ADMINISTRATION GUIDE

Cisco Small Business

RVS4000 4-Port Gigabit Security Router with VPN

1

Introduction

Thank you for choosing the Cisco RVS4000 4-Port Gigabit Security Router with VPN. The 4-Port Gigabit Security Router with VPN is an advanced Internet-sharing network solution for your small business needs. Like any router, it lets multiple computers in your office share an Internet connection.

The 4-Port Gigabit Security Router with VPN also features a built-in 4-Port full-duplex 10/100/1000 Ethernet switch to connect four PCs directly, or you can connect more hubs and switches to create as big a network as you need.

The Virtual Private Network (VPN) capability creates encrypted “tunnels” through the Internet, allowing up to 5 remote offices and 5 traveling users to securely connect into your office network from off-site. Users connecting through a VPN tunnel are attached to your company’s network — with secure access to files, email, and your intranet — just as if they were in the building. You can also use the VPN capability to allow users on your small office network to securely connect out to a corporate network. The QoS features provide consistent voice and video quality throughout your business.

The 4-Port Gigabit Security Router with VPN can serve as a DHCP Server, and has a powerful SPI firewall and Intrusion Prevention System (IPS) to protect your PCs against intruders and most known Internet attacks. You can configure the router to filter internal users’ access to the Internet, and has IP and MAC address filtering so you can specify exactly who has access to your network. Configuration is a snap with the web browser-based configuration utility.

This administration guide will give you all the information you need to connect, set up, and configure your router.

2

Networking and Security Basics

This chapter describes networking and security basics. It includes these sections:

An Introduction to LANs

A router is a network device that connects two networks together.

The router connects your local area network (LAN), or the group of PCs in your home or office, to the Internet. The router processes and regulates the data that travels between these two networks.

The router's Network Address Translation (NAT) technology protects your network of PCs so users on the Internet cannot "see" your PCs. This feature keeps your LAN remains private. The router protects your network by inspecting the first packet received through the Internet port before delivering it to the final destination on one of the Ethernet ports. The router inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

The Use of IP Addresses

IP stands for Internet Protocol. Every device in an IP-based network, including PCs, print servers, and routers, requires an IP address to identify its location, or address, on the network. This applies to both the Internet and LAN connections.

There are two ways of assigning IP addresses to your network devices.

A static IP address is a fixed IP address that you assign manually to a PC or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses are commonly used with network devices such as server PCs or print servers.

If you use the router to share your cable or DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the router. You can get the information from your ISP.

A dynamic IP address is automatically assigned to a device on the network. These IP addresses are called dynamic because they are only temporarily assigned to the PC or other device. After a certain time period, they expire and may change. If a PC logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will assign it a new dynamic IP address.

A DHCP server can either be a designated PC on the network or another network device, such as the router. By default, the router's Internet Connection Type is **Obtain an IP automatically** (DHCP).

The PC or network device that obtains an IP address is called the DHCP client. DHCP frees you from the requirement to assign an IP address manually when a new user is added to your network.

For DSL users, many ISPs may require you to log on with a user name and password to gain access to the Internet. This is a dedicated, high-speed connection type called Point to Point Protocol over Ethernet (PPPoE). PPPoE is similar to a dial-up connection, but PPPoE does not dial a phone number when establishing a connection. It also will provide the router with a dynamic IP address to establish a connection to the Internet.

By default, a DHCP server (on the LAN side) is enabled on the router. If you already have a DHCP server on your network, you MUST disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the router, see the Basic Setup section in **Chapter 5, "Setting Up and Configuring the Router."**

NOTE Since the router is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this Administration Guide, you'll see references to the "Internet IP address" and the "LAN IP address".

Since the router uses NAT technology, the only IP address that can be seen from the Internet for your network is the router's Internet IP address. However, even this Internet IP address can be blocked so the router and network seem invisible to the Internet.

The Intrusion Prevention System (IPS)

IPS is an advanced technology to protect your network from malicious attacks. IPS works together with your SPI Firewall, IP Based Access Control List (ACL), Network Address Port Translation (NAPT), and Virtual Private Network (VPN) to achieve the highest level of security. IPS works by providing real-time detection and prevention as an in-line module in a router.

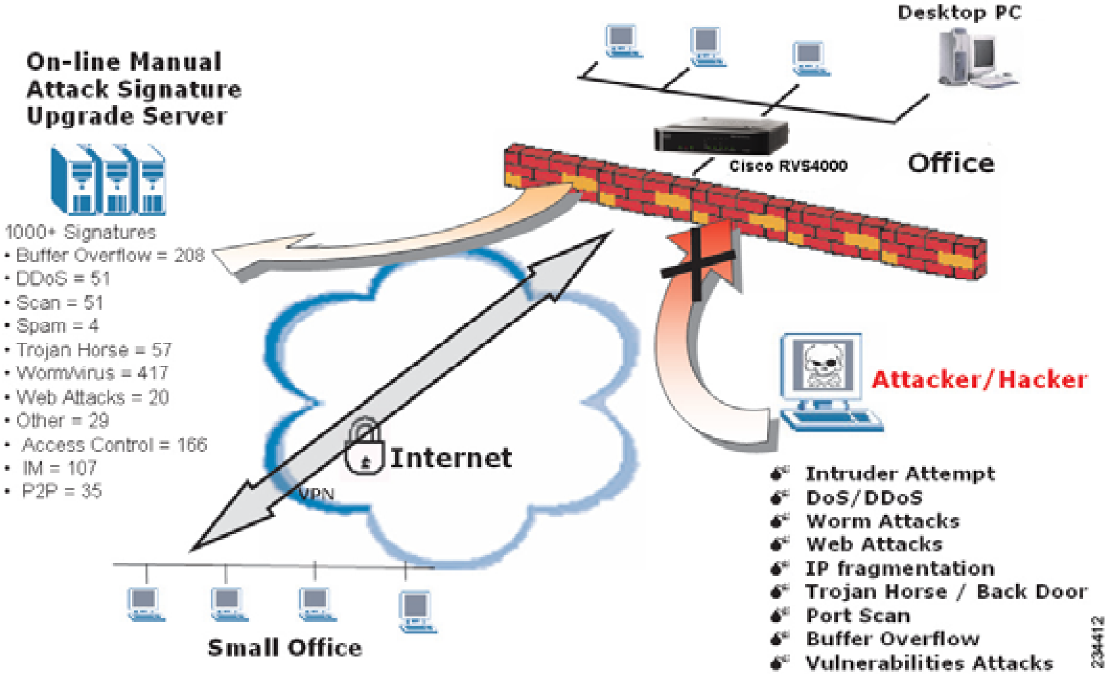
The RVS4000 has hardware-based acceleration for real-time pattern matching to detect malicious attacks. It actively filters and drops malicious TCP/UDP/ICMP/IGMP packets and can reset TCP connections. This feature prevents network worm attacks against client PCs and servers with various operating systems including Windows, Linux, and Solaris. However, this system does not prevent viruses contained in email attachments.

The P2P (Peer-to-Peer) and IM (Instant Messaging) control allows the system administrator to prevent network users from using those protocols to communicate with people over the Internet. This helps the administrators to set up company policies on how to use the Internet bandwidth wisely.

The signature file is the heart of the IPS system. It is similar to the Virus definition file on your PC's Anti-Virus software. IPS uses this file to match against packets coming into the router and performs actions accordingly. The RVS4000 has a signature file that contains 1000+ rules, which cover these categories: DDoS, Buffer Overflow, Access Control, Scan, Trojan Horse, Misc., P2P, IM, Virus, Worm, and Web Attacks.

Customers are encouraged to update their IPS signature file regularly to prevent any new types of attacks on the Internet.

IPS Scenarios



3

Planning Your Virtual Private Network (VPN)

This chapter provides information for planning your VPN. It includes these sections:

Why do I need a VPN?

Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security. Firewalls address this risk. Firewalls help to protect data inside of a local network. But what do you do when information leaves your local network, when emails go to their destination, or when you connect to your company's network from a hotel or remote office? How is your data protected?

A VPN can help. VPNs are called Virtual Private Networks because they secure data moving outside of your network as if it were still within that network.

When data travels across the Internet from your computer, it is always open to attacks. You may already have a firewall, which helps protect data in your network from being corrupted or intercepted by entities outside of your network. When data moves outside of your network—when you send data to someone via email or communicate with an individual over the Internet—the firewall no longer protects your data.

At this point, your data becomes open to hackers who use a variety of methods to steal not only the data you transmit but also your network login and security data. Some of the most common methods are described in on the next page.

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

Hackers use data “sniffing” to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the middle attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a “man in the middle” attack. Hackers use this attack when data is transmitted from one network to another, by rerouting the data to a new destination. Even though the data never reaches its intended recipient, it appears successful to the person who sent the data.

These are only a few of the methods hackers use, and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet often passes through many different servers around the world before reaching its final destination. That’s a long way to go for unsecured data and this is when a VPN serves its purpose.

What is a VPN?

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

This is done by creating a “tunnel”. A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques—IPSec, short for IP Security—VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. You can use VPN to create a secure network that links a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN router by using any computer with the Cisco QuickVPN Client software).

There are two basic ways to create a VPN connection:

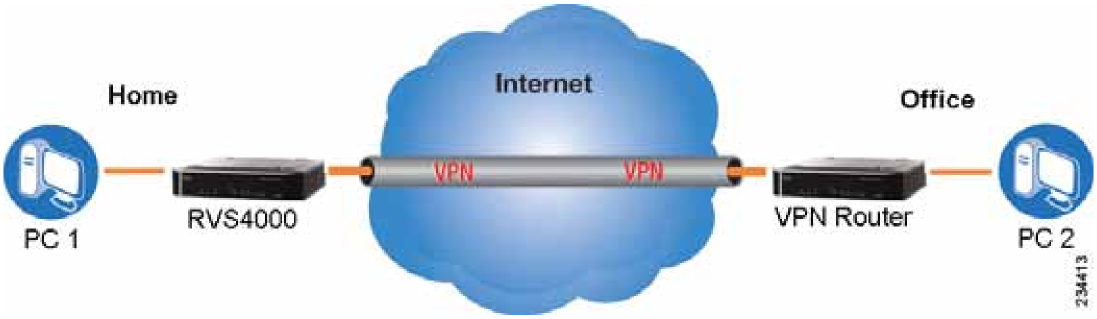
- VPN router to VPN router
- Computer (using the Cisco QuickVPN Client software) to VPN router

The VPN router creates a “tunnel” or channel between two endpoints, so that data transmissions between them are secure. A computer with the Cisco QuickVPN Client software can be one of the two endpoints (refer to **Appendix B, “Using Cisco QuickVPN for Windows 2000, XP, or Vista”**). If you choose not to run the VPN client software, any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN router to create a VPN tunnel by using IPSec (refer to **Appendix C, “Configuring IPSec with a Windows 2000 or XP Computer”**). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

VPN Router to VPN Router

With a VPN-router-to-VPN-router VPN, a telecommuter uses his VPN router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. While using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected. For more information, refer to **Appendix D, "Gateway-to-Gateway VPN Tunnel."**

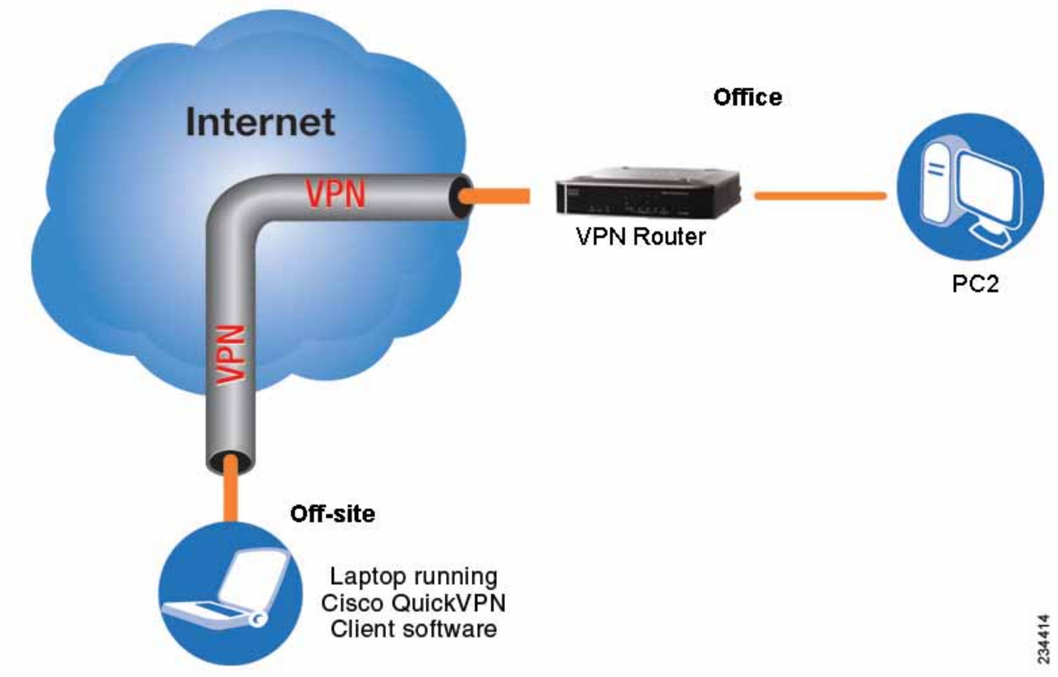
VPN Router to VPN Router



Computer (using the Cisco QuickVPN Client software) to VPN Router

In this illustration, you see an example of a computer-to-VPN router VPN. In her hotel room, a traveling businesswoman connects to her ISP. Her notebook computer has the Cisco QuickVPN Client software, which is configured with her office's IP address. She accesses the Cisco QuickVPN Client software and connects to the VPN router at the central office. As VPNs utilize the Internet, distance is not a factor. While using the VPN, she now has a secure connection to the central office's network, as if she were physically connected.

Computer to VPN Router



For additional information and instructions about creating your own VPN, please visit www.cisco.com. You can also refer to **Appendix B, "Using Cisco QuickVPN for Windows 2000, XP, or Vista"**, **Appendix C, "Configuring IPSec with a Windows 2000 or XP Computer"** and **Appendix D, "Gateway-to-Gateway VPN Tunnel."**

4

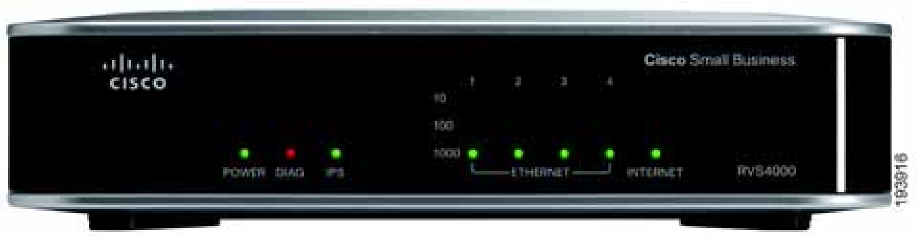
Getting Started with the RVS4000 Router

This chapter describes the physical features of the RVS4000 router and explains how to install the router. It includes these sections:

Front Panel

The LEDs are located on the front panel of the router.

Front Panel



🟢 **POWER LED**: Steady green when the router is powered on. Flashes when the router is running a diagnostic test.

🔴 **DIAG LED**: Unlit when the system is ready. Flashes red during firmware upgrades.

IPS LED: Steady green when the Intrusion Prevention System (IPS) function is enabled. Unlit when IPS functions are disabled. Flashes green when an external attack is detected. Flashes red when an internal attack is detected.

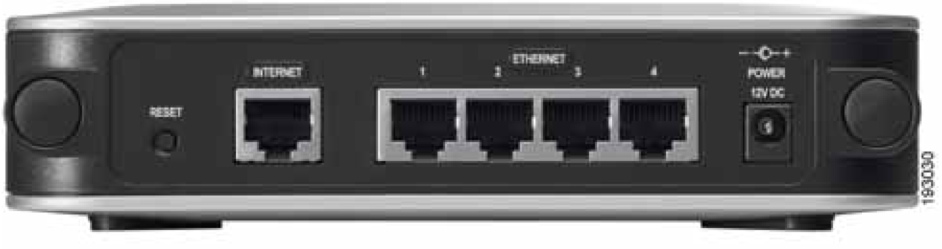
Ethernet Port LEDs 1-4: For each LAN port, there are three LEDs. Steady green when the router is connected to a device at the speed indicated through the corresponding port (1, 2, 3, or 4). Flashes green when a router is actively sending or receiving data on the port.

INTERNET LED: Steady green to indicate the line speed of the device attached to the Internet port. Flashes to indicates activity. If the router is connected to a cable or DSL modem, typically the 100 LED is the only LED lit up, indicating 100 Mbps.

Back Panel

The Ethernet ports, Internet port, Reset button, and Power port are on the back panel of the router.

Back Panel



RESET Button: You can use the Reset button in two ways:

- If the router has problems connecting to the Internet, press the Reset button for just a second with a paper clip or a pencil tip. This is similar to pressing the reset button on your PC to reboot it.
- If you experience extreme problems with the router and have tried all other troubleshooting measures, press and hold the Reset button for 10 seconds. This action restores the factory defaults and clear all of the router settings, such as port forwarding or a new password.

INTERNET Port: Provides a WAN connection to a cable modem or DSL modem.

ETHERNET Ports 1-4: Provide a LAN connection to network devices, such as PCs, print servers, or additional switches.

POWER Port: Connects the router to power via the supplied AC power adapter.

Placement Options

You can place the router horizontally on the rubber feet, mount it in the stand, or mount it on the wall.

Desktop Option

For desktop placement, place the Cisco RVS4000 router horizontally on a surface so it sits on its four rubber feet.

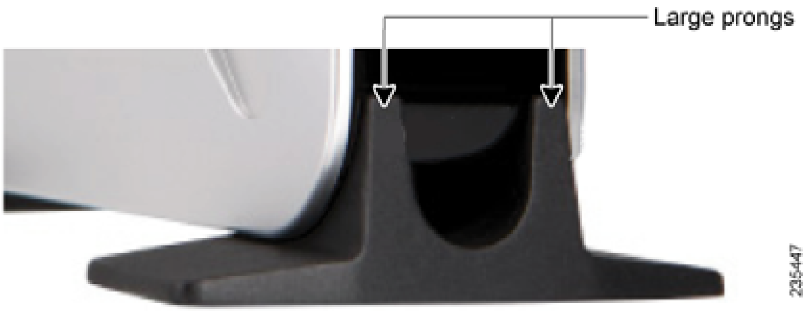
Stand Option

To install the router vertically in the supplied stands, follow the steps below.

To place the router vertically, follow these steps.

STEP 1 Locate the left side panel of the router.

STEP 2 With the two large prongs of one of the stands facing outward, insert the short prongs into the little slots in the router and push the stand upward until the stand snaps into place.



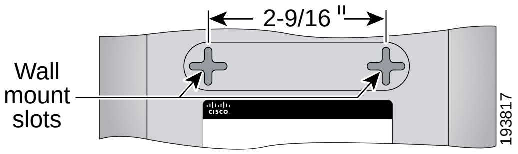
STEP 3 Repeat step 2 with the other stand.

Wall Option

To mount the Cisco RVS4000 router on the wall, follow these steps.

STEP 1 Determine where you want to mount the router and install two screws (not supplied) that are 2-9/16 in. apart (approximately 64.5 mm).

STEP 2 With the back panel pointing up (if installing vertically), line up the router so that the wall-mount crisscross slots on the bottom of the access point line up with the two screws.



STEP 3 Place the wall-mount slots over the screws and slide the router down until the screws fit snugly into the wall-mount slots.

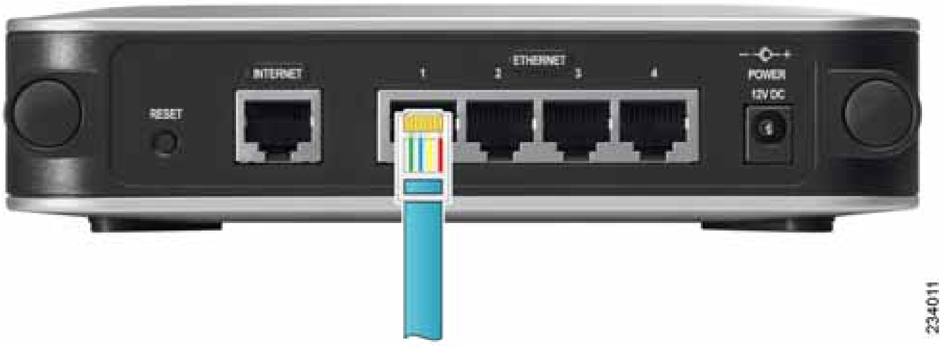
Installing the Router

To prepare the router for installation complete these tasks:

- Obtain the setup information for your specific type of Internet connection from your Internet Service Provider (ISP).
- Power off all of your network hardware, including the router, PCs, and cable modem or DSL modem.

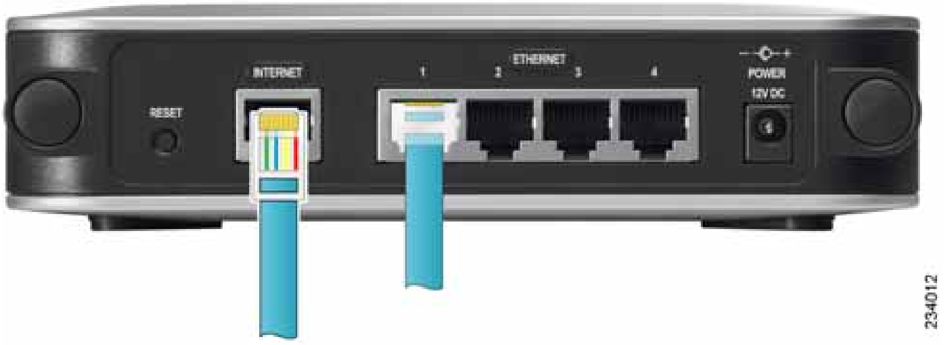
Perform the steps in this section to install the hardware.

STEP 1 Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the router. Connect the other end to an Ethernet port on a PC.



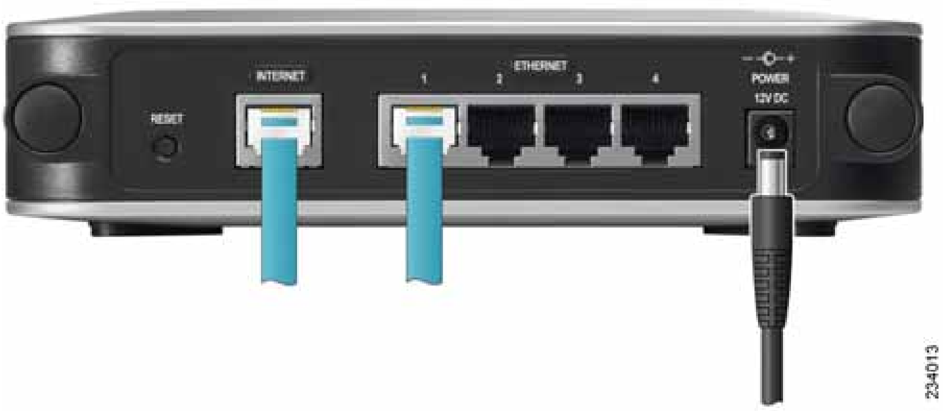
STEP 2 Repeat step 1 to connect up to four PCs, switches, or other network devices to the router.

STEP 3 Connect an Ethernet network cable from your cable modem or DSL modem to the Internet port on the back panel of the router.



STEP 4 Power on the cable or DSL modem.

STEP 5 Connect the power adapter to the router’s Power port and plug the other end into an electrical outlet.



STEP 6 The Power and Internet LEDs on the front panel lights up green as soon as the power adapter is connected.

STEP 7 Power on the PCs.

The router hardware installation is now complete.

Configuring the Router

To configure the RVS4000, connect a PC to the router and launch the configuration utility.

NOTE Before setting up the router, make sure your PCs are configured to obtain an IP (or TCP/IP) address automatically from the router.

STEP 1 Launch a web browser, such as Internet Explorer or Mozilla Firefox.

STEP 2 In the Address field enter **http://192.168.1.1** and press **Enter**.

STEP 3 In the User Name and Password fields, enter **admin**.

The default user name and password is **admin**.

STEP 4 Click **OK**.

For added security, you should later set a new password on the Administration > Management page of the configuration utility.

STEP 5 The configuration utility appears with the Setup menu and Summary selected. Click **WAN** under the Setup menu.

STEP 6 If requested by your ISP (usually cable ISPs), complete the Host Name and Domain Name fields, and the MTU and MTU Size fields. Otherwise, leave the defaults.

STEP 7 In the WAN screen, choose an Internet Connection Type from the drop-down menu. Depending on the Internet connection type that you select, addtional setup may be required.

The Internet Connection Types are:

Automatic Configuration - DHCP If you connect through DHCP or a dynamic IP address from your ISP, keep this default setting.

Static IP If your ISP assigns you a static IP address, select Static IP from the drop-down menu. Complete the Internet IP Address, Subnet Mask, Default Gateway, and DNS fields. Enter at least one DNS address.

PPPoE If you connect through PPPoE, select PPPoE from the drop-down menu. Complete the User Name and Password fields.

PPTP PPTP is used in Europe only. If you use a PPTP connection, check with your ISP for the necessary setup information.

Heartbeat Signal Heartbeat Signal is used primarily in Australia. Check with your ISP for the necessary setup information.

L2TP: L2TP is used mostly in Europe. Check with your ISP for the necessary setup information.

STEP 8 When you finish entering your Internet connection settings, click **Save**.

STEP 9 Restart or power on your PC to obtain the new router setting.

STEP 10 Test the setup by opening your web browser from any computer and entering http://www.cisco.com/smb.

Congratulations! The installation of the router is complete.

NOTE For more information about advanced settings and security options, refer to **Chapter 5, “Setting Up and Configuring the Router.”**

5

Setting Up and Configuring the Router

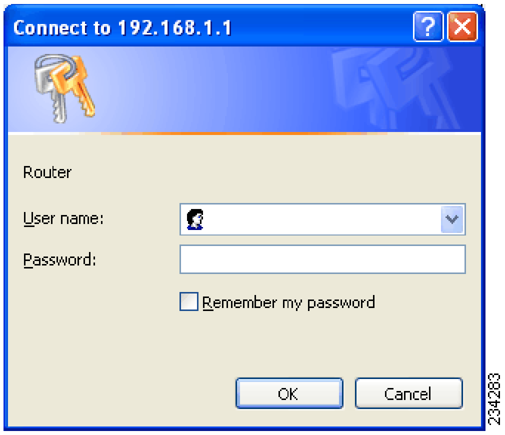
This chapter explains how to configure these router functions:

Configure the router by using the built-in web-based configuration utility. To access the configuration utility of the router, open your web browser and enter **http://192.168.1.1** into the Address field. Press the **Enter** key and the Login window appears.

NOTE The default IP address is **192.168.1.1**. If the IP address has been changed via DHCP or the console interface, enter the assigned IP address instead of the default.

The first time you open the configuration utility, enter **admin (**the default username) in the Username field and enter **admin** in the Password field. Click the **OK** button. You can change the password later from the Administration > Management window.

Login Window


Connect to 192.168.1.1

Router

User name:

Password:

□ Remember my password

OK Cancel

After you log in, the configuration utility starts. The menus appear as links in the navigation pane on the left side of the screen. After you select a menu, a list of windows appears. To perform a specific function, select a menu, and then select the appropriate window. By default, the Setup menu's Summary window appears after you log in.

The utility's menus and windows are described below. For brevity, window names are listed in this format: Menu > Window.

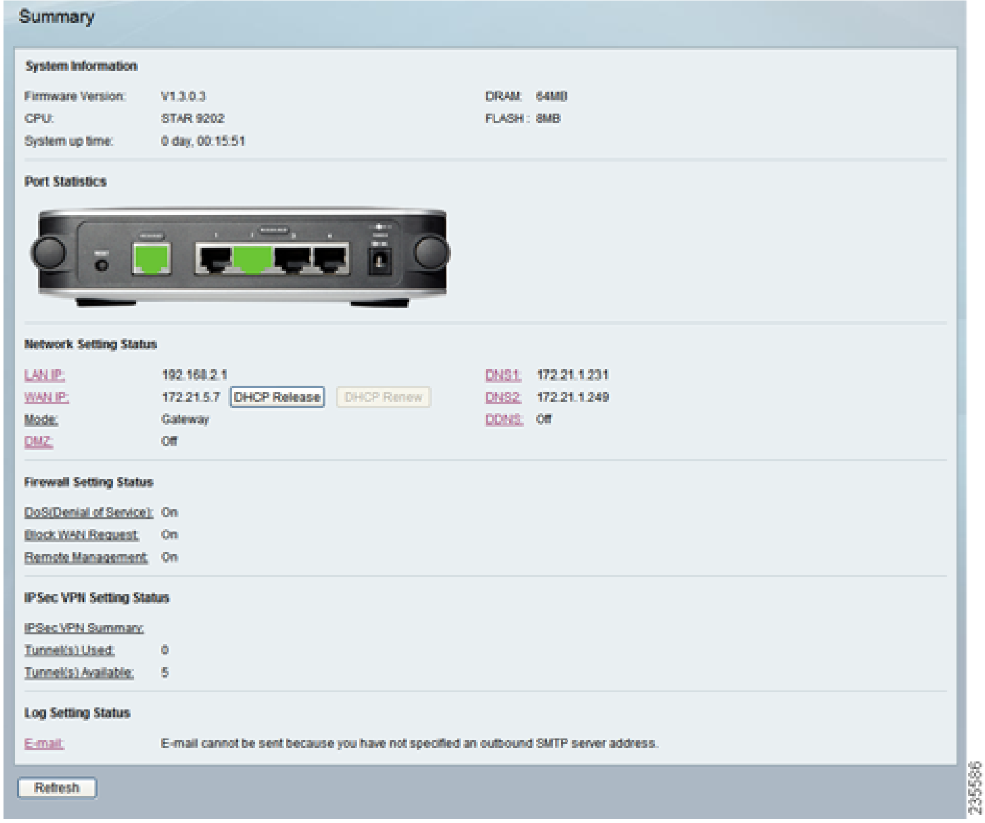
Setup

Use the Setup menu to access all of the router's basic setup functions. You can use the router in most network settings without changing any of the default values. Some users may need to enter additional information in order to connect to the Internet through an ISP (Internet Service Provider) or broadband (DSL, cable modem) carrier

Setup > Summary

The Setup > Summary window displays a read-only summary of the router's basic information. Click a hyperlink (underlined text) to open a related page where you can update the information.

Setup > Summary



Summary

System Information

Firmware Version: V1.3.0.3
CPU: STAR 9202
System up time: 0 day, 00:15:51
DRAM: 64MB
FLASH : 8MB

Port Statistics

Network Setting Status

LAN IP: 192.168.2.1
WAN IP: 172.21.5.7
Mode: Gateway
DMZ: Off
DNS1: 172.21.1.231
DNS2: 172.21.1.249
DDNS: Off

Firewall Setting Status

DoS(Denial of Service): On
Block WAN Request: On
Remote Management: On

IPSec VPN Setting Status

IPSec VPN Summary:
Tunnel(s) Used: 0
Tunnel(s) Available: 5

Log Setting Status

E-mail: E-mail cannot be sent because you have not specified an outbound SMTP server address.

System Information

Firmware version Displays the router's current firmware version.

CPU Displays the router's CPU type.

System up time Displays the length of time that has elapsed since the router was last reset.

DRAM Displays the amount of DRAM installed in the router.

Flash Displays the amount of flash memory installed in the router.

Port Statistics

This section displays color-coded status information on the router's Ethernet ports:

- **Green** Indicates that the port has a connection.
- **Black** Indicates that the port has no connection.

Network Setting Status

LAN IP The IP address of the router's LAN interface.

WAN IP The IP address of the router's WAN interface. If this address was assigned by using DHCP, click **DHCP Release** to release the address, or click **DHCP Renew** to renew the address.

Mode The operating mode, **Gateway** or **Router**.

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

DNS 1-2 The IP addresses of the Domain Name System (DNS) server(s) that the router is using.

DDNS Indicates whether the Dynamic Domain Name System (DDNS) feature is enabled.

DMZ Indicates whether the DMZ hosting feature is enabled.

Firewall Setting Status

DoS (Denial of Service) Indicates whether the DoS Protection feature is enabled to block DoS attacks.

Block WAN Request Indicates whether the Block WAN Request feature is enabled.

Remote Management Indicates whether the Remote Management feature is enabled.

IPSec VPN Setting Status

IPSec VPN Summary Click the **IPSec VPN Summary** hyperlink to display the VPN > Summary window.

Tunnel(s) Used Displays the number of VPN tunnels currently in use.

Tunnel(s) Available Displays the number of VPN tunnels that are available.

Log Setting Status

Email If this displays Email cannot be sent because you have not specified an outbound SMTP server address, then you have not set up the mail server. Click the **Email** hyperlink to display the Administration > Log window where you can configure the SMTP mail server.

Setup > WAN

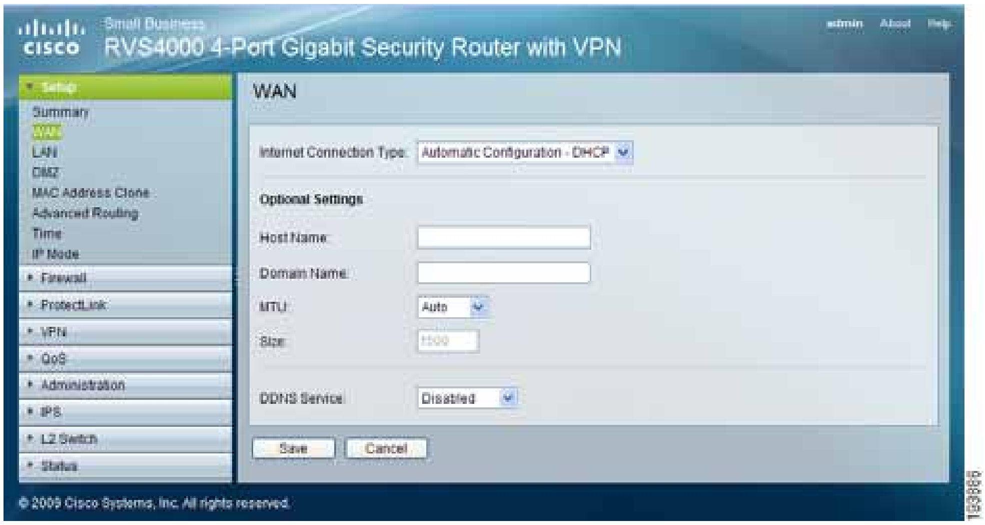
Internet Connection Type

The router supports six types of connections. Each Setup > WAN window and available features differ, depending on the selected connection type.

Automatic Configuration - DHCP

By default, the router's Configuration Type is set to **Automatic Configuration - DHCP**, and it should be kept only if your ISP supports DHCP or you connect through a dynamic IP address.

Automatic Configuration - DHCP



WAN

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings

Host Name:

Domain Name:

MTU: Auto

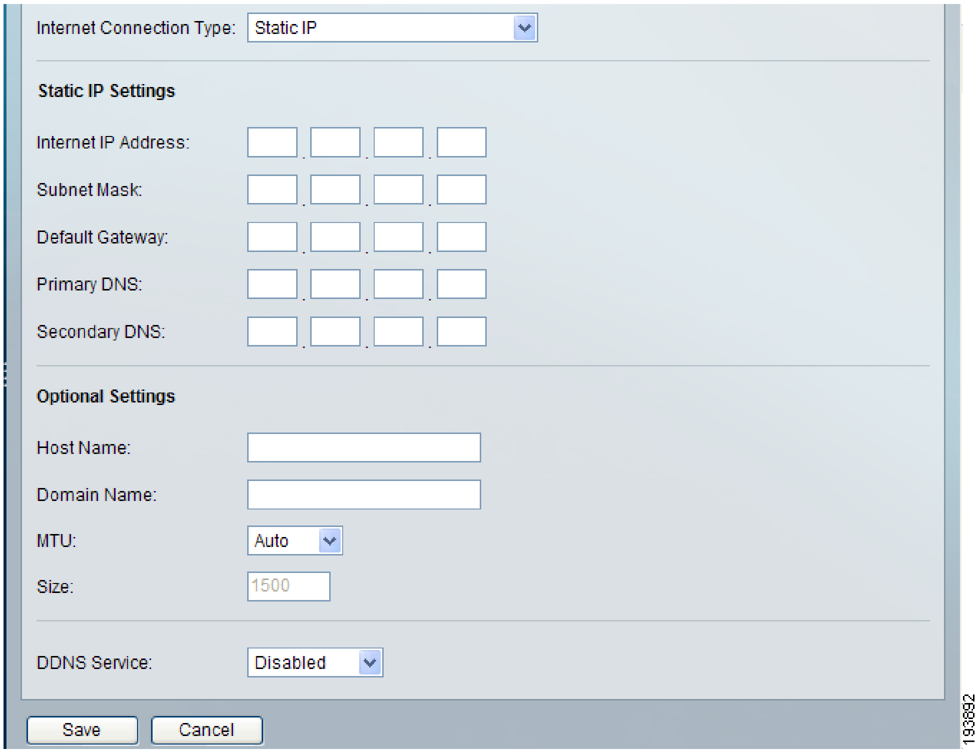
Size: 1500

DDNS Service: Disabled

Static IP

If your connection uses a permanent IP address to connect to the Internet, then select **Static IP.**

Static IP



Internet Connection Type:	Static IP

Static IP Settings

Internet IP Address:	. . .
Subnet Mask:	. . .
Default Gateway:	. . .
Primary DNS:	. . .
Secondary DNS:	. . .

Optional Settings

Host Name:	
Domain Name:	
MTU:	Auto
Size:	1500
DDNS Service:	Disabled

Internet IP Address The router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address to specify here.

Subnet Mask The router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

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

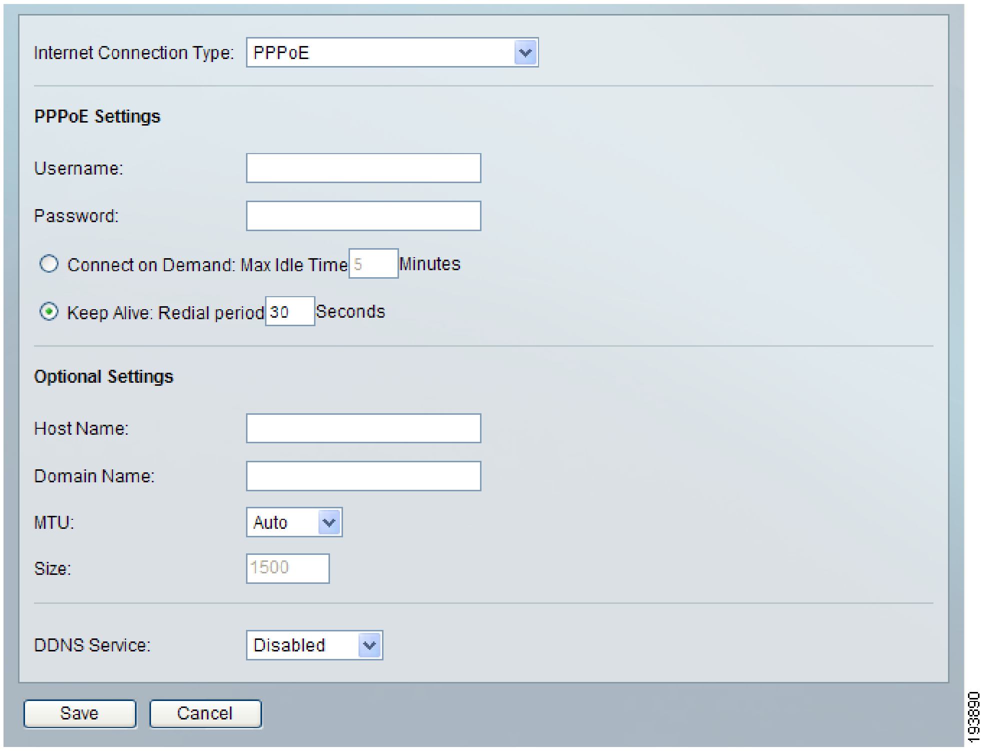
Primary DNS (Required) and Secondary DNS (Optional) Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

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

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you connect to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, enable PPPoE.

PPPoE



Internet Connection Type: PPPoE

PPPoE Settings

Username:

Password:

○ Connect on Demand: Max Idle Time 5 Minutes

● Keep Alive: Redial period 30 Seconds

Optional Settings

Host Name:

Domain Name:

MTU: Auto

Size: 1500

DDNS Service: Disabled

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

Connect on Demand: Max Idle Time You can configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the Max Idle Time field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

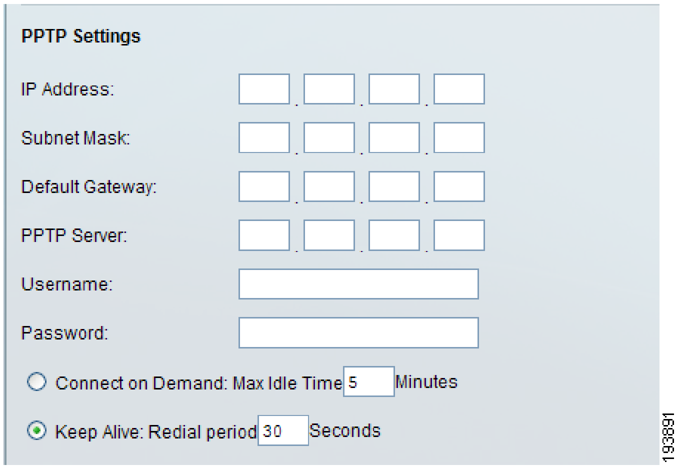
Keep Alive: Redial period If you select this option, the router periodically checks your Internet connection. If you are disconnected, then the router automatically re-establishes your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, specify how often you want the router to check the Internet connection. The default Redial Period is **30** seconds.

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

PPTP

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

PPTP



PPTP Settings

IP Address: ___ . ___ . ___ . ___

Subnet Mask: ___ . ___ . ___ . ___

Default Gateway: ___ . ___ . ___ . ___

PPTP Server: ___ . ___ . ___ . ___

Username: ___

Password: ___

○ Connect on Demand: Max Idle Time 5 Minutes

● Keep Alive: Redial period 30 Seconds

IP Address The router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask The router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Default Gateway Address.

PPTP Server Enter the IP address of the PPTP server.

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

Connect on Demand: Max Idle Time You can configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the Max Idle Time field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

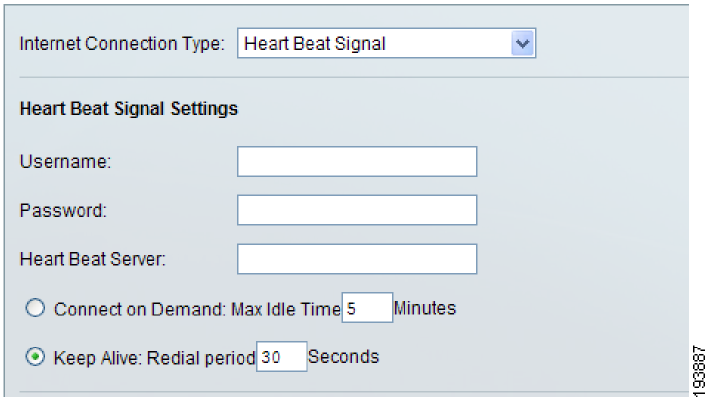
Keep Alive: Redial period If you select this option, the router periodically checks your Internet connection. If you are disconnected, then the router automatically re-establishes your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, specify how often you want the router to check the Internet connection. The default Redial Period is **30** seconds.

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

Heart Beat Signal

Heart Beat Signal is a service used in Australia. Check with your ISP for the necessary setup information.

Heart Beat Signal



Internet Connection Type: Heart Beat Signal

Heart Beat Signal Settings

Username:

Password:

Heart Beat Server:

○ Connect on Demand: Max Idle Time 5 Minutes

● Keep Alive: Redial period 30 Seconds

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

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

Connect on Demand: Max Idle Time You can configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the Max Idle Time field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

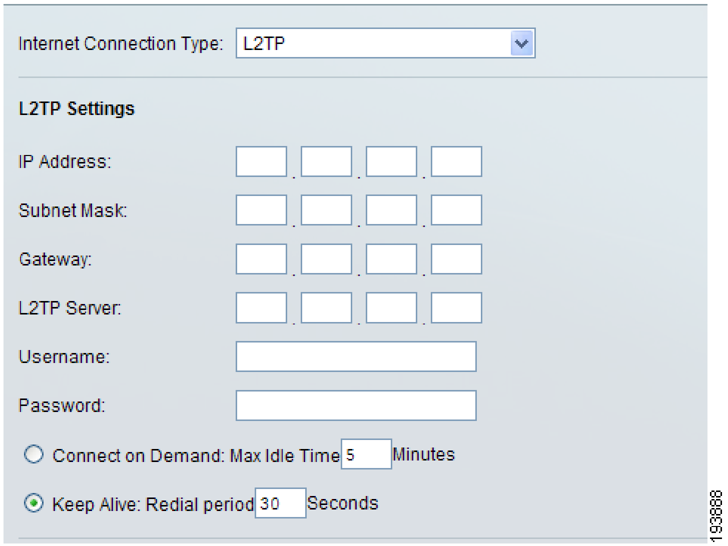
Keep Alive: Redial period If you select this option, the router periodically checks your Internet connection. If you are disconnected, then the router will automatically re-establishes your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, specify how often you want the router to check the Internet connection. The default Redial Period is **30** seconds.

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

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.

L2TP



Internet Connection Type: L2TP

L2TP Settings

IP Address: . . .
Subnet Mask: . . .
Gateway: . . .
L2TP Server: . . .
Username:
Password:

○ Connect on Demand: Max Idle Time 5 Minutes
● Keep Alive: Redial period 30 Seconds

IP Address The router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask The router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Gateway Your ISP will provide you with the Default Gateway Address.

L2TP Server Enter the IP address of the L2TP server.

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

Connect on Demand: Max Idle Time You can configure the router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time), and then automatically re-establish the connection as soon as you attempt to access the Internet again. To activate Connect on Demand, select the **Connect on Demand** option and enter in the Max Idle Time field the number of minutes of inactivity that must elapse before your Internet connection is terminated automatically.

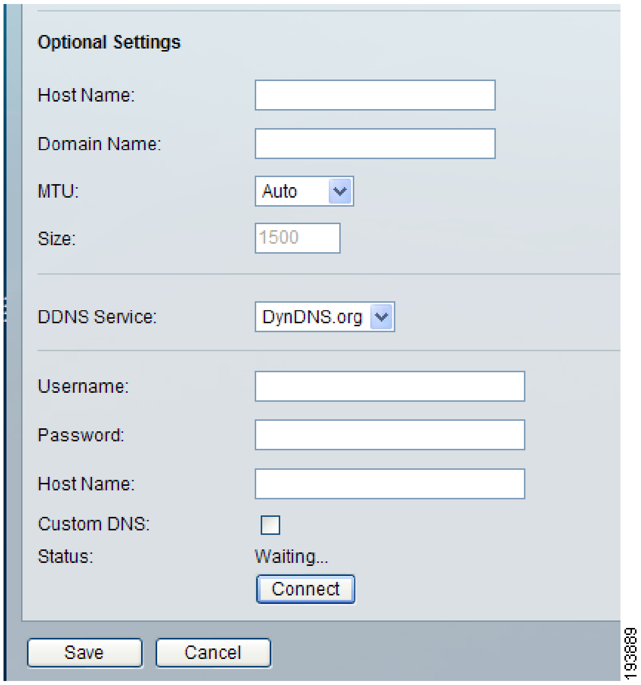
Keep Alive: Redial period If you select this option, the router periodically checks your Internet connection. If you are disconnected, then the router automatically re-establishes your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the router to check the Internet connection. The default Redial Period is **30** seconds.

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

Optional Settings (Required by some ISPs)

Your ISP may require some of these settings. Verify with your ISP before making any changes.

Optional Settings



Optional Settings

Host Name:	
Domain Name:	
MTU:	Auto
Size:	1500
DDNS Service:	DynDNS.org
Username:	
Password:	
Host Name:	
Custom DNS:	□
Status:	Waiting...

Host Name Some ISPs, usually cable ISPs, require a host name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host name. In most cases, you can leave this field blank.

Domain Name Some ISPs, usually cable ISPs, require a domain name as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a domain name. In most cases, you can leave this field blank.

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

Size When Manual is selected in the MTU field, this option is enabled. It is recommended that you set this value within the range of 1200 to 1500, but the value can be defined between 128 and 1500.

DDNS Service DDNS Service is disabled by default. To enable DDNS Service, follow these instructions:

Connect The **Connect** button is displayed when DDNS is enabled. You can click this button to contact the DDNS server to manually update your IP address information. The Status area on this window is also updated.

STEP 1 Sign up for DDNS Service:

- DynDNS - Sign up for DDNS service at www.dyndns.org and write down your User Name, Password, and Host Name information.
- TZO - Sign up for DDNS service at www.tzo.com and write down your email address, password and domain name information.

STEP 2 Select your DDNS service provider.

STEP 3 Configure these fields:

- User Name (DynDNS) or Email address (TZO).
- Password
- Host Name (DynDNS) or Domain name (TZO)
- Custom DNS (DynDNS)

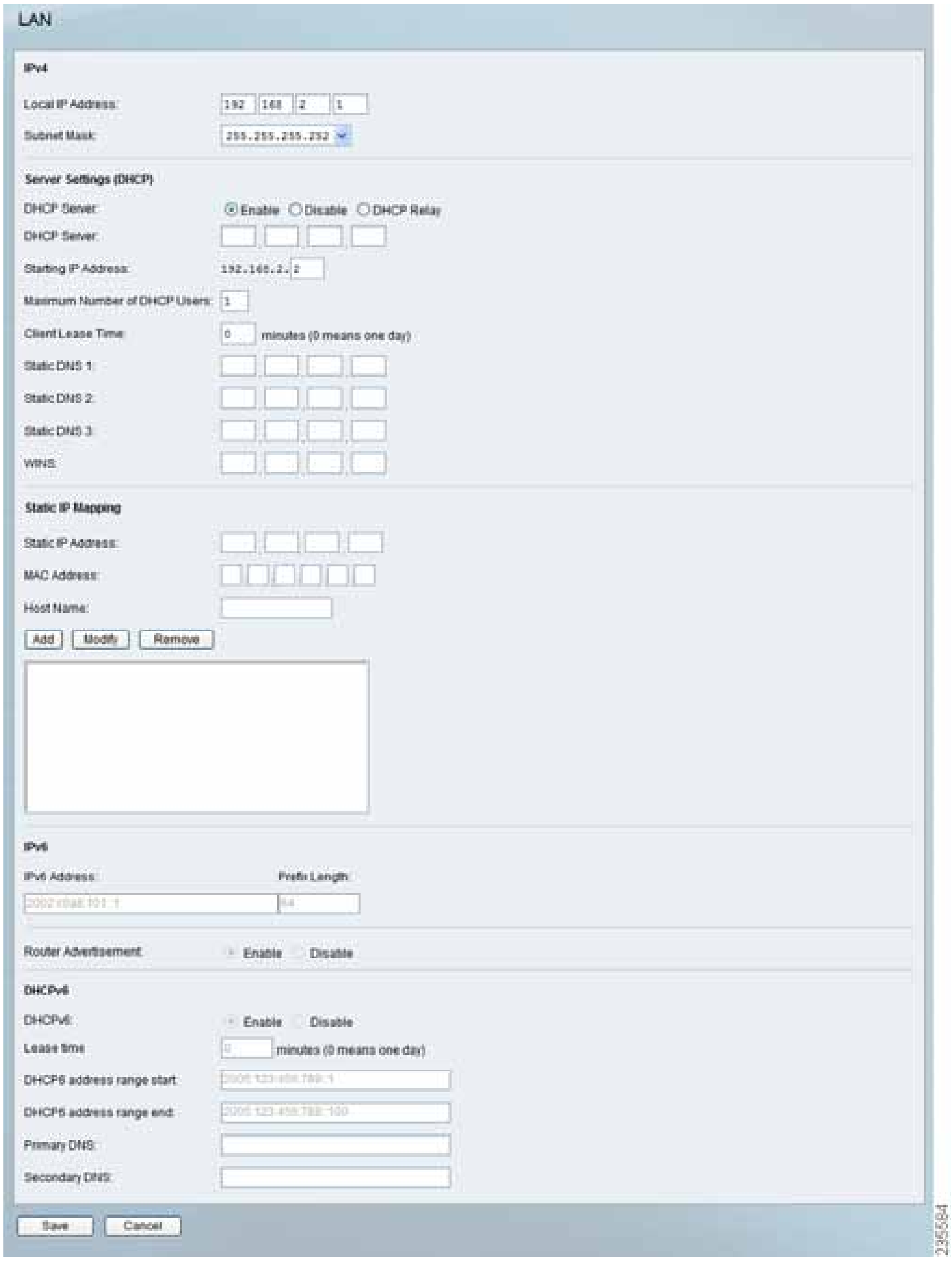
STEP 4 Click **Save**.

The router advises the DDNS Service of your current WAN (Internet) IP address whenever this address changes. If you use TZO, you should NOT use the TZO software to perform this “IP address update”.

Setup > LAN

The Setup > LAN window allows you to change the router's local network settings.

Setup > LAN



LAN

IPv4

Local IP Address: 192 . 168 . 2 . 1

Subnet Mask: 255.255.255.252

Server Settings (DHCP)

DHCP Server: ● Enable ○ Disable ○ DHCP Relay

DHCP Server:

Starting IP Address: 192.168.2. 2

Maximum Number of DHCP Users: 1

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1:

Static DNS 2:

Static DNS 3:

WINS:

Static IP Mapping

Static IP Address:

MAC Address:

Host Name:

IPv6

IPv6 Address: 2002:c0a8:101::1 Prefix Length: 64

Router Advertisement: ● Enable ○ Disable

DHCPv6

DHCPv6: ● Enable ○ Disable

Lease time: 0 minutes (0 means one day)

DHCP6 address range start: 2005:123:456:789::1

DHCP6 address range end: 2005:123:456:789::100

Primary DNS:

Secondary DNS:

VLAN Select the VLAN for the DHCP server from the drop-down menu.

NOTE This option appears only if you have created at least one VLAN from the L2 Switch > Create VLAN window.

IPv4

The router's Local IP Address and Subnet Mask appear here. In most cases, you can keep the defaults.

Local IP Address The default value is 192.168.1.1.

Subnet Mask The default value is 255.255.255.0.

Server Settings (DHCP)

You can use the router as your network's DHCP (Dynamic Host Configuration Protocol) server, which automatically assigns an IP address to each PC on your network. Unless you already have one, it is highly recommended that you leave the router enabled as a DHCP server.

DHCP Server DHCP is already enabled by factory default. If you already have a DHCP server on your network, or if you don't want a DHCP server, then select **Disabled** (no other DHCP features will be available). If you already have a DHCP server on your network, and you want this router to act as a Relay for that DHCP Server, select **DHCP Relay**, then enter the DHCP Server IP Address. If you disable DHCP, assign a static IP address to the router.

Starting IP Address Enter a value for the DHCP server to start with when it issues IP addresses. This value must be 192.168.1.2 or greater, but smaller than 192.168.1.254, because the default IP address for the router is 192.168.1.1, and 192.168.1.255 is the broadcast IP address.

Maximum Number of DHCP Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users.

Client Lease Time The amount of time a DHCP client can keep the assigned IP address before it sends a renewal request to the DHCP server.

Static DNS 1-3 If applicable, enter the IP address(es) of your DNS server(s).

WINS The Windows Internet Naming Service (WINS) provides name resolution service (similar to DNS) in Windows networks. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Static IP Mapping

Static IP Mapping is used to bind a specific IP address to a specific MAC address. This helps external (WAN) users to access LAN servers that are advertised through NAPT port forwarding. You can define up to 50 entries.

Static IP Address Enter the IP address to be mapped.

MAC Address Enter the MAC address to be mapped.

Host Name Enter the host name to be mapped.

Click **Add** to create the entry and add it to the list. To modify an existing entry, select it from the list, edit the appropriate field(s), and then click **Modify**. To delete an entry, select it and click **Remove**.

IPv6

IPv6 Address If your network has implemented IPv6, enter the proper IPv6 address in this field.

Prefix Length Enter the appropriate IPv6 prefix length.

Router Advertisement When enabled, this option allows IPv6 hosts to configure their IP addresses automatically by using the IPv6 prefix broadcast by the router.

DHCPv6

To enable the DHCP v6 feature, select **Enable**. To disable DHCP v6, select **Disable**.

Lease time Enter the lease time in minutes.

DHCP6 address range start Enter the starting DHCP v6 IP address.

DHCP6 address range end Enter the ending DHCP v6 IP address.

Primary DNS Enter the Primary DHCP v6 DNS server address.

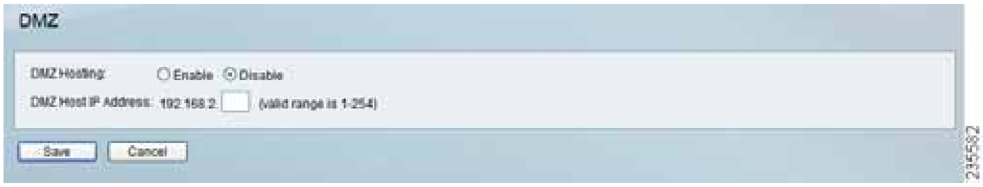
Secondary DNS Enter the Secondary DHCP v6 DNS server address.

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

Setup > DMZ

You can set up a DMZ to allow one local PC to be exposed to the Internet for a special service such as Internet gaming and videoconferencing. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.

Setup > DMZ



DMZ

DMZ Hosting: ○ Enable ● Disable

DMZ Host IP Address: 192.168.2. (valid range is 1-254)

DMZ Hosting This feature allows one local PC to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enable**. To disable the DMZ feature, select **Disable**.

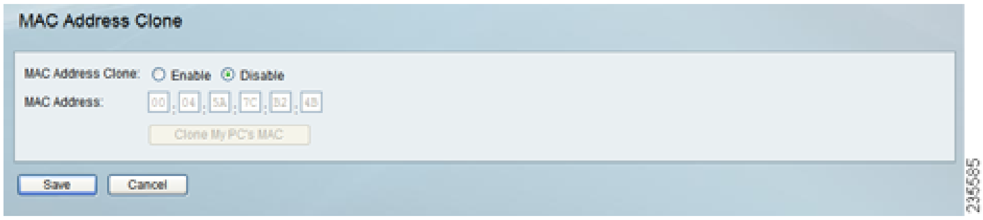
DMZ Host IP Address To expose one PC, enter the computer's IP address.

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

Setup > MAC Address Clone

Some ISPs require that you register a MAC address. This feature "clones" your 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 12-digit code assigned to a unique piece of hardware for identification.

Setup > MAC Address Clone



MAC Address Clone

MAC Address Clone: ○ Enable ● Disable

MAC Address: 00 : 04 : 5A : 7C : B2 : 4B

MAC Address Clone Select **Enabled** or **Disabled** from the drop-down menu.

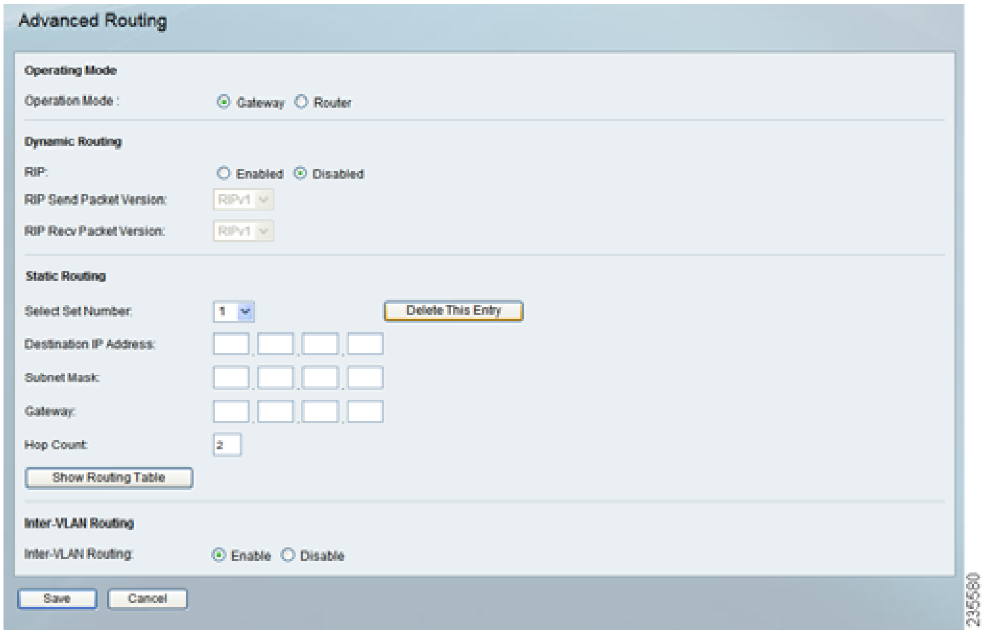
MAC Address Enter the MAC Address registered with your ISP in this field.

Clone My PC's MAC When MAC Address Clone is enabled, click this button to copy the MAC address of the network adapter in the computer that you use to connect to the web interface.

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

Setup > Advanced Routing

Setup > Advanced Routing



Advanced Routing

Operating Mode

Operation Mode : ● Gateway ○ Router

Dynamic Routing

RIP: ○ Enabled ● Disabled

RIP Send Packet Version: RIPv1

RIP Recv Packet Version: RIPv1

Static Routing

Select Set Number: 1

Destination IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

Hop Count: 2

Inter-VLAN Routing

Inter-VLAN Routing: ● Enable ○ Disable

Operating Mode

Operation Mode Select the Operating mode for this router:

- **Gateway** The normal mode of operation. This allows all devices on your LAN to share the same WAN (Internet) IP address. In Gateway mode, the NAT (Network Address Translation) mechanism is enabled.

- **Router** You either need another router to act as the Internet Gateway, or all PCs on your LAN must be assigned (fixed) Internet IP addresses. In Router mode, the NAT mechanism is disabled.

Dynamic Routing

You can use the router's dynamic routing feature to automatically adjust to physical changes in the network's layout. The router can use the dynamic RIP protocol to calculate the most efficient route for the network's data packets to travel between the source and the destination, based upon the shortest paths. The RIP protocol regularly broadcasts routing information to other routers on the network.

RIP (Routing Information Protocol) If you want the router to use the RIP protocol, select **Enabled**; otherwise, keep the default setting, **Disabled**.

RIP Send Packet Version Choose the TX protocol to use to transmit data on the network: **RIPv1** or **RIPv2**. This setting should match the version supported by other routers on your LAN.

RIP Recv Packet Version Choose the RX protocol to use to receive data from the network: **RIPv1** or **RIPv2**. This should match the version supported by other routers on your LAN.

Static Routing

Sometimes you may prefer to use static routes to build your routing table instead of using dynamic routing protocols. Static routes do not require CPU resources to exchange routing information with a peer router. You can also use static routes to reach peer routers that do not support dynamic routing protocols. Static routes can be used together with dynamic routes. Be careful not to introduce routing loops in your network.

To set up static routing, you should add route entries in the routing table that tell the router where to forward packets to specific IP destinations.

Enter this data to create a static route entry:

Select Set Number Select the set number (routing table entry number) that you wish to view or configure. If necessary, click **Delete This Entry** to clear the entry.

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

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

Gateway If this router is used to connect your network to the Internet, then your gateway IP is the router’s IP Address. If you have another router that manages your network’s Internet connection, enter the IP Address of that router instead.

Hop Count This value gives the number of nodes that a data packet passes through before it reaches its destination. A node is any device on the network, such as switches, PCs, etc. The maximum hop count value is 16.

Show Routing Table Click this button to show the routing table established either through dynamic or static routing methods.

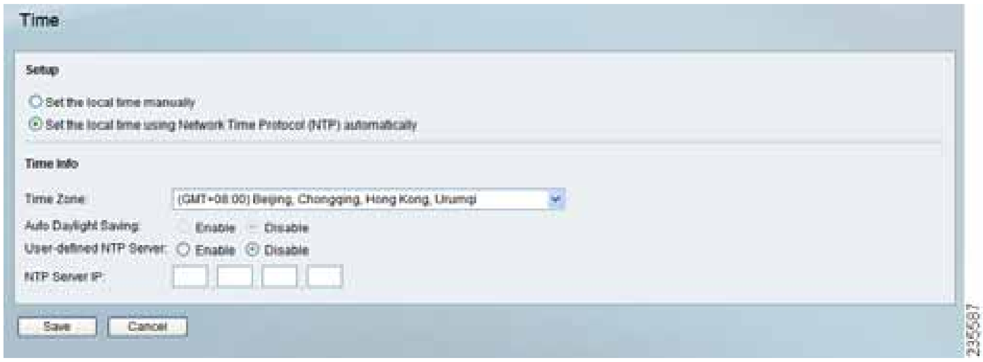
Inter-VLAN Routing

Inter-VLAN Routing Select **Enable** to allow packets to be routed between VLANs in different subnets. The default is **Enable**.

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

Setup > Time

Setup > Time



Time

Setup

○ Set the local time manually
● Set the local time using Network Time Protocol (NTP) automatically

Time Info

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Auto Daylight Saving: ○ Enable ○ Disable

User-defined NTP Server: ○ Enable ● Disable

NTP Server IP: □ □ □ □

Set the local time Manually If you wish to enter the time and date manually, select this option, then select the Date from the drop-down fields and enter the hour, minutes, and seconds in the Time fields in 24-hour format. For example, for 10:00 pm, enter **22** in the hours field, **0** in the minutes field, and **0** in the seconds field.

Set the local time using Network Time Protocol (NTP) Automatically If you wish to use a Network Time Protocol server to set the time and date, select this option, and then complete these fields:

Time Zone Select the time zone for your location and your time setting is synchronized over the Internet.

Auto Daylight Saving If your location observes daylight savings time, select the **Enable** option.

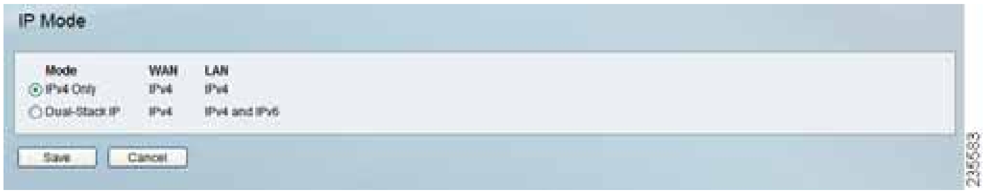
User-defined NTP Server To specify a user-defined NTP server, select the Enable option, then enter the NTP Server's IP address in the NTP Server IP field.

NTP Server IP If the User-defined NTP Server option is set to **Enable**, enter the IP address of the NTP server.

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

Setup > IP Mode

Setup > IP Mode



IP Mode

Mode	WAN	LAN
● IPv4 Only	IPv4	IPv4
○ Dual-Stack IP	IPv4	IPv4 and IPv6

IPv4 Only Select this option to use IPv4 on the Internet and local network.

Dual-Stack IP Select this option to use IPv4 on the Internet and IPv4 and IPv6 on the local network. IPv6 hosts in the LAN are connected to remote IPv6 islands over 6to4 tunnels (per RFC3056).

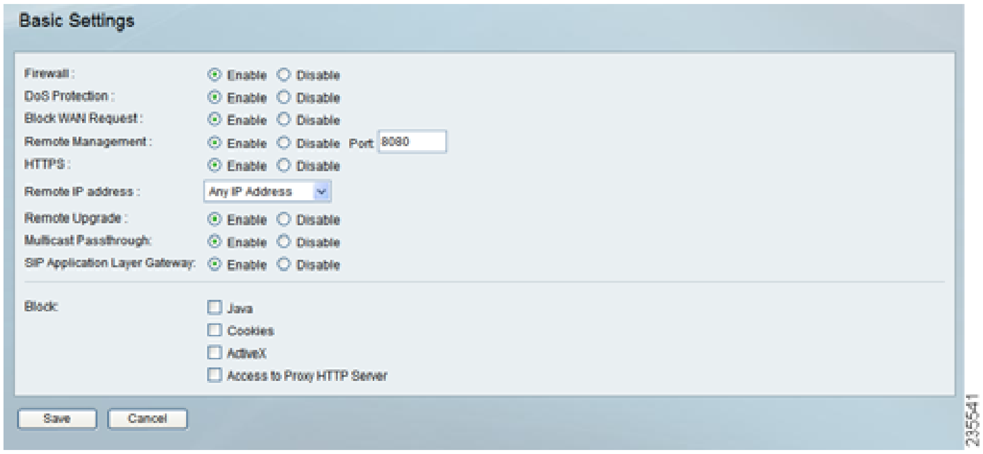
Click **Save** to save your settings or click **Cancel** to undo your changes.

Firewall

Use the Firewall menu to configure the router to deny or allow specific internal users from accessing the Internet. You can also configure the router to deny or allow specific Internet users from accessing the internal servers. You can set up different packet filters for different users on the internal (LAN) side or external (WAN) side based on their IP addresses or their network Port number.

Firewall > Basic Settings

Firewall > Basic Settings



Basic Settings

Firewall : ● Enable ○ Disable
DoS Protection : ● Enable ○ Disable
Block WAN Request : ● Enable ○ Disable
Remote Management : ● Enable ○ Disable Port 8080
HTTPS : ● Enable ○ Disable
Remote IP address : Any IP Address
Remote Upgrade : ● Enable ○ Disable
Multicast Passthrough: ● Enable ○ Disable
SIP Application Layer Gateway: ● Enable ○ Disable

Block: □ Java
□ Cookies
□ ActiveX
□ Access to Proxy HTTP Server

Firewall When this feature is enabled, the router's NAT firewall feature is enabled.

DoS Protection When this feature is enabled, the router blocks DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it.

Block WAN Request When this feature is enabled, the router filters out anonymous requests from the WAN.

Remote Management This feature allows you to use an http or https port to remotely manage the router. To enable this feature, select **Enable** and enter the port number in the Port field, then configure the HTTPS and Remote IP address settings that appear below.

HTTPS This option limits access to the configuration utility from the WAN to https sessions only. An https session uses SSL encryption, which provides better protection for your remote session than does http. The default is **Enable**.

- **Remote IP address** Select the appropriate value to specify which external IP address(es) can access the router.
- **Any IP Address** Allows access from any external IP address.
- **Single IP Address** Allows access from the single IP address that you enter in the field provided.
- **IP Range** Allows access from a range of IP addresses that you enter in the field provided.
- **Subnet** Allows access from the Subnet that you enter in the field provided.

Remote Upgrade This option allows you to upgrade the router remotely. To allow remote upgrade, select Enable. The Remote Management feature must be set to Enable as well. The default is **Disable**.

Multicast Passthrough If an IGMP Proxy is running on the router, enable this feature to allow IP Multicast traffic to come in from the Internet. The default is **Disable**.

SIP Application Layer Gateway When this feature is enabled, the SIP Application Layer Gateway (ALG) allows Session Initiation Protocol (SIP) packets (used for Voice over IP) to traverse the NAT firewall. You can disable this feature if the VoIP service provider uses other NAT traversal solutions such as STUN, TURN, and ICE.

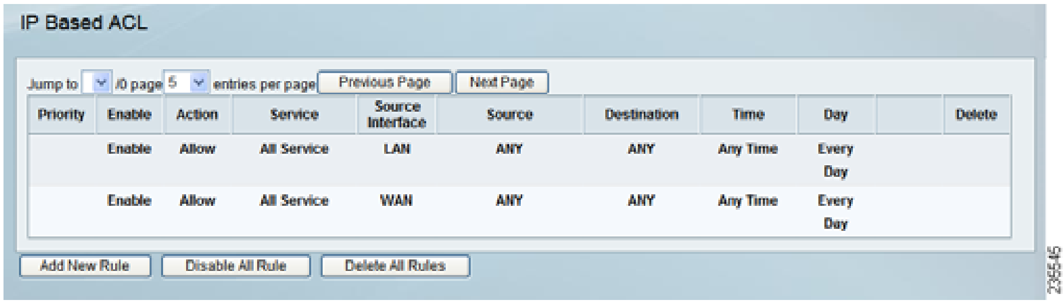
Block Place a checkmark next to the Web features that you wish to restrict.

- **Java** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites that use this programming language.
- **Cookies** A cookie is data stored on your PC and used by Internet sites when you interact with them, so you may not want to deny cookies.
- **ActiveX** ActiveX is a Microsoft (Internet Explorer) programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites that use this programming language. Also, Windows Update uses ActiveX, so if this is blocked, Windows update will not work.
- **Access to Proxy HTTP Server** If local users have access to WAN proxy servers, they may be able to circumvent the router’s content filters and access Internet sites blocked by the router. Denying Proxy will block access to any WAN proxy servers.

Firewall > IP Based ACL

The IP-Based ACL window allows you to create an Access Control List (ACL) with up to 50 rules. Each ACL rule denies or allows access to the network based on various criteria including priority, service type, interface, source IP address, destination IP address, day of the week, and time of day.

Firewall > IP Based ACL



Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
	Enable	Allow	All Service	LAN	ANY	ANY	Any Time	Every Day		
	Enable	Allow	All Service	WAN	ANY	ANY	Any Time	Every Day		

Priority The rule's priority.

Enable This indicates whether the rule is enabled or disabled.

Action The rule's action, either Allow or Deny.

Service The service(s) to which the rule applies.

Source Interface The source interface, either WAN, LAN, or ANY.

Source The source IP address, which can be one specific IP address, ANY (all IP addresses), a range of IP addresses, or a specific IP subnet.

Destination The destination IP address, which can be one specific IP address, ANY (all IP addresses), a range of IP addresses, or a specific IP subnet.

Time The time of day when the rule is in effect, either Any Time (24 hours) or a specific start and end time.

Day The day(s) of the week when the rule is in effect. This may be Any Day or a user-specified set of days.

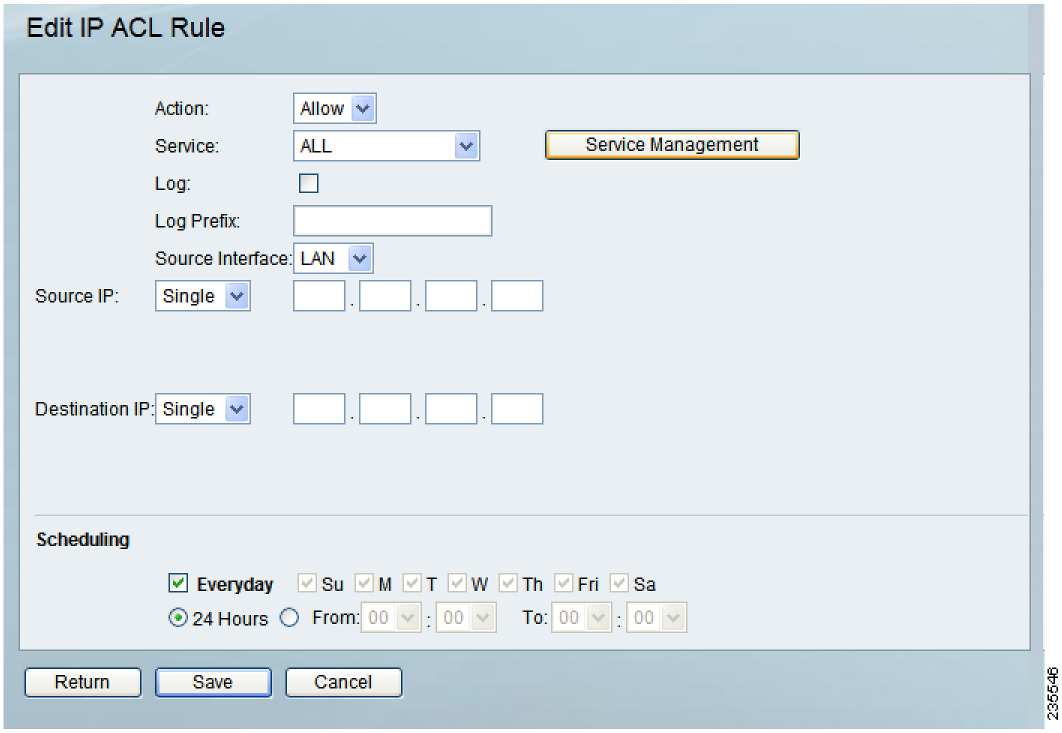
Edit button Click **Edit** at the end of a row to edit the associated rule.

Delete button Click **Delete** at the end of a row to delete the associated rule.

To add a new rule to the ACL rule table, click **Add New Rule** and the Edit IP ACL Rule window appears. Follow the instructions in the section below to create a new ACL rule. To disable all the rules without deleting them, click **Disable All Rules**. To delete all the rules from the table, click **Delete All Rules**.

Editing IP ACL Rules

Editing IP ACL Rules



Edit IP ACL Rule

Action: Allow
Service: ALL
Log: □
Log Prefix:
Source Interface: LAN
Source IP: Single . . .
Destination IP: Single . . .

Scheduling

☑ Everyday ☑ Su ☑ M ☑ T ☑ W ☑ Th ☑ Fri ☑ Sa
● 24 Hours ○ From: 00 : 00 To: 00 : 00

Action Select the desired action, **Allow** or **Deny**, from the drop-down menu.

Service Select the service types to which the rule applies. You can either select one of the predefined services in the drop-down menu; select **ALL** to allow or deny all types of IP traffic; or define a new service by clicking **Service Management** to bring up the Service Management window, then the new service's Name, select the Type (TCP, UDP, or TCP/UDP), enter the Start Port and Finish Port, then click **Save**. The new service appears in the drop-down menu on the Edit IP ACL Rule window.

Log Select this option to log all traffic that is filtered by this rule.

Log Prefix Enter a text string to prepend to each matched event in the log.

Source Interface Select the source interface, **WAN**, **LAN**, or **ANY**, from the drop-down menu.

Source IP To apply the rule to one source IP address, select **Single** from the drop-down menu, then enter the address in the field. To apply the rule to all source IP addresses, select **ANY** from the drop-down menu. To apply the rule to a range of IP addresses, select **Range** and enter the starting and ending IP addresses. To apply the rule to a subnet, select **Net** and enter the IP address and subnet mask.

Destination IP To apply the rule to one destination IP address, select **Single** from the drop-down menu, then enter the address in the field. To apply the rule to all destination IP addresses, select **ANY** from the drop-down menu. To apply the rule to a range of IP addresses, select **Range** and enter the starting and ending IP addresses. To apply the rule to a subnet, select **Net** and enter the IP address and subnet mask.

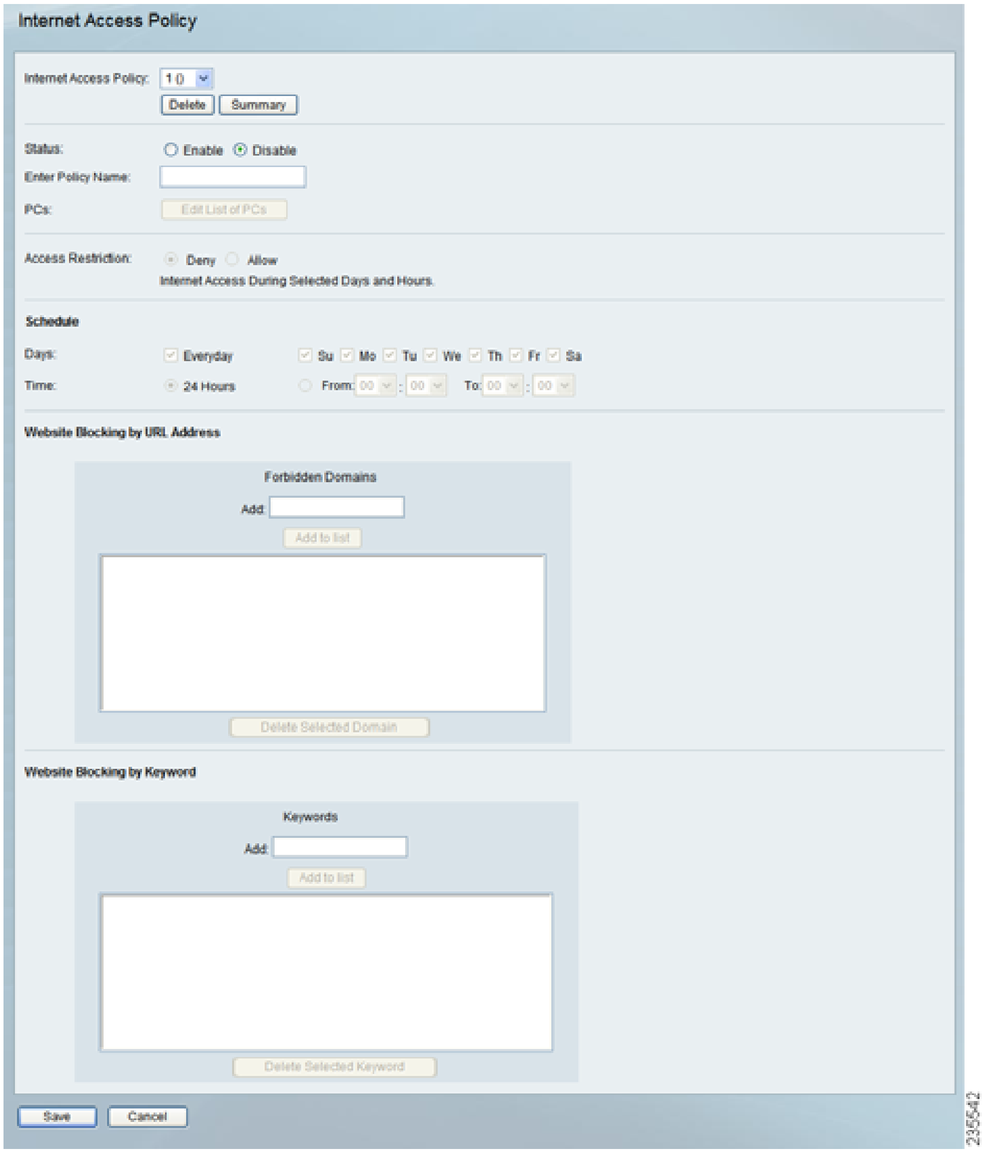
Days To make the rule apply on a daily basis, select **Everyday**. To make the rule apply on specific days of the week only, select the desired days.

Time To make the rule apply for an entire day, select **24 Hours**. To make the rule apply only during a specific period of the day, enter the starting time in the From field and the ending time in the To field.

Click **Save** to save your changes, or click **Cancel** to undo your changes. Click **Return** to return to the IP-Based ACL window.

Firewall > Internet Access Policy

Firewall > Internet Access Policy



Internet Access Policy

Internet Access Policy: 1 ()

Status: ○ Enable ● Disable

Enter Policy Name:

PCs:

Access Restriction: ● Deny ○ Allow
Internet Access During Selected Days and Hours.

Schedule

Days: ☑ Everyday ☑ Su ☑ Mo ☑ Tu ☑ We ☑ Th ☑ Fr ☑ Sa

Time: ● 24 Hours ○ From: 00 : 00 To: 00 : 00

Website Blocking by URL Address

Forbidden Domains

Add:

Website Blocking by Keyword

Keywords

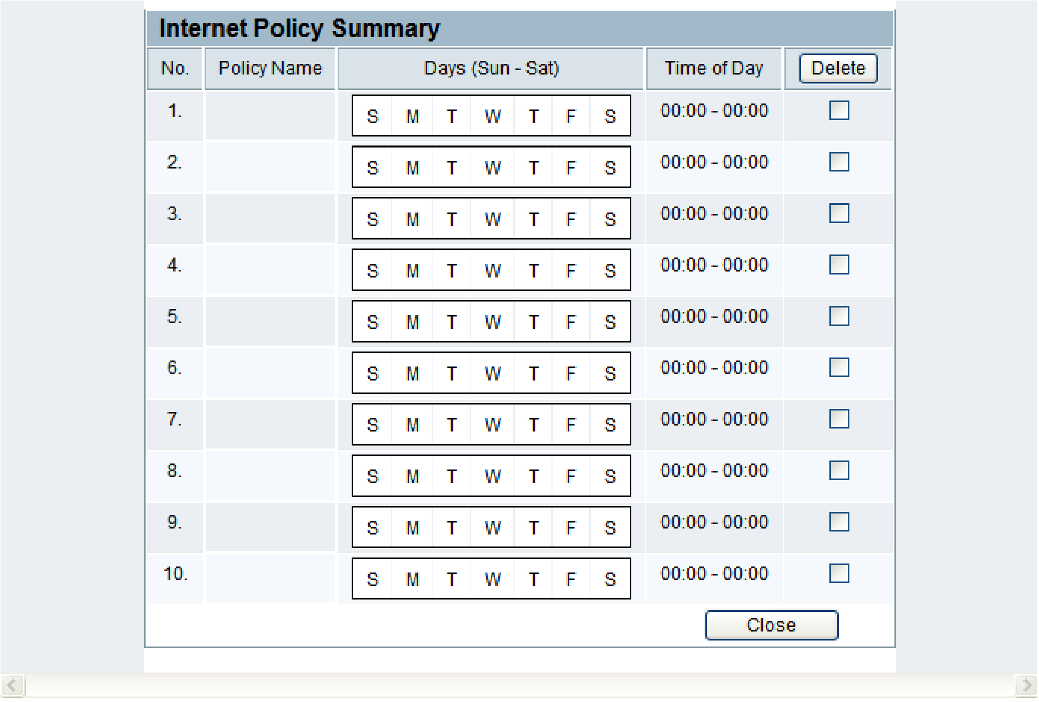
Add:

You can manage access to your network by configuring a policy. Use the settings on this window to establish an access policy. Select a policy from the drop-down menu to display the settings for a policy. You can then perform these operations:

- Create a Policy: See the instructions below.
- Delete the current policy: Click **Delete**.

- **View all policies**: Click **Summary** to display the Internet Policy Summary window, which lists all of the Internet access policies and includes this information: No., Policy Name, Days, Time, and a check box to delete (clear) the policy. To delete a policy, check the box in the Delete column, and then click **Delete**.
- **View or change the PCs covered by the current policy**: Click **Edit List of PCs** to display the List of PCs window.

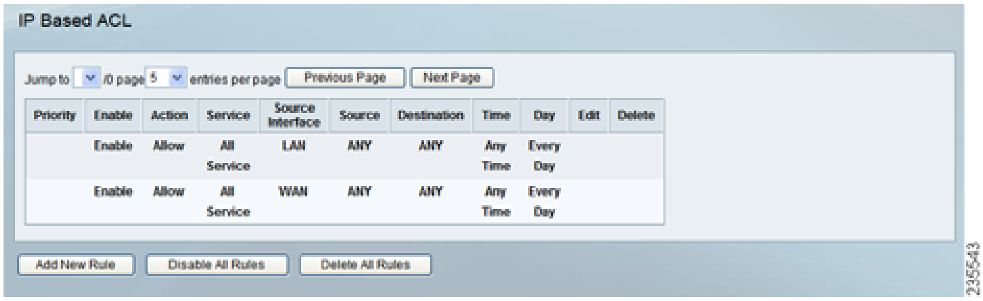
Internet Policy Summary



Internet Policy Summary

No.	Policy Name	Days (Sun - Sat)	Time of Day	Delete
1.		S M T W T F S	00:00 - 00:00	□
2.		S M T W T F S	00:00 - 00:00	□
3.		S M T W T F S	00:00 - 00:00	□
4.		S M T W T F S	00:00 - 00:00	□
5.		S M T W T F S	00:00 - 00:00	□
6.		S M T W T F S	00:00 - 00:00	□
7.		S M T W T F S	00:00 - 00:00	□
8.		S M T W T F S	00:00 - 00:00	□
9.		S M T W T F S	00:00 - 00:00	□
10.		S M T W T F S	00:00 - 00:00	□

List of PCs



IP Based ACL

Jump to /0 page 5 entries per page

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Edit	Delete
	Enable	Allow	All Service	LAN	ANY	ANY	Any Time	Every Day		
	Enable	Allow	All Service	WAN	ANY	ANY	Any Time	Every Day		

On the List of PCs popup, you can define PCs by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs.

To create an Internet Access policy:

STEP 1 Select the desired policy number from the Internet Access Policy drop-down menu.

STEP 2 Enter a Policy Name in the field provided.

STEP 3 To enable this policy, set the Status option to **Enable**.

STEP 4 Click **Edit List of PCs** to select which PCs will be affected by the policy. The List of PCs popup appears. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click **Save** to apply your changes.

STEP 5 Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs popup.

STEP 6 Decide which Days and what Times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

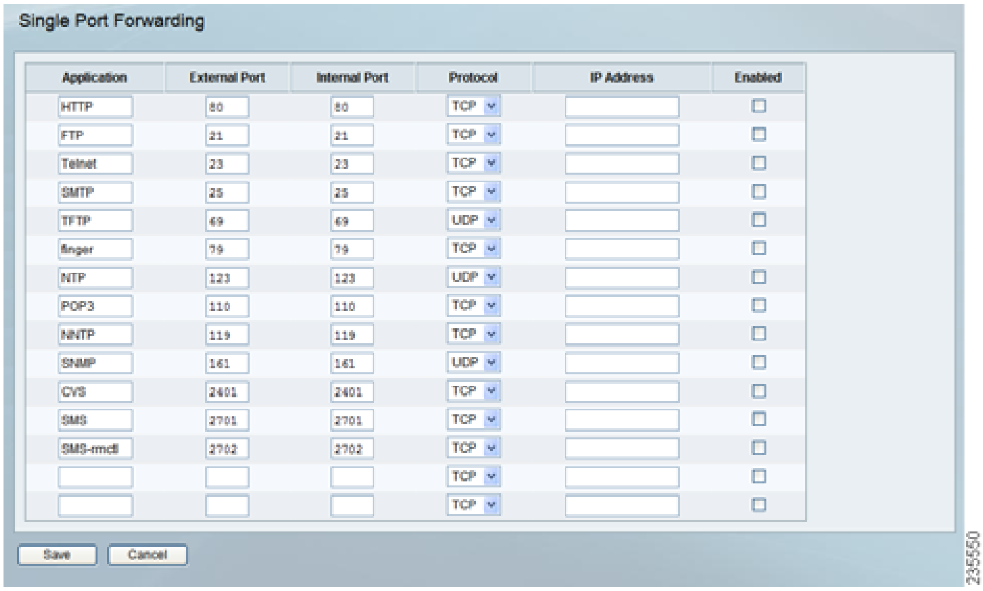
STEP 7 If you wish to block access to websites, use the **Website Blocking by URL Address** or **Website Blocking by Keyword** feature.

- **Website Blocking by URL Address**. Enter the URL or Domain Name of the websites you wish to block.
- **Website Blocking by Keyword**. Enter the keywords you wish to block in the fields provided. If any of these Keywords appears in the URL of a website, access to the site will be blocked. Note that only the URL is checked, not the content of each Web page.

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

Firewall > Single Port Forwarding

Firewall > Single Port Forwarding



Application	External Port	Internal Port	Protocol	IP Address	Enabled
HTTP	80	80	TCP		☐
FTP	21	21	TCP		☐
Telnet	23	23	TCP		☐
SMTP	25	25	TCP		☐
TFTP	69	69	UDP		☐
finger	79	79	TCP		☐
NTP	123	123	UDP		☐
POP3	110	110	TCP		☐
NNTP	119	119	TCP		☐
SNMP	161	161	UDP		☐
CVS	2401	2401	TCP		☐
SMS	2701	2701	TCP		☐
SMS-rmctl	2702	2702	TCP		☐
			TCP		☐
			TCP		☐

Application Enter the name of the application you wish to configure.

External Port The port number used by the server or Internet application. Internet users must connect using this port number. Check with the software documentation of the Internet application for more information.

Internal Port The port number used by the router when forwarding Internet traffic to the PC or server on your LAN. Normally, this port number is the same as the External Port number. If it is different, the router performs a “Port Translation”, so that the port number used by Internet users is different from the port number used by the server or Internet application.

For example, you could configure your Web Server to accept connections on both port 80 (standard) and port 8080. Then enable Port Forwarding, and set the External Port to 80, and the Internal Port to 8080. Now, any traffic from the Internet to your Web server uses port 8080, even though the Internet users used the standard port, 80. (Users on the local LAN can and should connect to your Web Server using the standard port 80.)

Protocol Select the protocol used for this application, TCP and/or UDP.

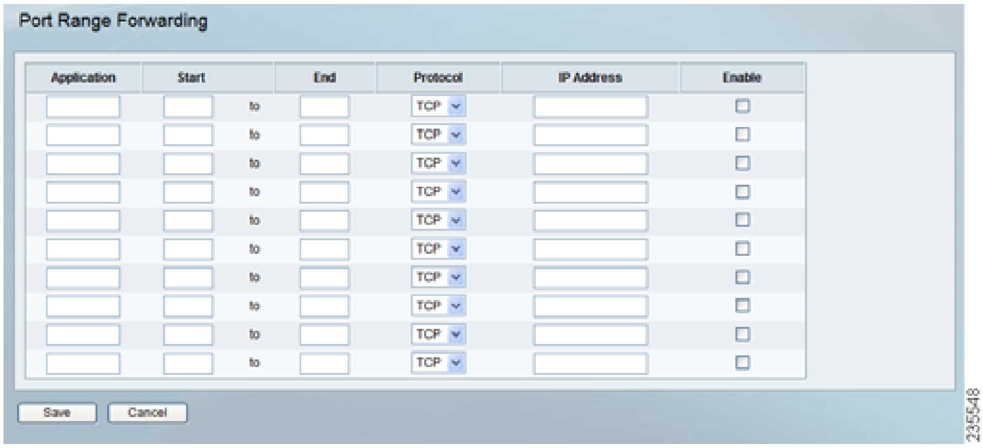
IP Address For each application, enter the IP address of the PC running the specific application.

Enabled Click the **Enabled** checkbooks to enable port forwarding for the relevant application.

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

Firewall > Port Range Forwarding

Firewall > Port Range Forwarding



Port Range Forwarding

Application	Start		End	Protocol	IP Address	Enable
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□
		to		TCP		□

Application Enter the name of the application you wish to configure.

Start The beginning of the port range. Enter the beginning of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.

End The end of the port range. Enter the end of the range of port numbers (external ports) used by the server or Internet application. Check with the software documentation of the Internet application for more information if necessary.

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

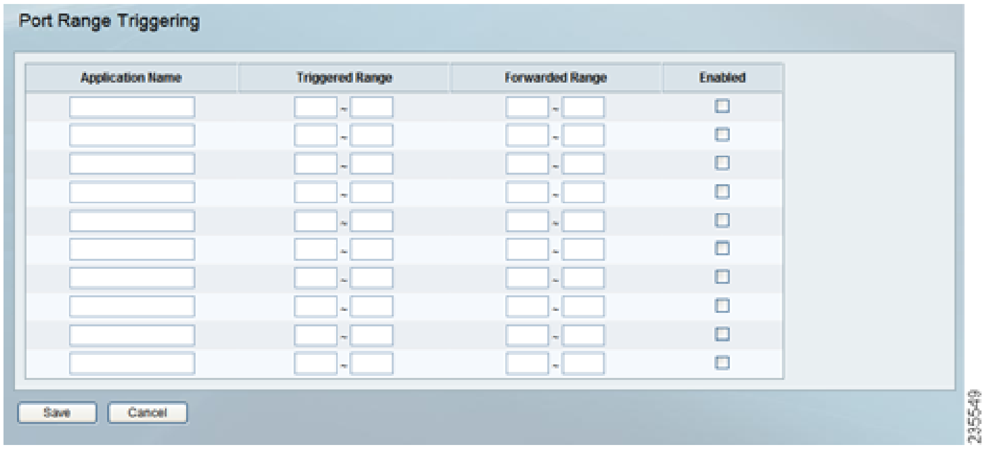
IP Address For each application, enter the IP address of the PC running the specific application.

Enabled Click the **Enabled** checkbooks to enable port range forwarding for the relevant application.

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

Firewall > Port Range Triggering

Firewall > Port Range Triggering



Port Range Triggering

Application Name	Triggered Range	Forwarded Range	Enabled
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□

Application Name Enter the name of the application you wish to configure.

Triggered Range For each application, list the triggered port number range. These ports are used by outgoing traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number of the Triggered Range.

Forwarded Range For each application, list the forwarded port number range. These ports are used by incoming traffic. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

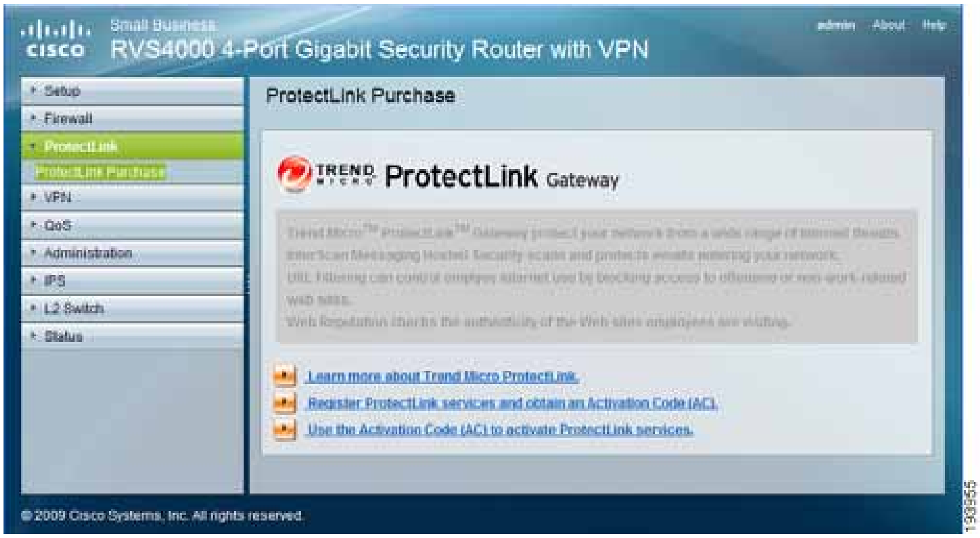
Enabled Click the **Enabled** checkbooks to enable port range triggering for the relevant application.

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

ProtectLink

ProtectLink > ProtectLink Purchase

ProtectLink > ProtectLink Purchase



Trend Micro™ ProtectLink™ Gateway protect your network from a wide range of Internet threats.
InterScan Messaging Hosted Security scans and protects emails entering your network.
URL Filtering can control employee Internet use by blocking access to offensive or non-work related web sites.
Web Reputation checks the authenticity of the Web sites employees are visiting.

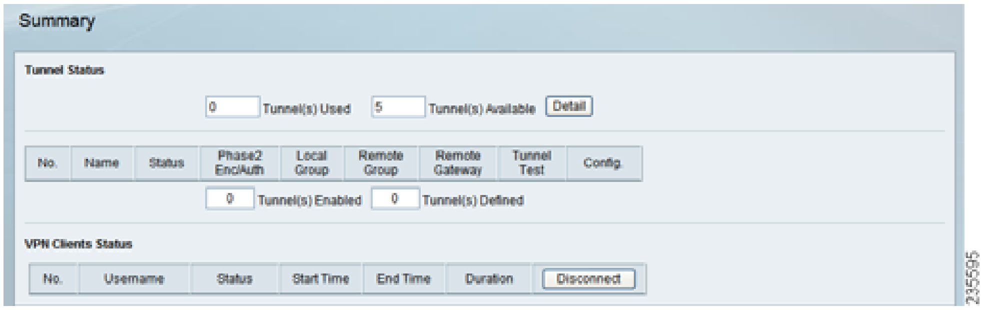
- Learn more about Trend Micro ProtectLink.
- Register ProtectLink services and obtain an Activation Code (AC).
- Use the Activation Code (AC) to activate ProtectLink services.

The optional Trend Micro ProtectLink Gateway service provides security for your network. For more information, see **Appendix E, "Trend Micro ProtectLink Gateway Service."**

VPN

VPN > Summary

VPN > Summary



Summary

Tunnel Status

0 Tunnel(s) Used 5 Tunnel(s) Available Detail

No.	Name	Status	Phase2 Enc/Auth	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.

0 Tunnel(s) Enabled 0 Tunnel(s) Defined

VPN Clients Status

No.	Username	Status	Start Time	End Time	Duration	Disconnect

Tunnels Used Displays the number of tunnels used.

Tunnel(s) Available Displays the number of available tunnels.

Detail button Click **Detail** to display more tunnel information.

Tunnel Status

No. Displays the number of the tunnel.

Name Displays the name of the tunnel, as defined by the Tunnel Name field on the VPN > IPSec VPN window.

Status Displays the tunnel's status: Connected, Hostname Resolution Failed, Resolving Hostname, or Waiting for Connection.

Phase2 Enc/Auth. Displays the Phase 2 Encryption type (3DES), Authentication type (MD5 or SHA1), and Group (768-bit, 1024-bit, or 1536-bit) that you chose in the VPN > IPSec VPN window.

Local Group Displays the IP address and subnet of the local group.

Remote Group Displays the IP address and subnet of the remote group.

Remote Gateway Displays the IP address of the remote gateway.

Tunnel Test Click **Connect** to verify the tunnel status; the test result is updated in the Status column. If the tunnel is connected, you can disconnect the IPSec VPN connection by clicking **Disconnect**.

Config Click **Edit** to change the tunnel's settings. Click **Trash** to delete all of the tunnel's settings.

Tunnel(s) Enabled Displays the total number of currently enabled tunnels.

Tunnel(s) Defined Displays the number of tunnels currently defined. This number will be greater than the Tunnels Enabled field if any defined tunnels have been disabled.

VPN Clients Status

No. Displays the user number from 1 to 5.

Username. Displays the username of the VPN Client.

Status Displays the connection status of the VPN Client.

Start Time Displays the start time of the most recent VPN session for the specified VPN Client.

End Time Displays the end time of a VPN session if the VPN Client has disconnected.

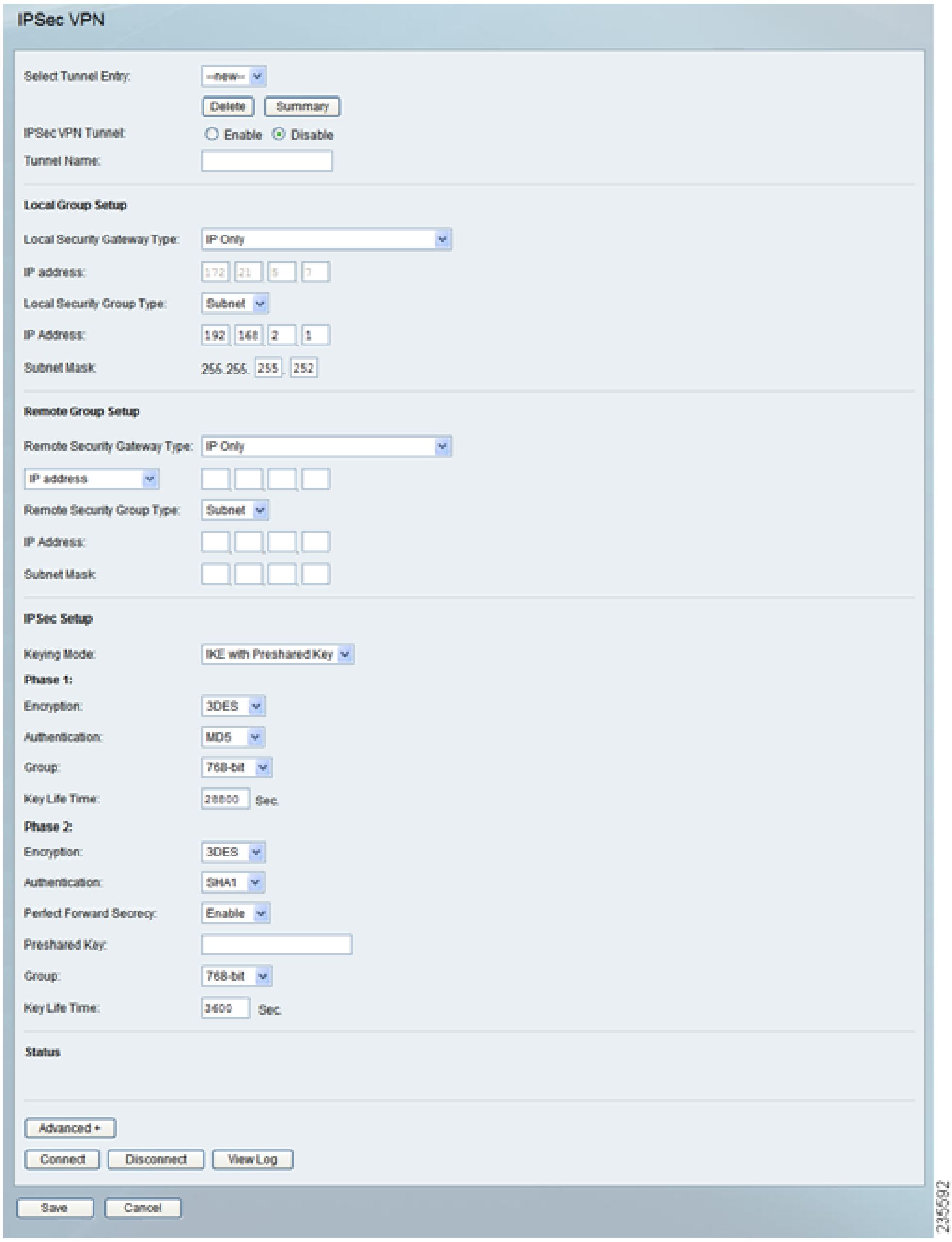
Duration Displays the total connection time of the latest VPN session.

Disconnect Check the Disconnect box at the end of each row in the VPN Clients Table and click the **Disconnect** button to disconnect a VPN Client session.

VPN > IPSec VPN

Use the VPN > IPSec VPN window to create and configure a Virtual Private Network (VPN) tunnel.

VPN > IPSec VPN



IPSec VPN

Select Tunnel Entry: --new--

IPSec VPN Tunnel: ○ Enable ● Disable

Tunnel Name:

Local Group Setup

Local Security Gateway Type: IP Only

IP address: 172 . 21 . 5 . 7

Local Security Group Type: Subnet

IP Address: 192 . 168 . 2 . 1

Subnet Mask: 255.255. 255 . 252

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

Select Tunnel Entry To create a new tunnel, select **new.** To configure an existing tunnel, select it from the drop-down menu.

Delete Click this button to delete all settings for the selected tunnel.

Summary Clicking this button shows the settings and status of all enabled tunnels.

IPSec VPN Tunnel Check the **Enable** option to enable this tunnel.

Tunnel Name Enter a name for this tunnel, such as “Anaheim Office”.

Local Group Setup

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

- **IP Only** With this setting, the IP Address field automatically displays the router’s WAN IP address.
- **IP + Domain Name (FQDN) Authentication** With this setting, the IP Address field automatically displays the WAN IP address and domain name for greater security. Enter an arbitrary domain name in the Domain Name 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** Choose this option to specify the remote device that can access 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 drop-down menu and enter the remote gateway’s domain name in the Domain Name field.
- **IP + Domain Name (FQDN) Authentication** Choose this option to include the IP address and 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 purposes. Note that both sides must use the same Key Management method.

Phase 1

- **Encryption** The Encryption method determines the length of the key used 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. 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 specifies the lifetime of the IKE-generated key. If the time expires, a new key is renegotiated automatically. Enter a value from 300 to 100,000,000 seconds. The default is **28800** seconds.

Phase 2

- **Encryption** The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Only 3DES is supported. Note that both sides must use the same Encryption method.
- **Authentication** Authentication determines a method to authenticate the ESP packets. Either MD5 or SHA1 may be selected. Note 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 generates a new key material for IP traffic encryption and authentication. Note that both sides must have this selected.
- **Preshared Key** IKE uses the Preshared Key field to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field; e.g., “My_@123” or “0x4d795f40313233”. Note that both sides must use the same Preshared 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 specifies the lifetime of the IKE-generated key. If the time expires, a new key is renegotiated automatically. Enter a value from 300 to 100,000,000 seconds. The default is **3600** seconds.

Status

Status Displays the connection status for the selected tunnel. The state is either connected or disconnected.

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

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

View Log Click this button to view the VPN log, which shows details of each tunnel established.

Advanced Click this button to display these additional settings.

Aggressive Mode Specifies 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.

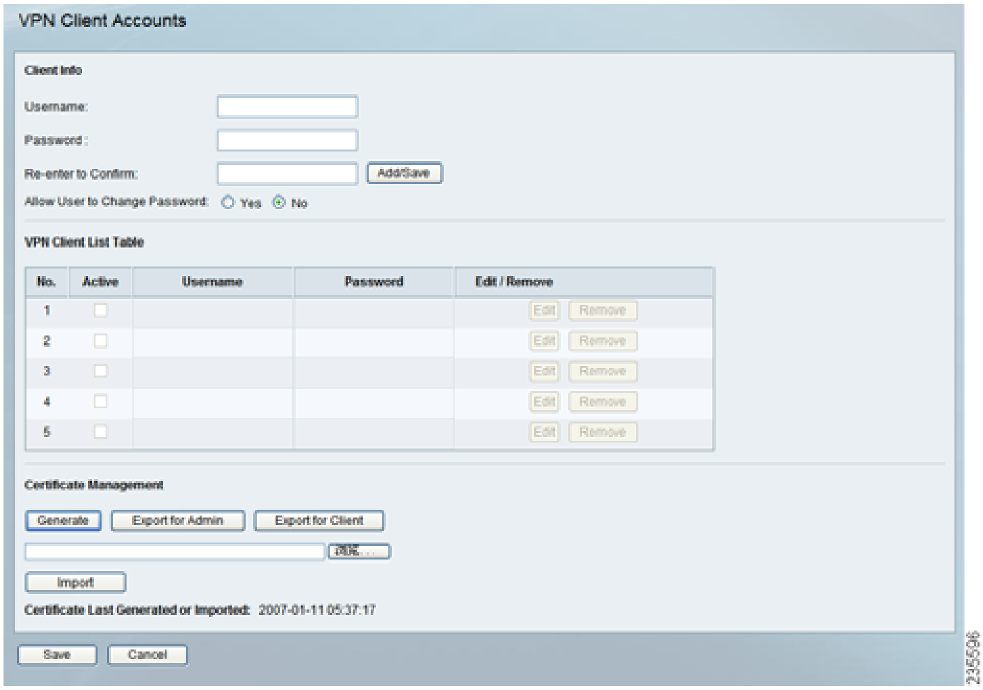
NetBios Broadcasts Check the box to enable NetBIOS traffic to pass through the VPN tunnel. By default, the RVS4000 blocks these broadcasts.

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

VPN > VPN Client Accounts

Use this window to administer your VPN Client users. After you enter the information at the top of the window, the information for the specified users appears in the table. This feature is available with the Cisco QuickVPN client only. The router supports up to five simultaneous Cisco QuickVPN sessions.

VPN > VPN Client Accounts



VPN Client Accounts

Client Info

Username:

Password :

Re-enter to Confirm:

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: 2007-01-11 05:37:17

Username Enter the username. It can include 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 it has been entered correctly.

Allow User to Change Password This option determines whether a user can change his or her own 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 Allows editing of the username or password.

Remove Click this button 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. When prompted, indicate where to store your certificate. The default file name is “RVS4000_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. When prompted, indicate where to store your certificate. The default file name is “RVS4000_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.

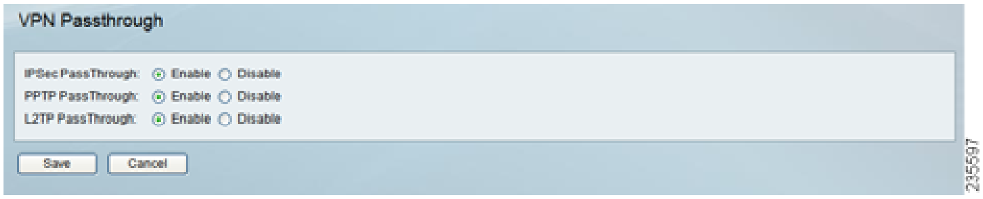
Import Click this button to import a certificate that was previously saved to a file by using **Export for Admin** or **Export for Client**. Enter the file name in the field or click **Browse** to locate the file on your computer, then click **Import**.

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

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

VPN > VPN Passthrough

VPN > VPN Passthrough



VPN Passthrough

IPSec PassThrough: ● Enable ○ Disable
PPTP PassThrough: ● Enable ○ Disable
L2TP PassThrough: ● Enable ○ Disable

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 **Disabled**.

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 it, select **Disabled**.

L2TP PassThrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select **Disabled**.

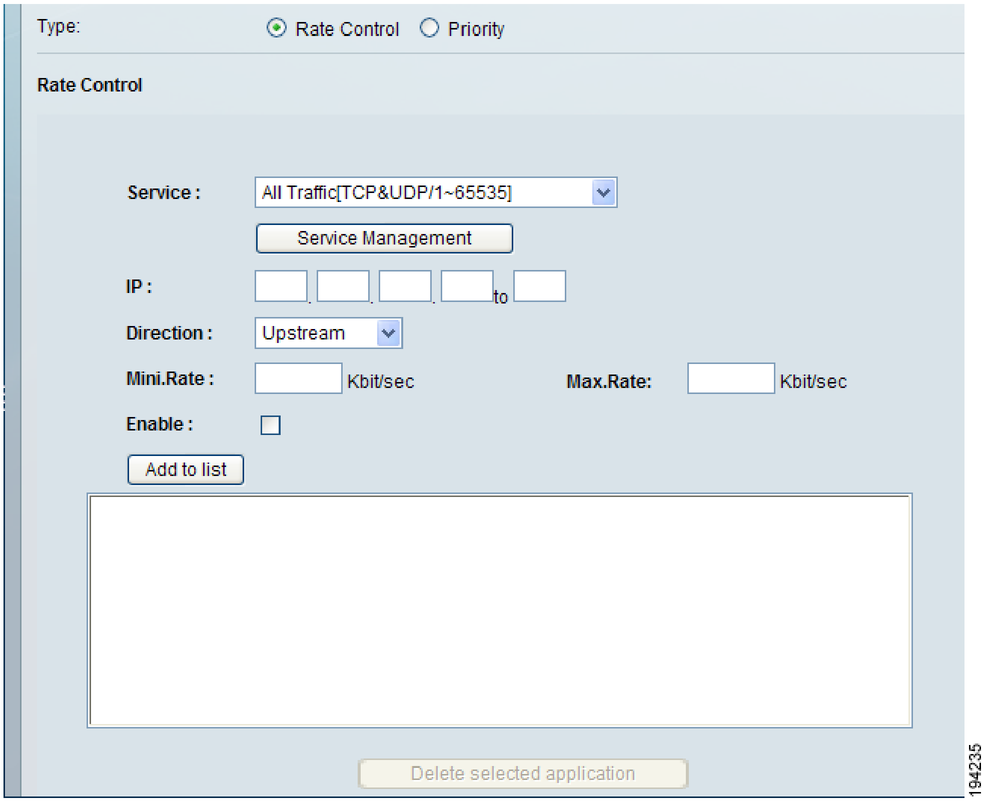
Click **Save** to save your changes, or click **Cancel** to undo your changes.

QoS

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

QoS > Bandwidth Management

QoS > Bandwidth Management - Rate Control



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

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** or **Priority** (default). Depending on your selection, the lower portion of the window 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.

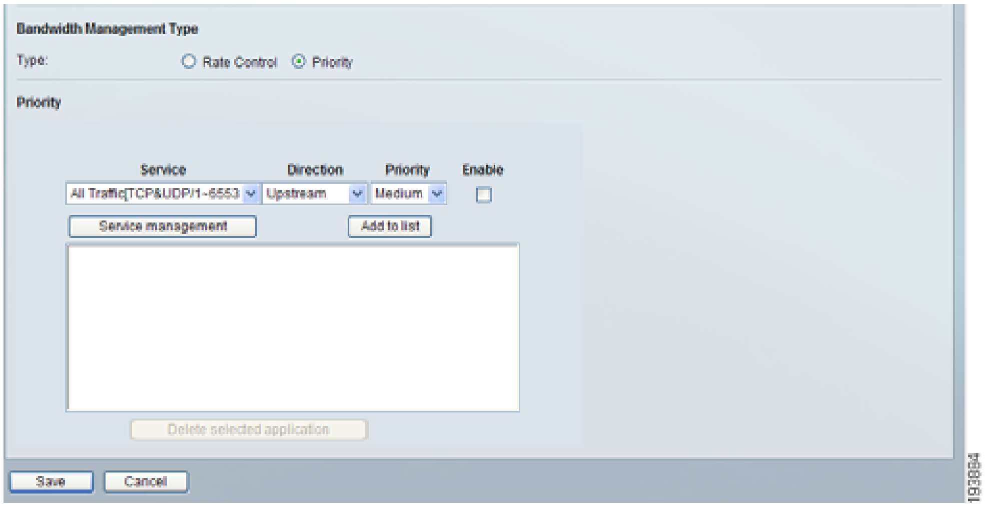
Enable Check this box to enable this Rate Control Rule.

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

QoS > Bandwidth Management - Priority



Bandwidth Management Type

Type: ○ Rate Control ● Priority

Priority

Service	Direction	Priority	Enable
All Traffic[TCP&UDP/1~6553	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**, **Normal**, 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.

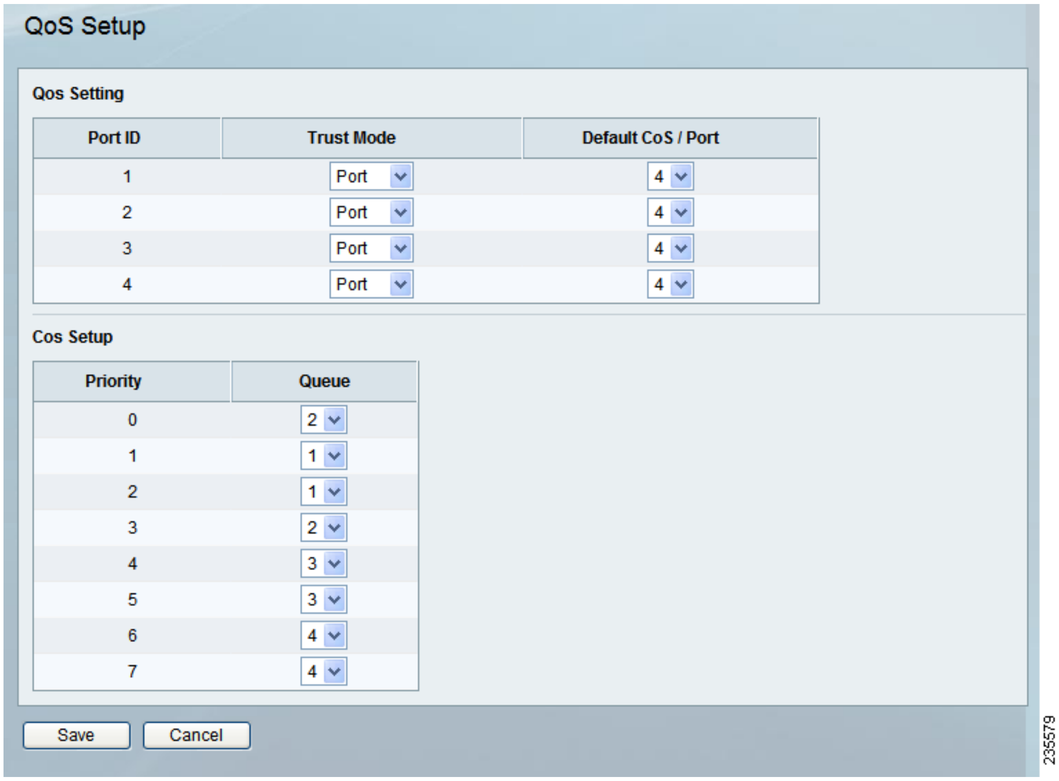
Delete selected application Click this button to delete a rule from the list.

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

QoS > QoS Setup

Use the QoS Setup window to configure QoS Trust Mode for each LAN port.

QoS > QoS Setup



QoS Setup

Qos Setting

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

Cos Setup

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, where **4** is the highest priority. If Trust Mode is set to **CoS**, select the default CoS priority from **0** to **7** from the drop-down menu.

CoS Setup

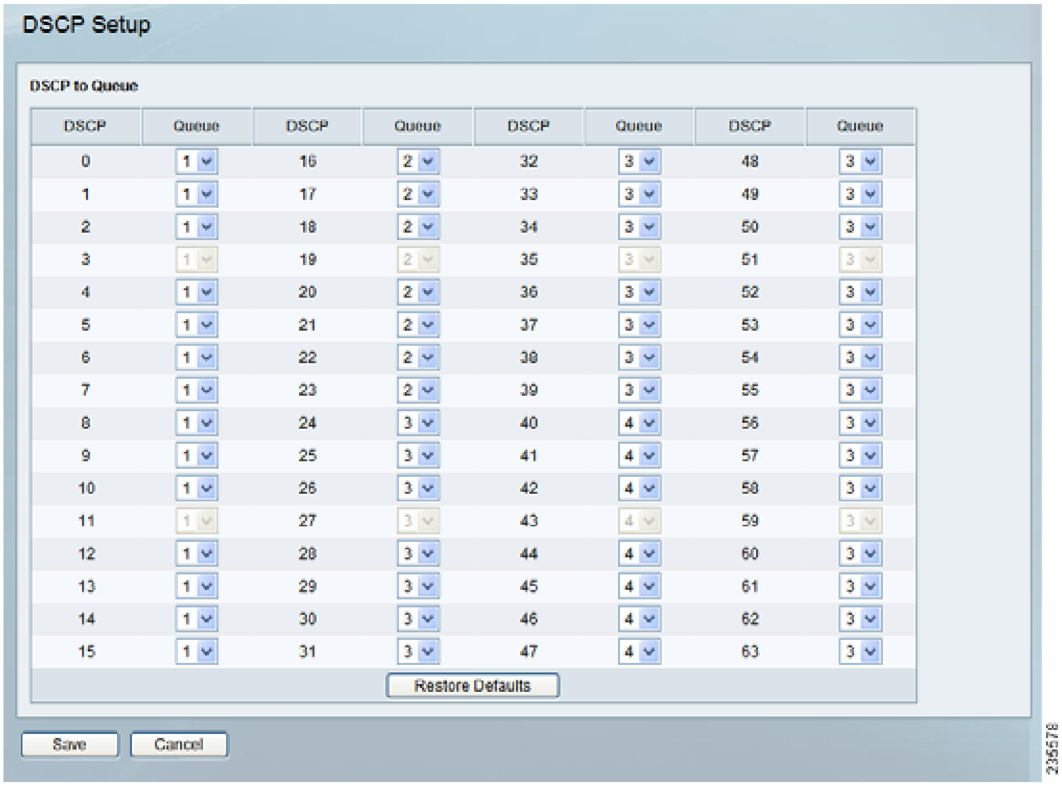
Priority The CoS priority from **0** to **7**.

Queue Select the traffic forwarding queue, **1** to **4**, to which the CoS priority is mapped. Queue **4** has the highest priority.

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

QoS > DSCP Setup

QoS > DSCP Setup



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

DSCP The Differentiated Services Code Point value in the incoming packet.

Queue Select the traffic forwarding queue, **1** to **4**, to which the DSCP priority is mapped. Queue **4** has the highest priority.

Restore Defaults Click this button to restore the default DSCP values.

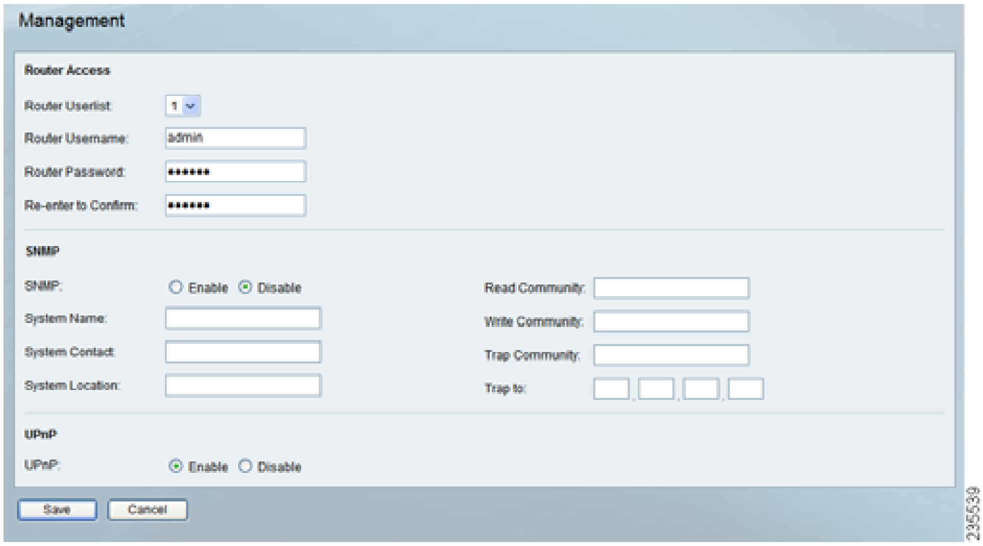
Click **Save** to save your changes, or click **Cancel** to undo your changes.

Administration

Use the Administration menu to configure the system administration settings and tools.

Administration > Management

Administration > Management



Management

Router Access

Router Userlist: 1

Router Username: admin

Router Password: ••••••

Re-enter to Confirm: ••••••

SNMP

SNMP: ○ Enable ● Disable

System Name:

System Contact:

System Location:

Read Community:

Write Community:

Trap Community:

Trap to: . . .

UPnP

UPnP: ● Enable ○ Disable

Router Access

Router Userlist Select the desired router user list.

Router Username Enter the user name here.

Router Password Enter the password.

Re-enter to Confirm Retype the password in this field.

SNMP

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 to identify this device. It 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 to which traps will be sent. If desired, this may be left blank.

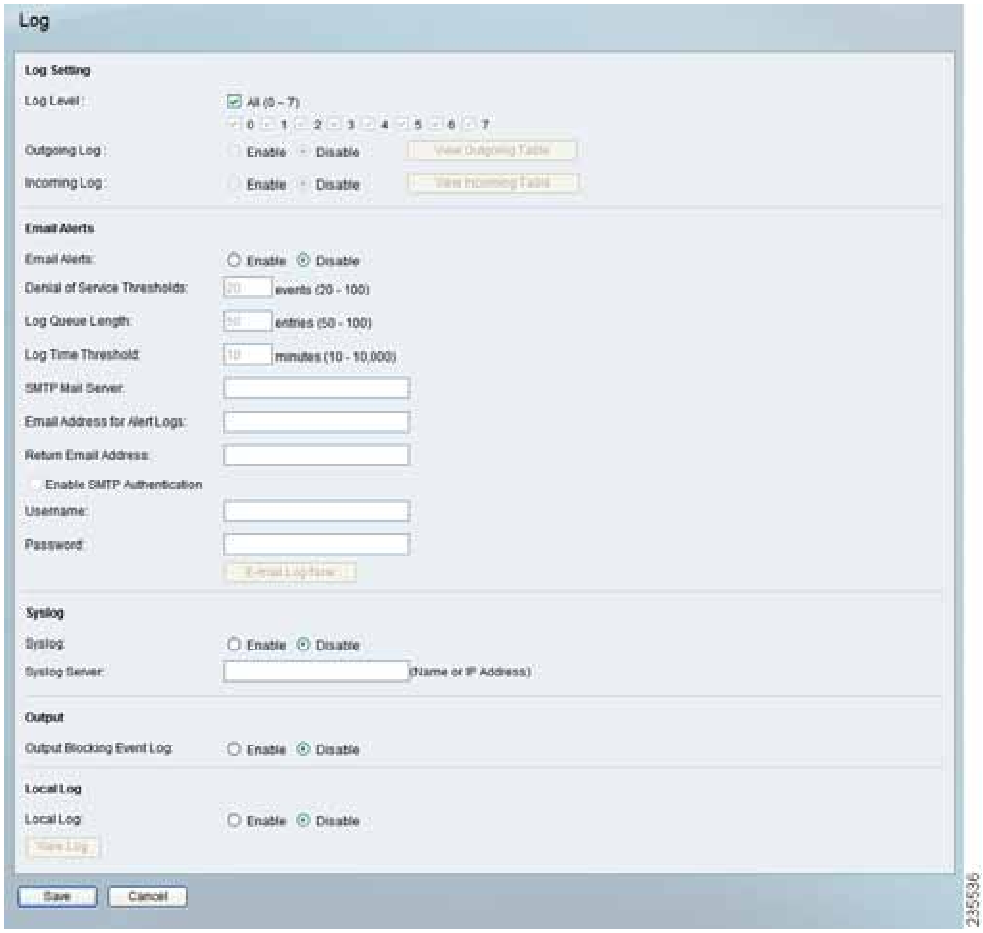
UPnP

You can use Universal Plug and Play (UPnP) to set up public services on your network. When the UPnP function is enabled, Windows XP can add or delete entries to the underlined UPnP Forwarding Table. Some Internet games require enabling UPnP.

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

Administration > Log

Administration > Log



Log

Log Setting

Log Level:	☑ All (0 – 7) ☑ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5 ☐ 6 ☐ 7
Outgoing Log:	○ Enable ● Disable [View Outgoing Table]
Incoming Log:	○ Enable ● Disable [View Incoming Table]

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:	
	[E-mail Log Now]

Syslog

Syslog:	○ Enable ● Disable
Syslog Server:	(Name or IP Address)

Output

Output Blocking Event Log:	○ Enable ● Disable

Local Log

Local Log:	○ Enable ● Disable

Log Setting

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

Log Levels

Level	Severity Name	Description
7	LOG_DEBUG	Debug-level message
6	LOG_INFO	Informational messages only
5	LOG_NOTICE	Normal but significant condition

Log Levels

Level	Severity Name	Description
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 Select **Enable** to cause an email to be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, fill in the email address information in the remaining fields in this section.

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 email alert is sent. The minimum value is 20, and the maximum value is 100.

Log Queue Length The default is **50** entries. The router emails the log if there are more than 50 entries.

Log Time Threshold The default is **10** minutes The router emails 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 email.

Email Address for Alert Logs Enter the email address the Log is to be sent to.

Return Email Address This address will appear as the Sender’s address in the email.

Enable SMTP Authentication If your SMTP server requires Authentication, you can enable it here, and enter the Username and Password.

Email Log Now Press this button to cause the log to be emailed immediately.

Syslog

Enable Syslog Check the box if you want to use this feature.

Syslog Server Enter the IP Address in this field when **Enable Syslog** is checked.

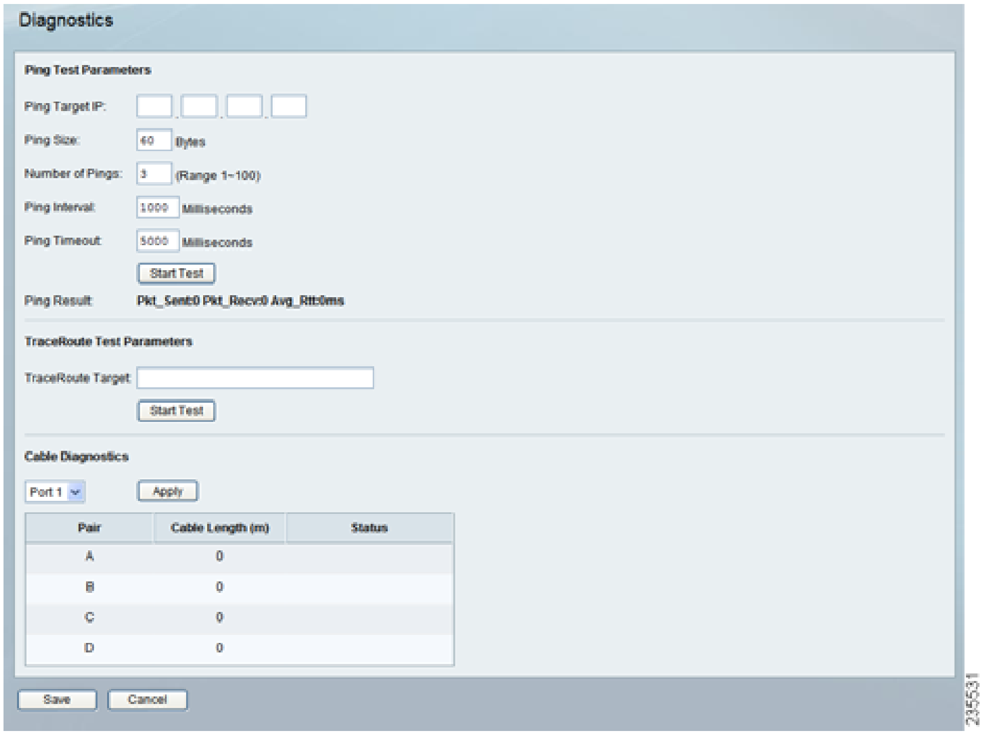
Local Log

Local Log Enable this if you want to see a log of all incoming and outgoing URLs or IP addresses.

View Log Click this button when you wish to view the logs. A new window appears with the log data.

Administration > Diagnostics

Administration > 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 Test Parameters

TraceRoute Target:

Cable Diagnostics

Port 1

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

Ping Test Parameters

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 (milliseconds) between each ping.

Ping Timeout Enter the desired time period (milliseconds). If a response is not received within the defined ping period, the ping is considered to have failed.

Start Test Click this button to begin the test. A new window appears with the test results.

Ping Result 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 window appears with the test results.

Cable Diagnostics

Port Select the port number from the drop-down menu.

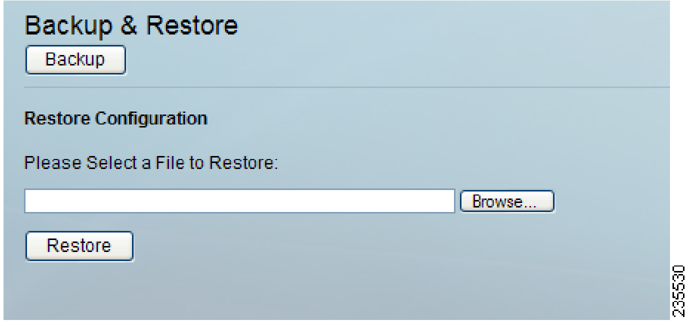
Pair Identifies a specific pair (A, B, C, or D) in the cable. Each cable consists of 8 pins (4 pairs).

Cable Length Displays the length of the cable in meters.

Status Displays the status of the pair.

Administration > Backup & Restore

Administration > Backup & Restore



Backup & Restore

Restore Configuration

Please Select a File to Restore:

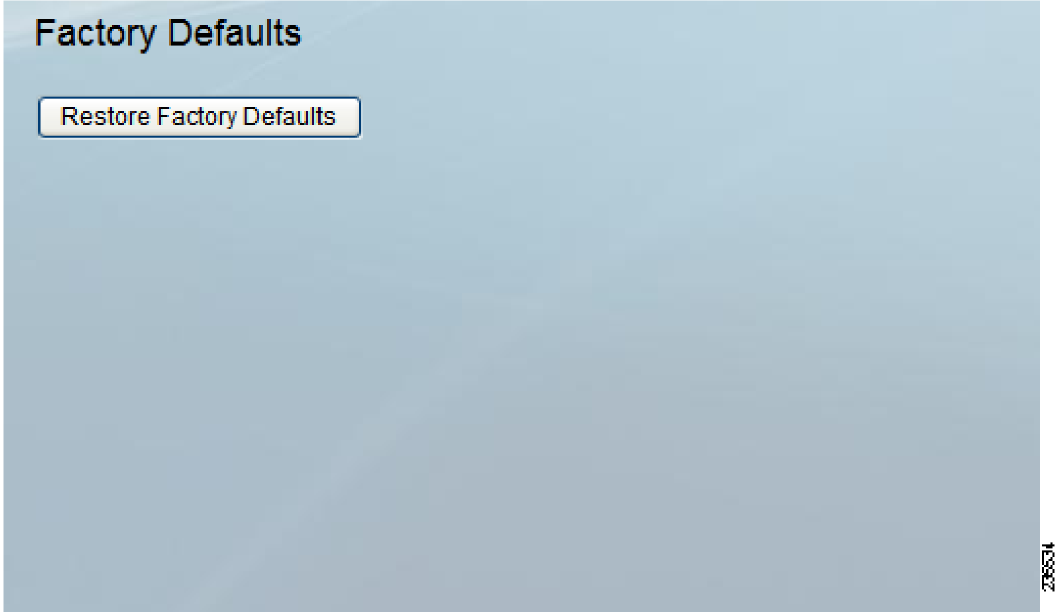
To download a copy of the current configuration and store the file on your PC, click **Backup** to start the download.

Restore Configuration

To restore a previously saved config file back to the router, enter the file name in the field or click **Browse** to select the config file, then click **Restore** to upload the config file.

Administration > Factory Default

Administration > Factory Default



Restore Factory Defaults Click this button to reset all configuration settings to their factory default values. Any previously saved settings will be lost when the default settings are restored. After clicking the button, another window appears. Click **OK** to continue. Another window appears while the system reboots.

Administration > Reboot

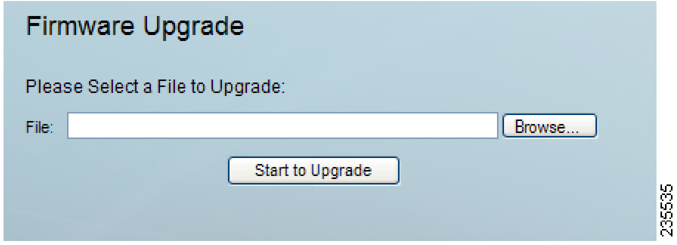
Administration > Reboot

Reboot

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

Administration > Firmware Upgrade

Administration > Firmware Upgrade



Firmware Upgrade

Please Select a File to Upgrade:

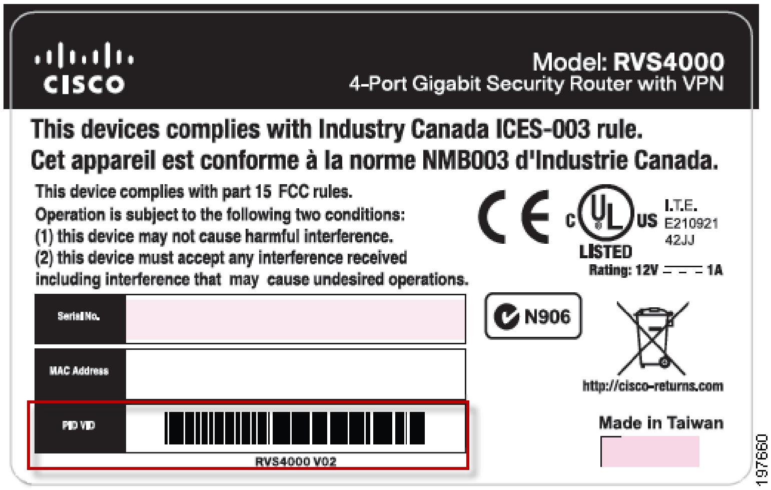
File:

Use this page to upgrade the router by using firmware from Cisco.com. Step-by-step instructions are provided on the next page.

File Type in the name of the extracted firmware upgrade , or click **Browse** to locate the file.

Start to Upgrade Once you have selected the appropriate file, click **Start to Upgrade** and follow the on-screen instructions to upgrade your firmware.

STEP 1 Check the hardware version of the router by referring to the label on the bottom panel. The PIDVID number includes the characters V01 (Version 1) or V02 (Version 2).



Model: **RVS4000**
4-Port Gigabit Security Router with VPN

This devices complies with Industry Canada ICES-003 rule.
Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

This device complies with part 15 FCC rules.
Operation is subject to the following two conditions:
(1) this device may not cause harmful interference.
(2) this device must accept any interference received
including interference that may cause undesired operations.

STEP 2 To find the latest firmware for the router, go to www.cisco.com/go/smallbizfirmware.

STEP 3 Click the link for your router.

STEP 4 Click the **Download Firmware** button.

STEP 5 Continue through the screens to download the most recent firmware.

STEP 6 Extract the firmware file on your computer.

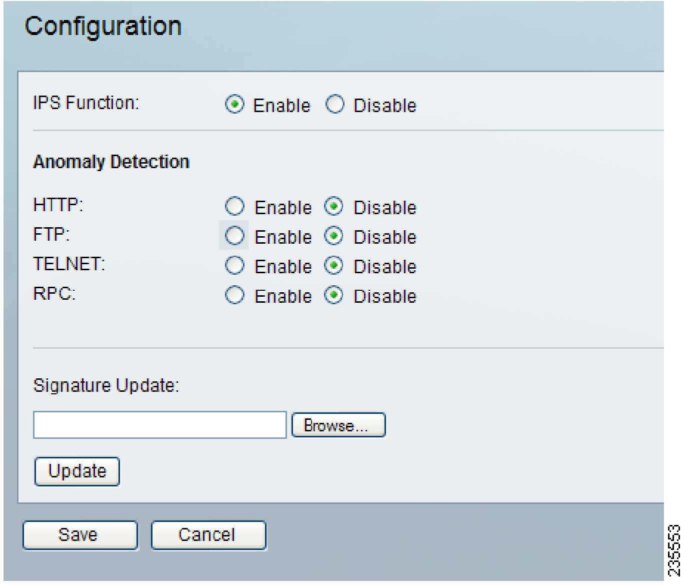
STEP 7 On the Administration > Firmware Upgrade page, click **Browse**, and then locate your file.

STEP 8 Click **Start to Upgrade**.

IPS

IPS > Configuration

IPS > Configuration



Configuration

IPS Function: ● Enable ○ Disable

Anomaly Detection

HTTP: ○ Enable ● Disable
FTP: ○ Enable ● Disable
TELNET: ○ Enable ● Disable
RPC: ○ Enable ● Disable

Signature Update:

IPS Function Select **Enable** to enable or **Disable** to disable the IPS Function.

Anomaly Detection

HTTP Web attack signature is matched. HTTP request decoder decodes UTF-8 (1, 2, and 3 byte) code and normalize URI (according to those evasion methods mentioned in whisker) before pattern match.

FTP FTP Bounce Detection and Inserting telnet opcodes into FTP command stream Detection.

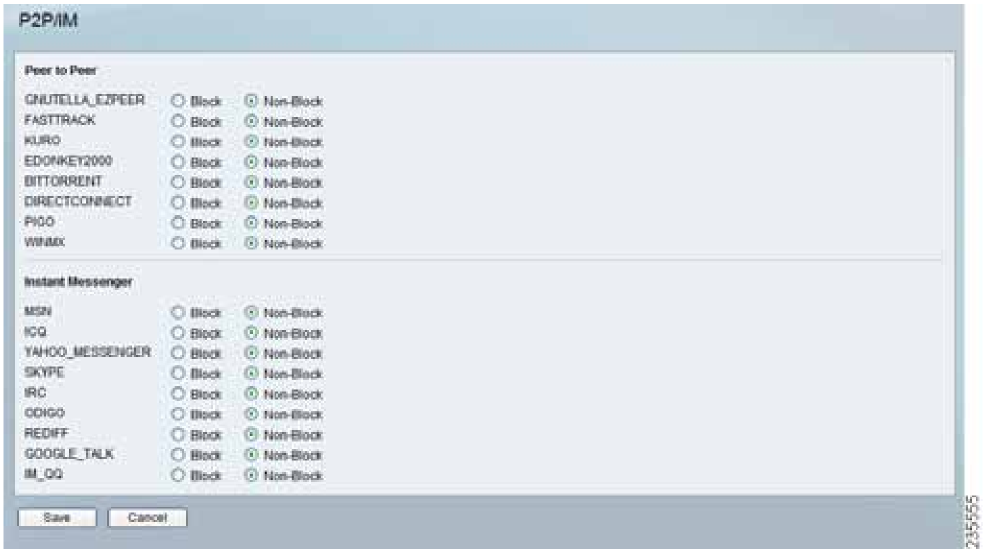
TELNET Normalization of Telnet negotiation strings.

RPC RPC record fragging detection.

Signature Update Before upgrading the signature file, get the Router Intrusion Prevention System (IPS) file from the Cisco website. To find the file, go to www.cisco.com/go/software (registration/login required), and search for RVS4000. After downloading and extracting the file, enter the IPS Signature file name in the Signature Update field, or click **Browse** to find the file. Then click **Update** and follow the on-screen instructions.

IPS > P2P/IM

Peer To Peer



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

Peer to Peer

Peer-to-peer file sharing applications can be blocked (**Block**) or allowed (**Non-Block**). The preconfigured file sharing networks are GNUTELLA (EZPEER), FASTTRACK, KURO, EDONKEY2000, BITTORRENT, DIRECTCONNECT, PIGO, and WINMX.

Instant Messenger

Instant messaging applications can be blocked (**Block**) or allowed (**Non-Block**). The preconfigured instant messaging applications are MSN, ICQ, YAHOO_MESSENGER, SKYPE, IRC, ODIGO, REDIFF, GOOGLE_TALK, and IM_QQ.

IPS > Report

Provides a graphical representation of the level of network traffic and attacks during the last twenty four hours.

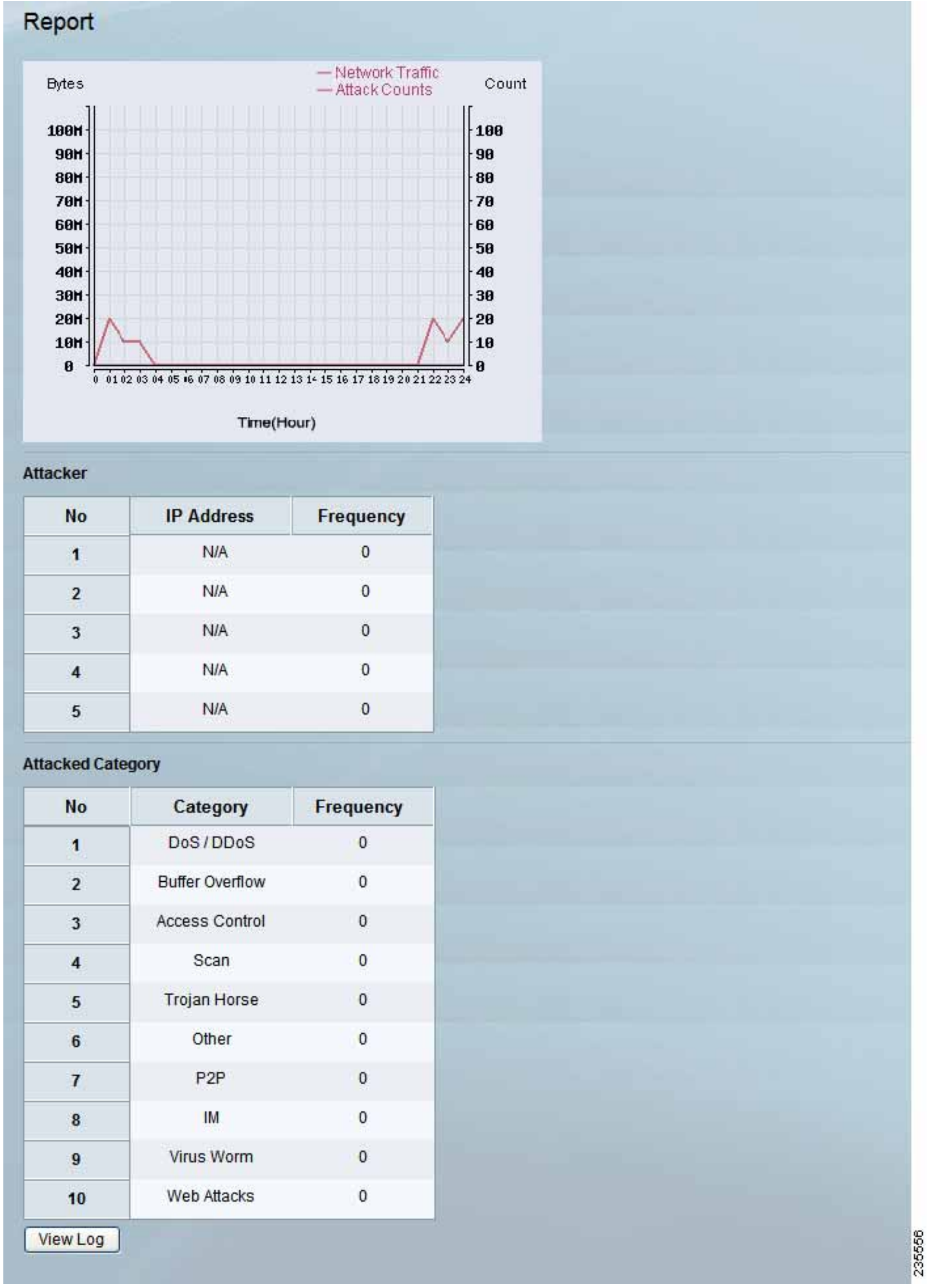
Attacker

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

Attack Category

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

IPS > Report



Report

Attacker

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

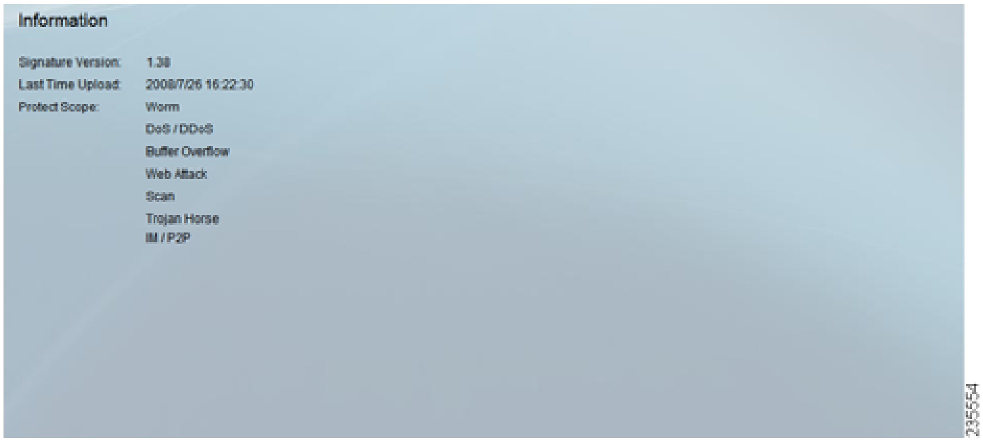
Attacked Category

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

View Log

IPS > Information

IPS > Information



Information

Signature Version: 1.38
Last Time Upload: 2008/7/26 16:22:30
Protect Scope: Worm
DoS / DDoS
Buffer Overflow
Web Attack
Scan
Trojan Horse
IM / P2P

Signature Version Displays the version of the signature patterns in the router that protects against malicious threats.

Last Time Upload This displays when the signature patterns in the router were last updated.

Protect Scope Lists the types of attacks that the router's IPS feature protects against.

L2 Switch

L2 Switch > 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 to implement network changes.

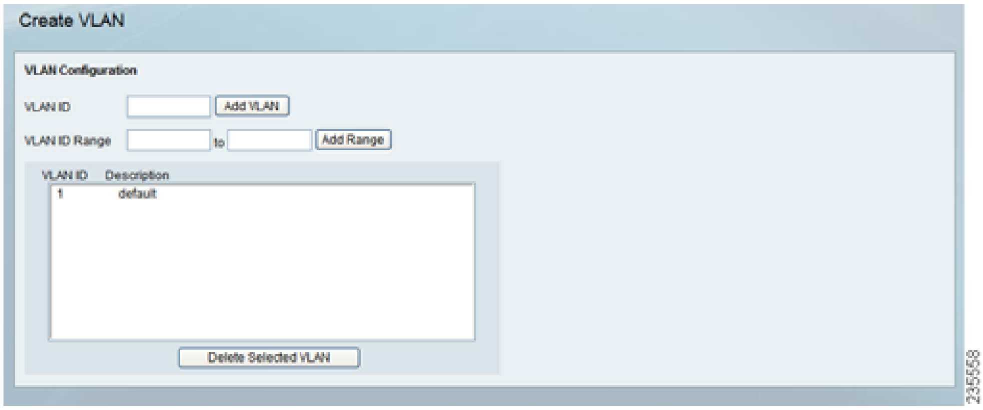
VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

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.

The RVS4000 supports up to 4 VLANs, including the default VLAN.

L2 Switch > Create VLAN



VLAN ID	Description
1	default

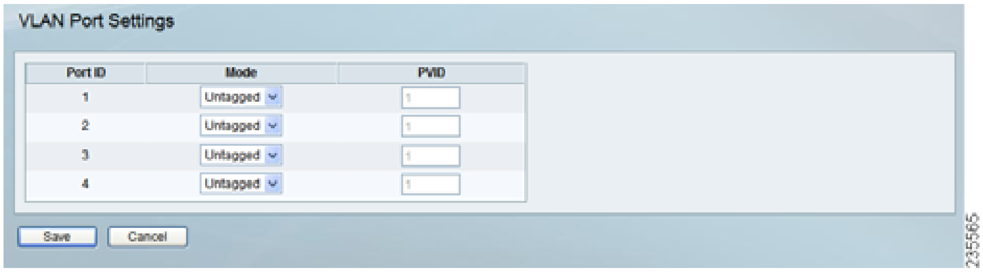
VLAN ID The VLAN ID number. This can be any number from 2 to 3290, or from 3293 to 4094. (VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 3291-3292 are reserved and cannot be used.) To create a VLAN, enter the ID number and click **Add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

L2 Switch > VLAN Port Setting

L2 Switch > VLAN Port Setting



VLAN Port Settings

Port ID	Mode	PVID
1	Untagged	1
2	Untagged	1
3	Untagged	1
4	Untagged	1

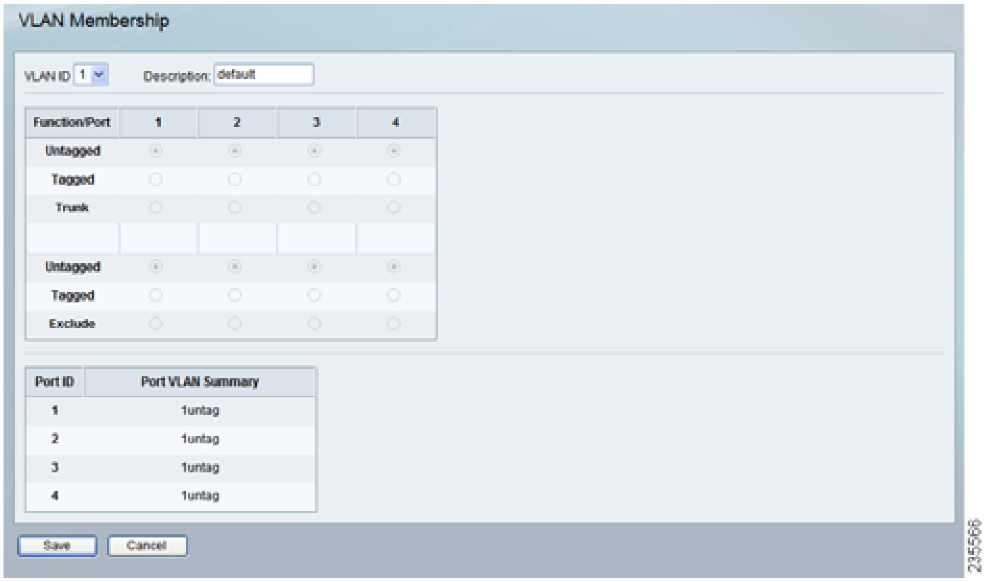
Port ID Displays the port number from **1** to **4**.

Mode Select the mode of the port, either **Trunk**, **Untagged**, or **Tagged**. The default is **Untagged**. In Trunk mode, incoming and outgoing frames can be either tagged or untagged; incoming untagged frames are tagged with the default PVID (Port VLAN ID). In Untagged mode, all incoming and outgoing frames are untagged. In Tagged mode, all incoming and outgoing frames must be tagged; all untagged frames are dropped.

PVID The Port VLAN ID (PVID) assigned to untagged frames received on the interface. The default is **1**. If the Mode is Tagged, the port receives only tagged frames and so the port has no PVID.

L2 Switch > VLAN Membership

L2 Switch > VLAN Membership



VLAN Membership

VLAN ID: 1

Description: default

Function/Port	1	2	3	4
Untagged	●	●	●	●
Tagged	○	○	○	○
Trunk	○	○	○	○
Untagged	●	●	●	●
Tagged	○	○	○	○
Exclude	○	○	○	○

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

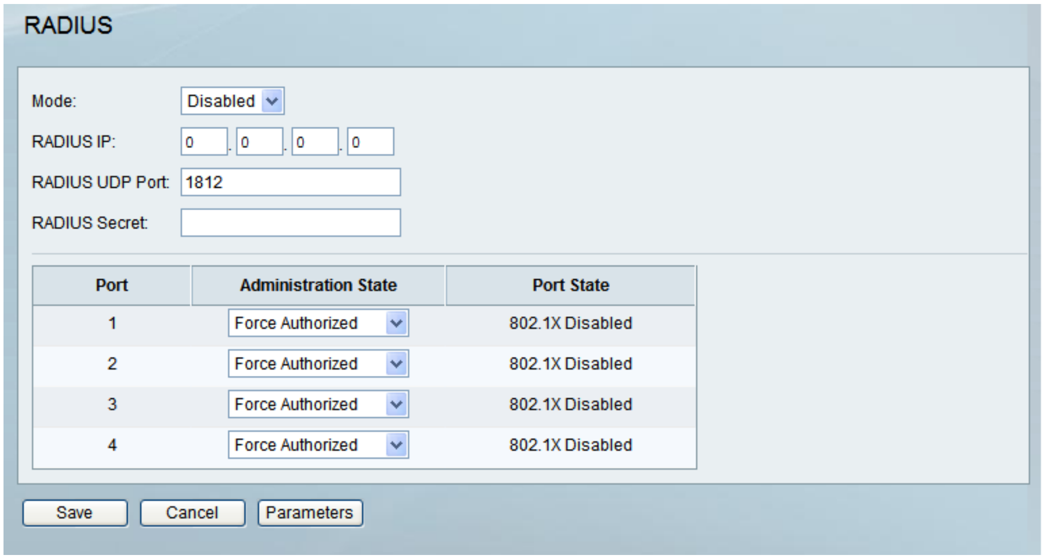
VLAN ID Select the VLAN whose membership you want to configure.

Description Enter a VLAN group name of up to 50 characters.

Function/Port table The top half of the table indicates each port’s current mode (Untagged, Tagged, or Trunk). The lower half of the table is used to assign port membership for the selected VLAN. The default for each port is **Exclude** (the port is not a member of the VLAN). To make a port a member of the VLAN, select the applicable mode(s). For example, if the port mode is Untagged, select Untagged; if the mode is Tagged, select Tagged; if the mode is Trunk, select either Tagged or Untagged.

L2 Switch > RADIUS

L2 Switch > RADIUS



RADIUS

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

Mode Select **Enabled** or **Disabled** from the drop-down menu to enable or disable RADIUS.

RADIUS IP Enter the Server IP address.

RADIUS UDP Port Enter the UDP port. The UDP port is used to verify the RADIUS server authentication.

RADIUS Secret Enter the Key string for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS server encryption key. If no host-specific value is specified, the global value applies to each host.

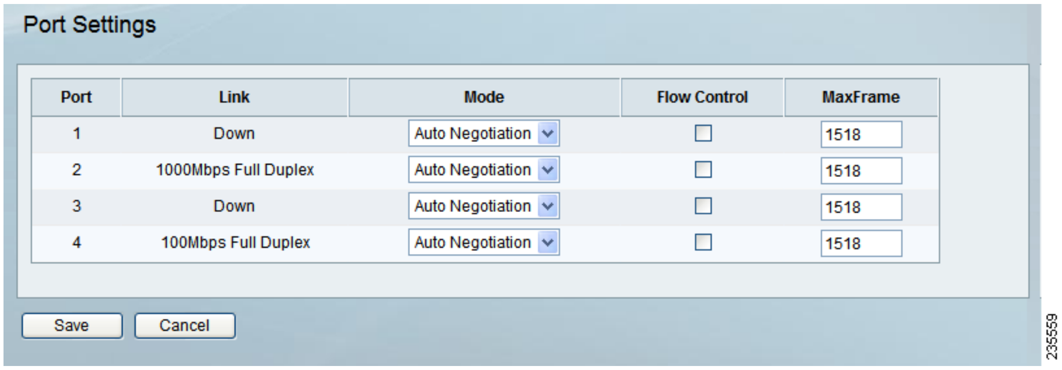
Administration State Specifies the port authorization state. The possible field values are:

- **Auto** The controlled port state is set by the Authentication method.
- **Force Authorized** The controlled port state is set to Force-Authorized (forward traffic).
- **Force Unauthorized** The controlled port state is set to Force-Unauthorized (discard traffic).

Port State Displays the state of the selected port.

L2 Switch > Port Setting

L2 Switch > Port Setting



Port Settings

Port	Link	Mode	Flow Control	MaxFrame
1	Down	Auto Negotiation	□	1518
2	1000Mbps Full Duplex	Auto Negotiation	□	1518
3	Down	Auto Negotiation	□	1518
4	100Mbps Full Duplex	Auto Negotiation	□	1518

Port Displays the physical port number.

Link Displays the port duplex mode and speed. **Full Duplex** indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. **Half Duplex** indicates that the interface supports transmission between the device and the client in only one direction at a time.

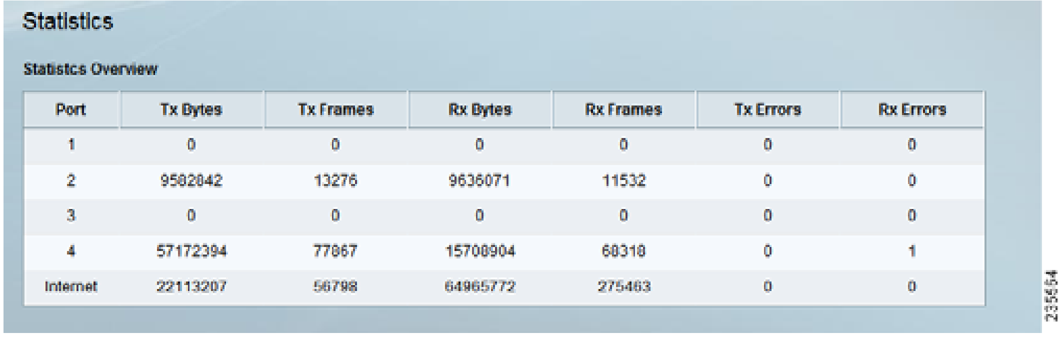
Mode Select the port duplex mode and speed from the drop-down menu. You can also select **Auto Negotiation**, which is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

Flow Control Displays the flow control status on the port. Operates when a port is in Full duplex mode.

MaxFrame Displays the maximum frame size the port can receive and send.

L2 Switch > Statistics

L2 Switch > Statistics



Statistics

Statistcs Overview

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	9582842	13276	9636071	11532	0	0
3	0	0	0	0	0	0
4	57172394	77867	15708904	68318	0	1
Internet	22113207	56798	64865772	275463	0	0

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.

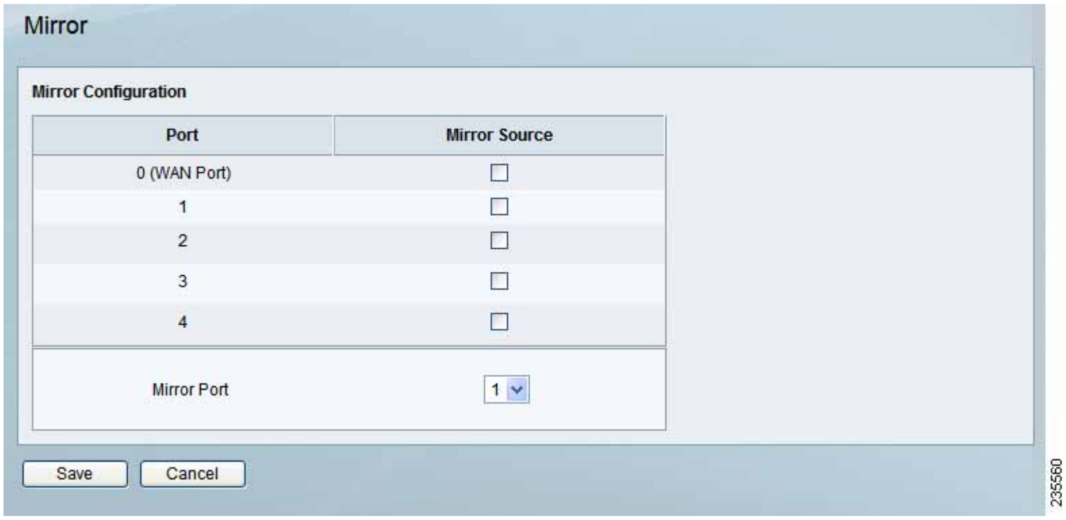
Rx Frames Displays the number of Frames received on the selected port.

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.

L2 Switch > Port Mirroring

L2 Switch > Port Mirroring



Mirror

Mirror Configuration

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

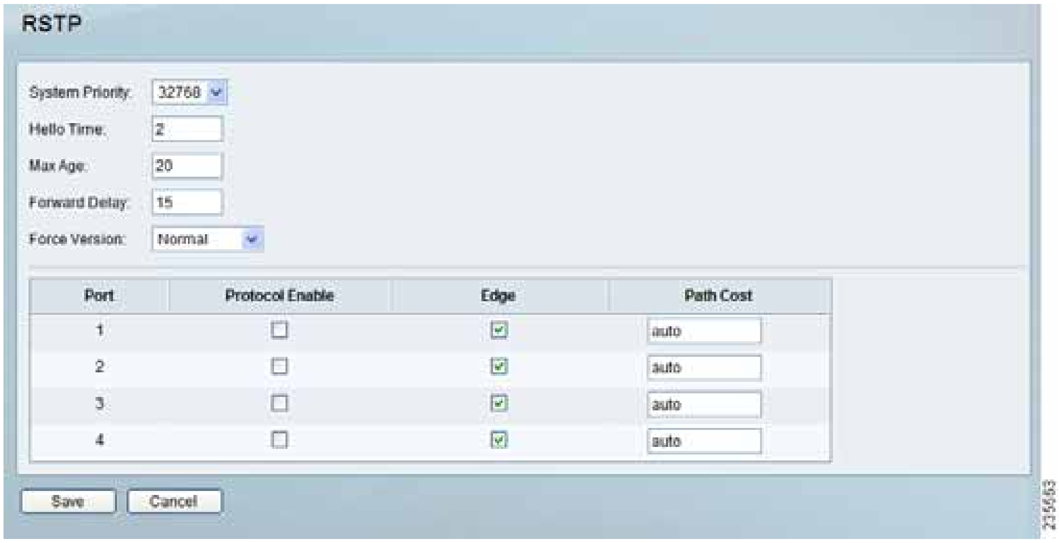
Mirror Port: 1

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.

L2 Switch > RSTP

L2 Switch > RSTP



RSTP

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

The RSTP (Rapid Spanning Tree Protocol) protocol 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 **32768**.

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 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**).

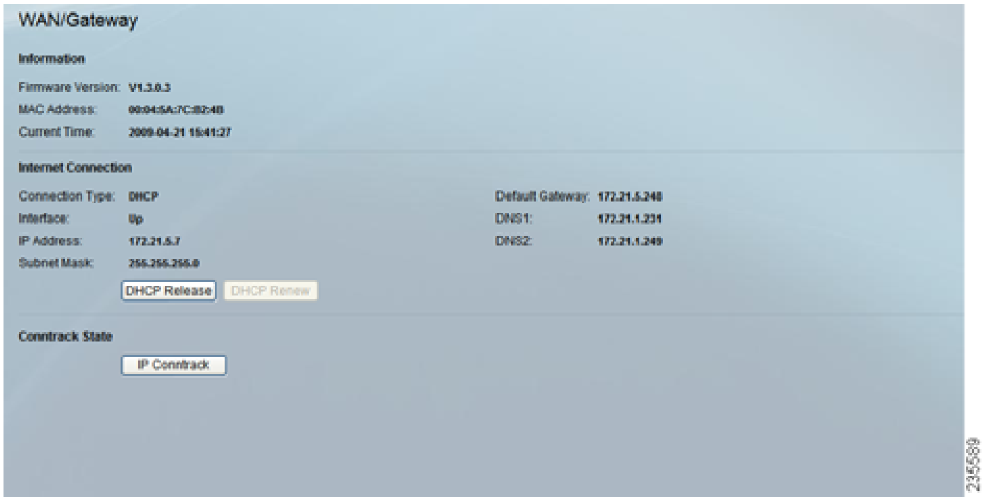
Edge Check this box to specify that the associated port is an edge port (end station). Uncheck the box to specify that the associated port is a link (bridge) to another STP device. The default is checked (**edge port**).

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

Status

Status > Gateway

Status > Gateway



WAN/Gateway

Information

Firmware Version: V1.3.0.3
MAC Address: 00:04:5A:7C:82:4B
Current Time: 2009-04-21 15:41:27

Internet Connection

Connection Type: DHCP
Interface: Up
IP Address: 172.21.5.7
Subnet Mask: 255.255.255.0
Default Gateway: 172.21.5.248
DNS1: 172.21.1.231
DNS2: 172.21.1.249

Conntrack State

Firmware Version Displays the Gateway's current firmware.

MAC Address Displays the Gateway MAC Address, as seen by your ISP.

Current Time Displays the time, based on the time zone you selected on the Setup menu.

Internet Connection

Connection Type Displays the type of the connection.

Interface Displays the Gateway Internet Interface.

IP Address Displays the Gateway Internet IP Address.

Subnet Mask Displays the Subnet Mask for the IP address above.

Default Gateway Displays your ISP's Gateway.

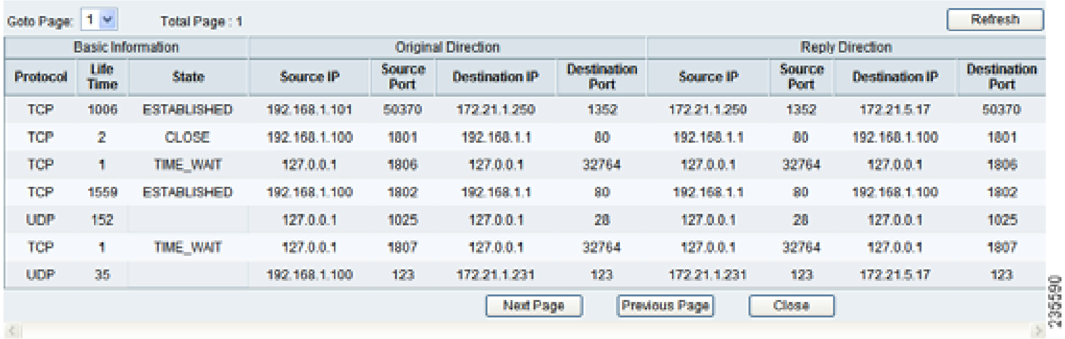
DNS 1-2 Displays the DNS (Domain Name System) IP addresses currently used by this Gateway.

IP Conntrack Click this button to display the IP Conntrack window.

IP Conntrack

The IP Conntrack (Connection Tracking) window 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 Go to Page drop-down menu. To see the latest information, click **Refresh**. Click **Close** to return to the Status > Gateway window.

Status > Gateway > IP Conntrack

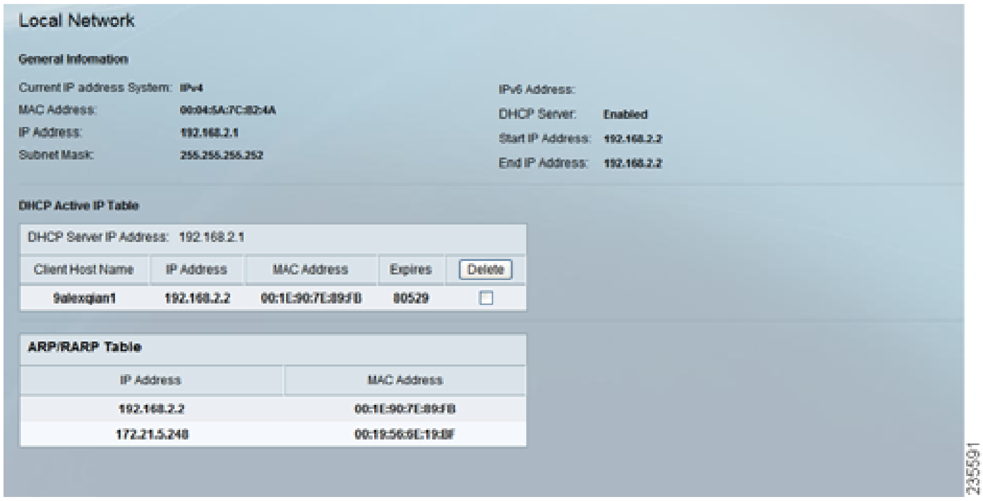


Goto Page: 1   Total Page : 1

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	1006	ESTABLISHED	192.168.1.101	50370	172.21.1.250	1352	172.21.1.250	1352	172.21.5.17	50370
TCP	2	CLOSE	192.168.1.100	1801	192.168.1.1	80	192.168.1.1	80	192.168.1.100	1801
TCP	1	TIME_WAIT	127.0.0.1	1806	127.0.0.1	32764	127.0.0.1	32764	127.0.0.1	1806
TCP	1559	ESTABLISHED	192.168.1.100	1802	192.168.1.1	80	192.168.1.1	80	192.168.1.100	1802
UDP	152		127.0.0.1	1025	127.0.0.1	28	127.0.0.1	28	127.0.0.1	1025
TCP	1	TIME_WAIT	127.0.0.1	1807	127.0.0.1	32764	127.0.0.1	32764	127.0.0.1	1807
UDP	35		192.168.1.100	123	172.21.1.231	123	172.21.1.231	123	172.21.5.17	123

Status > Local Network

Status > Local Network



Local Network

General Infomation

Current IP address System: IPv4
MAC Address: 00:04:5A:7C:82:4A
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.252

IPv6 Address:
DHCP Server: Enabled
Start IP Address: 192.168.2.2
End IP Address: 192.168.2.2

DHCP Active IP Table

DHCP Server IP Address: 192.168.2.1

Client Host Name	IP Address	MAC Address	Expires	Delete
9alexqian1	192.168.2.2	00:1E:90:7E:89:FB	80529	□

ARP/RARP Table

IP Address	MAC Address
192.168.2.2	00:1E:90:7E:89:FB
172.21.5.248	00:19:56:6E:19:BF

Current IP address System This shows the current system.

MAC Address The router MAC Address, as seen on your local, Ethernet network.

IP Address The Internet IP Address.

Subnet Mask The Subnet Mask for the IP address above.

IPv6 Address The IPv6 IP address, if applicable.

DHCP Server The status of the router’s DHCP server function.

Start IP Address The first address in the range of IP addresses used by the DHCP Server.

End IP Address The final address in the range of IP addresses used by the DHCP Server.

DHCP Client Table Click this button to open a window that displays the PCs that use the router as a DHCP server. The DHCP Client Table window displays all DHCP clients (PCs and other network devices) with this information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the length of time before their assigned IP addresses expire.

ARP/RARP Table Click this button to open a window that displays the PCs that use the router as an ARP/RARP server. The ARP/RARP Table window displays all ARPs/RARPs (PCs and other network devices) with this information: IP addresses and MAC addresses.

6

Using the VPN Setup Wizard

This chapter explains how to use the VPN Setup Wizard. It includes these sections:

VPN Setup Wizard

Now you can configure a gateway-to-gateway VPN tunnel between two VPN routers in a fast and efficient way by using the VPN Setup Wizard. The VPN Setup Wizard works with users running Microsoft Windows 2000, XP, and Vista. This document describes how to run the VPN Setup Wizard.

Before You Begin

The VPN Setup Wizard works with these routers:

- Cisco RVS4000 4-Port Gigabit Security Router with VPN
- Cisco WRVS4400N v1.1 Wireless-N 4-Port Gigabit Security Router with VPN
- Cisco WRVS4400N v2 Wireless-N 4-Port Gigabit Security Router with VPN

Use these instructions to configure required data using the Web Administrator Interface. For instructions on the Web Administrator Interface, see the Administration Guide for your router.

STEP 1 Click **Firewall > Basic Settings**.

STEP 2 Enable Remote Management and enter **8080** in the Port field. Please note that you cannot enter any other value if you want to use the VPN Wizard. Also, make sure that HTTPS has been selected.

STEP 3 Click **Save**.

STEP 4 Click **VPN > Summary** and make sure the **Tunnel(s) available** are not zero.

STEP 5 Ensure that the LAN IP addresses of routers with VPN are in different subnets in order for the VPN connection to work.

NOTE The VPN Setup Wizard assumes that no firewall/NAT device sits in front of the VPN router.

Running the VPN Setup Wizard

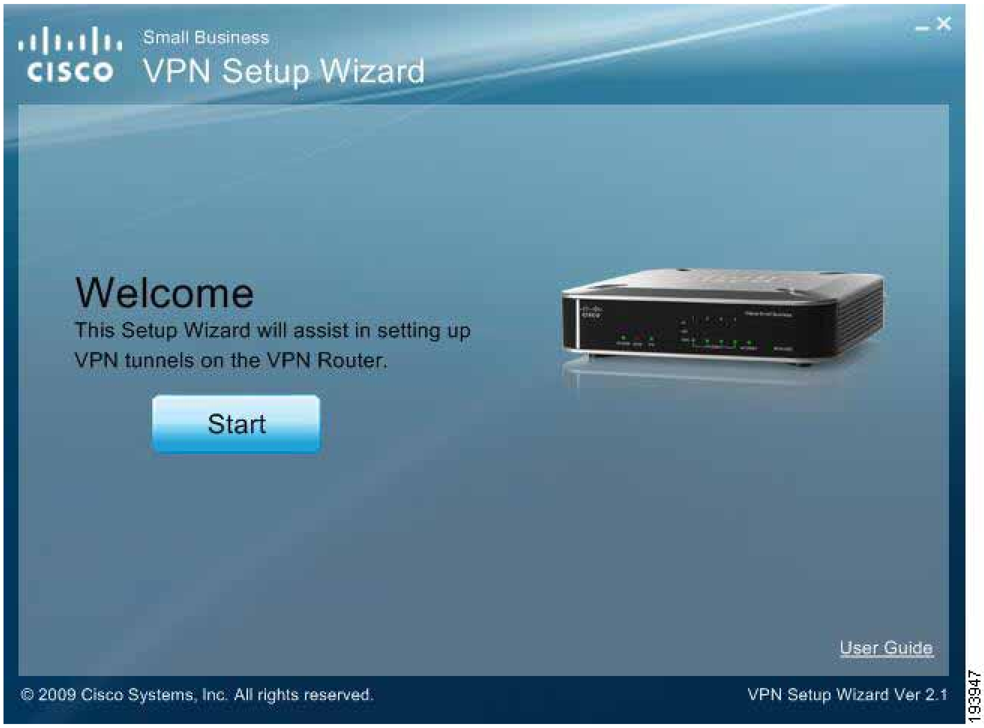
STEP 1 Access the VPN Setup Wizard in one of two ways:

- If you have an RVS4000, WRVS4400N v1.1, or WRVS4400N v2 Installation CD-ROM, insert it into your CD-ROM drive.
- Download the VPN Setup Wizard from the Cisco Support site for your router.

STEP 2 Go to the Start menu and click **Run**. In the field provided, enter:
D:\VPN Setup Wizard.exe

STEP 3 When the Welcome window appears, click **Start**.

Welcome Window

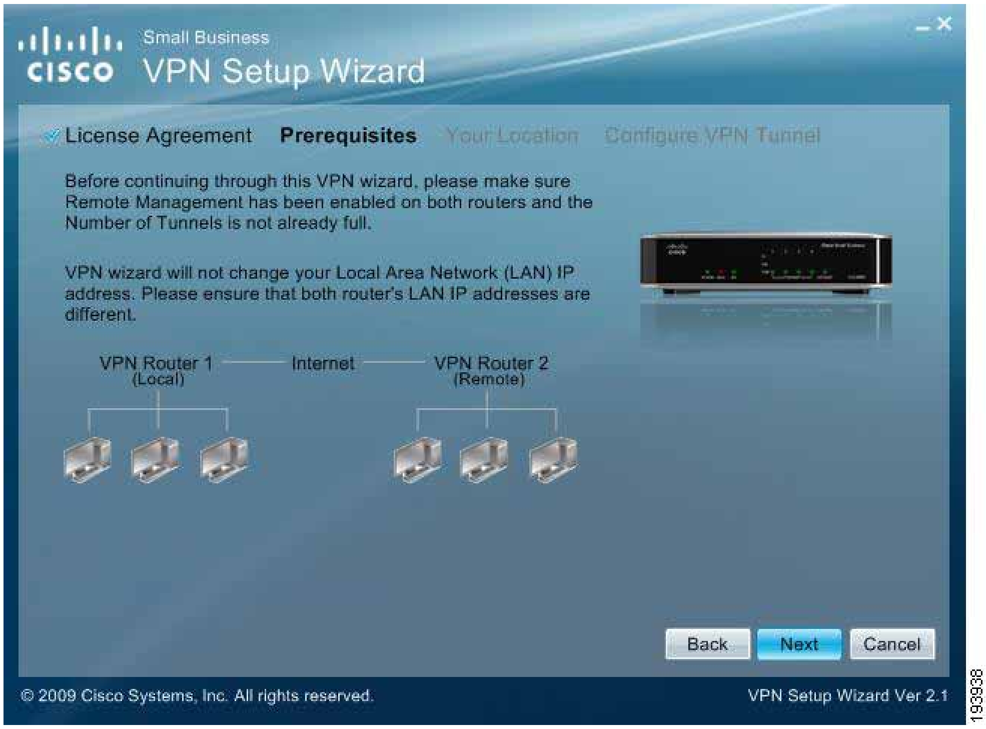


Welcome

This Setup Wizard will assist in setting up VPN tunnels on the VPN Router.

STEP 4 Read the information about the wizard, and then click **Next** to proceed.

Informational Window



Small Business

VPN Setup Wizard

✓ License Agreement **Prerequisites** Your Location Configure VPN Tunnel

Before continuing through this VPN wizard, please make sure Remote Management has been enabled on both routers and the Number of Tunnels is not already full.

VPN wizard will not change your Local Area Network (LAN) IP address. Please ensure that both router's LAN IP addresses are different.

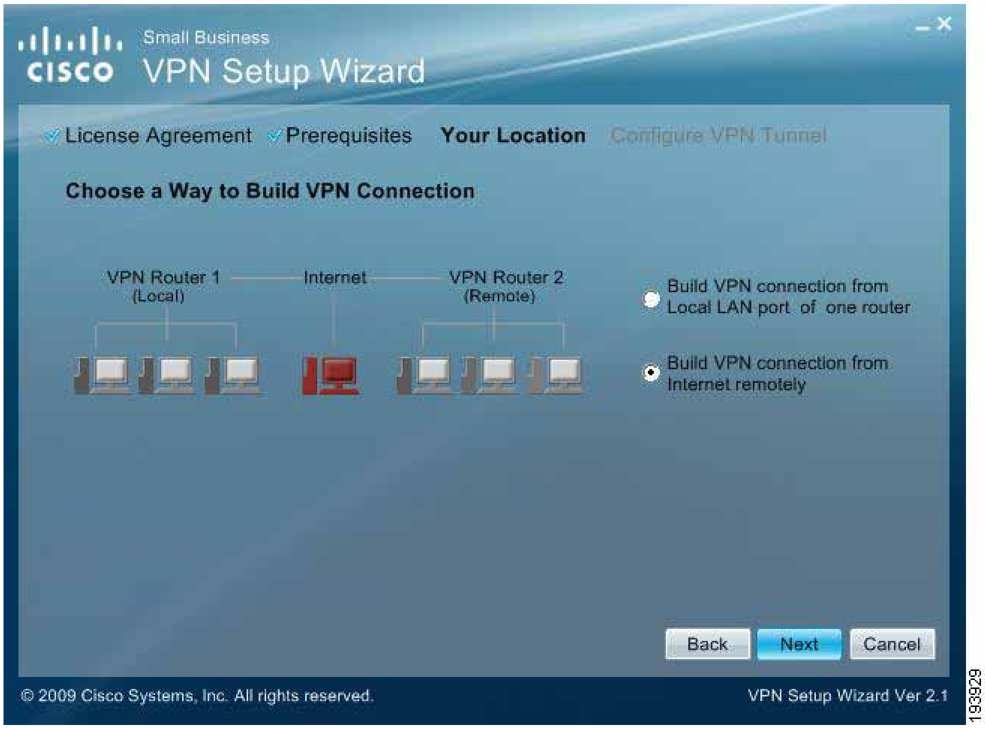
© 2009 Cisco Systems, Inc. All rights reserved.

VPN Setup Wizard Ver 2.1

STEP 5 Choose one method to build the VPN connection:

- If your PC is local to one of the two routers, choose **Build VPN connection from Local LAN port of one router**, click **Next**, and continue with these instructions.
- If your PC is remote to the routers, choose **Build VPN connection from Internet remotely**, and see the **"Building Your VPN Connection Remotely," on page 108** for instructions on this type of installation.

Build VPN Connection Remotely



Choose a Way to Build VPN Connection

○ Build VPN connection from Local LAN port of one router

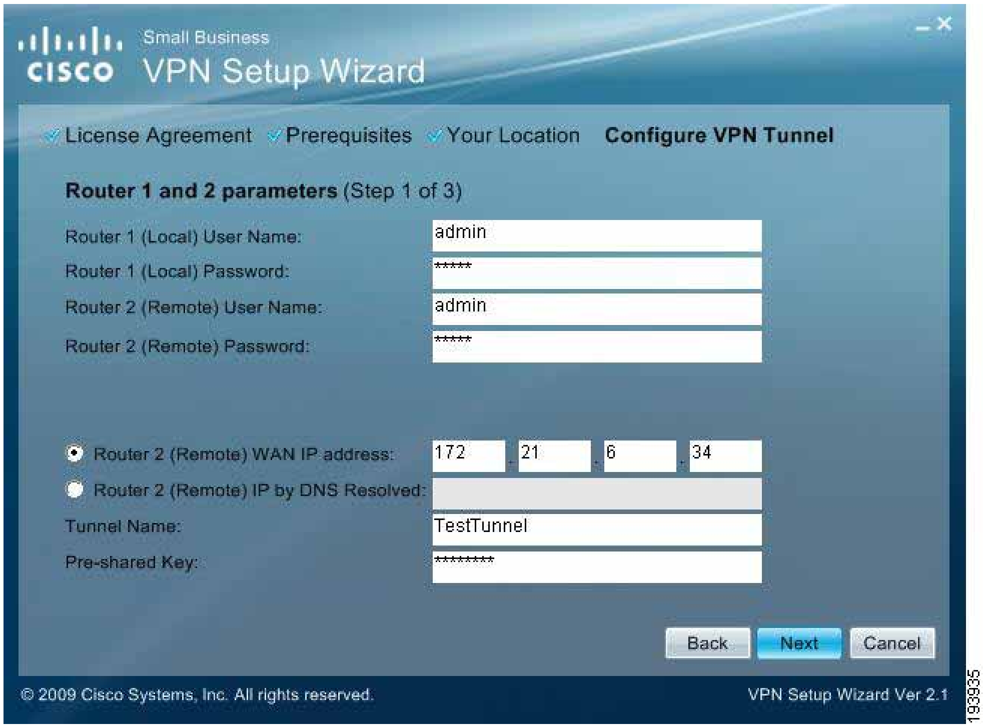
● Build VPN connection from Internet remotely

© 2009 Cisco Systems, Inc. All rights reserved.

VPN Setup Wizard Ver 2.1

STEP 6 Enter the required data in the Configure VPN Tunnel window and click **Next** to continue.

Configure VPN Tunnel


Small Business
cisco VPN Setup Wizard
✓ License Agreement ✓ Prerequisites ✓ Your Location **Configure VPN Tunnel**
Back
Next
Cancel
© 2009 Cisco Systems, Inc. All rights reserved.
VPN Setup Wizard Ver 2.1
193935

Router 1 and 2 parameters (Step 1 of 3)

Router 1 (Local) User Name: admin

Router 1 (Local) Password: *****

Router 2 (Remote) User Name: admin

Router 2 (Remote) Password: *****

● Router 2 (Remote) WAN IP address: 172 . 21 . 6 . 34

○ Router 2 (Remote) IP by DNS Resolved:

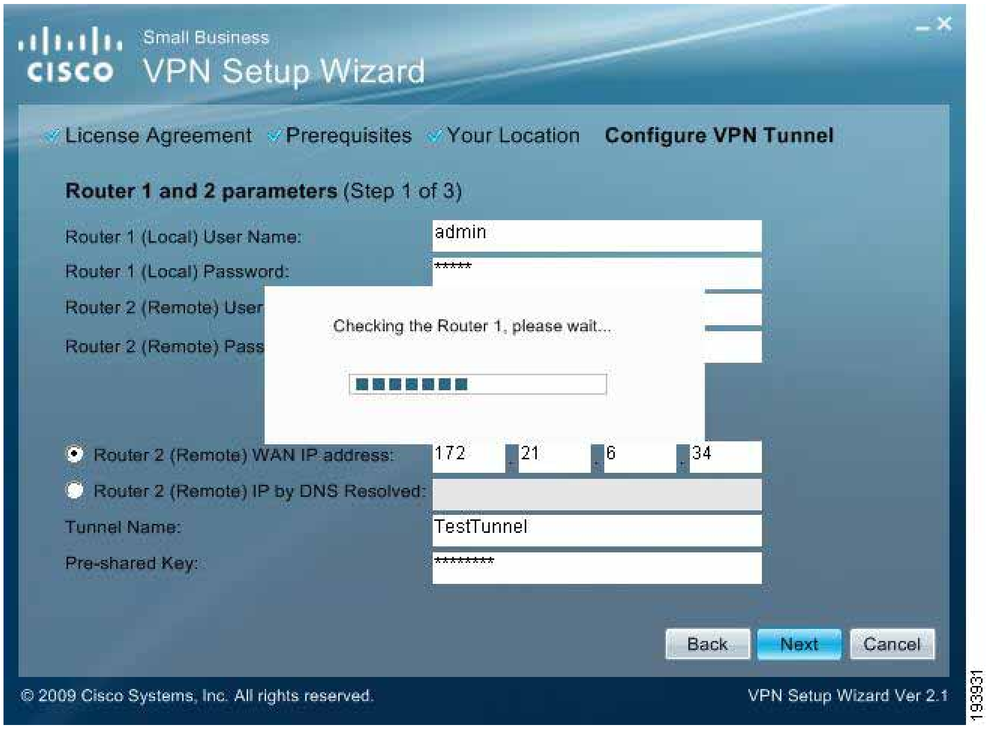
Tunnel Name: TestTunnel

Pre-shared Key: ********

- **Router 1 User Name**: Enter the user name of the Router 1.
- **Router 1 Password**: Enter the password of the Router 1.
- **Router 2 User Name**: Enter the user name of the Router 2.
- **Router 2 Password**: Enter the password of the Router 2.
- **Tunnel Name**: Enter a name for this tunnel.
- **Pre-shared Key**: IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both character 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.
- **Router 2 WAN IP address**: Enter the WAN IP address of Router 2.
- **Router 2 IP by DNS Resolved**: Enter the DDNS Domain Name of Router 2 if it does not have a static IP address for its internet connection.

The router configuration is checked.

Check Router Configuration



Small Business
VPN Setup Wizard
✓ License Agreement ✓ Prerequisites ✓ Your Location **Configure VPN Tunnel**

Router 1 and 2 parameters (Step 1 of 3)

Router 1 (Local) User Name: admin

Router 1 (Local) Password: *****

Router 2 (Remote) User

Router 2 (Remote) Pass

Checking the Router 1, please wait...

● Router 2 (Remote) WAN IP address: 172 . 21 . 6 . 34

○ Router 2 (Remote) IP by DNS Resolved:

Tunnel Name: TestTunnel

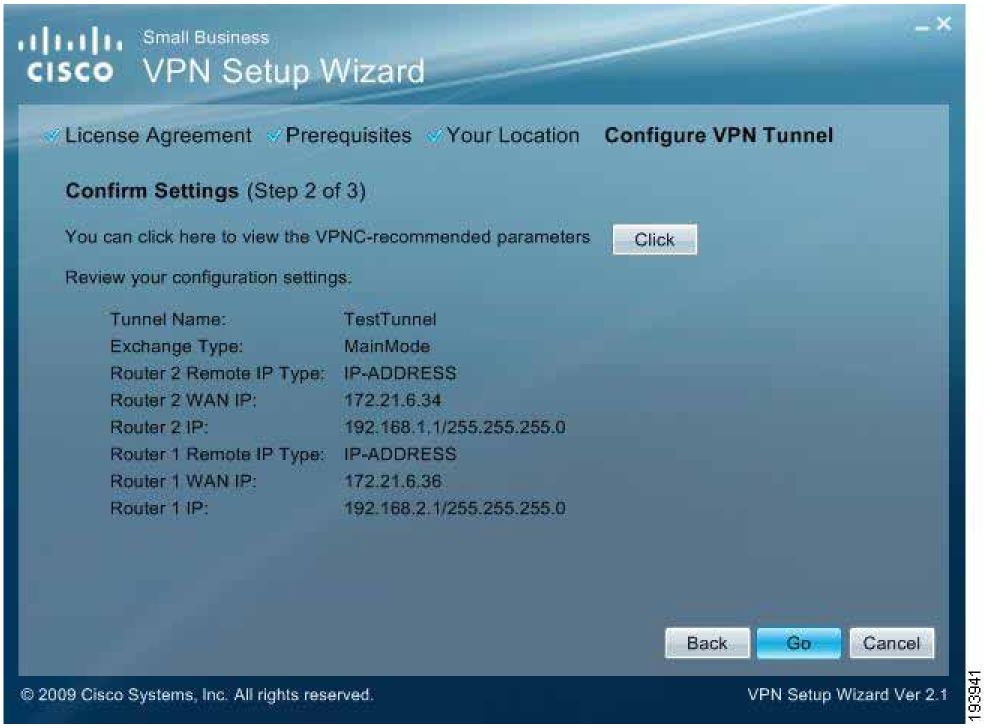
Pre-shared Key: *********

© 2009 Cisco Systems, Inc. All rights reserved.

VPN Setup Wizard Ver 2.1

STEP 7 When the Summary window appears, use the **Click** button to view the VPNC Summary window.

Summary Window



Confirm Settings (Step 2 of 3)

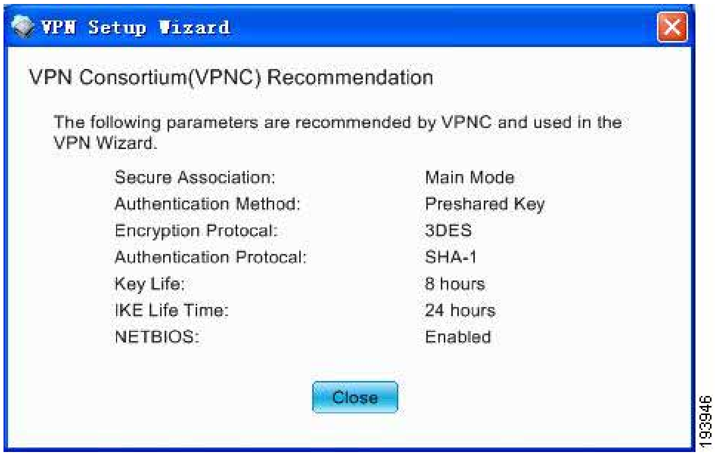
You can click here to view the VPNC-recommended parameters

Review your configuration settings.

Tunnel Name:	TestTunnel
Exchange Type:	MainMode
Router 2 Remote IP Type:	IP-ADDRESS
Router 2 WAN IP:	172.21.6.34
Router 2 IP:	192.168.1.1/255.255.255.0
Router 1 Remote IP Type:	IP-ADDRESS
Router 1 WAN IP:	172.21.6.36
Router 1 IP:	192.168.2.1/255.255.255.0

STEP 8 Review the settings, as needed. Click **Close** when you are ready to continue.

VPNC Summary Window



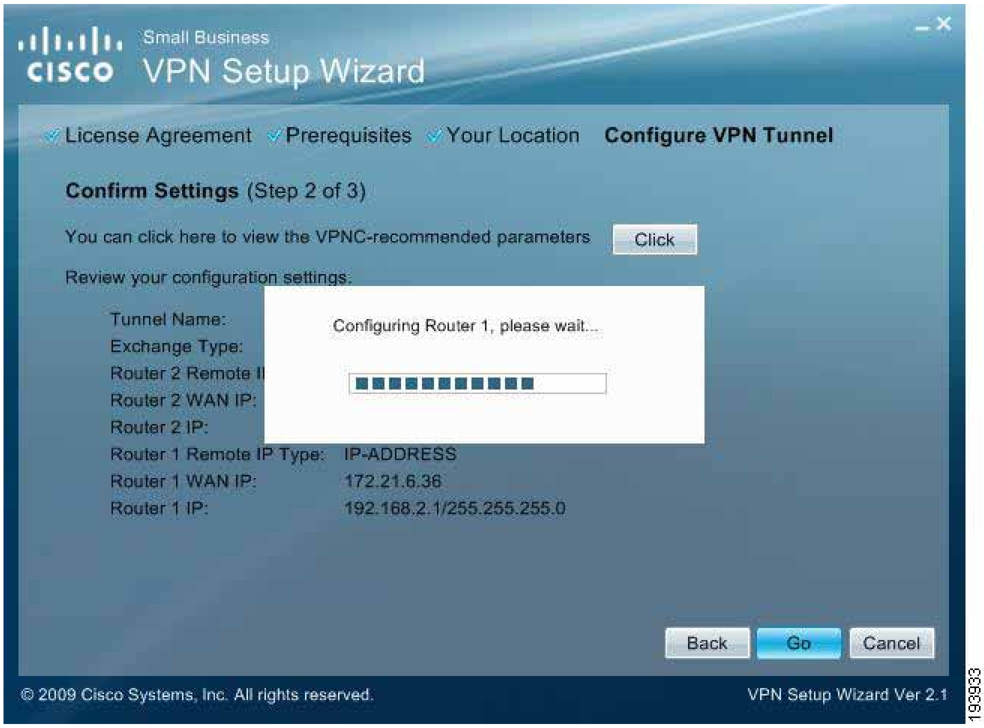
VPN Consortium(VPNC) Recommendation

The following parameters are recommended by VPNC and used in the VPN Wizard.

Secure Association:	Main Mode
Authentication Method:	Preshared Key
Encryption Protocal:	3DES
Authentication Protocal:	SHA-1
Key Life:	8 hours
IKE Life Time:	24 hours
NETBIOS:	Enabled

STEP 9 In the Summary window, if all your entries appear correct, click **Go**. Otherwise click **Back** to go back and make any corrections.

Configure the Router



Small Business
VPN Setup Wizard

✓ License Agreement ✓ Prerequisites ✓ Your Location **Configure VPN Tunnel**

Confirm Settings (Step 2 of 3)

You can click here to view the VPNC-recommended parameters [Click]

Review your configuration settings:

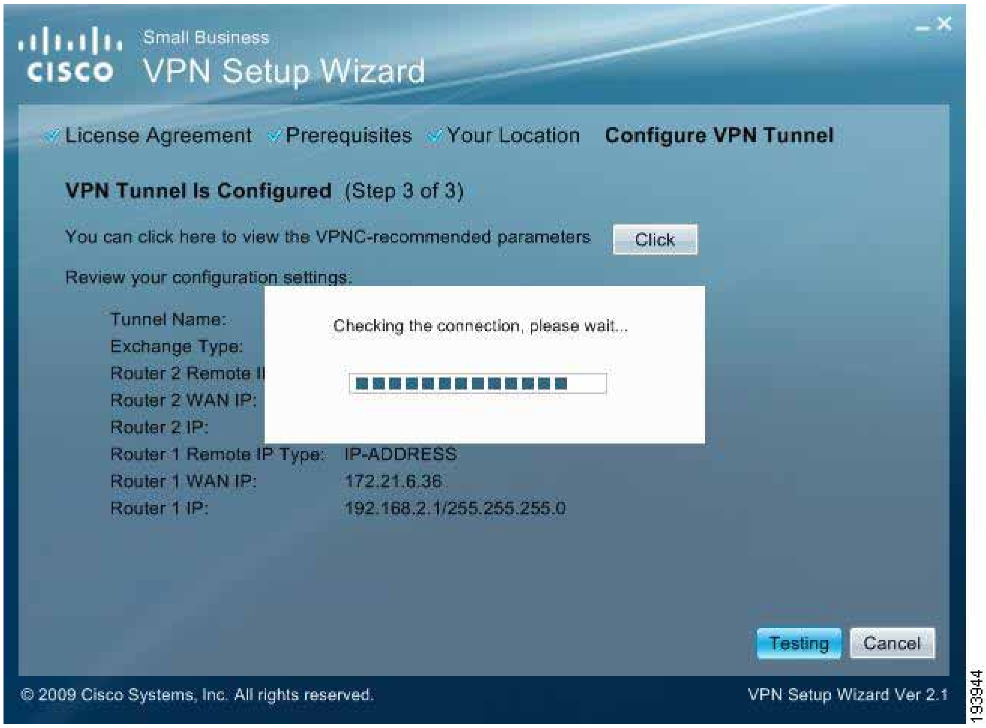
Tunnel Name:
Exchange Type:
Router 2 Remote I
Router 2 WAN IP:
Router 2 IP:
Router 1 Remote IP Type: IP-ADDRESS
Router 1 WAN IP: 172.21.6.36
Router 1 IP: 192.168.2.1/255.255.255.0

Configuring Router 1, please wait...

© 2009 Cisco Systems, Inc. All rights reserved.

STEP 10 Click **Testing** to make sure the connection is successfully established.

Test the Connection



VPN Tunnel Is Configured (Step 3 of 3)

You can click here to view the VPNC-recommended parameters

Review your configuration settings.

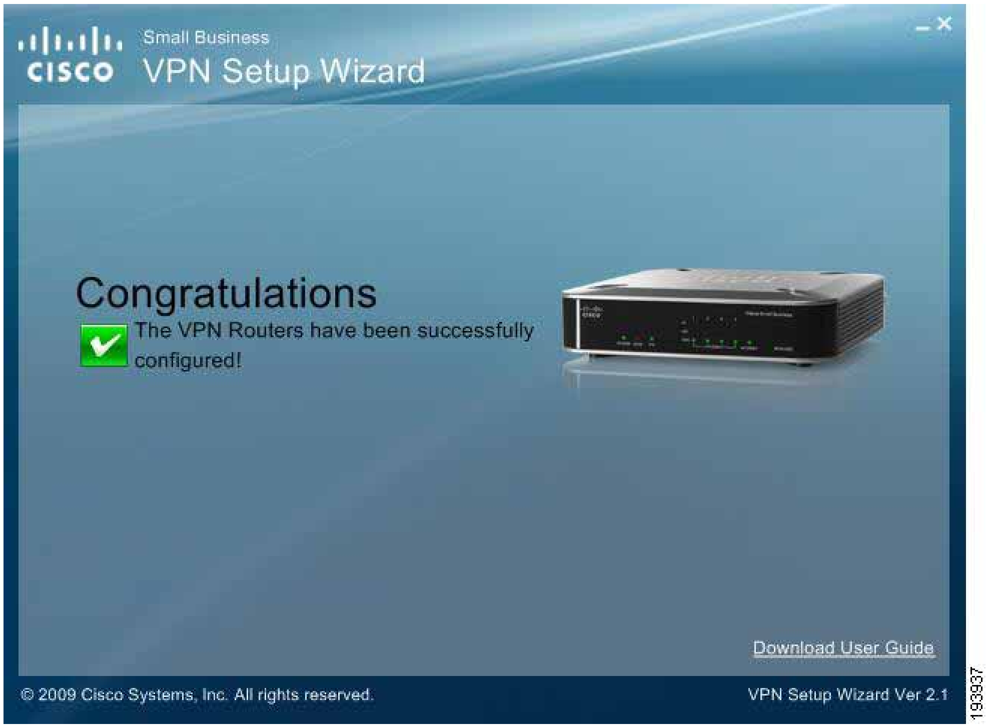
Checking the connection, please wait...

Tunnel Name:	
Exchange Type:	
Router 2 Remote I	
Router 2 WAN IP:	
Router 2 IP:	
Router 1 Remote IP Type:	IP-ADDRESS
Router 1 WAN IP:	172.21.6.36
Router 1 IP:	192.168.2.1/255.255.255.0

© 2009 Cisco Systems, Inc. All rights reserved. VPN Setup Wizard Ver 2.1

STEP 11 When testing is done, click **Exit** to end the Wizard.

Exit the Wizard

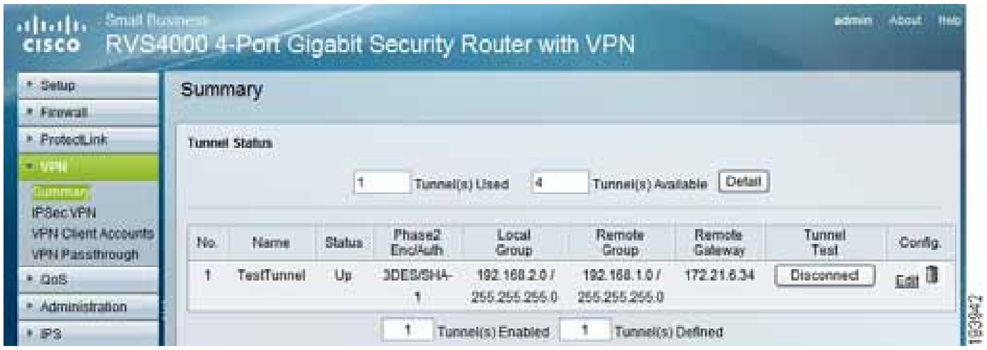


Congratulations

The VPN Routers have been successfully configured!

Congratulations! Setup is now complete. You may now log into the Web Administrator Interface and see the results.

Test Results



Summary

Tunnel Status

1 Tunnel(s) Used 4 Tunnel(s) Available

No.	Name	Status	Phase2 Enc/Auth	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	TestTunnel	Up	3DES/SHA-1	192.168.2.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0	172.21.6.34	Disconnect	Edit

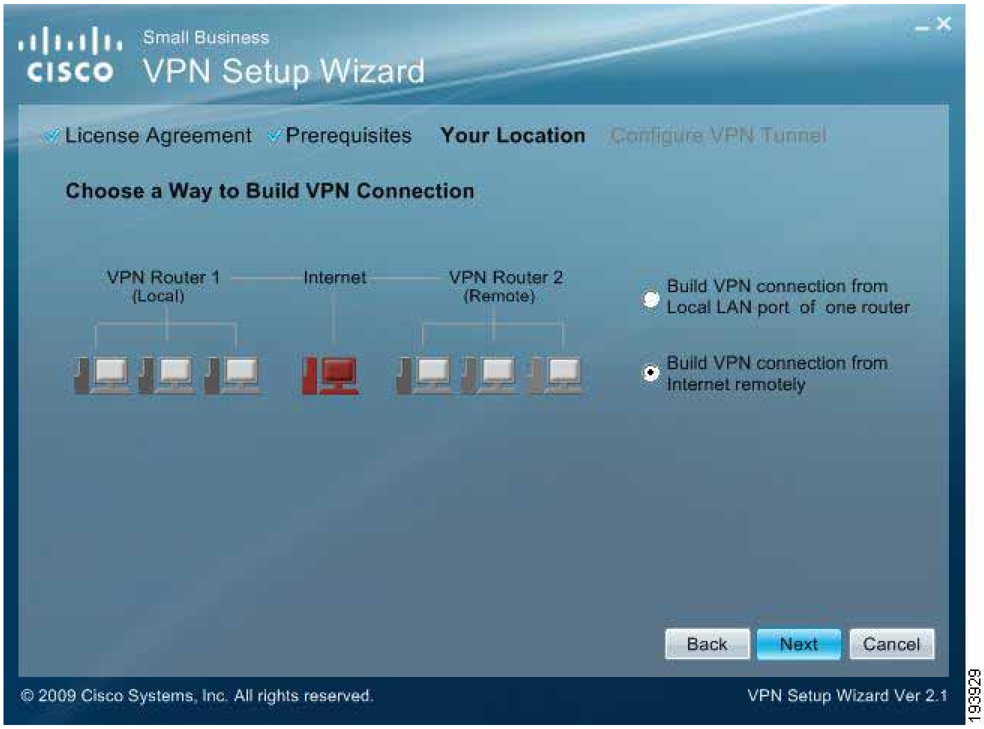
1 Tunnel(s) Enabled 1 Tunnel(s) Defined

Building Your VPN Connection Remotely

This procedure continues from **Step 5 on page 101**. Use this procedure to build your VPN connection from a remote PC.

STEP 1 Choose **Build VPN connection from Internet remotely**. Click **Next** to continue.

Build VPN Connection Remotely



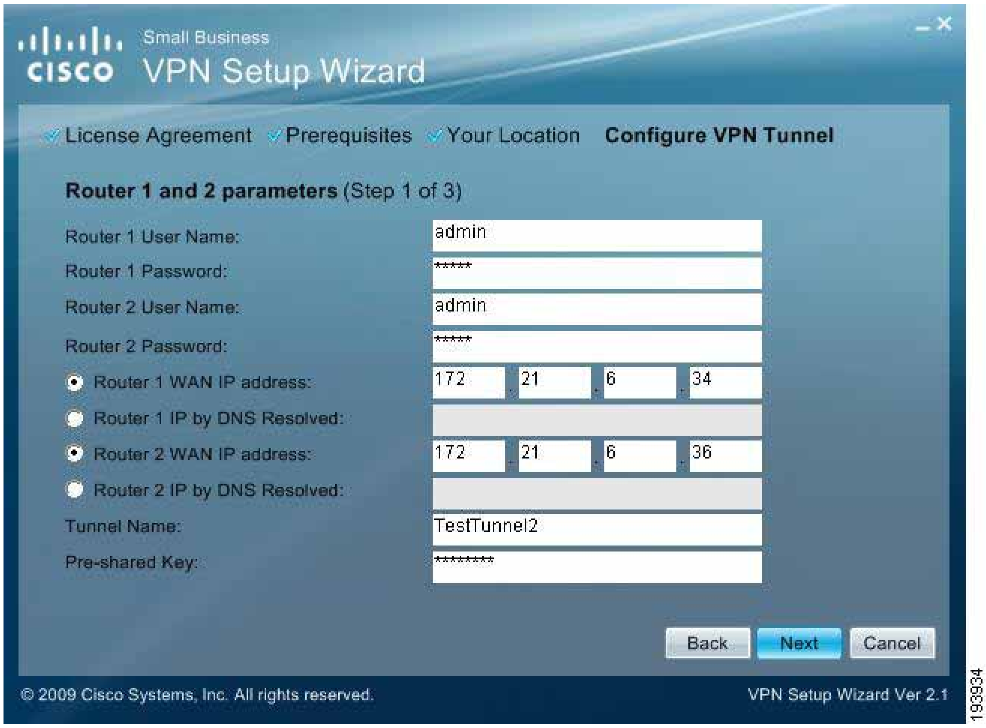
Choose a Way to Build VPN Connection

○ Build VPN connection from Local LAN port of one router

● Build VPN connection from Internet remotely

STEP 2 Enter the required data in the Configure VPN Tunnel window and then click **Next** to continue.

Configure VPN Tunnel Window



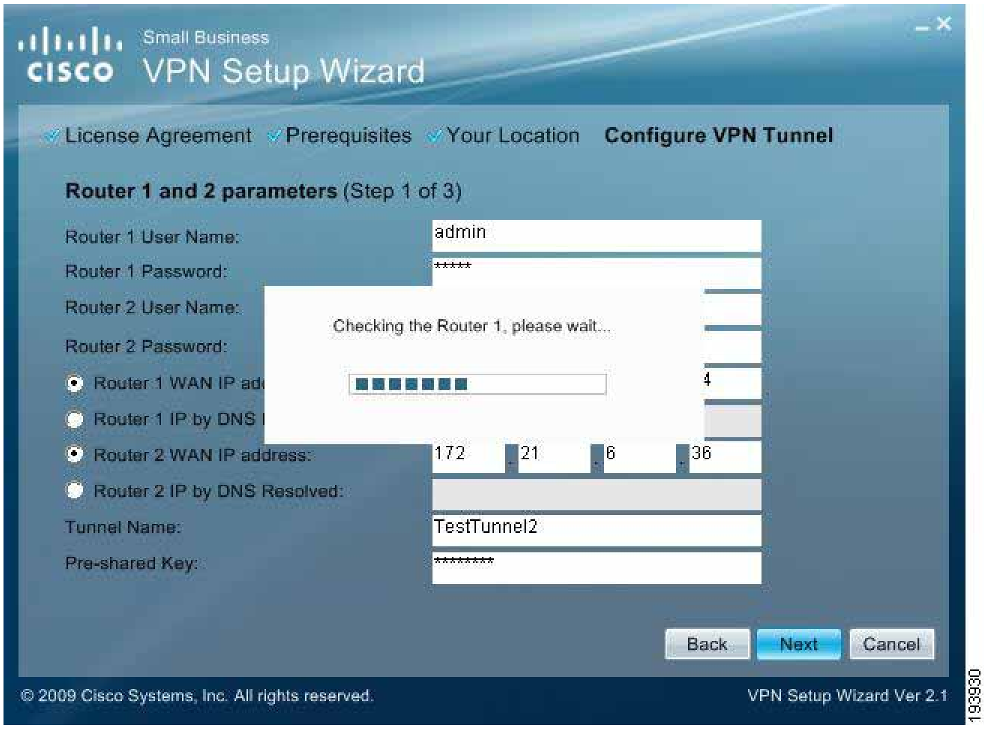
Router 1 and 2 parameters (Step 1 of 3)

Router 1 User Name:	admin
Router 1 Password:	*****
Router 2 User Name:	admin
Router 2 Password:	*****
● Router 1 WAN IP address:	172 . 21 . 6 . 34
○ Router 1 IP by DNS Resolved:	
● Router 2 WAN IP address:	172 . 21 . 6 . 36
○ Router 2 IP by DNS Resolved:	
Tunnel Name:	TestTunnel2
Pre-shared Key:	********

- **Router 1 User Name**: Enter the user name of the Router 1.
- **Router 1 Password**: Enter the password of the Router 1.
- **Router 2 User Name**: Enter the user name of the Router 2.
- **Router 2 Password**: Enter the password of the Router 2.
- **Tunnel Name**: Enter a name for this tunnel.
- **Pre-shared Key**: IKE uses the Pre-shared Key field to authenticate the remote IKE peer. Both character 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.
- **Router 1 WAN IP address**: Enter the WAN IP address of the Router 1.
- **Router 1 IP by DNS Resolved**: Enter the DDNS Domain Name of Router 1 if it does not have a static IP address for its internet connection.
- **Router 2 WAN IP address**: Enter the WAN IP address of the Router 2.
- **Router 2 IP by DNS Resolved**: Enter the DDNS Domain Name of Router 2 if it does not have a static IP address for its internet connection.

STEP 3 The router configuration is checked.

Check Router Configuration


Small Business
VPN Setup Wizard
✓ License Agreement ✓ Prerequisites ✓ Your Location Configure VPN Tunnel
Back
Next
Cancel
© 2009 Cisco Systems, Inc. All rights reserved.
VPN Setup Wizard Ver 2.1
193930

Router 1 and 2 parameters (Step 1 of 3)

Router 1 User Name: admin

Router 1 Password: *****

Router 2 User Name:

Router 2 Password:

● Router 1 WAN IP ad 4

○ Router 1 IP by DNS I

● Router 2 WAN IP address: 172 . 21 . 6 . 36

○ Router 2 IP by DNS Resolved:

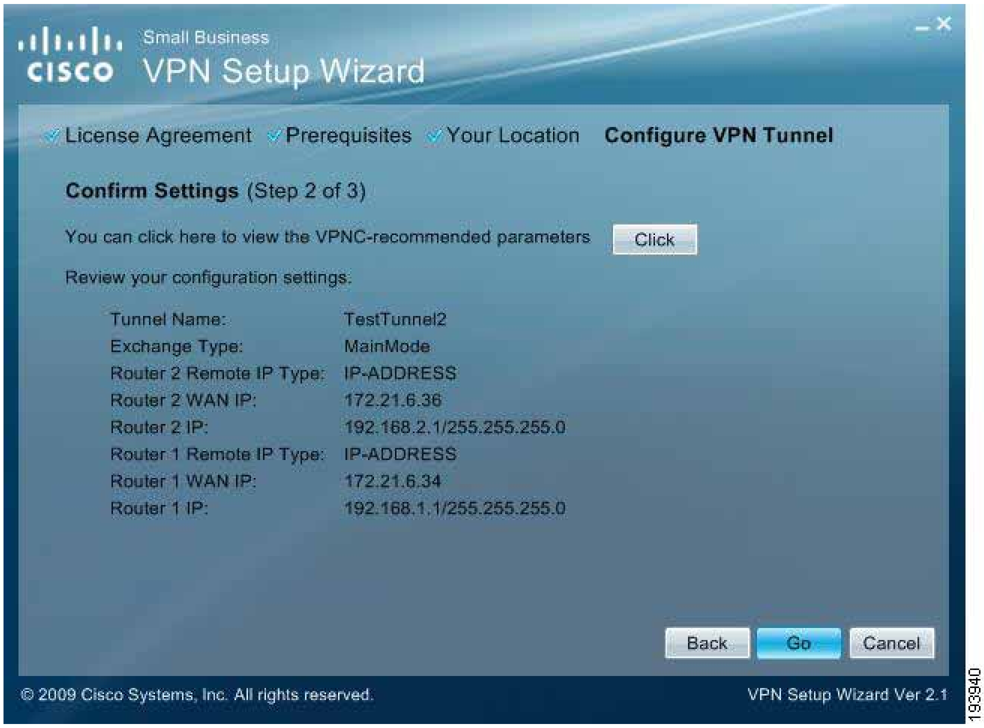
Tunnel Name: TestTunnel2

Pre-shared Key: *********

Checking the Router 1, please wait...

STEP 4 The Summary window appears. Use the **Click** box to view the VPNC Summary window.

Summary Window



Confirm Settings (Step 2 of 3)

You can click here to view the VPNC-recommended parameters

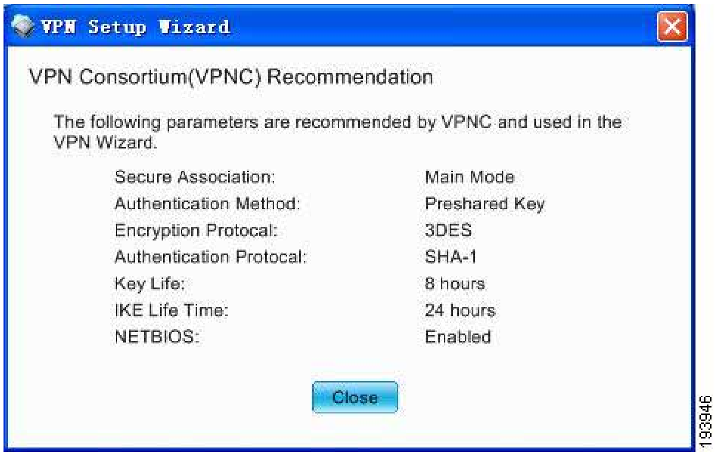
Review your configuration settings:

Tunnel Name:	TestTunnel2
Exchange Type:	MainMode
Router 2 Remote IP Type:	IP-ADDRESS
Router 2 WAN IP:	172.21.6.36
Router 2 IP:	192.168.2.1/255.255.255.0
Router 1 Remote IP Type:	IP-ADDRESS
Router 1 WAN IP:	172.21.6.34
Router 1 IP:	192.168.1.1/255.255.255.0

© 2009 Cisco Systems, Inc. All rights reserved.   VPN Setup Wizard Ver 2.1

STEP 5 The VPNC Summary window appears showing the settings that were made to industry standards. Click **Close** when you are ready to continue.

VPNC Summary Window



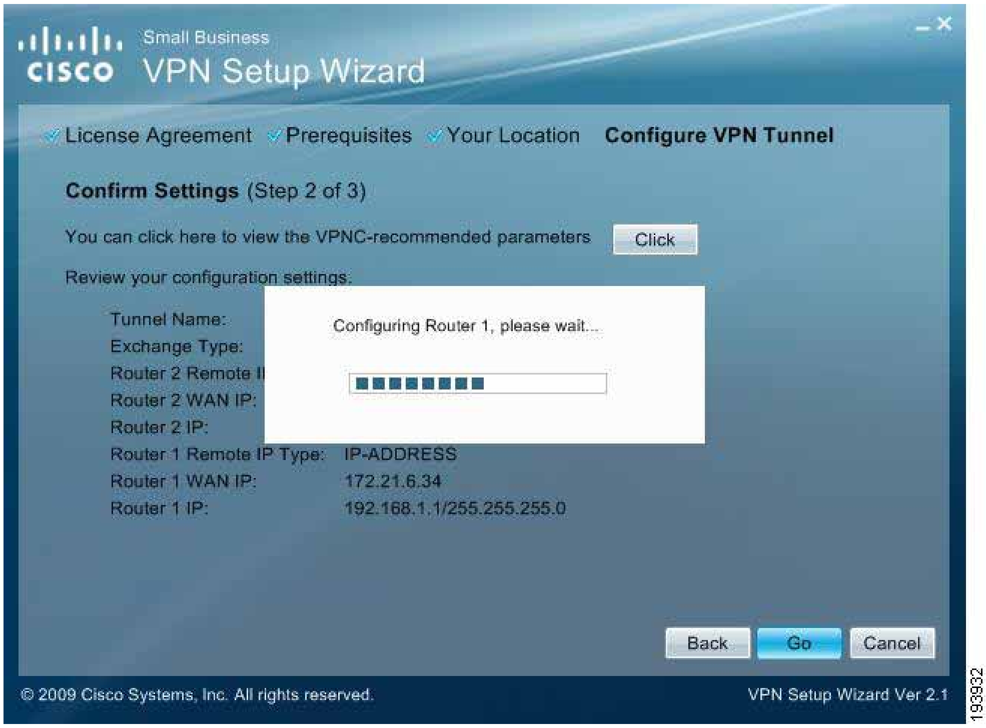
VPN Consortium(VPNC) Recommendation

The following parameters are recommended by VPNC and used in the VPN Wizard.

Secure Association:	Main Mode
Authentication Method:	Preshared Key
Encryption Protocal:	3DES
Authentication Protocal:	SHA-1
Key Life:	8 hours
IKE Life Time:	24 hours
NETBIOS:	Enabled

STEP 6 In the Summary window, if all your entries appear correct, click **Go**. Otherwise click **Back** to go back and make any corrections.

Configure the Router



Confirm Settings (Step 2 of 3)

You can click here to view the VPNC-recommended parameters Click

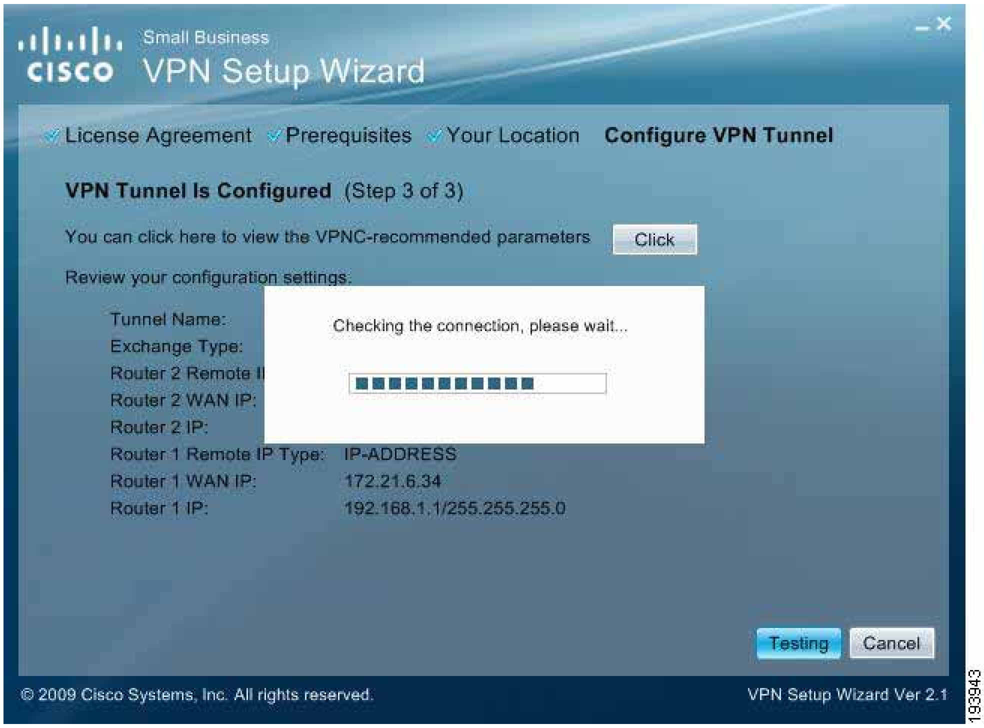
Review your configuration settings.

Tunnel Name:
Exchange Type:
Router 2 Remote I
Router 2 WAN IP:
Router 2 IP:
Router 1 Remote IP Type: IP-ADDRESS
Router 1 WAN IP: 172.21.6.34
Router 1 IP: 192.168.1.1/255.255.255.0

Configuring Router 1, please wait...

STEP 7 Click **Testing** to make sure the connection is successfully established.

Test the Connection



Small Business
VPN Setup Wizard

✓ License Agreement ✓ Prerequisites ✓ Your Location **Configure VPN Tunnel**

VPN Tunnel Is Configured (Step 3 of 3)

You can click here to view the VPNC-recommended parameters [Click]

Review your configuration settings.

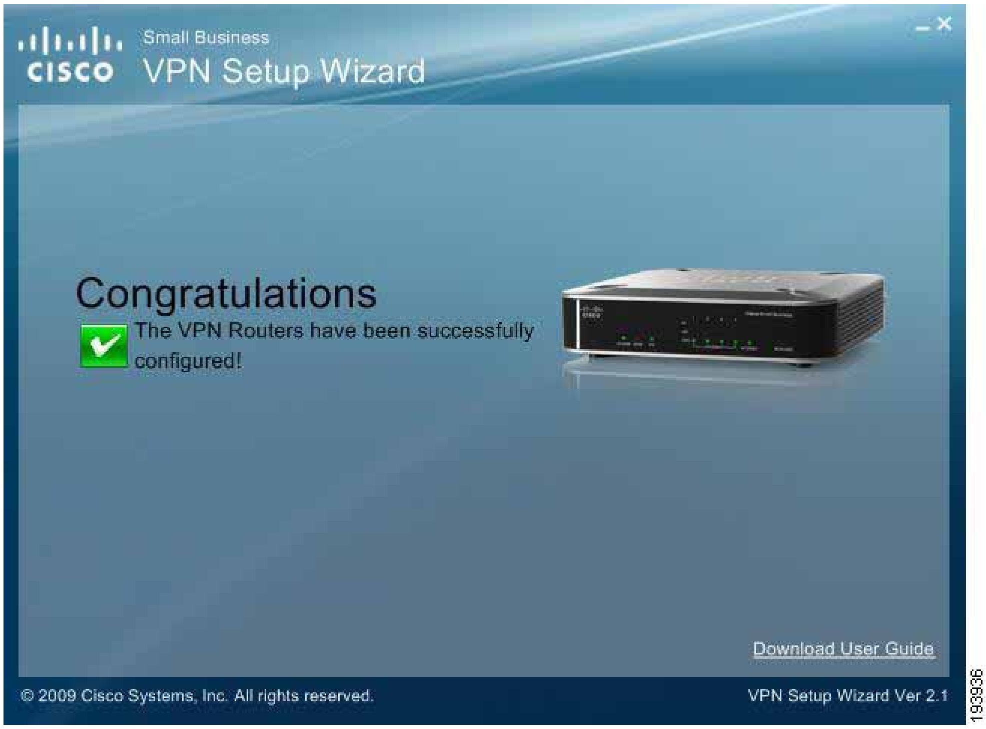
Tunnel Name:
Exchange Type:
Router 2 Remote I
Router 2 WAN IP:
Router 2 IP:
Router 1 Remote IP Type: IP-ADDRESS
Router 1 WAN IP: 172.21.6.34
Router 1 IP: 192.168.1.1/255.255.255.0

Checking the connection, please wait...

© 2009 Cisco Systems, Inc. All rights reserved.

VPN Setup Wizard Ver 2.1

STEP 8 When testing is done, click **Exit** to end the Wizard.



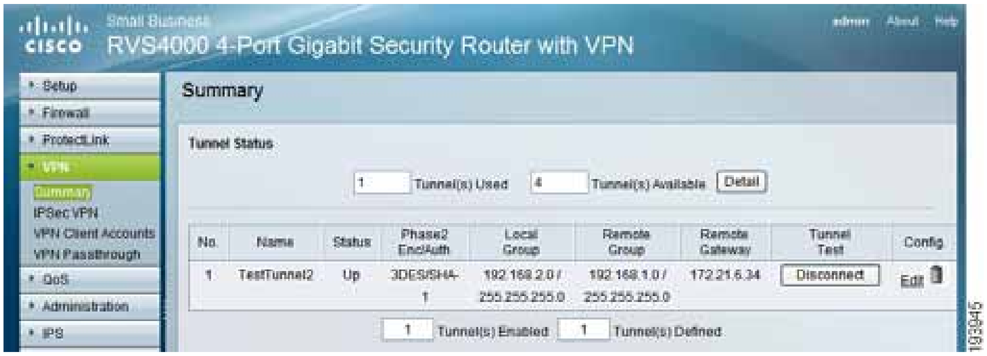
Congratulations

✓ The VPN Routers have been successfully configured!

© 2009 Cisco Systems, Inc. All rights reserved.

Congratulations! Setup is now complete. You may now log into the Web Administrator Interface and see the results.

View Test Results



Summary

Tunnel Status

1 Tunnel(s) Used 4 Tunnel(s) Available

No.	Name	Status	Phase2 Enc/Auth	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config
1	TestTunnel2	Up	3DES/SHA-1	192.168.2.0 / 255.255.255.0	192.168.1.0 / 255.255.255.0	172.21.6.34	Disconnect	Edit

1 Tunnel(s) Enabled 1 Tunnel(s) Defined

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 Cisco website at www.cisco.com.

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 these steps:

Windows 2000

STEP 1 Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.

STEP 2 Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and click **Properties**.

STEP 3 In the Components checked are used by this connection box, select **Internet Protocol (TCP/IP)**, and click **Properties**. Select **Use the following IP address**.

STEP 4 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.

STEP 5 Enter the Subnet Mask, **255.255.255.0**.

STEP 6 Enter the Default Gateway, **192.168.1.1** (Router's default IP address).

STEP 7 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.

STEP 8 Click **OK** in the Internet Protocol (TCP/IP) Properties window, and click **OK** in the Local Area Connection Properties window.

STEP 9 Restart the computer if asked.

Windows XP

STEP 1 Click **Start** and **Control Panel**.

STEP 2 Click the **Network and Internet Connections** icon and then the **Network Connections** icon.

STEP 3 Right-click the **Local Area Connection** associated with your Ethernet adapter, and click **Properties**.

STEP 4 In the This connection uses the following items box, select **Internet Protocol (TCP/IP)**. Click **Properties**.

STEP 5 Select **Use the following IP address**, and 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.

STEP 6 Enter the Subnet Mask, **255.255.255.0**.

STEP 7 Enter the Default Gateway, **192.168.1.1** (Router's default IP address).

STEP 8 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.

STEP 9 Click **OK** in the Internet Protocol (TCP/IP) Properties window. Click **OK** in the Local Area Connection Properties window.

I want to test my Internet connection.

STEP 1 Check your TCP/IP settings.

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 click **Properties**.

c. In the Components checked are used by this connection box, select **Internet Protocol (TCP/IP)**, and click **Properties**. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

d. Click **OK** in the Internet Protocol (TCP/IP) Properties window, and click **OK** in the Local Area Connection Properties window.

e. Restart the computer if asked.

Windows XP

These instructions are for the default interface of Windows XP. If you are using the Classic interface (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** associated with your Ethernet adapter, and click **Properties**.

d. In the This connection uses the following items box, select **Internet Protocol (TCP/IP)** and click **Properties**. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

STEP 2 Open a command prompt:

a. Windows 98 and Millennium: Click **Start** and **Run**. In the Open field, type **command**. Press **Enter** or click **OK**.

b. Windows 2000 and XP: Click **Start** and **Run**. In the Open field, type **cmd**. Press **Enter** or click **OK**.

STEP 3 At the command prompt, type **ping 192.168.1.1** and press **Enter**.

- 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.

STEP 4 At the command prompt, type **ping** followed by your Internet IP address and press **Enter**. You can find the Internet IP Address in the configuration utility 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 **Enter**.

- 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.

STEP 5 At the command prompt, type **ping www.cisco.com** and press **Enter**.

- If you get a reply, the computer is connected to the Internet. If you cannot open a web page, 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.

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

STEP 1 Refer to **“I want to test my Internet connection.” on page 117** above to verify that you have connectivity.

STEP 2 If you need to clone the MAC address of your Ethernet adapter onto the router, see the MAC Address Clone section of **Chapter 5, “Setting Up and Configuring the Router”** for details.

STEP 3 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 5, “Setting Up and Configuring the Router”** for details on Internet Connection Type settings.

STEP 4 Make sure you use the right cable. Check to see if the Internet LED is solidly lit.

STEP 5 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 configuration utility shows a valid IP address from your ISP.

STEP 6 Turn off the computer, router, and cable/DSL modem. Wait 30 seconds, and then turn on the router, cable/DSL modem, and computer. Check **System > Summary** from the router's configuration utility to see if you get an IP address.

I am not able to access the router's configuration utility Setup window.

STEP 1 Refer to **"I want to test my Internet connection.," on page 117** to verify that your computer is properly connected to the router.

STEP 2 Verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.

STEP 3 Set a static IP address on your system; refer to **"I need to set a static IP address on a PC." on page 115** above.

STEP 4 Refer to **"I am a PPPoE user and I need to remove the proxy settings or the dial-up pop-up window.," on page 123**.

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 **VPN > VPN Pass Through**. 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 Setup menu of the configuration 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 represents 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.

Check the Cisco website at www.cisco.com for more information.

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 documentation provided with the server you installed. Follow these steps to set up port forwarding through the router's configuration utility. We need to set up web, ftp, and mail servers.

STEP 1 Access the router's configuration utility by going to **http://192.168.1.1** or the IP address of the router. Go to **Firewall > Single Port Forwarding**.

STEP 2 Select the Service from the Application column.

STEP 3 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. Then check the Enable box for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
HTTP	80 to 80	Both	192.168.1.100	X
FTP	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

STEP 4 Configure as many entries as you like.

STEP 5 When you have completed the configuration, click **Save**.

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. In this situation, you need 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:

STEP 1 Access the router's configuration utility by going to **http://192.168.1.1** or the IP address of the router. Go to **Firewall > Single Port Forwarding**.

STEP 2 Select the Service from the Application column.

STEP 3 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. Then check the **Enable** box for the entry. Consider the examples below:

Application	Start and End	Protocol	IP Address	Enable
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

STEP 4 Configure as many entries as you like.

STEP 5 When you have completed the configuration, click **Save**.

I can’t get an Internet game, server, or application to work.

If you have difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet by 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 is 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:

STEP 1 Access the router’s configuration utility by going to **http://192.168.1.1** or the IP address of the router. Go to the **Firewall > Single Port Forwarding**.

STEP 2 Disable the entries you have entered for forwarding.

STEP 3 Go to **Setup > DMZ**.

STEP 4 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.

STEP 5 Select **Enable** to enable DMZ Hosting.

STEP 6 When you have completed the configuration, click **Save**.

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 prompted for a password when saving settings, then perform these steps:

STEP 1 Access the router’s web interface by going to http://192.168.1.1 or the IP address of the router.

STEP 2 To log in, enter the default password **admin**.

STEP 3 Click **Administration > Management** in the navigation tree.

STEP 4 Enter a new password in the **Router Password** field.

STEP 5 Re-enter the new password in the **Re-enter to Confirm** field.

STEP 6 Click **Save**.

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 Internet Explorer, click **Tools** > **Internet Options**, and then click the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit** > **Preferences** > **Advanced** > **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**. For more information, refer to the documentation for your web browser.

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.

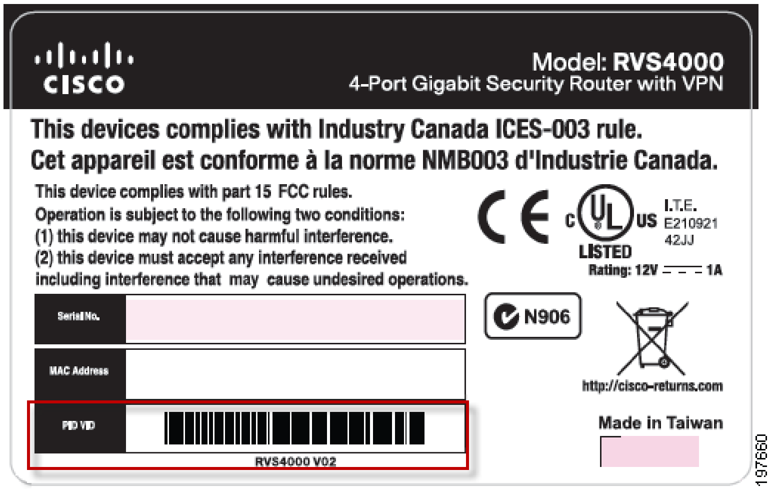
I need to upgrade the firmware.

Follow the instructions in **Administration > Firmware Upgrade, page 80**.

The firmware upgrade failed.

The upgrade could have failed for a number of reasons. You can reattempt the firmware upgrade by following the instructions in **Administration > Firmware Upgrade, page 80**. Alternatively, for hardware version 1, you can use the “rescue” procedure described below.

NOTE To determine the hardware version, refer to the PIDVID code on the label on the bottom panel of the router.



cisco

Model: RVS4000
4-Port Gigabit Security Router with VPN

This devices complies with Industry Canada ICES-003 rule.
Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

This device complies with part 15 FCC rules.
Operation is subject to the following two conditions:
(1) this device may not cause harmful interference.
(2) this device must accept any interference received
including interference that may cause undesired operations.

c UL US LISTED I.T.E. E210921 42JJ
Rating: 12V ⎓ 1A

N906

Serial No.	
MAC Address	
PID VID	RVS4000 V02

http://cisco-returns.com

Made in Taiwan

STEP 1 If your router has hardware version 1, go www.cisco.com/go/software.

STEP 2 In the Search box, enter: **RVS4000**

STEP 3 In the Search results, choose Download Software for Cisco RVS4000 4-port Gigabit Security Router - VPN.

When prompted, enter your Cisco.com user name and password. If you do not have a Cisco.com login, you can register as a new user.

STEP 4 Click the **Router Firmware Rescue Utility** link.

STEP 5 Save the zip file to your computer.

STEP 6 Extract the file **setup.exe** from the zip file, then run **setup.exe** to install the utility on your computer.

STEP 7 Disconnect the network cables from **all** of the router's LAN and WAN ports, **except** the network cable to the computer that has the firmware upgrade utility.

STEP 8 Double-click the **RVS4000 Upgrade Utility** icon on your desktop. Alternatively, run the utility by clicking **Start > All Programs > Cisco Small Business RVS4000**.

STEP 9 Follow the on-screen instructions to perform the upgrade.

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.

STEP 1 To connect to the router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the router.

STEP 2 Enter the password, if asked (default password is **admin**).

STEP 3 On the **Setup > WAN** menu, select the option **Keep Alive**, and set the Redial Period option at **20** (seconds).

STEP 4 Click **Save**.

If the connection is lost again, follow steps 1 and 2 to re-establish connection.

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

You may need to adjust the Maximum Transmission Unit (MTU) setting. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you have difficulties, perform these steps:

STEP 1 To connect to the router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the router.

STEP 2 Enter the password, if asked (the default password is **admin**).

STEP 3 Go to the **Setup > WAN** menu.

STEP 4 Look for the MTU option, and select **Manual**. In the Size field, enter **1492**.

STEP 5 Click **Save** to continue.

STEP 6 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

I need to use port triggering.

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

STEP 1 To connect to the router, go to the web browser, and enter **http://192.168.1.1** or the IP address of the router.

STEP 2 Enter the password, if asked (the default password is **admin**).

STEP 3 Click **Firewall > Port Range Triggering**.

STEP 4 Enter any name you want to use for the Application Name.

STEP 5 Enter the Start and End Ports of the Triggered Range. Check with your Internet application provider for more information on which outgoing port services it uses.

STEP 6 Enter the Start and End Ports of the Forwarded Range. Check with your Internet application provider for more information on which incoming port services are required by the Internet application.

STEP 7 Check the **Enabled** box for the entry.

STEP 8 When you have completed the configuration, click **Save**.

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 has a problem.
- If the PCs are configured correctly, but still do not work, 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 works 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**.

I'm trying to access the router's configuration utility but I do not see the login window. Instead, I see a window saying, "404 Forbidden."

If you are using Internet Explorer, perform these steps until you see the configuration utility's login window (Netscape Navigator will require similar steps):

STEP 1 Click **File**. Make sure **Work Offline** is NOT checked.

STEP 2 Press **CTRL + F5**. This is a hard refresh, which will force Internet Explorer to load new web pages, not cached ones.

STEP 3 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.

I have QuickVPN tunnel connected to my RVS4000 but I cannot see the computers in the remote network from Internet Explorer.

QuickVPN tunneling does not support NetBIOS Broadcast. To access the computers or shared drives on the remote network, users are advised to use the IP address to identify the resource.

I have a Gateway-to-Gateway IPSec VPN tunnel connected between two RVS4000 routers. The users in one network cannot see the computers in the remote network from Internet Explorer.

The RVS4000 supports NetBIOS Broadcast over a Gateway-to-Gateway IPSec VPN tunnel. However, the administrator needs to enable this feature in the Advanced section of the VPN > IPSec VPN window.

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.

Is IPSec Passthrough supported by the router?

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

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

Does the router support ICQ send file?

Yes. However, you may need to adjust the ICQ connection settings because your PC is behind a firewall. For instructions, refer to the ICQ documentation or online support pages.

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

If you are running a dedicated Unreal Tournament server, 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 the network game or the game server that 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 experience 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 displayed on the window. What do I need to do?

Change your Ethernet adapter properties to specify 10 Mbps/Half Duplex mode instead of Auto Detect.

STEP 1 On a Windows PC, click the **Start** button, point to **Control Panel**, and then click **System**.

STEP 2 Click the **Hardware** tab, and then click **Device Manager**.

STEP 3 Click the plus sign next to **Network adapters** to expand the listings.

STEP 4 Right-click your Network Connection adapter, and then click **Properties**.

STEP 5 Click the **Advanced** tab.

STEP 6 In the **Property** list, click **Link Speed & Duplex**. In the **Value** list, choose **10 Mbps/ Half Duplex**.

STEP 7 Also make sure that your proxy setting is disabled in the browser:

For Internet Explorer, click **Tools** > **Internet Options**, and then click the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit** > **Preferences** > **Advanced** > **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**. For more information, refer to the documentation for your web browser.

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 Cisco website at www.cisco.com.

How can I be notified of new router firmware upgrades?

All Cisco firmware upgrades are posted on www.cisco.com, where you can download the files for free. The router's firmware can be upgraded by using the configuration 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 window for the router. What can I do?

You may have to remove the proxy settings on your web browser. Or remove the dial-up settings on your browser. Check with your browser documentation. 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 click the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit** > **Preferences** > **Advanced** > **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.

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 2,048 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.

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?

From the **Firewall > SIngle Port Forwarding** menu, set port forwarding to 113 for the PC on which you are using mIRC.

B

Using Cisco QuickVPN for Windows 2000, XP, or Vista

Overview

This appendix explains how to install and use the Cisco QuickVPN software that can be downloaded from www.cisco.com. QuickVPN works with computers running Windows 2000, XP, Vista, or Windows 7. (Computers using other operating systems will have to use third-party VPN software.) For Windows Vista, QuickVPN Client version 1.2.5 or later is required. For Windows 7, version 1.4.0.5 or later is required.

This appendix includes these sections:

Before You Begin

The QuickVPN program only works with a Cisco 4-Port Gigabit Security Router with VPN that is properly configured to accept a QuickVPN connection. Follow these instructions to configure the router's VPN client settings:

STEP 1 Click the **VPN > VPN Client Accounts**.

STEP 2 Enter the username in the Username field.

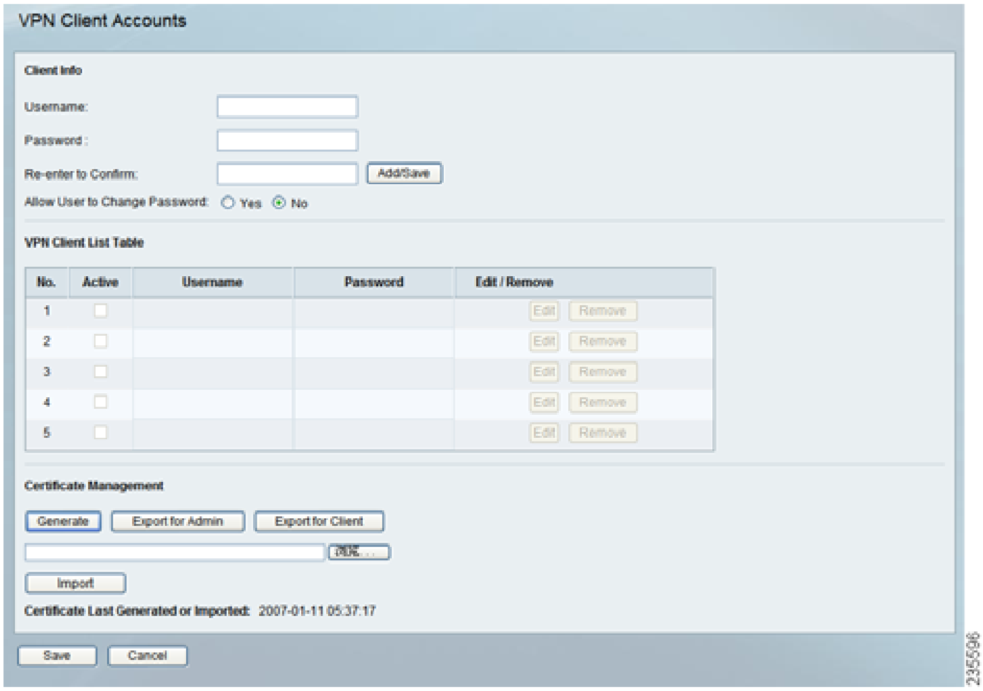
STEP 3 Enter the password in the Password field, and enter it again in the Re-enter to confirm field.

STEP 4 Click **Add/Save**.

STEP 5 Check the **Active** box for VPN Client No. 1.

STEP 6 Click **Save**.

VPN Client Accounts Window



VPN Client Accounts

Client Info

Username:

Password :

Re-enter to Confirm:

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: 2007-01-11 05:37:17

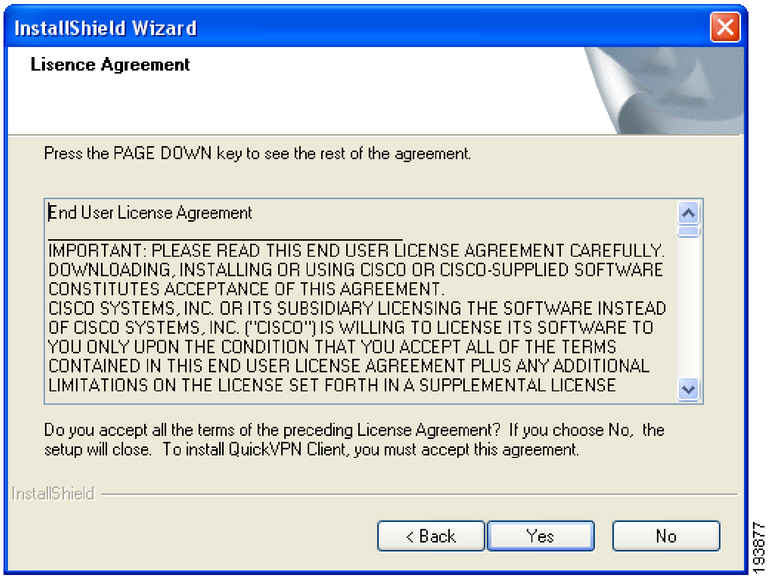
Installing the Cisco QuickVPN Software

Installing from the CD-ROM

STEP 1 Insert the RVS4000 CD-ROM into your CD-ROM drive. Go to the **Start** menu and then click **Run**. In the field provided, enter **D:\VPN_Client.exe** (if “**D**” is the letter of your CD-ROM drive).

STEP 2 The License Agreement window appears. Click **Yes** to accept the agreement and the appropriate files are copied to the computer.

License Agreement



Lisence Agreement

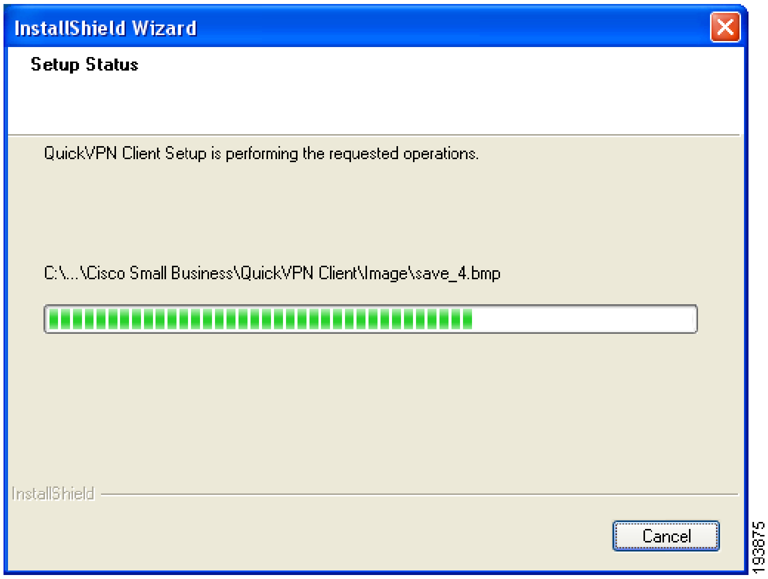
Press the PAGE DOWN key to see the rest of the agreement.

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install QuickVPN Client, you must accept this agreement.

Copying Files

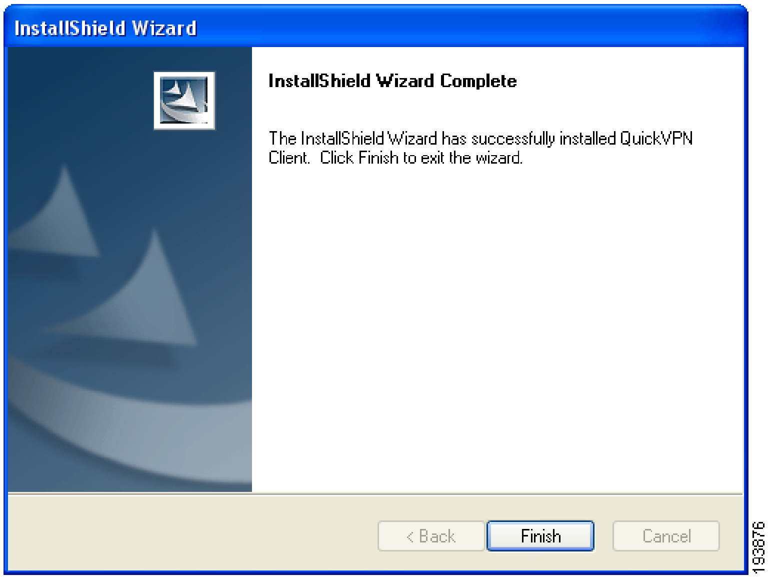


Setup Status

QuickVPN Client Setup is performing the requested operations.

C:\...\Cisco Small Business\QuickVPN Client\Image\save_4.bmp

Finished Installing Files



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed QuickVPN Client. Click Finish to exit the wizard.

STEP 3 Click **Finished** to complete the installation. Proceed to **"Using the Cisco QuickVPN Software," on page 137**.

Downloading and Installing from the Internet

STEP 1 Go to firmware download link in **Appendix G, "Where to Go From Here."**

STEP 2 From the firmware download link, click **Download Software**.

STEP 3 Select Cisco Small Business Routers > **RVS4000** from the menu.

STEP 4 Select **QuickVPN Utility**.

STEP 5 Save the zip file to your PC, and extract the .exe file.

STEP 6 Double-click the .exe file, and follow the on-screen instructions. Proceed to the next section, **"Using the Cisco QuickVPN Software," on page 137**.

Using the Cisco QuickVPN Software

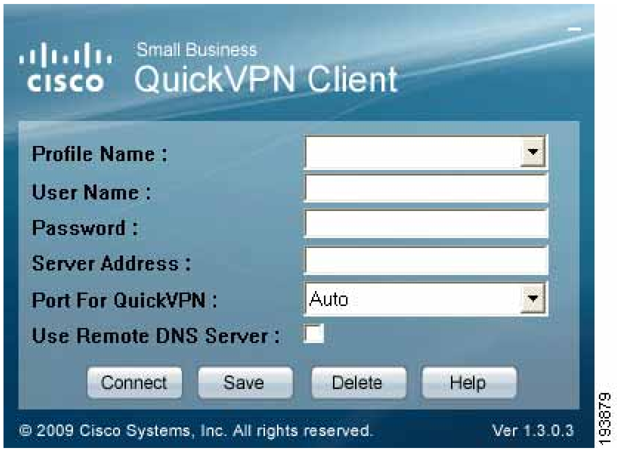
STEP 1 Double-click the Cisco QuickVPN software icon on your desktop or in the system tray.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

STEP 2 The QuickVPN Login window will appear. In the Profile Name field, enter a name for your profile. In the User Name and Password fields, enter the User Name and Password that were assigned to you. In the Server Address field, enter the IP address or domain name of the Cisco 4-Port Gigabit Security Router with VPN. In the Port For QuickVPN field, enter the port number that the QuickVPN client will use to communicate with the remote VPN router, or keep the default setting, **Auto**.

QuickVPN Login



Profile Name :	
User Name :	
Password :	
Server Address :	
Port For QuickVPN :	Auto
Use Remote DNS Server :	□

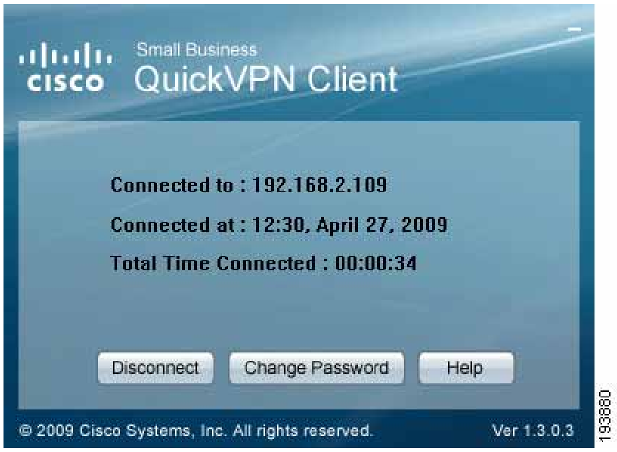
To save this profile, click **Save**. (If there are multiple sites to which you will need to create a tunnel, you can create multiple profiles, but note that only one tunnel can be active at a time.) To delete this profile, click **Delete**. For information, click **Help**.

STEP 3 To begin your QuickVPN connection, click **Connect**. The connection's progress is displayed: Connecting, Provisioning, Activating Policy, and Verifying Network.

STEP 4 When your QuickVPN connection is established, the QuickVPN tray icon turns green, and the QuickVPN Status window appears. The window displays 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.

QuickVPN Tray Icon—
Connection

QuickVPN Status



Connected to : 192.168.2.109

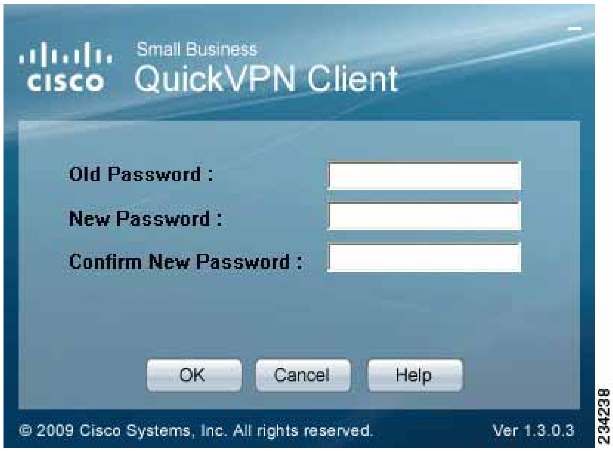
Connected at : 12:30, April 27, 2009

Total Time Connected : 00:00:34

To terminate the VPN tunnel, click **Disconnect**. To change your password, click **Change Password**. For information, click **Help**.

STEP 5 If you clicked **Change Password** and have permission to change your own password, you will see the Connect Virtual Private Connection window. 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 **OK** to save your new password. Click **Cancel** to cancel your change. For information, click **Help**.

Connect Virtual Private Connection



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

Distributing Certificates to QuickVPN Users

Follow this procedure to export a certificate from the RVS4000 for distribution to QuickVPN users, and to install the certificate on the QuickVPN users' PCs.

STEP 1 Generate the certificate as follows:

a. Log on to the configuration utility.

b. Select **VPN > VPN Client Accounts**.

c. Click **Generate** to generate a new certificate.

d. Click **Export for Client** and save the certificate as a **.PEM** file.

STEP 2 Distribute the certificate to all QuickVPN users.

STEP 3 Each QuickVPN user must then install the certificate as follows:

a. Save the certificate into the directory where the QuickVPN Client is installed. For example:
C:\Program Files\Cisco\QuickVPN Client

b. Launch the QuickVPN Client and specify the User Name, Password, and Server Address (IP address or domain name).

c. Click **Connect**.

For more information on certificate management, go to section **"VPN > VPN Client Accounts," on page 64** in **Chapter 5, "Setting Up and Configuring the Router."**

C

Configuring IPSec with a Windows 2000 or XP Computer

This appendix explains how to configure IPSec with a computer that is using Windows 2000 or Windows XP. Refer to these topics:

- **Introduction, page 141**
- **Environment, page 142**
- **How to Establish a Secure IPSec Tunnel, page 142**

Introduction

This appendix explains how to establish a secure IPSec tunnel using preshared keys to join a private network inside the router and a Windows 2000 or XP computer. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

Microsoft KB Q252735—How to Configure IPSec Tunneling in Windows 2000: http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225—Basic IPSec Troubleshooting in Windows 2000: http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

NOTE

- Keep a record of any changes you make. Those changes will be identical in the Windows “secpol” application and the router’s configuration utility.
- The text on your screen may differ from the text in your instructions regarding the **OK** or **Close** buttons; click the appropriate button on your screen.

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

Windows 2000 or Windows XP

IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

RVS4000

WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

How to Establish a Secure IPSec Tunnel

Establishing a secure IPSec tunnel requires these five steps that are described in this procedure:

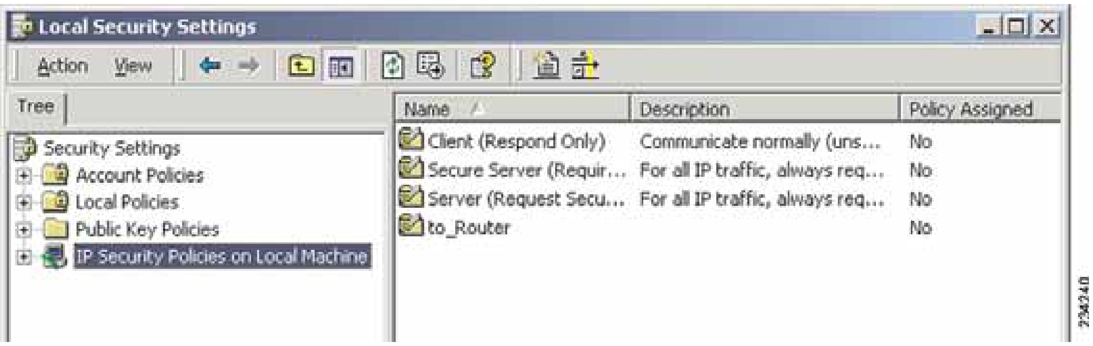
- Step 1: Create an IPSec Policy
- Step 2: Build Filter Lists
- Step 3: Configure Individual Tunnel Rules
- Step 4: Assign New IPSec Policy
- Step 5: Create a Tunnel Through the configuration utility

Establishing a Secure IPSec Tunnel

STEP 1 Create an IPSec policy.

a. Click **Start**, select **Run**, and type **secpol.msc** in the Open field. The Local Security Settings window appears.

Local Security Settings



- Security Settings
  - Account Policies
  - Local Policies
  - Public Key Policies
  - IP Security Policies on Local Machine

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_Router		No

b. Right-click **IP Security Policies on Local Computer** (Windows XP) or **IP Security Policies on Local Machine** (Windows 2000), and click **Create IP Security Policy**.

c. Click the **Next** button, and then enter a name for your policy (for example, to_Router). Then, click **Next**.

d. Uncheck the **Activate the default response rule** box, and then click **Next**.

e. Click **Finish**, making sure the **Edit** box is checked.

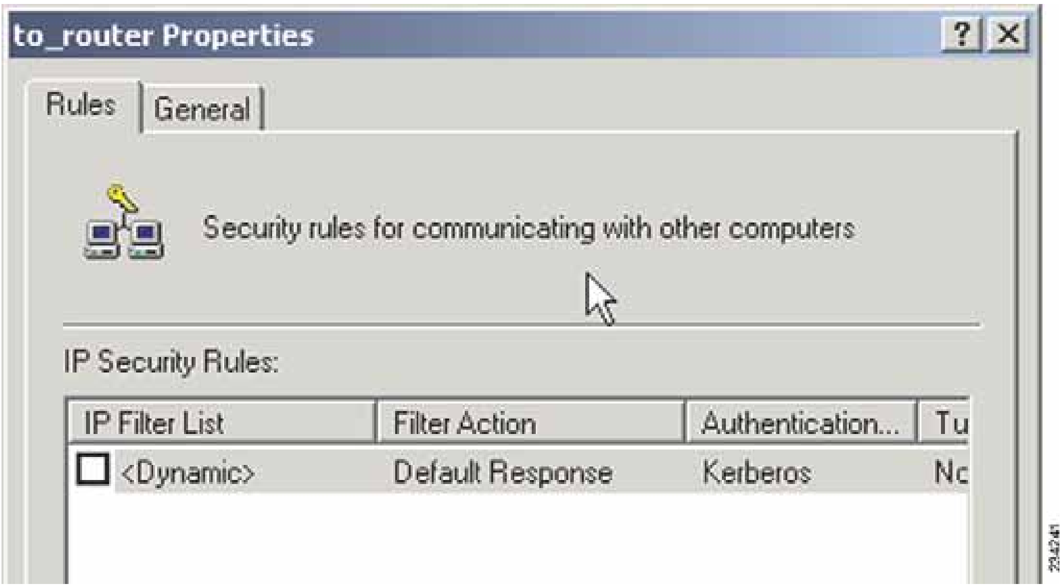
STEP 2 Build filter lists.

NOTE Throughout this section the term “win” refers to both Windows 2000 and Windows XP.

Filter List 1: win -> router

a. In the new policy's properties window, verify that the **Rules** tab is selected. Uncheck the **Use Add Wizard** box, and click **Add** to create a new rule.

Rules Tab



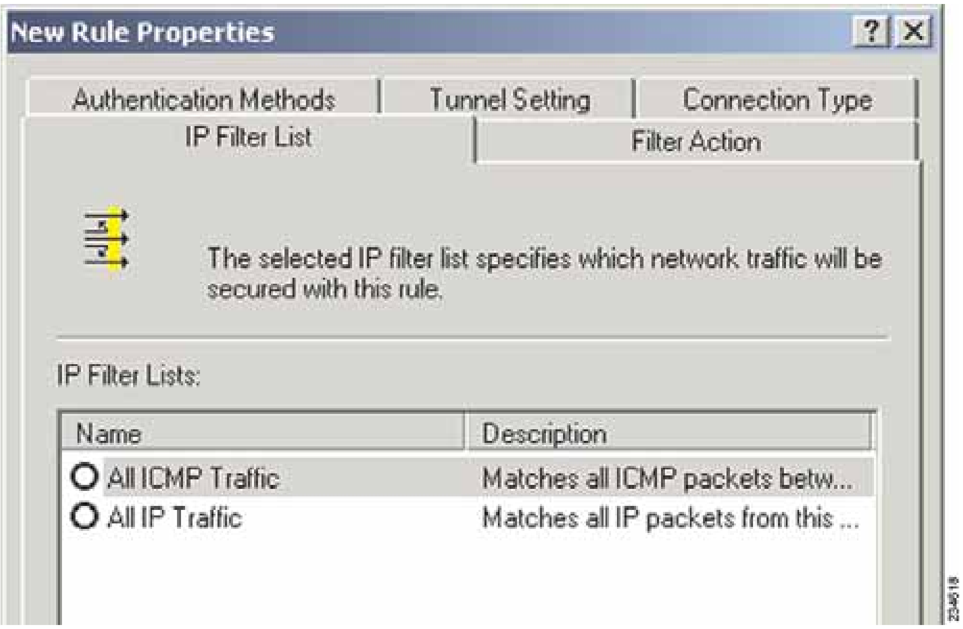
Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☐ <Dynamic>	Default Response	Kerberos	Nc

b. Make sure the **IP Filter List** tab is selected. Click **Add**.

IP Filter List Tab



New Rule Properties

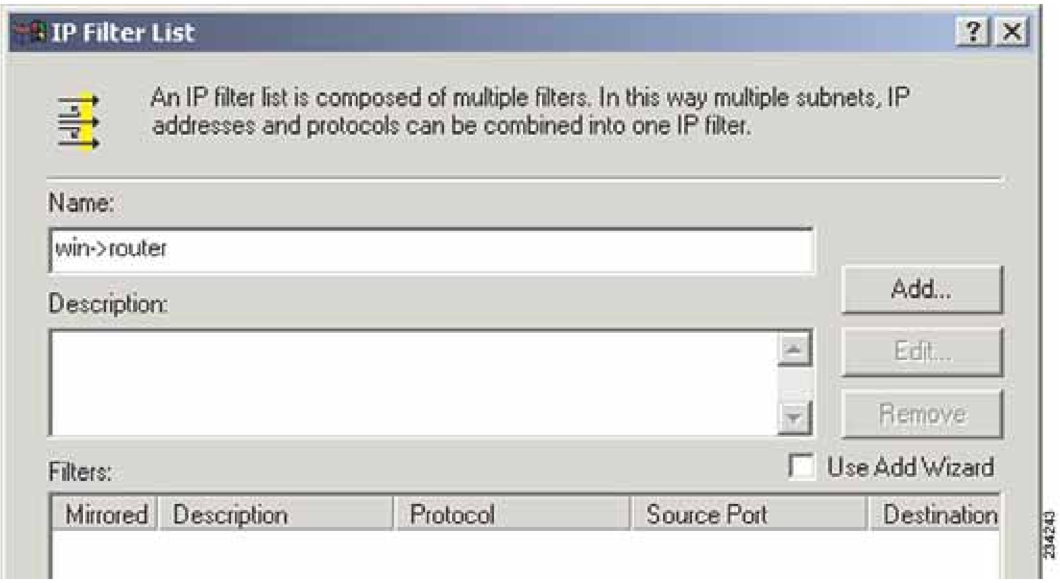
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

c. The IP Filter List window should appear. Enter an appropriate name, such as win-> Router, for the filter list, and uncheck the **Use Add Wizard** box. Then, click **Add**.

IP Filter List



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: win->router

Description:

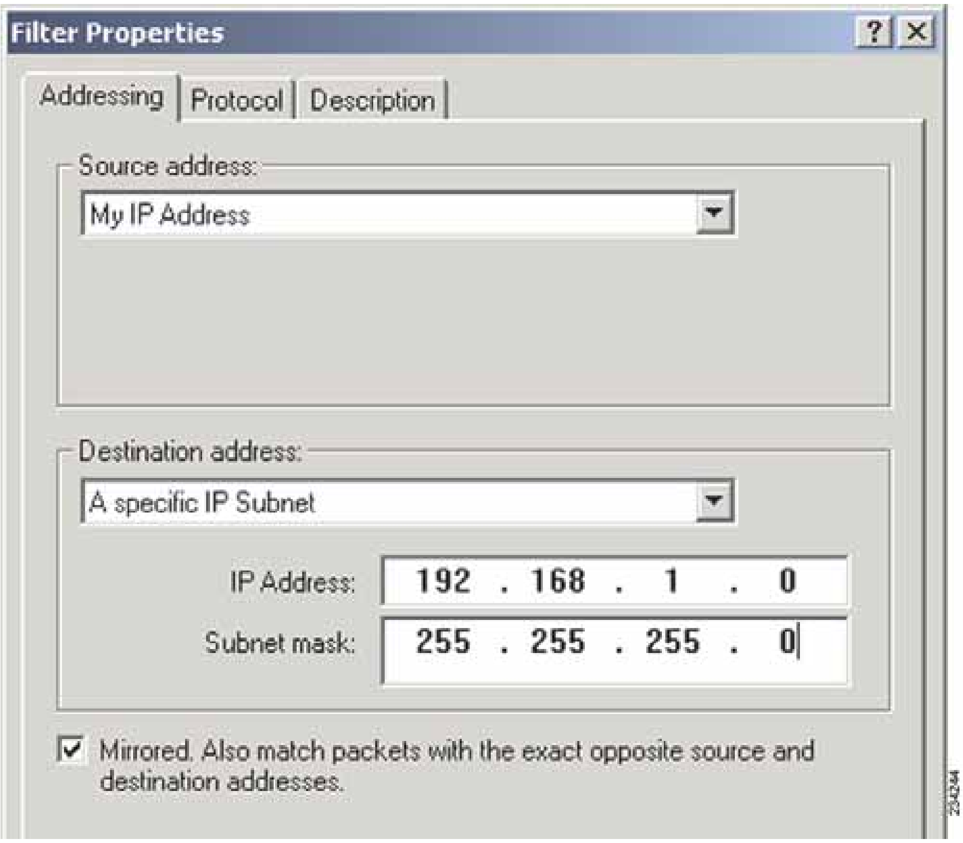
☐ Use Add Wizard

Filters:

Mirrored	Description	Protocol	Source Port	Destination

d. The Filters Properties window will appear. Select the **Addressing** tab.

Filters Properties



Source address:
My IP Address

Destination address:
A specific IP Subnet

IP Address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

In the Source address field, select **My IP Address**. In the Destination address field, select **A specific IP Subnet**, and enter the IP Address **192.168.1.0** and Subnet mask **255.255.255.0**. (These are the router's default settings. If you have changed these settings, enter your new values.)

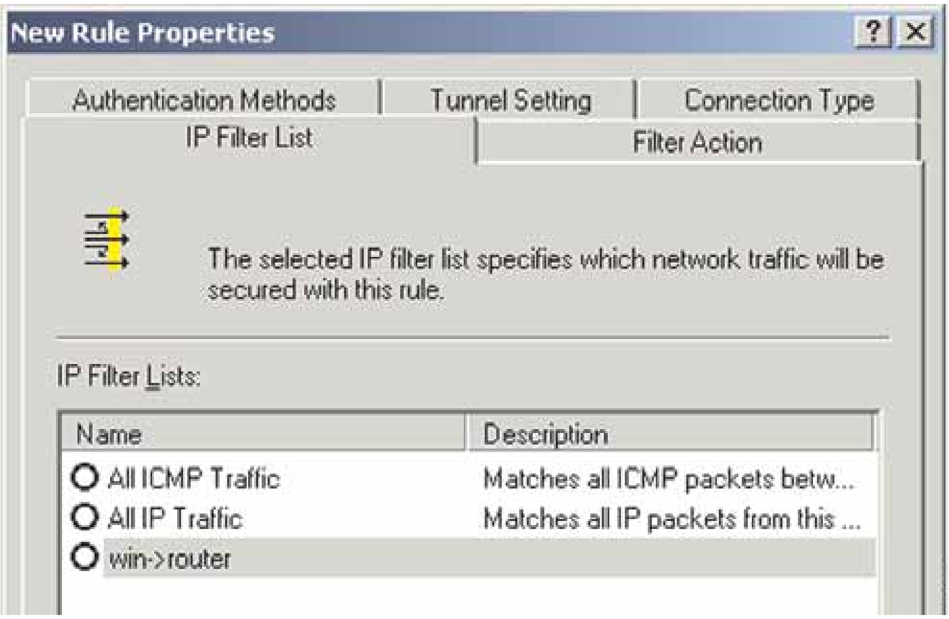
e. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

f. Click **OK**. Then, click **OK** or **Close** in the IP Filter List window.

Filter List 2: router -> win

g. The New Rule Properties window will appear. Select the **IP Filter List** tab, and make sure that **win -> Router** is highlighted. Then, click **Add**.

New Rules Properties



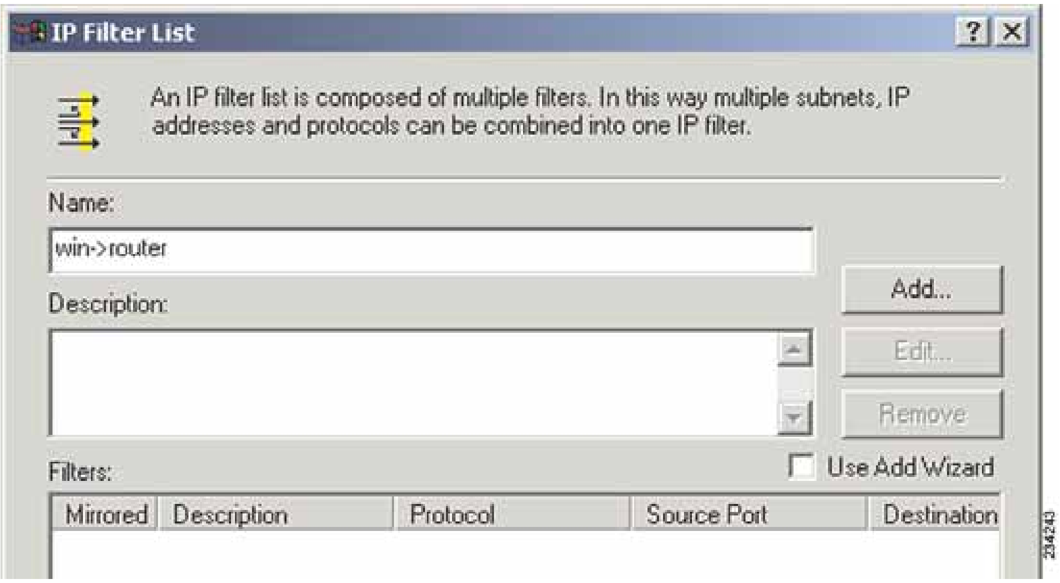
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ win->router	

h. The IP Filter List window should appear. Enter an appropriate name, such as **Router->win** for the filter list, and uncheck the **Use Add Wizard** box. Click **Add**.

IP Filter List



An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: win->router

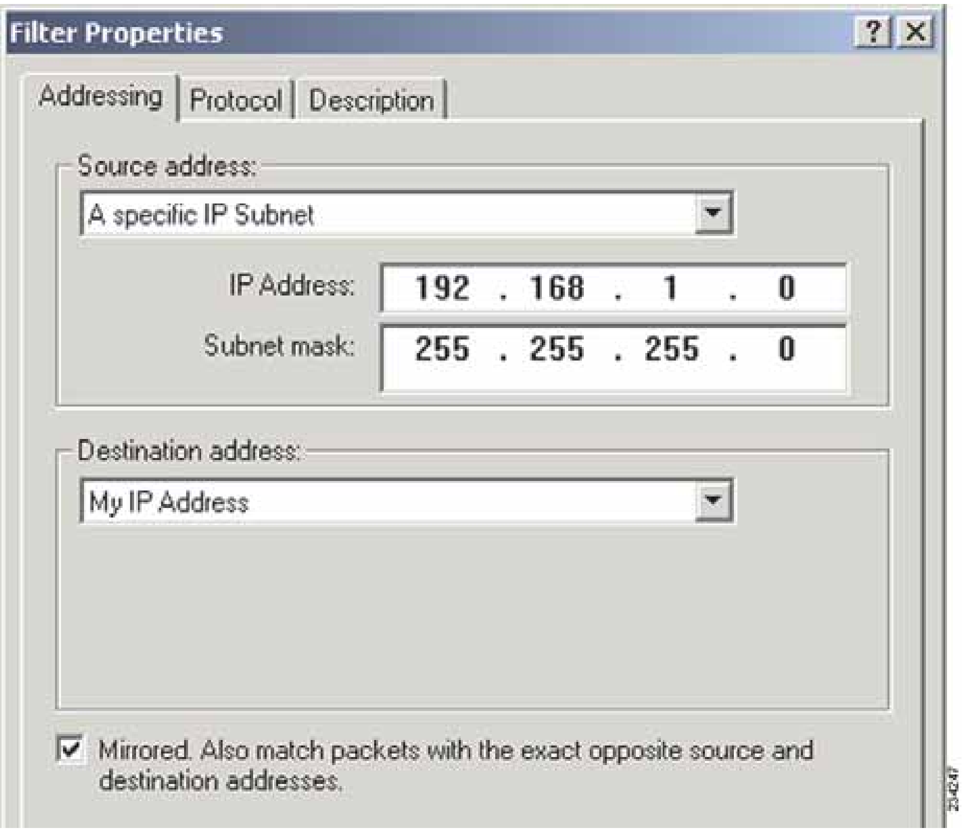
Description:

Filters:

□ Use Add Wizard

i. The Filters Properties window will appear. Select the **Addressing** tab. In the **Source address** field, select **A specific IP Subnet**, and enter the IP Address **192.168.1.0** and Subnet mask **255.255.255.0**. (Enter your new values if you have changed the default settings.) In the Destination address field, select **My IP Address**.

Filters Properties


Filter Properties

Addressing | Protocol | Description

Source address:
A specific IP Subnet
IP Address: 192 . 168 . 1 . 0
Subnet mask: 255 . 255 . 255 . 0

Destination address:
My IP Address

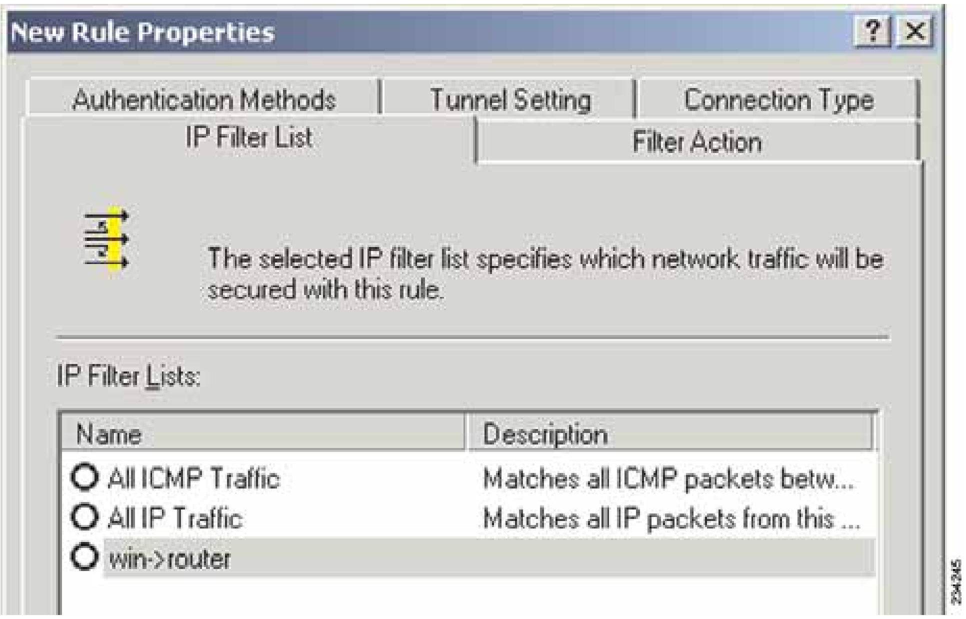
☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

j. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

k. Click **OK** or **Close**.

The New Rule Properties window appears with the **IP Filter List** tab selected. The window will contain listings for **Router->win** and **win->Router**.

New Rule Properties



The selected IP filter list specifies which network traffic will be secured with this rule.

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ win->router	

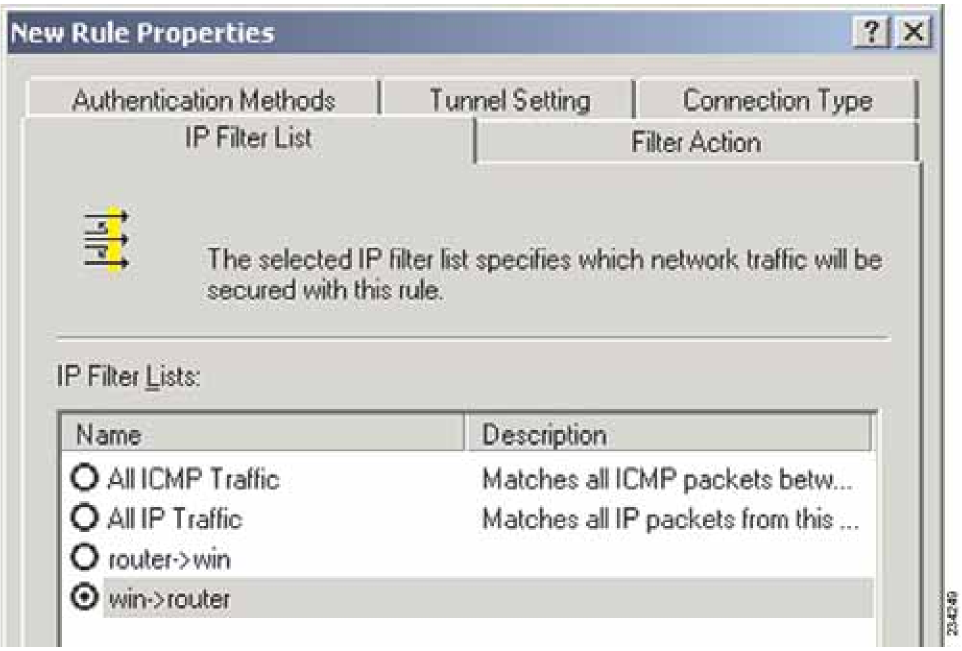
l. Click **OK** (Windows XP) or **Close** (Windows 2000) in the IP Filter List window.

STEP 3 Configure individual tunnel rules.

Tunnel 1: win->Router

a. On the **IP Filter List** tab, select filter list **win->Router**.

IP Filter List Tab



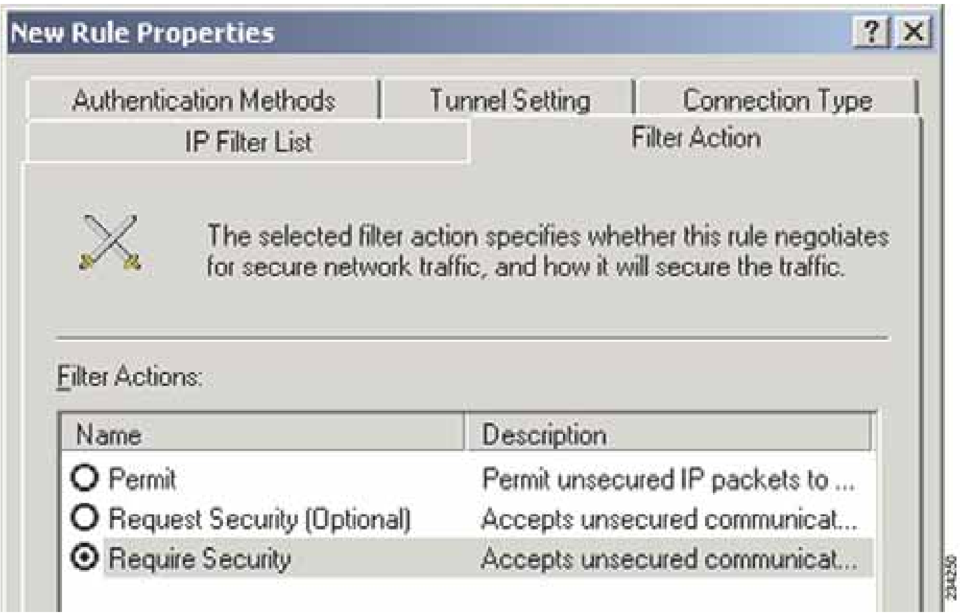
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ router->win	
● win->router	

b. Click the Filter Action tab, and click the filter action **Require Security** radio button. Then, click **Edit**.

Filter Action Tab



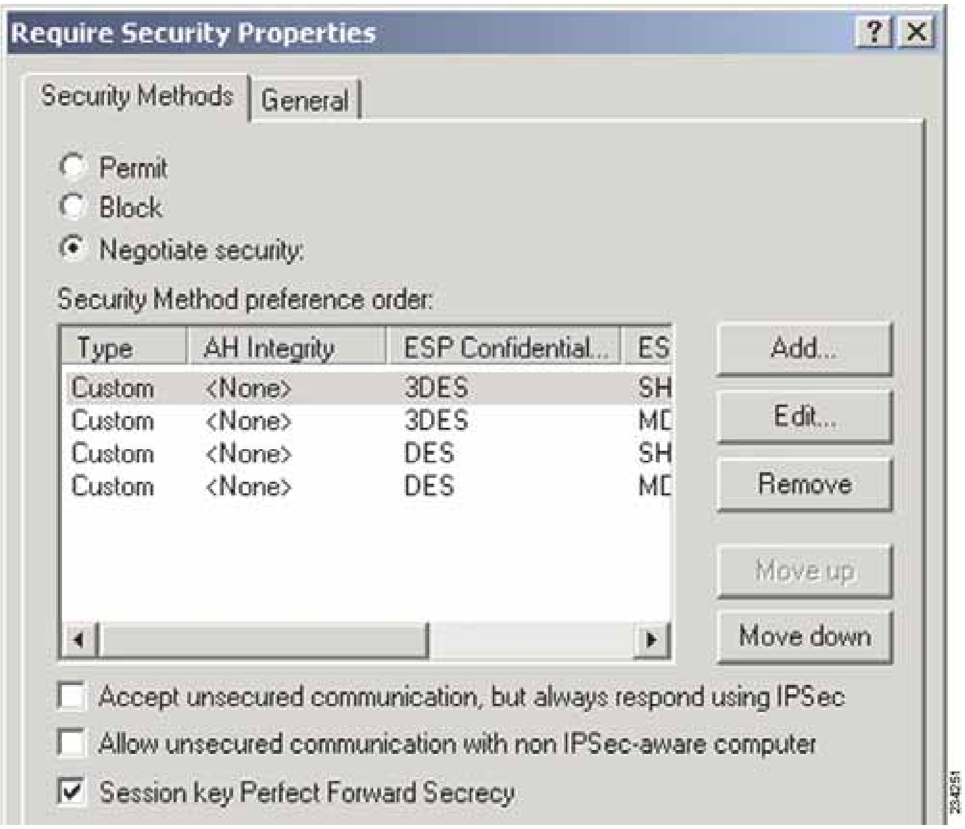
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

	Name	Description
○	Permit	Permit unsecured IP packets to ...
○	Request Security (Optional)	Accepts unsecured communicat...
●	Require Security	Accepts unsecured communicat...

c. On the Security Methods tab, verify that the **Negotiate security** option is enabled, and uncheck the **Accept unsecured communication, but always respond using IPSec** box. Select **Session key Perfect Forward Secrecy**, and click **OK**.

Security Methods Tab



Require Security Properties

Security Methods | General

○ Permit
○ Block
● Negotiate security:

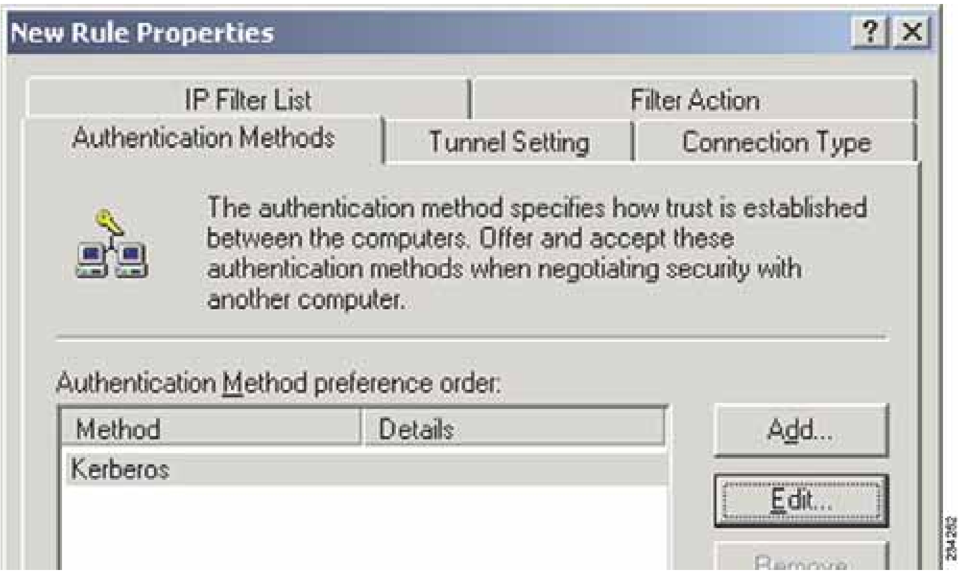
Security Method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non IPSec-aware computer
☑ Session key Perfect Forward Secrecy

d. Select the **Authentication Methods** tab, and click **Edit**.

Authentication Methods Tab



New Rule Properties

IP Filter List | Filter Action | Authentication Methods | Tunnel Setting | Connection Type

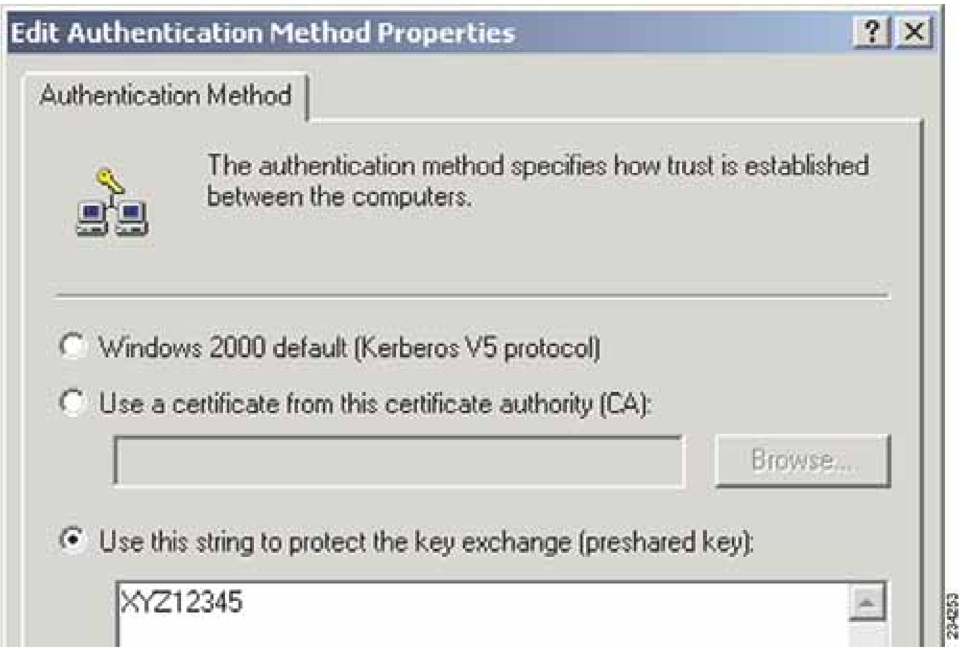
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Kerberos	

e. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345. Click **OK**.

Preshared Key



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Windows 2000 default (Kerberos V5 protocol)

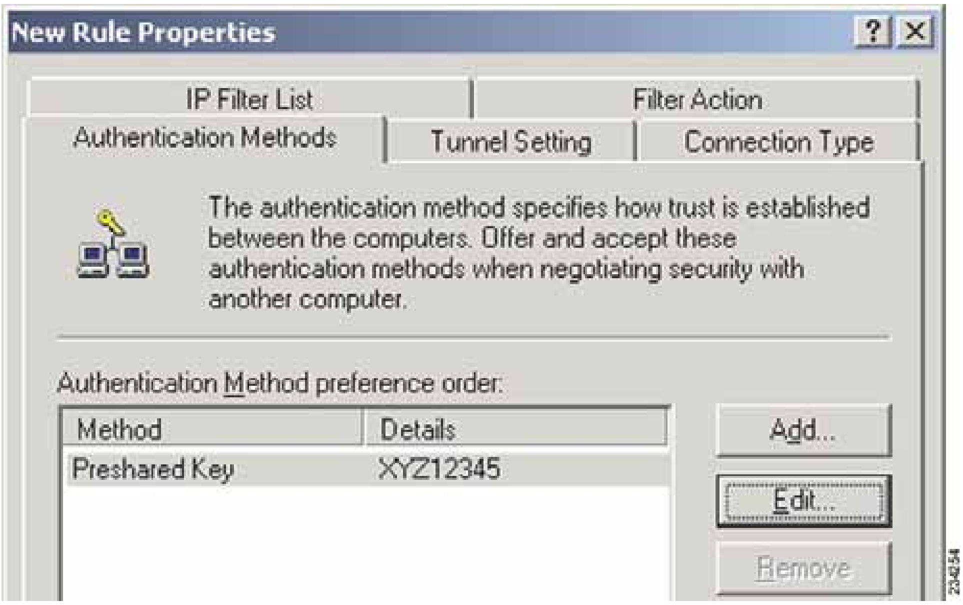
○ Use a certificate from this certificate authority (CA):

● Use this string to protect the key exchange (preshared key):

XYZ12345

f. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen; otherwise, proceed to the next step.

New Preshared Key



New Rule Properties

IP Filter List | Filter Action | Authentication Methods | Tunnel Setting | Connection Type

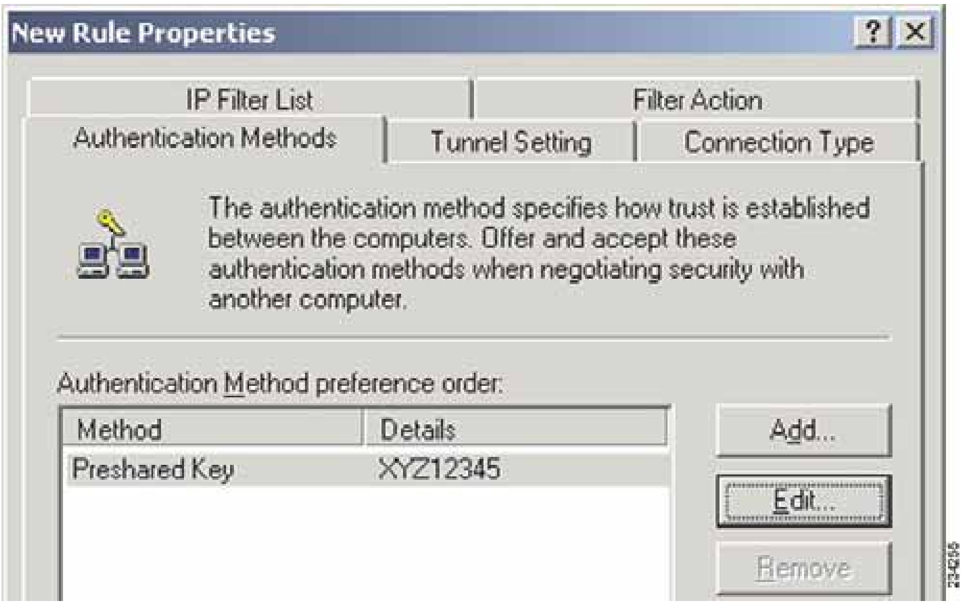
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Preshared Key	XYZ12345

g. Select the **Tunnel Setting** tab, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the router’s WAN IP Address.

Tunnel Setting Tab



New Rule Properties

IP Filter List | Filter Action | Authentication Methods | Tunnel Setting | Connection Type

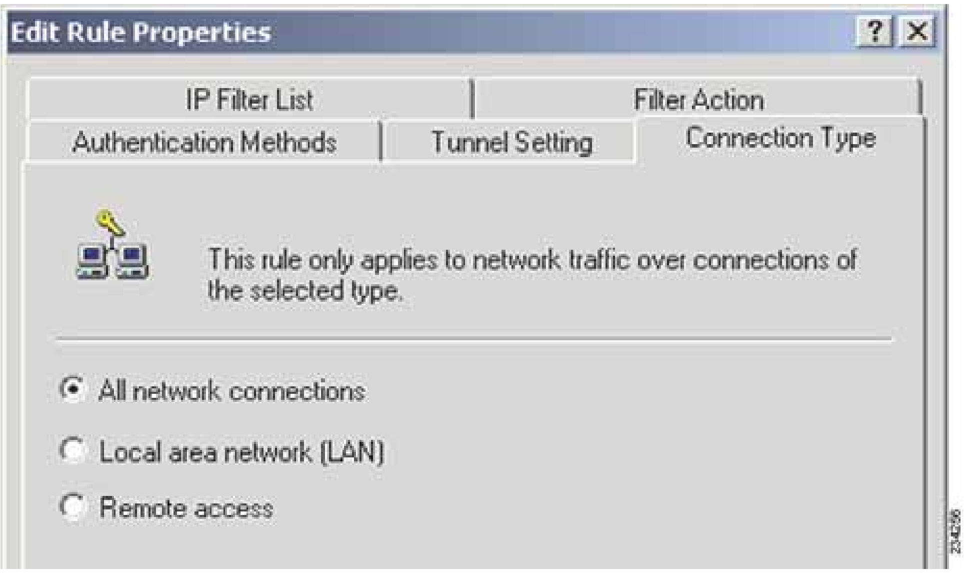
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Preshared Key	XYZ12345

h. Select the **Connection Type** tab, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

Connection Type Tab



This rule only applies to network traffic over connections of the selected type.

● All network connections

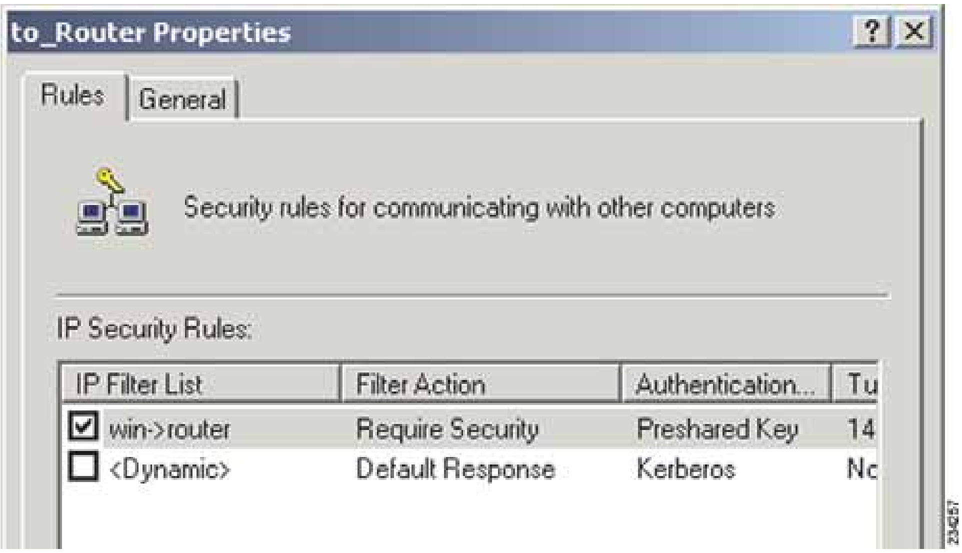
○ Local area network (LAN)

○ Remote access

Tunnel 2: Router->win

i. In the new policy's Properties window, make sure that **win -> Router** is selected and uncheck the **Use Add Wizard** box. Then, click **Add** to create the second IP filter.

Properties Window



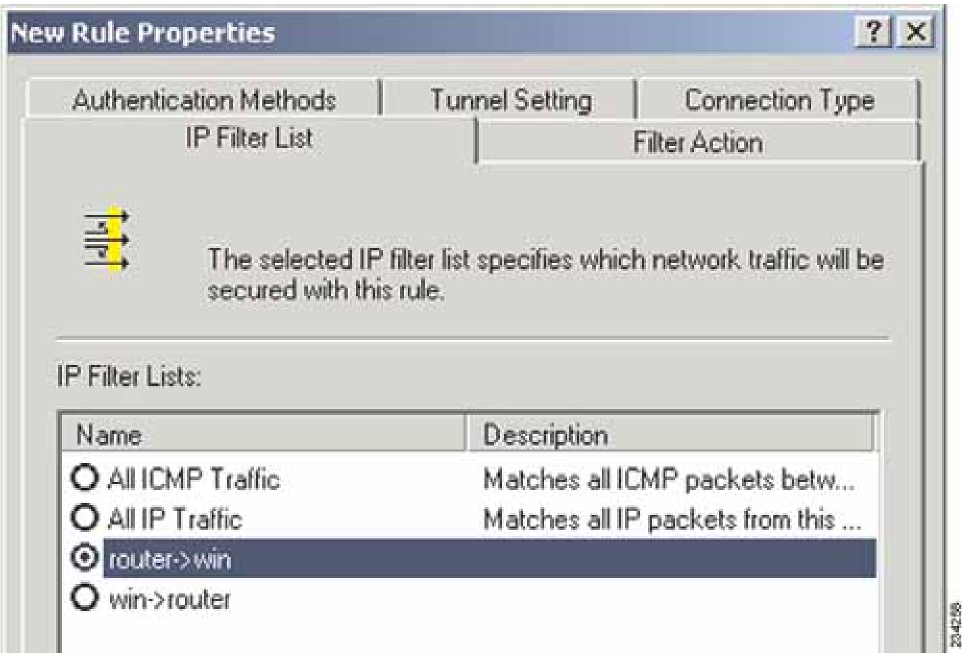
Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ win->router	Require Security	Preshared Key	14
☐ <Dynamic>	Default Response	Kerberos	Nc

j. Go to the **IP Filter List** tab, and click the filter list **Router->win**.

IP Filter List Tab



The selected IP filter list specifies which network traffic will be secured with this rule.

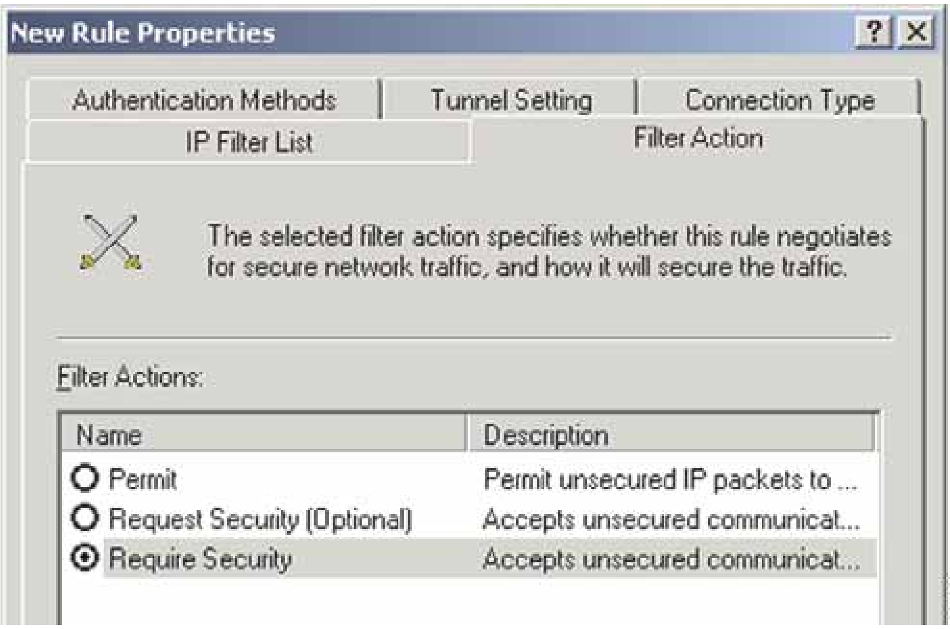
IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
◉ router->win	
○ win->router	

k. Click the **Filter Action** tab, and select the filter action **Require Security**. Then, click **Edit**. On the **Security Methods** tab, verify that the **Negotiate security** option is enabled, and uncheck the **Accept unsecured communication, but**

always respond using IPSec box. Select **Session key Perfect Forward Secrecy**, and click **OK**.

Filter Action Tab



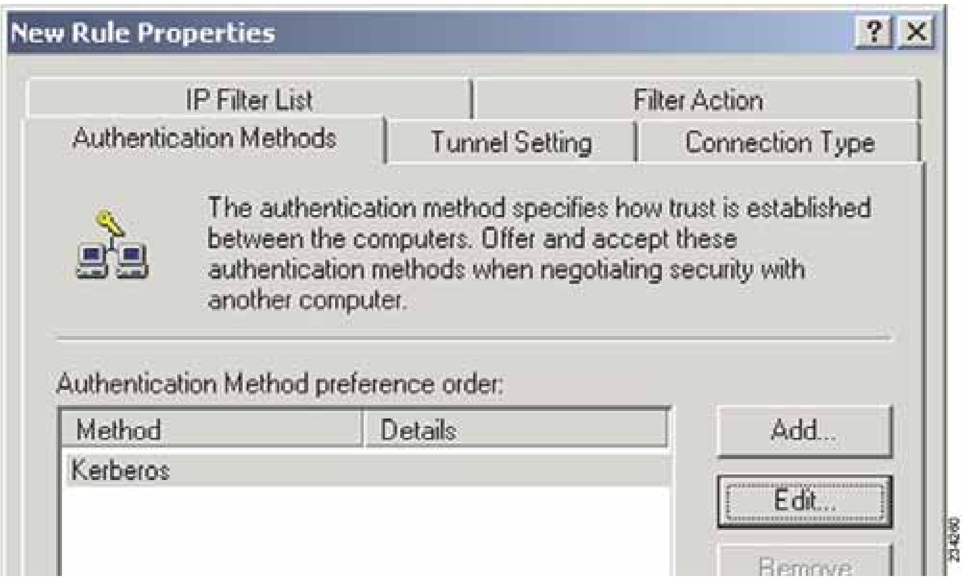
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

l. Click the **Authentication Methods** tab, and verify that the authentication method **Kerberos** is selected. Then, click **Edit**.

Authentication Methods Tab



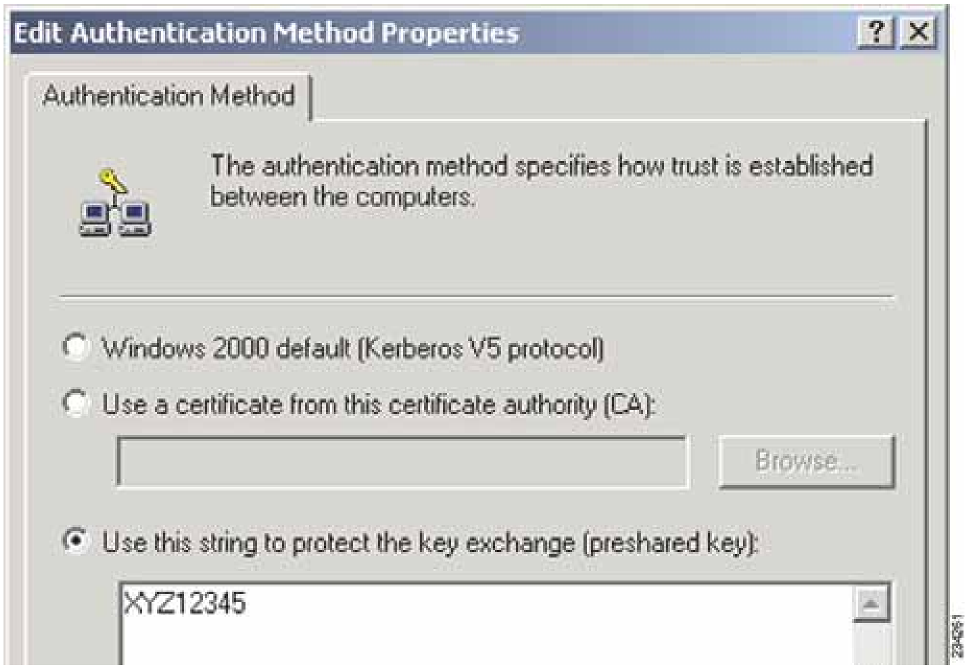
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Kerberos	

m. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click **OK**.

Preshared Key



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Windows 2000 default (Kerberos V5 protocol)

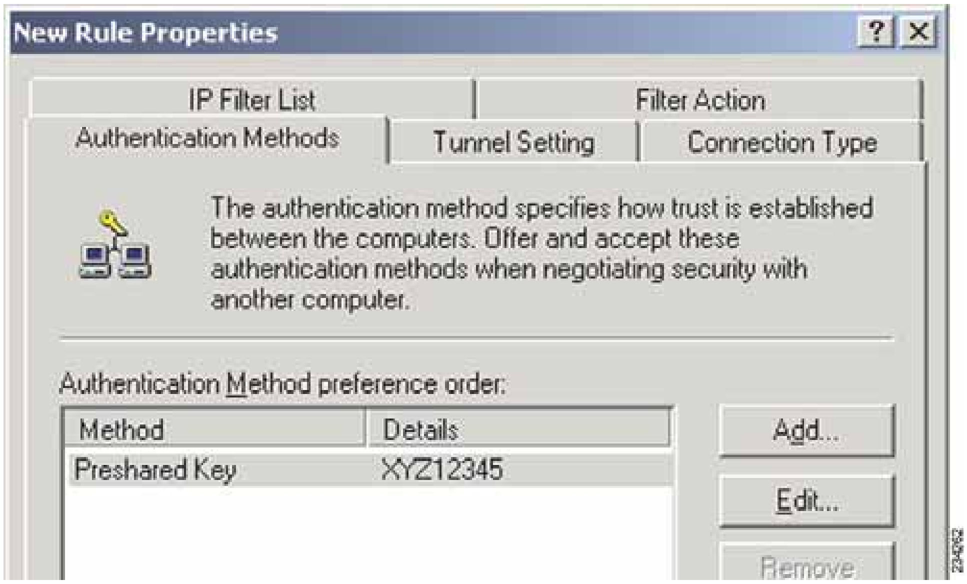
○ Use a certificate from this certificate authority (CA):

● Use this string to protect the key exchange (preshared key):

XYZ12345

n. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen; otherwise, proceed to the next step.

New Preshared Key


New Rule Properties

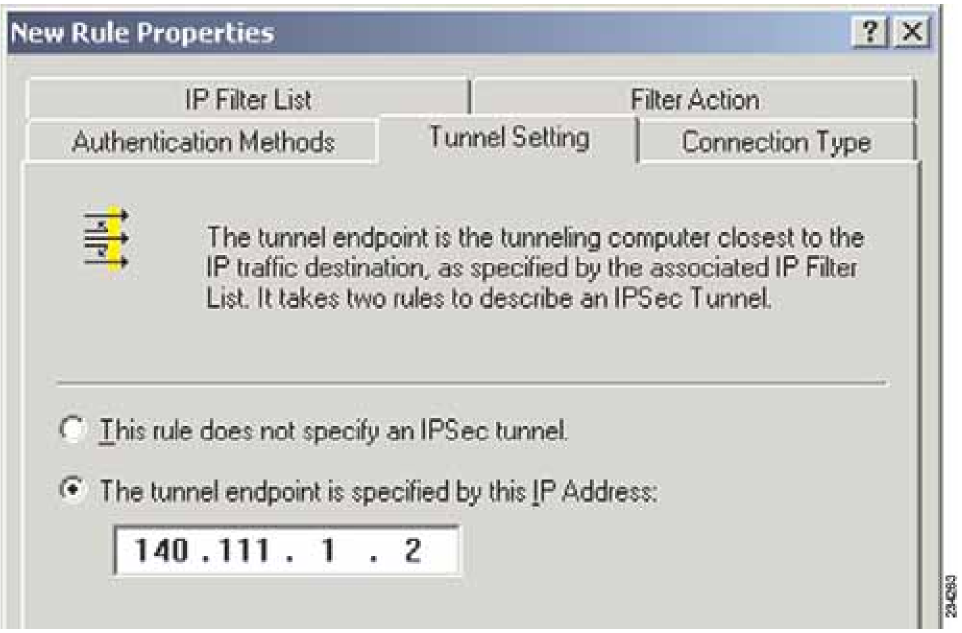
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Preshared Key	XYZ12345

o. Click the **Tunnel Setting** tab. Click the radio button **The tunnel endpoint is specified by this IP Address**, and enter the Windows 2000/XP computer’s IP Address.

Tunnel Setting Tab


New Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.

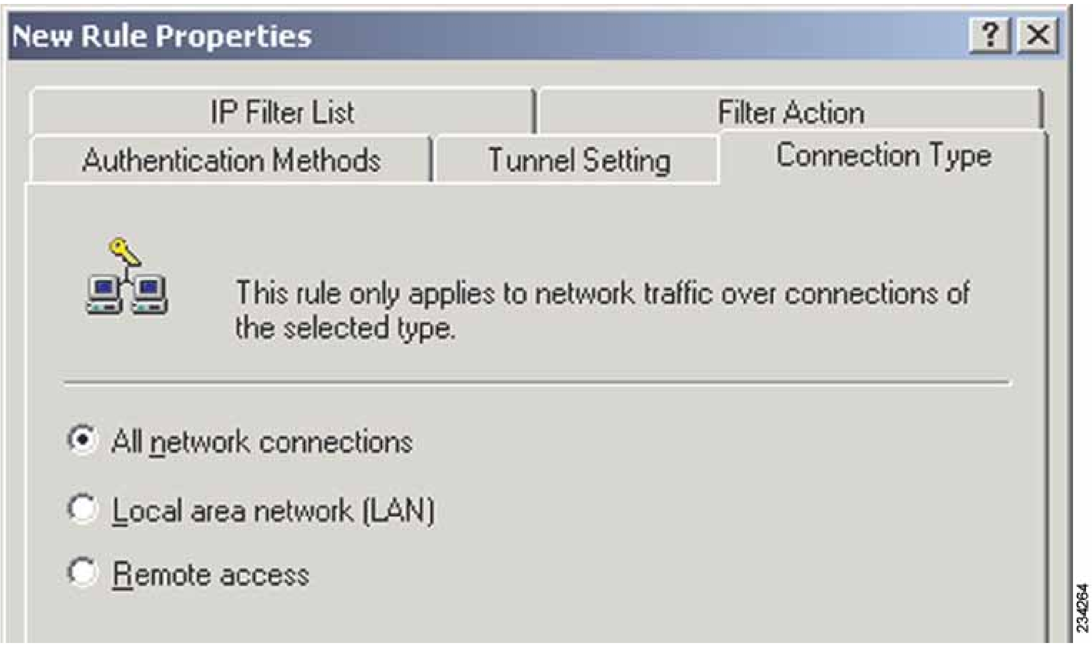
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP Address:

140 . 111 . 1 . 2

p. Click the **Connection Type** tab, and select **All network connections**. Then click **OK** or **Close** to finish.

Connection Type Tab



New Rule Properties

This rule only applies to network traffic over connections of the selected type.

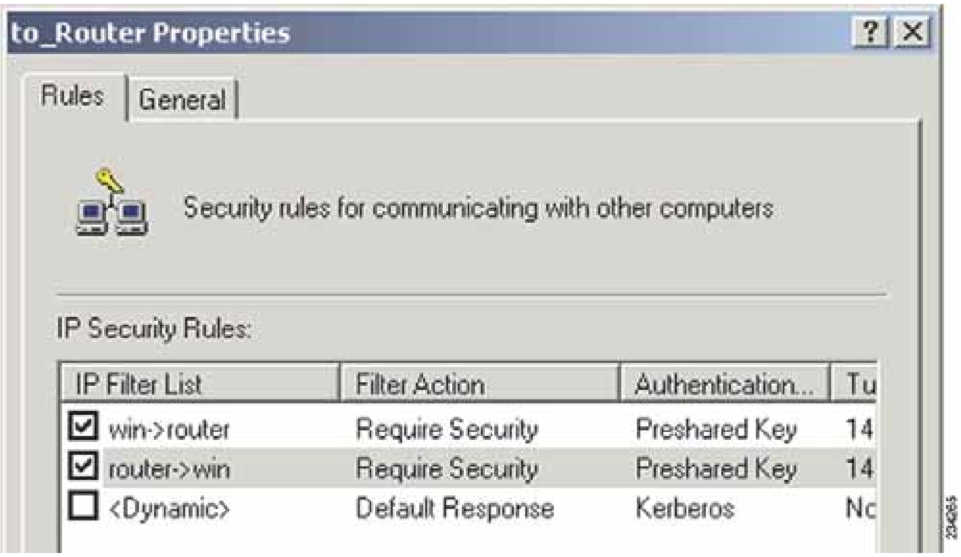
● All network connections

○ Local area network (LAN)

○ Remote access

q. On the **Rules** tab, click the **OK** or **Close** button to return to the window showing the security policies.

Rules Tab



Security rules for communicating with other computers

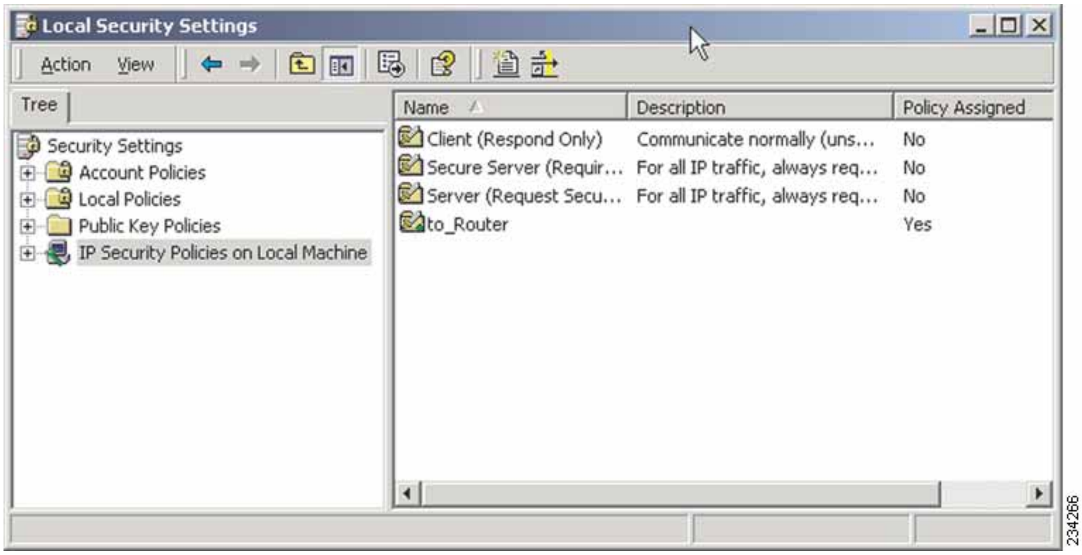
IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ win->router	Require Security	Preshared Key	14
☑ router->win	Require Security	Preshared Key	14
□ <Dynamic>	Default Response	Kerberos	Nc

STEP 4 Assign new IPSec policy.

In the IP Security Policies on Local Machine window, right-click the policy named **to_Router**, and click **Assign**. A green arrow appears in the folder icon.

Local Computer



- Security Settings
  - Account Policies
  - Local Policies
  - Public Key Policies
  - IP Security Policies on Local Machine

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_Router		Yes

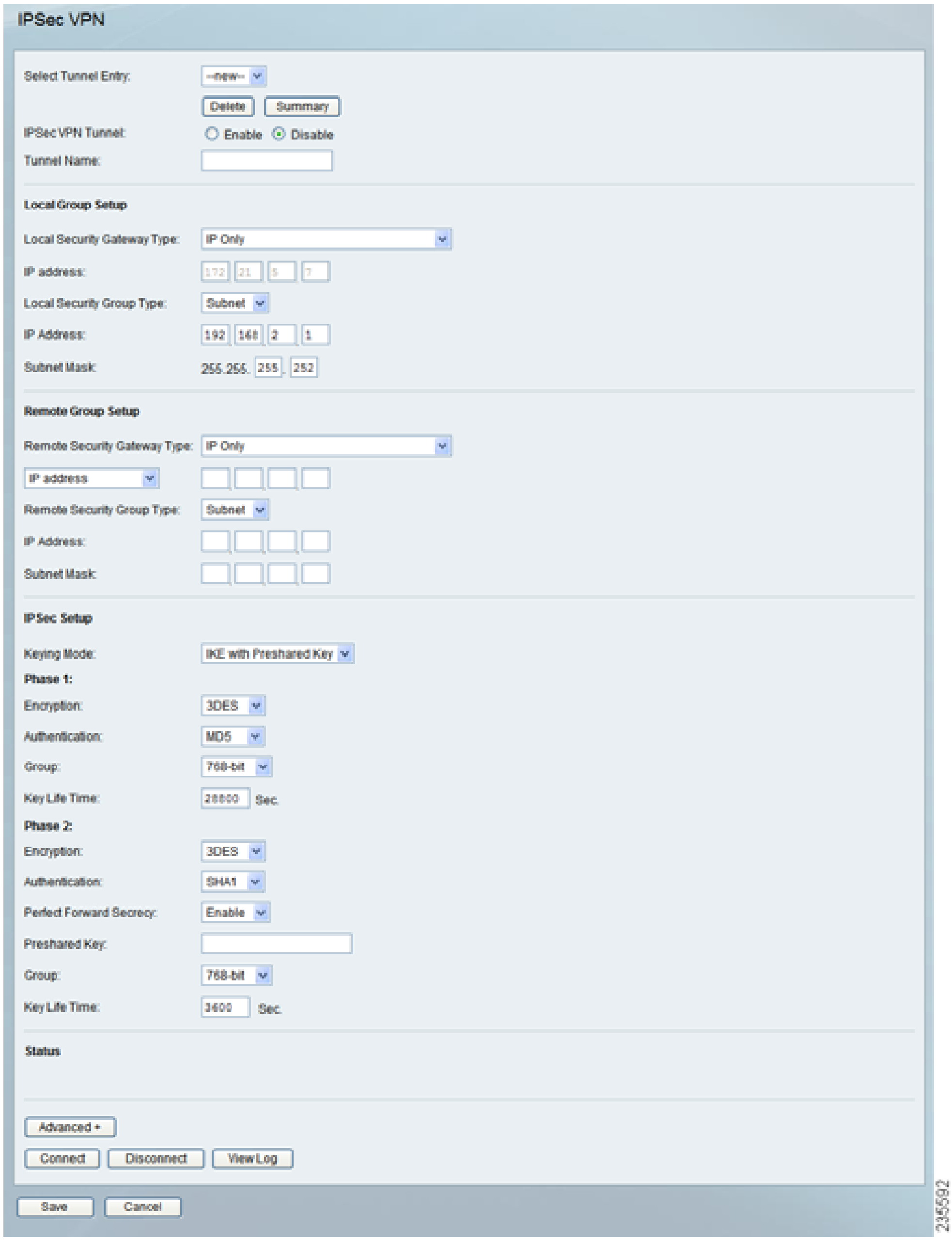
STEP 5 Create a tunnel through the configuration utility.

a. Open your web browser, and enter **192.168.1.1** in the Address field. Press **Enter**.

b. When the User name and Password fields appear, enter the default user name and password, **admin**. Press **Enter**.

c. Click **VPN > IPSec VPN**.

VPN > IPSec VPN



IPSec VPN

Select Tunnel Entry:	--new--
	Delete Summary
IPSec VPN Tunnel:	○ Enable ● Disable
Tunnel Name:	
Local Group Setup	
Local Security Gateway Type:	IP Only
IP address:	172 . 21 . 5 . 7
Local Security Group Type:	Subnet
IP Address:	192 . 168 . 2 . 1
Subnet Mask:	255.255. 255 . 252
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	

d. Select the tunnel you wish to create in the Select Tunnel Entry drop-down box. Then click **Enable**. Enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

e. Enter the IP Address and Subnet Mask of the local VPN router in the Local Group Setup fields. To allow access to the entire IP subnet, enter **0** for the last set of IP Addresses (e.g. 192.168.1.0).

f. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN router or device with which you wish to communicate) in the Remote Group Setup fields.

g. Select from two types of authentication: **MD5** and **SHA1** (SHA1 is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication.

h. From the **Keying Mode** list, choose **IKE with Preshared Key**. Then enter a series of numbers or letters in the **Preshared Key** field. Also enable **Perfect Forward Secrecy** to ensure that the initial key exchange and IKE proposals are secure.

i. Click **Save** to save these changes.

Your tunnel should now be established.

D

Gateway-to-Gateway VPN Tunnel

Overview

This appendix explains how to configure an IPSec VPN tunnel between two VPN routers by example. Two computers are used to test the liveliness of the tunnel. These sections are included:

Before You Begin

You need this equipment:

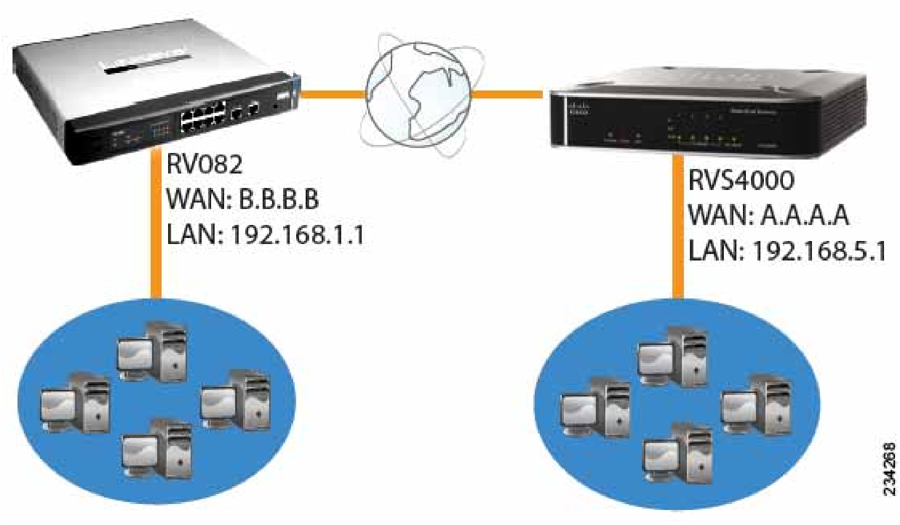
- Two Windows desktop computers (each computer will be connected to a VPN router)
- Two VPN routers (4-Port Gigabit Security Router with VPN, model number RVS4000, and 10/100 8-Port VPN Router, model number RV082) that are both connected to the Internet

Any VPN router can be deployed, such as the 10/100 16-, 8-, or 4-Port VPN Router (model numbers RV016, RV082, or RV042); however, this example uses the RV082.

Configuration when the Remote Gateway Uses a Static IP Address

This example assumes the Remote Gateway is using a static IP address. If the Remote Gateway uses a dynamic IP address, refer to**"Configuration when the Remote Gateway Uses a Dynamic IP Address," on page 171**.

Gateway-to-Gateway IPSec VPN Tunnel - Remote Gateway Using Static IP



NOTE Each computer must have a network adapter installed.

STEP 1 Configuration of the RVS4000.

Follow these instructions for the first VPN router, designated RVS4000. The other VPN router is designated the RV082.

a. Launch the web browser for a networked computer, designated PC 1.

b. Access the configuration utility of the RVS4000. (Refer to **Chapter 5, "Setting Up and Configuring the Router"** for details.)

c. Click **VPN > IPSec VPN**.

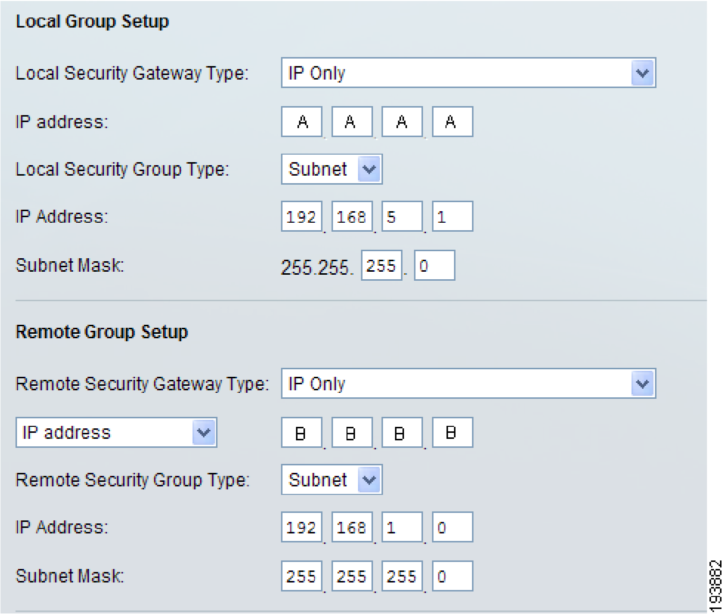
d. Enter a name in the Tunnel Name field.

e. For the IPSec VPN Tunnel setting, select **Enable**.

f. The WAN IP address (A.A.A.A) of the RVS4000 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the IP Address and Subnet Mask fields.

RVS4000 IPSec VPN Settings



Local Group Setup

Local Security Gateway Type:	IP Only
IP address:	A . A . A . A
Local Security Group Type:	Subnet
IP Address:	192 . 168 . 5 . 1
Subnet Mask:	255.255. 255 . 0

Remote Group Setup

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

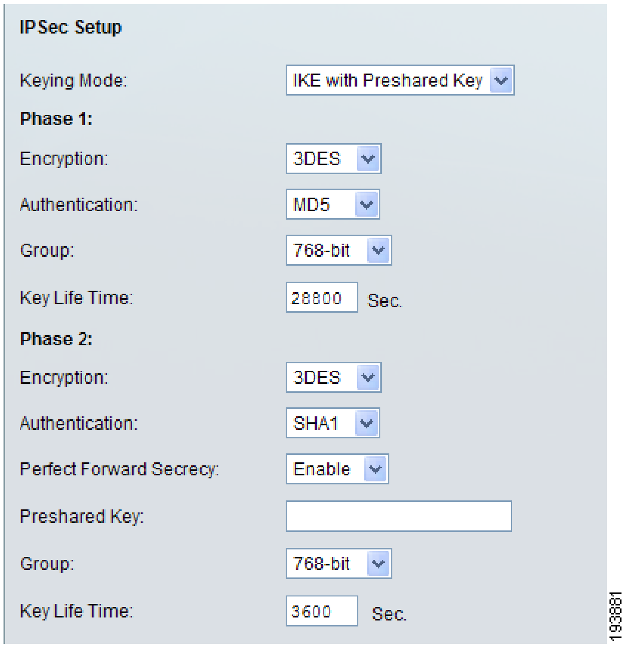
g. For the Remote Security Gateway Type, select **IP address**. Enter the RV082's WAN IP address in the IP Address field.

h. For the Remote Security Group Type, select **Subnet**. Enter the RV082's local network settings in the IP Address and Subnet Mask fields.

i. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

j. In the Preshared Key field, enter a string for this key, for example, 13572468.

RVS4000 IPSec Setup Settings



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.

k. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save** and proceed to the next step to configure the RV082.

STEP 2 Configuration of the RV082.

Follow similar instructions for the RV082.

a. Launch the web browser for a networked computer, designated PC 2.

b. Access the configuration utility of the RV082. (Refer to the of the RV082 for details.)

c. Click the **IPSec VPN** tab.

d. Click the **Gateway to Gateway** tab.

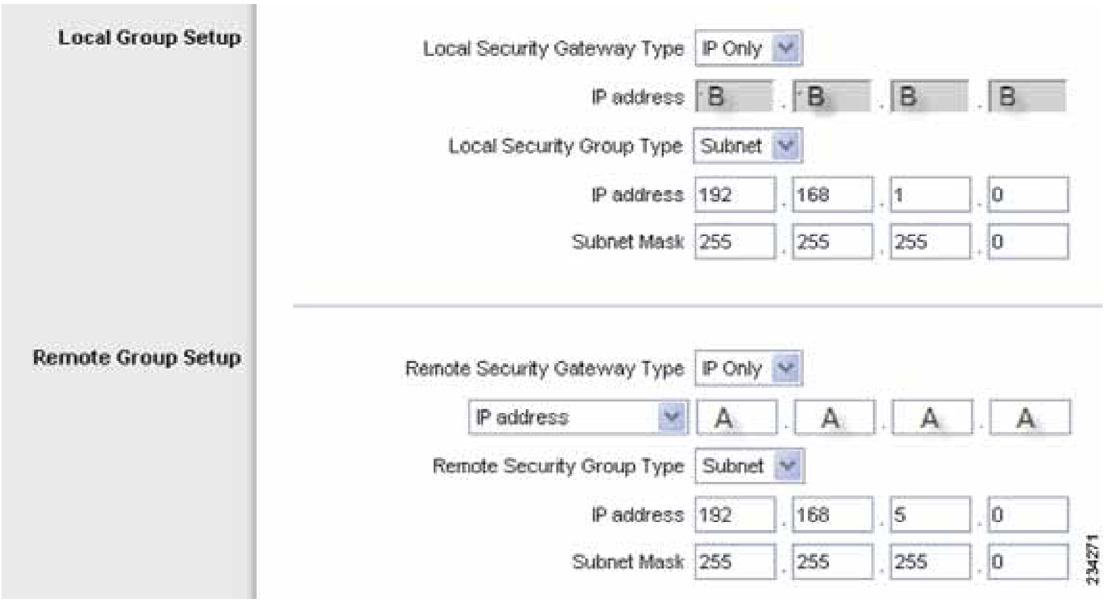
e. Enter a name in the Tunnel Name field.

f. For the VPN Tunnel setting, select **Enable**.

g. The WAN IP address (B.B.B.B) of the RV082 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RV082's local network settings in the IP Address and Subnet Mask fields.

RV082 VPN Settings



Local Group Setup

Local Security Gateway Type: IP Only

IP address: B . B . B . B

Local Security Group Type: Subnet

IP address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote Group Setup

Remote Security Gateway Type: IP Only

IP address: A . A . A . A

Remote Security Group Type: Subnet

IP address: 192 . 168 . 5 . 0

Subnet Mask: 255 . 255 . 255 . 0

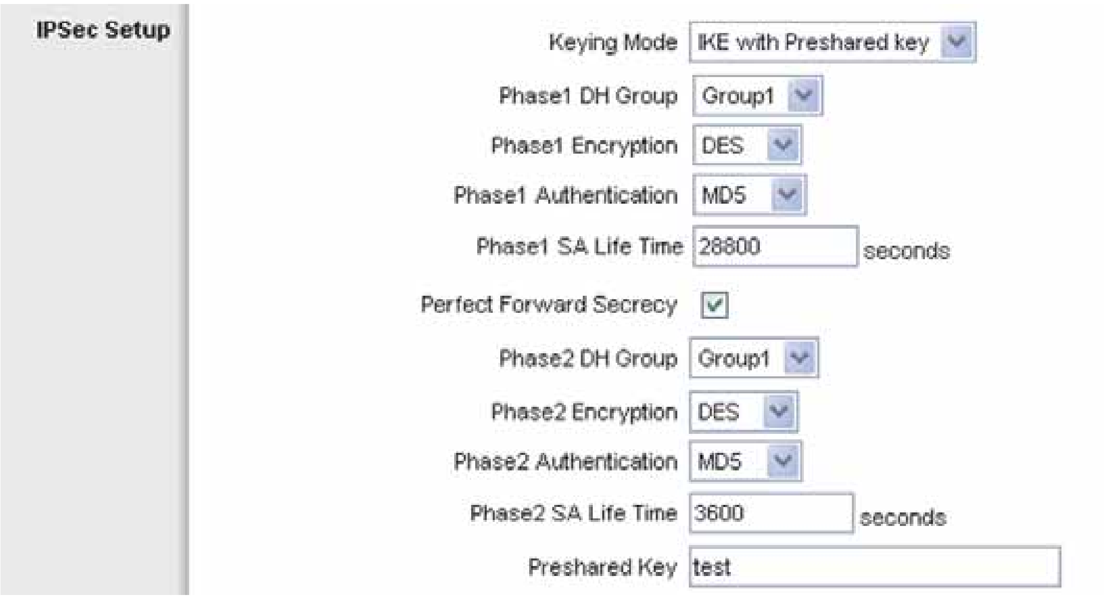
h. For the Remote Security Gateway Type, select **IP address**. Enter the RVS4000's WAN IP address in the IP Address field.

i. For the Remote Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the IP Address and Subnet Mask fields.

j. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVS4000.)

k. In the Preshared Key field, enter a string for this key, for example, 13572468.

RV082 IPSec Setup Settings



IPSec Setup

Keying Mode	IKE with Preshared key
Phase1 DH Group	Group1
Phase1 Encryption	DES
Phase1 Authentication	MD5
Phase1 SA Life Time	28800 seconds
Perfect Forward Secrecy	☑
Phase2 DH Group	Group1
Phase2 Encryption	DES
Phase2 Authentication	MD5
Phase2 SA Life Time	3600 seconds
Preshared Key	test

1. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save**.

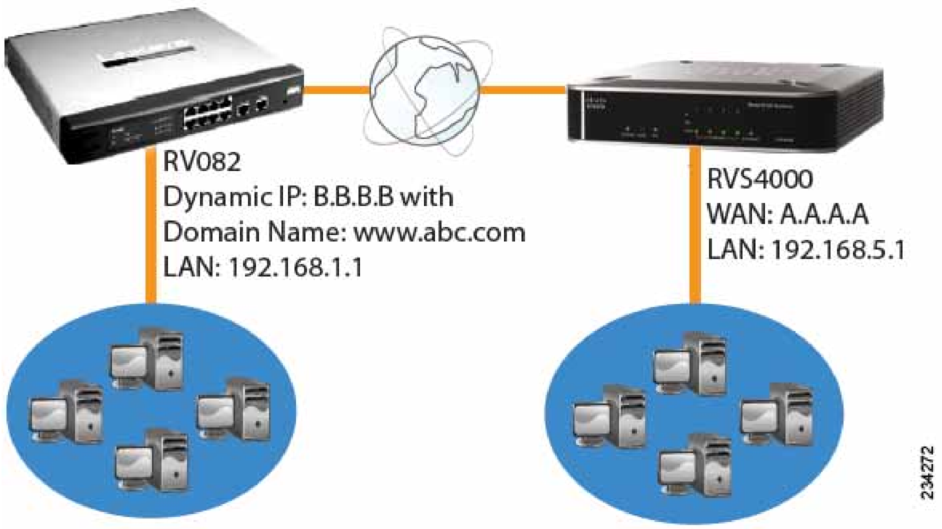
STEP 3 Configuration of PC 1 and PC 2.

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If the computers can ping each other, then you know the VPN tunnel is configured correctly.

Configuration when the Remote Gateway Uses a Dynamic IP Address

This example assumes the Remote Gateway is using a dynamic IP address. If the Remote Gateway uses a static IP address, refer to **"Configuration when the Remote Gateway Uses a Static IP Address," on page 166**.

Gateway-to-Gateway IPSec VPN Tunnel - Remote Gateway Using Dynamic IP



NOTE Each computer must have a network adapter installed.

STEP 1 Configuration of the RVS4000.

Follow these instructions for the first VPN router, designated RVS4000. The other VPN router is designated the RV082.

a. Launch the web browser for a networked computer, designated PC 1.

b. Access the configuration utility of the RVS4000. (Refer to **Chapter 5, "Setting Up and Configuring the Router"** for details.)

c. Click **VPN > IPSec VPN**.

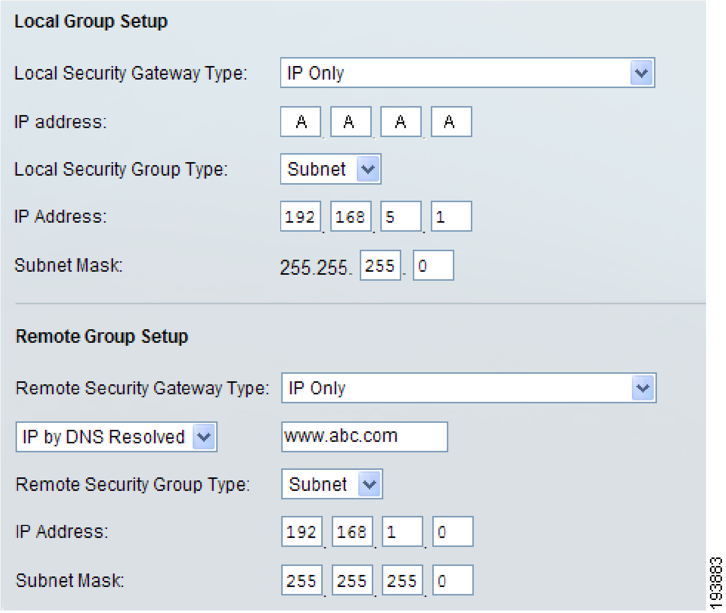
d. Enter a name in the Tunnel Name field.

e. For the IPSec VPN Tunnel setting, select **Enable**.

f. The WAN IP address (A.A.A.A) of the RVS4000 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the IP Address and Subnet Mask fields.

RVS4000 IPSec VPN Settings



Local Group Setup

Local Security Gateway Type: IP Only

IP address: A . A . A . A

Local Security Group Type: Subnet

IP Address: 192 . 168 . 5 . 1

Subnet Mask: 255.255. 255 . 0

Remote Group Setup

Remote Security Gateway Type: IP Only

IP by DNS Resolved: www.abc.com

Remote Security Group Type: Subnet

IP Address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

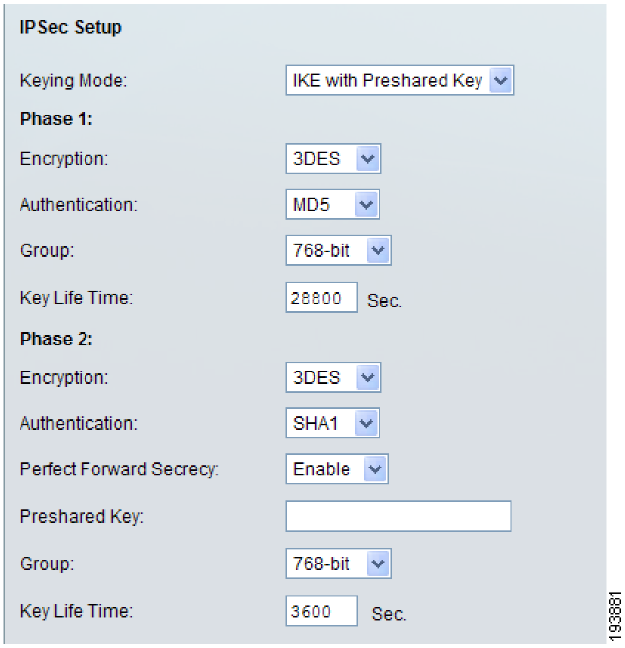
g. For the Remote Security Gateway Type, select **IP by DNS Resolved**. Enter the RV082's domain name in the field provided.

h. For the Remote Security Group Type, select **Subnet**. Enter the RV082's local network settings in the IP Address and Subnet Mask fields.

i. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

j. In the Preshared Key field, enter a string for this key. For example, 13572468.

RVS4000 IPSec Setup Settings



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.

k. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save** and proceed to the next step, “Configuration of the RV082.”

STEP 2 Configuration of the RV082.

Follow similar instructions for the RV082.

a. Launch the web browser for a networked computer, designated PC 2.

b. Access the configuration utility of the RV082. (Refer to the of the RV082 for details.)

c. Click the **IPSec VPN** tab.

d. Click the **Gateway to Gateway** tab.

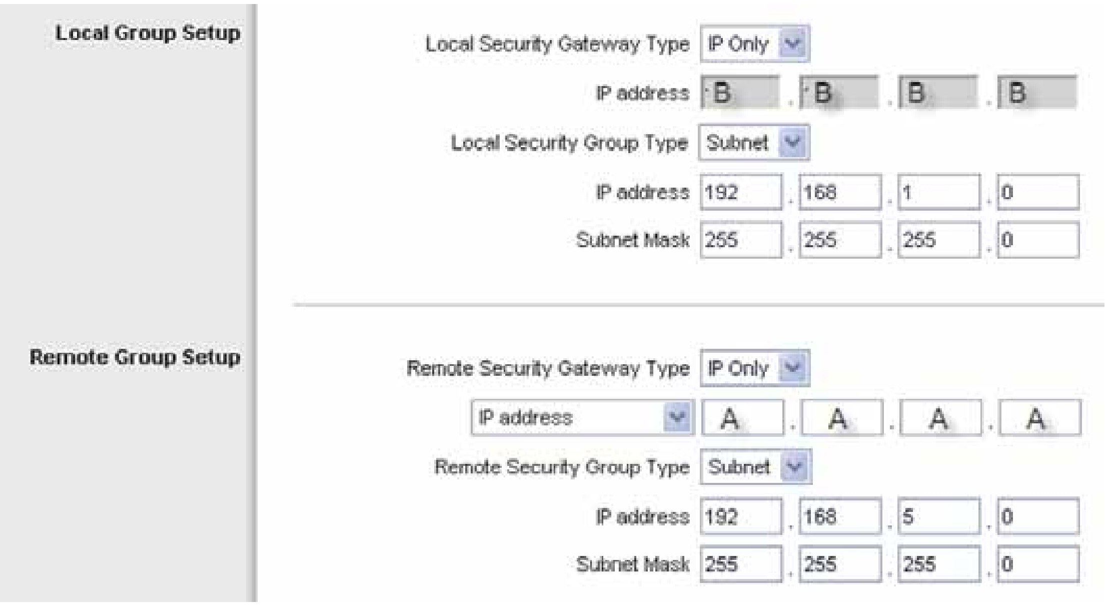
e. Enter a name in the Tunnel Name field.

f. For the VPN Tunnel setting, select **Enable**.

g. The WAN IP address (B.B.B.B) of the RV082 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RV082’s local network settings in the IP Address and Subnet Mask fields.

RV082 VPN Settings



Local Group Setup

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

Remote Group Setup

Remote Security Gateway Type: IP Only
IP address: A . A . A . A
Remote Security Group Type: Subnet
IP address: 192 . 168 . 5 . 0
Subnet Mask: 255 . 255 . 255 . 0

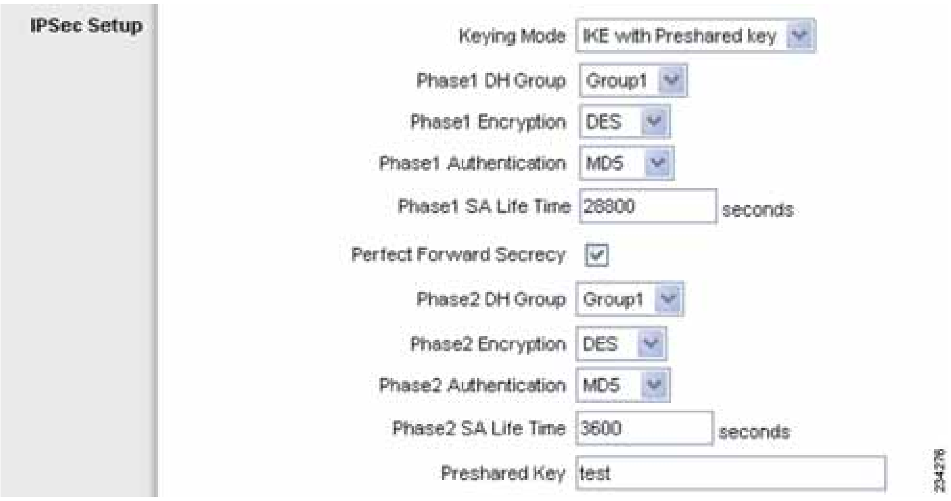
h. For the Remote Security Gateway Type, select **IP address**. Enter the RVS4000’s WAN IP address in the IP Address field.

i. For the Remote Security Group Type, select **Subnet**. Enter the RVS4000’s local network settings in the IP Address and Subnet Mask fields.

j. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVS4000.)

k. In the Preshared Key field, enter a string for this key, for example, 13572468.

RV082 IPSec Setup Settings



IPSec Setup

Keying Mode	IKE with Preshared key
Phase1 DH Group	Group1
Phase1 Encryption	DES
Phase1 Authentication	MD5
Phase1 SA Life Time	28800 seconds
Perfect Forward Secrecy	☑
Phase2 DH Group	Group1
Phase2 Encryption	DES
Phase2 Authentication	MD5
Phase2 SA Life Time	3600 seconds
Preshared Key	test

l. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save**.

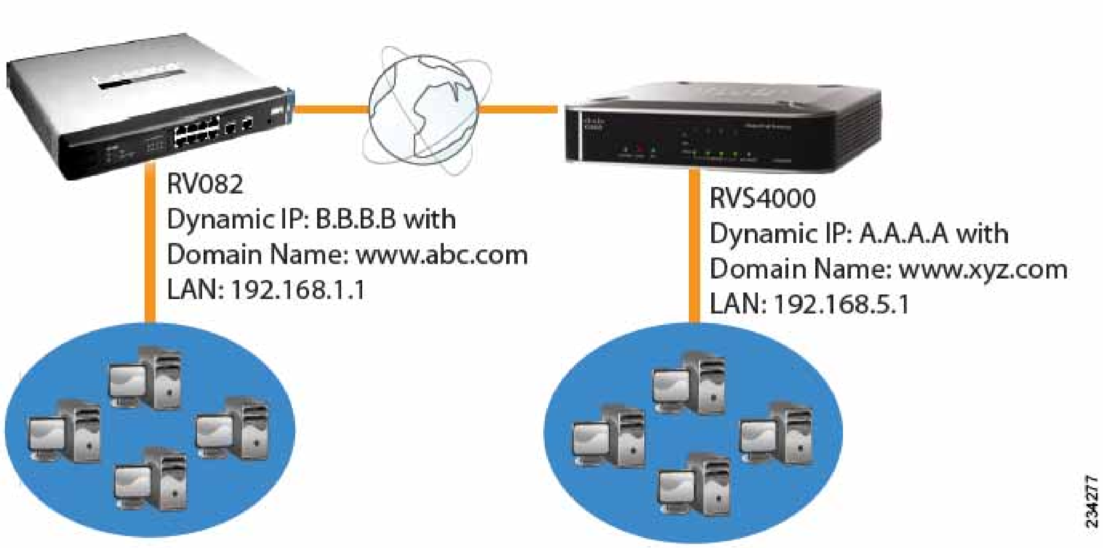
STEP 3 Configuration of PC 1 and PC 2.

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If the computers can ping each other, then you know the VPN tunnel is configured correctly.

Configuration When Both Gateways Use Dynamic IP Addresses

This example assumes both Gateways are using dynamic IP addresses. If only the Remote Gateway uses a dynamic IP address, refer to **"Configuration when the Remote Gateway Uses a Dynamic IP Address," on page 171**.

Gateway-to-Gateway IPSec VPN Tunnel - Both Gateways Using Dynamic IP



NOTE Each computer must have a network adapter installed.

STEP 1 Configuration of the RVS4000.

Follow these instructions for the first VPN router, designated RVS4000. The other VPN router is designated the RV082.

a. Launch the web browser for a networked computer, designated PC 1.

b. Access the configuration utility of the RVS4000. (Refer to **Chapter 5, "Setting Up and Configuring the Router"** for details.)

c. Click **VPN > IPSec VPN**.

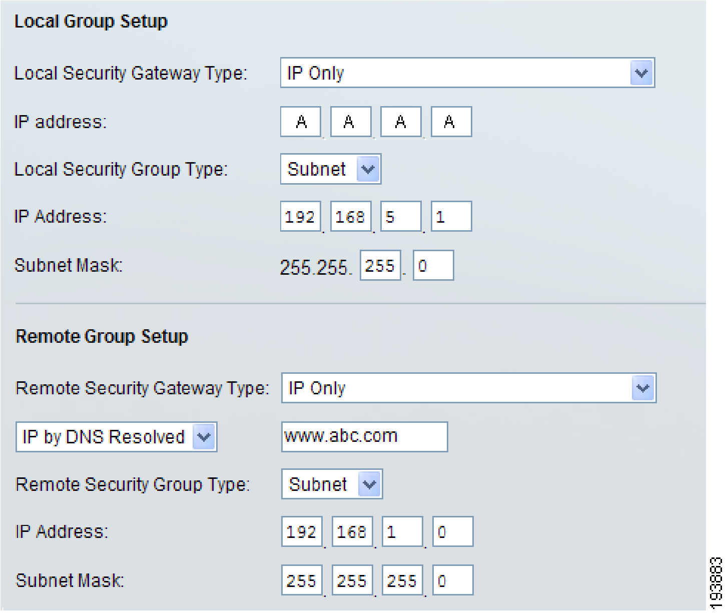
d. Enter a name in the Tunnel Name field.

e. For the IPSec VPN Tunnel setting, select **Enable**.

f. The WAN IP address (A.A.A.A) of the RVS4000 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the IP Address and Subnet Mask fields.

RVS4000 IPSec VPN Settings



Local Group Setup

Local Security Gateway Type:	IP Only
IP address:	A . A . A . A
Local Security Group Type:	Subnet
IP Address:	192 . 168 . 5 . 1
Subnet Mask:	255.255. 255 . 0

Remote Group Setup

Remote Security Gateway Type:	IP Only
IP by DNS Resolved	www.abc.com
Remote Security Group Type:	Subnet
IP Address:	192 . 168 . 1 . 0
Subnet Mask:	255 . 255 . 255 . 0

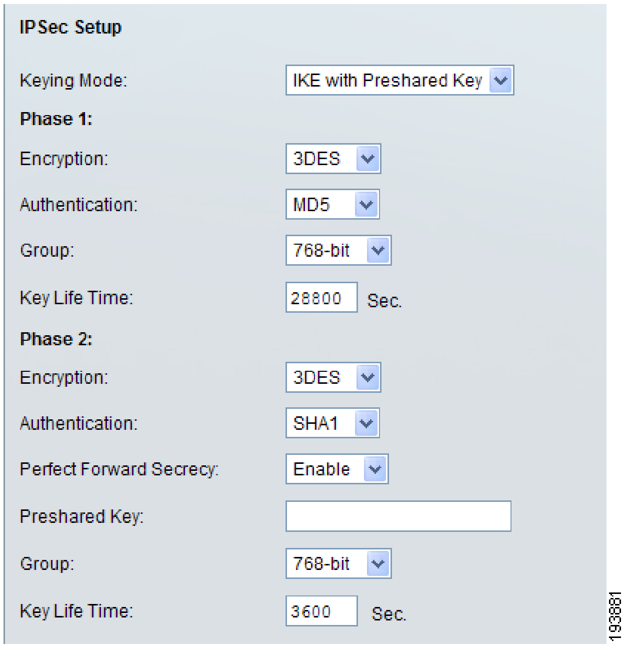
g. For the Remote Security Gateway Type, select **IP by DNS Resolved**. Enter the RV082's domain name in the field provided.

h. For the Remote Security Group Type, select **Subnet**. Enter the RV082's local network settings in the IP Address and Subnet Mask fields.

i. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.

j. In the Preshared Key field, enter a string for this key, for example, 13572468.

RVS4000 IPSec Setup Settings



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.

k. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save** and proceed to the next step, “Configuration of the RV082.”

STEP 2 Configuration of the RV082.

Follow similar instructions for the RV082.

a. Launch the web browser for a networked computer, designated PC 2.

b. Access the configuration utility of the RV082. (Refer to the of the RV082 for details.)

c. Click the **IPSec VPN** tab.

d. Click the **Gateway to Gateway** tab.

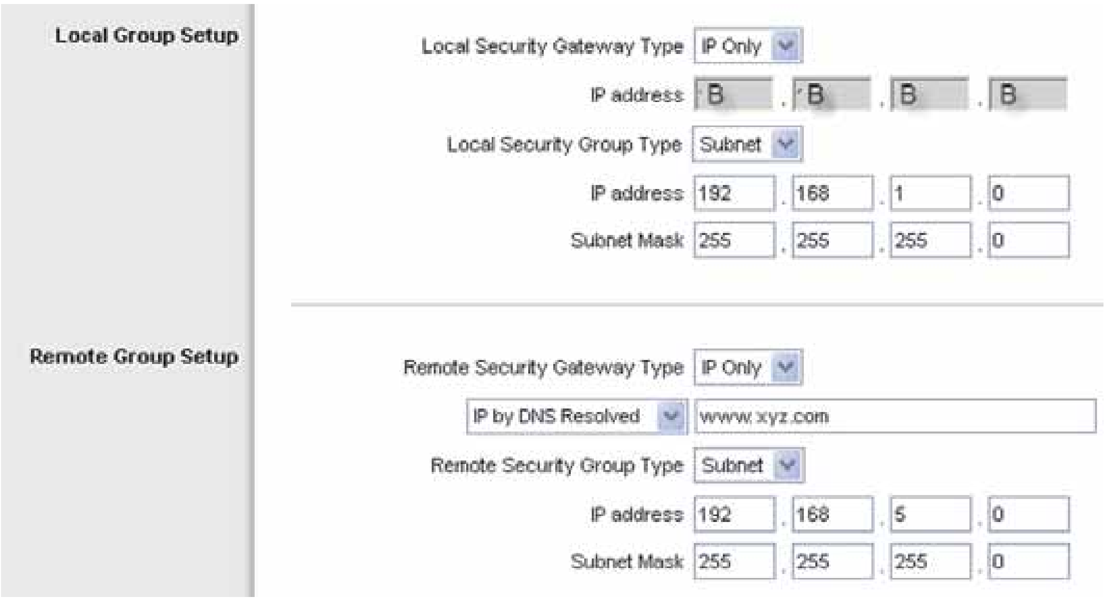
e. Enter a name in the Tunnel Name field.

f. For the VPN Tunnel setting, select **Enable**.

g. The WAN IP address (B.B.B.B) of the RV082 will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter the RV082’s local network settings in the IP Address and Subnet Mask fields.

RV082 VPN Settings



Local Group Setup

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

Remote Group Setup

Remote Security Gateway Type: IP Only
IP by DNS Resolved: www.xyz.com
Remote Security Group Type: Subnet
IP address: 192 . 168 . 5 . 0
Subnet Mask: 255 . 255 . 255 . 0

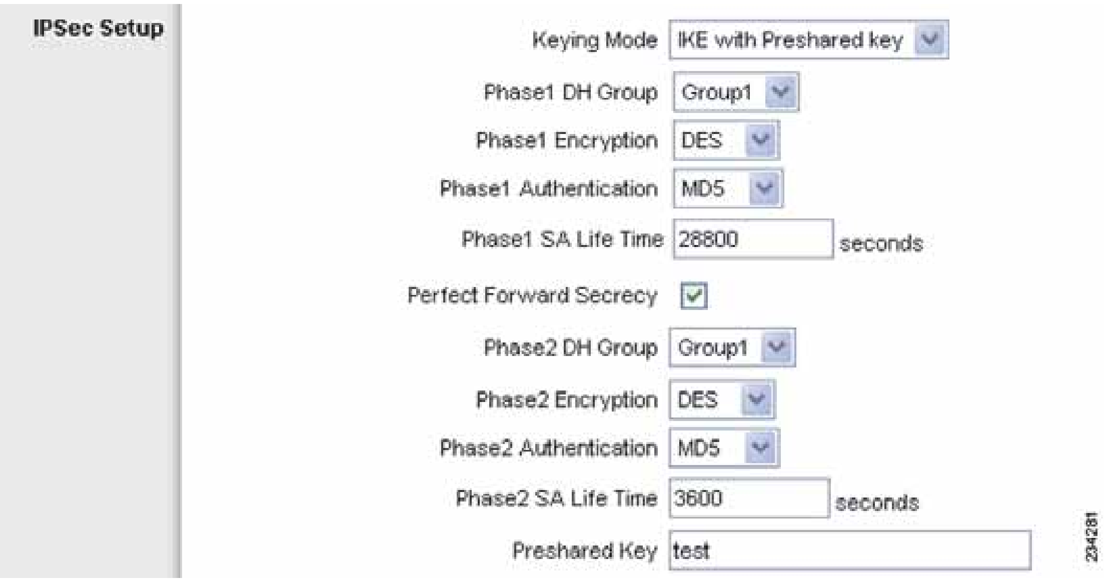
h. For the Remote Security Gateway Type, select **IP by DNS Resolved**. Enter the RVS4000's domain name in the field provided.

i. For the Remote Security Group Type, select **Subnet**. Enter the RVS4000's local network settings in the IP Address and Subnet Mask fields.

j. In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings. (These should match the settings of the RVS4000.)

k. In the Preshared Key field, enter a string for this key, for example, 13572468.

RV082 IPSec Setup Settings



IPSec Setup

Keying Mode	IKE with Preshared key
Phase1 DH Group	Group1
Phase1 Encryption	DES
Phase1 Authentication	MD5
Phase1 SA Life Time	28800 seconds
Perfect Forward Secrecy	☑
Phase2 DH Group	Group1
Phase2 Encryption	DES
Phase2 Authentication	MD5
Phase2 SA Life Time	3600 seconds
Preshared Key	test

l. If you need more detailed settings, click **Advanced Settings**. Otherwise, click **Save**.

STEP 3 Configuration of PC 1 and PC 2.

Verify that PC 1 and PC 2 can ping each other (refer to Windows Help for more information). If the computers can ping each other, then you know the VPN tunnel is configured correctly.

E

Trend Micro ProtectLink Gateway Service

Overview

The optional Trend Micro ProtectLink Gateway service provides security for your network. It scans email messages, filters website addresses (URLs), and blocks potentially malicious websites. ProtectLink is available for online purchase through online resellers such as CDW.com and PCConnection.com.

This appendix explains how to use this service and includes these sections:

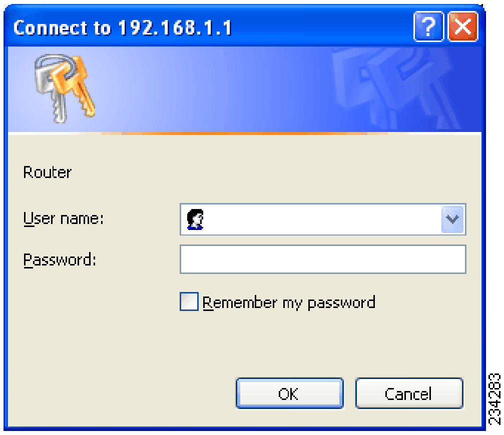
How to Access the Configuration Utility

STEP 1 For local access of the router's configuration 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.

NOTE If the Remote Management feature on the Firewall > General window has been enabled, then users with administrative privileges can remotely access the configuration 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.

STEP 2 A login window 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 window.) Then click **OK**.

Login Window



How to Purchase, Register, or Activate the Service

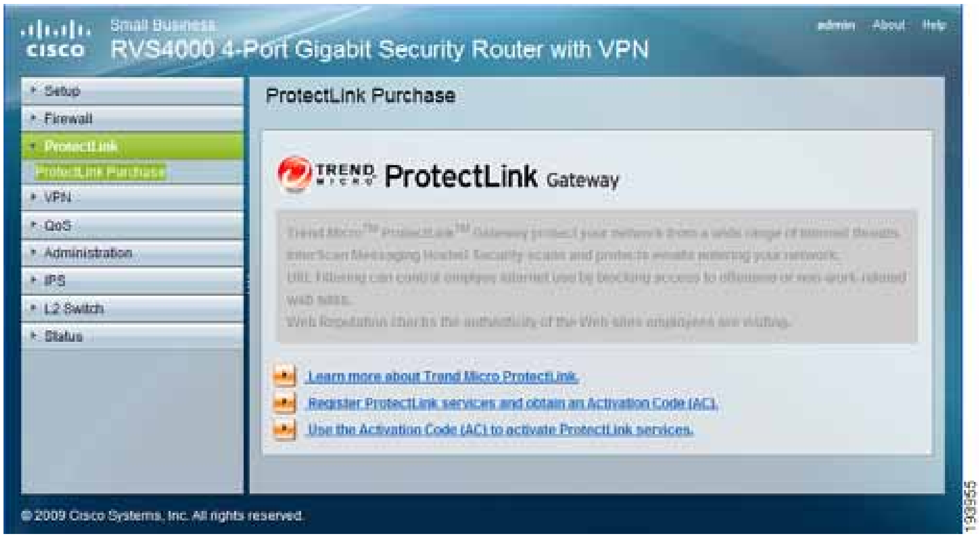
You can purchase, register, or activate the service using the ProtectLink window.

ProtectLink

Click the **ProtectLink** menu to display the ProtectLink window. This window appears if ProtectLink has not yet been activated.

NOTE If the ProtectLink menu is not displayed, upgrade the router's firmware. For the firmware download link, see **Appendix G, "Where to Go From Here."**

ProtectLink (Inactive)



Trend Micro™ ProtectLink™ Gateway protect your network from a wide range of Internet threats.
InterScan Messaging Hosted Security scans and protects emails entering your network.
URL Filtering can control employee Internet use by blocking access to offensive or non-work-related web sites.
Web Reputation checks the authenticity of the Web sites employees are visiting.

Learn more about Trend Micro ProtectLink.
Register ProtectLink services and obtain an Activation Code (AC).
Use the Activation Code (AC) to activate ProtectLink services.

© 2009 Cisco Systems, Inc. All rights reserved.

Follow the instructions for the appropriate option:

- I want to learn more about Trend Micro ProtectLink.
- I want to register online.
- I want to activate Trend Micro ProtectLink.

I want to learn more about Trend Micro ProtectLink Gateway. To learn more about this service, click this link. You will be redirected to a list of resellers for the ProtectLink Gateway service on Cisco.com.

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 email checked, you will need to provide the domain name and IP address of your email server. If you do not know this information, contact your ISP.

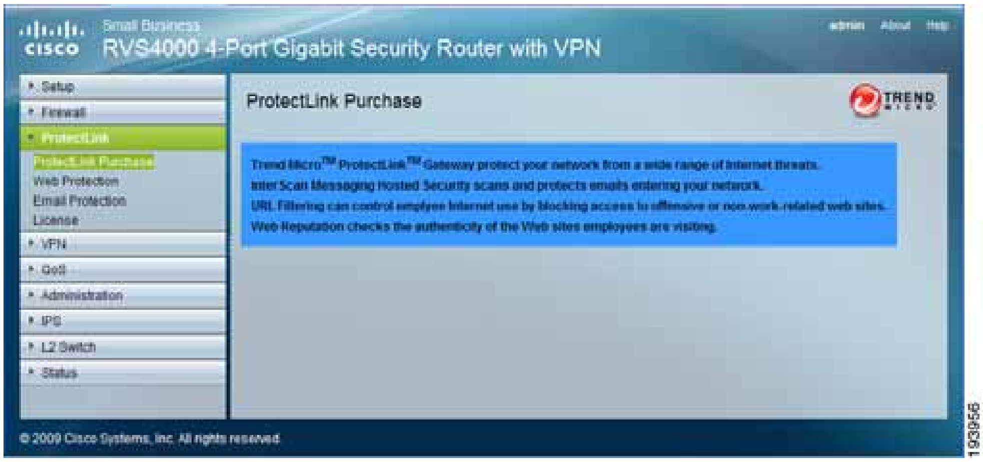
I have my Activation Code (AC) and want to activate ProtectLink Gateway. If you have registered, click this link. A wizard begins. Follow the on-screen instructions.

When the wizard is complete, the Web Protection, Email Protection, and License menus will appear.

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

After you activate ProtectLink, this window appears when you click **ProtectLink > ProtectLink Purchase** from the menu.

ProtectLink (Active)



Trend Micro™ ProtectLink™ Gateway protect your network from a wide range of Internet threats.
InterScan Messaging Hosted Security scans and protects emails entering your network.
URL Filtering can control employee Internet use by blocking access to offensive or non-work-related web sites.
Web Reputation checks the authenticity of the Web sites employees are visiting.

How to Use the Service

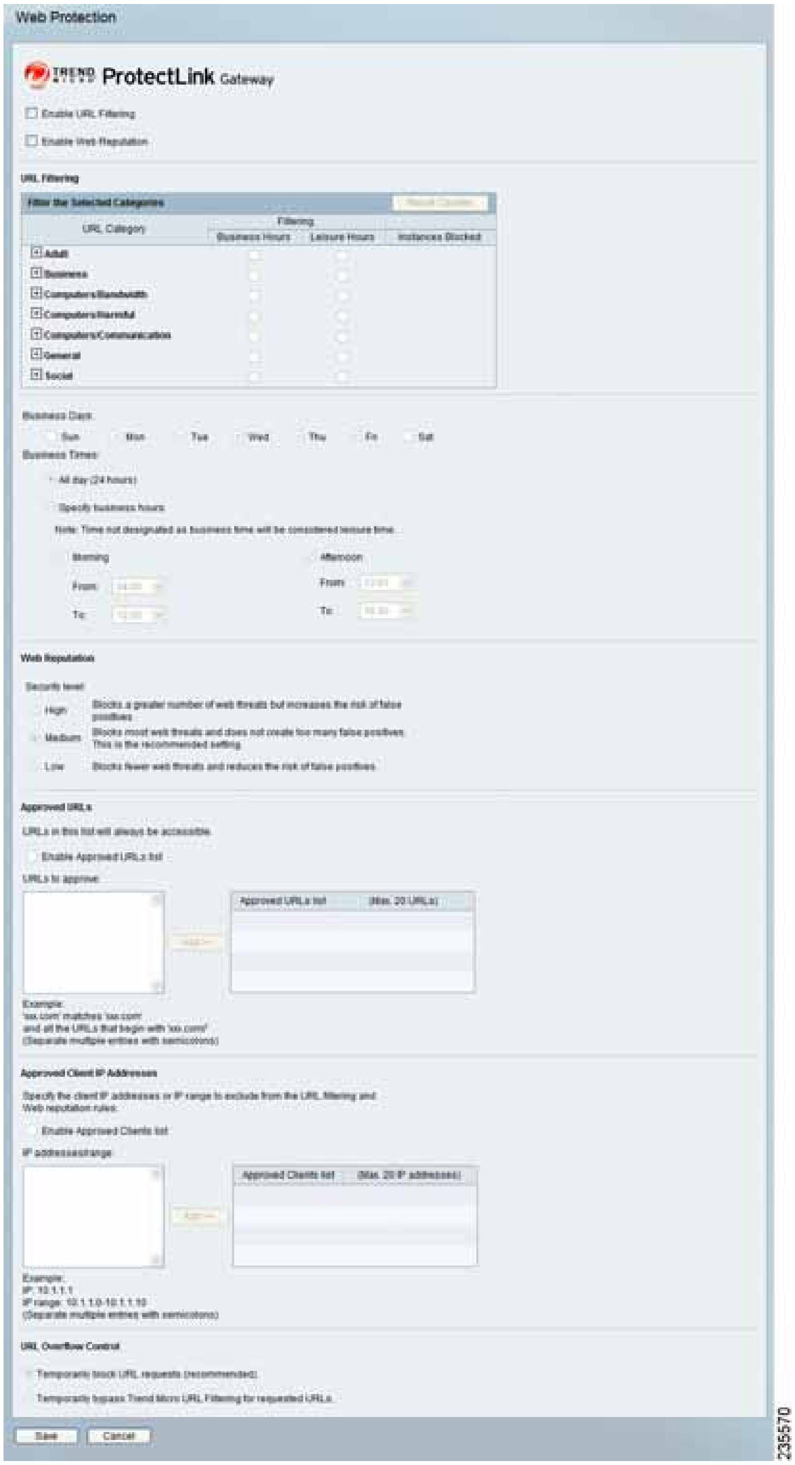
Configure the service to protect your network.

NOTE You need to purchase a ProtectLink Gateway license to use the Web Protection and Email Protection features. If you do not have a license, you will be prompted to purchase a license when you click **ProtectLink > Web Protection** or **ProtectLink > Email Protection**.

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

TREND MICRO ProtectLink Gateway

□ Enable URL Filtering

□ Enable Web Reputation

URL Filtering

Filter the Selected Categories

URL Category	Filtering		
	Business Hours	Leisure Hours	Instances Blocked
⊞ **Adult**	□	□	
⊞ **Business**	□	□	
⊞ **Computers/Bandwidth**	□	□	
⊞ **Computers/Harmful**	□	□	
⊞ **Computers/Communication**	□	□	
⊞ **General**	□	□	
⊞ **Social**	□	□	

Business Days:

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Business Times:

○ All day (24 hours)

○ Specify business hours

Note: Time not designated as business time will be considered leisure time.

□ Morning		□ Afternoon	
From:	08:00	From:	13:00
To:	12:00	To:	18:00

Web Reputation

Security level:

○ High — Blocks a greater number of web threats but increases the risk of false positives

○ Medium — Blocks most web threats and does not create too many false positives. This is the recommended setting.

○ Low — Blocks fewer web threats and reduces the risk of false positives.

Approved URLs

URLs in this list will always be accessible.

□ Enable Approved URLs list

URLs to approve:

Approved URLs list	(Max. 20 URLs)

Example:
'xxx.com' matches 'xxx.com'
and all the URLs that begin with 'xxx.com/'
(Separate multiple entries with semicolons)

Approved Client IP Addresses

Specify the client IP addresses or IP range to exclude from the URL filtering and Web reputation rules.

□ Enable Approved Clients list

IP addresses/range:

Approved Clients list	(Max. 20 IP addresses)

Example:
IP: 10.1.1.1
IP range: 10.1.1.0-10.1.1.10
(Separate multiple entries with semicolons)

URL Overflow Control

○ Temporarily block URL requests (recommended)

○ Temporarily bypass Trend Micro URL Filtering for requested URLs

Web Protection

Enable URL Filtering To filter website addresses (URLs), select this option.

Enable Web Reputation To block potentially malicious websites, select this option.

URL Filtering

Reset Counter The router counts the number of attempted visits to a restricted URL. To reset the counter to zero, click **Reset Counter**.

For each URL category, select the appropriate Filtering option. If you want to filter a sub-category, click **+** to view the sub-categories for each category. Then select the appropriate Filtering option:

Business Hours To filter this URL category during the business hours you have specified, select this option.

Leisure Hours To filter this URL category during non-business hours, select this option.

Instances Blocked The number of attempted visits is displayed.

Business Hour Setting

Business Days Select the appropriate days. The default days are **Mon.** through **Fri.**

Business Times To specify entire days, keep the default, **All day (24 hours)**. To specify hours, select **Specify business hours**. For morning hours, select **Morning**, and then select the appropriate From and To times. For afternoon hours, select **Afternoon**, and then select the appropriate From and To times.

Web Reputation

Select the appropriate security level:

High This level blocks a higher number of potentially malicious websites but also increases the risk of false positives. (A false positive is a website that can be trusted but seems potentially malicious.)

Medium This level blocks most potentially malicious websites and does not create too many false positives. The default is **Medium** and is the recommended setting.

Low This level blocks fewer potentially malicious websites and reduces the risk of false positives.

Approved URLs

You can designate up to 20 trusted URLs that will always be accessible.

Enable Approved URL list To set up a list of always accessible URLs, select this option.

URL(s) to approve Enter the trusted URL(s). Separate multiple URLs with semicolons (“**;**”).

Add To add the URLs, click **Add**.

Approved URLs list The trusted URLs are displayed. To delete a URL, click its **trash can** icon.

Approved Clients

You can designate up to 20 trusted clients (local IP addresses) that will always have access to filtered URLs.

Enable Approved Client list To set up a list of trusted clients, select this option.

IP addresses/range Enter the appropriate IP addresses or ranges. Separate multiple URLs with semicolons (“**;**”). For a range of IP addresses, use a hyphen (“**-**”). Example: 10.1.1.0-10.1.1.10.

Add To add the IP addresses or ranges, click **Add**.

Approved Clients list The IP addresses or range of trusted clients are displayed. To delete an IP address or range, click its **trash can** icon.

URL Overflow Control

Specify the behavior you want if there are more URL requests than the service can handle.

Temporarily block URL requests (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.

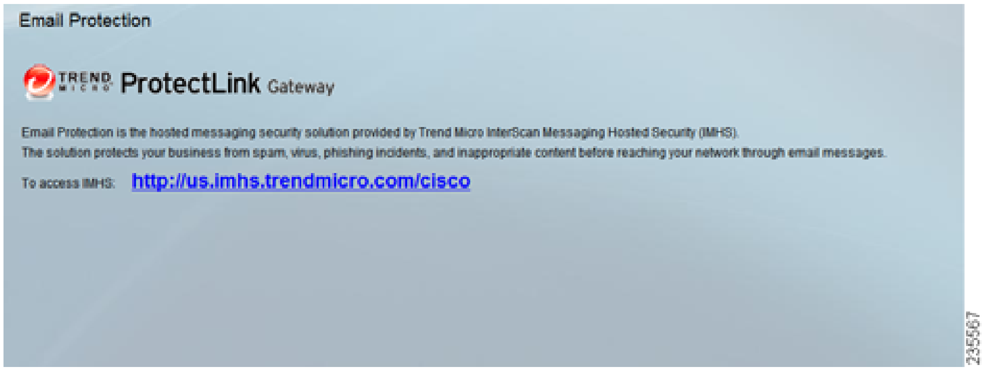
Temporarily bypass Trend Micro URL verification for requested URLs If there are too many URL requests, the overflow will be allowed without verification.

Click **Save** to save your changes, or click **Cancel** 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 email 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

TREND MICRO ProtectLink Gateway

Email Protection is the hosted messaging security solution provided by Trend Micro InterScan Messaging Hosted Security (IMHS).
The solution protects your business from spam, virus, phishing incidents, and inappropriate content before reaching your network through email messages.

To access IMHS: http://us.imhs.trendmicro.com/cisco

Email Protection

NOTE To have your email checked, you will need to provide the domain name and IP address of your email server. If you do not know this information, contact your ISP.

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

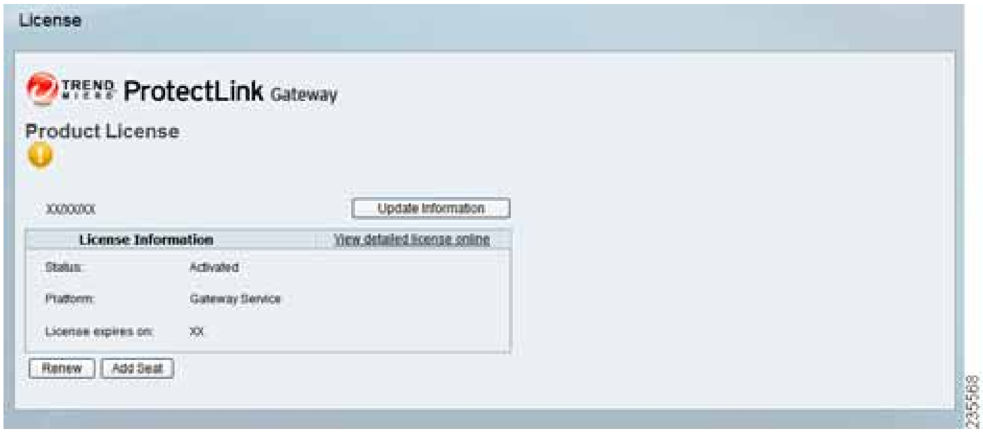
ProtectLink > License

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 window, license information is displayed. Use this window to renew your license, add seats, or view license information online.

ProtectLink > License



XXXXXX

License Information

Status: Activated

Platform: Gateway Service

License expires on: XX

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 email account to use Email Protection. To add seats to your license, click **Add Seats**. Then follow the on-screen instructions.

F

Specifications

The Cisco RVS4000 4-Port Gigabit Security Router with VPN specifications are described in this appendix.

Specifications

Model	RVS4000
Standards	IEEE802.3, 802.3u, 802.1X, RFC791 (IP Protocol), RFC2460, IPv4 (RFC791), IPv6 (RFC2460), RIPv1 (RFC1058), RIPv2 (RFC1723)
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP CAT 5e or better
LEDs	POWER, DIAG, IPS, ETHERNET (1-4), INTERNET
Operating System	Linux

Performance

NAT Throughput	800 Mbps when IPS is disabled

Setup/Config

Web User Interface	Built-in web UI for easy browser-based configuration (HTTP/HTTPS)

Management

SNMP Version	SNMP version 1, 2c
Event Logging	Local, Syslog, Email Alerts
Firmware Upgrade	Firmware available through web browser
Diagnostics	Flash, RAM

Security Features

Access Control	Access Control List (ACL) Capability: MAC-based, IP-based
Firewall	SPI stateful packet inspection firewall
Content Filtering	Static URL blocking or keyword blocking (included), Dynamic Filtering through Trend Micro™ ProtectLink™ Gateway Security Service (optional)
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
Secure Management	HTTPS, Username/Password
802.1X	Port-based RADIUS Authentication (EAP-MD5, EAP-PEAP)

QoS

Service-based	Service-based Bandwidth Management supports Rate Control and Priority
Prioritization Types	802.1p, DSCP, and Port-based
Queues	4 queues

Network

DHCP	DHCP Server, DHCP Client, DHCP Relay Agent
DNS	DNS Relay, Dynamic DNS (DynDNS, TZO)
NAT	PAT, NAPT
DMZ	Software configurable on any LAN port configuration, DHCPv6, ICMPv6
IPv6	Dual Stack IPv4 and IPv6, 6to4, Stateless Address Auto-
Static DHCP	DHCP Server supports static IP address based on MAC address

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, and IPSec

Routing

Static and RIP v1, v2 Inter-VLAN Routing

Layer 2

VLAN	Port-based and 802.1Q Tag-based VLANs
Number of VLANs	Support four 802.1Q VLANs (VLAN ID ranges from 1 to 4094)

Port Mirroring	One of the five WAN/LAN ports can be mirrored to a selected LAN port
RSTP	Supports Rapid Spanning Tree Protocol for loop detection and faster reconfiguration

Environmental

Dimensions	6.69 in. x 1.61 in. x 6.69 in.
W x H x D	(170 mm x 41 mm x 170 mm)
Unit Weight	0.84 lb (0.38 kg)
Power	12V 1A
Certification	FCC Class B, CE, ICES-003
Operating Temp.	32 to 104ºF (0 to 40ºC)
Storage Temp.	-4 to 158ºF (-20 to 70ºC)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

G

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco RVS4000 4-Port Gigabit Security Router with VPN.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation	www.cisco.com/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business _support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/smallbizfirmware Additional software for RVS4000 is available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
Product Documentation	
Cisco Small Business Routers: Resources	www.cisco.com/go/smallbizrouters
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

Related Documentation

For hardware setup for the Cisco RVS4000 router, see the *Cisco Small Business Model RVS4000 4-Port Gigabit Security Router with VPN Quick Start Guide*.

For compliance and safety information, see the *Regulatory Compliance and Safety Information for the Cisco Wired and Wireless Routers and Access Point Devices (EMC Class B Devices)*.