



# Quick Start Guide



Cisco Small Business

## WRV210 Wireless-G VPN Router with RangeBooster

### Package Contents

- WRV210 Router
- Ethernet Cable
- Power Adapter
- Product CD-ROM
- Quick Start Guide

# Welcome

Thank you for choosing the Cisco WRV210, a Wireless-G VPN Router with RangeBooster. The WRV210 router is a secure wireless networking device for your small business.

This guide describes how to physically install your WRV210 and how to install and launch the WRV210 Configuration Utility.

## 1 Before You Begin

Before you begin the installation, make sure that you have the following equipment and services:

- Broadband Internet access account
- PC with Ethernet interface (RJ-45)

## 2 Getting to Know the WRV210

### Front Panel



**POWER**—(Green) Shines steady when the router is powered on.

**DMZ**—(Green) Shines steady when the router has an available DMZ port. If the LED is flashing, the router is sending or receiving data over the DMZ port. A DMZ can be configured to allow Internet traffic to access a specified computer on your network, while protecting the rest of your LAN from exposure.

**INTERNET**—(Green) Shines steady when the router is connected to your broadband network device (cable, DSL modem, or other). Flashes when the router is sending or receiving data over the Internet port.

**WIRELESS**—(Green) Shines steady when there is a successful wireless connection. Flashes when the router is actively sending or receiving data over the wireless network.

**1-4 (ETHERNET)**—(Green) Shines steady when a device is connected to the specified port. Flashes when the router is actively sending or receiving data over the specified port.

## Back Panel



**POWER**—Connects the router to power, using the AC power cable.

**RESET**—Performs the following functions:

- Warm reboot—Press the button for one second to restart the router without losing any of the current configuration settings.
- Factory reset—Press the button for approximately 15 seconds to reset the router to the factory default settings. You can also restore the factory default settings from the Administration > Factory Defaults page in the web-based Configuration Utility.

**INTERNET**—Connects the router to your broadband network device (cable, DSL modem, or other).

**1-4 (ETHERNET)**—Connects the router to your PCs and network devices.

## Default Settings

Parameter	Value
Username	admin
Password	admin
LAN IP	192.168.1.1
DHCP Range	192.168.1.100 to 192.168.1.253

# 3

## Installing the WRV210

### Placement Options

You can place the router horizontally on a desktop or mount it on the wall.

#### Desktop Option

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

#### Wall Option

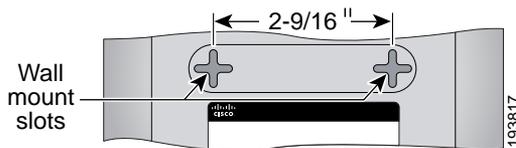
To mount the router on the wall, follow these steps.

---

**STEP 1** Determine where you want to mount the router.

**STEP 2** Install two screws (not supplied) 2-9/16 in. apart (approximately 6.45 cm.) Leave about 1/8 in. (about 3 mm) of the head exposed.

**STEP 3** With the back panel pointing up (if installing vertically), position the router so that the wall-mount crisscross slots on the bottom panel line up with the two screws.



**STEP 4** Place the wall-mount slots over the screws and slide the router down until the screws fit snugly into the wall-mount slots.

---

# 4

## Connecting the Equipment

- STEP 1** Make sure that all of your network hardware is powered off, including the router, PCs, and broadband network device.
- STEP 2** Connect one end of an Ethernet cable to one of the LAN ports (labeled 1-4) on the back of the router, and the other end to an Ethernet port on a PC.



**NOTE** You must connect one computer with an Ethernet cable for the purpose of the initial configuration. After you complete the initial configuration, administrative tasks can be performed from a wireless connection.



254174

- STEP 3** Repeat the previous step to connect more PCs, a switch, or other network devices to the router.

**STEP 4** Connect an Ethernet cable from the Broadband network device to the Internet port on the router's back panel.



734075

**STEP 5** Connect the power adapter to the router's Power port, and then insert the other end into an electrical outlet.



**NOTE**

---

Use only the power adapter that is supplied with the router. Using a different power adapter could damage the router.

---



734076

The Power and Internet LEDs on the front panel will shine green as soon as the power adapter is connected properly.

**STEP 6** Power on the connected devices and the broadband network device.

The hardware installation is now complete.

---

# 5

## Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the LED states, as described in [Getting to Know the WRV210, page 1](#).
- If the LED does not show the expected status, check the cable connections.



**NOTE**

---

If you need help resolving a problem, visit the Cisco Small Business Support Community at [www.cisco.com/go/smallbizsupport](http://www.cisco.com/go/smallbizsupport). For technical documentation and other links, see [Where to Go From Here, page 14](#).

---

# 6

## Getting Started with the Configuration

The following instructions explain how to set up the Internet connection, configure the wireless network, and secure the wireless network.

### Setting Up the Internet Connection

Before you begin, make sure that you have the setup information for the specific type of Internet connection for your Internet Service Provider (ISP). The installation technician from the ISP should have provided this information when installing the broadband connection. If not, contact your ISP to request the settings.

---

**STEP 1** Using one of the PCs that you previously connected to the router, start your web browser.



**NOTE**

---

You must complete the initial installation from a PC that is physically connected to the router. You cannot configure the router from a PC that is connected wirelessly.

---

**STEP 2** To connect to the web-based Configuration Utility, enter the router's default LAN IP address in the browser's Address bar:  
<http://192.168.1.1>

Address	<a href="http://192.168.1.1">http://192.168.1.1</a>
---------	---

A password request prompt appears.

**STEP 3** Enter the following user name and password, and then click **OK**.

- User name: **admin**
- Password: **admin**



---

**NOTE** For added security, you should later set a new administrator password by using the Administration > Management page in the web-based Configuration Utility.

---

The web-based Configuration Utility appears, displaying the Basic Setup page.

**STEP 4** In the **Internet Setup** section, choose the **Internet Connection Type** that was specified by your ISP:

- **Automatic Configuration - DHCP:** This type of connection allows your router to obtain an IP address dynamically from your ISP's network.
- **Static IP:** This type of connection requires that your ISP assigned a fixed IP address to your account.
- **PPPoE:** This type of connection requires a login for each Internet connection.
- **PPTP:** This type of connection is used in Europe only.
- **L2TP:** This type of connection is used mostly in Europe.
- **Heart Beat Signal:** This type of connection is used in Australia.

**STEP 5** Enter the information that your ISP provided. The fields vary, depending on the selected connection type.

- **IP Address, Subnet Mask, and Default Gateway:** Enter the information that the ISP provided for your fixed IP address.
- **Primary DNS and Secondary DNS:** Enter the IP address of at least one Domain Name System (DNS) server for your ISP.

- **Username and Password:** Enter the login information for your ISP account.
- **PPTP Server or Authentication Server:** Enter the server IP address or name, as provided by your ISP.
- **Host Name and Domain Name:** Complete these fields only if required by your ISP (often required by cable ISPs).
- **Connect on Demand and Max Idle Time:** Choose this option to automatically disconnect from the Internet if the connection is idle for the specified number of seconds. This option is helpful if you are billed based on the amount of connection time.
- **Keep Alive:** Choose this option to remain connected to the Internet regardless of the level of activity.

**STEP 6** When you are finished entering the Internet connection settings, click **Save** to save the changes.

**STEP 7** To test the Internet connection, start a web browser on any connected computer and enter a valid website address, such as [www.cisco.com](http://www.cisco.com).

---

## Configuring the Wireless Network

---

**STEP 1** To configure the router for the wireless network, click **Wireless > Basic Wireless Settings** in the navigation tree.

**STEP 2** From the **Wireless Network Mode** drop-down list, choose the appropriate mode for your network devices:

- **Mixed:** Supports Wireless-G and Wireless-B devices
- **G-Only:** Supports only Wireless-G devices
- **B-Only:** Supports only Wireless-B devices
- **Disable:** Disables wireless networking

**STEP 3** Enter the following information in the SSID table to configure up to four wireless networks:

- **Wireless Network Name (SSID):** Enter a name for your network to identify it to the wireless devices that connect to the router.
- **TX Rate Limitation:** Keep the default value for the transmission rate.

- **SSID Broadcast:** Click **Enabled** to allow all wireless devices in range to see the SSID for this wireless network. Click **Disabled** for increased privacy. With this feature disabled, your users will need to know the SSID in order to configure their wireless connections, since the SSID will not appear automatically when they scan the area for available networks.
- **WMM:** Check this box to enable Wi-Fi Multimedia. This feature provides basic prioritization of data packets to support voice and video applications.

**STEP 4** From the drop-down list, choose the **Wireless Channel** to be used by the wireless network devices. In most cases, the default selection should be sufficient, but you may need to change this setting if there is interference from other wireless networks in the area.



---

**NOTE** During the initial configuration, ignore the Wireless LAN Schedule section of this page. Later, if needed, you can configure a schedule to enable or disable each wireless network during specified days and times.

---

**STEP 5** When you are finished entering the wireless network settings, click **Save** to apply the changes.

---

## Securing the Wireless Network

---

**STEP 1** To choose the security options for your network, click **Wireless > Wireless Security** in the navigation tree.

**STEP 2** From the **Select SSID** drop-down list, choose the SSID that you want to configure. You will need to repeat this procedure for each SSID that you enabled on the Basic Wireless Settings page.

**STEP 3** Choose the **Security Mode**. Cisco recommends using the highest level of security that is supported by your network devices. Choose from the following options:

- **WEP:** Weak security with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA.

- **WPA Personal:** Provides strong wireless security with advanced encryption. Choose **WPA Personal** (TKIP or AES encryption), **WPA2 Personal** (AES encryption), **WPA2 Personal Mixed** (TKIP or AES encryption).
- **WPA Enterprise:** Strong security using authentication by a RADIUS server that is connected to the router. Choose **WPA Enterprise** (TKIP or AES encryption), **WPA2 Enterprise** (AES), or **WPA2 Enterprise Mixed** (TKIP or AES encryption).
- **RADIUS (WEP):** Weak security (WEP) with a basic encryption method that is not as secure as WPA. WEP may be required if your network devices do not support WPA. Authentication is provided by a RADIUS server that is connected to the router.

**STEP 4** From the **Wireless Isolation within SSID** drop-down list, choose **Enabled** to allow communication and file transfers between all wireless PCs that are connected to this SSID. This feature is useful when setting up a wireless hotspot location. Choose **Disabled** (the default option) to prevent communication and file transfers between the PCs.

**STEP 5** In the final section of the page, enter the required information, based on the chosen security mode, as described below.

**For WPA Enterprise modes and RADIUS (WEP) mode:**

RADIUS Server IP Address:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
RADIUS Server Port:	<input type="text" value="1812"/>

- **RADIUS Server IP Address:** Enter the IP address for the RADIUS server.
- **RADIUS Server Port:** Enter the port number for the RADIUS server.

**For WPA Personal modes and WPA Enterprise modes:**

Encryption:	<input type="text" value="TKIP"/> ▼
Shared Secret:	<input type="text"/>
Key Renewal:	<input type="text" value="3600"/> seconds

- **Encryption:** For WPA Personal and WPA Enterprise, choose either TKIP or AES encryption. The encryption method is chosen automatically for the other WPA modes.
- **Shared Secret:** Enter 8-32 characters. The Shared Secret is also known as a Pre-Shared Key.
  - For WPA Personal, this key also must be configured in the wireless clients who want to connect to the network.
  - For WPA Enterprise and RADIUS, this key is shared between the router and the RADIUS server.
- **Key Renewal:** For all security modes except WEP, enter the interval in seconds. The Key Renewal instructs the router how often it should change the encryption keys. The default is 3600 seconds, which is 1 hour.

### For WEP mode and RADIUS (WEP) mode:

Authentication Type:	<input type="text" value="Open System"/>	<input type="button" value="v"/>
Default Transmit Key:	<input checked="" type="radio"/> 1	<input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Encryption:	<input type="text" value="64 bits"/>	<input type="button" value="v"/> (10 hex digits or 5 ASCII characters)
Passphrase:	<input type="text"/>	<input type="button" value="Generate"/>
Key 1:	<input type="text"/>	
Key 2:	<input type="text"/>	
Key 3:	<input type="text"/>	
Key 4:	<input type="text"/>	

- **Authentication Type:** Choose one of the following options:
  - **Open System:** A wireless client doesn't need to provide a shared key in order to access the wireless network. Any client can associate to the router.
  - **Share Key:** A wireless client must provide the correct shared key in order to to access the wireless network.
- **Default Transmit Key:** To indicate which WEP key to use, select the appropriate Default Transmit Key number.
- **Encryption:** Choose the level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits). Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

- **Passphrase:** If you want to generate a key instead of entering a key manually, type a passphrase in the field. You can enter up to 32 alphanumeric characters. Then click **Generate**. A valid key appears in each of the Key 1 - Key 4 fields.
- **Key 1 - Key 4:** If you did not use the Generate feature, enter a valid WEP key. Do not leave a field blank, and do not enter all zeroes; they are not valid key values.
  - If you chose 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length.
  - If you chose 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0" to "9" and "A" to "F".

**STEP 6** Keep the default values for all other settings.

**STEP 7** Click **Save** to save the changes.

**STEP 8** To test the wireless setup, use the wireless client on any computer to enter the correct SSID and shared key for your wireless network. Verify that you can connect by entering a website address, such as [www.cisco.com](http://www.cisco.com).

Congratulations! The installation of the Wireless-G VPN router with RangeBooster is complete. For more advanced settings and security options, refer to the Administration Guide (see [Where to Go From Here, page 13](#)).

---

# 7

## Suggested Next Steps

The WRV210 is ready for use. It is not necessary to change any settings. However, the following steps are recommended:

- To protect your network, Cisco recommends that you reset the administrative password. Click **Administration > Management** in the navigation tree. In the **Admin Password** field, enter the new password. Enter it again in the **Re-enter to confirm field**. Click **Save** to save your settings.

- If you want to access the Configuration Utility from a PC that is connected wirelessly or is located outside the local network, use the **Local Router Access** section of the Administration > Management page to enable these features.

As needed, you can use the Configuration Utility to customize the router and to monitor the status of your network. Below is a brief guide to the main modules of the Configuration Utility.

- **Setup:** Set up the Internet connection, configure the Data and Voice VLANs, set up Dynamic DNS services for domain name resolution, clone a MAC address if required by your ISP, and set up advanced routing.
- **Wireless:** Adjust the basic wireless settings and security settings, restrict wireless network access, and configure advanced wireless settings. You also can configure a Wireless Distribution System (WDS) to allow wireless clients to connect through a repeater such as WAP54GP or WAP54GPE.
- **Firewall:** The default firewall settings provide security for your network. You can adjust the basic settings, or allow public access to specified services by enabling port forwarding or port triggering or by setting up a DMZ. You also can restrict your users' access to the Internet by configuring access policies and URL filtering.
- **VPN:** Configure a Virtual Private Network (VPN) to allow network access to your remote workers and business travelers.
- **QoS:** Adjust the default Quality of Service (QoS) settings to prioritize traffic for demanding, real-time applications such as videoconferencing.
- **Administration:** Manage access, set up alerts and system logs, perform diagnostic tests, back up and restore the configuration, upgrade the firmware, reboot the router, and revert to factory default settings.
- **Status:** Monitor the status and view statistics for your router, local network, wireless network, and VPN.

# 8

## Where to Go From Here

Support	
Cisco Small Business Support Community	<a href="http://www.cisco.com/go/smallbizsupport">www.cisco.com/go/smallbizsupport</a>
Online Technical Support and Documentation (Login Required)	<a href="http://www.cisco.com/support">www.cisco.com/support</a>
Phone Support Contacts	<a href="http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html">www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html</a>
Software Downloads (Login Required)	Go to <a href="http://tools.cisco.com/support/downloads">tools.cisco.com/support/downloads</a> , and enter the model number in the Software Search box.
Product Documentation	
Administration Guides for Cisco Small Business Routers	<a href="http://www.cisco.com/en/US/products/ps9923/prod_maintenance_guides_list.html">www.cisco.com/en/US/products/ps9923/prod_maintenance_guides_list.html</a>
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	<a href="http://www.cisco.com/web/partners/sell/smb">www.cisco.com/web/partners/sell/smb</a>
Cisco Small Business Home	<a href="http://www.cisco.com/smb">www.cisco.com/smb</a>
Marketplace	<a href="http://www.cisco.com/go/marketplace">www.cisco.com/go/marketplace</a>

## Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883



Cisco, Cisco Systems, the Cisco logo, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website 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. (0705R)

© 2009 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.