



ADMINISTRATION GUIDE

Cisco Small Business RV0xx Series Routers

RV042 Dual WAN VPN Router
RV042G Gigabit Dual WAN VPN Router
RV082 Dual WAN VPN Router
RV016 Multi-WAN VPN Router

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

| | |
|--|-----------|
| Chapter 1: Introduction | 7 |
| RV0xx Series Router Features | 7 |
| Ports | 9 |
| Status Lights | 10 |
| Other Hardware Features | 11 |
| Default Settings | 12 |
| Mounting Options | 12 |
| Placement Tips | 12 |
| Desktop Placement | 12 |
| Wall Mounting | 13 |
| Rack Mounting RV082 or RV016 | 14 |
| Connecting the Equipment | 15 |
| Getting Started with the Configuration | 16 |
| Troubleshooting Tips | 17 |
| Features of the User Interface | 18 |
| | |
| Chapter 2: Viewing System Summary Information | 20 |
| | |
| Chapter 3: Setup | 26 |
| Setting Up the Network | 27 |
| Changing the Administrator Username and Password | 40 |
| Setting the System Time | 42 |
| Setting Up a DMZ Host | 43 |
| Setting Up Port Forwarding and Port Triggering | 44 |
| Setting Up Universal Plug and Play (UPnP) | 48 |
| Setting Up One-to-One NAT | 51 |
| Cloning a MAC Address for the Router | 53 |
| Assigning a Dynamic DNS Host Name to a WAN Interface | 55 |
| Setting Up Advanced Routing | 57 |
| IPv6 Transition | 61 |

| | |
|--|------------|
| Chapter 4: DHCP | 63 |
| Setting Up the DHCP Server or DHCP Relay | 63 |
| Viewing the DHCP Status Information | 70 |
| Router Advertisement (IPv6) | 71 |
| Chapter 5: System Management | 73 |
| Setting Up Dual WAN and Multi-WAN Connections | 73 |
| Managing the Bandwidth Settings | 81 |
| Setting Up SNMP | 84 |
| Enabling Device Discovery with Bonjour | 85 |
| Using Built-In Diagnostic Tools | 87 |
| Restoring the Factory Default Settings | 89 |
| Upgrading the Firmware | 90 |
| Restarting the Router | 91 |
| Backing Up and Restoring the Settings | 92 |
| Chapter 6: Port Management | 95 |
| Configuring the Port Settings | 95 |
| Viewing the Status Information for a Port | 97 |
| Chapter 7: Firewall | 99 |
| Configuring the General Firewall Settings | 99 |
| Configuring Firewall Access Rules | 103 |
| Using Content Filters to Control Internet Access | 110 |
| Chapter 8: Cisco ProtectLink Web | 113 |
| Getting Started with Cisco ProtectLink Web | 113 |
| Specifying the Global Settings for Approved URLs and Clients | 115 |
| Approved URLs and Approved Clients | 116 |
| Enabling Web Protection for URL Filtering | 117 |

| | |
|---|------------|
| Updating the ProtectLink License | 120 |
| Chapter 9: VPN | 122 |
| Introduction to VPNs | 122 |
| Site to Site VPN (Gateway To Gateway) | 123 |
| Remote Access (Client To Gateway) | 123 |
| Remote Access with Cisco QuickVPN | 125 |
| Remote Access with PPTP | 125 |
| Viewing the Summary Information for VPN | 126 |
| Setting Up a Gateway to Gateway (Site to Site) VPN | 130 |
| Setting Up a Remote Access Tunnel for VPN Clients (Client To Gateway) | 139 |
| Managing VPN Users and Certificates | 147 |
| Setting Up VPN Passthrough | 149 |
| Setting Up PPTP Server | 150 |
| Chapter 10: Logging System Statistics | 153 |
| Setting Up the System Log and Alerts | 153 |
| Viewing the System Log | 157 |
| Chapter 11: Wizard | 159 |
| Appendix A: Glossary | 161 |
| Appendix B: Troubleshooting | 165 |
| Appendix C: Cisco QuickVPN for Windows | 167 |
| Introduction | 167 |
| Cisco QuickVPN Client Installation and Configuration | 168 |
| Using the Cisco QuickVPN Software | 168 |

| | |
|---|------------|
| Appendix D: Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers | 170 |
| Topology Options | 170 |
| VPN Hub and Spoke Topology | 171 |
| VPN Mesh Topology | 172 |
| Other Design Considerations | 173 |
| Configuring a VPN Tunnel on a Cisco RV0xx Series Router | 175 |
| Example: Sites with Static WAN IP Addresses | 176 |
| Example: Site with a Dynamic WAN IP Address | 179 |
| Appendix E: IPSec NAT Traversal | 183 |
| Overview | 183 |
| Appendix F: Bandwidth Management | 186 |
| Creation of New Services | 186 |
| Creation of New Bandwidth Management Rules | 187 |
| Appendix G: Specifications | 189 |
| RV042 | 189 |
| RV042G | 191 |
| Cisco RV082 | 194 |
| Cisco RV016 | 196 |
| Appendix H: Where to Go From Here | 199 |

Introduction

Thank you for choosing a RV0xx Series VPN Router. This guide provides complete information to help you configure and manage your router. This chapter includes information to help you get started using your router. Refer to these topics:

- [RV0xx Series Router Features, page 7](#)
- [Mounting Options, page 12](#)
- [Connecting the Equipment, page 15](#)
- [Getting Started with the Configuration, page 16](#)
- [Features of the User Interface, page 18](#)

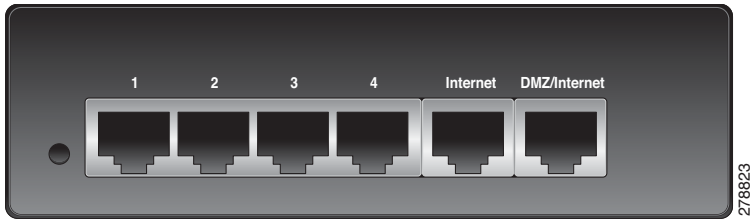
RV0xx Series Router Features

Cisco RV0xx Series dual WAN and multi-WAN VPN routers offer highly secure, high-performance, reliable connectivity. All of these routers can support a second Internet connection to ensure continuous connectivity or to increase available bandwidth and balance traffic. Three models are available. A comparison is provided below.

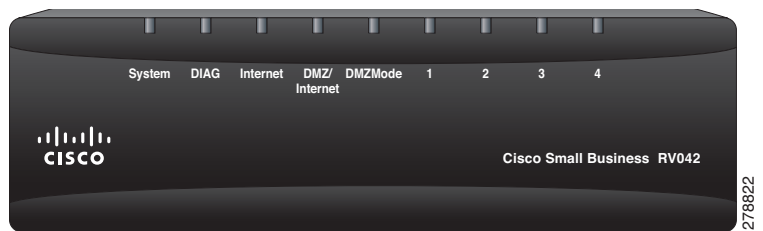
| Model | LAN Ports | WAN/DMZ Ports |
|-------------------------|-----------|-----------------------|
| RV042 and RV042G | 4 | 2 |
| RV082 | 8 | 2 |
| RV016 | 8-13 | 2-7 Internet 1 DMZ |

NOTE RV042, RV042G, and RV082 have one dedicated Internet port and a DMZ/Internet port. RV016 has two dedicated Internet ports, one dedicated DMZ port, and five dual-function ports that can be configured as LAN or Internet ports.

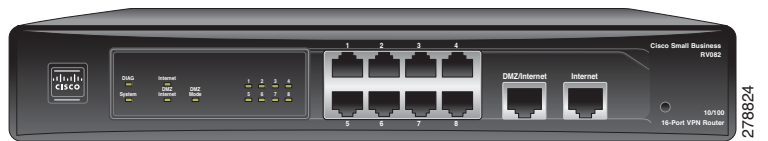
RV042 and RV042G Ports



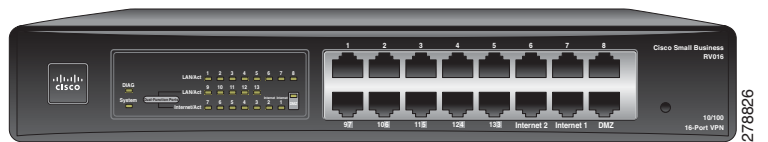
RV042 and RV042G Status Lights



RV082 Ports and Status Lights



RV016 Ports and Status Lights



Ports

| Port | Description |
|---|--|
| Internet (RV042 and RV082) or Internet 1-2 (RV016) | Use this port to connect the router to a broadband network device. |
| DMZ/Internet (RV042 and RV082) | Use this port to connect the router to either a second broadband network device or a DMZ host such as a web server or FTP server. A DMZ allows public Internet traffic to access a specified computer on your network without exposing your LAN. |
| DMZ (RV016) | Use this port to connect the router to a DMZ host such as a web server or FTP server. A DMZ allows public Internet traffic to access a specified computer on your network without exposing your LAN. |
| 1-4 (RV042 and RV042G) or 1-8 (RV082 and RV016) | Use these numbered ports to connect computers and other local network devices. |
| 9-13 and 3-7 Dual Function Ports (RV016) | Use these numbered ports as LAN ports (numbered 9-13) or configure them for use as Internet ports (numbered 3-7). The status is shown on the corresponding status lights: LAN/Act 9-13 or Internet/Act 3-7. |

Status Lights

| Light | Description |
|--|--|
| DIAG | Lit —The router is preparing for use. Unlit —The router is ready for use. |
| System | Steady —The router is powered on. Flashing —The router is running a diagnostic test. |
| Internet (RV082, RV042, RV042G) or Internet 1-2 (RV016) | Steady —A device is connected to the Internet port. Flashing —There is network activity over the Internet port. |
| DMZ/Internet (RV082, RV042, RV042G) or DMZ (RV016) | Steady —A device is connected to the DMZ/Internet or DMZ port. Flashing —There is network activity over the port. |
| DMZ Mode (RV082, RV042, RV042G) | Lit —The DMZ/Internet port is configured as a DMZ. Unlit —The DMZ/Internet port is configured as a secondary Internet connection. |
| 1-4, 1-8 | Steady —A device is connected to the numbered LAN port. Flashing —There is network activity over the numbered port. |
| RV042G Gigabit Ports | For the Internet, DMZ/Internet, and numbered ports, the color indicates the speed. Green —Gigabit. Amber —10/100M. |
| RV016 Dual-Function Ports: | |
| LAN/Act 9-13 | Lit if the port is configured as a LAN port. Steady —A device is connected to the port. Flashing —There is network activity over the port. |
| Internet/Act 3-7 (RV016) | Lit if the port is configured as an Internet port. Steady —A device is connected to the port. Flashing —There is network activity over the port. |

Other Hardware Features

| Feature | Description |
|----------------------|--|
| Reset | <p>The Reset button is an indented black button. On the back panel of the RV042 and RV042G, look for this button near the port labeled 1. On the front panel of the RV082 and RV016, look for this button near the Internet and DMZ ports .</p> <ul style="list-style-type: none"> ▪ To restart the router or restore connectivity: If the router is having problems connecting to the Internet, use the tip of a pen to press and hold the Reset button for one second. ▪ To restore factory default settings: If you are experiencing extreme problems with the router and have tried all other troubleshooting measures, press and hold the Reset button for 30 seconds to restore the factory default settings. All previously entered settings will be abandoned. |
| Security Slot | Use the security slot on the side panel to attach a lock to protect the router from theft. |
| Power | <ul style="list-style-type: none"> ▪ RV042 and RV042G: Connect the provided power adapter to the power port on the side panel. ▪ RV082 and RV016: Connect the provided AC power cable to the power port on the back panel. |

Default Settings

| Parameter | Default Value |
|------------|----------------------|
| Username | admin |
| Password | admin |
| LAN IP | 192.168.1.1 |
| DHCP Range | 192.168.1.100 to 149 |
| Netmask | 255.255.255.0 |

Mounting Options

Placement Tips

- **Ambient Temperature**—To prevent the router from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).
- **Air Flow**—Be sure that there is adequate air flow around the router.
- **Mechanical Loading**—Be sure that the router is level and stable to avoid any hazardous conditions.

Desktop Placement

Place the router on a flat surface near an electrical outlet.


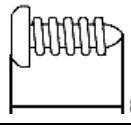


WARNING Do not place anything on top of the router; excessive weight could damage it.


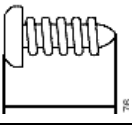
Wall Mounting

The router has two wall-mount slots on the bottom panel. To mount the router on a wall, you need mounting hardware (not included). Suggested hardware is illustrated below (not true to scale).

Suggested Hardware for RV042 and RV042G

| | |
|---|---|
|  |  |
| 5-5.5 mm | 20-22 mm |

Suggested Hardware for RV082 and RV016

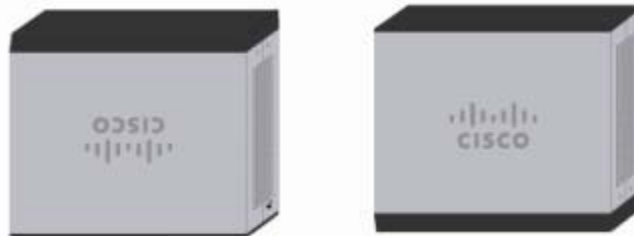
| | |
|--|---|
|  |  |
| 6.5-7 mm | 16.5-18.5 mm |



WARNING Insecure mounting might damage the router or cause injury. Cisco is not responsible for damages incurred by insecure wall-mounting.



WARNING For safety, ensure that the heat dissipation holes are facing sideways.



STEP 1 Drill two pilot holes into the surface.

- **RV042 and RV042G:** 58 mm apart
- **RV082 and RV016:** 94 mm apart

- STEP 2** Insert a screw into each hole, leaving a gap between the surface and the base of the screw head of 1 to 1.2 mm.
- STEP 3** Place the router wall-mount slots over the screws and slide the router down until the screws fit snugly into the wall-mount slots.

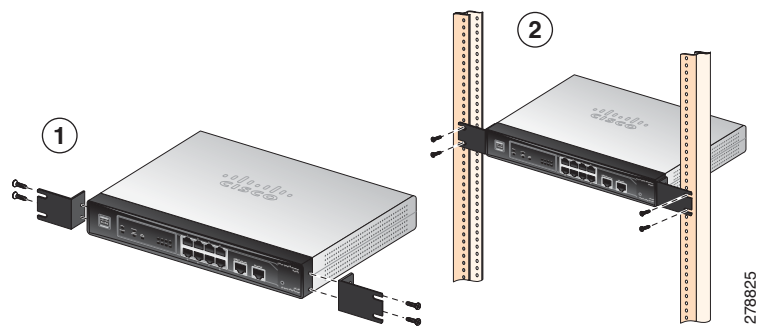
Rack Mounting RV082 or RV016

You can mount the RV082 or RV016 in a standard size, 19-inch (about 48 cm) wide rack. The router requires 1 rack unit (RU) of space, which is 1.75 inches (44.45mm) high. Mounting brackets are provided.



CAUTION Do not overload the power outlet or circuit when installing multiple devices in a rack.

- STEP 1** Place the router on a hard, flat surface.
- STEP 2** Attach one of the supplied rack-mount brackets to one side of the router with the supplied screws. Secure the bracket tightly.
- STEP 3** Follow the same steps to attach the other bracket to the opposite side.
- STEP 4** Use suitable screws to securely attach the brackets to any standard 19-inch rack.



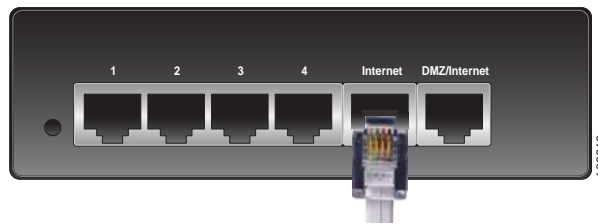
Connecting the Equipment

STEP 1 Make sure that all network devices are powered off, including the router, PCs, Ethernet switches, and broadband network device (DSL or cable modem).

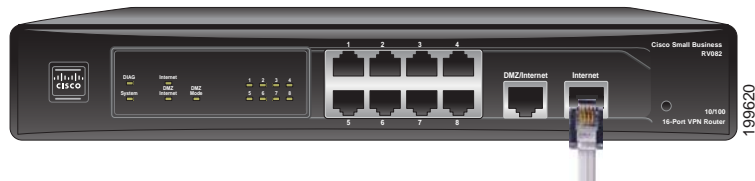
STEP 2 To connect to your Internet service:

- **RV042, RV042G, and RV082:** Connect an Ethernet cable from the broadband network device to the **Internet** port of the router.

RV042 and RV042G Internet Port

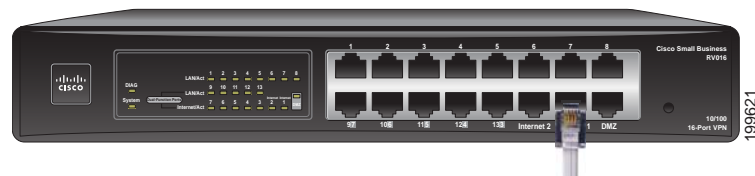


RV082 Internet Port



- **RV016:** Connect an Ethernet cable from the broadband network device to the **Internet 1** port of the router.

RV016 Internet 1 Port



STEP 3 To connect a secondary Internet service:

- **RV042, RV042G, and RV082:** Connect an Ethernet cable from the **DMZ/Internet** port to a second broadband network device.

- **RV016:** Connect an Ethernet cable from the **Internet 2** port to a second broadband network device.
- STEP 4** To connect a computer or server that will be a DMZ host:
- **RV042, RV042G, and RV082:** Connect an Ethernet cable from the **DMZ/Internet** port to the DMZ host.
 - **RV016:** Connect an Ethernet cable from the **DMZ** port to the DMZ host.
- STEP 5** To connect other network devices, such as computers, print servers, or Ethernet switches, connect an Ethernet cable from a numbered LAN port to the network device.
- STEP 6** Power on the broadband network device(s).
- STEP 7** Use the power adapter (RV042 and RV042G) or the power cable (RV082 and RV016) to connect the router to a power outlet. The System status light is green.
- STEP 8** Power on the other network devices.
-

Getting Started with the Configuration

- STEP 1** Connect a computer to a numbered LAN port on the router. Your PC will become a DHCP client of the router and will receive an IP address in the 192.168.1.x range.
- STEP 2** Start a web browser. To use the configuration utility, you need a PC with Internet Explorer (version 6 and higher), Firefox, or Safari (for Mac).
- STEP 3** In the address bar, enter the default IP address of the router: **192.168.1.1**
- STEP 4** When the login page appears, enter the default user name **admin** and the default password **admin** (lowercase).
- STEP 5** Click **Login**. The *System Summary* page appears.

The router's default settings are sufficient for many small businesses. Your Internet Service Provider may require additional settings. On the *System Summary* page, check the WAN Status to see if the router was able to receive an IP Address. If not, continue to the next step.

- STEP 6** To use the setup wizard to configure your Internet connection, click **Setup Wizard** on the *System Summary* page, or click **Wizard** in the navigation tree. In the *Basic Setup* section, click **Launch Now**. Follow the on-screen instructions.

If your web browser displays a warning message about the pop-up window, allow the blocked content.

- STEP 7** To configure other settings, use the links in the navigation tree.

Cisco strongly recommends setting a strong administrator password to prevent unauthorized access to your router. For more information about all settings, refer to the online Help and the *Cisco Small Business RV0xx Series VPN Router Administration Guide*.

Troubleshooting Tips

If you have trouble connecting to the Internet or the web-based configuration utility:

- Verify that your web browser is not set to Work Offline.
- Check the Local Area Connection settings for your Ethernet adapter. The PC needs to obtain an IP address through DHCP. Alternatively, it can have a static IP address in the 192.168.1.x range with the default gateway set to 192.168.1.1 (the router's default IP address).
- Verify that you entered the correct settings in the Wizard to set up your Internet connection, including the username and password if required.
- Try resetting the modem and the router by powering off both devices. Next, power on the modem and let it sit idle for about 2 minutes. Then power on the router. You should now receive a WAN IP address.
- Check the DHCP IP address range of your modem. If the modem uses the 192.168.1.x range, disconnect the cable from the modem to the router, and then launch the router configuration utility. In the navigation tree, choose **Setup > Network**. Enter a new Device IP Address, such as 10.1.1.1 or 192.168.0.1. Alternatively, if you have a DSL modem, leave all settings as is and instead ask your ISP to put the DSL modem into bridge mode.

Features of the User Interface

The user interface is designed to make it easy for you to set up and manage your router. Refer to these topics:

- [Navigation, page 18](#)
- [Pop-Up Windows, page 19](#)
- [Setup Wizards, page 19](#)
- [Saving the Settings, page 19](#)
- [Help, page 19](#)
- [Logout, page 19](#)

Navigation

The major modules of the configuration utility are represented by buttons in the left navigation pane. Click a button to view more options. Click an option to open a configuration page. The selected page appears in the main window of the configuration utility.

The screenshot shows the Cisco Small Business RV0xx Series Router configuration utility interface. The left navigation pane contains a tree view with the following items: System Summary (selected), Setup, DHCP, System Management, Port Management, Firewall, Cisco ProtectLink Web, VPN, Log, and Wizard. The main content area displays the 'System Summary' page, which includes the following sections:

- System Information:** Serial Number: C07z9Bx2090214100, Firmware Version: v1.0.0.22-tm (Jul 16 2010 08:35:39), PID VID: RV082 V3, Firmware MD5 Checksum: 809892c39240cac38a98f1450c38fdd, LAN IP / Subnet mask: 192.168.1.1/255.255.255.0, Working Mode: Gateway, System Up Time: 0 Days 5 Hours 54 Minutes 31 Seconds (Now: Mon Jul 20 2010 08:11:56).
- Cisco ProtectLink:** A banner with buttons for 'Go buy', 'Register', and 'Activate'.
- Configuration:** A section with a 'Setup Wizard' button and the text: 'If you need guideline to re-configure the router, you may launch wizard.'
- Port Statistics:** A table showing the status of 8 ports.

| Port ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|-----------|---------|-----------|---------|---------|---------|---------|---------|---------|
| Interface | LAN | | | | | | | |
| Status | Enabled | Connected | Enabled | Enabled | Enabled | Enabled | Enabled | Enabled |

Callout lines labeled '1' and '2' point to the navigation tree and the configuration page content, respectively.

1. Navigation tree
2. Configuration page

Pop-Up Windows

Some links and buttons launch pop-up windows that display more information or related configuration pages. If your web browser displays a warning message about the pop-up window, allow the blocked content.

Setup Wizards

Two setup wizards make it easy to set up your Internet connection and/or DMZ and to configure access rules for the WAN, LAN, and DMZ. You can use these wizards or use the other pages of the configuration utility.

To open the Wizard page: Click the **Setup Wizard** button in the *Configuration* section of the *System Summary* page. Alternatively, click **Wizard** in the navigation tree. There are two wizards:

- **Basic Setup:** Click **Launch Now** to configure the basic settings for your Internet connection and DMZ. Follow the on-screen instructions.
- **Access Rule Setup:** Click **Launch Now** to configure access rules for the WAN, LAN, and DMZ. Follow the on-screen instructions.

Saving the Settings

Your settings on a configuration page are not saved until you click the **Save** button. When you navigate to another page, any unsaved settings are abandoned.

To clear the settings without saving them, you can click the **Cancel** button.

Help

To view more information about the selected configuration page, click the **Help** link near the top right corner of the configuration utility. If your web browser displays a warning message about the pop-up window, allow the blocked content.

Logout

To exit the configuration utility, click the **Logout** link near the top right corner of the configuration utility. The *Login* page appears. You can close the browser window.

Viewing System Summary Information

The *System Summary* page appears after you log in to the configuration utility. You also can view this page by clicking **System Summary** in the navigation tree. Use this page to view information about the current status of the router and the settings. Refer to these topics:

- [System Information, page 21](#)
- [Cisco ProtectLink Web, page 21](#)
- [Configuration, page 22](#)
- [Port Statistics, page 22](#)
- [WAN Status, page 24](#)
- [Firewall Setting Status, page 25](#)
- [VPN Setting Status, page 25](#)
- [Log Setting Status, page 25](#)

The screenshot displays the 'System Summary' page in a web-based configuration utility. On the left is a navigation tree with 'System Summary' selected. The main content area is titled 'System Summary' and includes the following sections:

- System Information:** Displays details such as Serial Number (C07z9Bx2090214100), Firmware Version (v1.0.0.22-tm), PID VID (RV082 V3), LAN IP/Subnet mask (192.168.1.1/255.255.255.0), and System Up Time (0 Days 5 Hours 54 Minutes 31 Seconds).
- Cisco ProtectLink:** A section with buttons for 'Go buy', 'Register', and 'Activate'.
- Configuration:** A section with a 'Setup Wizard' button.
- Port Statistics:** A table showing the status of 8 ports.

| Port ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|-----------|---------|-----------|---------|---------|---------|---------|---------|---------|
| Interface | LAN | | | | | | | |
| Status | Enabled | Connected | Enabled | Enabled | Enabled | Enabled | Enabled | Enabled |

System Information

This section includes the following information:

- **Serial Number:** The serial number of the router.
- **Firmware version:** The current version number of the firmware installed on the router.
- **PID VID:** The current version number of the hardware.
- **MD5 Checksum:** A value used for file validation.
- **LAN IP / Subnet mask:** The current IP Address of the router on the local network.
- **Working Mode:** The working mode (Gateway or Router).
- **LAN:** If Dual-Stack IP is enabled, on the *Setup > Network* page, this section displays the IPv4 address and subnet mask as well as the IPv6 address and prefix length.
- **System Up time:** The length of time in days, hours, and minutes that the router has been active.

Cisco ProtectLink Web

This section displays buttons for the optional Cisco ProtectLink Web service. ProtectLink Web provides security for your network. It filters website addresses (URLs) and blocks potentially malicious websites. (Also see [Chapter 8, “Getting Started with Cisco ProtectLink Web.”](#))

NOTE This service is not available on Cisco RV042G.

You can use the following buttons:

- **Go buy:** Click this button to purchase a license to use this service. You will be redirected to a list of Cisco resellers on the Cisco website. Then follow the on-screen instructions.
- **Register:** Click this button if you have a license but have not yet registered it. You will be redirected to the Cisco ProtectLink Web website. Then follow the on-screen instructions.
- **Activate:** Click this button if you have registered for Cisco ProtectLink Web service and wish to activate it. You will be redirected to the Cisco ProtectLink Web website. Follow the on-screen instructions.

NOTE If the Cisco ProtectLink Web options are not displayed on the *System Summary* page, you can upgrade the router’s firmware to enable this feature.

Configuration

If you need help to configure the router, click **Setup Wizard**. You can then use these wizards:

- **Basic Setup Wizard:** Use this wizard to set up your Internet connection.
- **Access Rule Setup Wizard:** Use this Wizard to set up the security policy for your VPN.

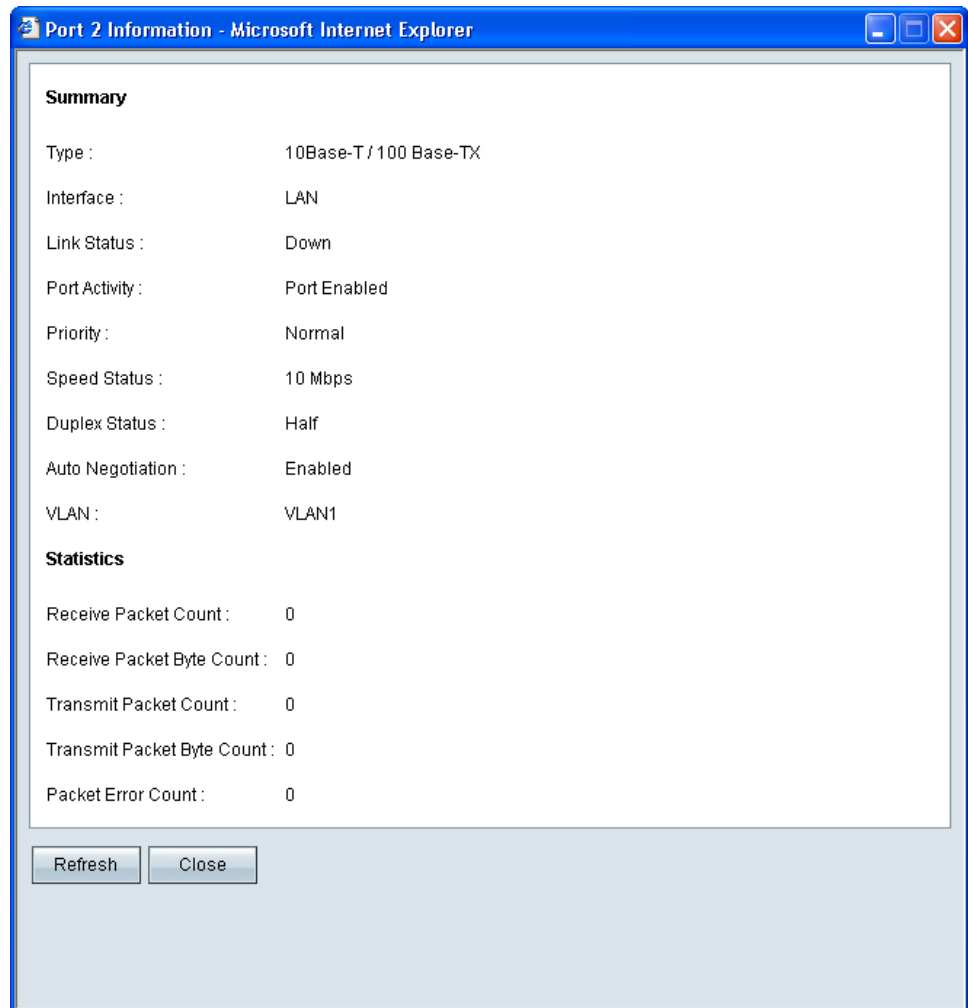
Port Statistics

This table shows the status and available statistics for each port. It also provides access to detailed information about current link activity.

- **Port ID:** The port label.
- **Interface:** The type of interface, such as LAN, WAN, or DMZ. Multiple WAN interfaces are indicated by a number, such as WAN1 or WAN2.
- **Status:** The status of the port: *Disabled* (red), *Enabled* (black), or *Connected* (green). The status is a hyperlink that you can click to open the *Port Information* window.

Port Information Window

If you click a status in the *Port Statistics* table, the *Port Information* window appears. This window displays the latest information about the interface and the current activity. To update the displayed information, click the **Refresh** button. To close the window, click the **Close** button.



This window displays the following information:

- **Type:** The type of port, 10Base-T/100 Base-TX.
- **Interface:** The type of interface, such as LAN, DMZ, or WAN.
- **Link Status:** The current status of the link: *Up* or *Down*.
- **Port Activity:** The current activity on the port, either Port Enabled, Port Disabled, or Port Connected.
- **Priority:** The priority setting, High or Normal.
- **Speed Status:** The speed, 10Mbps or 100Mbps.
- **Duplex Status:** The duplex mode, Half or Full.

- **Auto negotiation:** The auto negotiation setting, On or Off.
- **VLAN:** The VLAN ID.
- **Receive Packet Count:** The number of packets received through this port.
- **Receive Packet Byte Count:** The number of bytes received through this port.
- **Transmit Packet Count:** The number of packets transmitted through this port.
- **Transmit Packet Byte Count:** The number of bytes transmitted through this port.
- **Packet Error Count:** The number of packet errors.

WAN Status

This section displays information for the WAN1 interface as well as DMZ or WAN2, depending on your configuration. On Cisco RV016, additional WAN interfaces may be configured. Use the tabs to view the IPv4 and IPv6 information.

NOTE The IPv6 tab is available if Dual-Stack IP is enabled on the *Setup > Network* page.

- **WAN information:**
 - **IP Address:** The current public IP address for this interface.
 - **Default Gateway:** The default gateway for this interface.
 - **DNS:** The IP address of the DNS server for this interface.
 - **Dynamic DNS (IPv4 only):** The DDNS settings for this port, Disabled or Enabled.
 - **Release** and **Renew:** These buttons appear if the port is set to obtain an IP address automatically. Click **Release** to release the IP address, and click **Renew** to update the DHCP lease time or to get a new IP address.
 - **Connect** and **Disconnect:** These buttons appear if the port is set to PPPoE or PPTP. Click **Disconnect** to disconnect from the Internet service. Click **Connect** to re-establish the connection.

- **DMZ information:**
 - **IP Address:** The current public IP address for this interface.
 - **DMZ Host:** The DMZ private IP address of the DMZ host. The default is **Disabled**.

Firewall Setting Status

This section displays the following information:

- **SPI (Stateful Packet Inspection):** The status of this feature: *On* (green) or *Off* (red).
- **DoS (Denial of Service):** The status of this feature, *On* (green) or *Off* (red).
- **Block WAN Request:** The status of this feature, *On* (green) or *Off* (red).
- **Remote Management:** The status of this feature, *On* (green) or *Off* (red).
- **Access Rule:** The number of access rules that have been set.

VPN Setting Status

This section displays the following information:

- **Tunnel(s) Used:** The number of VPN tunnels in use.
- **Tunnel(s) Available:** The number of VPN tunnels available.

Log Setting Status

This section displays the following information:

- **Syslog Server:** The status of the syslog server, *On* (green) or *Off* (red).
- **Email Log:** The status of the email log, *On* (green) or *Off* (red).

Setup

Use the *Setup* module to set up the basic functions of the router. Refer to these topics:

- [Setting Up the Network, page 27](#)
- [DMZ Setting, page 32](#)
- [Changing the Administrator Username and Password, page 40](#)
- [Setting the System Time, page 42](#)
- [Setting Up a DMZ Host, page 43](#)
- [Setting Up Port Forwarding and Port Triggering, page 44](#)
- [Setting Up Universal Plug and Play \(UPnP\), page 48](#)
- [Setting Up One-to-One NAT, page 51](#)
- [Cloning a MAC Address for the Router, page 53](#)
- [Assigning a Dynamic DNS Host Name to a WAN Interface, page 55](#)
- [Setting Up Advanced Routing, page 57](#)
- [IPv6 Transition, page 61](#)

Setting Up the Network

Use the *Setup > Network* page to set up your LAN, WAN (Internet connections), and DMZ interface.

To open this page: Click **Setup > Network** in the navigation tree.

The screenshot shows the 'Network' configuration page. On the left is a navigation tree with 'Setup' expanded and 'Network' selected. The main content area has the following sections:

- Host Name:** routerd88880 (Required by some ISPs)
- Domain Name:** linksys.com (Required by some ISPs)
- IP Mode:** A table with columns for Mode, WAN, and LAN. The 'IPv4 Only' radio button is selected.
- LAN Setting:** Includes fields for MAC Address (68:EF:BD:D8:86:80), Device IP Address (192.168.1.1), and Subnet Mask (255.255.255.0). There is a checkbox for 'Multiple Subnet' and an 'Add/Edit' button.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

This page includes the following sections:

- [Host Name and Domain Name, page 27](#)
- [LAN Setting \(device IP address and subnets\), page 28](#)
- [WAN Setting \(Internet connection\), page 31](#)
- [DMZ Setting, page 32](#)

Host Name and Domain Name

Some ISPs require that you assign a host name and domain name to identify your router on the ISP network. Default values are provided, but you can change them if needed.

- **Host Name:** Keep the default setting or enter a host name specified by your ISP.
- **Domain Name:** Keep the default setting or enter a domain name specified by your ISP.

IP Mode

Choose the type of addressing to use on your network:

- **IPv4 Only**—Use only IPv4 addressing.
- **Dual-Stack IP**—Use IPv4 and IPv6 addressing. After you enable this option by saving the settings on this page, you can configure both IPv4 and IPv6 addresses for LAN, WAN, and DMZ settings on this page.

LAN Setting (device IP address and subnets)

The default LAN settings should be sufficient for most small businesses, but if needed, you can change the LAN IP address of the router and enable multiple subnets.

- **Changing the device IP address, page 28**
- **Enabling multiple subnets (IPv4 only), page 29**

NOTE If you enabled Dual-Stack IP for the IP Mode, you can click the IPv6 tab to configure IPv6 addresses.

Changing the device IP address

STEP 1 Enter the following information:

- **For IPv4:** Click the **IPv4** tab, and then enter the **Device IP Address** and **Subnet Mask**. The default IP address is 192.168.1.1, and the default subnet mask is 255.255.255.0.
Note: The MAC address of the router also appears in this section. This value cannot be changed.
- **For IPv6:** Click the **IPv6** tab, and then enter the **IPv6 Address** and the **Prefix Length**. The default IP address is fc00::1, and the default prefix length is 7. The IPv6 tab is available only if **Dual-Stack IP** is enabled in the *IP Mode* section. If you change the IP Mode setting, you must save the settings before you continue.

Note: To configure global IPv6 prefixes for your LAN devices, go to the *WAN Settings* section, click the **IPv6** tab, and click the **Edit** icon for the WAN interface. Then enter the LAN IPv6 Address. For more information, see **WAN Setting (Internet connection), page 31**.

STEP 2 Click **Save** to save your changes, or click **Cancel** to undo them.

After you click **Save**, a pop-up window displays a reminder that you will need to use the new device IP address to launch the configuration utility. Click **OK** to close the message and continue with the IP address change, or click **Cancel** to close the message without applying the changes.

STEP 3 Release and renew the IP address of your PC. You should then receive a new IP address in the new DHCP range for the router.

Notes:

- *To release and renew your address in Windows:* From the Start menu, open the *Network Connections* window. Right-click on the connection and choose **Disable**. Right-click again and enable the connection. To verify, right-click and choose **Status**. Then click the **Support** tab to view the assigned IP address.
- By default, the router is a DHCP server that assigns IP addresses dynamically to all connected devices. For example, if you choose 192.168.15.1 as the device IP address, devices will receive IP addresses in the range of 192.168.2.x.
- By default, a Windows PC receives an IP address dynamically.
- If you previously disabled the router's DHCP server or set a static IP address on the PC, you will need to configure a new static IP address in the new range.

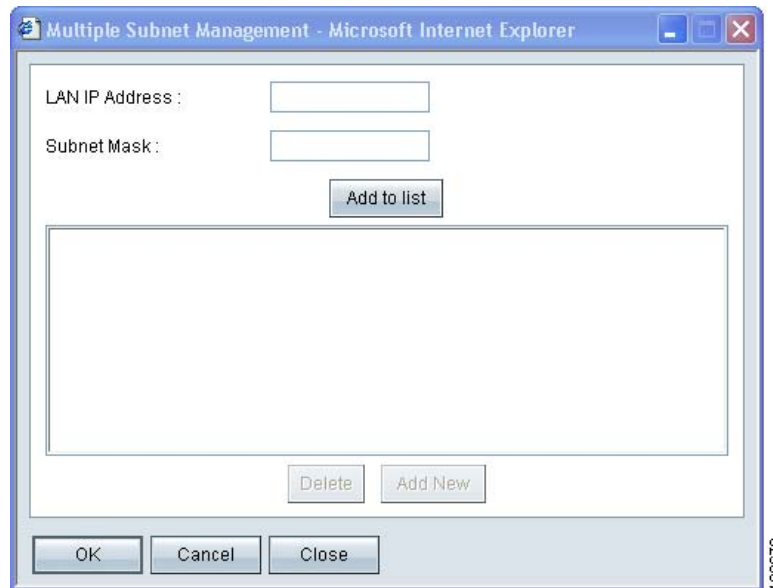
STEP 4 To reconnect to the configuration utility, enter the new device IP address in the address bar of your browser.

Enabling multiple subnets (IPv4 only)

Typically, a Cisco RV0xx Series router is used as an access router, with a single LAN subnet. By default, the firewall is pre-configured to deny LAN access if the source IP address is on a different subnet than the router's LAN IP address. However, you can enable multiple subnets to allow this router to work as an edge device that provides Internet connectivity to different subnets in your LAN.

STEP 1 On the IPv4 tab, check the **Enable Multiple Subnet** box to enable this feature. Uncheck the box to disable this feature.

STEP 2 Click **Add/Edit** to create or modify the subnets. After you click the button, the *Multiple Subnet Management* window appears.



STEP 3 In the pop-up window, add or edit entries as needed.

- **To add a new subnet:** Enter a LAN IP Address and a Subnet Mask. Click **Add to list**. The IP address and subnet mask appear in the list. Repeat this step as needed to add other subnets.

Examples:

- Two subnets: If the router has a LAN IP address of 192.168.1.1 with a subnet mask of 255.255.255.0, you could set up a second subnet with a LAN IP address of 192.168.2.1 and a subnet mask of 255.255.255.0.
 - Four subnets: If the router has a LAN IP Address of 192.168.1.1 and the Subnet Mask of 255.255.255.192, you could create three subnets with IP addresses of 192.168.2.65, 192.168.2.129, and 192.168.2.193, with the same subnet mask of 255.255.255.192.
- **To add another subnet:** Enter the information, and then click **Add to list**.
 - **To modify a subnet:** Click the subnet in the list. The existing values appear in the text fields. Enter the new information, and then click **Update**. If you do not want to modify the selected subnet, you can click **Add New** to clear the text fields.
 - **To delete a subnet:** Click the subnet in the list, and then click **Delete**.

- STEP 4** When you finish entering settings in the *Multiple Subnet* window, click **OK** to save your changes, or click **Cancel** to undo them.

WAN Setting (Internet connection)

The router is pre-configured with default settings that are sufficient for many networks. However, special settings may be required by your ISP (Internet Service Provider) or broadband (DSL or cable) carrier. Refer to the setup information provided by your ISP.

- NOTE** You also can set up your Internet connection by using the Basic Setup Wizard. In the navigation tree, click **Wizard**. In the *Basic Setup* section, click **Launch Now**.








The *WAN Setting* table displays the existing settings for each interface, such as DMZ, WAN1, or WAN2. The listed interfaces depend on the router model and the settings that you enter for ports such as DMZ/Internet (all models) and the Dual-Function ports (Cisco RV016).

Perform the following actions, as needed.

- **To configure the WAN with IPv6 addressing:** Click the **IPv6** tab. Then proceed with the other tasks listed below.
Note: The IPv6 tab is available only if **Dual-Stack IP** is enabled in the *IP Mode* section. If you change the IP Mode setting, you must save the settings before you continue.
- **To change the number of WAN ports (Cisco RV016 only):** Use the drop-down list to choose the number of WAN ports that you want to enable. The default selection is 2. If you configure additional WAN ports, the Dual-Function Ports are used for this purpose.

WAN Setting

Please choose how many WAN ports you prefer to use : (Default value is 2)

| Interface | Connection Type | Configuration |
|-----------|----------------------------|---|
| WAN1 | Obtain an IP automatically |  |
| WAN2 | PPTP |  |
| WAN3 | Obtain an IP automatically |  |
| WAN4 | Obtain an IP automatically |  |
| WAN5 | Obtain an IP automatically |  |
| WAN6 | Obtain an IP automatically |  |
| WAN7 | Obtain an IP automatically |  |

1395961

- **To modify the WAN settings:** If you have any unsaved changes on the *Network* page, click **Save** to save your settings before continuing. For the interface that you want to modify, click the **Edit** icon to open the *Edit WAN Connection* page. For more information, see [Editing a WAN Connection, page 34](#).

DMZ Setting

On Cisco RV042, RV042G, and RV082, you can configure the Internet/DMZ port for use as a DMZ (De-Militarized Zone or De-Marcation Zone). Cisco RV016 has a dedicated DMZ port. A DMZ allows Internet traffic to access specified hosts on your network, such as FTP servers and web servers. The rest of your network resources are kept private.

This feature requires that you have a publicly routable IP address for each host on the DMZ. You can contact your ISP about getting an additional IP address for this purpose.

NOTE

- Using the DMZ is preferred and is, if practical, a strongly recommended alternative to using public LAN servers or putting these servers on WAN ports where they are not protected and not accessible by users on the LAN.
- Each of the servers on the DMZ will need a unique, public Internet IP address. Your ISP should be able to provide these addresses, as well as information on setting up public Internet servers. If you plan to use the DMZ setting, contact your ISP for the static IP information. If your ISP provides only one static or several dynamic IP addresses, consider using the DMZ host feature. See [Setting Up a DMZ Host, page 43](#).

Perform the following actions, as needed.

- **To configure the DMZ with IPv6 addressing:** Click the **IPv6** tab. Then proceed with the other tasks in this section.
Note: The IPv6 tab is available only if **Dual-Stack IP** is enabled in the *IP Mode* section. If you change the IP Mode setting, you must save the settings before you continue.
- **To enable DMZ on the DMZ/Internet port (Cisco RV042, RV042G, and RV082 only):** Check the **Enable DMZ** box to enable this feature. Then edit the DMZ settings, as described below. If you want to use the port as a WAN port instead, uncheck the box, and be sure to configure the WAN settings on the *Dual WAN* page. (See [Setting Up Dual WAN and Multi-WAN Connections, page 73](#).)

-
- **To edit DMZ settings:** Click the **Edit** icon to open the *Edit DMZ Connection* page. For more information, see [Editing a DMZ Connection, page 38](#). If you have not saved your settings, a warning appears. Click **OK** to save your settings, or click **Cancel** to close the window without saving.

Editing a WAN Connection

Editing a WAN Connection with IPv4 Addressing

Editing a WAN Connection with IPv6 Addressing

The *Edit WAN Connection* page appears after you click an **Edit** icon in the *WAN Settings* section of the *Network* page. Enter the information provided by your ISP.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

- **Interface:** The selected WAN port appears. This ID cannot be changed.
- **WAN Connection Type:** Choose a connection type, as described below.
 - **Obtain an IP Automatically:** Choose this option if your ISP dynamically assigns an IP address. For example, most cable modem subscribers use this connection type. Your ISP will assign the settings, including the DNS server IP address. If you want to specify a DNS server, check the **Use**

the **Following DNS Server Addresses** box. Then enter an IP address in the **DNS Server (Required) 1** box. Optionally, you can enter a second DNS server. The first available DNS entry is used.

- **Static IP:** Choose this option if your ISP assigned a permanent IP address to your account. Then enter the settings provided by your ISP:

Specify WAN IP Address: The external IP address that your ISP assigned to your account.

Subnet Mask (IPv4): The subnet mask specified by your ISP.

Prefix Length (IPv6): The prefix length specified by your ISP.

Default Gateway Address: The IP address of the default gateway.

DNS Server (Required) 1: The IP address of the specified DNS server. Optionally, enter a second DNS server. The first available DNS entry is used.

- **PPPoE (Point-to-Point Protocol over Ethernet):** Choose this option if your ISP uses PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections (typical for DSL lines). Then enter the settings provided by your ISP:

Username and Password: Enter the username and password for your ISP account. The maximum number of characters is 60.

Connect on Demand: This feature may be helpful if you are billed based on the time that you are connected to the Internet. When this feature is enabled, the connection will be disconnected after a specified period of inactivity (Max Idle Time). As soon as you attempt to access the Internet again, the router automatically re-establishes your connection. If you enable this feature, also enter the **Max Idle Time**, which is number of minutes that the connection can be inactive; when this limit is reached, the connection is terminated. The default Max Idle Time is 5 minutes.

Keep Alive: This feature ensures that your router is always connected to the Internet. When this feature is enabled, the router keeps the connection alive by sending out a few data packets periodically. This option keeps your connection active indefinitely, even when it sits idle. If you enable this feature, also enter the **Redial Period** to specify how often the router verifies your Internet connection. The default period is 30 seconds.

- **PPTP (Point-to-Point Tunneling Protocol):** Choose this option if required by your ISP. PPTP is a service used in Europe, Israel, and other countries.

Specify WAN IP Address: The external IP address that your ISP assigned to your account.

Subnet Mask: The subnet mask specified by your ISP.

Default Gateway Address: The IP address of the default gateway.

Username and Password: Enter the username and password for your ISP account. The maximum number of characters is 60.

Connect on Demand: This feature may be helpful if you are billed based on the time that you are connected to the Internet. When this feature is enabled, the connection will be disconnected after a specified period of inactivity (Max Idle Time). As soon as you attempt to access the Internet again, the router automatically re-establishes your connection. If you enable this feature, also enter the **Max Idle Time**, which is number of minutes that the connection can be inactive; when this limit is reached, the connection is terminated. The default Max Idle Time is 5 minutes.

Keep Alive: This feature ensures that your router is always connected to the Internet. When this feature is enabled, the router keeps the connection alive by sending out a few data packets periodically. This option keeps your connection active indefinitely, even when it sits idle. If you enable this feature, also enter the **Redial Period** to specify how often the router verifies your Internet connection. The default period is 30 seconds.

- **Transparent Bridge:** Choose this option if you are using this router to connect two network segments. Only one WAN interface can be set as transparent bridge.

Specify WAN IP Address: The external IP address that your ISP assigned to your account.

Subnet Mask: The subnet mask specified by your ISP.

Default Gateway Address: The IP address of the default gateway.

DNS Server (Required) 1: The IP address of the specified DNS server. Optionally, enter a second DNS server. The first available DNS entry is used.

Internal LAN IP Range: The internal LAN IP range that will be bridged. The WAN and LAN of transparent bridge will be at the same subnet.

- **MTU:** Set the **MTU (Maximum Transmission Unit)** in bytes (see the Glossary). Unless a change is required by your ISP, Cisco recommends that you use the default setting, **Auto**. To specify another value, select **Manual**, and then enter the size in bytes.
- **Enabled DHCP-PD:** Check this box to enable the DHCPv6 client process and enable a request for prefix delegation through the selected interface. This option is typically used if your ISP is capable of sending LAN prefixes via DHCPv6 option. If your ISP does not support this option, then you can manually configure a LAN prefix by entering the LAN IPv6 address below.
Note: When DHCP-PD is enabled, the manual LAN IPv6 addressing below will be disabled and vice versa.
- **LAN IPv6 Address:** This option allows you to manually enter a global IPv6 prefix that was assigned by your ISP for your LAN devices, if applicable. Check with your ISP for more information.

Editing a DMZ Connection

Use the *Edit DMZ Connection* page to specify the settings for your DMZ. DMZ is enabled by default.

IPv4

The screenshot shows the 'Edit DMZ Connection' page for IPv4. The sidebar on the left lists various configuration sections, with 'Setup' expanded and 'Network' selected. The main content area is titled 'Network' and 'Edit DMZ Connection'. It includes the following fields and options:

- Interface:** DMZ
- Radio Buttons:** Subnet, Range (DMZ & WAN within same subnet)
- Specify DMZ IP Address:** 10.0.0.20
- Subnet Mask:** 255.255.255.0
- Buttons:** Save, Cancel

IPv6

The screenshot shows the 'Edit DMZ Connection' page for IPv6. The sidebar on the left lists various configuration sections, with 'Setup' expanded and 'Network' selected. The main content area is titled 'Network' and 'Edit DMZ Connection'. It includes the following fields and options:

- Interface:** DMZ
- Specify DMZ IPv6 Address:** ::
- Prefix Length:** 64
- Buttons:** Save, Cancel

The *Edit DMZ Connection* page appears after you click the **Edit** icon in the *DMZ Setting* section of the *Network* page.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

If you are using IPv4 addressing, enter the following information:

- **Subnet:** Choose this option to place the DMZ on a different subnet than the WAN (default setting). Enter an IP address and subnet mask for the DMZ.
- **Range:** Choose this option to place the DMZ on the same subnet as the WAN. Enter the range of IP addresses to reserve for the DMZ port.

If you are using IPv6 addressing, enter the following information:

- **Specify DMZ IPv6 Address:** Enter an IPv6 address for the DMZ. Replace the default double colon (::) with a valid IPv6 address for your DMZ.
- **Prefix Length:** Enter the prefix length. The default value is 64.

Changing the Administrator Username and Password

Use the *Setup > Password* page to update the administrator username and password. You can keep the default username (admin) if you like. However, Cisco strongly recommends changing the default password (admin) to a strong password that is hard to guess.



CAUTION

The password cannot be recovered if it is lost or forgotten. If the password is lost or forgotten, you have to reset the router to its factory default settings. Doing so will remove all of your configuration changes.

NOTE

- You must change the administrator password if you enable remote access on the *Firewall > General* page.
- Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. After you change the username or password, you will be required to log in with the new credentials when you select any option in the navigation tree.

To open this page: Click **Setup > Password** in the navigation tree.

The screenshot shows the 'Password' configuration page in the Cisco Small Business RV0xx Series Routers Administration Guide. The navigation tree on the left includes 'System Summary', 'Setup', 'Network', 'Password', 'Time', 'DMZ Host', 'Forwarding', 'UPnP', 'One-to-One NAT', 'MAC Address Clone', 'Dynamic DNS', 'Advanced Routing', 'DHCP', 'System Management', 'Port Management', 'Firewall', 'Cisco ProtectLink Web', 'VPN', 'Log', and 'Wizard'. The 'Password' page contains the following fields and options:

- Username: admin
- Old Password: [Text Input]
- New Username: [Text Input]
- Confirm New Username: [Text Input]
- New Password: [Text Input]
- Confirm New Password: [Text Input]
- Minimum Password Complexity: Enable
- Password Strength Meter: [Progress Bar]
- Password Aging Enforcement: Disable Change the password after 100 Days
- Buttons: Save, Cancel

- **Old Password:** Enter the old password. The default password is **admin**.
- **New Username:** Enter a new username, if desired. To keep the existing username, leave this field blank.

- **Confirm New Username:** To confirm, re-enter the new username, exactly as shown in the previous field.
- **New Password:** Enter a new password for the router. You can include alphanumeric characters and symbols, but no spaces.
- **Confirm New Password:** To confirm, re-enter the new password, exactly as shown in the previous field. An error message appears if the passwords do not match.
- **Minimum Password Complexity:** Check the **Enable** box if you want to enforce password complexity and enable the Password Strength Meter. This option is enabled by default and is recommended.

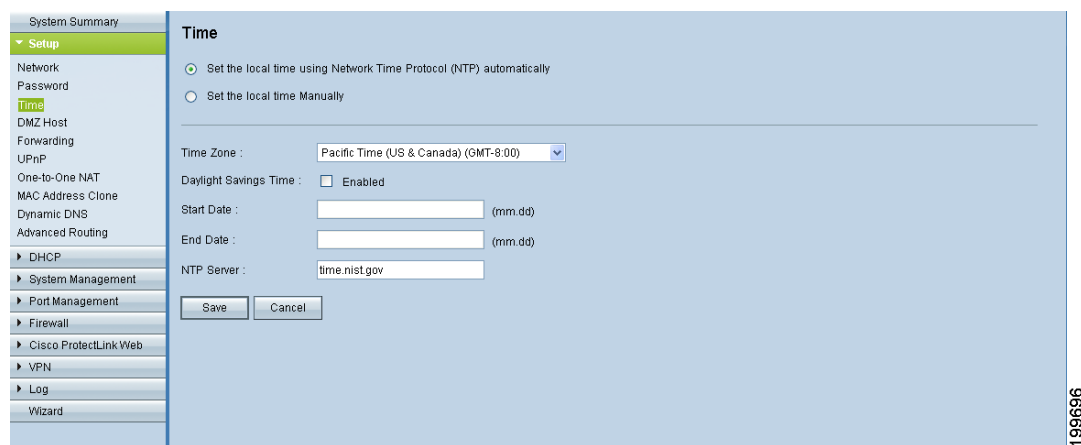
When Minimum Password Complexity is enabled, the password must meet the requirements listed below. Your entries are validated when you click the Save button.

- Includes at least 8 characters.
 - Is not the same as the username.
 - Is not the same as the current password.
 - Contains characters from at least 3 of the following 4 categories: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.
- **Password Strength Meter:** If you enable Minimum Password Complexity, the Password Strength Meter indicates the password strength, based on the complexity rules. As you enter a password, colored bars appear. The scale goes from red (unacceptable) to yellow (acceptable) to green (strong).
 - **Password Aging Enforcement:** Choose **Disable** if you do not want the password to expire. Choose **Change the password after** if you want the password to expire after the specified number of **Days** (default 180).

Setting the System Time

Use the *Setup > Time* page to specify the system time for your network. The router uses the time settings to time-stamp log events, to automatically apply the Access Rules and Content Filters, and to perform other activities for other internal purposes. You can allow the router to receive the local time settings automatically from a server, or you can enter the local time manually.

To open this page: Click **Setup > Time** in the navigation tree.



NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Choose one of the following options to set the time, and then enter the required information.

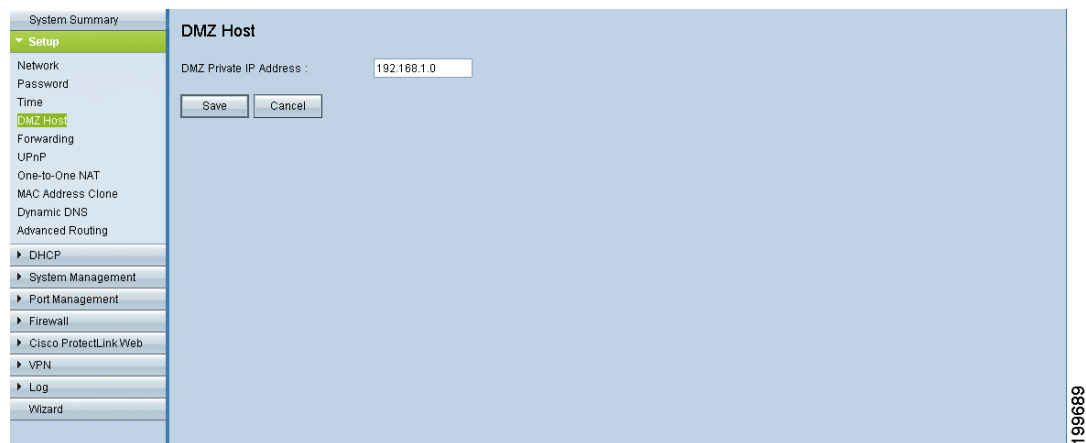
- **Set the local time using Network Time Protocol (NTP) automatically:**
Choose this option to allow the router to receive the time settings automatically from an NTP server. Then enter the following settings:
 - **Time Zone:** Select your time zone. The default is **(GMT-08:00) Pacific Time (US & Canada); Tijuana**.
 - **Daylight Saving:** To automatically adjust the time for daylight savings, select **Enabled**. In the **Start Date** field, enter the Month and Day when daylight savings time begins. Use mm.dd format, such as 6.25 for June 25. Also enter the **End Date** in the same format.
 - **NTP Server:** Enter the URL or IP address of the NTP server. The default is *time.nist.gov*.

- **Set the local time Manually:** Choose this option if you want to set the local time yourself. Then enter the following information:
 - **Date:** Enter the current date in yyyy.mm.dd format, such as 2010.06.25 for June 25, 2010.
 - **Hours, Minutes, Seconds:** Enter the current time in hh:mm:ss format, such as 15:17:00 for 3:17:00 p.m.

Setting Up a DMZ Host

Use the *Setup > DMZ Host* page to allow one host in the LAN to be exposed to the Internet to use services such as Internet gaming and video conferencing. Access to the DMZ Host from the Internet can be further restricted by using firewall access rules.

To open this page: Click **Setup > DMZ Host** in the navigation tree.



Enter the IP address of the network device that you want to use as a DMZ host.

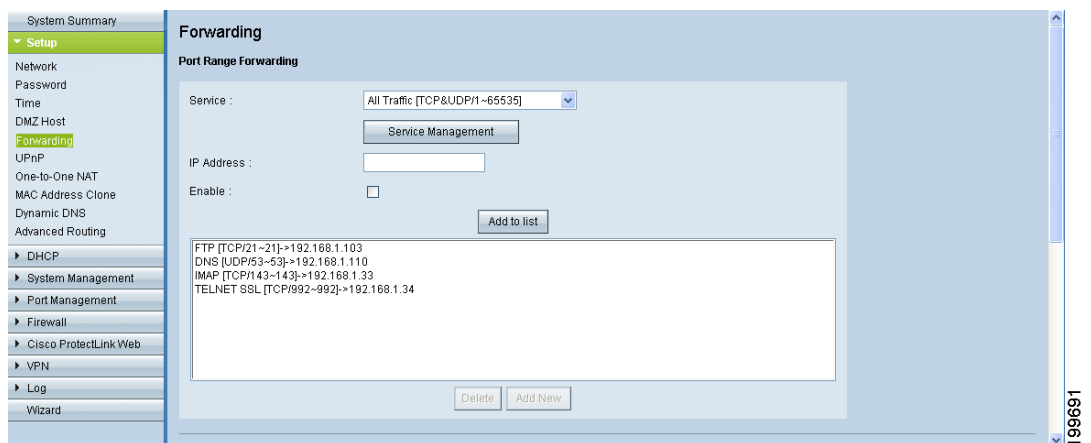
NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Setting Up Port Forwarding and Port Triggering

Use the *Setup > Forwarding* page if you need to allow public access to services on computers that are connected to the LAN ports. Port Forwarding opens a specified port or a port range for a service, such as FTP. Port Triggering opens a port range for services such as Internet gaming that use alternate ports to communicate between the server and LAN host. This page has the following sections:

- [Port Range Forwarding, page 44](#)
- [Port Triggering, page 47](#)

To open this page: Click **Setup > Forwarding** in the navigation tree.



NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Port Range Forwarding

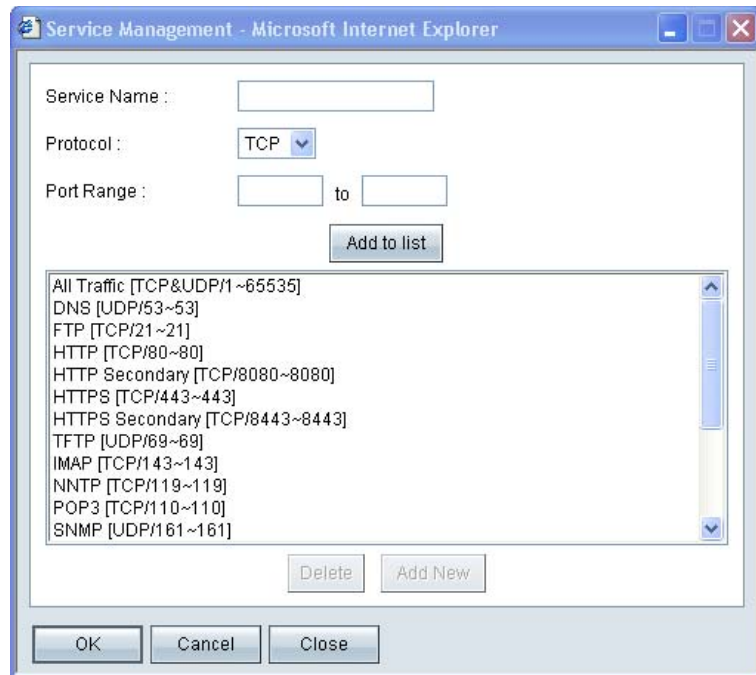
Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests to your network, the router can forward those requests to computers that are equipped to handle the requests. If, for example, you set the port number 80 (HTTP) to be forwarded to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

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

- **To add an entry to the list:** Enter the following information, and then click **Add to list**.
 - **Service:** Select the service. If a service is not listed, you can add a service. For details, see [Adding a service, page 46](#).
 - **IP Address:** Enter the LAN IP address of the server that you want the Internet users to access.
 - **Enable:** Check the box to enable this port range forwarding entry.
- **To add another new entry:** Enter the information, and then click **Add to list**.
- **To modify an entry in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.
- **To view the port range table:** Click **View**, near the bottom of the page. Choose **Port Range Forwarding** or **Port Triggering**. To update the display, click **Refresh**. To return to the *Forwarding* page, click **Close**.

Adding a service

To add a new entry to the *Service* list, or to change an entry that you created previously, click **Service Management**. If the web browser displays a warning about the pop-up window, allow the blocked content.



In the *Service Management* window, add or update entries as needed. Before closing this window, click **OK** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

- **To add a service to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 services in the list.
 - **Service Name:** Enter a short description.
 - **Protocol:** Choose the required protocol. Refer to the documentation for the service that you are hosting.
 - **Port Range:** Enter the required port range.
- **To add another new service:** Enter the information, and then click **Add to list**.

- **To modify a service you created:** Click the service in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the service and clear the text fields.
- **To delete a service from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Port Triggering

Port triggering allows the router to watch outgoing data for specified port numbers. The IP address of the computer that sends the matching data is remembered by the router, so that when the requested data returns through the router, the data is transmitted to the proper computer by using IP address and port mapping rules.

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

Add or edit entries as needed. Remember that the settings are not saved until you click the Save button.

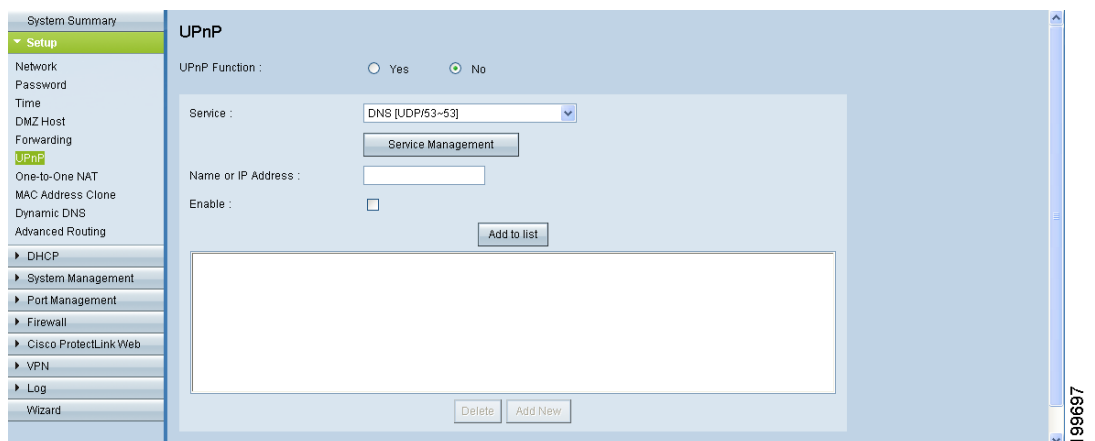
- **To add an entry to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 applications in the list.
 - **Application Name:** Enter the name of the application.
 - **Trigger Port Range:** Enter the starting and ending port numbers of the trigger port range. Refer to the documentation for the application.
 - **Incoming Port Range:** Enter the starting and ending port numbers of the incoming port range. Refer to the documentation for the application.
 - **Enable:** Check the box to enable port triggering for the application. Uncheck the box to disable the application.
- **To add another new entry:** Enter the information, and then click **Add to list**.
- **To modify an entry in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.

- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.
- **To view the port range table:** Click **View**, near the bottom of the page. Choose **Port Range Forwarding** or **Port Triggering**. To update the display, click **Refresh**. To return to the *Forwarding* page, click **Close**.

Setting Up Universal Plug and Play (UPnP)

Use the *Setup > UPnP* page to enable Universal Plug and Play (UPnP). This feature allows Windows to automatically configure the router to open and close ports for Internet applications such as gaming and videoconferencing.

To open this page: Click **Setup > UPnP** in the navigation tree.



NOTE

- As a security precaution, disable UPnP unless you require it for your applications.
- Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

To enable UPnP, click **Yes**. To disable this feature, click **No**. Add or edit entries as needed.

- **To add an entry to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 services in the list.
 - **Service:** Select the service. If a service is not listed, you can add a service. See [Adding a service, page 50](#).
 - **Name or IP Address:** Enter the name or IP address of the UPnP device.
 - **Enable:** Select **Enable** to enable this UPnP entry.
- **To add another new entry:** Enter the information, and then click **Add to list**.
- **To modify an entry in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

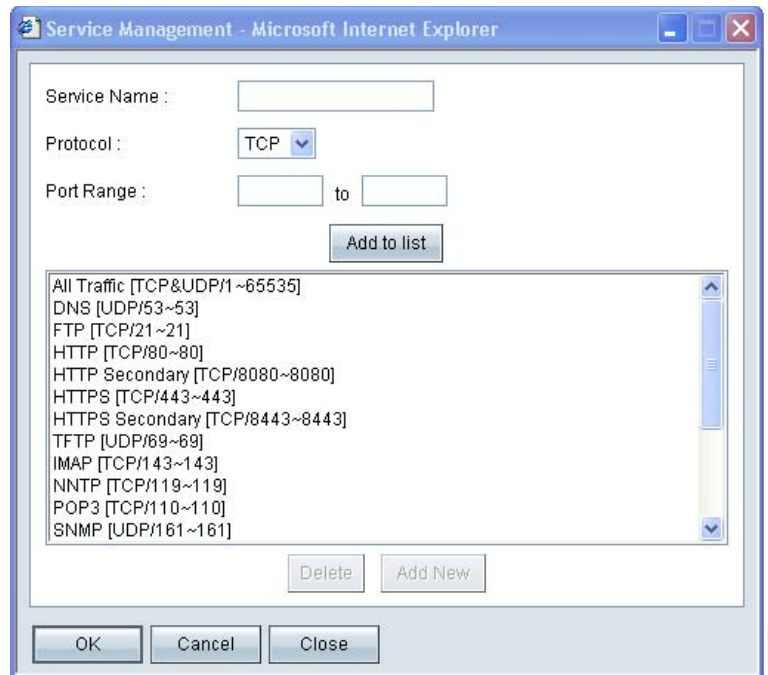
The *UPnP Forwarding Table List* displays the current data. You can click **Refresh** to update the data, or click **Close** to close the pop-up window.

- **To view the UPnP forwarding table:** Click **View**, near the bottom of the page. To update the display, click **Refresh**. To return to the *UPnP* page, click **Close**.

| Service Name | Protocol | Ext.Port | Internal Port | IP Address | Enabled |
|----------------|----------|----------|---------------|---------------|---------|
| HTTP Secondary | TCP | 8080 | 8080 | 192.168.1.100 | Enabled |
| SNMP | UDP | 161 | 161 | 10.0.0.103 | Enabled |

Adding a service

To add a new entry to the *Service* list, or to change an entry that you created previously, click **Service Management**. If the web browser displays a warning about the pop-up window, allow the blocked content.



In the *Service Management* window, add or update entries as needed. Before closing this window, click **OK** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

- **To add a service to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 services in the list.
 - **Service Name:** Enter a short description.
 - **Protocol:** Choose the required protocol. Refer to the documentation for the service that you are hosting.
 - **Port Range:** Enter the required port range.
- **To add another new service:** Enter the information, and then click **Add to list**.

- **To modify a service you created:** Click the service in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the service and clear the text fields.
- **To delete a service from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Setting Up One-to-One NAT

Use the *Setup > One-to-One NAT* page to enable One-to-One NAT (Network Address Translation). This process creates a relationship that maps a valid external IP address to an internal IP address that is hidden by NAT. Traffic can then be routed from the Internet to the specified internal resource.

NOTE For best results, reserve IP addresses for the internal resources that you want to reach through one-to-one NAT. See [About Static IP Addresses \(for IPv4 Only\)](#), page 66.

You can map a single relationship, or map an internal IP address range to an external range of equal length (for example, three internal addresses and three external addresses). The first internal address is mapped to the first external address, the second IP internal IP address is mapped to the second external address, and so on.

To open this page: Click **Setup > One-to-One NAT** in the navigation pane.



NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

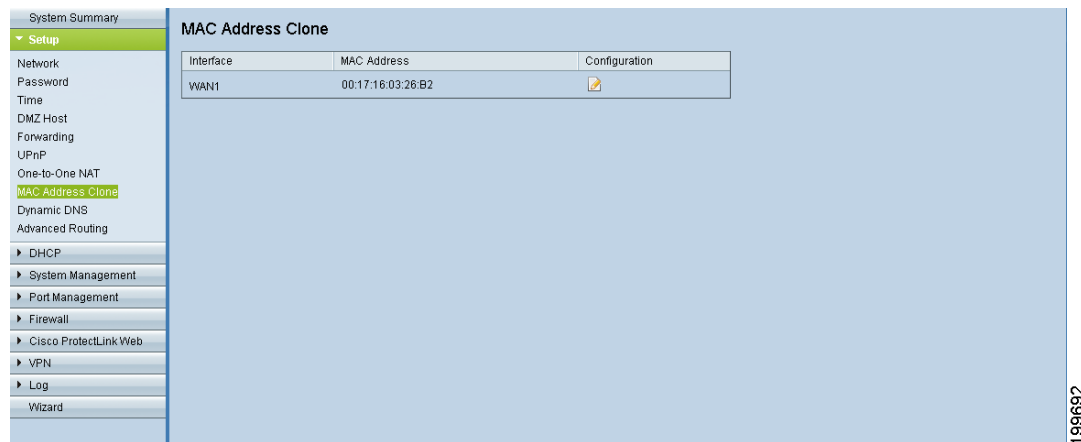
To enable this feature, check the **Enable One-to-One NAT** box. Add or edit entries as needed.

- **To add an entry to the list:** Enter the following information, and then click **Add to List**.
 - **Private Range Begin:** Enter the starting IP address of the internal IP address range that you want to map to the public range. Do not include the router's LAN IP address in this range.
 - **Public Range Begin:** Enter the starting IP address of the public IP address range provided by the ISP. Do not include the router's WAN IP address in this range.
 - **Range Length:** Enter the number of IP addresses in the range. The range length cannot exceed the number of valid IP addresses. To map a single address, enter 1.
- **To add another new entry:** Enter the information, and then click **Add to list**.
- **To modify an entry in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

Cloning a MAC Address for the Router

Some ISPs require that you register a MAC address, which is a 12-digit code assigned to a unique piece of hardware for identification. If you previously registered another MAC address with your ISP, you can use the *Setup > MAC Address Clone* page to “clone” that address to your Cisco RV0xx Series router. By using this process, you don’t have to call your ISP to change the registered MAC address.

To open this page: Click **Setup > MAC Address Clone** in the navigation tree.



This page displays the current settings. Click the **Edit** icon to display the *Edit MAC Address Clone* page. For more information, see [Editing the MAC Address Clone Settings, page 54](#).

Editing the MAC Address Clone Settings

The screenshot shows the 'MAC Address Clone' configuration page. On the left is a navigation menu with 'MAC Address Clone' highlighted. The main content area is titled 'Edit MAC Address Clone'. It shows the 'Interface' as 'WAN1'. There are two radio button options: 'User Defined WAN MAC Address' (selected) with a text input field containing '00:17:16:03:26:B2' and '(Default : 00:17:16:03:26:B2)', and 'MAC Address from this PC' with the value '00:1B:FC:FB:5C:EA'. At the bottom of the form are 'Save' and 'Cancel' buttons. A vertical ID number '199669' is on the right edge of the screenshot.

The *Edit MAC Address Clone* page appears after you click the **Edit** icon on the *MAC Address Clone* page.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

To clone a MAC address, enter the following settings.

- **User Defined WAN MAC Address:** To manually clone a MAC address, click the radio button, and then enter the 12 digits of the MAC address that you registered with your ISP.
- **MAC Address from this PC:** To clone the MAC address of the computer you are currently using to configure the router, click this radio button. The MAC address of your PC is displayed automatically.

Assigning a Dynamic DNS Host Name to a WAN Interface

Dynamic Domain Name System (DDNS) service allows you to assign a fixed domain name to a dynamic WAN IP address, so you can host your own web, FTP or other type of TCP/IP server in your LAN. Use the *Setup > Dynamic DNS* page to configure the WAN interfaces with your Dynamic DNS information.

Before configuring Dynamic DNS on the router, you need to visit www.dyndns.org and register a domain name. (The service is provided by DynDNS.org). For users in China, visit www.3322.org to register.

To open this page: Click **Setup > Dynamic DNS** in the navigation tree.

| Interface | Status | Host Name | Configuration |
|-----------|---|------------------------|---------------|
| WAN1 | Dyndns Enabled : The hostname does not exist. | Dyndns.test.Dyndns.org | |
| WAN2 | Disabled | --- | |
| WAN3 | Disabled | --- | |
| WAN4 | Disabled | --- | |
| WAN5 | Disabled | --- | |
| WAN6 | Disabled | --- | |
| WAN7 | Disabled | --- | |

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

This page displays the current settings. Click the **Edit** icon for the WAN interface to display the *Edit Dynamic DNS Setup* page. For more information, see [Editing the Dynamic DNS Setup, page 56](#).

Editing the Dynamic DNS Setup

The screenshot shows the 'Dynamic DNS' configuration page. On the left is a navigation menu with 'Dynamic DNS' selected. The main area is titled 'Dynamic DNS' and 'Edit Dynamic DNS Setup'. Fields include: Interface (WAN1), Service (DynDNS.org), Username (test), Password (masked with dots), Host Name (test, dyndns, org), and Internet IP Address (10.0.0.102). A red error message states 'The hostname does not exist.' There are 'Save' and 'Cancel' buttons at the bottom.

The *Edit Dynamic DNS Setup* page appears after you click an **Edit** icon on the *Dynamic DNS* page.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

From the **DDNS Service** list, choose your service. Then enter the information for your account, as described below. To disable this feature, choose **Disable**.

- **Username:** Enter the username for your DDNS account.

If you have not previously registered a host name, you can click **Register** to go to the DynDNS.com website, where you can sign up for free Dynamic DNS service. Click the **Sign up FREE** link, and then continue through all of the steps.

- **Password:** Enter the password for your DDNS account.
- **Host Name:** Use these three fields to enter the host name that you registered with your DDNS provider. For example, if your host name is *myhouse.dyndns.org*, then enter *myhouse* in the first field, *dyndns* in the second field, and *org* in the last field.

The following read-only information appears:

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

Setting Up Advanced Routing

Use the *Setup > Advanced Routing* page to configure the dynamic and static routing settings and to view current routing information.

To open this page: Click **Setup > Advanced Routing** in the navigation tree.

The screenshot shows the 'Advanced Routing' configuration page. On the left is a navigation tree with 'Advanced Routing' selected. The main content area is split into two sections:

- Dynamic Routing:**
 - Working Mode: Gateway, Router
 - RIP: Enabled, Disabled
 - Receive RIP versions:
 - Transmit RIP versions:
- Static Routing:**
 - Destination IP:
 - Subnet Mask:
 - Default Gateway:
 - Hop Count (Metric, max. is 15):
 - Interface:
 -

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Perform the following tasks:

- **To configure static or dynamic routing:** Click the **IPv4** or **IPv6** tab, and then enter the settings. See these topics:
 - [Configuring Dynamic Routing, page 58](#)
 - [Configuring Static Routing, page 59](#)
- **To view current data:** Click **View** near the bottom of the page. The *Routing Table Entry List* appears. You can click **Refresh** to update the data, or click **Close** to close the pop-up window.

Configuring Dynamic Routing

Enter the settings for **dynamic routing** by using **Routing Information Protocol (RIP)** (see the glossary for more information).

Dynamic Routing for IPv4:

Click the **IPv4** tab, and then enter the settings described below.

- **Working Mode:** Choose one of the following options.
 - **Gateway:** Choose this mode if the router is hosting your network's connection to the Internet. This is the default setting.
 - **Router:** Choose this mode if the router exists on a network with other routers, and another router acts as the network gateway to the Internet. In Router mode, Internet connectivity is available only if you have another router that functions as the Gateway. Since firewall protection is provided by the gateway router, disable this router's firewall. See [Configuring the General Firewall Settings, page 99](#).
- **RIP:** Routing Information Protocol allows a router to exchange its routing information automatically with other routers, and to dynamically adjust its routing tables as network changes occur. RIP prevents routing loops by using a hop limit. To enable this option, select **Enabled**. Otherwise, keep the default setting, **Disabled**. If you enable this feature, also configure the following settings:
- **Receive RIP versions:** Select the RIP protocol for receiving network data: **None**, **RIPv1**, **RIPv2**, or **Both RIP v1 and v2**.

RIPv1 is a class-based routing version. It does not include subnet information and therefore does not support variable length subnet masks (VLSM). RIPv1 also lacks support for router authentication, making it vulnerable to attacks. **RIPv2** carries a subnet mask and supports password authentication security.

- **Transmit RIP versions:** Select the RIP protocol for transmitting network data: **None**, **RIPv1**, **RIPv2 - Broadcast**, or **RIPv2 - Multicast**.

RIPv2 - Broadcast (recommended) broadcasts data in the entire subnet. **RIPv2 - Multicast** sends data to multicast addresses. RIPv2 - Multicast also helps to avoid unnecessary load by multicasting routing tables to adjacent routers rather than broadcasting to the entire network.

Dynamic Routing for IPv6:

NOTE The IPv6 tab is available if you enabled Dual-Stack IP on the *Setup > Network* page.

Check the box to enable **RIPng (RIP next generation)**, or uncheck the box to disable it. (See the Glossary for more information.)

Configuring Static Routing

Enter the settings for **static routing** (see the Glossary for more information).



WARNING Static routing is an advanced feature. Create these routes with care.

Add or edit entries as needed. Remember that the settings are not saved until you click the Save button.

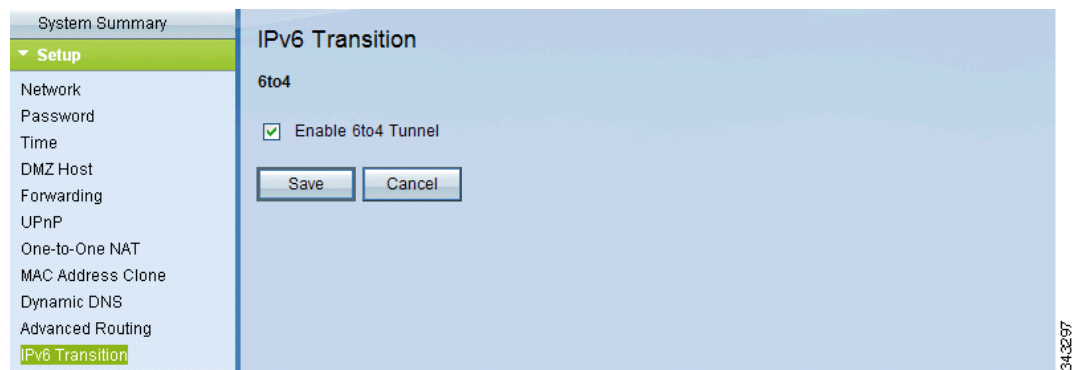
- **To add a new static route:** Enter the following settings, and then click **Add to List**. You can enter up to 30 routes.
 - **Destination IP:** Enter the network address of the remote LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be 0.
 - **Subnet Mask (IPv4 only):** Enter the subnet mask used on the destination LAN IP domain. For Class C IP domains, the subnet mask is 255.255.255.0.
 - **Prefix Length (Pv6 only):** Enter the prefix length.
 - **Default Gateway:** Enter the IP address of the router of the network, for which this static route is created. For example, if this network is connected to the local router's LAN port through another router, use the WAN IP address of that router.
 - **Hop Count:** Enter the appropriate value (maximum is 15). This indicates the number of nodes that a data packet passes through before reaching its destination. A node is any device on the network, such as a computer or router.
 - **Interface:** Select the interface to use for this route. Select a WAN interface if this router provides Internet connectivity for your network. Select **LAN** if this router gets Internet connectivity from a gateway router on your LAN.

-
- **To add another new static route:** Enter the information, and then click **Add to list**.
 - **To modify a static route in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
 - **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.
 - **To view current data:** Click **View** near the bottom of the page. The *Routing Table Entry List* appears. You can click **Refresh** to update the data, or click **Close** to close the pop-up window.
-

IPv6 Transition

When Dual-Stack IP is enabled on the *Network > Setup* page, a 6to4 tunnel is enabled by default for IPv6 packets via 6to4 source/destination addressing exchange. This feature allows the router to establish auto-tunnel in IPv4 network (or a real IPv4 Internet connection) across two independent IPv6 networks. Use the *Setup > IPv6 Transition* page to disable or enable this feature.

To open this page: Click **Setup > IPv6 Transition** in the navigation tree.



Check the box to enable the 6to4 tunnel, or uncheck the box to disable it.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Next steps: For a typical deployment, such as setting up a 6to4 tunnel between your RV0xx Series router and a Cisco RV Series router at another site, you also should complete the tasks listed below.

- On the *DHCP->Router Advertisement* page, enable managed RA flags to support auto-configuration of connected devices. Verify that your IPv6 devices acquire 6to4 prefixes. The prefixes will be in the following format: `2002:<your WAN IP in hexadecimal format>::`
- Temporarily disable the router firewall for testing of your 6to4 tunnel. On the *Firewall > General* page, choose **Disable**. To test the tunnel, attempt to ping an IPv6 address at the remote location.
- After verifying the tunnel as described above, enable the firewall and add access rules on the *Firewall > Access Rules* page. For example, add a rule to allow all traffic through the WAN interface where the source is a single IP

address or a range of addresses on the local network and the destination is a single IP address or a range of addresses on the remote network.

- Complete the required tasks on the router at the other end of the 6to4 tunnel.

NOTE For detailed application notes, see the documentation links in [Appendix H, “Where to Go From Here.”](#)

DHCP

Use the *DHCP* module to configure the settings for the DHCP server or DHCP relay agent, and to view DHCP summary information.

If Dual-Stack IP is enabled on the *Network > Setup* page, you can configure IPv4 and IPv6 settings.

Refer to these topics:

- [Setting Up the DHCP Server or DHCP Relay, page 63](#)
- [Viewing the DHCP Status Information, page 70](#)
- [Router Advertisement \(IPv6\), page 71](#)

Setting Up the DHCP Server or DHCP Relay

Use the *DHCP > DHCP Setup* page to configure this router as a DHCP (Dynamic Host Configuration Protocol) server or as a DHCP relay agent.

A DHCP server automatically assigns available IP addresses to computers on your network. An address is “leased” to a client for a specified time, and then it expires and can be assigned to a different device. If a device needs to have an unchanging IP addresses, you can add the device to the Static IP list. Optionally, you can use the Static IP list to block access by devices that are not on the list or do not have the correct IP address.

If you have another DHCP server on your network, or if you want to assign IP addresses manually, you can disable the DHCP feature and enable DHCP Relay. For more information, see [Enabling DHCP Server and DHCP Relay, page 64](#).

NOTE DHCP Relay is available only on the IPv4 tab. DHCPv6 Relay is not available.

To open this page: Click **DHCP > DHCP Setup** in the navigation tree.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Enabling DHCP Server and DHCP Relay

Click the **IPv4** tab or the **IPv6** tab.

Note: The IPv6 tab is available only if you enabled Dual-Stack IP on the *Network > Setup* page.

Enter the following settings:

- **Enable DHCP server:** Check the box to allow the router to dynamically assign IP addresses to up to 50 connected devices. Uncheck the box if you have another DHCP server on the network or you want to configure static IP addresses for your network devices. If you enable this feature, enter the settings in the **Dynamic IP** section of the page, as described below. Other sections of this page are optional.
- **DHCP Relay (IPv4 only):** If you have another DHCP server, enable DHCP Relay to allow this router to communicate the clients' DHCP requests to the DHCP server. The DHCP Relay mechanism allows the DHCP clients and the DHCP server to be located on different networks. The DHCP clients will send DHCP discover broadcast packets to get IP addresses from the DHCP server. This router will act as DHCP Relay agent and send DHCP unicasts to DHCP server.

Required: Enter the **DHCP Server IP Address**. Other sections of this page are optional.

NOTE *IPv4 only:* If you disable both DHCP server and DHCP Relay, configure each device on your network with a static IP address, subnet mask, and DNS settings. Do not assign the same IP address to different computers.

Dynamic IP (used for DHCP Server only)

- **Client Lease Time:** The Client Lease Time is the amount of time that a network user is allowed to connect to the router with the current dynamic IP address. Enter the amount of time in minutes. Valid values are 5~43,200 minutes. The default is 1440 minutes, which is 24 hours.

NOTE: To receive an IP address from the DHCP server, a client device must be configured to obtain an IP address automatically from a DHCP server. By default, Windows computers are set to obtain an IP automatically.

- **Range Start and Range End:** Enter a starting IP address and an ending IP address to create a range of IP addresses that can be assigned dynamically. The range can include up to 50 IP addresses, which is the maximum that the server can assign. Valid values are 100~149. Do not include the router's LAN IP address in this dynamic IP range. For example, if the router uses the default LAN IP address, **192.168.1.1**, then the starting value must be 192.168.1.2 or greater.

DNS (used for DHCP Server only)

Optionally, enter the IP address of a **DNS Server**. You also can enter a secondary DNS server. Specifying a DNS server can provide quicker access than using a DNS server that is dynamically assigned through the WAN settings. You can keep the default setting of 0.0.0.0 to use a dynamically assigned DNS server.

WINS (used for DHCP Server, IPv4 Only)

Optionally, enter the IP address of a **WINS Server**. Windows Internet Naming Service resolves NetBIOS names to IP addresses. If you do not know the IP address of the WINS server, keep the default, 0.0.0.0.

NOTE To support NetBIOS for DHCP clients, the router uses two methods:

- When the DHCP clients receive dynamic IP addresses from the router, it automatically includes the information of the WINS server to support NetBIOS.
- If a client has a static IP address, then the IP address, subnet mask, default gateway address, and DNS server settings must be configured on the Internet Protocol (TCP/IP) page of the Windows operating system. Then the WINS IP address must be configured on the advanced TCP/IP page. (For more information, refer to Windows Help.)

About Static IP Addresses (for IPv4 Only)

When DHCP is enabled, you may wish to assign static IP addresses to certain devices, such as a web server or an FTP server. You can add up to 100 devices to the *Static IP* list.

TIP Ensure that each of these devices is configured to use a static IP address. For example, on a Windows computer, open the Local Area Connection Properties, select **Internet Protocol (TCP/IP)**, and then click the **Properties** button. Choose **Use the following IP address**, and enter the IP address, subnet mask, and default gateway (the router IP address). Optionally, enter a preferred DNS server.

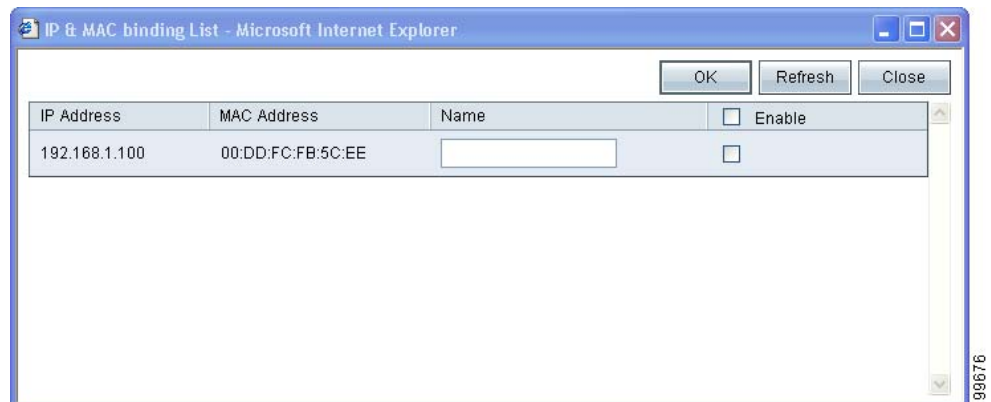
Choose devices from a list or enter the device IP addresses and MAC addresses manually.

- [Assigning static IP addresses by adding devices from a list, page 66](#)
- [Assigning static IP addresses by entering devices manually, page 67](#)
- [Using the Static IP List to Block Devices, page 68](#)

NOTE You can use this feature even if the router is not the DHCP server.

Assigning static IP addresses by adding devices from a list

STEP 1 Click **Show unknown MAC addresses**. The *IP & MAC binding list* appears. If the web browser displays a message about the pop-up window, allow the blocked content.



The devices are listed by the IP address and the MAC address. (Typically the MAC address appears on a label on the bottom panel or back panel of a device.) If needed, you can click **Refresh** to update the data.

- STEP 2** To select a device, first enter a descriptive **Name**. Then check the **Enable** box. Alternatively, select all devices in the list by clicking the check box at the top of the *Enable* column.
- STEP 3** Click **OK** to add the devices to the *Static IP* list, or click **Close** to close the pop-up window without adding the selected devices. After you click **OK**, a message appears. The message includes important information. Read it before clicking **OK**. Keep the browser open and wait until the selected MAC addresses appear in the *Static IP* list.
- STEP 4** Modify or remove list entries, as needed:
- **To modify the settings:** Click a device in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
 - **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

Assigning static IP addresses by entering devices manually

In the *Static IP Address* section, add or edit entries as needed. Remember that the settings are not saved until you click the Save button.

- **To add a new device to the list:** Enter the following information, and then click **Add to list**.
 - **Static IP Address:** Enter the static IP address. You can enter 0.0.0.0 if you want the router to assign a static IP address to the device.
 - **MAC Address:** Enter the MAC address of the device. (Typically the MAC address appears on a label on the bottom panel or the back panel of a device.) Enter the address without punctuation.
 - **Name:** Enter a descriptive name for the device.
 - **Enable:** Check this box to assign the static IP address to this device.
- **To add another new entry:** Enter the information, and then click **Add to list**.

- **To modify the settings:** Click a device in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

Using the Static IP List to Block Devices

You can use the *Static IP list* to control access to your network. You can block access by devices that are not on the list or do not have the correct IP address.

STEP 1 Add devices to the *Static IP list* as described in [About Static IP Addresses \(for IPv4 Only\)](#), page 66.

STEP 2 Enable or disable the following features:

- **Block MAC address on the list with wrong IP address:** Check this box to prevent a computer from accessing your network if its IP address has been changed. For example, if you previously assigned a static IP address of 192.168.1.100 and someone configures the device to use 192.168.149, the device will not be allowed to connect to your network. This feature discourages users from changing their device IP addresses without your permission. Uncheck the box to allow access regardless of the current IP address assignment.
 - **Block MAC address not on the list:** Check this box to block access from devices that are not included in the *Static IP list*. This feature prevents unknown devices from accessing your network. Uncheck the box to allow access by any connected device that is configured with an IP address in the correct range.
-

DNS Local Database

Domain Name Service (DNS) is a service that matches a domain name to its routable IP address. You can set up a DNS Local Database that enables the router to act as a local DNS server for commonly used domain names. Using a local database may be faster than using an external DNS server. If a requested domain name is not found in the local database, then the request is forwarded to the DNS server that is specified on the *Setup > Network* page, *WAN Setting* section.

If you enable this feature, you also must configure the client devices to use the router as the DNS server. By default, Windows computers are set to obtain a DNS server address automatically, from the WAN settings. You need to change the TCP/IP connection settings. For example, on a PC running Windows, go to the *Local Area Connection Properties > Internet Protocol > TCP/IP Properties* window. Choose *Use the following DNS server address*, and then enter the LAN IP address of the router as the Preferred DNS Server. For more information, refer to the documentation for the client that you are configuring.

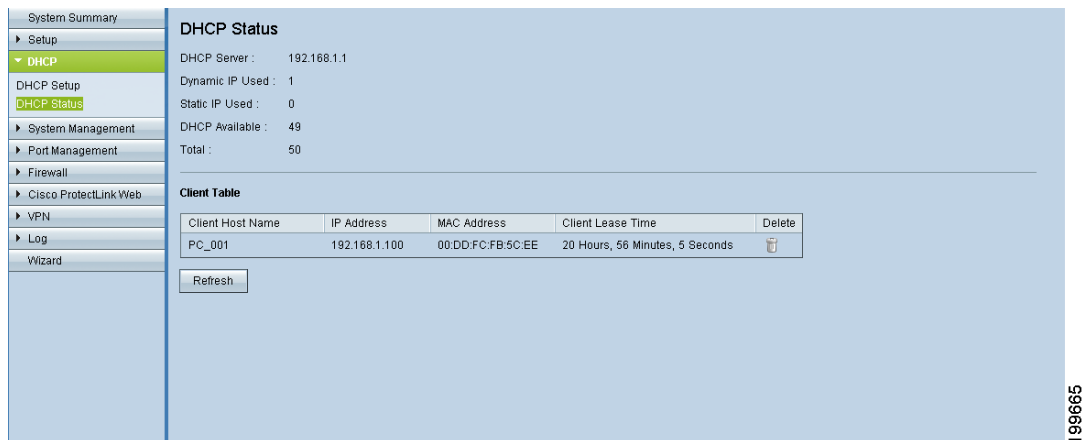
Add or update entries as needed. Remember that the settings are not saved until you click the Save button.

- **To add a new entry:** Enter the following information. Then click **Add to list**.
 - **Host Name:** Enter the domain name, such as *example.com* or *example.org*. If you do not include the final level of the domain name, Microsoft Windows® will automatically append your entry with *.com*.
 - **IP Address:** Enter the IP address of the resource.
- **To add another new entry:** Enter the information, and then click **Add to list**.
- **To modify the settings for a device:** Click a device in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

Viewing the DHCP Status Information

Use the *DHCP > Status* page to view the status of the DHCP server and its clients. You can click **Refresh** to refresh the data. To release a client's IP address, you can click the **Delete** icon.


To open this page: Click **DHCP > DHCP Status** in the navigation tree.



The screenshot displays the DHCP Status page. On the left is a navigation tree with 'DHCP' selected. The main content area shows the following statistics:

- DHCP Server : 192.168.1.1
- Dynamic IP Used : 1
- Static IP Used : 0
- DHCP Available : 49
- Total : 50

Below the statistics is a 'Client Table' with the following data:

| Client Host Name | IP Address | MAC Address | Client Lease Time | Delete |
|------------------|---------------|-------------------|---------------------------------|---|
| PC_001 | 192.168.1.100 | 00:DD:FC:FB:5C:EE | 20 Hours, 56 Minutes, 5 Seconds |  |

A 'Refresh' button is located below the table. The page number '199665' is visible in the bottom right corner.

DHCP Server

For the DHCP server, the following information is shown:

- **DHCP Server:** The IP address of the DHCP server
- **Dynamic IP Used:** The number of dynamic IP addresses used.
- **Static IP Used (IPv4 only):** The number of static IP addresses used.
- **DHCP Available:** The number of dynamic IP addresses available
- **Total:** The total number of dynamic IP addresses that can be assigned by the DHCP server.

Client Table

For all network clients using the DHCP server, the Client Table shows the current DHCP client information. Click the **IPv4** tab or the **IPv6** tab to view the clients. Note: The IPv6 tab is available only if you enabled Dual-Stack IP on the *Network > Setup* page.

- **Client Host Name:** The name assigned to a client host.
- **IP Address:** The dynamic IP address assigned to a client.

- **MAC Address (IPv4 only):** The MAC address of a client.
- **Client Lease Time:** The amount of time that a network user can remain connected to the router with a dynamic IP address.
- **Delete (IPv4 only):** Click the icon to delete the lease and disconnect the client.

Router Advertisement (IPv6)

Use the *DHCP > Router Advertisement* page to enable the **RADVD (Router Advertisement Daemon)** for IPv6 auto-configuration and routing. When this feature is enabled, messages are sent by the router periodically and in response to solicitations. A host uses the information to learn the prefixes and parameters for the local network. Disabling this feature effectively disables auto-configuration, requiring manual configuration of the IPv6 address, subnet prefix, and default gateway on each device.

This page is available if you enabled Dual-Stack IP on the *Setup > Network* page. If you did not do so, a message appears when you try to open this page. After reading the message, you can click **OK** to configure the network settings, or click **Cancel** simply to close the message.

To open this page: Click **DHCP > Router Advertisement** in the navigation tree.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

- **Enable Router Advertisement:** To enable this feature, check the box, and then complete the other fields on the page. To disable this feature, uncheck the box.
- **Advertise Mode:** Choose one of the following options:
 - **Unsolicited Multicast:** Select this option to send Router Advertisement messages to all interfaces in the multicast group. This option is the default setting. If you choose this option, also enter the **Advertisement Interval**, which is the interval at which Router Advertisement messages are sent. Enter any value between 10 and 1800 seconds. The default is 30 seconds.
 - **Unicast only:** Select this option to send Router Advertisement messages only to well-known IPv6 addresses.

- **RA Flags:** Choose whether or not hosts can use DHCPv6 to obtain addresses and other information. The options are described below.
 - *Enabling the Managed flag only:* Check the **Managed** box if you want hosts to use an administered /stateful configuration protocol (DHCPv6) to obtain stateful addresses and other information through DHCPv6.
 - *Enabling the Other flag only:* Check the **Other** box if you want hosts to use an administered/stateful configuration protocol (DHCPv6) to obtain other, non-address information, such as DNS server addresses.
 - *Enabling both flags:* Check both boxes if you want hosts to obtain addresses and other information through DHCPv6.
 - *Disabling both flags:* Uncheck both boxes if you want hosts to obtain addresses and other information through router advertisements and not DHCPv6.
- **Router Preference:** Choose **High**, **Medium**, or **Low**. This preference metric is useful in a network topology in which multi-homed hosts have access to multiple routers. This metric helps a host to choose an appropriate router. If two routers are reachable, the one with the higher preference will be chosen. These values are ignored by hosts that do not implement router preference. The default setting is High.
- **MTU:** Enter the size of the largest packet that can be sent over the network. The **MTU (Maximum Transmission Unit)** is used in Router Advertisement messages to ensure that all nodes on the network use the same MTU value when the LAN MTU is not well-known. The default setting is 1500 bytes, which is the standard value for Ethernet networks. For PPPoE connections, the standard is 1492 bytes. Unless your ISP requires a different setting, this setting should not be changed.
- **Router Lifetime:** Enter the time in seconds that the Router Advertisement messages will exist on the route. The default is 3600 seconds.

System Management

Use the System Management module to manage advanced settings, to configure diagnostic tools, and to perform tasks such as firmware upgrades, backups, and reboots. Refer to these topics:

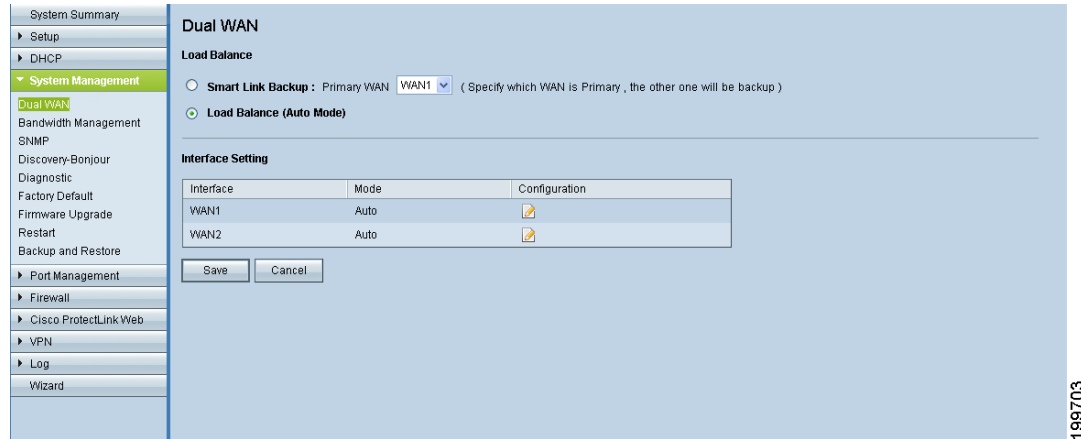
- [Setting Up Dual WAN and Multi-WAN Connections, page 73](#)
- [Managing the Bandwidth Settings, page 81](#)
- [Setting Up SNMP, page 84](#)
- [Enabling Device Discovery with Bonjour, page 85](#)
- [Using Built-In Diagnostic Tools, page 87](#)
- [Restoring the Factory Default Settings, page 89](#)
- [Upgrading the Firmware, page 90](#)
- [Restarting the Router, page 91](#)
- [Backing Up and Restoring the Settings, page 92](#)

Setting Up Dual WAN and Multi-WAN Connections

Use the *System Management > Dual WAN* page (or *Multi-WAN* on RV016) to configure the settings for your Internet connections, if you are using more than one WAN interface.

To open this page: Click **System Management > Dual WAN (or Multi-WAN on RV016)** in the navigation tree.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Mode - Cisco RV042, RV042G, and RV082

You can configure up to two Internet connections by using the Internet port and the DMZ/Internet port. You can choose one of the following modes to manage your WAN connections:

- **Smart Link Backup:** Choose this mode to ensure continuous connectivity. If the primary WAN connection is unavailable, the backup WAN connection is used.
- **Load Balance:** Choose this mode to use both Internet connections simultaneously to increase the available bandwidth. The router balances the traffic between the two interfaces in a weighted round robin fashion.

NOTE: DNS queries are not subject to load balancing.

Mode - Cisco RV016

| Interface | Mode | Configuration |
|-----------|------|---------------|
| WAN1 | Auto | |
| WAN2 | Auto | |
| WAN3 | Auto | |
| WAN4 | Auto | |
| WAN5 | Auto | |
| WAN6 | Auto | |
| WAN7 | Auto | |

You can configure up to seven Internet connections by using the two Internet ports and the five dual-function ports. You can choose one of the following modes to manage your WAN connections:

- **Intelligent Balancer (Auto Mode):** Select this option to balance traffic between all interfaces to increase the available bandwidth. The router balances the traffic between the interfaces in a weighted round robin fashion.
- **IP Group (By Users):** Select this option to group traffic on each WAN interface by priority levels or classes of service (CoS). With this feature, you can ensure bandwidth and higher priority for the specified services and users. All traffic that is not added to the IP Group uses Intelligent Balancer mode. To specify the services and users, click the **Edit** icon for the WAN interface and then add protocol binding entries for each service, IP address, or range of IP addresses.

NOTE: The Router reserves at least one WAN port for non-IP Group users, so WAN1 will always be set to Intelligent Balancer (Auto Mode). Protocol binding is not available for WAN1.

Interface Setting

Click the **Edit** icon for the interface that you want to set up. Then enter the settings on the *Edit Dual WAN* settings page. For more information, see [Editing the Dual WAN and Multi-WAN Settings, page 77](#).

NOTE If there are unsaved changes on the *Dual WAN* page, a warning appears. You can click **OK** to close the message. Then click **Save** to save your changes. After saving your changes, click the **Edit** icon. Alternatively, when the warning appears, click **Cancel** to continue to the edit page without saving the changes.

Editing the Dual WAN and Multi-WAN Settings

The *Dual WAN Settings* page (*Multi-WAN Settings* on RV016) appears after you click the **Edit** icon for a WAN interface on the *Dual WAN* (or *Multi-WAN*) page. Enter the interface settings, as needed.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Max Bandwidth Provided by ISP:

In this section, enter the maximum bandwidth settings as specified by your Internet Service Provider. If the bandwidth exceeds the specified number, then the router uses another WAN interface for the next connection.

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

Network Service Detection:

Optionally, check the box to allow the router to detect network connectivity by pinging specified devices. Then enter the settings below. Uncheck the box to disable this feature.

- **Retry count:** Enter the number of times to ping a device. The default is 5.
- **Retry timeout:** Enter the number of seconds to wait between pings. The default is 30 seconds.
- **When Fail:** Choose the action that will be taken if a ping test fails. If you choose **Generate the Error Condition in the System Log**, the router

records the failure in the System Log. There is no failover to the other interface. If you choose **Remove the Connection**, failover occurs and the backup interface is used. When the WAN port's connectivity is restored, its traffic is restored.

- **Default Gateway, ISP Host, Remote Host, and DNS Lookup Host:** Check the box for each device that you want to ping to determine network connectivity. For an ISP host or a remote host, enter the IP address. For a DNS Lookup host, enter a host name or domain name. Uncheck a box if you do not want to ping this device for network service detection.

Protocol Binding (for Cisco RV016 only, when Load Balancer is selected):

Use this feature to require this interface to be used for specified protocols and specified source and destination addresses. If you enabled IP Group mode, this feature is not available.

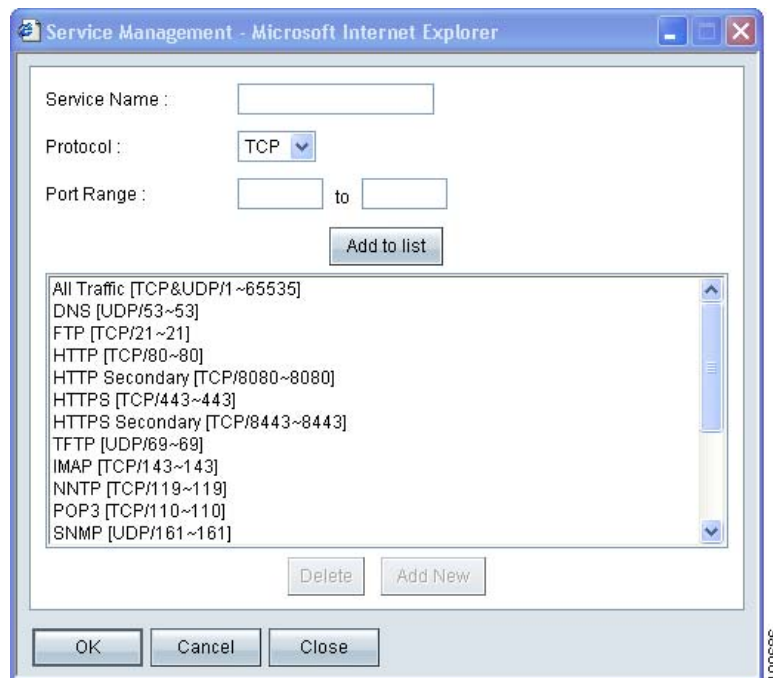
Add or update entries as needed. Remember that your entries are not saved until you click the Save button.

- **To add a new entry to the list:** Enter the settings as described below, and then click **Add to list**.
 - **Service:** Choose a service (or All Traffic) to bind to this WAN interface. If a service is not listed, you can click **Service Management** to add it. For more information, see [Adding a service, page 79](#).
 - **Source IP and Destination IP:** Specify the internal sources and the external destinations for the traffic that goes through this WAN port. For a range of IP addresses, enter the first address in the first field and the final address in the *To* field. For a single IP address, enter the same address in both fields.
 - **Enable:** Check the box to enable this rule, or uncheck the box to disable it.
- **To add another entry to the list:** Enter the information, and then click **Add to list**.
- **To modify an entry in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to deselect the entry and clear the text fields.

- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

Adding a service

To add a new entry to the *Service* list, or to change an entry that you created previously, click **Service Management**. If the web browser displays a warning about the pop-up window, allow the blocked content.



In the *Service Management* window, add or update entries as needed. Before closing this window, click **OK** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

- **To add a service to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 services in the list.
 - **Service Name:** Enter a short description.
 - **Protocol:** Choose the required protocol. Refer to the documentation for the service that you are hosting.
 - **Port Range:** Enter the required port range.

-
- **To add another new service:** Enter the information, and then click **Add to list**.
 - **To modify a service you created:** Click the service in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the service and clear the text fields.
 - **To delete a service from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Managing the Bandwidth Settings

Use the *System Management > Bandwidth Management* page to adjust the bandwidth settings for upstream and downstream traffic and to configure Quality of Service (QoS) settings for various types of traffic. For example, you can enter bandwidth rules to ensure quality for voice services. For a detailed example, see [Appendix F, “Bandwidth Management.”](#)

To open this page: Click **System Management > Bandwidth Management** in the navigation tree.

| Interface | Upstream (Kbit/sec) | Downstream (Kbit/sec) |
|-----------|---------------------|-----------------------|
| WAN1 | 512 | 512 |
| WAN2 | 512 | 512 |

Bandwidth Management Type

Type : Rate Control Priority

Interface : WAN1 WAN2

Service : All Traffic [TCP&UDP(1-65535)]

IP : _____ to _____

Direction : Upstream

Mini. Rate : _____ Kbit/sec

Max. Rate : _____ Kbit/sec

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Max Bandwidth Provided by ISP

Enter the maximum bandwidth settings as specified by your Internet Service Provider.

- **Upstream:** Enter the maximum upstream bandwidth provided by your ISP. The default is **512** kbit/sec.
- **Downstream:** Enter the maximum downstream bandwidth provided by your ISP. The default is **12** kbit/sec.

Bandwidth Management Type

Choose one of the following management options:

- **Rate Control:** Choose this option to specify minimum (guaranteed) bandwidth and maximum (limited) bandwidth for each service or IP address.

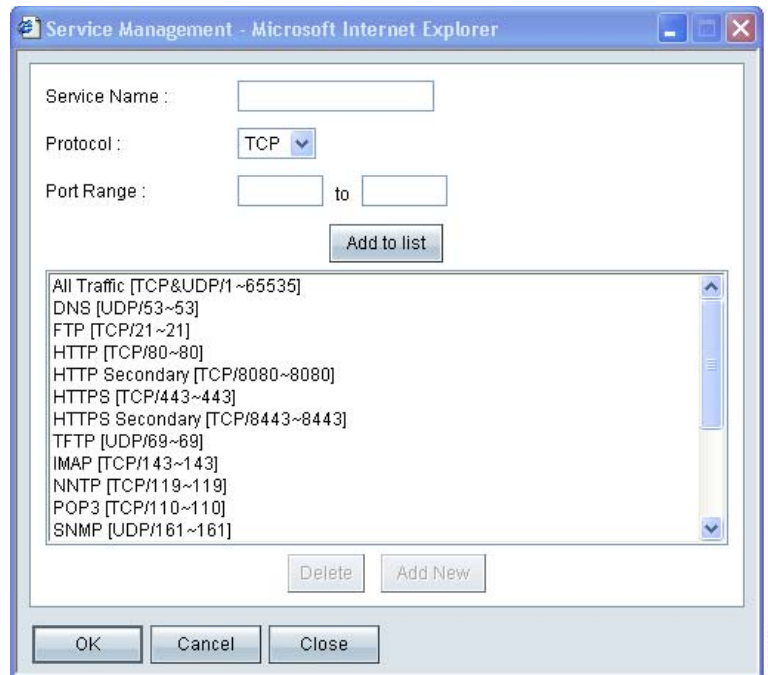
- **Priority:** Choose this option to manage the bandwidth by identifying high-priority and low-priority services.

Select an **Interface**. Add the services that are subject to bandwidth management.

- **To add a new service to the list:** Enter the settings as described below, and then click **Add to List**. You can add up to 100 services.
 - **Service:** Select a service to manage. If a service is not listed, you can click **Service Management** to add a service. For more information, see [Adding a service, page 83](#).
 - **IP (for Rate Control only):** Enter the IP address or range you need to control. To include all internal IP addresses, keep the default setting.
 - **Direction:** Select **Upstream** for outbound traffic, or select **Downstream** for inbound traffic.
 - **Min. Rate (for Rate Control only):** Enter the minimum rate (Kbit/sec) for the guaranteed bandwidth.
 - **Max. Rate (for Rate Control only):** Enter the maximum rate (Kbit/sec) for the guaranteed bandwidth.
 - **Priority (for Priority management only):** Choose the priority for this service: **High** or **Low**.
 - **Enable:** Check the box to enable this feature, or uncheck the box to disable this feature.
- **To add another service to the list:** Enter the information, and then click **Add to list**.
- **To modify a service in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete an entry from the list:** Click the entry that you want to delete, and then click **Delete**. To select a block of entries, click the first entry, hold down the **Shift** key, and then click the final entry in the block. To select individual entries, press the **Ctrl** key while clicking each entry. To de-select an entry, press the **Ctrl** key while clicking the entry.

Adding a service

To add a new entry to the *Service* list, or to change an entry that you created previously, click **Service Management**. If the web browser displays a warning about the pop-up window, allow the blocked content.



In the *Service Management* window, add or update entries as needed. Before closing this window, click **OK** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

- **To add a service to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 services in the list.
 - **Service Name:** Enter a short description.
 - **Protocol:** Choose the required protocol. Refer to the documentation for the service that you are hosting.
 - **Port Range:** Enter the required port range.
- **To add another new service:** Enter the information, and then click **Add to list**.

- **To modify a service you created:** Click the service in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the service and clear the text fields.
- **To delete a service from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Setting Up SNMP

Use the *System Management > SNMP* page to set up SNMP for this router. SNMP, or Simple Network Management Protocol, is a network protocol that allows network administrators to manage, monitor, and receive notifications of critical events as they occur on the network. The router supports SNMP v1/v2c. The router supports standard MIBs (Management Information Bases) such as MIBII, as well as private MIBs. The router acts as an SNMP agent that replies to SNMP commands from SNMP Network Management Systems. The commands it supports are the standard SNMP commands get/next/set. It also generates trap messages to notify the SNMP manager when alarm conditions occur. Examples include reboots, power cycles, and WAN link events.

To open this page: Click **System Management > SNMP** in the navigation tree.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

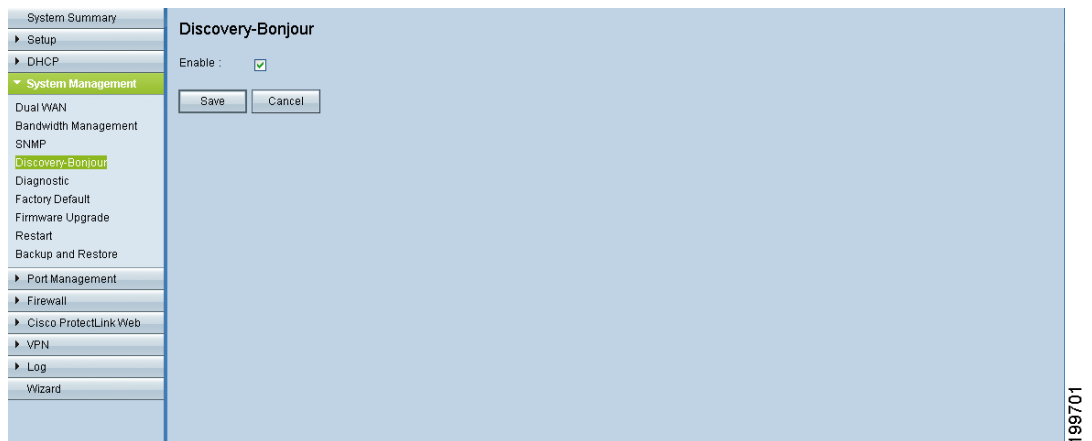
- **Enabled SNMP:** Check this box to enable SNMP. Uncheck the box to disable the this feature. This feature is enabled by default.
- **System Name:** Set the hostname for the router.
- **System Contact:** Enter the name of the network administrator who can be contacted with updates about the router.
- **System Location:** Enter the network administrator's contact information: an e-mail address, telephone number, or pager number.
- **Get Community Name:** Enter a community string for authentication for SNMP GET commands. You can enter a name including up to 64 alphanumeric characters. The default is **public**.
- **Set Community Name:** Enter a community string for authentication for SNMP SET commands. You can enter a name including up to 64 alphanumeric characters. The default is **private**.
- **Trap Community Name:** Create the password that will be sent with each trap to the SNMP manager. You can enter a name including up to 64 alphanumeric characters. The default is **public**.
- **Send SNMP Trap to (For IPv4):** Enter the IP address or domain name for the server where you are running your SNMP management software.
- **Send SNMP Trap to (For IPv6):** When Dual-Stack IP is enabled on the *Network > Setup* page, this field is available. Enter an IPv6 address or domain name for the server where you are running your SNMP management software.

Enabling Device Discovery with Bonjour

Use the *System Management > Discovery-Bonjour* page to enable or disable Bonjour, a service discovery protocol. Bonjour locates network devices such as computers and servers on your LAN. It may be required by network management systems that you use. When this feature is enabled, the router periodically multicasts Bonjour service records to its entire local network to advertise its existence.

NOTE For discovery of Cisco Small Business products, Cisco provides a utility that works through a simple toolbar on the web browser. This utility discovers Cisco devices in the network and display basic information, such as serial numbers and IP addresses, to aid in the configuration and deployment. For more information and to download the utility, please visit www.cisco.com/go/findit.

To open this page: Click **System Management > Discovery-Bonjour** in the navigation tree.



Check the **Enable** box to enable Bonjour. Uncheck the box to disable this feature. It is enabled by default.

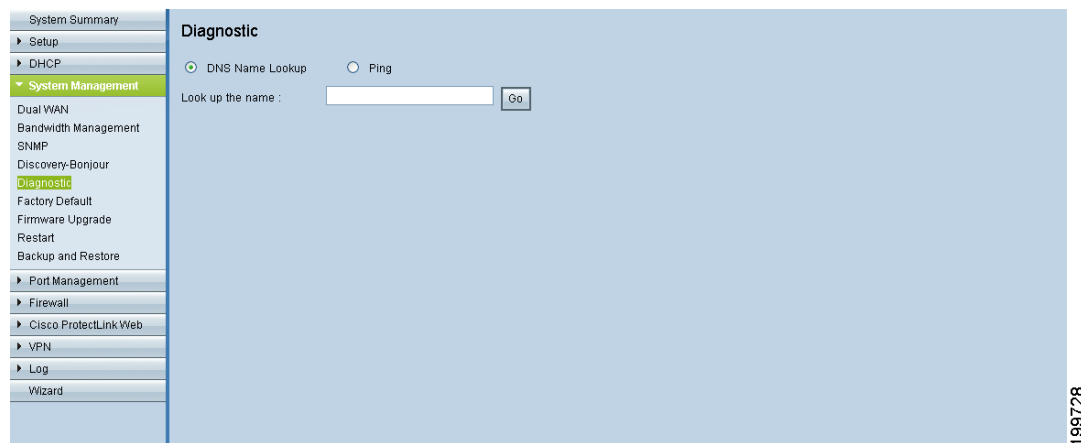
Using Built-In Diagnostic Tools

Use the *System Management > Diagnostic* page to access two built-in tools, DNS Name Lookup and Ping. If you suspect a problem with connectivity, you can use these tools to investigate.

To open this page: Click **System Management > Diagnostic**.

Choose **DNS Name Lookup** if you know a DNS name and want to learn the IP address. Choose **Ping** to test the connectivity to a particular IP address on the Internet.

DNS Name Lookup

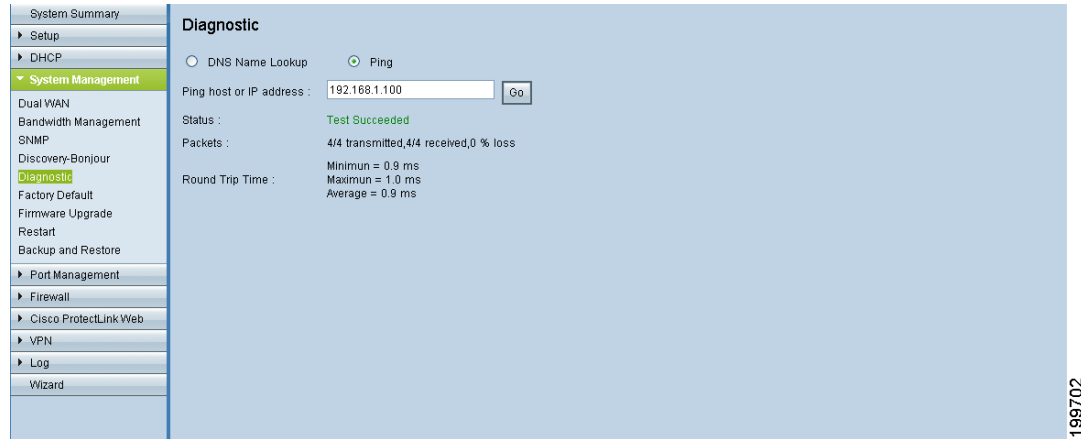


Choose this option to test connectivity to the DNS server that you specified on the *Setup > Network* page, or to look up an IP address that you want to use in the Ping test.

In the **Look up the name** field, enter a host name, such as `www.cisco.com`. Do not include a prefix such as `http://`. Then click **Go**. If the test is successful, the IP address of the host appears.

NOTE This tool requires that the router can connect to a valid DNS server, based on the WAN interface settings (*Setup > Network* page).

Ping



Choose this option to test connectivity to a specified host by entering the IP address. If you do not know the IP address, use the DNS Lookup tool to learn it. The ping test shows if the router is able to send a packet to a remote host and receive a response. If users on the LAN are having problems accessing services on the Internet, first try pinging your DNS server or other server at your ISP. If this test is successful, try pinging devices outside the ISP. This will show if the problem lies with the ISP's connection.

Enter the IP Address, and then click **Go**. If the test is successful, the following information appears:

- **Status:** The status of the ping test: *Testing*, *Test Succeeded*, or *Test Failed*
- **Packets:** The number of packets transmitted, number of packets received, and percentage of packets lost in the ping test
- **Round Trip Time:** The minimum, maximum, and average round trip times for the ping test

Restoring the Factory Default Settings

Use the *System Management > Factory Default* page to clear all of your configuration information and restore the router to its factory default settings. Only use this feature if you want to discard all the settings and preferences that you have configured.

To open this page: Click **System Management > Factory Default** in the navigation tree.



- STEP 1** Click **Return to Factory Default Setting** if you want to restore the router to its factory default settings.
- STEP 2** When the confirmation message appears, click **OK** to continue. If you do not want to restore the factory default settings, click **Cancel**.

Upgrading the Firmware

Use the *System Management > Firmware Upgrade* page to download the latest firmware for your router and to install it.

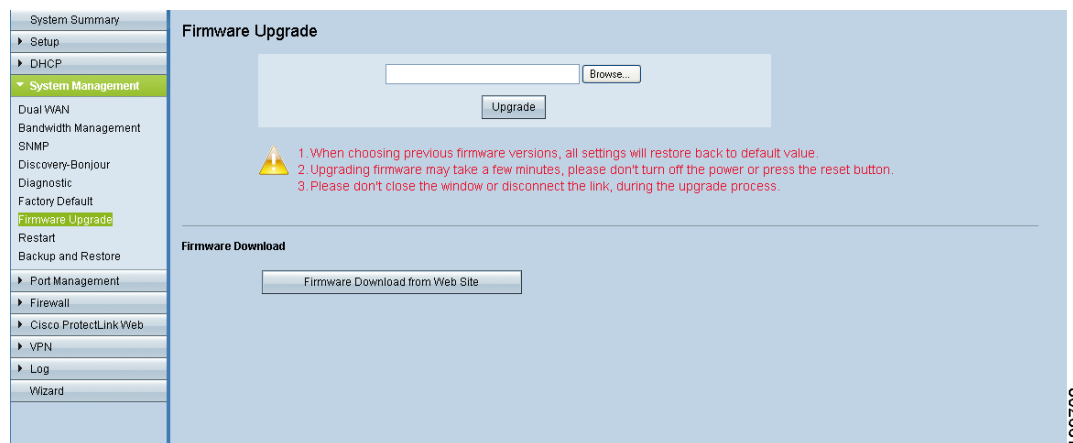


WARNING If you choose an earlier firmware version, the factory default settings will be used. All custom settings.



WARNING Upgrading firmware may take several minutes. Do not turn off the power, press the reset button, close the browser, or disconnect the link during this process.

To open this page: Click **System Management > Firmware Upgrade** in the navigation tree.



Proceed as needed:

- To upgrade from a firmware file on your computer:** Click the **Browse** button, and select the extracted file. Click **Firmware Upgrade Right Now**. After several minutes, the Rebooting message appears. Wait about a minute for the browser to refresh. If the browser does not automatically display the login page, you may need to re-enter the IP address in the browser address bar. If your PC cannot reconnect to the configuration utility, you may need to release and restore your IP address.

- **To download the latest firmware from Cisco:** Click **Firmware Download from Web Site**. Your web browser opens the router information page on Cisco.com. Click the **Download Firmware** button. Continue through the screens to select the latest router firmware and to download the file. Extract the file on your computer. Then perform the firmware upgrade as described above.

Restarting the Router

If you need to restart the router, Cisco recommends that you use the Restart tool on this page. When you restart from the *System Management > Restart* page, the router will send out your log file (if logging is enabled) before it is reset.

To open this page: Click **System Management > Restart** in the navigation tree.



STEP 1 Click **Restart Router** to restart the router.

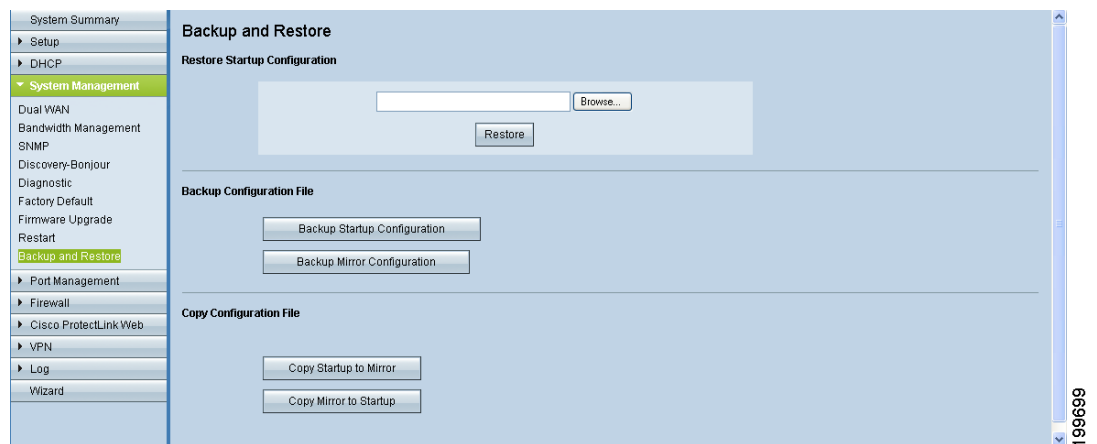
STEP 2 When the confirmation message appears, click **OK** to continue. If you do not want to restart the router, click **Cancel**.

Backing Up and Restoring the Settings

Use the *System Management > Backup and Restore* page to import, export, and copy your configuration files. The router has two configuration files: the startup and the mirror. The Startup file is the configuration file that the router loads when it boots up. The router automatically copies the startup file to the mirror. Thus, the Mirror file contains the last known valid configuration. In the future, if the Startup configuration file fails for any reason, then the Mirror configuration file is used.

NOTE The router automatically copies the startup configuration to the mirror configuration after 24 hours of running in stable condition (no reboot and no configuration changes within a 24-hour period).

To open this page: Click **System Management > Backup and Restore** in the navigation tree.



You can perform the following tasks:

- [Restoring the Settings from a Configuration File, page 92](#)
- [Backing Up Configuration Files and Mirror Files, page 93](#)
- [Copying a Startup File or Mirror File, page 93](#)

Restoring the Settings from a Configuration File

If you want to revert to previously saved settings, you can import a configuration file.

-
- STEP 1** In the *Restore Startup Configuration File* section, click **Browse**.
 - STEP 2** Select a configuration file (.config).
 - STEP 3** Click **Restore**. This process may take up to a minute.
 - STEP 4** Click **System Management > Restart** in the navigation tree.
 - STEP 5** When the confirmation message appears, click **OK**. If you do not want to restart the router, click **Cancel**. The imported settings are not applied until you restart the router.

NOTE: Alternatively, you can use the Restart button. Press the **Restart** button for one second and then release it to restart the router.

Backing Up Configuration Files and Mirror Files

You can save your startup and mirror configuration files to your computer. If needed, you can use these files to restore the settings.

-
- STEP 1** Click **Backup Startup Configuration** or **Backup Mirror Configuration**.
 - STEP 2** When the *File Download* window appears, click **Save**, and then choose a file location. Optionally, you can enter a descriptive filename. Then click **Save**.
TIP: The default filenames are *Startup.config* and *Mirror.config*. It may be helpful to enter a filename that includes the current date and time, for easier identification if you need to import a file later.
 - STEP 3** Close the *Download Complete* window.

Copying a Startup File or Mirror File

If needed, you can manually copy your startup configuration file to your mirror configuration file or you can copy your mirror to your startup.

- TIP** You can use this process to back up a known configuration before you make changes. Copy the startup file to the mirror before making your changes. If you are dissatisfied with your changes, copy the mirror to the startup to restore the settings.

NOTE

- The startup configuration file is automatically copied to the mirror configuration file every 24 hours.

- If a setting is changed, the time counter resets, and the next automatic copy will occur 24 hours later.
- If the mirror config file is still in its factory default state, copying the mirror to the startup immediately resets the router to the factory default settings.

To copy a file, click the button:

- **Copy Startup to Mirror:** Click this button to replace the mirror file with the startup file. The copy operation is performed immediately, with no option to cancel. When the operation is finished, the browser page refreshes.
- **Copy Mirror to Startup:** Click this button to replace the startup file with the mirror file. The copy operation is performed immediately, with no option to cancel. After a short time, the router restarts. If your PC is unable to immediately reload the login page, re-enter the IP address for the configuration utility in the Address bar. Then log in.

Port Management

Use the Port Management module to configure port settings and view the port status.

- [Configuring the Port Settings, page 95](#)
- [Viewing the Status Information for a Port, page 97](#)

Configuring the Port Settings

The default port settings should be sufficient for most small businesses, but you can use the *Port Management > Port Setup* page to customize these settings if needed. You can disable a port or customize its priority, speed, duplex mode, and auto-negotiation settings. You also can enable port-based VLANs to control traffic between devices on your network.

To open this page: Click **Port Management > Port Setup** in the navigation tree.

| Port ID | Interface | Disable | Priority | Speed | Duplex | Auto Negotiation | VLAN |
|--------------|-----------|--------------------------|----------|----------|-----------|--|-------|
| 1 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 2 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 3 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 4 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 5 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 6 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 7 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| 8 | LAN | <input type="checkbox"/> | Normal | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | VLAN1 |
| DMZ/Internet | WAN2 | <input type="checkbox"/> | | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | |
| Internet | WAN1 | <input type="checkbox"/> | | 10M 100M | Half Full | <input checked="" type="checkbox"/> Enable | |

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

For Cisco RV016 only, choose the number of WAN ports from the drop-down list, or keep the default number, 2. If you change the number, save your settings. (You can also change the number of WAN ports by using the *Setup > Network* page.)

The following read-only information is displayed for each port:

- **Port ID:** The port number or name, as it is labeled on the device
- **Interface:** The interface type: LAN, WAN, or DMZ

Enter the following settings, as needed:

- **Disable:** Check this box to disable a port. By default, all ports are enabled.
- **Priority** (for LAN ports only): Use this setting to ensure Quality of Service by prioritizing the traffic for devices on particular ports. For example, you might assign High priority to a port that is used for gaming or videoconferencing. For each port, select the appropriate priority level, **High** or **Normal**. The default setting is Normal.
- **Speed:** If you want to adjust this setting, first uncheck the **Enable** box in the *Auto Neg* column to disable auto-negotiation. Then select the port speed: **10M** or **100M**.
- **Duplex:** If you want to set the duplex mode, first uncheck the **Enable** box in the *Auto Neg* column to disable auto-negotiation. Select the duplex mode, **Half** or **Full**.
- **Auto Neg.:** Check the **Enable** box to allow the router to auto-negotiate connection speeds and duplex mode. This feature is enabled by default.
- **VLAN** (for LAN ports only): All LAN ports are on VLAN 1 by default. To place a port on a separate VLAN, choose a VLAN from the drop-down list.

The number of available VLANs equals the number of LAN ports: 4 on Cisco RV042 and RV042G, 8 on Cisco RV082, and up to 13 on Cisco RV016 (depending on the usage of the dual-function ports). For example, on Port 4, you may have an Ethernet switch that provides Internet connectivity to guest users in a conference room. To prevent your guests from accessing the file servers and printers on your LAN, you could put Port 4 on VLAN 2 and leave the other ports on VLAN 1. There is no communication between devices on separate VLANs.

Viewing the Status Information for a Port

Use the *Port Management > Port Status* page to view information and statistics for a selected port.

To open this page: Click **Port Management > Port Status** in the navigation tree.

| Port Status | |
|------------------------------|------------------------|
| Port ID | 1 |
| Summary | |
| Type : | 10Base-T / 100 Base-TX |
| Interface : | LAN |
| Link Status : | Down |
| Port Activity : | Port Enabled |
| Priority : | Normal |
| Speed Status : | 10 Mbps |
| Duplex Status : | Half |
| Auto Negotiation : | Enabled |
| VLAN : | VLAN1 |
| Statistics | |
| Receive Packet Count : | 0 |
| Receive Packet Byte Count : | 0 |
| Transmit Packet Count : | 0 |
| Transmit Packet Byte Count : | 0 |
| Packet Error Count : | 0 |

From the **Port ID** list, choose a port. You can click **Refresh** to update the data.

Summary

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

- **Type:** The port type
- **Interface:** The interface type, LAN or WAN,
- **Link Status:** The status of the connection
- **Port Activity:** The status of the port
- **Speed Status:** The speed of the port, 10 Mbps or 100 Mbps
- **Duplex Status:** The duplex mode: *Half* or *Full*.
- **Auto negotiation:** The status of the feature
- **VLAN:** The VLAN of the port

Statistics

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

- **Port Receive Packet Count:** The number of packets received
- **Port Receive Packet Byte Count:** The number of packet bytes received
- **Port Transmit Packet Count:** The number of packets transmitted
- **Port Transmit Packet Byte Count:** The number of packet bytes transmitted
- **Port Packet Error Count:** The number of packet errors

Firewall

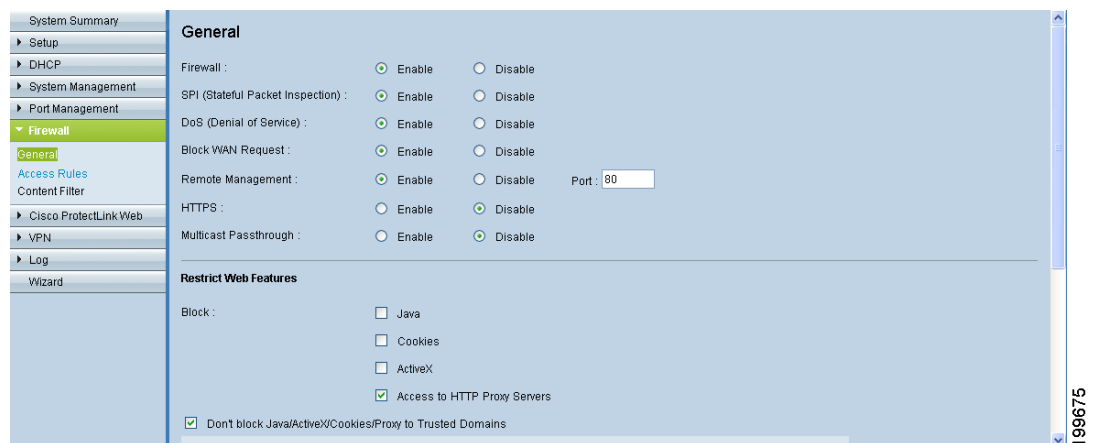
Use the Firewall module to configure the firewall features, create access rules, and set content filters to control your users' Internet activities. Refer to these topics:

- [Configuring the General Firewall Settings, page 99](#)
- [Managing Access Rules, page 104](#)
- [Configuring Firewall Access Rules, page 103](#)
- [Using Content Filters to Control Internet Access, page 110](#)

Configuring the General Firewall Settings

The default firewall settings should be sufficient for most small businesses. However, you can use the *Firewall > General* page to disable the firewall or to specify the types of attacks that you want to block. You also can restrict potentially risky website features such as Java and cookies.

To open this page: Click **Firewall > General** in the navigation tree.



NOTE

- If you want to disable the firewall (not recommended), you can do so only if you have configured the administrator password. If you are still using the default password, you must change it. For more information, see [Changing the Administrator Username and Password, page 40](#).
- Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Enable or disable the firewall and related features:

- **Firewall:** Choose to enable or disable the firewall. This feature is enabled by default and is strongly recommended to protect your network. Enabling or disabling the firewall also affects several related features, as described below. Disabling the firewall also disables Access Rules and Content Filters.

If you choose **Disable** and you are still using the default administrator password, a message appears. To protect your router from unauthorized access, you must change the password before you can disable the firewall. Click **OK** to continue to the *Password* page, or click **Cancel** to remain on the current page. After you change your password, you can return to this page to resume this procedure.

- **SPI (Stateful Packet Inspection):** When enabled, this feature allows the router to review the information that passes through the firewall. It inspects all packets based on the established connection, prior to passing the packets for processing through a higher protocol layer. This feature can be enabled only when the firewall is enabled.
- **DoS (Denial of Service):** When enabled, this feature protects internal networks from Internet attacks, such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing, and reassembly attacks. This feature can be enabled only when the firewall is enabled.
- **Block WAN Request:** When enabled, this feature allows the router to drop both unaccepted TCP requests and ICMP packets from the WAN side. Hackers will not find the router by pinging the WAN IP address. This feature can be enabled only when the firewall is enabled.
- **Remote Management:** When enabled, this feature allows you to connect to the router's web-based configuration utility through a WAN connection. This feature is disabled by default. It can be enabled only when the firewall is enabled. If you want to enable remote management, you should first configure a strong administrator password on the *Setup > Password* page. This precaution prevents an unauthorized user from accessing the router with the default password. If you enable this feature, you can keep the

default **Port** setting, 80, or enter another port number (8080 is usually used for this purpose).

NOTE: When remote management is enabled, you can use a web browser to access the configuration utility from anywhere on the Internet. In a web browser, enter **http://<WAN IP address of the router>:port**, or enter **https://<WAN IP address of the router>:port** if you have enabled the HTTPS feature.

- **HTTPS:** When enabled, this feature allows secured HTTP sessions. This feature is enabled by default.

NOTE: If you disable the HTTPS feature, then users cannot connect by using QuickVPN.

- **Multicast Pass Through:** When enabled, this feature allows IP multicast packets to be forwarded to the appropriate LAN devices. Multicast Pass Through is used for Internet games, videoconferencing, and multimedia applications. This option is disabled by default.

IMPORTANT: This router does not support passing multicast traffic over an IPSec tunnel. The multicast passthrough option determines whether the router allows the multicast traffic originating from the Internet to pass through the firewall to the LAN.

Restrict Web Features

- **Java:** Check the box if you want to block Java applets at the firewall. Java is a common programming language for websites. If you deny Java applets, you run the risk of losing access to Internet sites created with this programming language. As a compromise, you can check this box to block Java on untrusted or unknown sites, while allowing Java on trusted sites (see *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains* below). By default, Java is not blocked.
- **Cookies:** Check this box if you want to block all cookies at the firewall. A cookie is data that a web site stores on a user's PC. If you block cookies, a web site may not function as expected. As a compromise, you can check this box to block cookies on untrusted or unknown sites, while allowing them on trusted sites (see *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains* below). By default, cookies are not blocked.
- **ActiveX:** Check the box if you want to block ActiveX controls at the firewall. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of losing access to Internet sites created using this programming language. As a compromise, you can check this box to block ActiveX on untrusted or unknown sites, while allowing ActiveX on trusted

sites (see *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains* below). By default, ActiveX is not blocked.

- **Access to HTTP Proxy Servers:** Check this box if you want to block access to HTTP proxy servers. Use of WAN proxy servers may compromise the router's security. If you enable this feature, you block access to proxy servers using port 80 or 8080. As a compromise, you can check this box to block access to untrusted or unknown servers, while allowing access to trusted servers (see *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains* below). By default, access to HTTP proxy servers is not blocked.
- **Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains:** If you blocked any of the web features, you can check this box to allow these features for the domains that you enter on the trusted list. (This area of the page is available only if you checked one of the other boxes to disable a web feature.) If you leave the box unchecked, then the selected web features are blocked for all websites.
 - **To add a domain to the trusted list:** Enter the domain that you want to add to the trusted list. Then click **Add to list**.
 - **To add another domain to the trusted list:** Enter the domain, and then click **Add to list**.
 - **To modify a domain in the trusted list:** Click the domain. The information appears in the text field. Make changes, and then click **Update**.
 - **To remove a domain from the trusted list:** Click the domain, and then click **Delete**.

Configuring Firewall Access Rules

The default access rules should be sufficient for most small businesses. However, you can use the *Firewall > Access Rules* page to modify or add new access rules for your network. Access rules determine which traffic is allowed to pass through the router's firewall. Optionally, you can set a schedule to activate or deactivate each access rule for specified days and times.

To open this page: Click **Firewall > Access Rules** in the navigation tree.

| Priority | Enable | Action | Service | Source Interface | Source | Destination | Time | Day | Delete |
|----------|-------------------------------------|--------|-----------------|------------------|--------|-----------------------------|--------|-----|--------|
| | <input checked="" type="checkbox"/> | Deny | All Traffic [1] | WAN5 | Any | Any | Always | | |
| | <input checked="" type="checkbox"/> | Allow | All Traffic [1] | WAN6 | Any | 10.0.0.0 - 10.0.0.255 | Always | | |
| | <input checked="" type="checkbox"/> | Deny | All Traffic [1] | WAN6 | Any | Any | Always | | |
| | <input checked="" type="checkbox"/> | Allow | All Traffic [1] | WAN7 | Any | 10.0.0.0 - 10.0.0.255 | Always | | |
| | <input checked="" type="checkbox"/> | Deny | All Traffic [1] | WAN7 | Any | Any | Always | | |
| | <input checked="" type="checkbox"/> | Deny | All Traffic [1] | DMZ | Any | 192.168.1.0 - 192.168.1.255 | Always | | |
| | <input checked="" type="checkbox"/> | Allow | All Traffic [1] | DMZ | Any | Any | Always | | |

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Refer to these topics:

- [About Access Rules, page 103](#)
- [Managing Access Rules, page 104](#)
- [Configuring Access Rules, page 106](#)

About Access Rules

The router has the following default rules:

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

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



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

There are four additional default rules that will be always active and cannot be overridden by any custom rules:

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

Managing Access Rules

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

Click the **IPv4** tab to set rules for traffic with IPv4 addressing, or click the **IPv6** tab to set rules for traffic with IPv6 addressing.

Note: The IPv6 tab is available only if you enabled Dual-Stack IP on the *Network > Setup* page.

NOTE As an alternative to this procedure, you can use the Access Rule Wizard. For more information, see [Chapter 11, “Wizard.”](#)

If you have numerous rules, you can adjust the display. Use the *Rows per page list* at the top right corner of the table to choose the number of rules to display on each page. Use the *Page list* below the table to choose a particular page. Use the navigation buttons to view the first page, previous page, next page, or final page. Some buttons may be unavailable, depending on the number of pages and the current selection.

- **Priority:** The priority of the access rule, with 1 indicating the highest priority. To change the priority for a rule, select an option from the drop-down list. If there is a conflict between two access rules, then the higher

priority rule takes precedence. The default access rules have the lowest priority.

When an access rule is created, the router automatically assigns a priority; however, you can change the priority after the rule is created.

- **Enable:** To enable a rule, check the **Enable** box. To disable a rule, uncheck the box. You cannot change the default rules.

Additional information appears that cannot be changed on this page:

- **Action:** The action that the rule performs, to Allow or Deny access
- **Service:** The service that is affected by this rule
- **Source Interface:** The source interface that is affected by this rule
- **Source:** The IP address for the source of the traffic, or Any
- **Destination:** The IP address for the destination of the traffic, or Any
- **Time:** A specific time interval when the access rule is active, or Always
- **Day:** Specific days when the access rule is active, or Always

Add or edit rules as needed.

- **To add a rule:** Click **Add New Rule**. Enter the settings, as described in [Configuring Access Rules, page 106](#).
- **To modify a custom rule:** Click the **Edit** icon. Enter the settings, as described in [Configuring Access Rules, page 106](#).
- **To delete an access rule:** Click the **Delete** icon. When the confirmation message appears, click **OK** to continue, or click **Cancel** to close the message without deleting the rule.
- **To delete all custom rules:** Click **Restore to Default Rules**.

Configuring Access Rules

After you click **Add New Rule** or the **Edit** icon on the *Access Rules* table, enter the following information on the add/edit page.

NOTE Before navigating away from this page, click **Save** to save your settings. When the Success message appears, click **OK** to remain on the current page to add another access rule, or click **Cancel** to return to the *Access Rules* table. To undo your changes on this page, click **Cancel**. Any unsaved changes are abandoned.

Services (IPv4 and IPv6)

- **Action:** Choose the action that the rule performs, to Allow or Deny access.
- **Service:** Choose the service that is affected by this rule. If you need to add a service, click **Service Management**. For more information, see [Adding a service, page 108](#).
- **Log:** To include events for this rule in the log, click **Log packets match this rule**. Otherwise, click **Not log**. This setting is applicable when logging is enabled. For more information, see [Chapter 10, “Logging System Statistics.”](#)
- **Source Interface:** Choose the source interface that is affected by this rule.
- **Source IP (IPv4) or Source IP / Prefix Length (IPv6):** Identify the source of the traffic that is affected by this rule. From the drop-down list, choose one of the following options:
 - **Single:** This rule applies to a single IP address. Enter the IP address.

- **Range:** This rule applies to a range of IP addresses (IPv4 only). Enter the first IP address of the range in the first box, and then enter the final IP address in the second box.
- **Subnet:** This rule applies to a subnetwork (IPv6 only). Enter the IP address and the prefix length.
- **ANY:** This rule applies to any IP address.
- **Destination IP (IPv4) or Destination IP / Prefix Length (IPv6):** Identify the destination of the traffic that is affected by this rule. From the drop-down list, choose one of the following options:
 - **Single:** This rule applies to a single IP address. Enter the IP address.
 - **Range:** This rule applies to a range of IP addresses (IPv4 only). Enter the first IP address of the range in the first box, and then enter the final IP address in the second box.
 - **Subnet:** This rule applies to a subnetwork (IPv6 only). Enter the IP address and the CIDR notation number for the subnet.
 - **ANY:** This rule applies to any IP address.

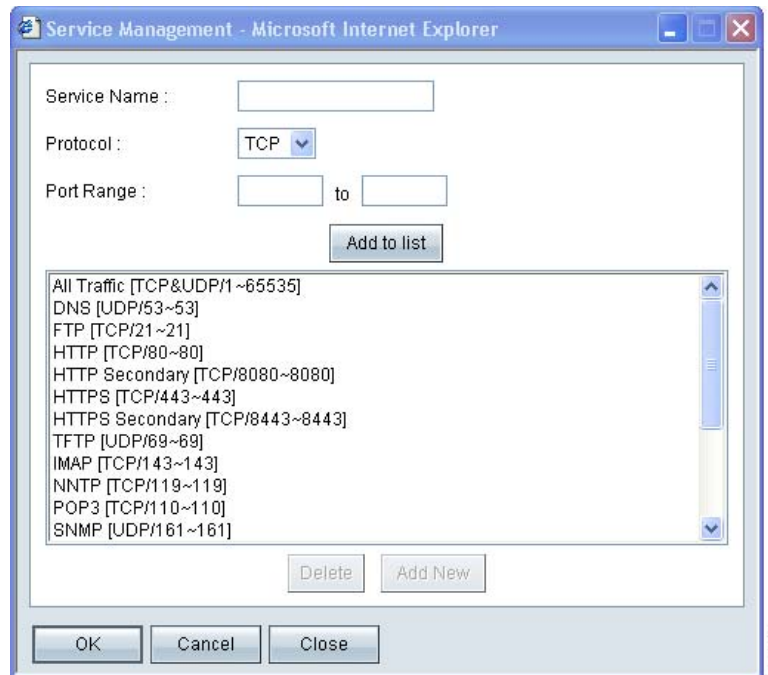
Schedule (IPv4 Only)

Keep the default settings or specify a schedule when this rule is active:

- **Time:** Choose one of the following options:
 - **Always:** Choose this option if the rule applies at all times and on all days of the week. Optionally, you can enter a time period in the *From* and *To* fields.
 - **Interval:** Choose this option to specify the time period when the rule is active. If you choose this option, you must enter a time period in the *From* and *To* fields. Optionally, you can specify the days of the week.
- **From and To:** If you chose Interval, use these fields to specify the times and days when the rule is active. Enter the start time in the *From* field and enter end time in the *To* field. Use hh:mm format, such as 15:30 for 3:30 p.m. Enter 00:00 to 00:00 if the rule applies during all times of day.
- **Effective on:** If you chose Interval, use these check boxes to specify the days when the rule is active. Check the **Everyday** box if the rule is active on all days. To choose specific days, uncheck the **Everyday** box and then check the box for each day when the rule is active.

Adding a service

To add a new entry to the *Service* list, or to change an entry that you created previously, click **Service Management**. If the web browser displays a warning about the pop-up window, allow the blocked content.



In the *Service Management* window, add or update entries as needed. Before closing this window, click **OK** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

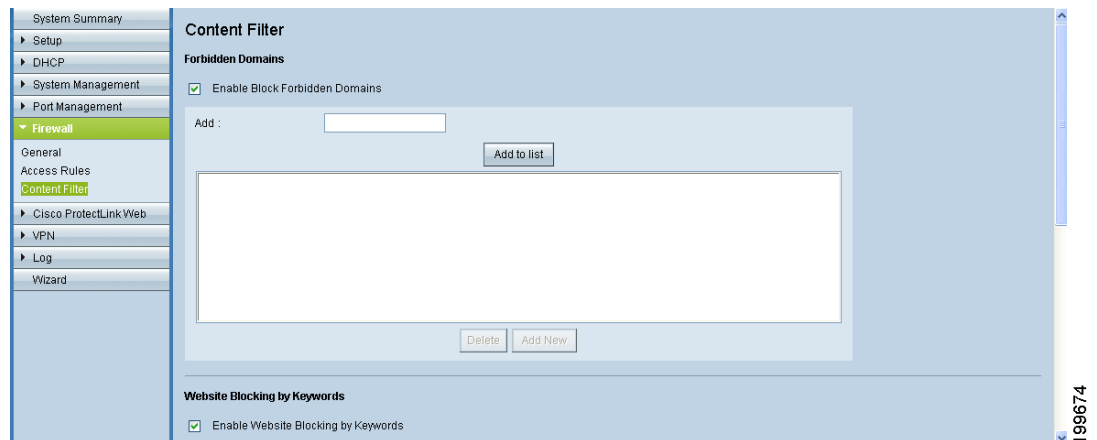
- **To add a service to the list:** Enter the following information, and then click **Add to List**. You can have up to 30 services in the list.
 - **Service Name:** Enter a short description.
 - **Protocol:** Choose the required protocol. Refer to the documentation for the service that you are hosting.
 - **Port Range:** Enter the required port range.
- **To add another new service:** Enter the information, and then click **Add to list**.

-
- **To modify a service you created:** Click the service in the list. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the service and clear the text fields.
 - **To delete a service from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Using Content Filters to Control Internet Access

Use the *Firewall > Content Filter* page to prevent your users from accessing inappropriate websites. You can block access by specifying domains and keywords.

To open this page: Click **Firewall > Content Filter** in the navigation tree.



NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

You can block access to specified domains or, to block a wider range of sites, block access to URLs containing specified keywords. You also can specify the days and hours when these filters are active. This page includes these sections:

- [Forbidden Domains, page 111](#)
- [Website Blocking by Keywords, page 111](#)
- [Schedule, page 112](#)

NOTE The content filter rules will be automatically disabled if the Cisco ProtectLink service is activated on the router. Instead configure the ProtectLink features to control Internet access. For more information, see [Chapter 8, “Cisco ProtectLink Web.”](#)

Forbidden Domains

Check the **Enable Block Forbidden Domains** box to allow the router to block access to specified domains. Uncheck the box to disable this feature.

Add or edit rules as needed. Remember that your entries are not saved until you click the Save button.

- **To add an entry to the list:** Type the domain name in the **Add** box. Then click **Add to list**. Repeat this task as needed to add other domains.

Access is blocked if a user enters a specified domain name in the browser address bar or navigates to a web page within a specified domain. For example, assume that *yahoo.com* is blocked. The user cannot successfully enter any URL that begins with *yahoo.com*. Access also is blocked if the user performs a web search and clicks a link for a page within the specified domain, such as *yahoo.com/news*. However, the user can connect to *mail.yahoo.com*, which is a different domain.

- **To modify an entry in the list:** Click the entry that you want to modify. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text field.
- **To delete an entry from the list:** Click the entry that you want to delete. Then click **Delete**.

Website Blocking by Keywords

Check the **Enable Website Blocking By Keywords** box to allow the router to block access to URLs that include specified characters. Uncheck the box to disable this feature.

Add or edit rules as needed. Remember that your entries are not saved until you click the Save button.

- **To add an entry to the list:** Type a keyword in the **Add** box. Then click **Add to list**. A keyword can be a complete word, such as *government*, or a few characters, such as *gov*. Repeat this task as needed to add other keywords.

Access is blocked if the user enters or navigates to a URL that includes the specified characters. For example, assume that *yahoo* is blocked. The user cannot access *www.yahoo.com*, *finance.yahoo.com*, or *mydomain.com/news/yahoo*.

- **To modify an entry in the list:** Click the entry that you want to modify. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text field.

- **To delete an entry from the list:** Click the entry that you want to delete. Then click **Delete**.

Schedule

Keep the default settings or specify a schedule when content filtering is active:

- **Time:** Choose one of the following options:
 - **Always:** Choose this option if the rule applies at all times and on all days of the week. Optionally, you can enter a time period in the *From* and *To* fields.
 - **Interval:** Choose this option to specify the time period when the rule is active. If you choose this option, you must enter a time period in the *From* and *To* fields. Optionally, you can specify the days of the week.
- **From and To:** If you chose Interval, use these fields to specify the times and days when the rule is active. Enter the start time in the *From* field and enter end time in the *To* field. Use hh:mm format, such as 15:30 for 3:30 p.m. Enter 00:00 to 00:00 if the rule applies during all times of day.
- **Effective on:** If you chose Interval, use these check boxes to specify the days when the rule is active. Check the **Everyday** box if the rule is active on all days. To choose specific days, uncheck the **Everyday** box and then check the box for each day when the rule is active.

Cisco ProtectLink Web

The optional Cisco ProtectLink Web service provides security for your network. This service is available for all RV0xx Series routers except Cisco RV042G. Cisco ProtectLink web filters website addresses (URLs) and blocks potentially malicious websites. Refer to these topics:

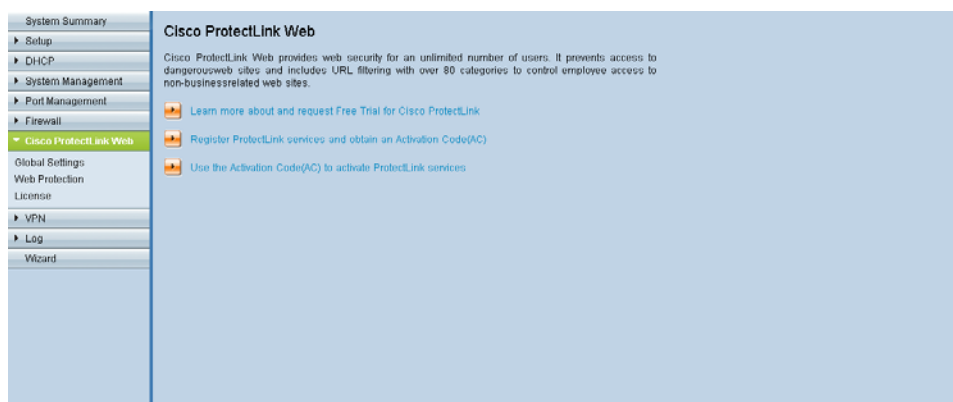
- [Getting Started with Cisco ProtectLink Web, page 113](#)
- [Specifying the Global Settings for Approved URLs and Clients, page 115](#)
- [Updating the ProtectLink License, page 120](#)

NOTE For more information about this Cisco product, visit the Cisco ProtectLink Web information page at www.cisco.com/en/US/products/ps9953/index.html

Getting Started with Cisco ProtectLink Web

You can purchase, register, and activate the service by using the links on the *Cisco ProtectLink Web* page.

To open this page: Click **Cisco ProtectLink Web** in the navigation tree.



Choose the appropriate option:

- **Learn more about and request Free Trial for Cisco ProtectLink:** Click this link to open the Cisco ProtectLink Security Solutions page on Cisco.com. You can read product information and get a 30-day trial for your RV router.
- **Register ProtectLink services and obtain an Activation Code (AC):** Click this link if you purchased the product and are ready to register it. When the registration page appears, follow the on-screen instructions to enter your Registration Key and provide the required information. Close the web page when you complete this process. The activation code will appear on the screen and will be sent to the email address that you provided.
- **Use the Activation Code (AC) to activate ProtectLink services:** Click this link if you registered the product and received an activation code. When the activation page appears, enter your activation code and follow the on-screen instructions to proceed. Close the web page when you complete this process. Refresh the web browser, and now the ProtectLink Web features are available on your router. The *Global Settings* page appears.

NOTE If you replace one router with another router that supports this service, you can use the **Use the Activation Code** link to transfer your license for the ProtectLink service to the new router.

Specifying the Global Settings for Approved URLs and Clients

After you activate your service, you can use the *Cisco ProtectLink Web > Global Settings* page to configure the services on the router.

To open this page: Click **ProtectLink > Global Settings** in the navigation tree.

The screenshot shows the 'Global Settings' page in the Cisco ProtectLink Web interface. On the left is a navigation tree with 'Cisco ProtectLink Web' expanded to 'Global Settings'. The main content area is titled 'Global Settings' and contains two sections: 'Approved URLs' and 'Approved Clients'. Each section has a checkbox to enable the list, a table with columns for the list items and 'Configuration', and an 'Add' button. At the bottom are 'Save' and 'Cancel' buttons. A vertical ID number '199684' is visible on the right side of the screenshot.

NOTE This page is available only if you activated your Cisco ProtectLink Web service. See [Getting Started with Cisco ProtectLink Web, page 113](#).

You can specify approved URLs that the users are always able to access. You also can specify approved clients who are not subject to the restrictions that you configure in Web Protection.

To add an entry to the *Approved URLs* table or the *Approved Clients* table, click **Add**. To delete an entry, click the Delete icon.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Approved URLs and Approved Clients

After you click the Add button on the *Cisco ProtectLink Web > Global Settings* page, the Configuration page appears.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Approved URL Configuration

The domains on this list are always accessible, regardless of the Web Protection settings.

Check the **Enable Approved URL list** box to enable this feature. Then add up to 20 trusted URLs that are always accessible.

- **To add entries:** Click **Add New** to open the *Approved URL Configuration* page. Enter the trusted URL(s) in the box. To enter multiple URLs, type a semi-colon between entries, such as *www.cisco.com;www.google.com;www.mycompany.com*. All pages in the specified domains will be accessible. Click **Save** to save your changes, or click **Cancel** to undo them.

If you entered any invalid characters, a message appears. Click **OK** to close the message, and edit your entries. Spaces, commas, and symbols are not allowed.

- **To delete an entry:** Click the **Delete** icon.

Approved Clients Configuration

The clients on this list are always able to connect to all websites. Web Protection will not restrict URL requests from these IP addresses.

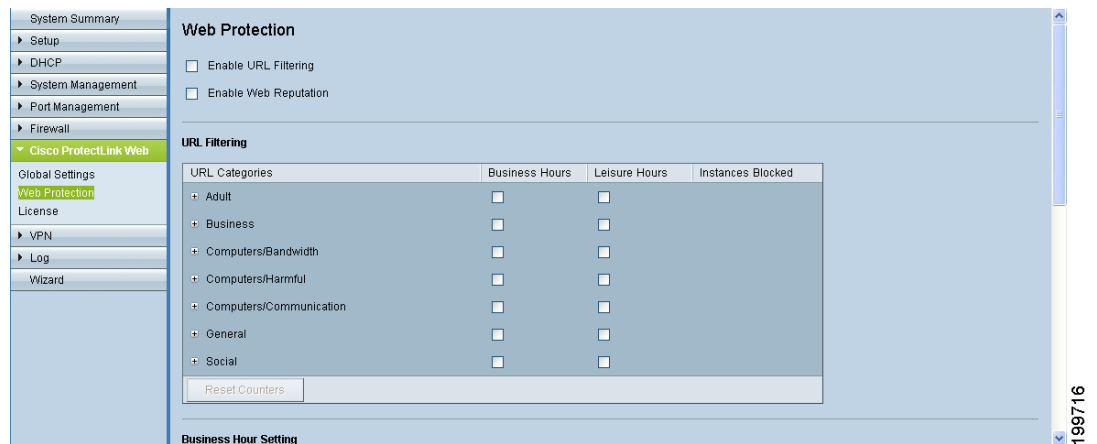
Check the **Enable Approved Client list** box to enable this feature. Then add up to 20 trusted clients (local IP addresses) that will always have access to the filtered URLs.

- **To add entries:** Enter IP addresses or ranges. To enter non-consecutive IP addresses, type a semi-colon between entries, such as *10.1.1.1;10.1.1.5*. To enter a range of IP addresses, type a hyphen between the first and last address in the range, such as *10.1.1.0-10.1.1.10*.
- **To delete an entry:** Click the **Delete** icon.

Enabling Web Protection for URL Filtering

Use the *Cisco ProtectLink Web > Web Protection* page to configure URL filtering and Web Reputation settings.

To open this page: Click **ProtectLink > Web Protection** in the navigation tree.



NOTE

- This page is available only if you activated your Cisco ProtectLink Web service. See [Getting Started with Cisco ProtectLink Web, page 113](#).
- Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Web Protection

- **Enable URL Filtering:** Check this box to block access to websites based on pre-defined categories. Uncheck the box to disable this service.
- **Enable Web Reputation:** Check this box to verify URL requests against the Cisco ProtectLink Web Security database. This service is recommended to block potentially malicious websites. Uncheck the box to disable this service.

URL Filtering

Select the categories and sub-categories for websites that you want to block during Business Hours and Leisure Hours.

| URL Filtering | | | |
|--|-------------------------------------|--------------------------|-------------------|
| URL Categories | Business Hours | Leisure Hours | Instances Blocked |
| + Adult | <input type="checkbox"/> | <input type="checkbox"/> | |
| + Business | <input type="checkbox"/> | <input type="checkbox"/> | |
| - Computers/Bandwidth | <input type="checkbox"/> | <input type="checkbox"/> | 0 |
| Internet Radio and TV | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 0 |
| Internet Telephony | <input type="checkbox"/> | <input type="checkbox"/> | |
| Photo Searches | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 0 |
| Personal Network Storage/File Download Servers | <input type="checkbox"/> | <input type="checkbox"/> | |
| Peer-to-Peer | <input type="checkbox"/> | <input type="checkbox"/> | |
| Streaming Media/MP3 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 0 |
| Ringtones/Mobile Phone Downloads | <input type="checkbox"/> | <input type="checkbox"/> | |

NOTE To define Business Hours and Leisure Hours, see the *Business Hour Setting* section. If you keep the default Business Hour settings, all days and all times are classified as Business Hours. You can ignore the Leisure Hours check boxes.

- To view sub-categories under a category, click the plus sign (+).
- To block access for all sub-categories within a category, check the box for the category. To disable filtering for a category, uncheck the box.
- To block access for individual sub-categories, check the individual boxes. To disable filtering for a sub-category, uncheck each box.
- **Instances Blocked:** For each filter that you enable, this column displays the number of times that someone has attempted to visit a blocked site.
- **Reset Counters:** The router counts the number of attempted visits to a restricted URL. To reset the counter to zero, click the button.

Business Hour Setting

Use the settings in this section to define Business Hours and Leisure Hours for URL Filtering.

NOTE If you keep the default Business Hour settings, all days and all times are classified as Business Hours. If you select specific days and times, the selected periods are Business Hours, and the unselected periods are Leisure Hours.

- **Business Days:** Check the box for each day when your business is open. Uncheck the box for each day when your business is closed. On the checked days, the Business Hours filters apply. On the unchecked days, the Leisure Hours filters apply.
- **Business Times:** To use the same settings all day, keep the default setting, **All day (24 hours)**. To specify the hours when your business is open, click **Specify business hours**. Check the **Morning** box and select the *From* and *To* times. Then check the **Afternoon** box and select the *From* and *To* times. During the selected periods, the Business Hours filters apply. During all other periods, the Leisure Hours filters apply.

Web Reputation

Select the appropriate security level:

- **High:** This option blocks a higher number of potentially malicious websites, but also has a higher incidence of false positives (legitimate sites that are classified as malicious).
- **Medium:** This option blocks most potentially malicious websites, and has a lower incidence of false positives (legitimate sites that are classified as malicious). **Medium** is the recommended setting.
- **Low:** This option blocks fewer potentially malicious websites, and therefore reduces the risk of false positives.

URL Overflow Control

Specify the behavior of this service during periods when there are more URL requests than the service can handle.

- **Temporarily block URL requests:** This setting is recommended. Select this option to hold back the overflow until the requests can be processed. This is the default setting.
- **Temporarily bypass URL verification for requested URLs:** Select this option to allow all overflow requests to go through without verification. This setting is not recommended.

Updating the ProtectLink License

Use the *Cisco ProtectLink Web > License* page to view your license information or to renew your license.

To open this page: Click **ProtectLink > License** in the navigation tree.

The screenshot shows the Cisco ProtectLink Web interface. On the left is a navigation tree with the following items: System Summary, Setup, DHCP, System Management, Port Management, Firewall, Cisco ProtectLink Web (expanded), Global Settings, Web Protection, License (selected), VPN, Log, and Wizard. The main content area is titled 'License' and contains a green checkmark icon followed by the text 'Cisco ProtectLink is active.'. Below this is a box with the text 'License information last updated on: 06/27/2010 22:32:50' and an 'Update' button. Underneath is a section titled 'License Information' with the following details: Status: Activated (with a link 'View detailed license online'), Platform: Gateway Service, and License expires on: 02/12/2011 00:00:00. A 'Renew' button is located at the bottom of this section.

NOTE This page is available only if you activated your Cisco ProtectLink Web service. See [Getting Started with Cisco ProtectLink Web, page 113](#).

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. Your web browser opens the *ProtectLink Product Detail* page. You can close that page when you finish reading the information.
- **Status:** The status of your license: *Activated* or *Expired*
- **Platform:** The platform type, Gateway Service.
- **License expires on:** The date and time your license when the license expires (one year after the service was activated)
- **Renew:** For information about renewing your license, click **Renew**. After you purchase an extension key, you can register it and activate your service.

VPN

Use the VPN module to configure a Virtual Private Network (VPN) to allow secure access to your site from other locations. Refer to these topics:

- [Introduction to VPNs, page 122](#)
- [Viewing the Summary Information for VPN, page 126](#)
- [Setting Up a Gateway to Gateway \(Site to Site\) VPN, page 130](#)
- [Setting Up a Remote Access Tunnel for VPN Clients \(Client To Gateway\), page 139](#)
- [Managing VPN Users and Certificates, page 147](#)
- [Setting Up VPN Passthrough, page 149](#)
- [Setting Up PPTP Server, page 150](#)

Introduction to VPNs

A VPN is a connection between two endpoints in different networks to allow private data to be sent securely over a shared or public network, such as the Internet. This tunnel establishes a private network that can send data securely between these two locations or networks. A VPN tunnel uses industry-standard encryption and authentication techniques to secure the data sent between the two networks. It can be used to create secure networks linking a central office with remote offices, telecommuters, and/or professionals on the road.

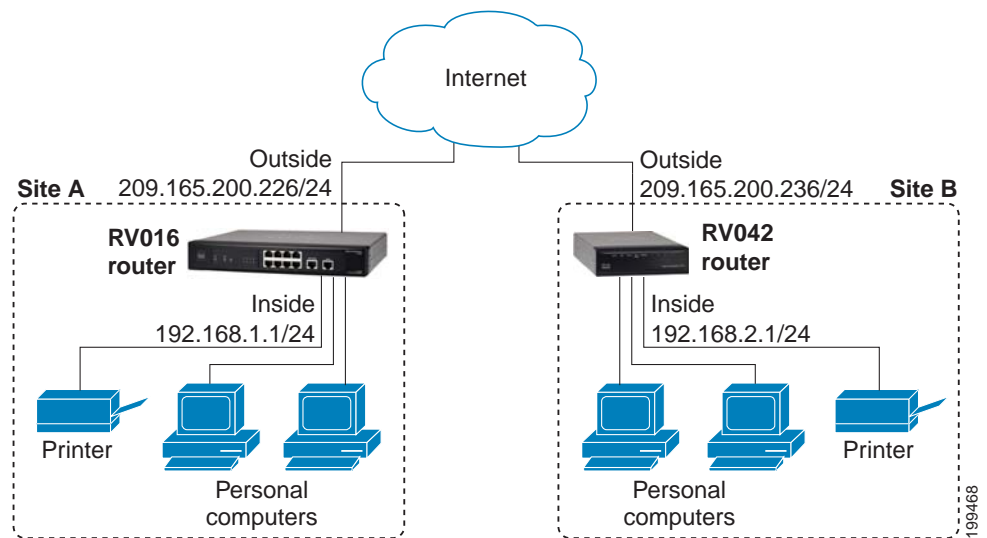
There are several ways to create a VPN connection:

- [Site to Site VPN \(Gateway To Gateway\), page 123](#)
- [Remote Access \(Client To Gateway\), page 123](#)
- [Remote Access with Cisco QuickVPN, page 125](#)
- [Remote Access with PPTP, page 125](#)

Site to Site VPN (Gateway To Gateway)

In a site-to-site or gateway-to-gateway VPN, a VPN router at one office connects to a VPN router at a remotely located office. Client devices can access network resources as if they were all at the same site. This model can be used for multiple users at a remote office.

In the following example, the main office (Site A) and a remote office (Site B) are connected by a VPN tunnel. Users at both sites have access to the network resources at both sites.



Configuration tasks:

Use the *VPN > Gateway to Gateway* page to configure the VPN tunnel. For instructions, see [Setting Up a Gateway to Gateway \(Site to Site\) VPN, page 130](#). For more details and examples, see [Appendix D, “Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers.”](#)

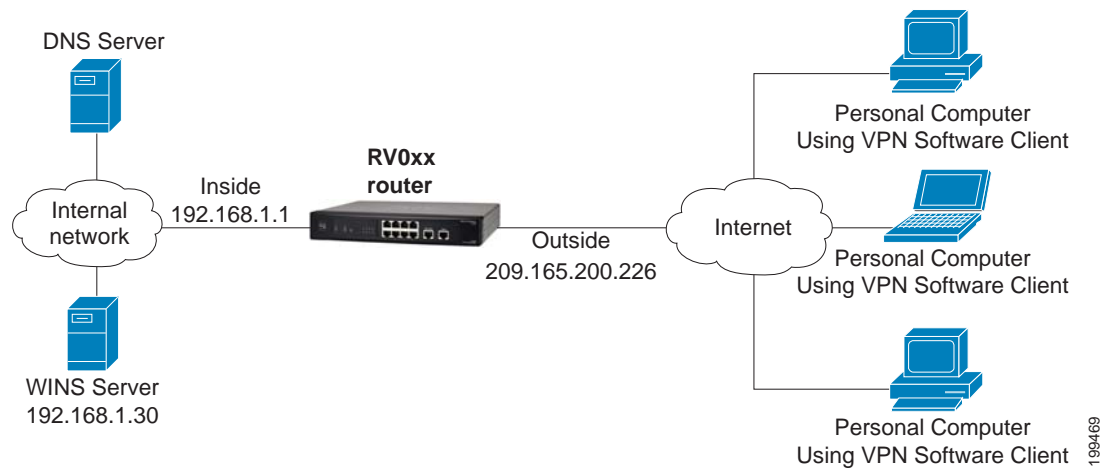
Remote Access (Client To Gateway)

In a remote access or client-to-gateway VPN, a computer with VPN client software connects to a VPN router. For this scenario, you can install third-party VPN client software on the users' computers. Alternatively, a VPN tunnel can be accessed from any computer with the built-in IPsec Security Manager (Windows 2000, Windows XP, and Windows 7).

You will need to configure this router with the specific IPsec policies required for the IPsec client. You also will need to install and configure the IPsec client software on the users' computers.

NOTE Consider two other remote access options: [Remote Access with Cisco QuickVPN, page 125](#) and [Remote Access with PPTP, page 125](#).

The following is an example of a client-to-gateway VPN. A business traveler connects to the Internet from her hotel room. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software and connects to the VPN router at the central office. Using the VPN, she now has a secure connection to the central office's network, as if she were physically connected.



Configuration tasks:

1. Use the *VPN > Client to Gateway* page to configure the VPN tunnel with the settings required by the third-party client, such as TheGreenbow. For instructions, see [Setting Up a Remote Access Tunnel for VPN Clients \(Client To Gateway\), page 139](#).
2. Install the client software on the users' computers.

Remote Access with Cisco QuickVPN

Users with Cisco QuickVPN software can establish a VPN tunnel to your network. Use this option if you want to simplify the VPN setup process. You do not have to configure VPN policies. Remote users can connect securely with the Cisco QuickVPN client and an Internet connection. For information about the benefits and limitations, see “Easy and Secure Access with Cisco QuickVPN” at http://www.cisco.com/en/US/docs/routers/csbr/app_notes/QuickVPN_an_OL-25680.pdf

Configuration Tasks:

1. Use the *VPN Client Access* page to add the usernames and passwords.
2. Optionally, use the *VPN > VPN Client Access* page to generate certificates to install on the users computers. For more information, see [Certificate Management, page 148](#).
3. Install Cisco QuickVPN on the users' computers. To get the software, go to www.cisco.com/go/software. Enter the router's model number in the search box and then click **Find**. In the list of links, click **Quick Virtual Private Network (QVPN) Utility**. After downloading the software on the computer, double-click **Setup.exe** to start the installation.
4. If you generated certificates, copy the certificate to the directory where Cisco QuickVPN is installed, typically C:\Program Files\Cisco Small Business\QuickVPN client.

Remote Access with PPTP

A remote user with a Microsoft computer can establish a VPN tunnel by connecting to a PPTP server at your site. Use this option to simplify VPN setup. You do not have to configure VPN policies on the router, and there is no need to install a VPN client on the users' computers. However, be aware that security vulnerabilities have been found in this protocol.

Configuration Tasks:

1. Use the *VPN > PPTP Server* page to enable PPTP server, set the IP address range for clients, and enter the usernames and passwords.
2. Distribute the user names and passwords to the users.

Viewing the Summary Information for VPN

The *VPN > Summary* page displays general information about the router's VPN tunnel settings. The router supports up to 100 tunnels.

NOTE If the PPTP Server is enabled, summary information about PPTP clients appears on the *VPN > PPTP Server* page. For more information, see [Setting Up PPTP Server, page 150](#).

To open this page: Click **VPN > Summary** in the navigation tree.

Summary

0 Tunnel(s) Used 100 Tunnel(s) Available [Details](#)

Tunnel Status

2 Tunnel(s) Enabled 2 Tunnel(s) Defined

Items 1-2 of 2 Rows per page: 5

| No. | Name | Status | Phase2 Enc/Auth/Grp | Local Group | Remote Group | Remote Gateway | Tunnel Test | Config. |
|-----|---------|------------------------|---------------------|------------------------------|----------------------------|----------------|-------------------------|---------|
| 1 | toRV016 | waiting for connection | DES/MD5/1 | 192.168.1.0 255.255.255.0 | 12.2.2.0 255.255.255.0 | 11.0.0.100 | Connect | |
| 2 | toRV042 | waiting for connection | DES/MD5/1 | 192.168.1.0 255.255.255.0 | 13.13.1.0 255.255.255.0 | 11.0.0.103 | Connect | |

[Add](#) [Refresh](#) Page 1 of 1

Group VPN Status

| Group Name | Connected Tunnels | Phase2 Enc/Auth/Grp | Local Group | Remote Client | Remote Client Status | Tunnel Test | Config. |
|------------|-------------------|---------------------|------------------------------|------------------|-----------------------------|-------------|---------|
| Group1 | 0 | DES/MD5/1 | 192.168.1.0 255.255.255.0 | vpnclient@mic... | Detail List | N/A | |

Summary

- **Tunnel(s) Used:** The number of VPN tunnels in use.
- **Tunnels Available:** The number of available VPN tunnels.
- **Detail:** Click **Detail** for more information. Click **Refresh** to update the data, or click **Close** to return to the *VPN > Summary* page. For each VPN tunnel, the No., Name, Status, Phase 2 Enc/Auth/Grp, Local Group, Remote Group, and Remote Gateway will be displayed.

Tunnel Status

Above the table, the following information appears:

- **Tunnel(s) Enabled:** The number of tunnels that are enabled.
- **Tunnel(s) Defined:** The number of tunnels that are defined, including enabled and disabled tunnels.

The table displays the following information about each tunnel:

- **No.:** The identification number of the VPN tunnel.
- **Name:** A descriptive name for the VPN tunnel.
- **Status:** The status of the VPN tunnel: *Connected* or *Waiting for Connection*.
- **Phase2 Enc/Auth/Grp:** The Phase 2 Encryption type (NULL/DES/3DES/AES-128/AES-192/AES-256), Authentication method (NULL/MD5/SHA1), and DH Group number (1/2/5) that you chose in the IPsec Setup section.

If you selected Manual for the Keying Mode in the IPsec section, then only the Encryption type and Authentication method appear.

- **Local Group:** The IP address and subnet mask of the Local Group.
- **Remote Group:** The IP address and subnet mask of the Remote Group.
- **Remote Gateway:** The IP address of the Remote Gateway.
- **Tunnel Test:** Click **Connect** to verify the status of the VPN tunnel. The test result will be updated in the *Status* column. If the tunnel is connected, a Disconnect button will be available so you can end the connection.
- **Configure:** Click the **Edit** icon to open a new page where you can change the tunnel's settings. To delete tunnel settings, select a tunnel, and then click the **Delete** icon
- **Tunnel Enabled:** The number of enabled VPN tunnels.
- **Tunnel Defined:** The number of defined VPN tunnels.
- **Add:** Click this button to add a tunnel. Then choose one of the following options:
 - To create a tunnel for a remote site with a VPN router, choose **Gateway to Gateway**. The *Gateway to Gateway* page appears. See [Setting Up a Gateway to Gateway \(Site to Site\) VPN, page 130](#).

- To create a tunnel for a remote worker using VPN client software, choose **Client to Gateway**. The *Client to Gateway* page appears. See **Setting Up a Remote Access Tunnel for VPN Clients (Client To Gateway)**, page 139.
- **Navigation controls:** If you have numerous rules, you can adjust the display. Use the *Rows per page list* at the top right corner of the table to choose the number of rules to display on each page. Use the *Page list* below the table to choose a particular page. Use the navigation buttons to view the first page, previous page, next page, or final page. Some buttons may be unavailable, depending on the number of pages and the current selection.

GroupVPN Status

If you enable the GroupVPN setting for any of your Client to Gateway tunnels, the status information appears in this table.

- **Group Name:** A descriptive name for the group VPN.
- **Connected Tunnels:** The number of users logged into the group VPN.
- **Phase2 Enc/Auth/Grp:** The Phase 2 Encryption type (NULL/DES/3DES/AES-128/AES-192/AES-256), Authentication method (NULL/MD5/SHA1), and DH Group number (1/2/5), as configured in the *IPSec Setup* section.
- **Local Group:** The IP address and subnet mask of the Local Group.
- **Remote Client:** The remote clients in the group VPN.
- **Remote Clients Status:** The status of the remote clients: *Online* or *Offline*. Click **Detail List** to open the *Group List* window. This window displays the Group Name, IP address, and Connection Time. You can click **Refresh** to update the data, or click **Close** to close the pop-up window and return to the *VPN > Summary* page.
- **Tunnel Test:** Click **Connect** to verify the status of the group VPN. The test result will be updated in the *Status* column. If the group VPN is connected, a **Disconnect** button will be available so you can end the connection.
- **Configure:** Click the **Edit** icon to open a new page where you can change the tunnel's settings. To delete tunnel settings, select a tunnel, and then click the **Delete** icon.
- **Navigation controls:** If you have numerous rules, you can adjust the display. Use the *Rows per page list* at the top right corner of the table to choose the number of rules to display on each page. Use the *Page list* below the table to choose a particular page. Use the navigation buttons to view the first

page, previous page, next page, or final page. Some buttons may be unavailable, depending on the number of pages and the current selection.

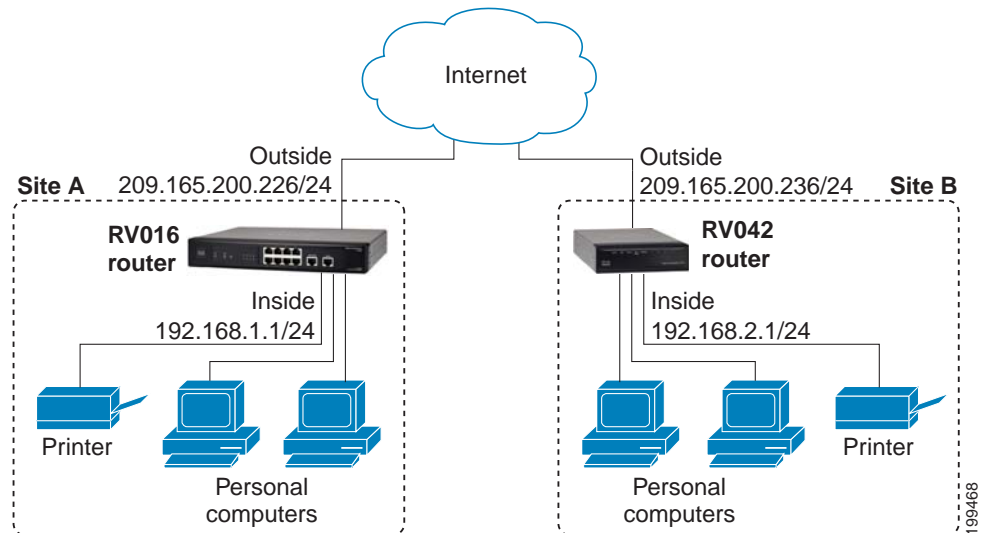
VPN Clients Status

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

- **No.:** The ID number of the VPN client.
- **Username:** The name of the VPN client.
- **Status:** The status of the VPN client connection.
- **Start Time:** The time when the VPN client established its VPN connection to the router.
- **End Time:** The time when the VPN client ended its VPN connection to the router.
- **Duration:** The period of time that the VPN connection has been active.
- **Disconnect:** Click this button to disconnect any VPN client.
- **Navigation controls:** If you have numerous rules, you can adjust the display. Use the *Rows per page list* at the top right corner of the table to choose the number of rules to display on each page. Use the *Page list* below the table to choose a particular page. Use the navigation buttons to view the first page, previous page, next page, or final page. Some buttons may be unavailable, depending on the number of pages and the current selection.

Setting Up a Gateway to Gateway (Site to Site) VPN

Use the *VPN > Gateway to Gateway* page to create a new tunnel between two VPN devices, such as a Cisco RV082 router at your office and a Cisco RV042 router at a remote office.



You will enter the settings for the local group and the remote group, and you will enter the corresponding settings (reversing “local” and “remote”) when configuring the other router. A successful connection requires that at least one router is identifiable by a static IP address or a Dynamic DNS hostname. Alternatively, if one router has only a dynamic IP address, you can use any email address as authentication to establish the connection.

NOTE The two ends of the tunnel cannot be on the same subnet. For example, if the Site A LAN uses the 192.168.1.x subnet, Site B could use 192.168.2.x.

You will enter corresponding settings (reversing “local” and “remote”) when configuring the two routers. When you configure this router (Router A), enter its settings in the *Local Group Setup* section, and enter the settings for the other router (Router B) in the *Remote Group Setup* section. When you configure the other router (Router B), enter its settings in the *Local Group Setup* section, and enter the Router A settings in the *Remote Group Setup* section. For more details and examples, see [Appendix D, “Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers.”](#)

To open this page: Click **VPN > Gateway to Gateway** in the navigation tree. Alternatively, you can click the **Add Tunnel** button on the *VPN > Summary* page, in the *Tunnel Status* section. Then choose **Gateway to Gateway**.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Add a New Tunnel

- **Tunnel No:** The ID number, which is automatically generated
- **Tunnel Name:** Enter a name for this VPN tunnel, such as Los Angeles Office, Chicago Branch, or New York Division. This description is for your reference. It does not have to match the name used at the other end of the tunnel.
- **Interface:** Select the WAN port to use for this tunnel.
- **Enable:** Check this box to enable the VPN tunnel, or uncheck it to disable the tunnel. By default, the tunnel is enabled.

Local Group Setup and Remote Group Setup

Enter the settings described below. The Local settings are for this router, and the Remote settings are for the router on the other end of the tunnel. Mirror these settings when configuring the VPN tunnel on the other router.

- **Local/Remote Security Gateway Type:** Specify the method for identifying the router to establish the VPN tunnel. The Local Security Gateway is on this router; the Remote Security Gateway is on the other router. At least one of the routers must have either a static IP address or a dynamic DNS hostname to make a connection.

- **IP Only:** Choose this option if this router has a static WAN IP address. The WAN IP address appears automatically.

For the *Remote Security Gateway Type*, an extra field appears. If you know the IP address of the remote VPN router, choose **IP Address**, and then enter the address. If you do not know the IP address of the remote VPN router, select **IP by DNS Resolved**, and then enter the real domain name of the router on the Internet. Cisco RV082 will get the IP address of remote VPN device by DNS Resolved, and IP address of remote VPN device will be displayed in the VPN Status section of the *VPN > Summary* page.

- **IP + Domain Name (FQDN) Authentication:** Choose this option if this router has a static IP address and a registered domain name, such as *MyServer.MyDomain.com*. Also enter the **Domain Name** to use for authentication. The domain name can be used only for one tunnel connection.

For the *Remote Security Gateway Type*, an extra field appears. If you know the IP address of the remote VPN router, choose **IP Address**, and then enter the address. If you do not know the IP address of the remote VPN router, select **IP by DNS Resolved**, and then enter the real domain name of the router on the Internet. Cisco RV082 will get the IP address of remote VPN device by DNS Resolved, and the IP address of remote VPN device will be displayed in the VPN Status section of the *VPN > Summary* page.

- **IP + E-mail Addr.(USER FQDN) Authentication:** Choose this option if this router has a static IP address and you want to use an email address for authentication. The current WAN IP address appears automatically. Enter any **Email Address** to use for authentication.

For the *Remote Security Gateway Type*, an extra field appears. If you know the IP address of the remote VPN router, choose **IP Address**, and then enter the address. If you do not know the IP address of the remote VPN router, select **IP by DNS Resolved**, and then enter the real domain name of the router on the Internet. Cisco RV082 will get the IP address of remote VPN device by DNS Resolved, and IP address of remote VPN device will be displayed in the VPN Status section of the *VPN > Summary* page.

- **Dynamic IP + Domain Name (FQDN) Authentication:** Choose this option if this router has a dynamic IP address and a registered Dynamic DNS hostname (available from providers such as DynDNS.com). Enter a **Domain Name** to use for authentication. The domain name can be used only for one tunnel connection.

- **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** Choose this option if this router has a dynamic IP address and does not have a Dynamic DNS hostname. Enter any **Email Address** to use for authentication.

If both routers have dynamic IP addresses (as with PPPoE connections), do not choose Dynamic IP + Email Addr. for both gateways. For the remote gateway, choose **IP Address** and **IP Address by DNS Resolved**.
- **Local/Remote Security Group Type:** Specify the LAN resources that can use this tunnel. The Local Security Group is for this router's LAN resources; the Remote Security Group is for the other router's LAN resources.
 - **IP Address:** Choose this option to specify one device that can use this tunnel. Then enter the IP address of the device.
 - **Subnet:** Choose this option (the default option) to allow all devices on a subnet to use the VPN tunnel. Then enter the subnetwork IP address and mask.
 - **IP Range:** Choose this option to specify a range of devices that can use the VPN tunnel. Then identify the range of IP addresses by entering the first address in the **Begin IP** field and the final address in the **End IP** field.

IPSec Setup

Enter the Internet Protocol Security settings for this tunnel.

IMPORTANT: In order for any encryption to occur, the two ends of a VPN tunnel must agree on the methods of encryption, decryption, and authentication. Enter exactly the same settings on both routers.

- **Keying Mode:** Choose one of the following key management methods:
 - **Manual:** Choose this option if you want to generate the key yourself and you do not want to enable key negotiation. Manual key management is used in small static environments or for troubleshooting purposes. Enter the required settings. For information, see [Required fields for Manual mode, page 134](#).
 - **IKE with Preshared Key:** Choose this option to use the Internet Key Exchange protocol to set up a Security Association (SA) for your tunnel. IKE uses a preshared key to authenticate the remote IKE peer. This setting is recommended and is selected by default. Enter the required settings. For more information, see [Required fields for IKE with](#)

Preshared Key, page 135 and Advanced settings for IKE with Preshared Key, page 136.

- **Required fields for Manual mode**

Enter the settings for manual mode. Be sure to enter the same settings when configuring other router for this tunnel. The Incoming / Outgoing SPI settings must be mirrored on the other router.

- **Incoming / Outgoing SPI:** The Security Parameter Index is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to select the security association, under which a packet should be processed. You can enter hexadecimal values from 100~ffffff. Each tunnel must have a unique Incoming SPI and Outgoing SPI. No two tunnels share the same SPI. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.
- **Encryption:** Select a method of encryption: DES or 3DES. This setting determines the length of the key used to encrypt or decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure.
- **Authentication:** Select a method of authentication: MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method.
- **Encryption Key:** Enter a key to use to encrypt and decrypt IP traffic. If you selected DES encryption, enter 16 hexadecimal values. If you selected 3DES encryption enter 40 hexadecimal values. If you do not enter enough hexadecimal values, then zeroes will be appended to the key to meet the required length.
- **Authentication Key:** Enter a key to use to authenticate IP traffic. If you selected MD5 authentication, enter 32 hexadecimal values. If you selected SHA1, enter 40 hexadecimal values. If you do not enter enough hexadecimal values, then zeroes will be appended to the key to meet the required length.

- **Required fields for IKE with Preshared Key**

Enter the settings for Phase 1 and Phase 2. Phase 1 establishes the preshared keys to create a secure authenticated communication channel. In Phase 2, the IKE peers use the secure channel to negotiate Security Associations on behalf of other services such as IPsec. Be sure to enter the same settings when configuring other router for this tunnel.

- **Phase 1 / Phase 2 DH Group:** DH (Diffie-Hellman) is a key exchange protocol. There are three groups of different prime key lengths: Group 1 - 768 bits, Group 2 - 1,024 bits, and Group 5 - 1,536 bits. For faster speed but lower security, choose **Group 1**. For slower speed but higher security, choose **Group 5**. Group 1 is selected by default.
- **Phase 1 / Phase 2 Encryption:** Select a method of encryption for this phase: DES, 3DES, AES-128, AES-192, or AES-256. The method determines the length of the key used to encrypt or decrypt ESP packets. AES-256 is recommended because it is more secure.
- **Phase 1 / Phase 2 Authentication:** Select a method of authentication for this phase: MD5 or SHA1. The authentication method determines how the ESP (Encapsulating Security Payload Protocol) header packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method.
- **Phase 1 / Phase 2 SA Life Time:** Configure the length of time a VPN tunnel is active in this phase. The default value for Phase 1 is 28800 seconds. The default value for Phase 2 is 3600 seconds.
- **Perfect Forward Secrecy:** If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPsec keys. Check the box to enable this feature, or uncheck the box to disable this feature. This feature is recommended.
- **Preshared Key:** Enter a pre-shared key to use to authenticate the remote IKE peer. You can enter up to 30 keyboard characters and hexadecimal values, such as My_@123 or 4d795f40313233. Both ends of the VPN tunnel must use the same Preshared Key. It is strongly recommended that you change the Preshared Key periodically to maximize VPN security.

- **Minimum Preshared Key Complexity:** Check the **Enable** box if you want to enable the Preshared Key Strength Meter.
- **Preshared Key Strength Meter:** If you enable Minimum Preshared Key Complexity, this meter indicates the preshared key strength. As you enter a preshared key, colored bars appear. The scale goes from red (weak) to yellow (acceptable) to green (strong).

TIP: Enter a complex preshared key that includes more than eight characters, upper- and lowercase letters, numbers, and symbols such as `-*^+=`.

- **Advanced settings for IKE with Preshared Key**

When the Keying Mode is set to IKE with Preshared Key mode, advanced settings are available. For most users, the basic settings should suffice; advanced users can click **Advanced +** to view the advanced settings. To hide these settings, click **Advanced -**.

Important: If you change the Advanced settings on one router, be sure to enter the same settings on the other router.

- **Aggressive Mode:** Two modes of IKE SA negotiation are possible: Main Mode and Aggressive Mode. If network security is preferred, Main Mode is recommended. If network speed is preferred, Aggressive Mode is recommended. You can adjust this setting if the Remote Security Gateway Type is *IP Only* or one of the *IP +* types. Check this box to enable Aggressive Mode, or uncheck the box to disable Aggressive Mode and use Main Mode.

NOTE: If the Remote Security Gateway Type is one of the *Dynamic IP* types, Aggressive Mode is required. The box is checked automatically, and this setting cannot be changed.

- **Compress (Support IP Payload Compression Protocol (IP Comp)):** IP Comp is a protocol that reduces the size of IP datagrams. Check the box to enable the router to propose compression when it initiates a connection. If the responder rejects this proposal, then the router will not implement compression. When the router works as a responder, it will always accept compression, even if compression is not enabled. If you enable this feature for this router, also enable it on the router at the other end of the tunnel.
- **Keep-Alive:** This feature enables the router to attempt to automatically re-establish the VPN connection if it is dropped. Check the box to enable this feature, or uncheck the box to disable it.

- **AH Hash Algorithm:** The AH (Authentication Header) protocol describes the packet format and default standards for packet structure. With the use of AH as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet. Check the box to use this feature. Then select an authentication method: MD5 or SHA1. MD5 produces a 128-bit digest to authenticate packet data. SHA1 produces a 160-bit digest to authenticate packet data. Both sides of the tunnel should use the same algorithm.
- **NetBIOS Broadcast:** NetBIOS broadcast messages are used for name resolution in Windows networking, to identify resources such as computers, printers, and file servers. These messages are used by some software applications and Windows features such as Network Neighborhood. LAN broadcast traffic is typically not forwarded over a VPN tunnel. However, you can check this box to allow NetBIOS broadcasts from one end of the tunnel to be rebroadcast to the other end.
- **NAT Traversal:** Network Address Translation (NAT) enables users with private LAN addresses to access Internet resources by using a publicly routable IP address as the source address. However, for inbound traffic, the NAT gateway has no automatic method of translating the public IP address to a particular destination on the private LAN. This issue prevents successful IPsec exchanges. If your VPN router is behind a NAT gateway, check this box to enable NAT traversal. Uncheck the box to disable this feature. The same setting must be used on both ends of the tunnel.
- **Dead Peer Detection (DPD):** Check the box to enable the router to send periodic HELLO/ACK messages to check the status of the VPN tunnel. This feature can be used only when it is enabled on both ends of the VPN tunnel. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent).

Tunnel Backup: When DPD determines that the remote peer is unavailable, this feature enables the router to re-establish the VPN tunnel by using either an alternative IP address for the remote peer or an alternative local WAN interface. Check the box to enable this feature. Then enter the settings described below. This feature is available only if Dead Peer Detection is enabled.

Remote Backup IP Address: Specify an alternative IP address for the remote peer, or re-enter the WAN IP address that was already set for the remote gateway.

Local Interface: Choose the WAN interface to use to reestablish the connection.

VPN Tunnel Backup Idle Time: This setting is used when the router boots up. If the primary tunnel is not connected within the specified period, then the backup tunnel is used. The default idle time is 30 seconds.

- **Split DNS:** Split DNS enables the router to send some DNS requests to one DNS server and other DNS requests to another DNS server, based on specified domain names. When the router receives an address resolution request from client, it inspects the domain name. If it matches one of the domain names in the Split DNS settings, then it passes the request to the specified DNS server. Otherwise, the request is passed to the DNS server that is specified in the WAN interface settings. Check the box to enable this feature, or uncheck the box to disable it.

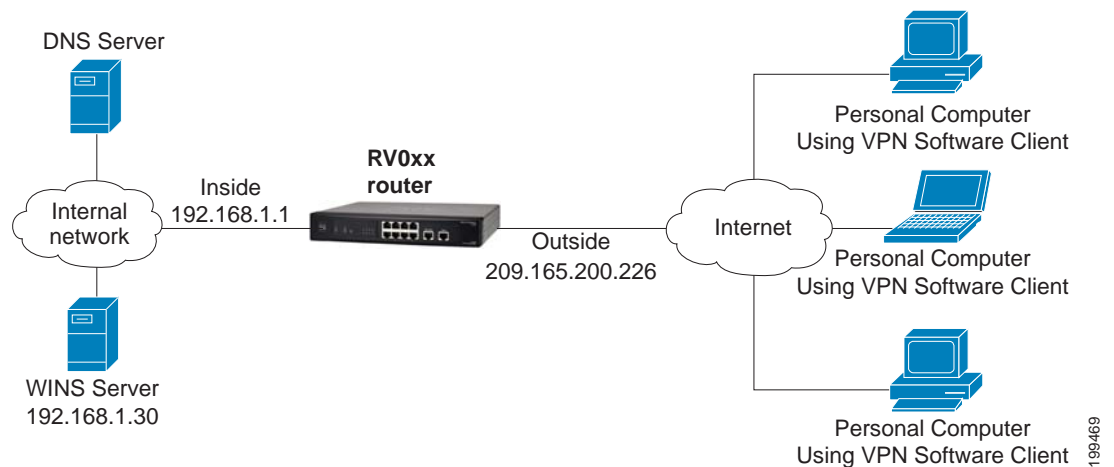
DNS1: Specify the IP address of the DNS server to use for the specified domains. Optionally, specify a secondary DNS server in the **DNS2** field.

Domain Name 1 - Domain Name 4: Specify the domain names for these DNS servers. Requests for these domains will be passed to the specified DNS server(s).

Setting Up a Remote Access Tunnel for VPN Clients (Client To Gateway)

Use *VPN > Client To Gateway* page to create a new VPN tunnel to allow teleworkers and business travelers to access to your network by using third-party VPN client software, such as TheGreenBow.

NOTE For information about third-party clients, see application notes by visiting www.cisco.com/go/smallbizrouters (see the *Technical Documentation* section).



To open this page: Click **VPN > Client to Gateway** in the navigation tree. Alternatively, you can click the **Add Tunnel** button on the *VPN > Summary* page, in the *Tunnel Status* section. Then choose **Client to Gateway**.

The screenshot shows the 'Client To Gateway' configuration page. The left navigation pane is expanded to 'VPN > Client To Gateway'. The main content area is titled 'Client To Gateway' and contains the following sections:

- Add a New Tunnel:**
 - Tunnel No.: 1
 - Tunnel Name: [Text Field]
 - Interface: WAN1 (Dropdown)
 - Enable:
- Local Group Setup:**
 - Local Security Gateway Type: IP Only (Dropdown)
 - IP Address: 10.0.0.102
 - Local Security Group Type: Subnet (Dropdown)
 - IP Address: 192.168.1.0
 - Subnet Mask: 255.255.255.0
- Remote Client Setup:** (Section header, content not fully visible)

Add a New Tunnel

You can configure a VPN tunnel for one remote user or configure a group VPN for multiple remote users. You have two options:

- **Tunnel:** Choose this option to create a tunnel for a single remote user. The tunnel number is automatically generated and appear in the *Tunnel No* field.
- **Group VPN:** Choose this option to create a tunnel for a group of users. Group VPN facilitates setup and eliminates the need to configure individual users. All of the remote users can use the same Preshared Key to connect to RV0xx, up to the maximum number of supported tunnels. The router supports up to two VPN groups. The group number is automatically generated and appears in the *Group No* field.

Enter the following information:

- **Tunnel Name:** Enter a name to describe the tunnel. For a single user, you could enter the user's name or location. For a group VPN, you could identify the group's business role or location. This description is for your reference and does not have to match the name used at the other end of the tunnel.
- **Interface:** Select the appropriate WAN port.
- **Enable:** Check this box to enable a group VPN.

Local Group Setup

Enter the following information about this router.

- **Local Security Gateway Type:** Specify the method for identifying this router to establish the VPN tunnel.
 - **IP Only:** Choose this option if this router has a static WAN IP address. The WAN IP address appears automatically.
 - **IP + Domain Name (FQDN) Authentication:** Choose this option if this router has a static IP address and a registered domain name. Also enter any **Domain Name** to use for authentication. The domain name can only be used only for one tunnel connection.
 - **IP + E-mail Addr.(USER FQDN) Authentication:** Choose this option if this router has a static IP address and you want to use an email address for authentication. The current WAN IP address appears automatically. Enter any **Email Address** to use for authentication.
 - **Dynamic IP + Domain Name (FQDN) Authentication:** Choose this option if this router has a dynamic IP address and a registered Dynamic

DNS hostname (available from providers such as DynDNS.com). Enter a **Domain Name** to use for authentication. The domain name can be used only for one tunnel connection.

- **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** Choose this option if this router has a dynamic IP address and does not have a Dynamic DNS hostname. Enter any **Email Address** to use for authentication.
- **Local Security Group Type:** Specify the LAN resources that can access this tunnel.
 - **IP Address:** Choose this option to allow only one LAN device to access the VPN tunnel. Then enter the IP address of the computer. Only this device can use this VPN tunnel.
 - **Subnet:** Choose this option (the default option) to allow all devices on a subnet to access the VPN tunnel. Then enter the subnetwork IP address and mask.
 - **IP Range:** Choose this option to allow a range of devices to access the VPN tunnel. Then identify the range of IP addresses by entering the first address in the **Begin IP** field and the final address in the **End IP** field.
- **Domain Name:** If you chose to use domain name authentication, enter the domain name.
- **Email:** If you chose to use email authentication, enter the email address.

Remote Client Setup for Single User (“Tunnel” Type)

Specify the method for identifying the client to establish the VPN tunnel. The following options are available for a Single User, or “Tunnel” type, VPN.

- **IP Only:** Choose this option if the remote VPN client has a static WAN IP address. If you know the IP address of the client, choose **IP Address**, and then enter the address. If you do not know the IP address of the client, select **IP by DNS Resolved**, and then enter the real domain name of the client on the Internet. The router will get the IP address of the remote VPN client by DNS Resolved, and the IP address of the remote VPN client will be displayed in the VPN Status section of the *Summary* page.
- **IP + Domain Name (FQDN) Authentication:** Choose this option if this client has a static IP address and a registered domain name. Also enter a **Domain Name** to use for authentication. The domain name can only be used only for one tunnel connection.

If you know the IP address of the remote VPN client, choose **IP Address**, and then enter the address. If you do not know the IP address of the remote VPN client, select **IP by DNS Resolved**, and then enter the real domain name of the client on the Internet. The router will get the IP address of remote VPN client by DNS Resolved, and the IP address of remote VPN client will be displayed in the VPN Status section of the *Summary* page.

- **IP + Email Address (USER FQDN) Authentication:** Choose this option if this client has a static IP address and you want to use any email address for authentication. The current WAN IP address appears automatically. Enter any **Email Address** to use for authentication.

If you know the IP address of the remote VPN client, choose **IP Address**, and then enter the address. If you do not know the IP address of the remote VPN client, select **IP by DNS Resolved**, and then enter the real domain name of the client on the Internet. Cisco RV082 will get the IP address of remote VPN client by DNS Resolved, and IP address of remote VPN device will be displayed in the VPN Status section of the *Summary* page.

- **Dynamic IP + Domain Name (FQDN) Authentication:** Choose this option if this client has a dynamic IP address and a registered Dynamic DNS hostname (available from providers such as DynDNS.com). Enter the **Domain Name** to use for authentication. The domain name can be used only for one tunnel connection.
- **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** Choose this option if this client has a dynamic IP address and does not have a Dynamic DNS hostname. Enter any **Email Address** to use for authentication.

Remote Client Setup for a Group (“Group VPN” Type)

Specify the method for identifying the clients to establish the VPN tunnel. The following options are available for a Group VPN.

- **Domain Name (FQDN) Authentication:** Choose this option to identify the client by a registered domain name. Also enter a **Domain Name** to use for authentication. The domain name can only be used only for one tunnel connection.
- **Email Address (USER FQDN) Authentication:** Choose this option to identify the client by an email address for authentication. Enter the address in the fields provided.
- **Microsoft XP/2000 VPN Client:** Choose this option if the client software is the built-in Microsoft XP/2000 VPN Client.

IPSec Setup

Enter the Internet Protocol Security settings for this tunnel.

IMPORTANT: In order for any encryption to occur, the two ends of a VPN tunnel must agree on the methods of encryption, decryption, and authentication.

- **Keying Mode:** Choose one of the following key management methods:
 - **Manual:** Choose this option if you want to generate the key yourself and you do not want to enable key negotiation. Manual key management is used in small static environments or for troubleshooting purposes. Enter the required settings. For information, see [Required fields for Manual mode, page 143](#).
 - **IKE with Preshared Key:** Choose this option to use the Internet Key Exchange protocol to set up a Security Association (SA) for your tunnel. IKE uses a preshared key to authenticate the remote IKE peer. This setting is recommended and is selected by default. Enter the required settings. For more information, see [Required fields for IKE with Preshared Key, page 144](#) and [Advanced settings for IKE with Preshared Key, page 145](#).

- **Required fields for Manual mode**

Enter the settings for manual mode.

- **Incoming / Outgoing SPI:** The Security Parameter Index is carried in the ESP (Encapsulating Security Payload Protocol) header and enables the receiver and sender to select the security association, under which a packet should be processed. You can enter hexadecimal values from 100~ffffff. Each tunnel must have a unique Incoming SPI and Outgoing SPI. No two tunnels share the same SPI. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.
- **Encryption:** Select a method of encryption: DES or 3DES. This setting determines the length of the key used to encrypt or decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure.
- **Authentication:** Select a method of authentication: MD5 or SHA1. The authentication method determines how the ESP packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method.

- **Encryption Key:** Enter a key to use to encrypt and decrypt IP traffic. If you selected DES encryption, enter 16 hexadecimal values. If you selected 3DES encryption enter 40 hexadecimal values. If you do not enter enough hexadecimal values, then zeroes will be appended to the key to meet the required length.
- **Authentication Key:** Enter a key to use to authenticate IP traffic. If you selected MD5 authentication, enter 32 hexadecimal values. If you selected SHA1, enter 40 hexadecimal values. If you do not enter enough hexadecimal values, then zeroes will be appended to the key to meet the required length.

- **Required fields for IKE with Preshared Key**

Enter the settings for Phase 1 and Phase 2. Phase 1 establishes the preshared keys to create a secure authenticated communication channel. In Phase 2, the IKE peers use the secure channel to negotiate Security Associations on behalf of other services such as IPsec.

- **Phase 1 / Phase 2 DH Group:** DH (Diffie-Hellman) is a key exchange protocol. There are three groups of different prime key lengths: Group 1 - 768 bits, Group 2 - 1,024 bits, and Group 5 - 1,536 bits. For faster speed but lower security, choose **Group 1**. For slower speed but higher security, choose **Group 5**. Group 1 is selected by default.
- **Phase 1 / Phase 2 Encryption:** Select a method of encryption for this phase: DES, 3DES, AES-128, AES-192, or AES-256. The method determines the length of the key used to encrypt or decrypt ESP packets. AES-256 is recommended because it is more secure.
- **Phase 1 / Phase 2 Authentication:** Select a method of authentication for this phase: MD5 or SHA1. The authentication method determines how the ESP (Encapsulating Security Payload Protocol) header packets are validated. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA1 is a one-way hashing algorithm that produces a 160-bit digest. SHA1 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method.
- **Phase 1 / Phase 2 SA Life Time:** Configure the length of time a VPN tunnel is active in this phase. The default value for Phase 1 is 28800 seconds. The default value for Phase 2 is 3600 seconds.
- **Perfect Forward Secrecy:** If the Perfect Forward Secrecy (PFS) feature is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication, so hackers using brute force to break encryption keys will not be able to obtain future IPsec keys.

Check the box to enable this feature, or uncheck the box to disable this feature. This feature is recommended.

- **Preshared Key:** Enter a pre-shared key to use to authenticate the remote IKE peer. You can enter up to 30 keyboard characters and hexadecimal values, such as My_@123 or 4d795f40313233. Both ends of the VPN tunnel must use the same Preshared Key. It is strongly recommended that you change the Preshared Key periodically to maximize VPN security.
- **Minimum Preshared Key Complexity:** Check the **Enable** box if you want to enable the Preshared Key Strength Meter.
- **Preshared Key Strength Meter:** If you enable Minimum Preshared Key Complexity, this meter indicates the preshared key strength. As you enter a preshared key, colored bars appear. The scale goes from red (weak) to yellow (acceptable) to green (strong).

TIP: Enter a complex preshared key that includes more than eight characters, upper- and lowercase letters, numbers, and symbols such as `-*^+=.`

- **Advanced settings for IKE with Preshared Key**

When the Keying Mode is set to IKE with Preshared Key mode, advanced settings are available. For most users, the basic settings should suffice; advanced users can click **Advanced +** to view the advanced settings. To hide these settings, click **Advanced -**

- **Aggressive Mode** (*available for Tunnel, not Group VPN*): Two modes of IKE SA negotiation are possible: Main Mode and Aggressive Mode. If network security is preferred, Main Mode is recommended. If network speed is preferred, Aggressive Mode is recommended. You can adjust this setting if the Remote Security Gateway Type is *IP Only* or one of the *IP +* types. Check this box to enable Aggressive Mode, or uncheck the box to disable Aggressive Mode and use Main Mode.

NOTE: If the Remote Security Gateway Type is one of the *Dynamic IP* types, Aggressive Mode is required. The box is checked automatically, and this setting cannot be changed.

- **Compress (Support IP Payload Compression Protocol (IP Comp)):** IP Comp is a protocol that reduces the size of IP datagrams. Check the box to enable the router to propose compression when it initiates a connection. If the responders reject this proposal, then the router will not implement compression. When the device works as a responder, it will

always accept compression, even if compression is not enabled. If you enable this feature for this router, also enable it on the client.

- **Keep-Alive:** This feature enables the router to attempt to automatically re-establish the VPN connection if it is dropped. Check the box to enable this feature, or uncheck the box to disable it.
- **AH Hash Algorithm:** The AH (Authentication Header) protocol describes the packet format and default standards for packet structure. With the use of AH as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet. Check the box to use this feature. Then select an authentication method: MD5 or SHA1. MD5 produces a 128-bit digest to authenticate packet data. SHA1 produces a 160-bit digest to authenticate packet data. Both sides of the tunnel should use the same algorithm.
- **NetBIOS Broadcast:** NetBIOS broadcast messages are used for name resolution in Windows networking, to identify resources such as computers, printers, and file servers. These messages are required by some software applications and Windows features such as Network Neighborhood. LAN broadcast traffic is typically not forwarded over a VPN tunnel. However, you can check this box to allow NetBIOS broadcasts from one end of the tunnel to be rebroadcast to the other end.
- **Dead Peer Detection (DPD)** (*available for Tunnel, not Group VPN*): Check the box to enable the router to send periodic HELLO/ACK messages to check the status of the VPN tunnel. This feature can be used only when it is enabled on both ends of the VPN tunnel. Specify the interval between HELLO/ACK messages (how often you want the messages to be sent).
- **NAT Traversal:** Network Address Translation (NAT) enables users with private LAN addresses to access Internet resources by using a publicly routable IP address as the source address. However, for inbound traffic, the NAT gateway has no automatic method of translating the public IP address to a particular destination on the private LAN. This issue prevents successful IPsec exchanges. If your VPN router is behind a NAT gateway, check this box to enable NAT traversal. Uncheck the box to disable this feature. The same setting must be used on both ends of the tunnel.

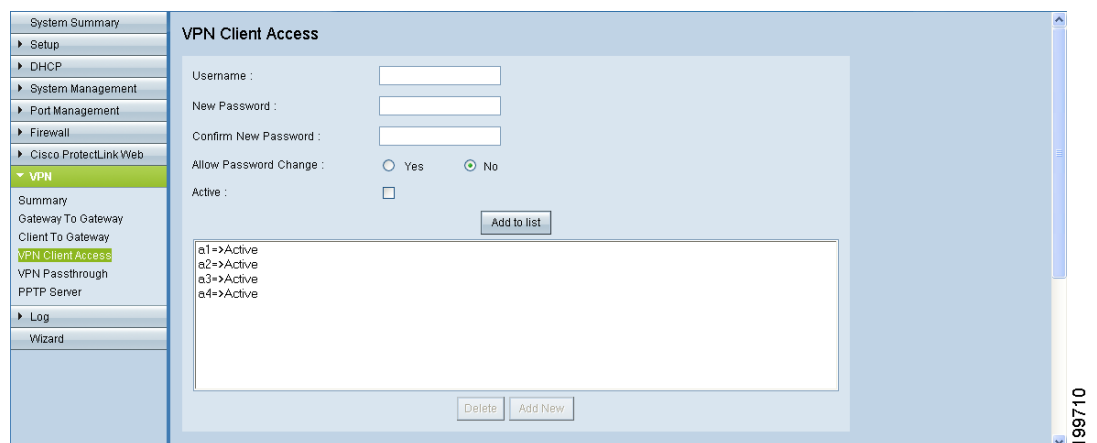
Managing VPN Users and Certificates

Use the *VPN > VPN Client Access* page to configure usernames and passwords for Cisco QuickVPN users and to generate the SSL certificates to install on their computers. You can add up to 50 users. First, export a certificate and use the exported client certificate for the Cisco QuickVPN Client. Then enter the information at the top of the screen and the users you've entered will appear in the list at the bottom, showing their status. The Router supports up to 50 Cisco QuickVPN Clients.

NOTE

- QuickVPN Client 1.4.0.5 or later supports Windows 7/XP/Vista. Firewall must be enabled on Vista and Windows 7. QuickVPN users must have the administrator rights to the PC.
- A user can connect without a certificate installed on the PC. The user will see a security warning when connecting to the VPN tunnel, but can proceed without this extra security protection.
- For more information about QuickVPN, see [Cisco QuickVPN for Windows, page 167](#).

To open this page: Click **VPN > VPN Client Access** in the navigation tree.



Add or update users as needed. For each new user, export a client certificate to install on the user's PC for a more secure connection.

- [Users, page 148](#)
- [Certificate Management, page 148](#)

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned. When you first save these settings, a message will appear, asking if you would like the router to automatically change the LAN IP address to prevent conflicting IP addresses. To change the LAN IP address, click **Yes**. If an IP conflict occurs, the QuickVPN client will not connect to the router.

Users

- **To add a VPN user to the list:** Enter the following information, and then click **Add to list**. After adding users, you can generate certificates to be installed on their computers (see details in [Certificate Management, page 148](#)).
 - **Username:** Enter a name for this user.
 - **New Password:** Enter a password.
 - **Confirm New Password:** Re-enter the password to confirm.
 - **Allow Password Change:** Check **Yes** to allow the user to change the password, or click **No** to prevent the user from changing the assigned password.
 - **Active:** Check the box to make the new user active.
- **To add another new user:** Enter the information, and then click **Add to list**.
- **To modify a user in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete a user from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Certificate Management

- **Generate New Certificate:** To generate a new certificate to replace the existing certificate on the router, click **Generate**. After clicking the button, a confirmation page appears. Click **OK** to continue.
- **Export Certificate for Administrator:** The administrator certificate on the router contains the private key. You can export a copy of the certificate to save as a backup file. For example, if you reset the router to the factory default settings, you should first export the certificate. After you restart the router, you can import this file to restore the certificate. To export the

administrator certificate, click **Export for Admin**. When the *File Download* window appears, click **Save**. Choose a safe place to save the certificate, enter a descriptive filename, and click **Save**. When the *Download complete* window appears, click **Close**.

- **Export Certificate for Client:** You can install a client certificate on a user's PC to prevent a man-in-the-middle attack. To export the client certificate, click **Export for Client**. When the *File Download* window appears, click **Save**. Locate the install directory for the client software (typically C:\Program Files\Cisco Small Business\QuickVPN client), enter a descriptive filename, and then click **Save**. When the *Download complete* window appears, click **Close**.

NOTE: A user can connect without a certificate installed on the PC. The user will see a security warning when connecting to the VPN tunnel, but can proceed without this extra security protection.

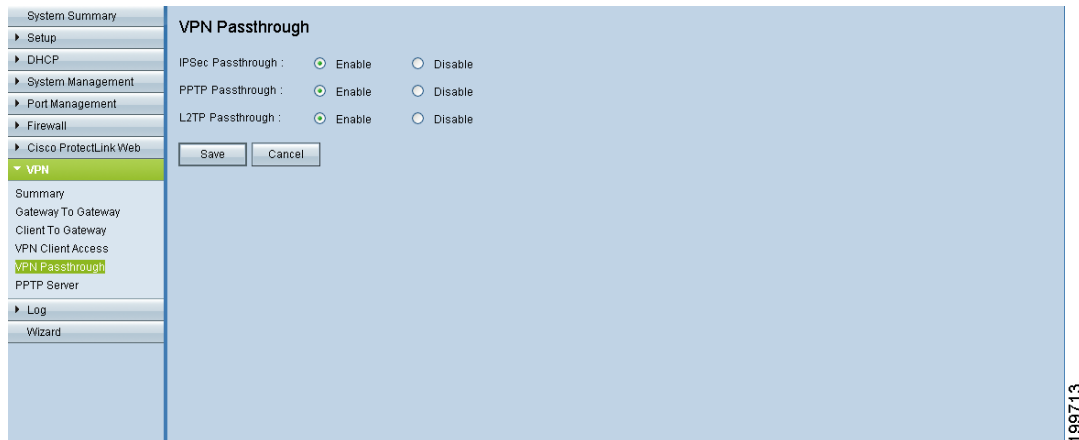
- **Import Certificate:** To restore a previously saved administrator certificate, click **Browse**, locate the file, and click **Open**. Then click **Import**. When the confirmation message appears, click **OK** to replace the existing certificate with the specified file. Click **Cancel** to close the message without importing the certificate.
- **Existing Certificate:** The filename of the current certificate, which is stored on the router.

Setting Up VPN Passthrough

Use the *VPN > VPN Passthrough* page to enable or disable passthrough for a variety of VPN methods. VPN passthrough is enabled by default to allow VPN clients on the LAN of the router to reach the VPN server on the Internet.

Cisco recommends enabling VPN Passthrough to allow VPN clients to pass through the router to connect to the VPN endpoint without problems. The administrator can disable the VPN Passthrough to block VPN clients from reaching the VPN endpoint on the Internet.

To open this page: Click **VPN > VPN Passthrough** in the navigation tree.



NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Enable or disable the following settings, as needed:

- **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.
- **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.
- **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.

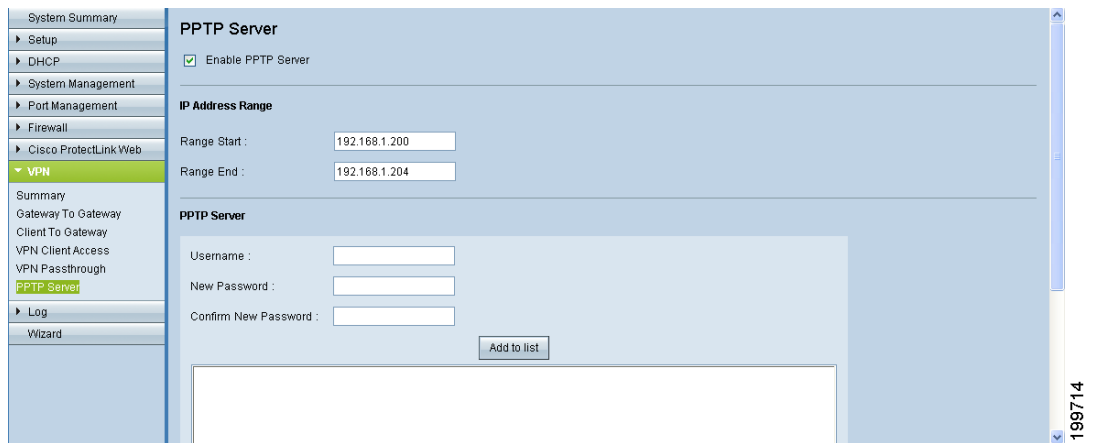
Setting Up PPTP Server

Use the *VPN > PPTP Server* page to enable up to five PPTP (Point-to-Point Tunneling Protocol) VPN tunnels for users who are running PPTP client software on Windows XP or 2000. PPTP clients are included by default in Microsoft Windows.

NOTE In Windows XP/2000, a user opens the Network Connections panel and creates a new connection. In the wizard, the user selects the option to create a connection to the workplace using a Virtual Private Network connection. The user will need to know the host name or IP address for the router. This value needs to match the value that you enter on the *VPN > PPTP Server* page. The wizard guides the user to create a desktop shortcut, which can be used to launch the client. To connect, the

user launches the client and logs in with the user name and password that you configured. For more information, users should refer to the Windows documentation or Help files.

To open this page: Click **VPN > PPTP Server** in the navigation tree.



NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

Check the **Enable PPTP Server** box to allow PPTP VPN tunnels. Uncheck the box to disable this feature. It is disabled by default. After you check the box, additional fields appear.

IP Address Range

Enter the range of LAN address to assign to the PPTP VPN clients. Enter the first address in the **Range Start** field, and enter the final address in the **Range End** field. The default range is 192.168.1.200 to 92.168.1.204.

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

PPTP Server

Add or edit the list of PPTP VPN users.

- **To add a user to the list:** Enter the following information, and then click **Add to list**.
 - **Username:** Enter a name for this user.
 - **New Password:** Enter a password.
 - **Confirm New Password:** Re-enter the password to confirm.

- **To add another new user:** Enter the information, and then click **Add to list**.
- **To modify a user in the list:** Click the entry that you want to modify. The information appears in the text fields. Make the changes, and then click **Update**. If you do not need to make changes, you can click **Add New** to de-select the entry and clear the text fields.
- **To delete a user from the list:** Click the entry that you want to delete. To select a block of entries, click the first entry, hold down the **Shift** key, and click the final entry in the block. To select individual entries, hold down the **Ctrl** key while clicking. Click **Delete**.

Connection List

The following read-only information appears. You can click **Refresh** to update the data.

- **Username:** The name of the PPTP VPN client.
- **Remote Address:** The WAN IP address of the PPTP VPN client.
- **PPTP IP Address:** The LAN IP address that the PPTP server assigned to the client upon connection.

Logging System Statistics

Use the Log module to set up the system log, to configure alerts, and to view system statistics. Refer to these topics:

- [Setting Up the System Log and Alerts, page 153](#)
- [Viewing the System Log, page 157](#)

Setting Up the System Log and Alerts

Use the *Log > System Log* page to configure logs and alerts and to view the log tables.

To open this page: Click **Log > System Log** in the navigation tree.

The screenshot displays the 'System Log' configuration interface. On the left, a navigation tree includes 'System Summary', 'Setup', 'DHCP', 'System Management', 'Port Management', 'Firewall', 'Cisco ProtectLink Web', 'VPN', 'Log' (expanded), 'System Log' (selected), 'System Statistics', and 'Wizard'. The main panel is titled 'System Log' and is divided into three sections:

- Syslog:** Contains an unchecked 'Enable Syslog' checkbox and a text input field for 'Syslog Server' with the placeholder '(Name or IP Address)'.
- Email:** Contains an unchecked 'Enable Email Alert' checkbox, a 'Mail Server' text field (placeholder: '(Name or IP Address)'), a 'Send Email to' text field (placeholder: '(Email Address)'), a 'Log Queue Length' field set to '50' with the unit 'Entries', and a 'Log Time Threshold' field set to '10' with the unit 'Minutes'. Below these fields is an 'Email Log Now' button.
- Log Setting:** Contains an unchecked 'Alert Log' checkbox.

NOTE Before navigating away from this page, click **Save** to save your settings, or click **Cancel** to undo them. Any unsaved changes are abandoned.

This page has the following sections:

- [Syslog section, page 154](#)
- [E-mail section, page 154](#)

- [Log Setting, page 155](#)
- [Buttons, page 156](#)

Syslog section

You can enable the router to send detailed log files to your syslog server when events are logged.

- **Enable Syslog:** Syslog is an industry-standard protocol used to capture information about network activity. When this feature is enabled, the router will send all log activities, including every source/destination IP address and service, to syslog server. Check the box to enable syslog. Uncheck the box to disable this feature.
- **Syslog Server:** Enter the Syslog server name or IP address. Restart the RV0xx for the change to take effect.

E-mail section

You can enable the router to send email alerts when events are logged.

- **Enable E-Mail Alert:** Check this box to enable the router to send email alerts to the specified email address. Uncheck the box to disable this feature.
- **Mail Server:** Enter the IP address or name of your ISP's SMTP server.
NOTE: Your ISP may require that you identify your router by entering a host name on the *Setup > Network* page.
- **Send Email to:** Enter the email address where you want to send the alerts.
- **Log Queue Length:** Specify the number of log entries to include in the email. The default is 50.
- **Log Time Threshold:** Log time threshold is the maximum wait time before a email log message is sent. When the Log Time Threshold expires, an email is sent whether the email log buffer is full or not. Specify the number of minutes to collect data before sending the log. The default is 10.
- **Email Log Now:** Click this button to immediately send a message to the specified email address, to test your settings.

Log Setting

Choose the events to report in the logs:

- **Alert Log:** These events include common types of attacks as well as unauthorized login attempts. Check each type of attack to include in the alert log. Uncheck each event to omit from the alert log.
 - **Syn Flooding:** An attacker sends a succession of SYN packets, causing the router to open so many sessions that it is overwhelmed and denies service to legitimate traffic.
 - **IP Spoofing:** An attacker sends packets with a forged source IP address to disguise an attack as legitimate traffic.
 - **Win Nuke:** An attacker sends an Out-of-Band message to a Windows machine with the purpose of causing the target computer to crash.
 - **Ping of Death:** An attacker sends a very large IP packet with the purpose of causing the target computer to crash.
 - **Unauthorized Login Attempt:** Someone tried to log in to the router configuration utility without providing the correct username or password.
 - **Output Blocking Event:** There was an event in ProtectLink web reputation or URL filtering.
- **General Log:** These events include actions that are performed to enforce configured policies as well as routine events such as authorized logins and configuration changes. Check each type of event to include in the general log. Uncheck each event to omit from the general log.
 - **System Error Messages:** All system error messages.
 - **Deny Policies:** Instances when the router denied access based on your Access Rules.
 - **Allow Policies:** Instances when the router allowed access based on your firewall access rules. Note that events for specific access rules can be included in the log or excluded based on the *Log* setting in the access rule configuration. For more information, see [Configuring Firewall Access Rules, page 103](#).
 - **Configuration Changes:** Instances when someone saved changes in the configuration.

- **Authorized Login:** Instances when someone successfully logged into the router configuration utility after entering the correct username and password.

Buttons

Use the following buttons to view additional information:

- **View System Log:** Click this button to view the System Log. The information appears in a new window. If the web browser displays a warning about the pop-up window, allow the blocked content.

In the *System Log* window, you can use the drop-down list to choose a particular log to display. Click **Refresh** to update the data, or click **Clear** to erase all displayed information. When you finish viewing the log, click **Close** to close the pop-up window.

Log entries include the date and time of the event, the event type, and a message. The message specifies the type of policy, such as Access Rule, the LAN IP address of the source (SRC), and the MAC address

- **Outgoing Log Table:** Click this button to view the outgoing packet information. The information appears in a new window.

In the *Outgoing Log Table* window, you can click **Refresh** to update the data. When you finish viewing the log, click **Close** to close the pop-up window.

- **Incoming Log Table:** Click this button to display the incoming packet information. The information appears in a new window. If the web browser displays a warning about the pop-up window, allow the blocked content.

In the *Incoming Log Table* window, you can click **Refresh** to update the data. When you finish viewing the log, click **Close** to close the pop-up window.

- **Clear Log Now:** Click this button to clear out your log without emailing it. Use this button only if you do not want to view the information again in the future.

Viewing the System Log

Use the *Log > System Log* page to display statistics about all of the router's ports (LAN and WAN ports).

To open this page: click **Log > System Statistics** in the navigation tree.

| Interface | LAN | WAN1 | WAN2 |
|--------------------------|-------------------|-------------------|-------------------|
| Device Name | eth0 | eth1 | eth2 |
| Status | --- | Connected | Enabled |
| IP Address | 192.168.1.1 | 10.0.0.102 | 0.0.0.0 |
| MAC Address | 00:17:16:03:26:B1 | 00:17:16:03:26:B2 | 00:17:16:03:26:B3 |
| Subnet Mask | 255.255.255.0 | 255.255.255.0 | 0.0.0.0 |
| Default Gateway | --- | 10.0.0.1 | 0.0.0.0 |
| DNS | --- | 192.168.5.121 | 0.0.0.0 |
| Received Packets | 1815 | 6492 | 0 |
| Sent Packets | 2356 | 5893 | 0 |
| Total Packets | 4171 | 12385 | 0 |
| Received Bytes | 242977 | 4252265 | 0 |
| Sent Bytes | 1909276 | 886008 | 0 |
| Total Bytes | 2152253 | 5138273 | 0 |
| Error Packets Received | 0 | 0 | 0 |
| Dropped Packets Received | 0 | 0 | 0 |

Statistics appear for each interface, such as LAN, WAN1, WAN2 or DMZ. You can click **Refresh** to update the data.

For each port, the following statistics are listed:

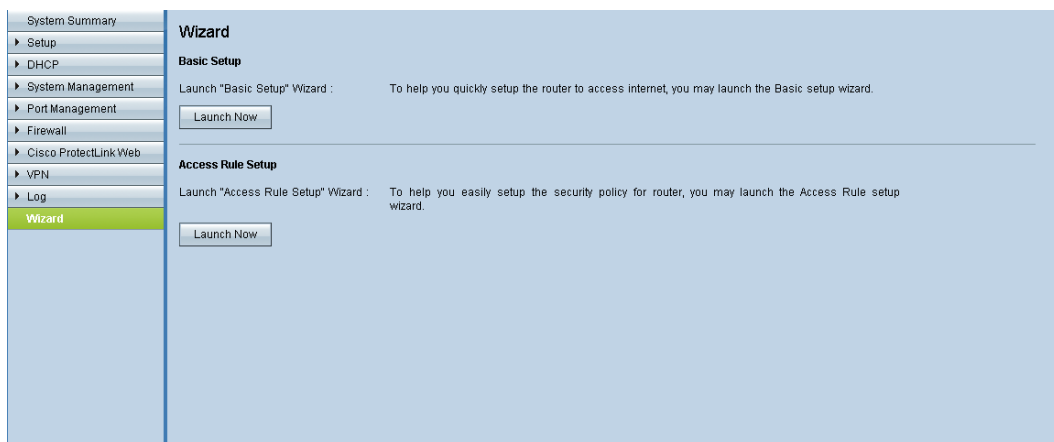
- **Device Name:** The port ID, such as eth0, eth1, eth2, and so on
- **Status:** The port status. Depending on the interface type, the status may be Connected, Disconnected, Enabled, or Disabled.
- **IP Address:** The IP address of the interface
- **MAC Address:** The MAC of the connected device
- **Subnet Mask:** The subnet mask
- **Default Gateway:** The default gateway
- **DNS:** The DNS server for DNS name resolution
- **Received Packets:** The number of packets received through this interface
- **Sent Packets:** The number of packets sent through this interface
- **Total Packets:** The total number of packets sent and received through this interface

- **Received Bytes:** The number of bytes received through this interface
- **Sent Bytes:** The number of bytes sent through this interface
- **Total Bytes:** The total number of bytes sent and received through this interface
- **Error Packets Received:** The number of error packets received through this interface
- **Dropped Packets Received:** The number of received packets that were dropped due to issues such as error checksum.

Wizard

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

To open this page: Click **Wizard** in the navigation tree. Alternatively click **Setup Wizard** on the *System Summary* page.



This page includes the following sections:

- **Basic Setup, page 160**
- **Access Rule Setup, page 160**

Basic Setup

Use the Basic Setup Wizard to change the number of WAN ports or to configure the Internet connection.

Click **Launch Now** to run the Basic Setup Wizard. Follow the on-screen instructions to proceed. Refer to the information from your ISP to enter the required settings for your connection.

Access Rule Setup

Use the Access Rule Setup Wizard to create firewall access rules. Click **Launch Now** to run the Access Rule Setup Wizard. The wizard provides information about the router's default rules to help you get started. Follow the on-screen instructions to proceed.

Glossary

| Term | Definition |
|---|--|
| beacon interval | The time interval at which beacon frames are transmitted. Beacon frames announce the existence of the wireless network. |
| DTIM (Delivery Traffic Indication Message) | A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Cisco RV220W has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. |
| dynamic routing | Dynamic routing enables the router to adjust automatically to physical changes in the network's layout. Using the dynamic RIP protocol, the router calculates the most efficient route for the network's data packets to travel between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network. It determines the best route based on the fewest number of hops between the source and the destination. |

| Term | Definition |
|--|---|
| Fragmentation Threshold | The frame length, in bytes, that requires packets to be fragmented into two or more frames. Setting a lower value can reduce collisions, which occur more often in the transmission of long frames. You may need to use a lower setting in areas where communication is poor or where there is a great deal of radio interference. However, setting the fragmentation threshold too low may result in poor network performance. |
| IKE (Internet Key Exchange) | The Internet Key Exchange (IKE) protocol dynamically exchanges keys between two IPsec hosts. |
| MTU (Maximum Transmission Unit) | The largest packet that can be sent over the network. |
| Network Address Translation (NAT) | Network Address Translation (NAT) is a technique that allows several endpoints on a LAN to share an Internet connection. In this scenario, the computers on the LAN use a “private” IP address range while the WAN port on the router is configured with a single “public” IP address. The router translates the internal private addresses into a public address, hiding internal IP addresses from computers on the Internet. |
| Preamble Mode | The 802.11b standard requires adding a preamble to every frame before it is transmitted through the air. The traditional long preamble requires 192 μ s for transmission. A short preamble requires only 96 μ s. A long preamble is needed for compatibility with the legacy 802.11 systems operating at 1 and 2 Mbps. |

| Term | Definition |
|--|--|
| RADVD (Router Advertisement Daemon) | RADVD is an open-source software product that uses the Neighbor Discovery Protocol (NDP) to listen for router solicitations in the IPv6 LAN. It responds with router advertisements to support stateless address auto-configuration. When a new host connects to the network, it sends a request for its configuration parameters, and the router responds with a router advertisement packet that contains the network-layer configuration parameters including IPv6 prefixes. The node takes the prefix and extends it to a full 128 bit address by adding an EUID based on its hardware address. |
| Request to Send (RTS) Threshold | The packet size, in bytes, that requires an RTS/Clear to Send (CTS) handshake before sending. A low setting can be useful in areas where many client devices are associating with the wireless device, or in areas where the clients are far apart and can detect only the access point but not other clients. Although a low threshold value consumes more bandwidth and reduces the throughput of the packet, frequent RTS packets can help the network to recover from interference or collisions. |
| Routing Information Protocol (RIP) | <p>This protocol uses use distance vectors to mathematically compare routes to identify the best path to any given destination address. RIP sends routing-update messages at regular intervals and when the network topology changes. Upon receiving a RIP message, a router updates its routing table and transmits the updates to other routers. RIP prevents loops and has features to provide stability despite potentially rapid changes in a network's topology.</p> <p>RIPv2 supports subnet masks, allows more information to be included in RIP packets, and provides a simple authentication mechanism that is not supported by RIP.</p> |

| Term | Definition |
|------------------------------------|---|
| RIPng (RIP next generation) | RIPng is an extension of RIPv2 for support of IPv6. (See the information about RIP in this Glossary.) |
| static routing | <p>A static route is a pre-determined pathway that a packet must travel to reach a specific host or network.</p> <p>CAUTION: Static routing is a powerful feature that should be used by advanced users only. In many cases, it is better to use dynamic routing because it enables the router to automatically adjust to physical changes in the network's layout.</p> <p>Use cases for static routing include the following:</p> <ul style="list-style-type: none">▪ Some ISPs require static routes to build your routing table instead of using dynamic routing protocols.▪ You can use static routes to reach peer routers that do not support dynamic routing protocols.▪ If the router is connected to more than one network or there are multiple routers installed on your network, it may be necessary to set up static routes to enable traffic between them.▪ You can use static routing to allow users in different IP domain to access the Internet through the router. |
| VLAN (Virtual LAN) | A VLAN is a group of endpoints in a network that are associated by function or other shared characteristics. Unlike LANs, which are usually geographically based, VLANs can group endpoints without regard to the physical location of the equipment or users. |

Troubleshooting

The firmware upgrade has failed.

A firmware upgrade takes approximately ten minutes. An error may occur if you powered off the router, pressed the Reset button, closed the *System Management > Firmware Upgrade* page, or disconnected the computer from the router during the firmware upgrade.

If the firmware upgrade failed, repeat the firmware upgrade procedure using the *System Management > Firmware Upgrade* page of the configuration utility. For more information, see [Upgrading the Firmware, page 90](#).

If the Diag status light continues to flash, the firmware image is damaged. Use the TFTP utility to upgrade the firmware. You can download the TFTP utility at www.cisco.com.

Your computer cannot connect to the Internet.

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

- Make sure that the router is powered on. The System status light should be green and not flashing.
- If the System status light is flashing, then power off all of your network devices, including the modem, router, and computers. Then power on each device in **the following order**:
 - Cable or DSL modem
 - Router
 - Computer
- Check the cable connections. The computer should be connected to one of the ports numbered 1 to 4 on the router, and the modem must be connected to the Internet port on the router.

The DSL telephone line does not fit into the router's Internet port.

The router does not replace your modem. You still need your DSL modem in order to use the router. Connect the telephone line to the DSL modem, insert the setup CD into your computer, and then follow the on-screen instructions.

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

The router does not replace your modem. You still need your cable modem in order to use the router. Connect your cable connection to the cable modem, insert the setup CD into your computer, and then follow the on-screen instructions.



Cisco QuickVPN for Windows

Cisco QuickVPN can be used for client access to a Client to Gateway tunnel that you configured on this router. Refer to these topics:

- [Introduction, page 167](#)
- [Cisco QuickVPN Client Installation and Configuration, page 168](#)
- [Using the Cisco QuickVPN Software, page 168](#)

NOTE For more information about the configuration process, see [Managing VPN Users and Certificates, page 147](#).

Introduction

The Cisco RV0xx Series VPN routers support IPSec VPN client software, including the Cisco QuickVPN software. For the latest features, install QuickVPN Client 1.4.0.5 or later, which supports Windows 7.

The router supports up to 50 Cisco QuickVPN clients free of charge. If the router you have only supports up to ten clients, then upgrade its firmware.

You can create a VPN tunnel between a computer using VPN client software and a VPN router. The following is an example of a computer-to-VPN router VPN. In her hotel room, a traveling businesswoman connects to her Internet Service Provider (ISP). Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software and connects to the VPN router at the central office. As VPNs use the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.

Cisco QuickVPN Client Installation and Configuration

For each QuickVPN client, complete the following tasks:

-
- STEP 1** To download QuickVPN, complete the following tasks:
- Start a web browser, and enter the following address: www.cisco.com/go/software
 - In the Software Download Search box, enter: **QuickVPN**
 - Click **Go**.
 - In the search results, click the link for your router.
 - Follow the on-screen instructions to download the QuickVPN client.

- STEP 2** To install the client certificate, save the client certificate to the directory where the QuickVPN program is installed.

Example: C:\Program Files\Cisco Small Business\QuickVPN Client\

NOTE: QuickVPN can be used without a certificate installed on the PC. The user will see a security warning but can use QuickVPN without this added security.

Using the Cisco QuickVPN Software

NOTE: Optionally, an SSL certificate can be installed on the PC for extra security; if this certificate is not installed, you can still use QuickVPN, but you will see a pop-up warning during this process.

For each QuickVPN client, follow these instructions:

-
- STEP 1** Double-click the Cisco QuickVPN software icon on your desktop or in the system tray.
- STEP 2** When the *QuickVPN Login* page appears, enter the following information:
- Profile Name:** Enter a name for your profile.
 - Username:** Enter the username assigned to you.
 - Password:** Enter the password assigned to you.

- **Server Address:** Enter the WAN IP address or domain name of the remote router.
- **Port for QuickVPN:** Enter the port number that the QuickVPN client will use to communicate with the remote VPN router, or keep the default, **Auto**.
- **Use Remote DNS Server:** When this feature is enabled, QuickVPN users use the Remote DNS Server (provided by the QuickVPN Server) to resolve the hostname of the computers in the remote subnet over a QuickVPN tunnel.

STEP 3 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 4 To begin your QuickVPN connection, click **Connect**. The connection's progress is displayed in this **order**: *Connecting, Provisioning, Activating Policy, and Verifying Network*.

STEP 5 When your QuickVPN connection is established, the QuickVPN tray icon turns green, and the *QuickVPN Status* page appears. The page 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.

STEP 6 To terminate the VPN tunnel, click **Disconnect**.

If you clicked Change Password and have permission to change your own password, the *Connect Virtual Private Connection* page appears.

- **Old Password:** Enter your password.
- **New Password:** Enter your new password.
- **Confirm New Password:** Re-enter your new password.

STEP 7 Click **OK** to save your new password. Click **Cancel** to cancel your change. For information, click **Help**.

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

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

This appendix explains how to set up a VPN between two RV0xx Series routers. You can then repeat the procedures to add tunnels to your other sites. A Cisco RV0xx Series router supports up to 100 VPN tunnels.

NOTE Even if you have an RV0xx Series router on one end of the tunnel, and a different model on the other end, you can use this information to set up your RV0xx Series router. Note the shared settings that you need to configure on your other router. Both devices must use a common key or certificate and must have the same security policies set up.

Refer to these topics:

[Overview, page 1](#)

[Topology Options, page 170](#)

[Other Design Considerations, page 173](#)

[Configuring a VPN Tunnel on a Cisco RV0xx Series Router, page 175](#)

Topology Options

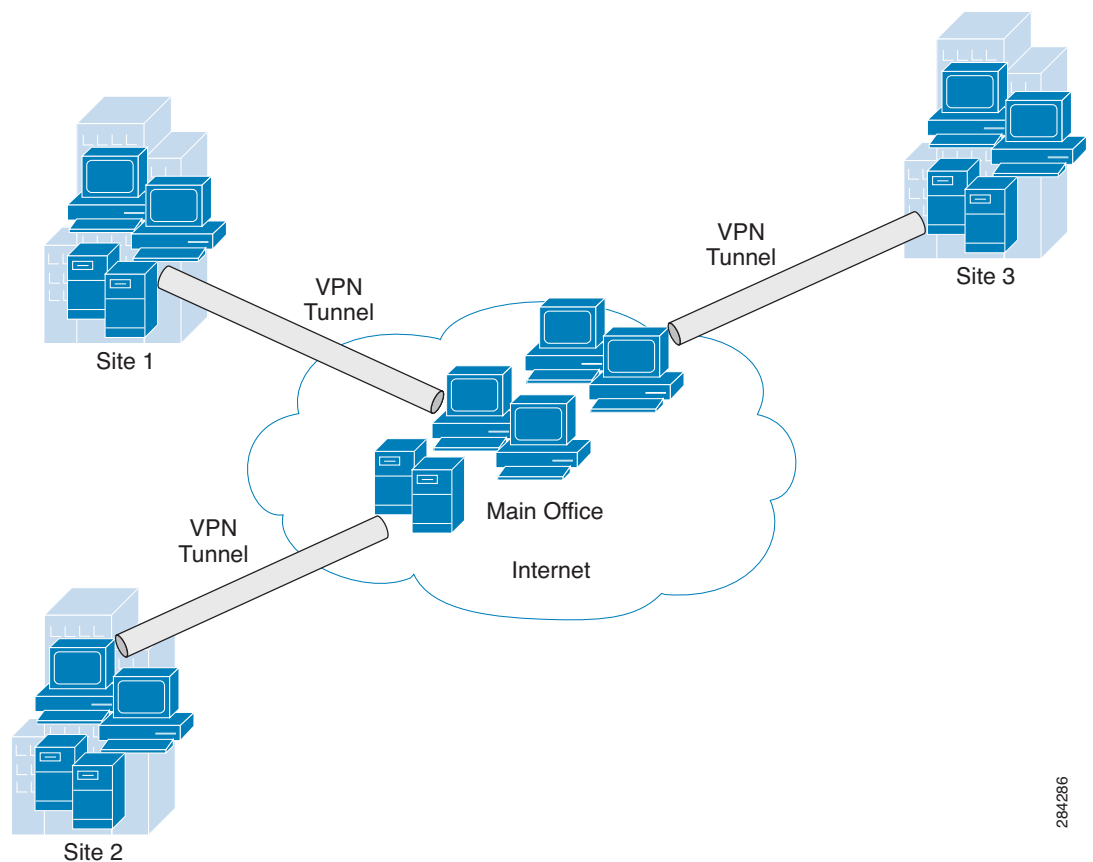
Before you configure the VPN settings on your routers, consider the topology options. A VPN topology specifies the peers and the networks that are part of the VPN and how they connect to one another. Depending on the number of sites and the nature of traffic, you can choose a hub-and-spoke topology or a mesh topology.

VPN Hub and Spoke Topology

In a VPN hub-and-spoke topology, multiple VPN routers (spokes) communicate securely with a central VPN router (hub). A separate, secured tunnel extends between each individual spoke and the hub.

In the following example, two branch offices (spokes) have site-to-site VPN tunnels to the main office (hub). The traffic typically is between a remote site and the main office. Inter-site traffic must pass through the hub first and then out to a spoke.

Figure 1 Hub and Spoke



This topology is a simple way to allow all branch employees to access the main network. It works well if most traffic is from the remote sites to the main network and there is little traffic among the sites. Too much inter-site traffic may create bottlenecks at the hub.

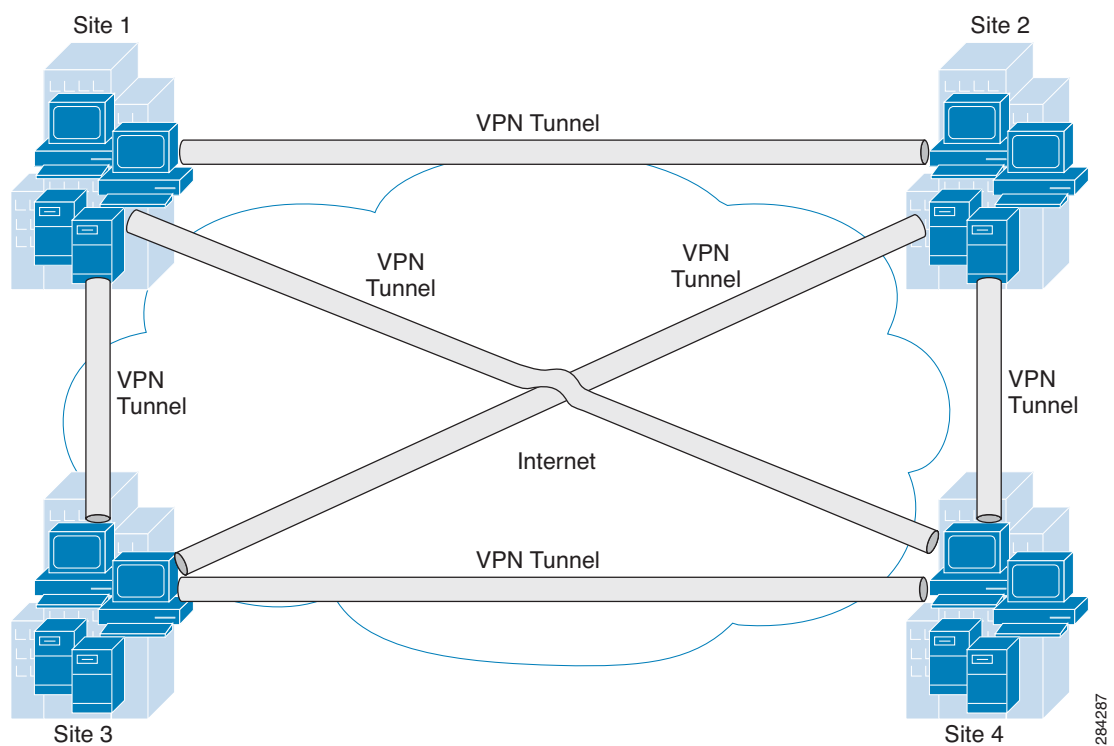
284286

VPN Mesh Topology

In a VPN mesh topology, each VPN router can communicate securely with all other VPN routers. Multiple secured tunnels extend from each site to all other sites.

In the following example, four sites are connected in a VPN mesh topology. Three VPN tunnels extend from each site, providing secure communications with all other sites. Data can travel directly between any two sites.

Figure 2 Mesh



This topology requires much more configuration on each router. However, it works well in a complicated network with data traveling between multiple sites. Because all devices have direct peer relationships with one another, this design prevents the bottlenecks that can occur with a hub-and-spoke topology. This design also ensures that if one site is down, the other sites can continue to exchange data.

NOTE When the number of nodes in a full mesh topology increases, scalability may become an issue—the limiting factor being the number of tunnels that the devices can support at a reasonable CPU utilization.

Other Design Considerations

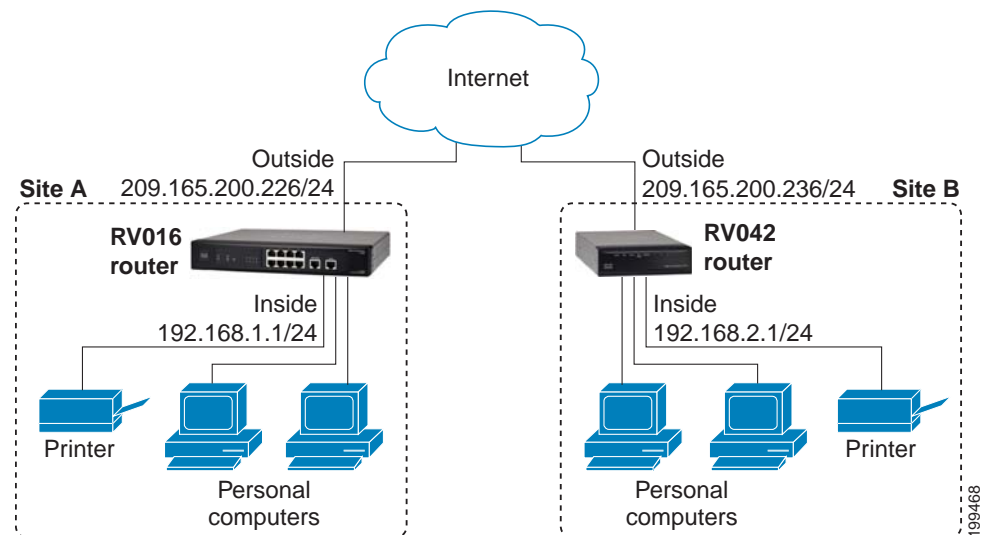
Before you configure your VPN tunnels, consider the following points about your network setup.

WAN Setup

The WAN setup pertains to the network that your router connects to outside your office. The first consideration is the type of IP addresses that you received for your Internet service at your two sites. As when constructing a physical tunnel or bridge, you need to know where the VPN tunnel is going.

- **If at least one site has a static IP address:** A VPN tunnel easily can be established if at least one of the sites has a static IP address for the WAN connection. A static IP address is a publicly routable Internet address that does not change. In this scenario, establishing a VPN tunnel can be compared to building a bridge between two docks (two sites with static IP addresses), or even setting a gangplank between a dock and an unanchored boat (one site with a static IP address and one with a dynamic IP address).

Figure 3 Gateway To Gateway Tunnel with Static IP Addresses

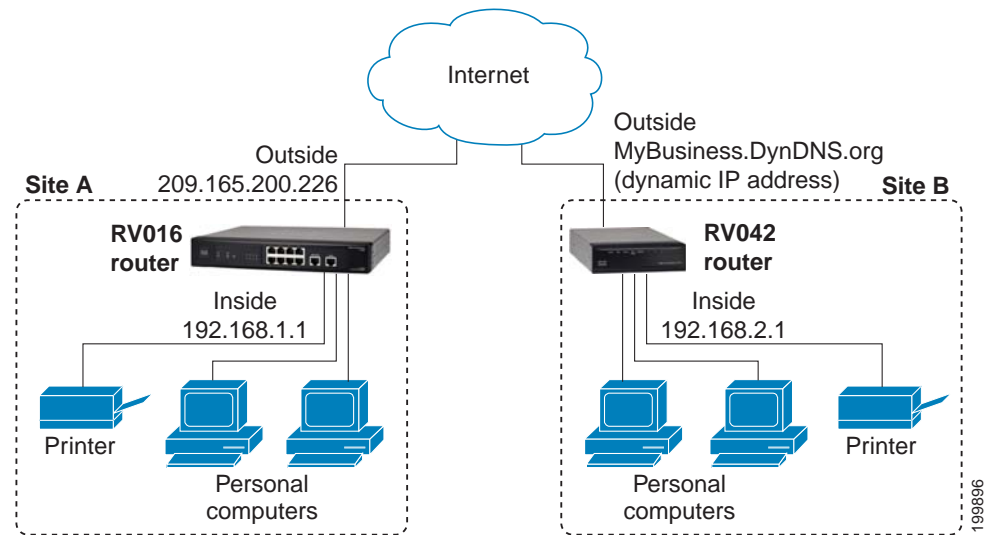


- **If both sites have dynamic IP addresses:** A dynamic IP address is a publicly routable IP address that is issued for your use when you connect to your service provider's network. Dynamic IP addresses may change without warning. In this scenario, establishing a VPN tunnel is like trying to build a bridge between two unanchored boats. However, you can "anchor"

one boat, so to speak, by obtaining a Fully Qualified Domain Name (FQDN) and registering at least one site with a Dynamic DNS service. This service associate tracks your dynamic IP address to ensure that your router is reachable even when the address changes.

As illustrated below, Dynamic DNS service ensures that traffic for the FQDN, MyBusiness.DynDNS.org, is routed to the dynamic IP address.

Figure 4 Gateway To Gateway Tunnel with a Dynamic IP Address



Free Dynamic DNS accounts are available through many providers. Examples are listed below.

- <http://dyn.com/dyndns>
- <http://update.ods.org>
- <http://www.dhs.org>
- <http://www.3322.org>
- <http://www.no-ip.com>

LAN Setup

The LAN setup pertains to the network that your router connects to inside your office. It should not be necessary to make any changes in your LAN setup, unless both sites have the same addressing. The two ends of the tunnel cannot be on the same subnet. For example, if the LAN IP address of the RV0xx router at Site A is 192.168.15.1, Site B must use a different subnet, such as 192.168.75.1.

Configuring a VPN Tunnel on a Cisco RV0xx Series Router

This procedure describes the basic tasks in configuring your router. Example entries are provided on [page 176](#).

NOTE

- For a hub-and-spoke topology, configure one tunnel between each remote site and the central site. For the scenario illustrated in [Figure 1](#), configure three VPN tunnels on the router at the main site, and configure one VPN tunnel on the router at each remote site.
- For a mesh topology, configure multiple tunnels on each router to ensure connectivity between all sites. For the scenario illustrated in [Figure 2](#), configure three VPN tunnels on each router.

STEP 1 Connect a computer to your Cisco RV0xx Series router (called Site A in the examples), and start the web-based configuration utility.

STEP 2 Click **VPN > Gateway to Gateway** in the navigation tree.

STEP 3 Enter the following information about the tunnel:

- **Tunnel Name**—Enter a name, for your reference. This name will be used on the *VPN > Summary* page.
- **Interface**—Select the appropriate Interface, **WAN1** or **WAN2**.

Note: The **Enable** check box is unavailable until after you save the configuration.

STEP 4 In the *Local Group Setup* section, enter the following information about this router (Site A):

- **Local Security Gateway Type**—Select **IP Only**. The WAN IP address of the router will be automatically detected and will appear in the *IP Address* field.
- **Local Security Group Type**—Select **Subnet**. Enter the **LAN IP Address** and the subnet mask.

STEP 5 In the *Remote Group Setup* section, enter the following information about the router at the other end of the tunnel (Site B):

- **Remote Security Gateway Type**—Depending on the type of IP address for the Internet connection, choose one of the following options:
 - *If the remote gateway (Site B) has a static WAN IP address:* Select **IP Only**. Enter the **WAN IP Address** of the Site B router.

- If the remote gateway (Site B) has a dynamic IP address and a Dynamic DNS hostname: Select **Dynamic IP + Domain Name (FQDN) Authentication**. Enter the registered **Domain Name** of the Site B router, such as MyBusiness.DynDNS.org.
 - **Remote Security Group Type**—Select **Subnet**. Enter the LAN **IP Address** and **Subnet Mask** of the Site B router.
- STEP 6** In the *IPSec Setup* section, keep the default settings (recommended) or enter other settings if desired. Ensure that you configure the Site B router with the same settings.
- STEP 7** In the **Preshared Key** field, enter a string for this key, for example, 13572468. Ensure that you configure the other router with the same preshared key.
- STEP 8** If you need more detailed settings, click **Advanced**. Otherwise, click **Save**.
- Note:** Advanced settings can be used to enable features such as dead peer detection, NAT traversal, split DNS, and NetBIOS broadcast messages.
- STEP 9** At the remote site (Site B), set up the router with the corresponding settings (where Site B is the “local gateway” and Site A is the “remote gateway”).
- STEP 10** Use the *VPN > Summary* page to verify that the tunnel is active.
- STEP 11** Verify that a computer at Site A can ping a computer at Site B, and vice versa. (Refer to Windows Help for more information). If the ping test is successful, then the VPN tunnel is configured correctly.
- STEP 12** Repeat this procedure to configure additional VPN tunnel.

Example: Sites with Static WAN IP Addresses

Settings on the Site A Router:

| Field | Value |
|------------------------------------|--|
| Local Group Setup | |
| Local Security Gateway Type | IP Only |
| IP Address | (Automatically detected) 203.165.200.226 |
| Local Security Group Type | Subnet |

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

Configuring a VPN Tunnel on a Cisco RV0xx Series Router



| Field | Value |
|------------------------------|------------------------|
| IP Address | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |
| Remote Group Setup | |
| Remote Security Gateway Type | IP Only |
| IP Address | 209.165.200.238 |
| Remote Security Group Type | Subnet |
| IP Address | 192.168.2.0 |
| Subnet Mask | 255.255.255.0 |
| IPSec Setup | |
| Keying Mode | IKE with Preshared Key |
| Phase 1 Encryption | DES |
| Phase 1 Authentication | MD5 |
| Phase 1 SA Life Time | 28800 |
| Perfect Forward Secrecy | Enabled |
| Phase 2 DH Group | Group 1 - 768 bit |
| Phase 2 Encryption | DES |
| Phase 2 Authentication | MD5 |
| Phase 2 SA Life Time | 3600 |
| Preshared Key | 13572468#123456789 |

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

Configuring a VPN Tunnel on a Cisco RV0xx Series Router



| Field | Value |
|----------------------------------|------------------|
| Minimum Preshared Key Complexity | Enabled |
| Advanced | Default settings |

Settings on the Site B Router:

| Field | Values |
|------------------------------|--|
| Local Group Setup | |
| Local Security Gateway Type | IP Only |
| IP Address | (Automatically detected) 209.165.200.238 |
| Local Security Group Type | Subnet |
| IP Address | 192.168.2.0 |
| Subnet Mask | 255.255.255.0 |
| Remote Group Setup | |
| Remote Security Gateway Type | IP Only |
| IP Address | 203.165.200.226 |
| Remote Security Group Type | Subnet |
| IP Address | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |
| IPSec Setup | |
| Keying Mode | IKE with Preshared Key |
| Phase 1 Encryption | DES |

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

Configuring a VPN Tunnel on a Cisco RV0xx Series Router



| Field | Values |
|----------------------------------|--------------------|
| Phase 1 Authentication | MD5 |
| Phase 1 SA Life Time | 28800 |
| Perfect Forward Secrecy | Enabled |
| Phase 2 DH Group | Group 1 - 768 bit |
| Phase 2 Encryption | DES |
| Phase 2 Authentication | MD5 |
| Phase 2 SA Life Time | 3600 |
| Preshared Key | 13572468#123456789 |
| Minimum Preshared Key Complexity | Enabled |
| Advanced | Default settings |

Example: Site with a Dynamic WAN IP Address

Settings on the Site A Router:

| Field | Value |
|-----------------------------|--|
| Local Group Setup | |
| Local Security Gateway Type | IP Only |
| IP Address | (Automatically detected) 203.165.200.226 |

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

Configuring a VPN Tunnel on a Cisco RV0xx Series Router



| Field | Value |
|-------------------------------------|--|
| Local Security Group Type | Subnet |
| IP Address | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |
| Remote Group Setup | |
| Remote Security Gateway Type | Dynamic IP + Domain Name (FQDN) Authentication |
| Domain Name | cisco.com |
| Remote Security Group Type | Subnet |
| IP Address | 192.168.2.0 |
| Subnet Mask | 255.255.255.0 |
| IPSec Setup | |
| Keying Mode | IKE with Preshared Key |
| Phase 1 Encryption | DES |
| Phase 1 Authentication | MD5 |
| Phase 1 SA Life Time | 28800 |
| Perfect Forward Secrecy | Enabled |
| Phase 2 DH Group | Group 1 - 768 bit |
| Phase 2 Encryption | DES |
| Phase 2 Authentication | MD5 |

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

Configuring a VPN Tunnel on a Cisco RV0xx Series Router



| Field | Value |
|----------------------------------|--------------------|
| Phase 2 SA Life Time | 3600 |
| Preshared Key | 13572468#123456789 |
| Minimum Preshared Key Complexity | Enabled |
| Advanced | Default settings |

Settings on the Site B Router:

| Field | Values |
|------------------------------|--|
| Local Group Setup | |
| Local Security Gateway Type | Dynamic IP + Domain Name (FQDN) Authentication |
| Domain Name | cisco.com |
| Local Security Group Type | Subnet |
| IP Address | 192.168.2.0 |
| Subnet Mask | 255.255.255.0 |
| Remote Group Setup | |
| Remote Security Gateway Type | IP Only |
| IP Address | 203.165.200.226 |
| Remote Security Group Type | Subnet |
| IP Address | 192.168.1.0 |
| Subnet Mask | 255.255.255.0 |

Configuring a Gateway-to-Gateway VPN Tunnel Between RV0xx Series Routers

Configuring a VPN Tunnel on a Cisco RV0xx Series Router



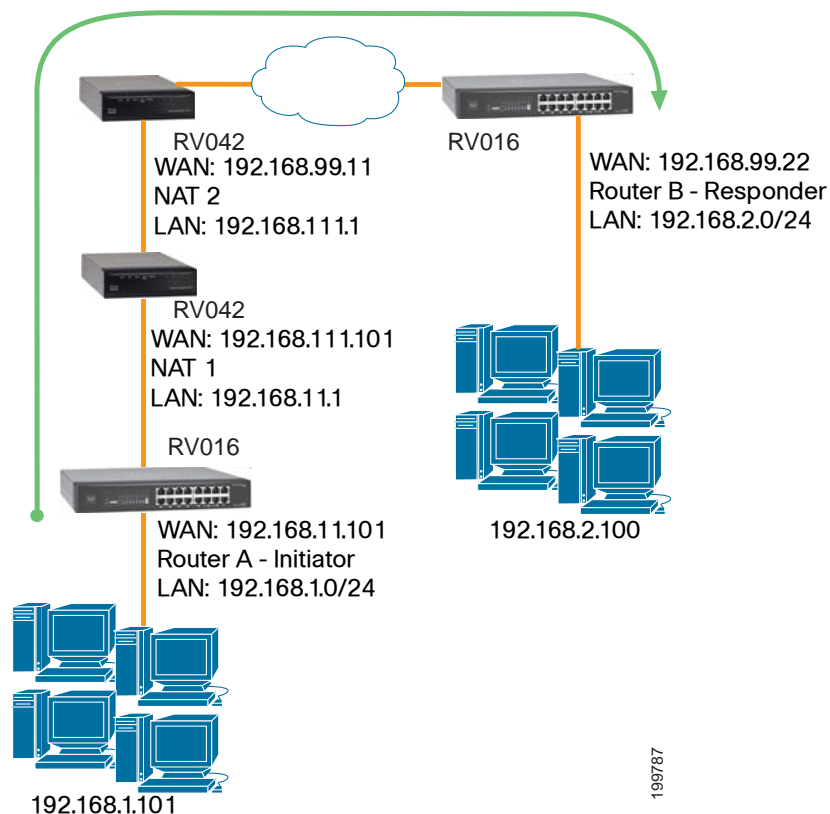
| Field | Values |
|---|------------------------|
| IPSec Setup | |
| Keying Mode | IKE with Preshared Key |
| Phase 1 Encryption | DES |
| Phase 1 Authentication | MD5 |
| Phase 1 SA Life Time | 28800 |
| Perfect Forward Secrecy | Enabled |
| Phase 2 DH Group | Group 1 - 768 bit |
| Phase 2 Encryption | DES |
| Phase 2 Authentication | MD5 |
| Phase 2 SA Life Time | 3600 |
| Preshared Key | 13572468#123456789 |
| Minimum Preshared Key Complexity | Enabled |
| Advanced | Default settings |

IPSec NAT Traversal

Overview

Network Address Translation (NAT) traversal is a technique developed so that data protected by IPSec can pass through a NAT. Since IPSec provides integrity for the entire IP datagram, any changes to the IP addressing will invalidate the data. To resolve this issue, NAT traversal appends a new IP and UDP header to the incoming datagram, ensuring that no changes are made to the incoming datagram stream.

In the following scenario, Router A initiates IKE negotiation, while Router B is the responder.



NOTE Both the IPSec initiator and responder must support the mechanism for detecting the NAT router in the path and changing to a new port, as defined in RFC 3947.

Configuration of Router A

Follow these instructions for Router A.

-
- STEP 1** Launch the web browser for a networked computer, designated PC 1.
 - STEP 2** Access the configuration utility of Router A.
 - STEP 3** Click **VPN > Gateway to Gateway** in the navigation tree.
 - STEP 4** Enter a name in the *Tunnel Name* field.
 - STEP 5** For the VPN Tunnel setting, select **Enable**.
 - STEP 6** For the Local Security Gateway Type, select **IP Only**. The WAN IP address of Router A will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter Router A's local network settings in the *IP Address* and *Subnet Mask* fields.
 - STEP 7** For the Remote Security Gateway Type, select **IP Only**. Enter Router B's WAN IP address in the *IP Address* field.
 - STEP 8** For the Remote Security Group Type, select **Subnet**. Enter Router B's local network settings in the *IP Address* and *Subnet Mask* fields.
 - STEP 9** In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.
 - STEP 10** In the *Preshared Key* field, enter a string for this key, for example, 13572468.
 - STEP 11** Click **Advanced Settings**.
 - STEP 12** Check the **NAT Traversal** box to enable this feature.
 - STEP 13** Click **Save**.
 - STEP 14** Proceed to the next section, [Configuration of Router B, page 185](#).
-

Configuration of Router B

Follow these instructions for Router B.

-
- STEP 1** Launch the web browser for a networked computer, designated PC 2.
 - STEP 2** Access the configuration utility of Router B.
 - STEP 3** Click **VPN > Gateway to Gateway** in the navigation tree.
 - STEP 4** Enter a name in the *Tunnel Name* field.
 - STEP 5** For the VPN Tunnel setting, select **Enable**.
 - STEP 6** For the Local Security Gateway Type, select **IP Only**. The WAN IP address of Router B will be automatically detected.

For the Local Security Group Type, select **Subnet**. Enter Router B's local network settings in the *IP Address* and *Subnet Mask* fields.
 - STEP 7** For the Remote Security Gateway Type, select **IP Only**. Enter the WAN IP address of the NAT 2 router in the *IP Address* field.
 - STEP 8** For the Remote Security Group Type, select **Subnet**. Enter Router A's local network settings in the *IP Address* and *Subnet Mask* fields.
 - STEP 9** In the IPSec Setup section, select the appropriate encryption, authentication, and other key management settings.
 - STEP 10** In the *Preshared Key* field, enter a string for this key, for example, 13572468.
 - STEP 11** Click **Advanced Settings**.
 - STEP 12** Check the **NAT Traversal** box to enable this feature.
 - STEP 13** Click **Save**.
-

Bandwidth Management

This scenario explains how to ensure Quality of Service (QoS) on Vonage Voice over Internet Protocol (VoIP) phone service. This example uses Vonage; however, similar instructions will apply to other VoIP services. Refer to these topics:

- [Creation of New Services, page 186](#)
- [Creation of New Bandwidth Management Rules, page 187](#)

Creation of New Services

Create two new services, Vonage VoIP and Vonage 2.

-
- STEP 1** Visit Vonage's website at <http://www.vonage.com>. Find out the ports used for Vonage VoIP service.
 - STEP 2** Access the router's configuration utility.
 - STEP 3** Click the **System Management** tab.
 - STEP 4** On the *Bandwidth Management* page, click **Service Management**.
 - STEP 5** On the *Service Management* page, enter a name, such as Vonage VoIP, in the *Service Name* field.
 - STEP 6** From the *Protocol* drop-down menu, select the protocol the VoIP service uses. For example, some VoIP devices use UDP.
 - STEP 7** Enter its SIP port range in the *Port Range* fields. For example, you can set the Port Range to 5060 to 5070 to make sure that all active ports are covered.
 - STEP 8** Click **Add to List**.
 - STEP 9** Add a second service. Enter a name, such as Vonage 2, in the *Service Name* field.
 - STEP 10** From the *Protocol* drop-down menu, select **UDP**.

STEP 11 Enter the RTP port range in the *Port Range* fields. These are required for both incoming and outgoing traffic. For example, you can set the Port Range to 10000 to 25000 to make sure that all active ports are covered.

STEP 12 Click **Add to List**.

STEP 13 Click **Save** to save your changes.

Creation of New Bandwidth Management Rules

Create four new rules: Vonage VoIP (Upstream), Vonage VoIP (Downstream), Vonage 2 (Upstream), and Vonage 2 (Downstream).

STEP 1 Set up a rule for upstream bandwidth for Vonage 1:

- a. On the *Bandwidth Management* page, select **Vonage VoIP** from the *Service* drop-down menu.
- b. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default value.
- c. From the *Direction* drop-down menu, select **Upstream** for outbound traffic.
- d. In the *Min. Rate* field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
- e. In the *Max. Rate* field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
- f. Select **Enable** to enable this rule.
- g. After you have set up the rule, click **Add to list**.

STEP 2 Set up the rule for downstream bandwidth for Vonage 1.

- a. Select **Vonage VoIP** from the *Service* drop-down menu.
- b. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default value.
- c. From the *Direction* drop-down menu, select **Downstream** for inbound traffic.
- d. In the *Min. Rate* field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.

- e. In the *Max. Rate* field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
- f. Select **Enable** to enable this rule.
- g. After you have set up the rule, click **Add to list**.

STEP 3 Set up an upstream rule for Vonage 2.

- a. Select **Vonage 2** from the *Service* drop-down menu.
- b. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, **0**.
- c. From the *Direction* drop-down menu, select **Upstream** for outbound traffic.
- d. In the *Min. Rate* field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
- e. In the *Max. Rate* field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
- f. Select **Enable** to enable this rule.
- g. After you have set up the rule, click **Add to list**.

STEP 4 Set up a downstream rule for Vonage 2.

- a. Select **Vonage 2** from the *Service* drop-down menu.
- b. Enter the IP address or range you need to control. To include all internal IP addresses, keep the default, **0**.
- c. From the *Direction* drop-down menu, select **Downstream** for inbound traffic.
- d. In the *Min. Rate* field, enter the minimum rate for the guaranteed bandwidth. For example, you can set a minimum rate of 40 kbit/sec.
- e. In the *Max. Rate* field, enter the maximum rate for the maximum bandwidth. For example, you can set a maximum rate of 80 kbit/sec.
- f. Select **Enable** to enable this rule.
- g. After you have set up the rule, click **Add to list**.

STEP 5 Click **Save**.



Specifications

NOTE Specifications are subject to change without notice.

RV042

NOTE This product (RV042) is intended to be supplied by a Listed or "Class 2" Power Unit, which has an output rate of 12V DC, 1.0A at minimum.

Specifications

| | |
|----------------------|--|
| Model | Cisco RV042 |
| Standards | IEEE 802.3, 802.3u |
| Ports | 4 10/100 RJ-45 ports, 1 10/100 RJ-45 Internet port, 1 10/100 RJ-45 DMZ/Internet port |
| Button | Reset |
| Cabling Type | Category 5 Ethernet |
| Status Lights (LEDs) | System, Internet, DMZ/Internet, DMZ Mode, Diag, 1 to 4 |
| Operating System | Linux |

Performance

| | |
|------------------|----------|
| NAT Throughput | 100 Mbps |
| IPSec Throughput | 59 Mbps |

Security

| | |
|--------------|------------------|
| Firewall | SPI Firewall |
| Access Rules | Up to 50 entries |

| | |
|-----------------|--|
| Port Forwarding | Up to 30 entries |
| Port Triggering | Up to 30 entries |
| URL Filtering | Static list by domain or keywords (included), dynamic filtering through Cisco ProtectLink Web service (optional) |

Network

| | |
|------------------|--|
| Dual WANs | Can be configured for Smartlink backup or load balance |
| Protocol Binding | Protocols can be bound to particular WAN port under load balancing |
| DHCP | DHCP Server, DHCP Client |
| DNS | DNS Proxy, Dynamic DNS (DynDNS, 3322) |
| NAT | Many-to-One, One-to-One |
| DMZ | DMZ port, DMZ host |
| Routing | Static and RIP v1, v2 |

QoS

| | |
|-------------------|---|
| Port-based QoS | Configurable per LAN port |
| Service based QoS | Supports rate control or priority |
| Rate Control | Upstream/downstream bandwidth can be configured per service |
| Priority | Each service can be mapped to one of the 3 priority levels |

VPN

| | |
|-----------------|--|
| IPSec | 50 IPSec tunnels for branch office connectivity |
| QuickVPN | 50 QuickVPN users for remote client access |
| PPTP | Built-in PPTP server supporting 5 PPTP clients |
| Encryption | DES, 3DES, AES-128, AES-192, AES-256 |
| Authentication | MD5, SHA1 |
| IPSec NAT-T | Supported for gateway-to-gateway and client-to-gateway tunnels |
| VPN Passthrough | PPTP, L2TP, IPSec |

Management

| | |
|-----------|--------------------------|
| Web-Based | HTTPS |
| SNMP | Supports SNMP v1 and v2c |
| Log | Syslog, Email Alert |

Environmental

| | |
|--------------------|--|
| Dimensions | 5.12 x 1.52 x 7.87 in. W x H x D (130 x 38.5 x 200 mm) |
| Unit Weight | 1.27 lb (0.576 kg) |
| Power | 12V, 1A |
| Certifications | FCC Class B, CE Class B |
| Operating Temp. | 0 to 40°C (32 to 104°F) |
| Storage Temp. | 0 to 70°C (32 to 158°F) |
| Operating Humidity | 10 to 85% noncondensing |
| Storage Humidity | 5 to 90% noncondensing |

RV042G

NOTE This product (RV042G) is intended to be supplied by a Listed or Class 2 Power Unit, which has an output rate of 12V DC, 1.0A at minimum.

Specifications

| | |
|----------------------|---|
| Model | Cisco RV042G |
| Standards | IEEE 802.3, 802.3u |
| Ports | 4 10/100/1000 RJ-45 ports, 1 10/100/1000 RJ-45 Internet port, 1 10/100/1000 RJ-45 DMZ/Internet port |
| Button | Reset |
| Cabling Type | Category 5 Ethernet |
| Status Lights (LEDs) | System, Internet, DMZ/Internet, DMZ Mode, Diag, 1 to 4 |

| | |
|--------------------|---|
| Operating System | Linux |
| Performance | |
| NAT Throughput | 800 Mbps |
| IPSec Throughput | 75 Mbps |
| Security | |
| Firewall | SPI Firewall |
| Access Rules | Up to 50 entries |
| Port Forwarding | Up to 30 entries |
| Port Triggering | Up to 30 entries |
| URL Filtering | Static list by domain or keywords (included) Note: Cisco ProtectLink Web service is not available on this model. |
| Network | |
| Dual WANs | Can be configured for Smartlink backup or load balance |
| Protocol Binding | Protocols can be bound to particular WAN port under load balancing |
| DHCP | DHCP Server, DHCP Client |
| DNS | DNS Proxy, Dynamic DNS (DynDNS, 3322) |
| NAT | Many-to-One, One-to-One |
| DMZ | DMZ port, DMZ host |
| Routing | Static and RIP v1, v2 |
| QoS | |
| Port-based QoS | Configurable per LAN port |
| Service based QoS | Supports rate control or priority |
| Rate Control | Upstream/downstream bandwidth can be configured per service |
| Priority | Each service can be mapped to one of the 3 priority levels |

VPN

IPSec 50 IPSec tunnels for branch office connectivity

QuickVPN 50 QuickVPN users for remote client access

PPTP Built-in PPTP server supporting 5 PPTP clients

Encryption DES, 3DES, AES-128, AES-192, AES-256

Authentication MD5, SHA1

IPSec NAT-T Supported for gateway-to-gateway and client-to-gateway tunnels

VPN Passthrough PPTP, L2TP, IPSec

Management

Web-Based HTTPS

SNMP Supports SNMP v1 and v2c

Log Syslog, Email Alert

Environmental

Dimensions 5.12 x 1.52 x 7.87 in. W x H x D (130 x 38.5 x 200 mm)

Unit Weight 1.27 lb (0.576 kg)

Power 12V, 1A

Certifications FCC Class B, CE Class B

Operating Temp. 0 to 40°C (32 to 104°F)

Storage Temp. 0 to 70°C (32 to 158°F)

Operating Humidity 10 to 85% noncondensing

Storage Humidity 5 to 90% noncondensing

Cisco RV082

Specifications

| | |
|----------------------|--|
| Model | Cisco RV082 10/100 8-port VPN router |
| Standards | IEEE 802.3, 802.3u |
| Ports | 8 10/100 RJ-45 ports, 1 10/100 RJ-45 Internet port, 1 10/100 RJ-45 DMZ/Internet port |
| Button | Reset |
| Cabling Type | Category 5 Ethernet |
| Status Lights (LEDs) | System, Internet, DMZ/Internet, DMZ Mode, Diag, 1 to 8 |
| Security Features | SPI Firewall, DES, 3DES and AES encryption for IPSec VPN Tunnel |
| Operating System | Linux |

Performance

| | |
|------------------|----------|
| NAT Throughput | 200 Mbps |
| IPSec Throughput | 97 Mbps |

Security

| | |
|-----------------|--|
| Firewall | SPI Firewall |
| DoS Prevention | Block various Denial of Service attacks |
| Access Rules | Up to 50 entries |
| Port Forwarding | Up to 30 entries |
| Port Triggering | Up to 30 entries |
| Blocking | Java, Cookies, ActiveX, HTTP Proxy |
| URL Filtering | Static list by domain or keywords (included), dynamic filtering through Cisco ProtectLink Web service (optional) |

Network

| | |
|-----------|--|
| Dual WANs | Can be configured for Smartlink backup or load balance |
| WAN Type | DHCP, Static IP, PPPoE, PPTP, Dynamic DNS |

| | |
|-------------------|--|
| Protocol Binding | Protocols can be bound to particular WAN port under load balancing |
| DHCP | DHCP Server, DHCP Client, DHCP Relay |
| DNS | DNS Proxy, Dynamic DNS (DynDNS, 3322) |
| NAT | Many-to-One, One-to-One |
| DMZ | DMZ port, DMZ host |
| Routing | Static and RIP v1, v2 |
| QoS | |
| Port-based QoS | Configurable per LAN port |
| Service based QoS | Supports rate control or priority |
| Rate Control | Upstream/downstream bandwidth can be configured per service |
| Priority | Each service can be mapped to one of the 3 priority levels |
| VPN | |
| IPSec | 100 IPSec tunnels for branch office connectivity |
| QuickVPN | 50 QuickVPN users for remote client access |
| PPTP | Built-in PPTP server supporting 5 PPTP clients |
| Encryption | DES, 3DES, AES-128, AES-192, AES-256 |
| Authentication | MD5, SHA1 |
| IKE | Support Internet Key Exchange |
| IPSec NAT-T | Supported for gateway-to-gateway and client-to-gateway tunnels |
| Advanced Options | DPD, Split DNS, VPN Backup |
| VPN Passthrough | PPTP, L2TP, IPSec |
| Management | |
| Web-Based | HTTPS |
| SNMP | Supports SNMP v1 and v2c |

| | |
|----------------------|--|
| Log | Syslog, Email Alert, VPN Tunnels, Status Monitor |
| Environmental | |
| Dimensions | 11.00 x 1.75 x 9.50 W x H x D (279.4 x 44.45 x 241.3 mm) |
| Unit Weight | 3.25 lb (1.475 kg) |
| Power | AC 100~240V, 50~60 Hz |
| Certifications | FCC Class B, CE Class A |
| Operating Temp. | 0 to 40°C (32 to 104°F) |
| Storage Temp. | 0 to 70°C (32 to 158°F) |
| Operating Humidity | 10 to 85% noncondensing |
| Storage Humidity | 5 to 90% noncondensing |

Cisco RV016

Specifications

| | |
|----------------------|---|
| Model | Cisco RV016 10/100 16-port VPN router |
| Standards | IEEE 802.3, 802.3u |
| Ports | 16 10/100 RJ-45 ports, including 2 Internet ports, 1 DMZ port, 8 LAN ports, and 5 Configurable Internet/LAN ports |
| Button | Reset |
| Cabling Type | Category 5 Ethernet |
| Status Lights (LEDs) | Diag, System, LAN/Act 1 to 13, Internet/Act 1 to 7, DMZ |
| Operating System | Linux |

Performance

| | |
|------------------|----------|
| NAT Throughput | 200 Mbps |
| IPSec Throughput | 97 Mbps |

Security

Firewall/SPI Firewall

| | |
|-----------------|--|
| DoS Prevention | Blocks various Denial of Service attacks |
| Access Rules | Up to 50 entries |
| Port Forwarding | Up to 30 entries |
| Port Triggering | Up to 30 entries |
| URL Filtering | Static list by domain or keywords (included), dynamic filtering through Cisco ProtectLink Web service (optional) |

Network

| | |
|------------------|---|
| Multi-WANs | Support up to 7 WAN ports with load balancing, where certain WAN ports can be dedicated to specified IP ranges and services |
| WAN Type | DHCP, Static IP, PPPoE, PPTP, Dynamic DNS |
| Protocol Binding | Protocols can be bound to particular WAN port |
| DHCP | DHCP Server, DHCP Client |
| DNS | DNS Proxy, Dynamic DNS (DynDNS, 3322) |
| NAT | Many-to-One, One-to-One |
| DMZ | DMZ port, DMZ host |
| Routing | Static and RIP v1, v2 |

QoS

| | |
|-------------------|---|
| Port-based QoS | Configurable per LAN port |
| Service based QoS | Supports rate control or priority |
| Rate Control | Upstream/downstream bandwidth can be configured per service |
| Priority | Each service can be mapped to one of the 3 priority levels |

VPN

| | |
|----------|--|
| IPSec | 100 IPSec tunnels for branch office connectivity |
| QuickVPN | 50 QuickVPN users for remote client access |

| | |
|----------------------|---|
| PPTP | Built-in PPTP server supporting 10 PPTP clients |
| Encryption | DES, 3DES, AES-128, AES-192, AES-256 |
| Authentication | MD5, SHA1 |
| IKE | Support Internet Key Exchange |
| IPSec NAT-T | Supported for gateway-to-gateway and client-to-gateway tunnels |
| Dead Peer Detection | Support for DPD |
| VPN Passthrough | PPTP, L2TP, IPSec |
| Management | |
| Web-Based | HTTPS |
| SNMP | Supports SNMP v1 and v2c |
| Log | Syslog, Email Alert, VPN Tunnels, Status Monitor |
| Environmental | |
| Dimensions | 11.00 x 1.75 x 9.50 in. W x H x D (279.4 x 44.45 x 241.3 mm) |
| Unit Weight | 3.25 lb (1.475 kg) |
| Power | AC 100~240V, 50 to 60 Hz |
| Certifications | FCC Class B, CE Class A |
| Operating Temp. | 0 to 40°C (32 to 104°F) |
| Storage Temp. | 0 to 70°C (32 to 158°F) |
| Operating Humidity | 10 to 85% noncondensing |
| Storage Humidity | 5 to 90% noncondensing |

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of your Cisco Small Business router.

| Support | |
|---|--|
| Cisco Small Business Support Community | www.cisco.com/go/smallbizsupport |
| Cisco Small Business Support and Resources | www.cisco.com/go/smallbizhelp |
| Cisco Small Business Firmware Downloads | www.cisco.com/go/software |
| Product Documentation | |
| Cisco Small Business Routers Documentation | 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 |