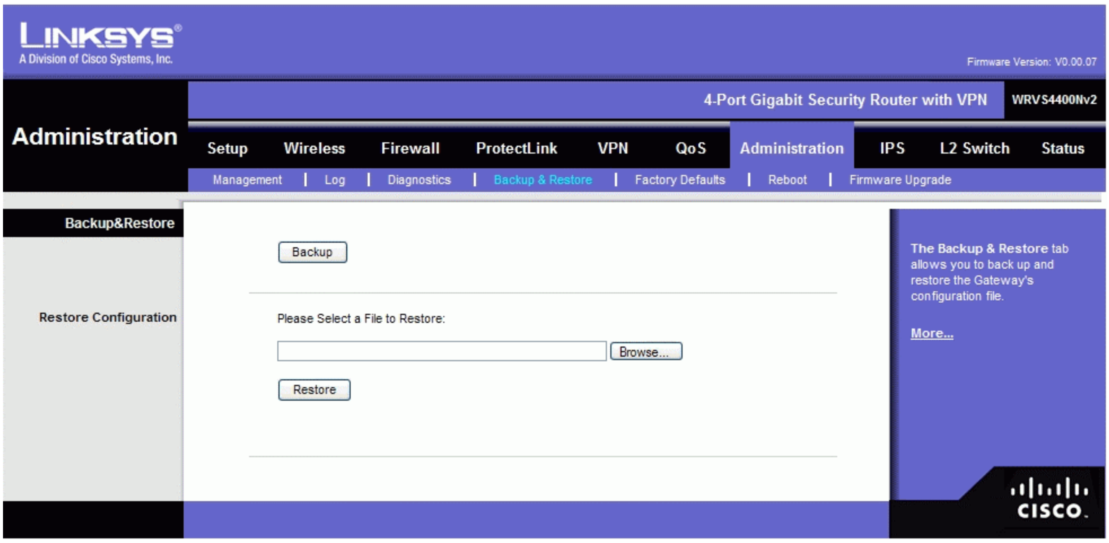
Traceroute Test Parameters



```
traceroute to 192.168.1.100 (192.168.1.100), 30 hops max, 40 b
 1  192.168.1.100 (192.168.1.100)  1.[illegible] ms  1.[illegible] ms  1.[illegible] m
```

TraceRoute Target. Enter the IP address or Host name to perform the traceroute testing. **Start Test button.** Click this button to begin the test. A new screen will appear and display the test results.

Backup & Restore



Please Select a File to Restore:

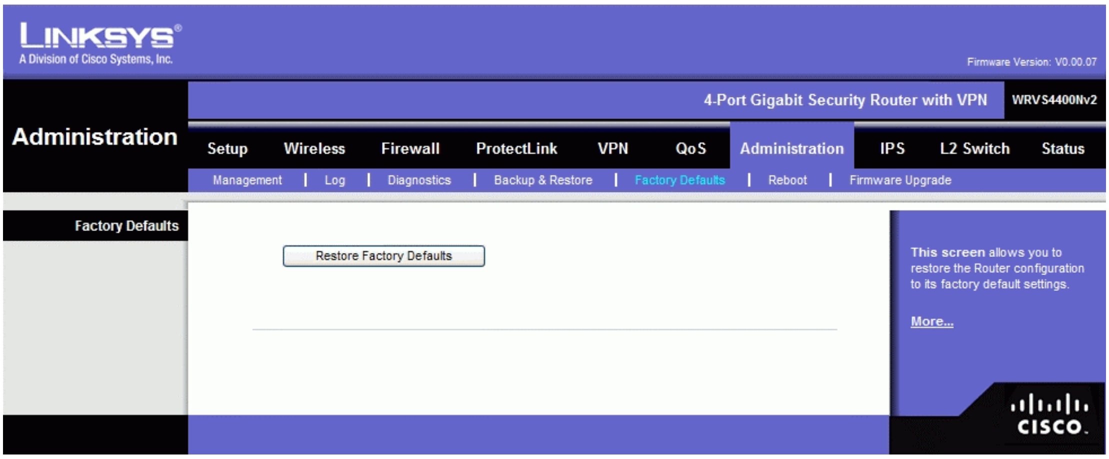
The Backup & Restore tab allows you to back up and restore the Gateway's configuration file.

Backup button. To download a copy of the current configuration and storethe file on your PC, click **Backup** to start the download.

Restore Configuration

Select a previously saved configuration file to restore the configuration to the Wireless Router. This could be helpful if you want to use the same configuration on a new hardware or after resetting to the factory defaults. You can either enter the file path name yourself or use the **Browse** button to select a file from the Windows file system.
Browse button. Click this button to select a previously saved configuration from the Windows file system.
Restore button. Click this button to start the restoration process.

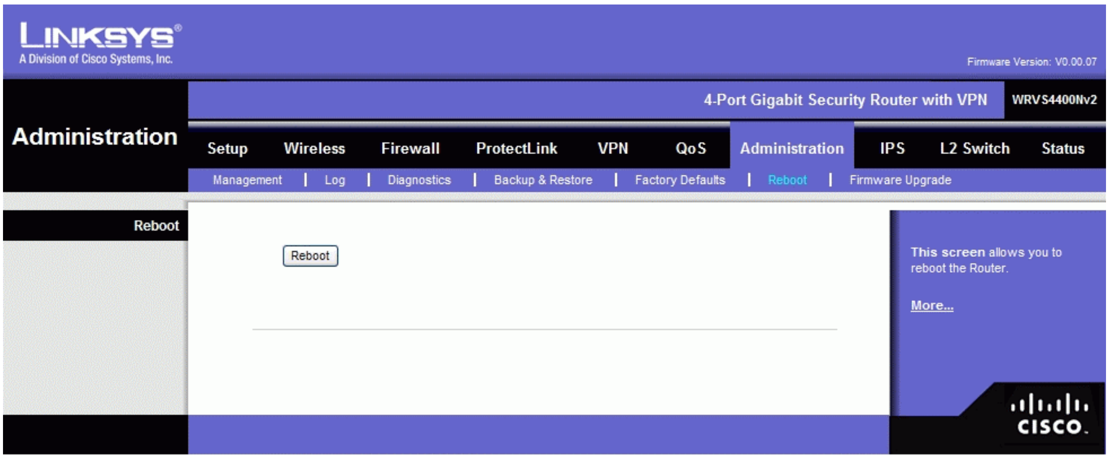
Factory Defaults



This screen allows you to restore the Router configuration to its factory default settings.

Restore Factory Defaults. Click this button to reset all configuration settings to their default values. All settings that have been saved will be lost when the default settings are restored. After clicking the button, another screen will appear. Click **OK** to continue. Another screen will appear while the system reboots.

Reboot

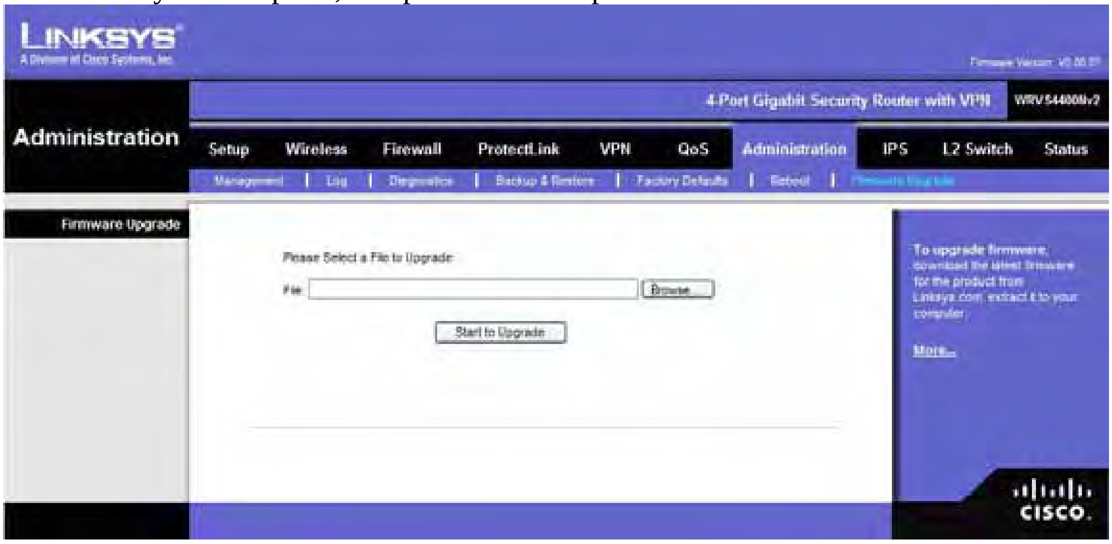


This screen allows you to reboot the Router.

Reboot. Click this button to reboot the Router. This operation will not cause the Router to lose any of its stored settings.

Firmware Upgrade

To upgrade firmware, download the latest firmware for the product from Linksys.com, extract it to your computer, and perform the steps below:



Please Select a File to Upgrade:

File:

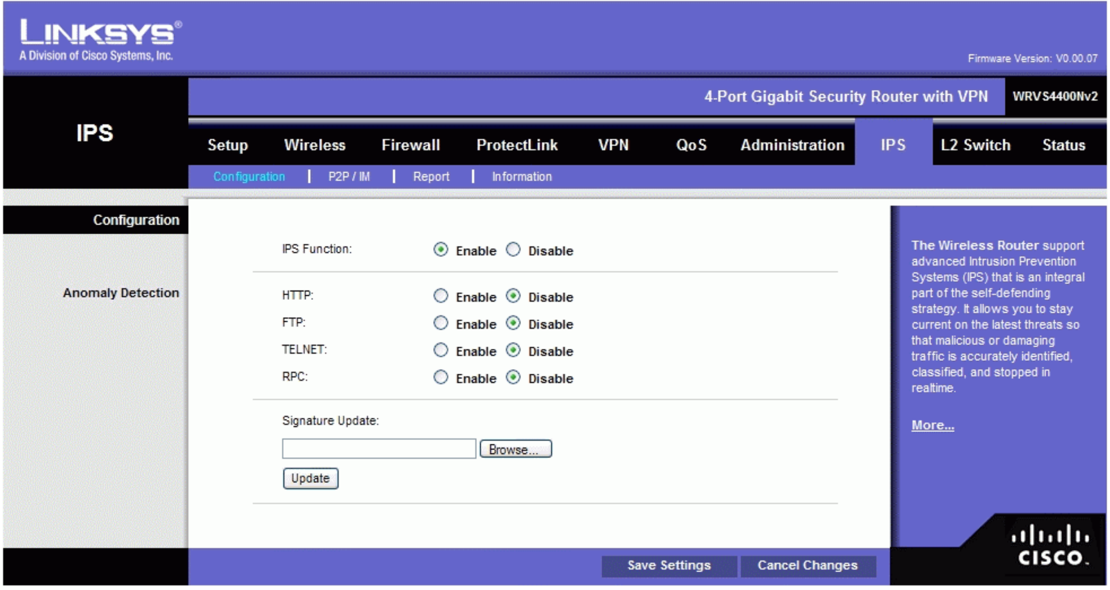
To upgrade firmware, download the latest firmware for the product from Linksys.com, extract it to your computer.

1. **File**. Type in the name of the extracted firmware upgrade file or click **Browse** to locate the file from the file system.
2. **Start to Upgrade**. Once you have selected the appropriate file, click the **Start to Upgrade** button and follow the on-screen instructions to upgrade your firmware.

IPS

The Wireless Router supports advanced Intrusion Prevention Systems (IPS), which is an integral part of the self-defending strategy. It allows you to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped in realtime. You can use IPS together with Firewall, IP based ACL, and IPsec VPN to achieve maximum securities. The IPS is hardware-accelerated on this Wireless Router.

Configure IPS functions on this screen after enabling IPS.



IPS Function: ● Enable ○ Disable

HTTP: ○ Enable ● Disable

FTP: ○ Enable ● Disable

TELNET: ○ Enable ● Disable

RPC: ○ Enable ● Disable

Signature Update:

The Wireless Router support advanced Intrusion Prevention Systems (IPS) that is an integral part of the self-defending strategy. It allows you to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped in realtime.

Configuration

IPS Function. **Enable** or **Disable** the IPS Function as desired.

Abnormally Detection

- **HTTP**. Web attacks use weaknesses on HTTP protocol to trigger the buffer overflow on Web servers. The default is Disable.
- **FTP**. FTP attacks use weaknesses on FTP protocol to generate illegal FTP commands to the FTP server. The default is Disable.
- **TELNET**. Telnet attacks use weakness on TELNET protocol to execute illegal commands on the TELNET server. The default is Disable.
- **RPC**. Remote Procedure Call allows attackers to issue illegal commands to be executed on RPC server. The default is Disable

Signature Update. To protect your local network from the latest Internet threats, you are encouraged to upgrade the IPS Signature file bi-weekly. First, you need to download the Signature file from www.linksys.com to your PC. Then you can select this file by clicking the **Browse** button. Use the **Upgrade** button to start an upgrade.

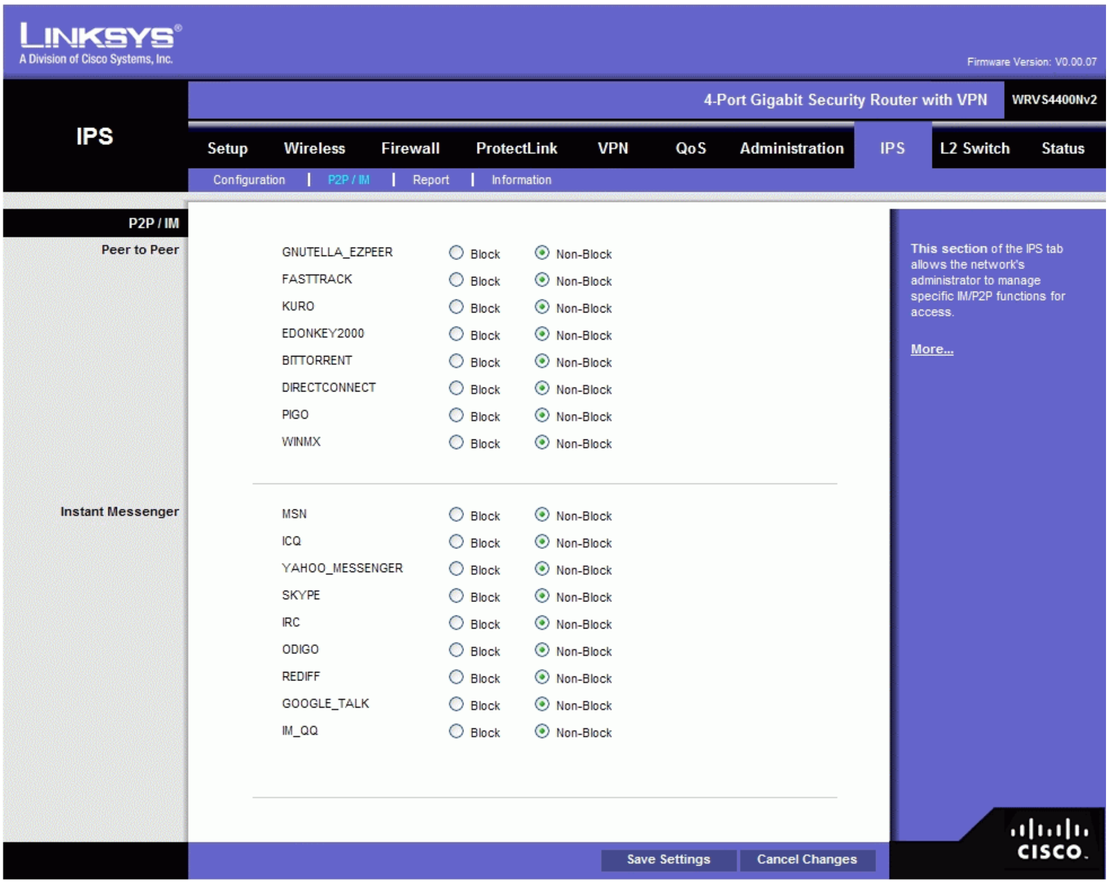
Browse button. Enter the path name of the new signature file In the field provided, or click the **Browse** button to find this file from your Windows file system.

Update button. After you have selected the file, click this button to start an upgrade.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

P2P/M

This tab allows the system administrator to set up policies on using P2P or IM software across the Internet.



Peer to Peer		
GNUTELLA_EZPEER	○ Block	● Non-Block
FASTTRACK	○ Block	● Non-Block
KURO	○ Block	● Non-Block
EDONKEY2000	○ Block	● Non-Block
BITTORRENT	○ Block	● Non-Block
DIRECTCONNECT	○ Block	● Non-Block
PIGO	○ Block	● Non-Block
WINMX	○ Block	● Non-Block

Instant Messenger		
MSN	○ Block	● Non-Block
ICQ	○ Block	● Non-Block
YAHOO_MESSENGER	○ Block	● Non-Block
SKYPE	○ Block	● Non-Block
IRC	○ Block	● Non-Block
ODIGO	○ Block	● Non-Block
REDIFF	○ Block	● Non-Block
GOOGLE_TALK	○ Block	● Non-Block
IM_QQ	○ Block	● Non-Block

This section of the IPS tab allows the network's administrator to manage specific IM/P2P functions for access.

More...

Peer to Peer

When users download files from the Internet by Peer to Peer (P2P) software, the WAN port bandwidth will be occupied. You can enable the blocking to the following P2P software applications. The defaults are **non-block** for the following applications:

GNUTELLA(EZPEER), FASTTRACK, KURO, EDONKEY2000, BITTORRECT, DIRECTCONNECT, PIGO, and WINMX.

Instant Messenger

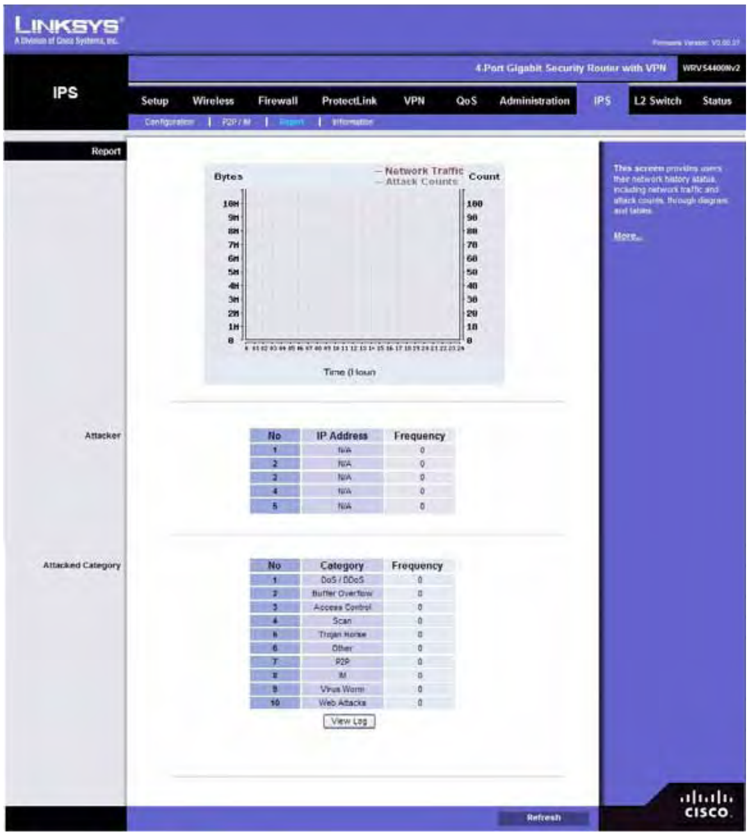
Users might use IM software to chat with friends or transferring files (bandwidth hogging). You can enable the blocking to the following IM software applications. The defaults are **non-block** for the following applications.

MSN, ICQ, YAHOO MESSEGER, SKYPE, IRC, ODIGO, REDIFF, GOOGLE TALK, and IM QQ.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

Report

This screen provides the network history status, including network traffic and attack counts, through diagram and tables.



This screen provides users their network history status, including network traffic and attack counts, through diagram and tables.

No	IP Address	Frequency
1	N/A	0
2	N/A	0
3	N/A	0
4	N/A	0
5	N/A	0

No	Category	Frequency
1	DoS / DDoS	0
2	Buffer Overflow	0
3	Access Control	0
4	Scan	0
5	Trojan Horse	0
6	Other	0
7	P2P	0
8	IM	0
9	Virus Worm	0
10	Web Attacks	0

Report Diagram: Twenty-four hour diagram displays network traffic and attacks.

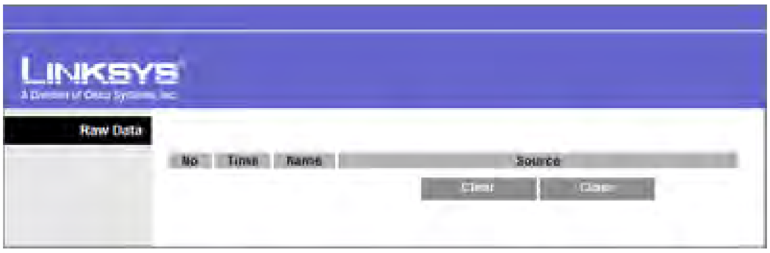
Attacker

Displays the IP Address of attackers and the frequency (number of times) of the attacks in a table.

Attacked Category

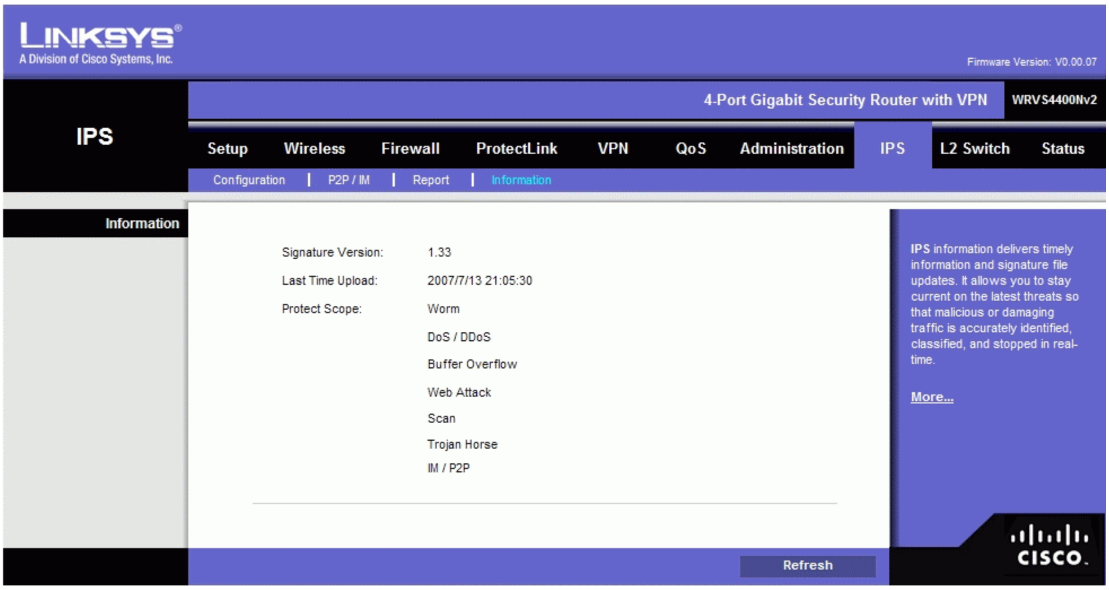
Displays the category (type) of attack and the frequency (number of times) of the attacks in a table.

Click the **View Log** button to view the log.



No	Time	Name	Source

Information



Signature Version: 1.33

Last Time Upload: 2007/7/13 21:05:30

Protect Scope: Worm
DoS / DDoS
Buffer Overflow
Web Attack
Scan
Trojan Horse
IM / P2P

IPS information delivers timely information and signature file updates. It allows you to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped in real-time.

Signature Version. The Signature Version displays the version of the signature patterns file loaded in the Wireless Router that protects against malicious threats.

Last Time Upload. This displays when the signature patterns file in the Wireless Router were last updated.

Protect Scope. Displays a list of the categories of attacks that the IPS feature in the Router protects against.

Those includes Worm, DoS/DDoS, Buffer Overflow, Web Attack, Scan, Trojan Horse, and IM / P2P.

L2 Switch Tab

The Layer 2 Switch Tab provides configurations to the layer 2 switching features on the four Ethernet LAN ports of the Wireless Router. They include VLAN, port configuration, cable diagnostics, and RADIUS authentication.

VLAN

Create VLAN

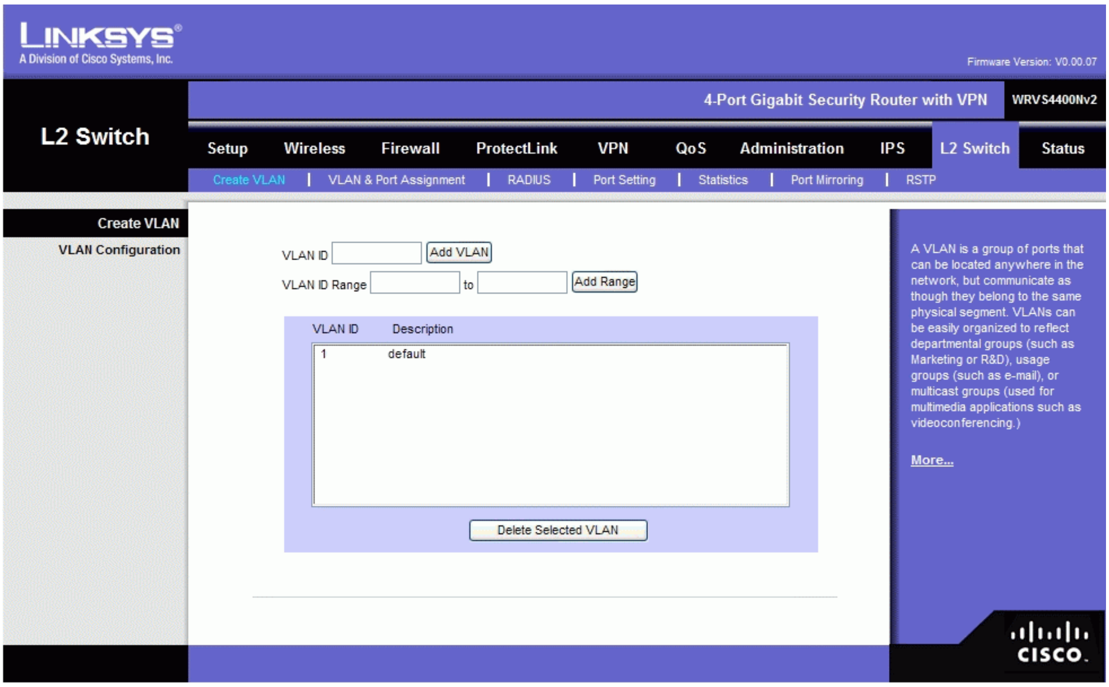
VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduce the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

VLANs function at layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router is needed to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs.

VLANs are broadcast and multicast domains. Broadcast and multicast traffic is transmitted only in the VLAN in which the traffic is generated.

This device supports up to 4 VLANs, including the default VLAN.



VLAN ID

VLAN ID Range to

VLAN ID	Description
1	default

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing.)

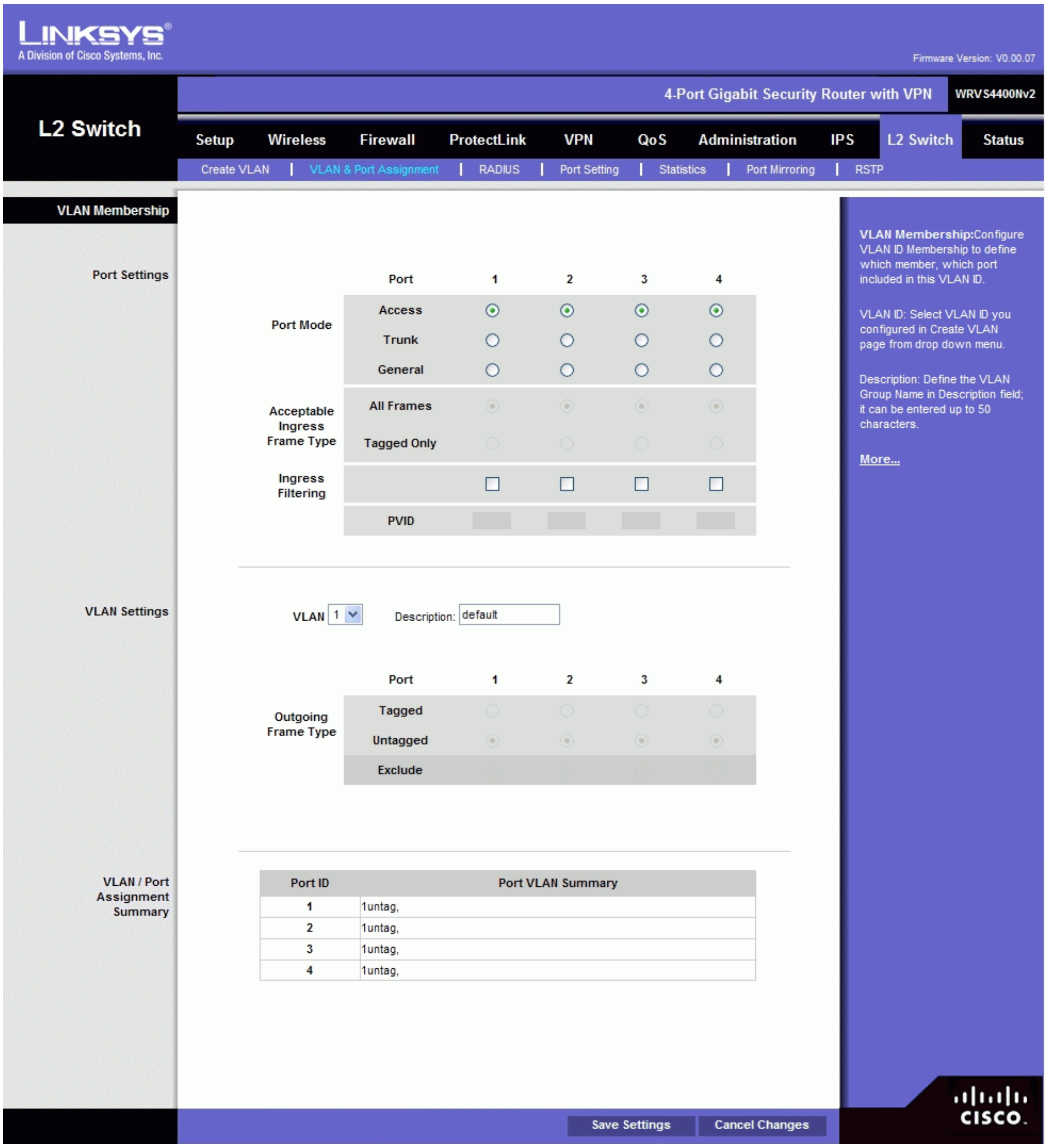
VLAN ID The VLAN ID number. This can be any number from 2 to 3290, or from 3293 to 4094. (VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 3291-3292 are reserved and cannot be used.) To create a VLAN, enter the ID number and click **Add VLAN**.

VLAN ID Range To create multiple VLANs with a range of ID numbers, enter the starting and ending ID numbers and click **Add Range**.

Delete Selected VLAN To delete a VLAN, select it form the VLAN list and click **Delete Selected VLAN**.

VLAN & Port Assignment

This Tab is a combination of Port settings and VLAN membership tabs in one on this device and other routers.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: V0.00.07
4-Port Gigabit Security Router with VPN
WRVS4400Nv2
L2 Switch
Setup
Wireless
Firewall
ProtectLink
VPN
QoS
Administration
IPS
L2 Switch
Status
Create VLAN | VLAN & Port Assignment | RADIUS | Port Setting | Statistics | Port Mirroring | RSTP
VLAN Membership
Port Settings
VLAN Settings
VLAN / Port Assignment Summary
More...
Save Settings
Cancel Changes
cisco

	Port	1	2	3	4
Port Mode	Access	●	●	●	●
	Trunk	○	○	○	○
	General	○	○	○	○
Acceptable Ingress Frame Type	All Frames	●	●	●	●
	Tagged Only	○	○	○	○
Ingress Filtering		□	□	□	□
	PVID				

VLAN 1 Description: default

	Port	1	2	3	4
Outgoing Frame Type	Tagged	○	○	○	○
	Untagged	●	●	●	●
	Exclude	○	○	○	○

Port ID	Port VLAN Summary
1	1untag,
2	1untag,
3	1untag,
4	1untag,

VLAN Membership:Configure VLAN ID Membership to define which member, which port included in this VLAN ID.

VLAN ID: Select VLAN ID you configured in Create VLAN page from drop down menu.

Description: Define the VLAN Group Name in Description field; it can be entered up to 50 characters.

The first section is port specific settings regarding the use of VLAN (nothing to do with individual VLANs). It requires users to specify the port mode for each port. The "acceptable frame type" and "PVID" options are for "General" port mode only

Port Mode: select one of the three modes:

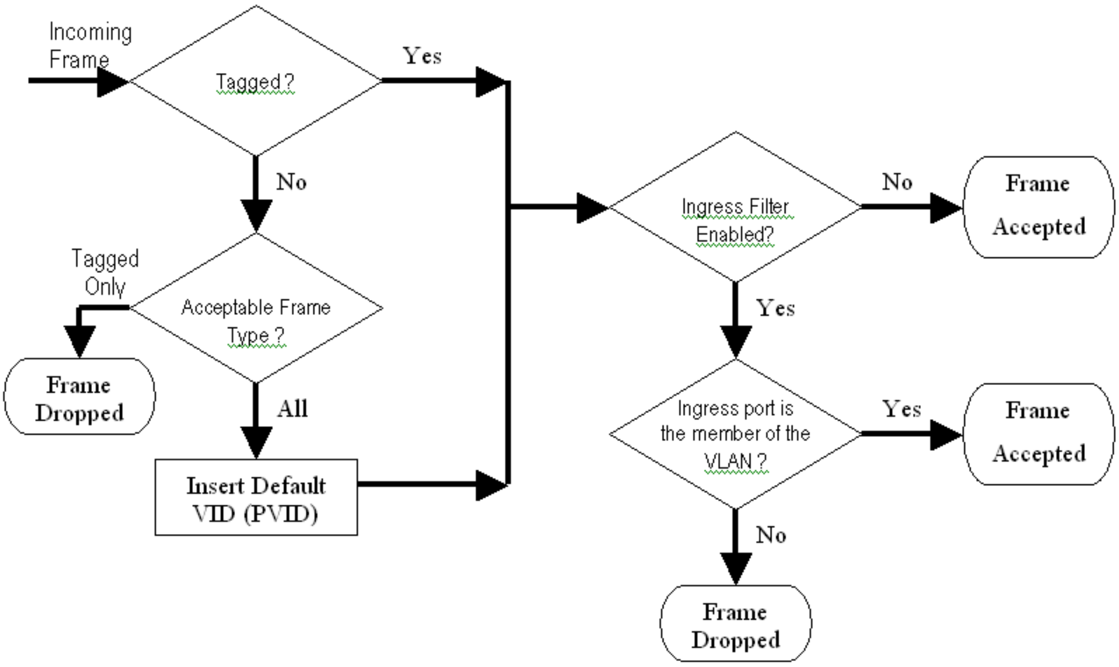
- **Access**: all the frames are untagged coming in or going out of the switch port. Wireless port can be set to this mode only.
- **Trunk**: all the frames are tagged coming in or going out of the switch except for VLAN ID 1 (called native VLAN or default VLAN in Cisco)

Note: this cannot be supported on Vitesse 7385 switch chipset.

- **General**: all the frames can be tagged or untagged coming in to the switch. If it is untagged, default PVID will apply to the packet. Only the General mode users can choose the following two options.
  - Acceptable Ingress Frame Type:

    All Frames: all the incoming frames are acceptable
    Tagged Only: only tagged incoming frames are acceptable
  - **Ingress Filtering**: check the VLAN ID on the incoming packet. If the port is a member of this VLAN, accept the frame. Otherwise, drop it. If not enabled, all frames are accepted.
  - **PVID**: the VLAN ID of the default (untagged) VLAN

The following diagram describes the packet flow on General mode. It first checks the filter on "acceptable frame type", then check again on "ingress filtering" option.



The second section is per VLAN settings to be used with each port. It requires users to specify each VLAN to be tagged, untagged, or excluded on the specific port.

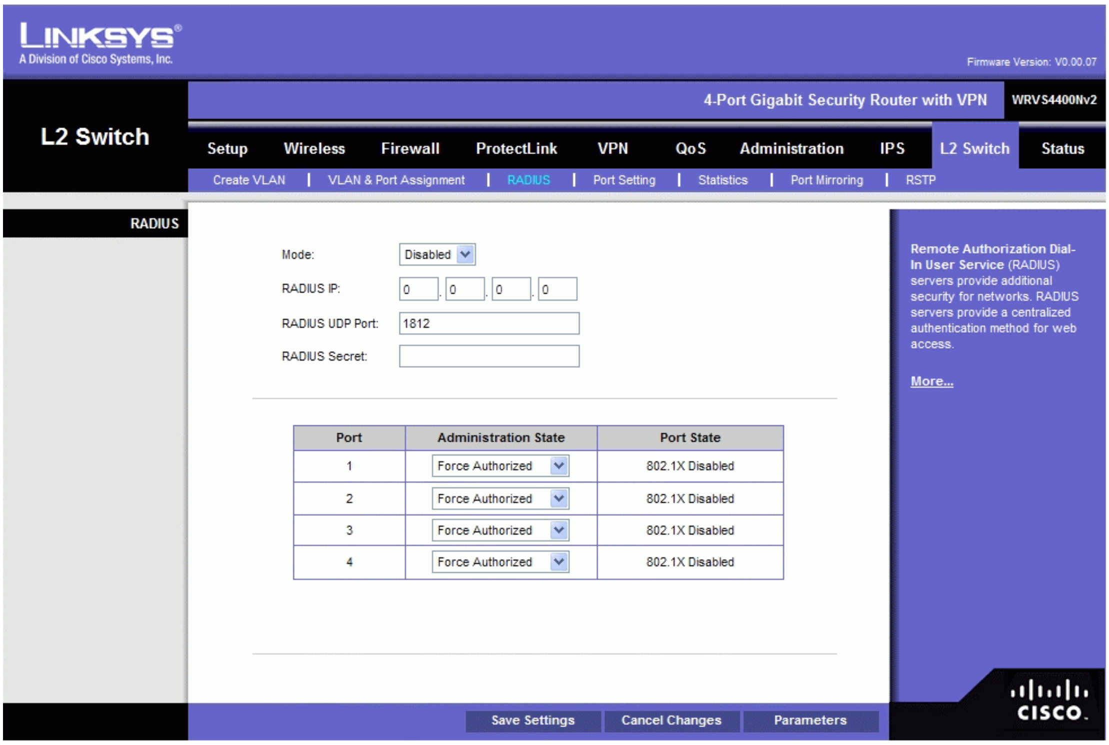
- VLAN: Select a VLAN ID to be configured
- VLAN NAME: VLAN description (read-only) to help user identify this VLAN
- Tagged: egress frames from this port is tagged for this VLAN
- Untagged: egress frames from this port is untagged for this VLAN
- Excluded: this port does not participate in this VLAN at all

For Access port, the available options are either untagged or excluded. Therefore, wireless port can set to one of these two modes for each VLAN. Only one of the VLAN ID can be selected (untagged).
For Trunk port, the options are tagged or excluded for all VLAN IDs except VLAN 1. VLAN 1 must be untagged.
For General port, the options are tagged or untagged for PVID; tagged or excluded for all other VLAN IDs.
The third section is a summary of VLAN subscriptions on each port. "U" means

untagged while “T” means tagged.

Radius

RADIUS mode provides authentication on devices connecting to the LAN ports. It requires installation of a RADIUS server on your local network.



LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: V0.00.07
4-Port Gigabit Security Router with VPN
WRVS4400Nv2
L2 Switch
Setup
Wireless
Firewall
ProtectLink
VPN
QoS
Administration
IPS
L2 Switch
Status
Create VLAN | VLAN & Port Assignment | RADIUS | Port Setting | Statistics | Port Mirroring | RSTP
RADIUS
Save Settings
Cancel Changes
Parameters
cisco.

Mode: Disabled

RADIUS IP: 0 . 0 . 0 . 0

RADIUS UDP Port: 1812

RADIUS Secret:

Port	Administration State	Port State
1	Force Authorized	802.1X Disabled
2	Force Authorized	802.1X Disabled
3	Force Authorized	802.1X Disabled
4	Force Authorized	802.1X Disabled

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

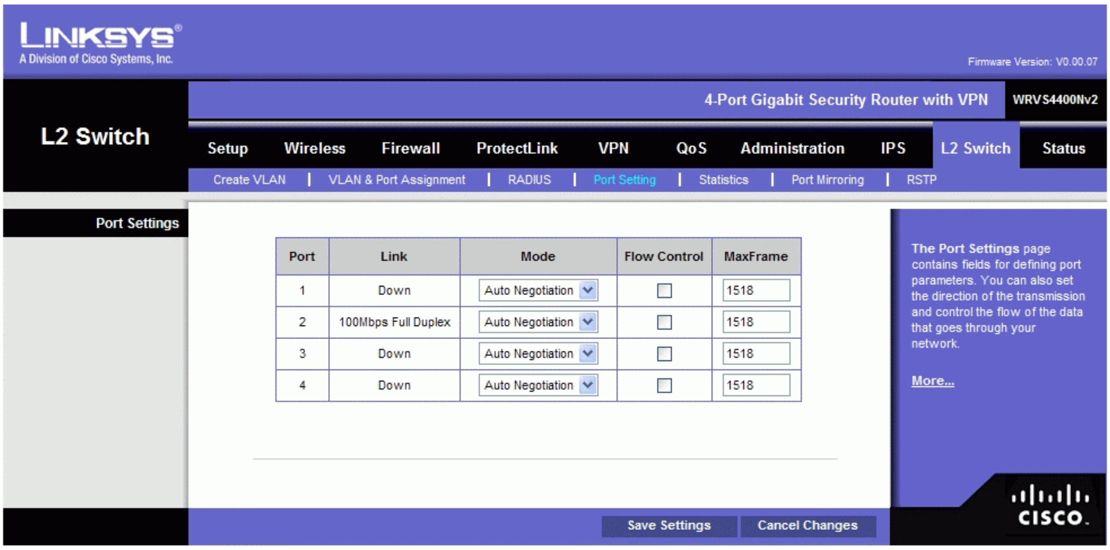
More...

Mode. Select **Enabled** or **Disabled**, as desired.
RADIUS IP. Enter the RADIUS server IP address.
RADIUS UDP Port. Identifies the UDP port. The UDP port is used to verify the RADIUS server authentication.
RADIUS Secret. Indicates the Key string used for authenticating and encrypting all RADIUS communications between the Wireless Router and the RADIUS server. This key must match the RADIUS server's configuration.
Administration State. Specifies if each port needs RADIUS authentication. The defaults are **Force Authorized** so no authentication is needed. The possible field values are:

- **Auto.** The controlled port state is set by the RADIUS Mode.
- **Force Authorized**. The controlled port state is set to Force-Authorized (forward traffic). All connections can be made.
- **Force Unauthorized**. The controlled port state is set to Force-Unauthorized (discard traffic). All connections are blocked.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

Port Settings



Port	Link	Mode	Flow Control	MaxFrame
1	Down	Auto Negotiation	☐	1518
2	100Mbps Full Duplex	Auto Negotiation	☐	1518
3	Down	Auto Negotiation	☐	1518
4	Down	Auto Negotiation	☐	1518

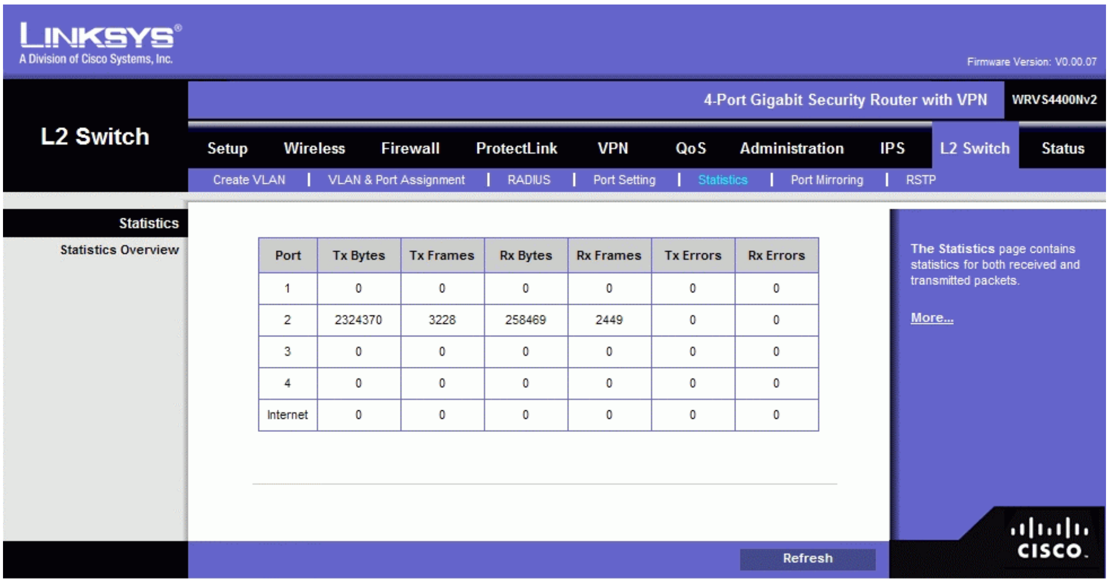
The Port Settings page contains fields for defining port parameters. You can also set the direction of the transmission and control the flow of the data that goes through your network.

More...

Port. Specifies the number of the four LAN ports.
Link. Displays the port duplex mode (Full or Half) and speed (10/100/1000 Mbps). Full indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. Half indicates that the interface supports transmission between the device and the client in only one direction at a time.
Mode. Specifies port duplex mode (Full or Half) and speed (10/100/1000 Mbps). Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner. Default is **Auto.**
Flow Control. Configure the flow control setting on the port. Select to enable. The default is disabled.
MaxFrame. Configure the maximum ethernet frame size sent or received on the port. Default is 1518. You can set only to a value lower than 1518.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

Statistics



Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	2324370	3228	258469	2449	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
Internet	0	0	0	0	0	0

The **Statistics** page contains statistics for both received and transmitted packets.

Statistics Overview

Tx Bytes Displays the number of Bytes transmitted from the selected port.

Tx Frames Displays the number of Frames transmitted from the selected port.

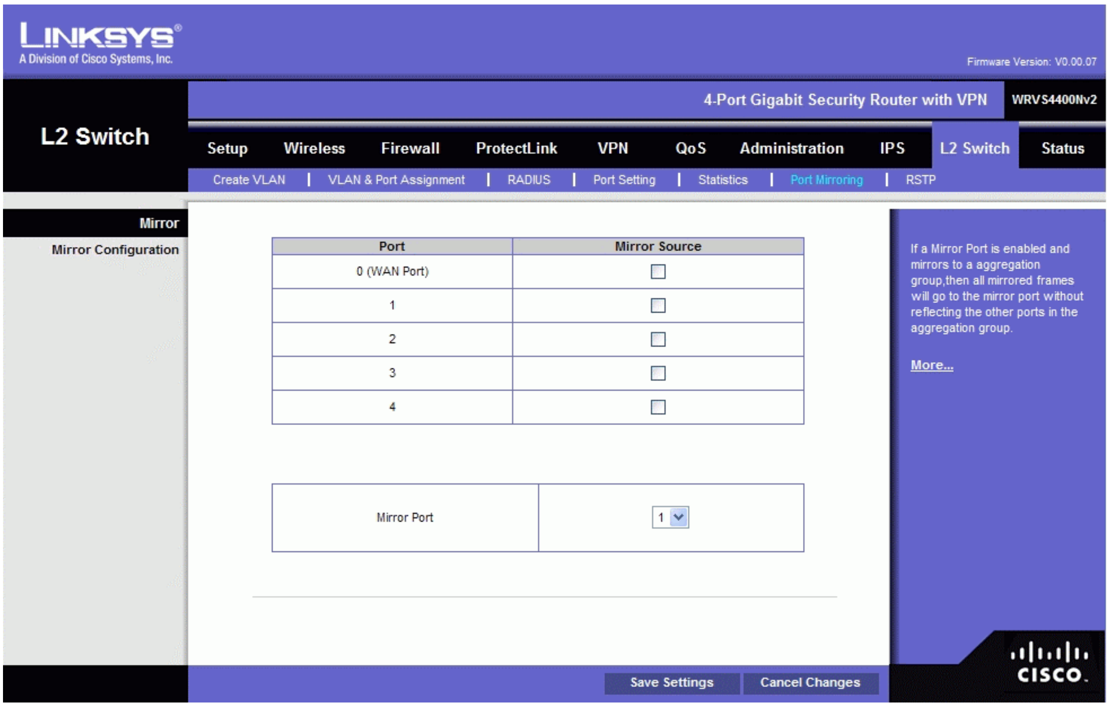
Rx Bytes Displays the number of Bytes received on the selected port.

Rx Frames Displays the number of Frames received on the selected port.

Tx Errors Displays the number of error packets transmitted from the selected port.

Rx Errors Displays the number of error packets received from the selected port.

Port Mirroring



Port	Mirror Source
0 (WAN Port)	□
1	□
2	□
3	□
4	□

Mirror Port	1

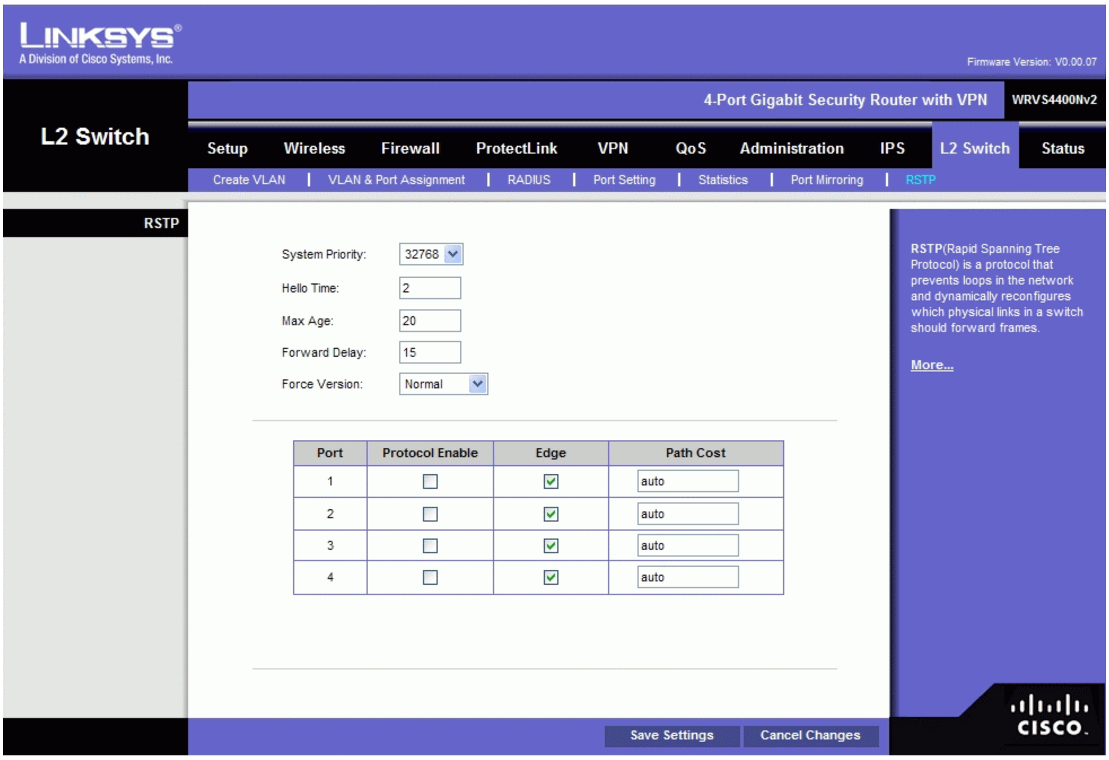
If a Mirror Port is enabled and mirrors to a aggregation group,then all mirrored frames will go to the mirror port without reflecting the other ports in the aggregation group.

Mirror Source Use this to enable or disable source port mirroring for each port on the Router. To enable source port mirroring on a port, check the box next to that port. To disable source port mirroring on a port, leave the box unchecked. The default is **disabled**.

Mirror Port Select the mirror destination port from the drop-down menu.

RSTP

The RSTP (Rapid Spanning Tree Protocol) protocol prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames.


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: V0.00.07
L2 Switch
4-Port Gigabit Security Router with VPN
WRVS4400Nv2
Setup
Wireless
Firewall
ProtectLink
VPN
QoS
Administration
IPS
L2 Switch
Status
Create VLAN | VLAN & Port Assignment | RADIUS | Port Setting | Statistics | Port Mirroring | RSTP
RSTP
More...
Save Settings
Cancel Changes
CISCO.

System Priority: 32768

Hello Time: 2

Max Age: 20

Forward Delay: 15

Force Version: Normal

Port	Protocol Enable	Edge	Path Cost
1	□	☑	auto
2	□	☑	auto
3	□	☑	auto
4	□	☑	auto

RSTP(Rapid Spanning Tree Protocol) is a protocol that prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames.

System Priority Enter the system priority from 0 to 61440 in increments of 4096. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344, and 61440. The lower the system priority, the more likely the Router is to become the root in the Spanning Tree. The default is 327688.

Hello Time Enter a number from 1 to 10. The default is 2.

Max Age Enter a number from 6 to 40. The default is 20.

Forward Delay Enter a number from 4 to 30. The default is 15.

Force Version This is the default protocol version to use. Select Normal (use RSTP) or Compatible (compatible with old STP). The default is **Normal**.

Protocol Enable Check this box to enable RSTP on the associated port. The default is unchecked (RSTP disabled).

Edge Check this box to specify that the associated port is an edge port (end station). Uncheck the box to specify that the associated port is a link (bridge) to another STP device. The default is checked (edge port).

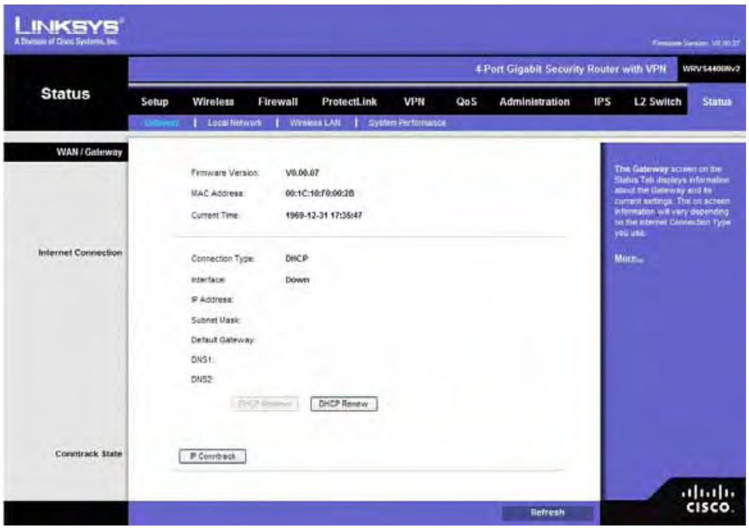
Path Cost This is the RSTP path cost for the designated ports. Enter a number from 1 to 200000000, or auto (autogenerated path cost). The default is auto.

Status Tab

The Status Tab provides current status on this Wireless Router including WAN, LAN, Wireless LAN, System Performance, VPN client connections, and IPsec VPN connections.

WAN / Gateway

This screen provides some basic information on the Wireless Router (e.g. firmware version, time) and WAN port MAC/IP address and connection status.



Firmware Version: V0.00.07

MAC Address: 00:1C:10:F0:00:2B

Current Time: 1969-12-31 17:35:47

Connection Type: DHCP

Interface: Down

IP Address:

Subnet Mask:

Default Gateway:

DNS1:

DNS2:

The Gateway screen on the Status Tab displays information about the Gateway and its current settings. The on screen information will vary depending on the Internet Connection Type you use.

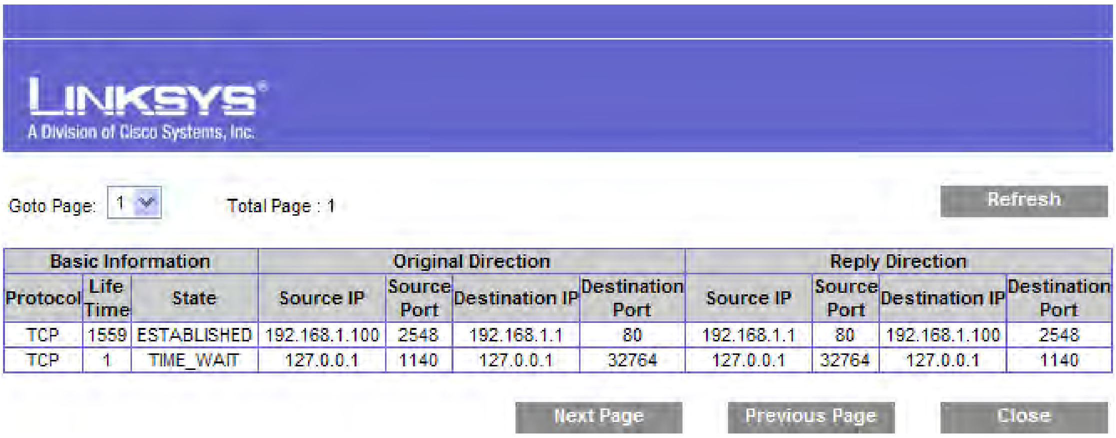
Firmware Version. Displays the current firmware version.
MAC Address. Displays the WAN port MAC Address, as seen by your ISP.
Current Time. Displays the time on this Wireless Router according to your settings on the Setup->Time tab.

Internet Connection

Connection Mode. Displays the Internet connection type setting on WAN port.
Interface. Displays the WAN port Interface status (Up or Down).
IP Address. Displays the WAN port IP Address.
Subnet Mask. Displays the WAN port IP subnetmask.
Default Gateway. Displays the default Router to reach Internet or other networks from the WAN port.
DNS. Displays the DNS (Domain Name System) IP addresses currently used by this Gateway.
DHCP Release button. Click this button to release IP address on WAN port if using DHCP.
DHCP Renew button. Click this button to renew IP address on the WAN port if using DHCP.
IP Conntrack Click this button to display the IP Conntrack screen.

IP Conntrack

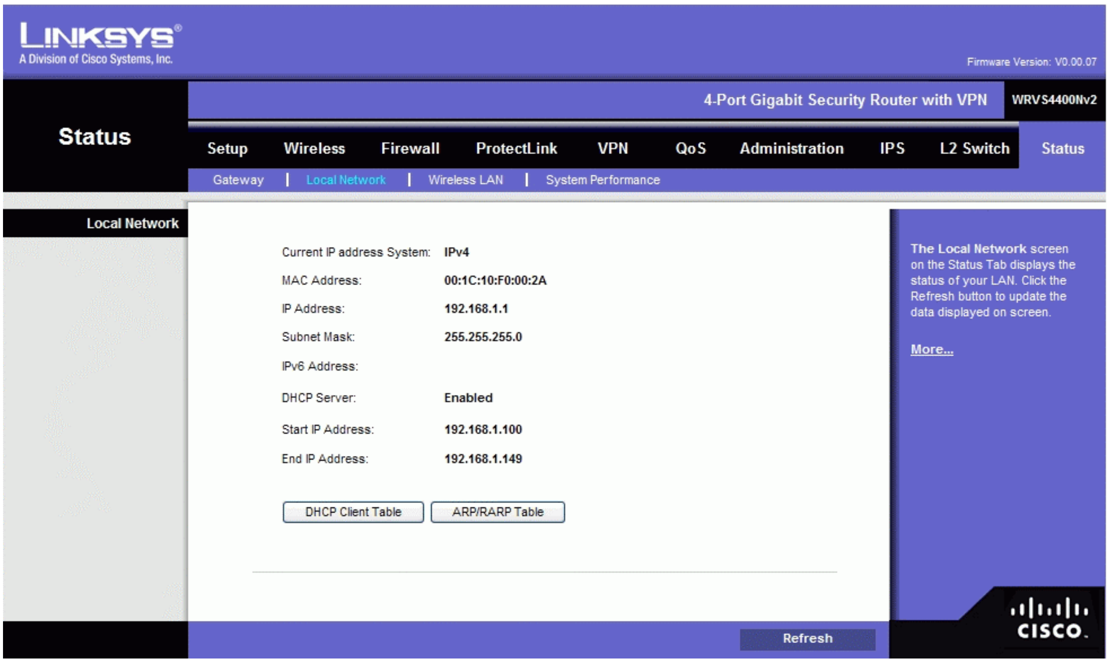
The IP Conntrack (Connection Tracking) screen displays information about TCP/UDP connections, such as source and destination IP address and port number pairs (known as socket pairs), protocol types (TCP/UDP/ICMP), connection state and timeouts. To see more information, click Next Page or Previous Page, or select the page from the Goto Page drop-down menu. To see the latest information, click Refresh. Click Close to return to the Status > Gateway screen.



Basic Information			Original Direction				Reply Direction			
Protocol	Life Time	State	Source IP	Source Port	Destination IP	Destination Port	Source IP	Source Port	Destination IP	Destination Port
TCP	1559	ESTABLISHED	192.168.1.100	2548	192.168.1.1	80	192.168.1.1	80	192.168.1.100	2548
TCP	1	TIME_WAIT	127.0.0.1	1140	127.0.0.1	32764	127.0.0.1	32764	127.0.0.1	1140

Local Network

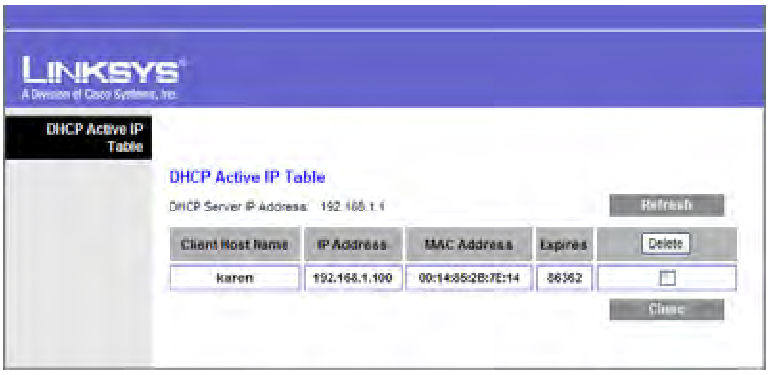
This screen provides some basic information on the LAN ports of this Wireless Router.



Current IP address System: IPv4
MAC Address: 00:1C:10:F0:00:2A
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
IPv6 Address:
DHCP Server: Enabled
Start IP Address: 192.168.1.100
End IP Address: 192.168.1.149

The Local Network screen on the Status Tab displays the status of your LAN. Click the Refresh button to update the data displayed on screen.

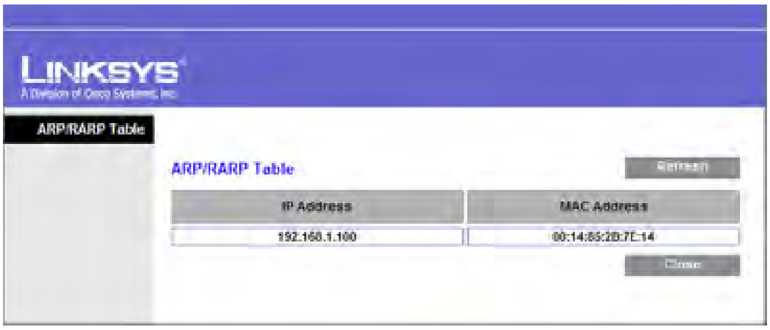
Current IP address System. Displays the IP versions configured on the LAN side.
MAC Address. Displays the LAN port MAC Address. All four LAN ports share the same MAC address.
IP Address. Displays the LAN port IPv4 Address. All four LAN ports share the same MAC address.
Subnet Mask. Displays the LAN port IPv4 subnet mask.
IPv6 Address. Displays the LAN port IPv6 IP address, if IPv6 is enabled.
DHCP Server. Displays the status of the Router's DHCP server.
Start IP Address. Displays the beginning of the range of IP addresses used by the DHCP Server.
End IP Address. Displays the end of the range of IP addresses used by the DHCP Server.
DHCP Client Table button. Click this button to open the DHCP Client Table screen, which shows you which PCs have been assigned an IP address from the Wireless Router’s DHCP server. You will see a list of DHCP clients (PCs and other network devices) with the following information: Client Host Name, IP Address, MAC Address, and the length of time (in second) before its assigned IP address expires.
ARP/RARP Table button. Click this button will open the ARP Table screen, which shows you the ARP Table on the Wireless Router. The ARP Table provides IP address to MAC address mapping. On the ARP Table screen, you will see a list of address mapping between IP (layer 3) and MAC (layer 2).



DHCP Active IP Table

DHCP Server IP Address: 192.168.1.1

Client Host Name	IP Address	MAC Address	Expires	Delete
karen	192.168.1.100	00:14:85:2B:7E:14	86362	□

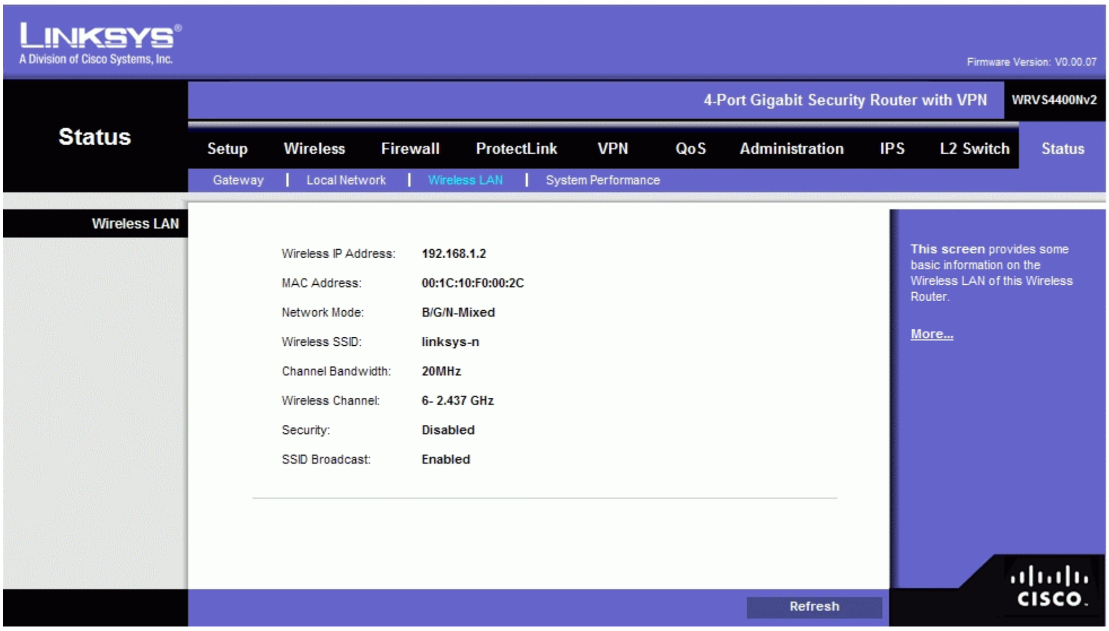


ARP/RARP Table

IP Address	MAC Address
192.168.1.100	00:14:85:2B:7E:14

Wireless LAN

This screen provides some basic information on the Wireless LAN of this Wireless Router.



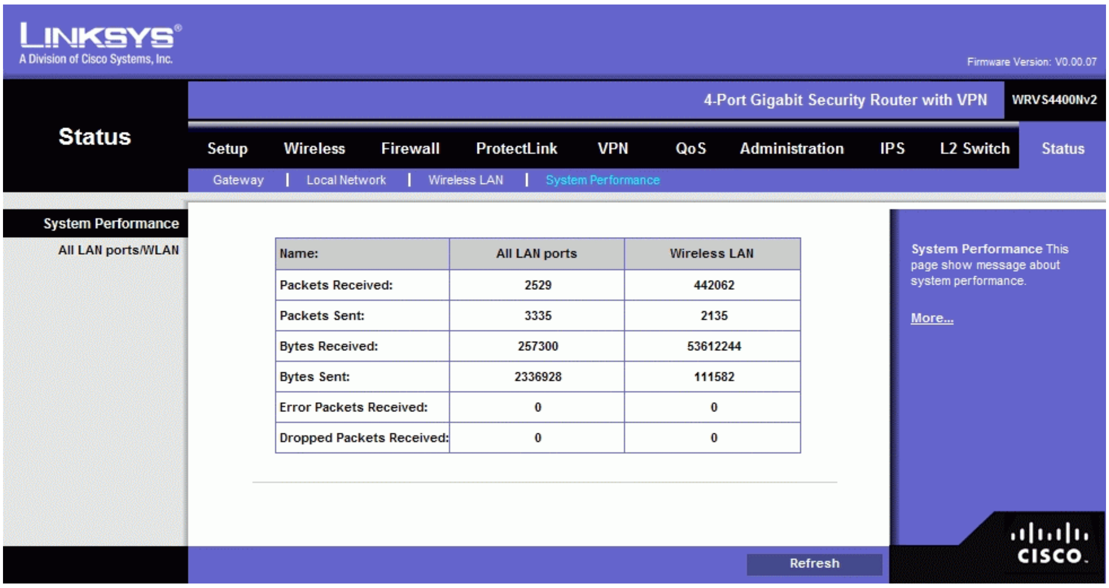
Wireless IP Address:	192.168.1.2
MAC Address:	00:1C:10:F0:00:2C
Network Mode:	B/G/N-Mixed
Wireless SSID:	linksys-n
Channel Bandwidth:	20MHz
Wireless Channel:	6- 2.437 GHz
Security:	Disabled
SSID Broadcast:	Enabled

This screen provides some basic information on the Wireless LAN of this Wireless Router.

Wireless IP Address. The IP address assigned to the wireless interface of this router.
MAC Address. Displays the MAC address on the Wireless LAN interface.
Network Mode. Displays the Wireless network operating mode (e.g. B/G/N-Mixed).
Wireless SSID. Displays the Wireless network name.
Channel Bandwidth. Displays the wireless channel bandwidth setting.
Wireless Channel. Displays the radio channel number used.
Security. Displays the Wireless Security mode.
SSID Broadcast. Displays the setting on SSID Broadcast.

System Performance

This screen provides data packet statistics on the LAN switch and Wireless LAN of the Router.



Name:	All LAN ports	Wireless LAN
Packets Received:	2529	442062
Packets Sent:	3335	2135
Bytes Received:	257300	53612244
Bytes Sent:	2336928	111582
Error Packets Received:	0	0
Dropped Packets Received:	0	0

System Performance This page show message about system performance.

More...

All LAN Ports / WLAN

The All LAN Ports column shows the aggregate traffic statistics from all four LAN ports.

Packets Received. This shows the number of packets received.
Packets Sent. This shows the number of packets sent.
Bytes Received. This shows the number of bytes received.
Bytes Sent. This shows the number of bytes sent.
Error Packets Received. This shows the number of error packets received.
Dropped Packets Received. This shows the number of packets being dropped after they were received.

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. ***I need to set a static IP address on a PC.***
   The Router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.149 using the DHCP server on the Router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.150 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

   ### For Windows 98 and Millennium:

   A. Click **Start**, **Setting**, and **Control Panel**. Double-click **Network**.
   B. In *The following network components are installed* box, select the **TCP/IP**-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.
   C. In the *TCP/IP properties* window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Make sure that each IP address is unique for each PC or network device.
   D. Click the **Gateway** tab, and in the *New Gateway* prompt, enter **192.168.1.1**, which is the default IP address of the Router. Click the **Add** button to accept the entry.
   E. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
   F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the *Network* window.
   G. Restart the computer when asked.

For Windows 2000:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
C. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
D. Enter a unique IP address that is not used by any other computer on the network connected to the

Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.

E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
I. Restart the computer if asked.

For Windows XP: The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

A. Click **Start** and **Control Panel**.
B. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
C. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
D. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
E. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
F. Enter the Subnet Mask, **255.255.255.0**.
G. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
H. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
I. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window. Click the **OK** button in the *Local Area Connection Properties* window.

Wireless-N Gigabit Security Router with VPN

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98 and Millennium:

Refer to Windows Help for details. Make sure **Obtain IP address automatically** is selected in the settings.

For Windows 2000:

1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
2. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
3. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

1. 4. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
2. 5. Restart the computer if asked.
3. 6. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.

4. 7. Restart the computer if asked.

For Windows XP: The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. 1. Click **Start** and **Control Panel**.
2. 2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.

3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
4. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

B. Open a command prompt.

. • For Windows 98 and Millennium, click **Start** and **Run**. In the *Open* field, type **command**. Press the **Enter** key or click the **OK** button.

. • For Windows 2000 and XP, click **Start** and **Run**. In the *Open* field, type **cmd**. Press the **Enter** key or click the **OK** button.

Wireless-N Gigabit Security Router with VPN

C. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.

. • If you get a reply, the computer is communicating with the Router.

. • If you do NOT get a reply, check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

D. In the command prompt, type **ping** followed by your Internet IP address and press the **Enter** key. The Internet IP Address can be found in the web interface of the Router. For example, if your Internet IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.

. • If you get a reply, the computer is connected to the Router.

. • If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E. In the command prompt, type **ping www.linksys.com** and press the **Enter** key.

. • If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

. • If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the Internet with my Internet connection.

A. Refer to “Problem #2, I want to test my Internet connection” to verify that you have connectivity.

B. If you need to register the MAC address of your Ethernet adapter with your ISP, please see “Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter.” If you need to clone the MAC address of your Ethernet adapter onto the Router, see the MAC Address Clone section of “Chapter 6: Setting Up and Configuring the Router” for details.

C. Make sure you are using the right Internet settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Basic Setup section of “Chapter 6: Setting Up and Configuring the Router” for details on Internet Connection Type settings.

D. Make sure you use the right cable. Check to see if the Internet LED is solidly lit.

E. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's Web-based Utility shows a valid IP address from your ISP.
F. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the System Summary tab of the Router's Web-based Utility to see if you get an IP address.

4. ***I am not able to access the Router's Web-based Utility Setup page.***
   A. Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
   B. Refer to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
   C. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."
   D. Refer to "Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

5. ***I can't get my Virtual Private Network (VPN) to work through the Router.***
   Access the Router's web interface by going to **http://192.168.1.1** or the IP address of the Router, and go to the **VPN** => **VPN Pass Through** tab. Make sure you have IPsec passthrough and/or PPTP passthrough enabled.

   VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

   VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

   Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Basic Setup tab of the Web-based Utility. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

   Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

   Check the Linksys website at *www.linksys.com* for more information.

6. ***I need to set up a server behind my Router.***
   To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the

A. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Firewall** => **Single Port Forwarding** tab.

B. Enable one of the pre-defined applications in the Table or you can add or modify existing entries for your application.
C. Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address. Then check the **Enable** checkbox for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

7. ***I need to set up online game hosting or use other Internet applications.***
If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

A. Access the Router's Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Firewall** => **Port Range Forwarding** tab.
B. Enter the Service Application Name, Range of Port used by this Application, and Layer 4 Protocol used by this Application to the Table.
C. Enter the IP Address of the server that you want the Internet users to access. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check

Application	Start and End	Protocol	IP Address	Enabled
UT	7777 to 27900	Both	192.168.1.100	X
Halflife	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

D. Configure as many entries as you like.

When you have completed the configuration, click the **Save Settings** button.

8. ***I can’t get the Internet game, server, or application to work.***
   If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.) Follow these steps to set DMZ hosting:

   A. Access the Router’s Web-based Utility by going to **http://192.168.1.1** or the IP address of the Router. Go to the **Firewall** => **Single Port Forwarding** tab.
   B. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
   C. Go to the **Setup** => **DMZ** tab.
   D. Enter the Ethernet adapter’s IP address of the computer you want exposed to the Internet. This will bypass the NAT security for that computer. Please refer to “Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter” for details on getting an IP address.

   Once completed with the configuration, click the **Save Settings** button.

9. ***I forgot my password, or the password prompt always appears when saving settings to the Router.***
   Reset the Router to factory defaults by pressing the Reset button for ten seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

   A. Access the Router’s web interface by going to **http://192.168.1.1** or the IP address of the Router. Enter the default password admin, and click the **Administration** => **Management** tab.
   B. Enter the old password in the *Old Password* field.
   C. Enter a different password in the *New Password* field, and enter the new password in the *Confirm New Password* field to confirm the password.
   D. Click the **Save Settings** button.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Internet Options**.
B. Click the **Connections** tab.
C. Click the **LAN settings** button and remove anything that is checked.
D. Click the **OK** button to go back to the previous screen.
E. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:

A. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
B. Make sure you have **Direct connection to the Internet** selected on this screen.
C. Close all the windows to finish.

11. To start over, I need to set the Router to factory default.

Hold the Reset button for up to 30 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at *www.linksys.com*. Follow these steps:

Wireless-N Gigabit Security Router with VPN

A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware. Select the Router from the pull-down menu and choose the firmware from the options.
B. Extract the firmware file on your computer.
C. To upgrade the firmware, follow the steps in the Upgrade section found in "Chapter 6: Setting Up and Configuring the Router".

13. The firmware upgrade failed.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware:

A. Use the Linksys TFTP program to upgrade the firmware. Go to the Linksys website at **http://www.linksys.com** and download the TFTP program, which will be listed with the firmware.
B. Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

IP Address: 192.168.1.50
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

C. Perform the upgrade using the TFTP utility.

If the firmware upgrade failed, the Router will still work using its current firmware.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.

B. Enter the password, if asked. (The default password is admin.)

C. On the **Setup** => **WAN** tab, select the option **Keep Alive**, and set the *Redial Period* option at **20** (seconds).

D. Click the **Save Settings** button.

If the connection is lost again, follow steps E and F to re-establish connection.

15. I can't access my email, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.

B. Enter the password, if asked. (The default password is **admin**.)

C. Go to Setup => WAN tab.

D. Look for the MTU option, and select **Enable**. In the *Size* field, enter 1492.

E. Click the **Save Settings** button to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved: 1462 1400 1362 1300

16. I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the Router to open a specific incoming port, depending on which port an Internet application uses. Follow these steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the Router.

B. Enter the password, if asked. (The default password is **admin**.)

C. Click the **Firewall** => **Port Range Triggering** tab.

D. Enter any name you want to use for the Application Name.

E. Enter the Start and End Ports of the Triggered Port Range. Check with your Internet application provider for more information on which outgoing port services it is using.

F. Enter the Start and End Ports of the Forwarded Port Range. Check with your Internet application provider for more information on which incoming port services are required by the Internet application.

Once completed with the configuration, click the **Save Settings** button.

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

. • Check if other PCs work. If they do, ensure that your workstation’s IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.

. • If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

. • If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.

. • Manually configure the TCP/IP with a DNS address provided by your ISP.

. • Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

18. I'm trying to access the Router's Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, "404 Forbidden."

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility's login screen (Netscape Navigator will require similar steps):

A. Click **File**. Make sure *Work Offline* is NOT checked.

B. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.

C. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support?

The Router will support up to 253 IP addresses if the subnetmask is set to 255.255.255.0.

Is IPSec Passthrough supported by the Router?

Yes, enable or disable IPSec Passthrough on the VPN => VPN Pass Through tab.

Where is the Router installed on the network?

In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Does the Router support IPX or AppleTalk?

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to the LAN.

What is Network Address Translation and what is it used for?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Router support any operating system other than Windows 98, Millennium, 2000, or XP?

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 to 27900. If you want to use the UT Server Admin, forward another port (8080 usually works well but is used for remote admin. You may have to disable this.), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get* Half-Life: Team Fortress *to work with the Router?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

How can I block corrupted FTP downloads?
If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?
Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's

If all else fails in the installation, what can I do?
Reset the Router by holding down the Reset button for ten seconds. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

How can I be notified of new Router firmware upgrades?
All Linksys firmware upgrades are posted on the Linksys website at *www.linksys.com*, where they can be downloaded for free. The Router's firmware can be upgraded using the Web-based Utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment?
Yes, but the Router's setup pages are accessible only through Internet Explorer 5.0 or Netscape Navigator 5.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

What is DMZ Hosting?
Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with

a static IP if you want to use DMZ Hosting. To get the LAN IP address, see “Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter.”

If DMZ Hosting is used, does the exposed user share the public IP with the Router?
No.

Does the Router pass PPTP packets or actively route PPTP sessions?
The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded?
Theoretically, the Router can establish 4,000 sessions at the same time, but you can only forward 30 ranges of ports.

Does the Router replace a modem? Is there a cable or DSL modem in the Router?
No, this version of the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router?
The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

What is the maximum number of VPN sessions allowed by the Router?
The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

How can I check whether I have static or DHCP IP addresses?
Ask your ISP to find out.

How do I get mIRC to work with the Router?
Under the **Firewall** => **Single Port Forwarding** tab, set port forwarding to **113** for the PC on which you are using mIRC.

If your questions are not addressed here, refer to the Linksys website, *www.linksys.com*.

Appendix B: Using the Linksys QuickVPN Software for Windows 2000 or XP

Overview

The Linksys Wireless-N Gigabit Security Router with VPN offers a free QuickVPN software program for computers ***vpn** (virtual private network): a security* running Windows 2000 or XP. (Computers running other operating systems will have to use a third-party VPN *measure to protect data as it leaves one* software program.) This guide describes how to install and use the Linksys QuickVPN software.

network and goes to another over the Internet.

Before You Begin ***software**: instructions for the computer.*

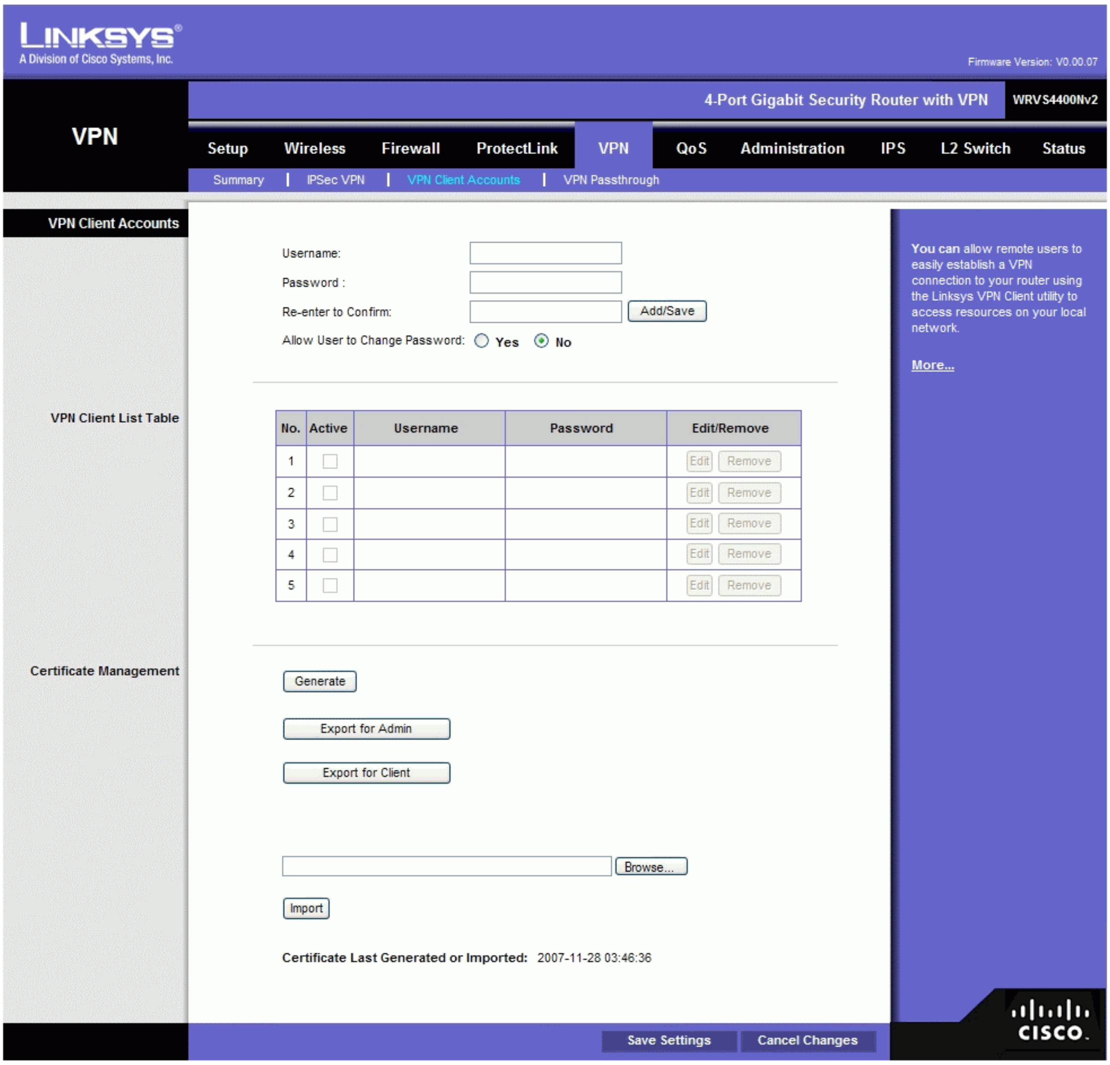
The QuickVPN software program only works with a 4-Port Gigabit Security Router with VPN that is properly configured to accept a QuickVPN connection. Follow these instructions for configuring the VPN client settings for the Router:

1. Click the **VPN** tab.

2. Click the **VPN Client Accounts** tab.

1. 3. Enter the username in the *Username* field.
2. 4. Enter the password in the *Password* field, and enter it again in the *Re-enter to confirm* field.
3. 5. Click the **Add/Save** button.
4. 6. Click the **Active** checkbox for VPN Client No. 1.

Click the **Save Settings** button. **Figure B-1: VPN Client Accounts Screen**


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: V0.00.07
VPN
4-Port Gigabit Security Router with VPN
WRVS4400Nv2
Setup
Wireless
Firewall
ProtectLink
VPN
QoS
Administration
IPS
L2 Switch
Status
Summary | IPSec VPN | VPN Client Accounts | VPN Passthrough
VPN Client Accounts

Username:

Password :

Re-enter to Confirm: Add/Save

Allow User to Change Password: ○ Yes ● No

VPN Client List Table

No.	Active	Username	Password	Edit/Remove
1	□			Edit Remove
2	□			Edit Remove
3	□			Edit Remove
4	□			Edit Remove
5	□			Edit Remove

Certificate Management

Certificate Last Generated or Imported: 2007-11-28 03:46:36

You can allow remote users to easily establish a VPN connection to your router using the Linksys VPN Client utility to access resources on your local network.

Wireless-N Gigabit Security Router with VPN

Installing from the CD-ROM

1. Click Install QuickVPN and follow the on-screen instructions. Downloading and Installing from the Internet

1. Go to *www.linksys.com* and select **Products**.

1. 2. Click **Business Solutions**.
2. 3. Click **Router/VPN Solutions**.
3. 4. Click **RVS4000**.

1. 5. Click **Linksys QuickVPN Utility** in the More Information section.
2. 6. Save the zip file to your PC, and extract the .exe file.
3. 7. Double-click the .exe file, and follow the on-screen instructions. Then proceed to the next

section, “Using the Linksys QuickVPN Software.”

NOTE: You can change your password only if you have been granted that privilege by your system administrator.

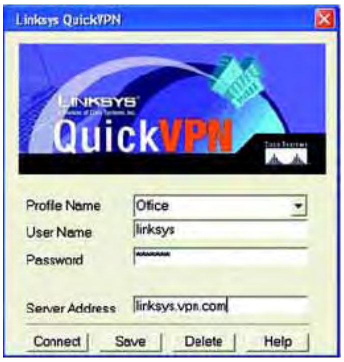
Figure B-2: QuickVPN Figure B-3: QuickVPN Tray Desktop Icon Icon - No Connection

1. 1. Double-click the Linksys QuickVPN software icon on your desktop or in the system tray.
2. 2. The login screen will appear. Enter a name for your profile.

Then enter the User Name and Password you have been assigned.

In the *Server Address* field, enter the IP address or domain name of the Wireless-G VPN Router with RangeBooster. To save this profile, click the **Save** button. Multiple profiles can be set up if you want to establish a tunnel to multiple sites. Note that only one tunnel can be active at a time. To delete this profile, click the **Delete** button. For information, click the **Help** button.

3. To begin your QuickVPN connection, click the **Connect** button and the Connecting, Activating Policy, and Verifying Network screens appear.



Profile Name: Office
User Name: linksys
Password: *******
Server Address: linksys.vpn.com

Activating Policy...

Figure B-6: Activating Policy

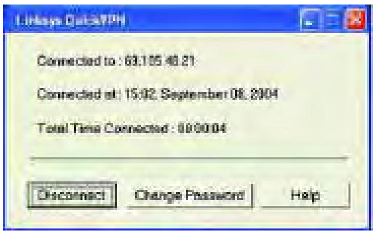
Verifying Network...

Figure B-7: Verifying Network

4. When your QuickVPN connection is established, the status screen will appear, and the QuickVPN tray icon will turn green. It will display the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.

To terminate the VPN tunnel, click the **Disconnect** button. If you want to change your password, click the **Change Password** button. For information, click the **Help** button.

2. 5. If you clicked the Change Password button and have permission to change your own password, you will see the *Connect Virtual Private Connection* screen. Enter your password in the *Old Password* field. Enter your new password in the *New Password* field. Then enter the new password again in the *Confirm New Password* field. Click the **OK** button to save your new password. Click the **Cancel** button to cancel your change. For information, click the **Help** button.



Linksys QuickVPN

Connected to : 63.105.48.21

Connected at : 15:02, September 08, 2004

Total Time Connected : 00:00:04

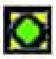


Figure B-9: QuickVPN Tray Icon - Connection

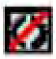
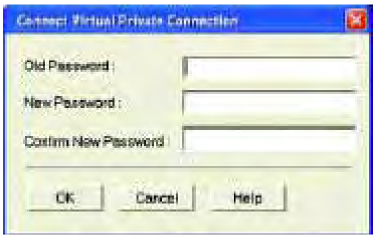


Figure B-10: QuickVPN Tray Icon - No Connection



Connect Virtual Private Connection

Old Password :

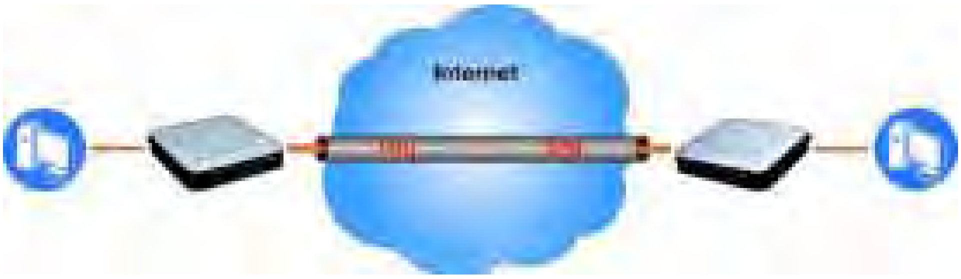
New Password :

Confirm New Password :

Appendix C: Configuring a Gateway-to-Gateway IPSec Tunnel

Overview

This appendix explains how to configure an IPSec VPN tunnel between two VPN Routers by example. Two PCs are used to test the liveliness of the tunnel. You can think of the VPN Router1, Internet, VPN Router2 as a big virtual router that connects PC1 on LAN1 and PC2 on LAN2.



Before You Begin

The following is a list of equipment you need:

. • Two Windows desktop PCs (each PC will be connected to a VPN Router)
. • Two VPN Routers that are both connected to the Internet

Wireless-N Gigabit Security Router with VPN

Configuring VPN Router 1

Follow these instructions for the first VPN Router, designated VPN Router 1. The other VPN Router is designated VPN Router 2.

1. 1. Launch the web browser for a networked PC, designated PC 1.
2. 2. Enter the VPN Router’s local IP address in the *Address* field (default is **192.168.1.1**). Then press **Enter**.
3. 3. A password request page will appear. (Non-Windows XP users will see a similar screen.) Complete the *User Name* and *Password* fields (**admin** is the default user name and password). Then click

the **OK** button.

4. 4. Click the **VPN** tab.

5. 5. Click the **IPSec VPN** tab.

6. 6. For the VPN Tunnel setting, select **Enabled**.

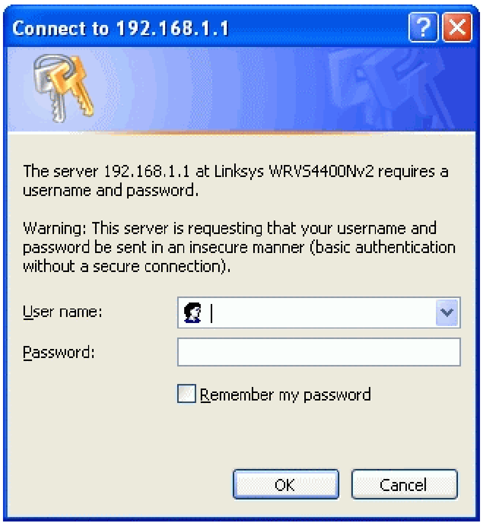
7. 7. Enter a name in the *Tunnel Name* field.

8. 8. For the Local Secure Group, select **Subnet**. Enter VPN Router 1's local network settings in the *IP Address* and *Mask* fields.

9. 9. For the Remote Secure Group, select **Subnet**. Enter VPN Router 2's local network settings in the *IP Address* and *Mask* fields. Note that the subnet of Router 2 must be different than the subnet of Router 1.

10. 10. For the Remote Secure Gateway, select **IP Addr**. Enter VPN Router 2's WAN IP address in the *IP Address* field.

11. 11. Click the **Save Settings** button.



Connect to 192.168.1.1

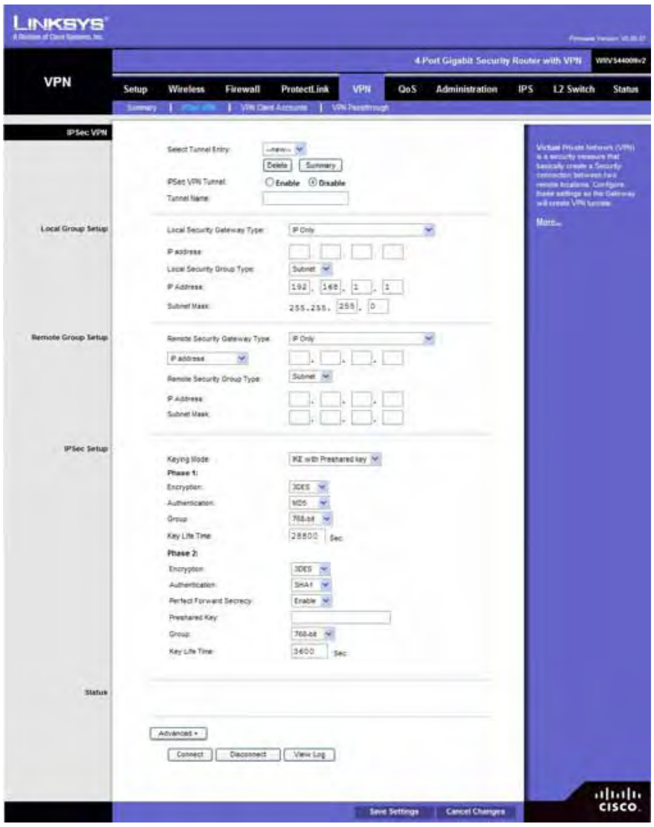
The server 192.168.1.1 at Linksys WRVS4400Nv2 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

□ Remember my password



Virtual Private Network (VPN) is a security measure that basically create a Security connection between two remote locations. Configure these settings so the Gateway will create VPN tunnels.

Select Tunnel Entry: --new--

IPSec VPN Tunnel: ○ Enable ● Disable

Tunnel Name:

Local Group Setup

Local Security Gateway Type: IP Only

IP address: . . .

Local Security Group Type: Subnet

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255. 255 . 0

Remote Group Setup

Remote Security Gateway Type: IP Only

IP address: . . .

Remote Security Group Type: Subnet

IP Address: . . .

Subnet Mask: . . .

IPSec Setup

Keying Mode: IKE with Preshared key

Phase 1:

Encryption: 3DES

Authentication: MD5

Group: 768-bit

Key Life Time: 28800 Sec

Phase 2:

Encryption: 3DES

Authentication: SHA1

Perfect Forward Secrecy: Enable

Preshared Key:

Group: 768-bit

Key Life Time: 3600 Sec

Status

Wireless-N Gigabit Security Router with VPN

1. 1. Launch the web browser for a networked PC, designated PC 2.
2. 2. Enter the VPN Router’s local IP address in the *Address* field (default is **192.168.1.1**). Then press **Enter**.
3. 3. A password request page will appear. (Non-Windows XP users will see a similar screen.) Complete the *User Name* and *Password* fields (**admin** is the default user name and password). Then click the **OK** button.
4. 4. If the LAN IP address is still the default one, change it to 172.168.1.1 and save the setting.
5. 5. Click the **VPN** tab.
6. 6. Click the **IPSec VPN** tab.
7. 7. For the VPN Tunnel setting, select **Enabled**.
8. 8. Enter a name in the *Tunnel Name* field.
9. 9. For the Local Secure Group, select **Subnet**. Enter VPN Router 2’s local network settings in the *IP Address* and *Mask* fields.
10. 10. For the Remote Secure Group, select **Subnet**. Enter VPN Router 1’s local network settings in the *IP Address* and *Mask* fields.
11. 11. For the Remote Secure Gateway, select IP Addr. Enter VPN Router 1’s WAN IP address in the *IP Address* field.
12. 12. Click the **Save Settings** button.

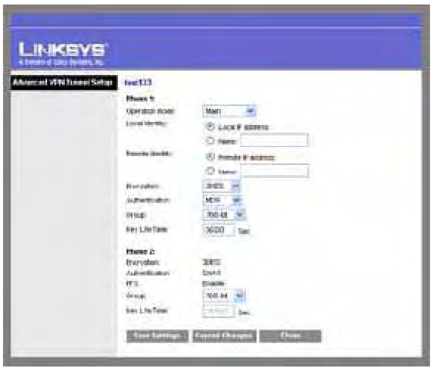
Wireless-N Gigabit Security Router with VPN

Configuring VPN Router 1 Following these instructions for VPN Router 1.

1. 1. On the *IPSec VPN* screen, select **3DES** from the *Encryption* drop-down menu.
2. 2. Select **MD5** from the *Authentication* drop-down menu.

3. 3. Keep the default Key Exchange Method, **Auto(IKE)**.
4. 4. Select **Pre-Shared Key**, and enter a string for this key., e.g. 13572468.
5. 5. For the PFS setting, select **Enabled**.
6. 6. If you need more detailed settings, click the **Advanced Settings** button. Otherwise, click the **Save Settings** button and proceed to the next section, “Configuring VPN Router 2.”
7. 7. On the *Advanced VPN Tunnel Setup* screen, keep the default Operation Mode, **Main**.
8. 8. For Phase 1, select 3**DES** from the *Encryption* drop-down menu.
9. 9. Select **MD5** from the *Authentication* drop-down menu.
10. 10. Select **1024-bit** from the *Group* drop-down menu.

11. Enter **3600** in the *Key Life Time* field. **Figure C-4: Advanced IPsec VPN Tunnel Settings**



Phase 1:
Operation mode: Main
Local Identity: ○ Local IP address ○ Name:
Remote Identity: ○ Remote IP address ○ Name:
Encryption: 3DES
Authentication: MD5
Key Life Time: 3600 Sec.

Phase 2:
Encryption: 3DES
PFS: Enable

1. 12. For Phase 2, the Encryption, Authentication, and PFS settings were set on the *VPN* screen. Select **1024-bit** from the *Group* drop-down menu.
2. 13. Keep the default Key Life Time value, **28800**.
3. 14. Click the **Save Settings** button on the *Advanced VPN Tunnel Setup* screen.
4. 15. Click the **Save Settings** button on the *IPSec VPN* screen.

Configuring PC 1 and PC 2

1. 1. Set PC 1 and PC 2 to be DHCP clients (refer to Windows Help for more information).
2. 2. Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information).

If the computers can ping each other, then you know the VPN tunnel is configured correctly. You can select different algorithms for the encryption, authentication, and other key management settings for VPN Routers 1 and
2. Refer to the previous section, “Configuring the Key Management Settings,” for details.

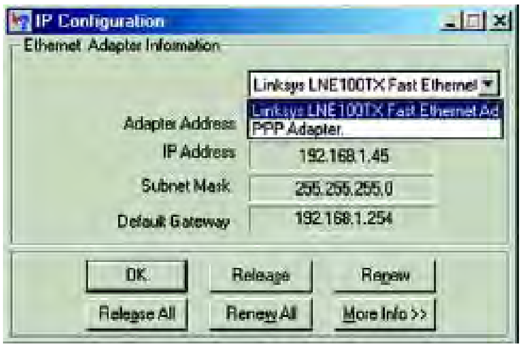
Congratulations! You have successfully configured a VPN tunnel between two VPN Routers.

Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC address cloning feature of the Router. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Router's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. 1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. 2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Router via a CAT 5 Ethernet network cable. See Figure D-1.
3. 3. Write down the Adapter Address as shown on your computer screen (see Figure D-2). This is the MAC address for your Ethernet adapter and is shown as a series of numbers and letters.



IP Configuration

Ethernet Adapter Information

Linksys LNE100TX Fast Ethernet

Adapter Address: Linksys LNE100TX Fast Ethernet Ad / PPP Adapter

IP Address: 192.168.1.45

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

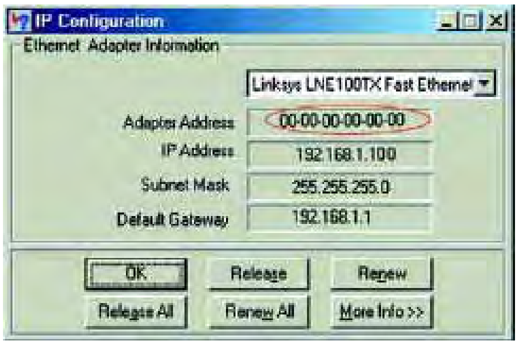
The MAC address/Adapter Address is what you will use for MAC address cloning or MAC

The example in Figure D-2 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may
show something different.

NOTE: The MAC address is also called the Adapter Address.

Windows 2000 or XP Instructions

1. 1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.
2. 2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
3. 3. Write down the Physical Address as shown on your computer screen (Figure D-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

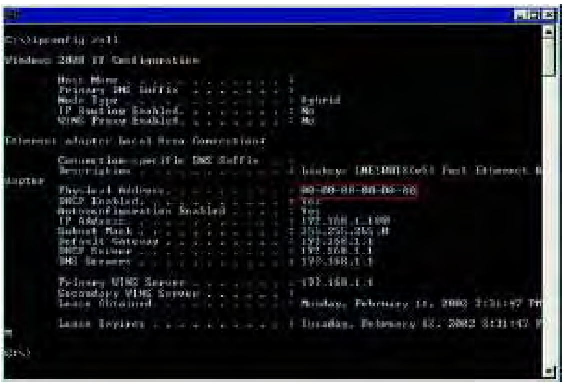


Adapter Address: 00-00-00-00-00-00
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.

NOTE: The MAC address is also called the Physical Address.

The example in Figure D-3 shows the Ethernet adapter’s IP address as 192.168.1.100. Your computer may show something different.

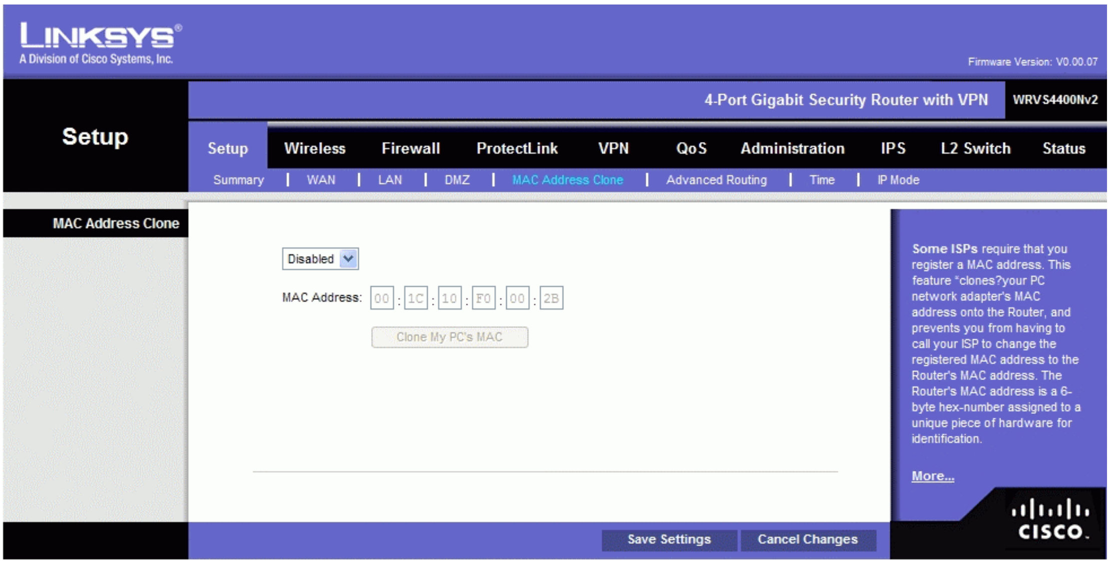


```
C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . :
        Primary DNS Suffix  . . . . . . :
        Node Type . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . : No
        WINS Proxy Enabled. . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
        Physical Address. . . . . . . . . : 00-00-00-00-00-00
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1

        Primary WINS Server . . . . . . . : 192.168.1.1
        Secondary WINS Server . . . . . . :
        Lease Obtained. . . . . . . . . . : Monday, February 11, 2002 3:31:47 PM

        Lease Expires . . . . . . . . . . : Tuesday, February 12, 2002 3:31:47 P
M

C:\>
```

For the Router’s Web-based Utility

For MAC address cloning, enter the MAC Address in the MAC Address field or select **Clone My PCs MAC**. See Figure D-4.

Click **Save Settings** to save the MAC Cloning settings or click the **Cancel Changes** button to undo your changes.



Disabled

MAC Address: 00 : 1C : 10 : F0 : 00 : 2B

Some ISPs require that you register a MAC address. This feature "clones?your PC network adapter's MAC address onto the Router, and prevents you from having to call your ISP to change the registered MAC address to the Router's MAC address. The Router's MAC address is a 6-byte hex-number assigned to a unique piece of hardware for identification.

Wireless-N Gigabit Security Router with VPN

Appendix E: 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.

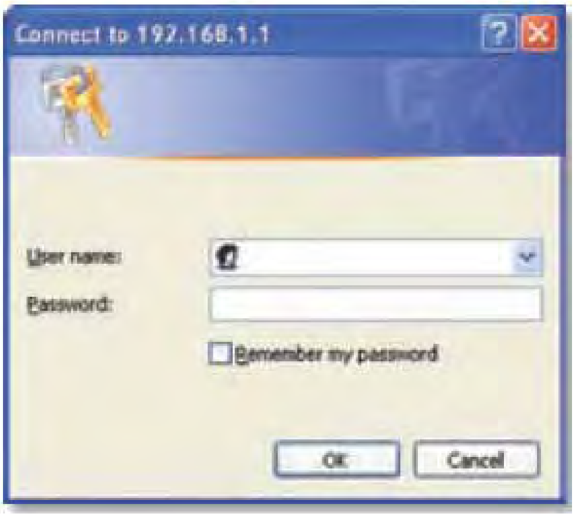
How to Access the Web-Based Utility

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 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.

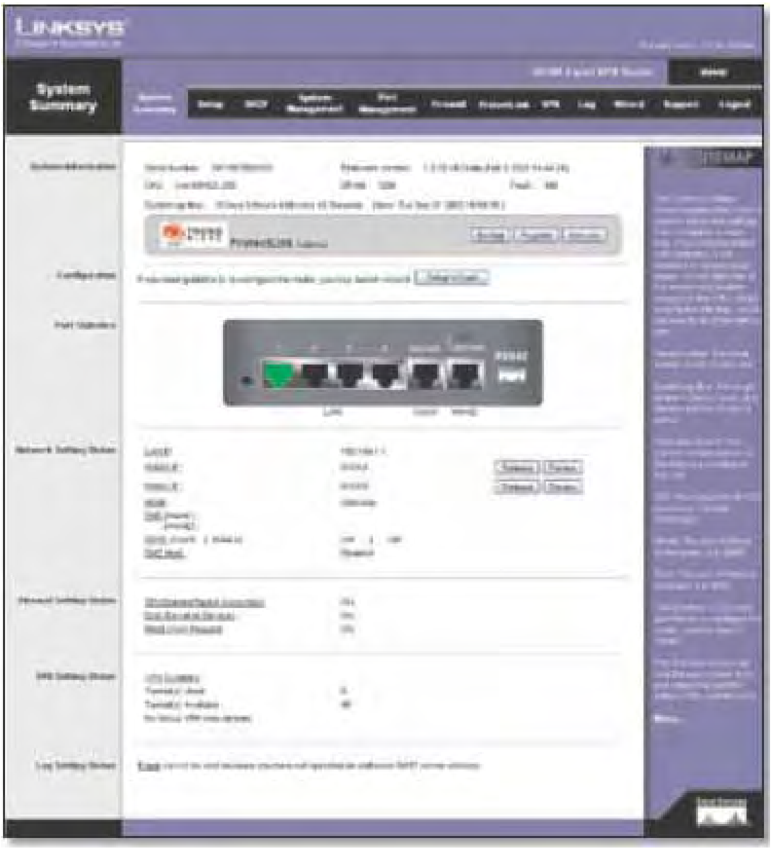
2. A login screen prompts you for your User name and Password. Enter **admin** in the User name field, and enter **admin** in the Password field. (You can change the Password on the Setup > Password screen.) Then click **OK**.



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



System Summary (ProtectLink Available)

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.

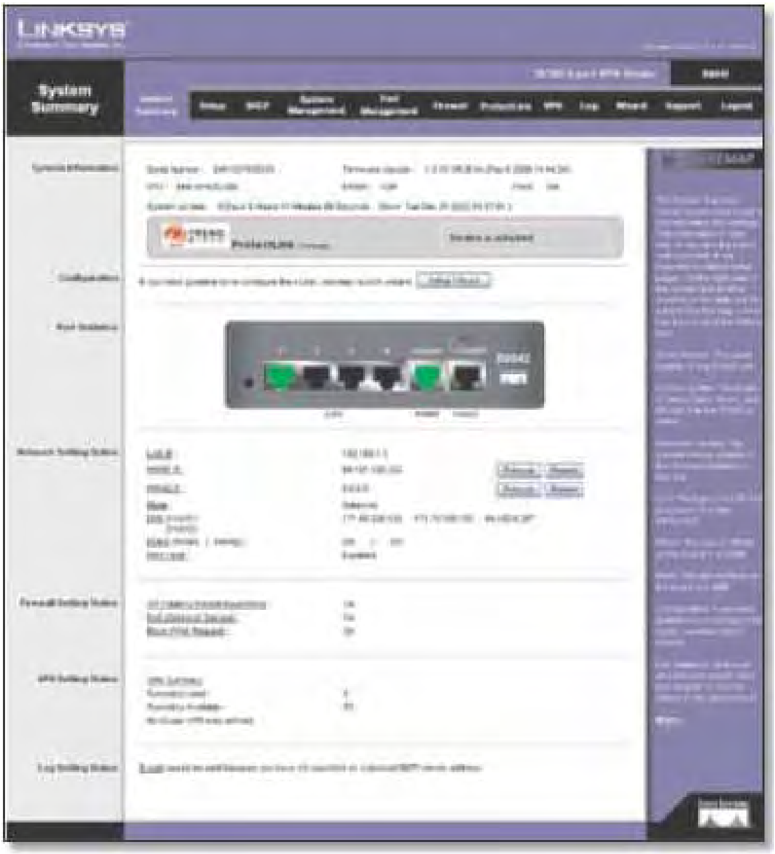
Go buy To purchase a license to use this service, click Go buy. You will be redirected to a list of Linksys resellers on the Linksys website. Then follow the on-screen instructions.

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.

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.

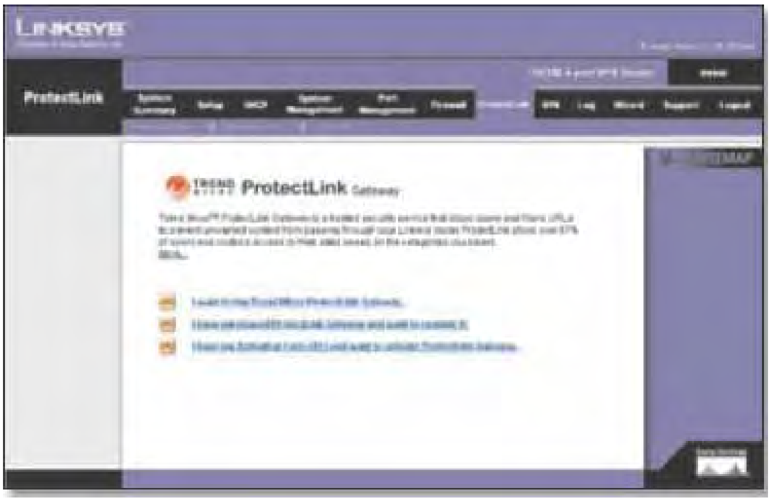


System Summary (ProtectLink Activated)

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.



ProtectLink

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 M cro 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 Act vat on 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.

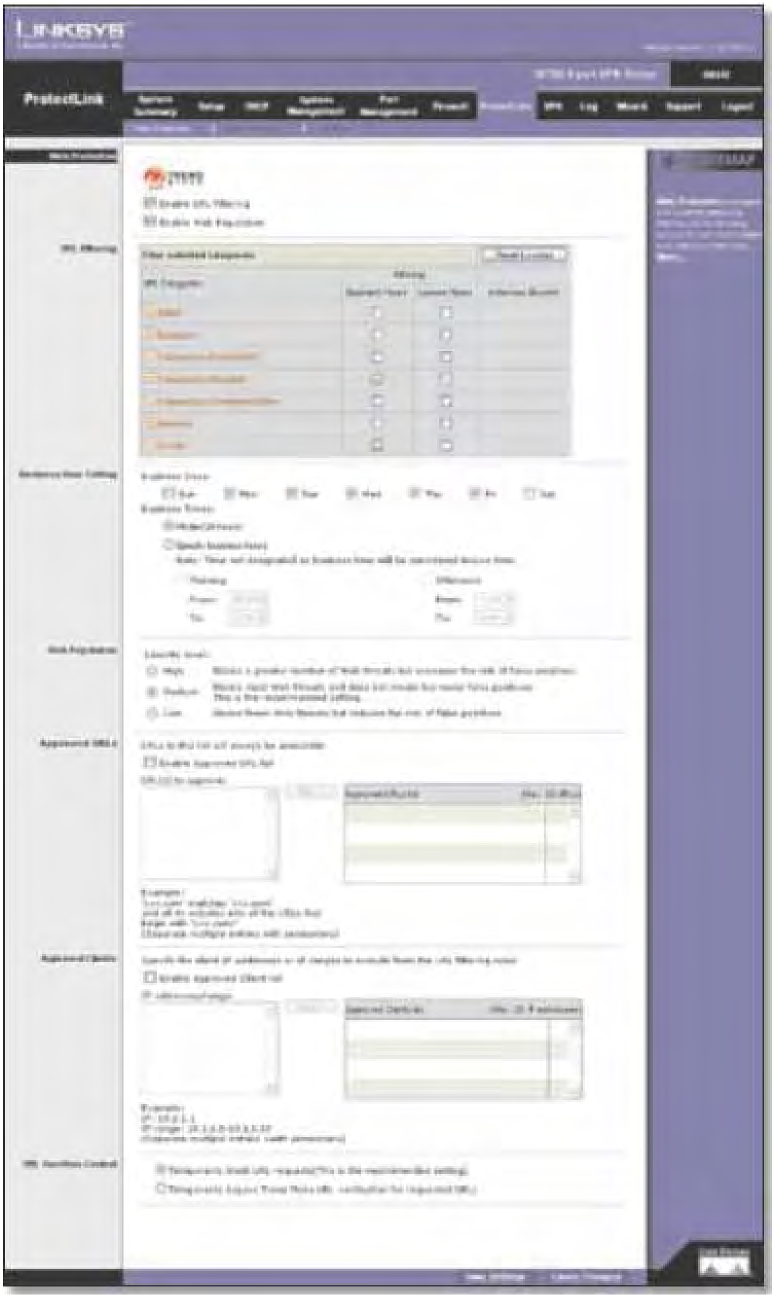
NOTE: If you replace the Router with a new router that supports this service, click I have my Act vat on Code (AC) and want to activate ProtectLink Gateway. Then use your current activation code to transfer your license for the ProtectLiink service to the new router.

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.



ProtectLink>Web Protection

Web Protection

Enable URL Filtering To filter website addresses (URLs), select this option.
Enable Web Reputat on 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:
Bus ness Hours To filter this URL category during the business hours you have specified, select this option.
Le sure 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 Fr.
Business Times To specify entire days, keep the default, All day (4 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 email messages will be checked online before appropriate messages are forwarded to your network.

ProtectLink>Email Protection

Email Protection

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.

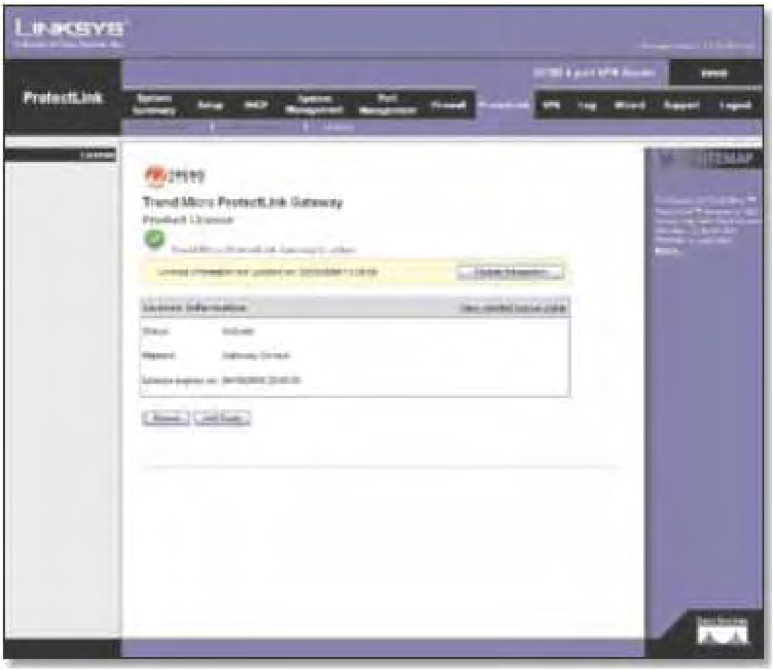
https://us. mhs.trendmicro.com/linksys To set up e-mail protection, click this link. You will be redirected to the Trend Micro ProtectLink Gateway website. Then follow the on-screen instructions.

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.



ProtectLink>License

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 F: Glossary

Adapter - A device that adds network functionality to your PC.

AES (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

Backbone - The part of a network that connects most of the systems and networks together, and handles the

most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the

World Wide Web.

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the

Internet.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**Dem**ilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access.

Many specific authentication methods work within this framework.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords. **EAP-TLS** (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - A networking protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World

Wide Web.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a username

and password system.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking
device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet. **Network** - A series of computers or devices connected for the purpose of data sharing, storage, and/or

transmission between users.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

Packet - A unit of data sent over a network.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is

online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and

power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides

authentication

(username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe. **RADIUS** (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control

network access.

RJ-45 (**R**egistered **J**ack-**45**) - An Ethernet connector that holds up to eight wires.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold

setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications,

and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices. **SPI** (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of

devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an

electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of

instructions PCs use to communicate over
a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.
TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (**U**ser **D**atagram **P**rotocol) - A network protocol for transmitting data that does not require

acknowledgement

from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

Appendix G: Specifications

Model	WRVS4400Nv2
Standards	IEEE802.11n draft, 802.11g, 802.11b, 802.3u, 802.1X
Ports	10/100/1000 Base-T Ethernet, 12VDC Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, Diag, IPS (Blinks RED - Internal attack, Blinks Green - external attack), Wireless, LAN 1-4, Internet
Wireless	
Radio Transmit Power	19dBm for 802.11b, 16dBm for 802.11g and 802.11n
Wireless Securities	WEP, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise

Antenna	3 external 1.8dBi omni-directional antennas, 2x3 MIMO diversity
Performance	
NAT Throughput	800 Mb/s
Setup/Config	
WebUI	Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
Management	
SNMP Version	SNMP Version 1, 2c

Wireless-N Gigabit Security Router with VPN

Event Logging	Event Logging: Local, Syslog, E-mail Alerts
Web F/W upgrade	Firmware Upgradable Through Web-Browser
Diagnostics	DIAG LED for Flash and RAM failure; Ping Test for network diagnostics
Security	
VPN	5 QuickVPN Tunnels for remote client access 5 IPSec Gateway-to-Gateway Tunnels for branch office connectivity 3DES Encryption MD5/SHA1 Authentication IPSec NAT-T VPN Passthrough of PPTP, L2TP, IPSec
Access Control	IP-based ACL, Internet Access Policy Control
Firewall	SPI stateful packet inspection firewall
Content Filtering	URL blocking, keyword blocking
IPS (Intrusion Prevention System)	IP Sweep Detection, Application Anomaly Detection (HTTP, FTP, Telnet, RCP), P2P Control, Instant Messenger Control, L3-L4 Protocol (IP, TCP, UDP, ICMP) Normalization, L7 Signature Matching
Signature Update	Manual download from the web (Free download for 1 year)
Secure Management	HTTPS, Username/Password

802.1x	Port-based Radius Authentication (EAP-MD5, EAP-PEAP)
NAT	PAT, NAPT, ALG support, NAT Traversal
QoS	
Prioritization types	Port-based and Application-based Priority

Queues	4 queues
Network	
VLAN Support	Port-based VLAN
DHCP	DHCP Server, DHCP Client, DHCP Relay Agent
DNS	DNS Relay, Dynamic DNS (DynDNS, TZO)
DMZ	Any host IP address on LAN side
Routing	Static and RIP v1,v2
Environmental	
Device Dimensions (W x H x D)	7.8 x 5.16 x 7.8 inches 198 x 131 x 198 mm
Weight	0.99 lbs (0.45kg)
Power	12V 1A
Certification	FCC class B, CE, ICES-003
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix H: Warranty Information

LIMITED WARRANTY

Linksys warrants to You that, for a period of three years (the “Warranty Period”), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY 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 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 warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

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 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.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix I: 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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment
should be installed and operated with minimum distance 20cm between the radiator and your body.

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

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.

Industry Canada (Canada)

This device complies with Canadian ICES-003 and RSS210 rules. Cet appareil est conforme aux normes NMB-003 et
RSS210 d'Industrie Canada.

IC Statement

Operation is subject to the following two conditions:

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

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

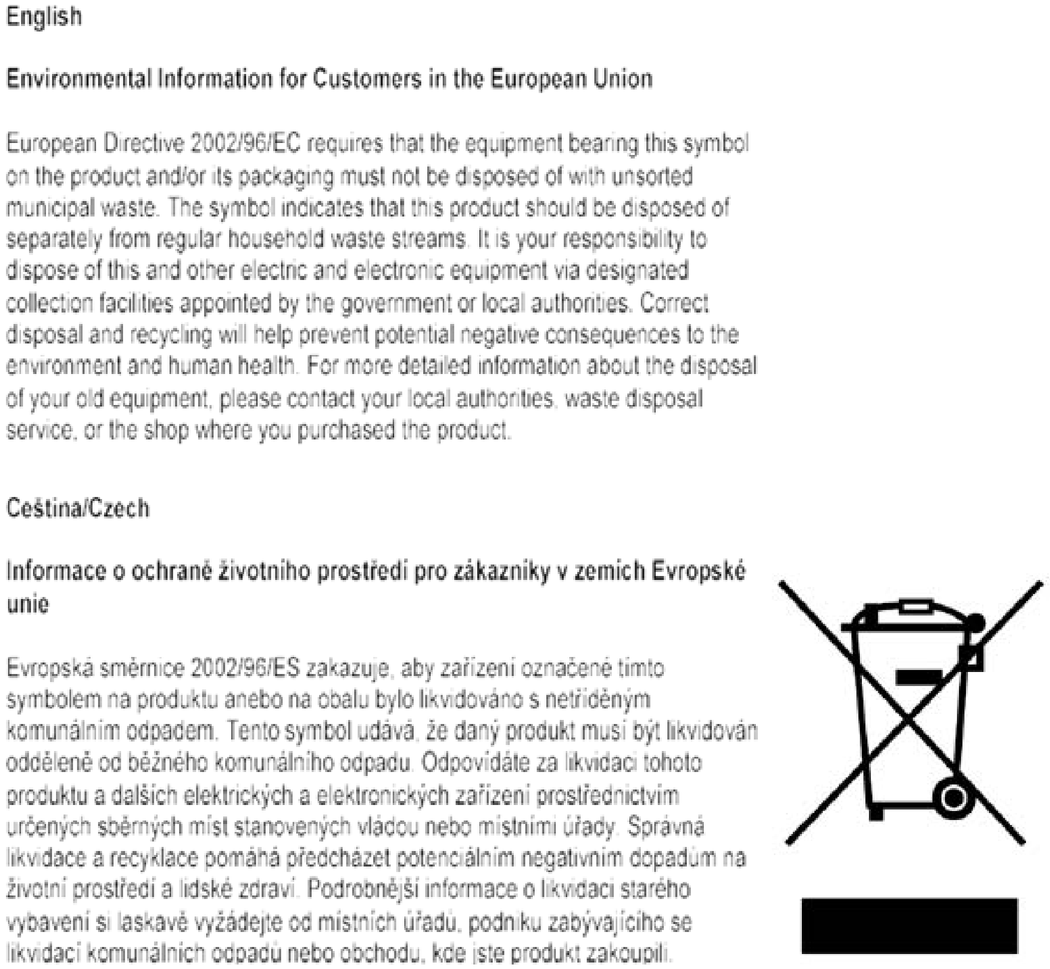
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation

operation of the device.

Le fonctionnement est soumis aux conditions suivantes :
1.	1.	Ce périphérique ne doit pas causer d'interférences;
2.	2.	Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

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

This document contains important information for users with regards to the proper disposal and recycling of 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.

Čeština/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

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish

Información medioambiental para clientes de la Unión Europea

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

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

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

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 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 ed 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/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőredszereken keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

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 op het product of de verpakking, niet 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 en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi 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. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą 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.

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 eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão 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.

Slovenčina/Slovak

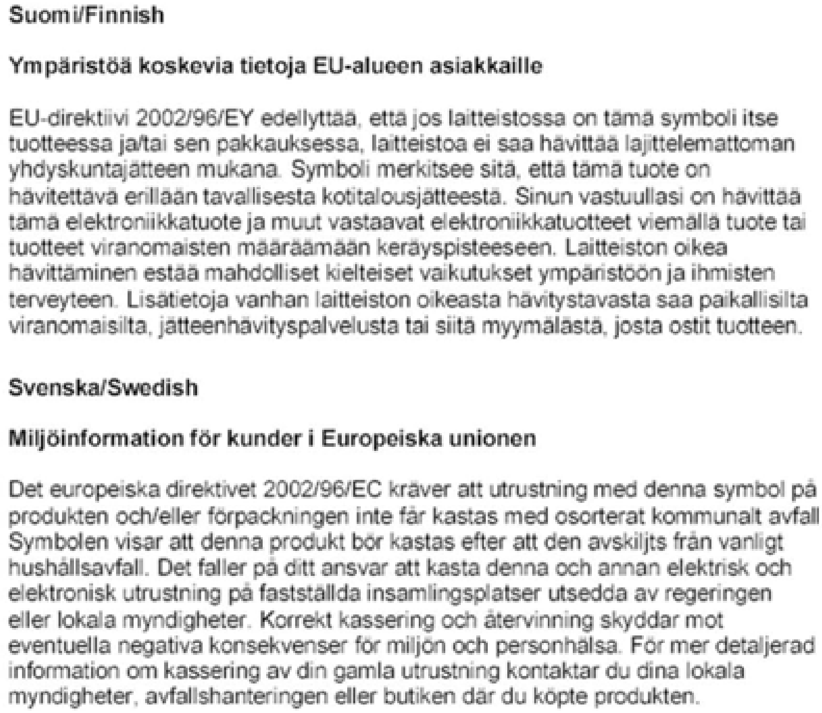
Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.



Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

Appendix J: Contact Information

Need to contact Linksys?
Visit us online for information on the latest products and updates
to your existing products at:

Can't find information about a product you want to buy
on the web? Do you want to know more about networking
with Linksys products? Give our advice line a call at:
Or fax your request in to:

If you experience problems with any Linksys product,
you can call us at:
Don't wish to call? You can e-mail us at:

If any Linksys product proves defective during its warranty period,
you can call the Linksys Return Merchandise Authorization
department for obtaining a Return Authorization Number at:
(Details on Warranty and RMA issues can be found in the Warranty
Information section in this Guide.)

http://www.linksys.com or ftp.linksys.com

800-546-5797 (LINKSYS) 949-823-3002

800-326-7114 support@linksys.com

949-823-3000