NETGEAR ProSafe 802.11g Wireless Access Point WG302v2 Reference Manual

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10146-01
May 2006

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to *http://www.NETGEAR.com*. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at: *http://www.NETGEAR.com/* through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and ProSafe is a trademark, of NETGEAR, INC. Windows is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

Statement of Conditions

NOTE: In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

NOTE: Modifications made to the product, unless expressly approved by NETGEAR, could void the user's authority to operate the equipment. NETGEAR does not assume any liability that may occur due to such condition.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

ProSafe 802.11g Wireless Access Point WG302v2

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

FCC ID: PY3WG302v2

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

FCC Statement

Declaration of Conformity

We NETGEAR,
4500 Great America Parkway
Santa Clara, CA 95054, USA
Tel: +1 408 907 8000
declare under our sole responsibility that the product(s)
WG302v2 *(Model Designation)*
ProSafe™ 802.11g Wireless Access Point *(Product Name)*
complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or locate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Placement and Range Guidelines

Indoors, computers can connect over 802.11 wireless networks at a maximum range of several hundred feet for 802.11b/g devices. However, the operating distance or range of your wireless connection can vary significantly, based on the physical placement of the wireless access point.

For best results, identify a location for your wireless access point according to these guidelines:

- Away from potential sources of interference, such as PCs, large metal surfaces, microwaves, and 2.4 GHz cordless phones.
- In an elevated location such as a high shelf that is near the center of the wireless coverage area for all mobile devices.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

RF Exposure Warning for North America, and Australia

WARNING! To meet FCC and other national safety guidelines for RF exposure, the antennas for this device (see below) must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be colocated with other antenna or radio transmitter.

Antenna Statement for North America and Australia

In addition to its own antenna, the WG302v2 device has been approved for use with the following detachable antennas and antenna cables.

Approved Antennas	Antenna Gain and type	Approved Antenna Cable	Antenna Cable Length	Maximum Transmitted Power[a]
NETGEAR ANT24D18v2	14.5 dBi, directional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	18 dBm + 14.5 dBi ant.
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	18 dBm + 9 dBi ant.
NETGEAR ANT24O5	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	18 dBm + 5 dBi ant.

[a] WG302v2 maximum radiated power in North America and Australia: 19 dBm – cable loss + antenna gain

Please see the product specifications at *http://kbserver.netgear.com/products/wg302.asp* for an updated list of wireless accessories approved to be used with the WG302v2.

Industry Canada Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference Causing Equipment Regulations ICES 003.

Cet appareil numerique de classe B respecte les exigences du reglement du Canada sur le materiel brouilleur NMB-003.

The device is certified to the requirements of RSS-210 for 2.4 GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

Europe – Declaration of Conformity in Languages of the European Community

Èesky [Czech]	*NETGEAR Inc.* tímto prohlašuje, _e tento Radiolan je ve shodě se základními po_adavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
ÅëëçíéêÞ [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spÍňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below.

Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

This device may be operated **indoors or outdoors** in all countries of the European Community using the 2.4GHz band: Channels 1 – 13, except where noted below:

- In **Italy** the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In **France** outdoor operation is only permitted using the 2.4 – 2.454 GHz band: Channels 1 – 7.
- **Belgium** requires notifying spectrum agency if deploying >300meter wireless links in outdoor public areas using 2.4GHz band.

European Spectrum Usage Rules - Effective April 11, 2006	
Country	**2.4-2.4835 (GHz)** **Channels: 1 to 13** **(Except Where Noted)**
ALL EC Countries	Indoor or Outdoor
Belgium	Indoor or Outdoor
France	Indoor Ch. 1-13 Outdoor 1-7 Only
Greece	Indoor Only
Italy	Indoor (Outdoor w/License)
Turbo Mode	Same 2.4 GHz rules as above
AdHoc Mode	Same 2.4 GHz rules as above

Antenna Statement for the European Community

Please note that the 100mW EIRP limit and regulations could vary in Europe from country to country. Please check the regulations in your country.

The antenna cable type and length must comply with European regulations. Refer to the table below for approved antenna and cable accessories.

In addition to its own antenna, the WG302v2 device has been approved for use with the following detachable antennas and antenna cables:

Approved Antennas	Antenna Gain and type	Approved Antenna Cable	Minimum Antenna Cable Length	Minimum Antenna Cable Attenuation	Maximum Transmitted Power[a]
NETGEAR ANT24D18v2	14.5 dBi, directional outdoor/indoor	NETGEAR ACC-10314-05	30 m	18 dB	-3 dBm + 14.5 dBi = 15 dBm EIRP
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-04 or ACC-10314-05	10 m	6.1 dB	8.9 dBm + 9 dBi = 17.9 dBm EIRP
NETGEAR ANT24O5	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m	1.1 dB	14 dBm + 5 dBi = 19 dBm EIRP

[a] WG302v2 maximum radiated power in the European Community: 15 dBm – cable loss + antenna gain

Please go to *http://www.NETGEAR.com* and use the search feature to find an updated list of wireless accessories approved to be used with the WG302v2 in the European Community.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe 802.11g Wireless Access Point gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe 802.11g Wireless Access Point has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Product and Publication Details

Model Number:	WG302v2
Publication Date:	May 2006
Product Family:	Wireless Access Point
Product Name:	ProSafe 802.11g Wireless Access Point
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10146-01

Contents

About This Manual

Chapter 1
Introduction

Chapter 2
Basic Installation and Configuration

Chapter 3
Management and Information

Chapter 4
Advanced Configuration

Chapter 5
Troubleshooting

Appendix A
Related Documents

Appendix B
Specifications

Appendix C
Command Line Reference

About This Manual

The *NETGEAR® ProSafe™ Wireless Access Point 802.11g WG302 Reference Manual* describes how to install, configure and troubleshoot the ProSafe 802.11g Wireless Access Point.The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.**This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.

Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the ProSafe 802.11g according to these specifications:

Product Version	ProSafe 802.11g Wireless Access Point
Manual Publication Date	May 2006

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents".

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/WG302v2.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A button that displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs. Your computer must have the free Adobe Acrobat Reader installed in order to view and print PDF files. The Acrobat Reader is available on the Adobe website at *http://www.adobe.com*.

- **Printing a Page in the HTML View**. Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.
- **Printing a Chapter**. Use the *PDF of This Chapter* link at the top left of any page.

– Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

– Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**. Use the *Complete PDF Manual* link at the top left of any page.

– Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

– Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 1
Introduction

This chapter introduces the NETGEAR® ProSafe™ 802.11g Wireless Access Point WG302v2. The WG302v2 is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The wireless access point provides wireless connectivity within about a 300-foot radius. The wireless access point can support up to 40 users simultaneously.

The WG302v2 acts as a bridge between the wired LAN and wireless clients. You can connect multiple wireless access points via a wired Ethernet backbone to add more wireless network coverage. As a wireless device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point to another and still maintain seamless connection to the network.

The auto-sensing capability of the ProSafe 802.11g allows packet transmission at up to 108 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Key Features

The ProSafe 802.11g Wireless Access Point is easy-to-use and provides solid wireless and networking support.

Supported Standards and Conventions

The following standards and conventions are supported:

- **Standards Compliant.** The Wireless Access Point complies with IEEE 802.11b/g standards for Wireless LANs.
- **WEP support.** Includes support for 64-bit, 128-bit, and 152-bit WEP keys.
- **Full WPA and WPA2 support.** WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK and WPA2-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.

- **Multiple BSSIDs.** Support for multiple BSSIDs. When one AP is connected to a wired network and a set of wireless stations, it is referred to as a Basic Service Set (BSS). The Basic Service Set Identifier (BSSID) is a 32-character unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network.
- **DHCP Client and Server Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The WG302v2 can obtain network information from a DHCP server on your network. The AP can also act as a DHCP server and provide network information for wireless clients.
- **SNMP Support.** Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.

WG302v2 Key Features

The WG302v2 provides solid functionality, including these features:

- Multiple Operating Modes
  - **Wireless Access Point.** Operates as a standard 802.11b/g wireless access point.
  - **Point-to-Point Bridge.** In this mode, the WG302v2 communicates with another bridge-mode wireless station.
  - **Point-to-Multi-Point Bridge.** This mode allows the WG302v2 to bridge to several other access points at the same time.
  - **Wireless Repeater.** In this mode, the WG302v2 operates as both a wireless access point and a wireless bridge.
- **Rogue Access Point Detection.** For enhanced security, you can scan the wireless network to detect rogue access points.
- **Hotspot Settings.** You can allow all HTTP (TCP, port 80) requests to be captured and re-directed to the URL you specify.
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely. You can also upgrade firmware from the command line interface (CLI) by using TFTP.
- **Access Control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the WG302v2 to gain access to your LAN.
- **Security Profiles.** When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, etc.) for each BSSID.

- **Simple Configuration.** If the default settings are unsuitable, they are easy to change.
- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Configuration Backup.** Configuration settings can be backed up to a file and restored.
- **Secure and Economical Operation.** Adjustable power output allows more secure or economical operation.
- **Power over Ethernet.** Power can be supplied to the WG302v2 over the Ethernet port from any 802.3af compliant mid-span or end-span source such as the NETGEAR FSM7326P Managed Power over Ethernet Layer 3 managed switch.
- **Autosensing Ethernet Connection with Auto Uplink™ Interface.** Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power, Test, LAN speed, LAN activity, and wireless activity are easily identified.
- **Wireless Virtual LAN (VLAN) Support.** VLANs enable a network of computers to behave as if they are connected to the same network even though they might actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user/host management, bandwidth allocation, and resource optimization.
- **Wireless Multimedia (WMM) Support.** WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.
- **Quality of Service (QoS) Support.** You can configure parameters that affect traffic flowing from the access point to the client station and traffic flowing from the client station to the access point. The QoS feature allows you to prioritize traffic, such as voice and video traffic, so that packets do not get dropped.

Compatible and Related NETGEAR Products

For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance Web site (WECA): *http://www.wi-fi.net*.

The following NETGEAR products work with the ProSafe 802.11g :

- WAG511 ProSafe 108 Mbps Dual Band PC Card
- WAG311 ProSafe 108 Mbps Dual Band PCI Card
- WG311T 802.11g 108 Mbps Wireless PCI Card

- WG511T 802.11g 108 Mbps Wireless CardBus Adapter
- WG511 802.11g 54 Mbps Wireless CardBus Adapter
- WG111 801.11g 54 Mbps Wireless USB 2.0 Adapter

What's In the Box?

The product package should contain the following items:

- ProSafe 802.11g Wireless Access Point WG302v2.
- Power adapter and cord.
- Straight through Category 5 Ethernet cable.
- *Resource CD for the NETGEAR ProSafe 802.11g Wireless Access Point WG302*.
- Support Registration card.

Contact your reseller or customer support in your area if there are any missing or damaged parts. See the Support Information card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WG302v2 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: *http://www.NETGEAR.com*.

Hardware Description

This section describes the WG302v2 front and rear hardware functions.

Front Panel

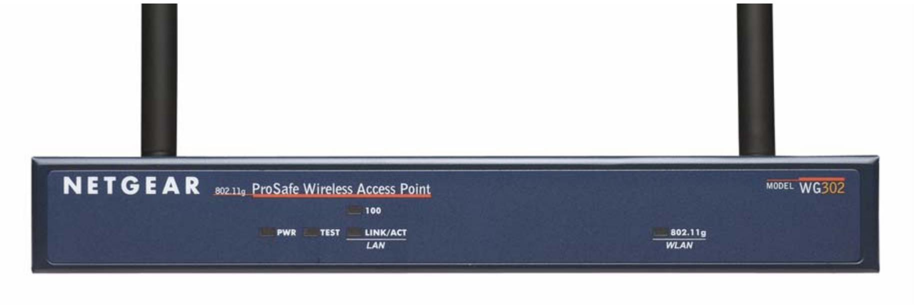


Figure 0-1

Viewed from left to right, the WG302v2 has these status LEDs: PWR, TEST, LAN, and 802.11g WLAN.

LED	Description	
PWR	Power Indicator	
	Off	No power. If this LED does not come on with the power adapter and cord correctly installed, see Chapter 5, “Troubleshooting.
	On	Power is on.
TEST	Self Test Indicator	
	Blink	Indicates self test, loading software, or system fault (if continues). Note: This LED may blink for a minute before going off.
LAN	Ethernet link indicator	
	Off	No connection detected on the Ethernet link
	Amber On	10 Mbps Ethernet link detected
	Amber Blink	Data is being transmitted or received on the 10 Mbps Ethernet link
	Green On	100 Mbps Fast Ethernet link detected.
	Green Blink	Data is being transmitted or received on the 100 Mbps Ethernet link

LED	Description	
802.11g WLAN	Wireless LAN Link Activity Indicator (2.4 MHz)	
	Off	No wireless link activity.
	Green Blink	Wireless link activity.

Rear Panel

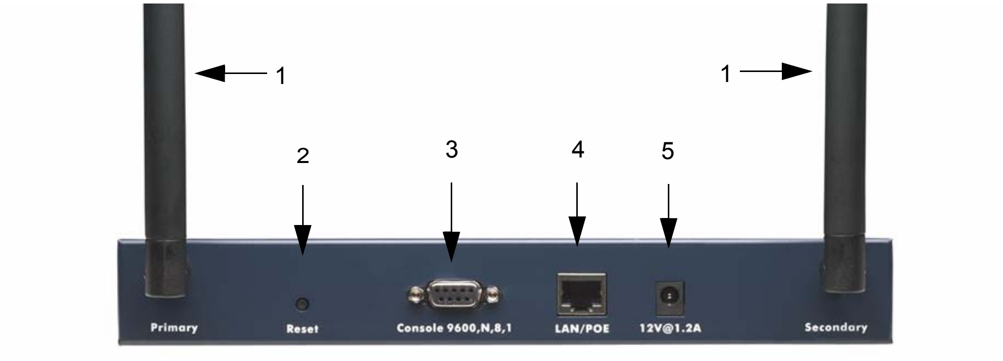


Figure 0-2

The numbers in Figure 0-2 correspond to the following features on the back of the WG302v2:

1. Primary and Secondary 2.4 GHz detachable antennas.
2. Reset button. This restores the default factory settings.
3. Serial Console Port. Use the male DB-9 serial port for serial DTE connections.
4. RJ-45 Ethernet LAN/POE Port. Use the WG302v2 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or Power Over Ethernet (POE) switch.
5. Power socket. This connects to the WG302v2 power adapter.

Chapter 2
Basic Installation and Configuration

This chapter describes how to set up your ProSafe 802.11g Wireless Access Point WG302v2 for wireless connectivity to your LAN. This basic configuration enables computers with 802.11b/g wireless adapters to do such things as connect to the Internet or access printers and files on your LAN.

> **Note:** Indoors, computers can connect over 802.11b/g wireless networks at ranges of several hundred feet or more. This distance can allow others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The ProSafe 802.11g provides highly effective security features which are covered in detail on the NETGEAR Web site. For more information, see Appendix A, "Related Documents. Deploy the security features appropriate to your needs.

You need to prepare the following three things before you can establish a connection through your wireless access point:

- A location for the WG302v2 that conforms to the Wireless Equipment Placement and Range Guidelines described in this chapter.
- A wired connection from the WG302v2 to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b/g wireless adapters.

System Requirements

Before you install the WG302v2, make sure you have the following equipment and that your system meets these requirements:

- A 10/100 Mbps Local Area Network device such as a hub or switch.
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it.
- A 100-240 V, 50-60 HZ AC power source.

- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.
- At least one computer with the TCP/IP protocol installed.
- 802.11g or 802.11b-compliant devices, such as the NETGEAR WG511 Wireless Adapter.

The WG302v2 can connect to you LAN via twisted-pair Category 5 Ethernet cable with RJ-45 connectors. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

The wireless access point uses Auto Uplink™ technology. The Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a computer or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself correctly. This feature eliminates any concerns about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

➡	**Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WG302v2. For complete performance specifications, see “Specifications for the WG302v2” in Appendix B.

For best results, place your wireless access point:

- Near the center of the area in which your PCs operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.

If you use multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is five Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement.

Installing the ProSafe 802.11g Wireless Access Point

Before you install the Wireless Access Point, make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network. Then computers with 802.11b/g wireless adapters will be able to communicate with the Ethernet network. In order for this to work correctly, verify that you have met all of the network and system requirements described in "System Requirements" on page 2-1.

Note: To view a list of the factory default settings, see "Default Factory Settings" in Appendix B.

To set up and install your WG302v2 Wireless Access Point:

1. Set up the WG302v2.

   Tip: Before mounting the WG302v2 in a high location, first set up and test the WG302v2 to verify wireless network connectivity.

   a. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

   b. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.

   c. Connect an Ethernet cable from the WG302v2 to the computer.

   d. Connect the power adapter to the WG302v2 and verify the following:

      – The PWR power light goes on.

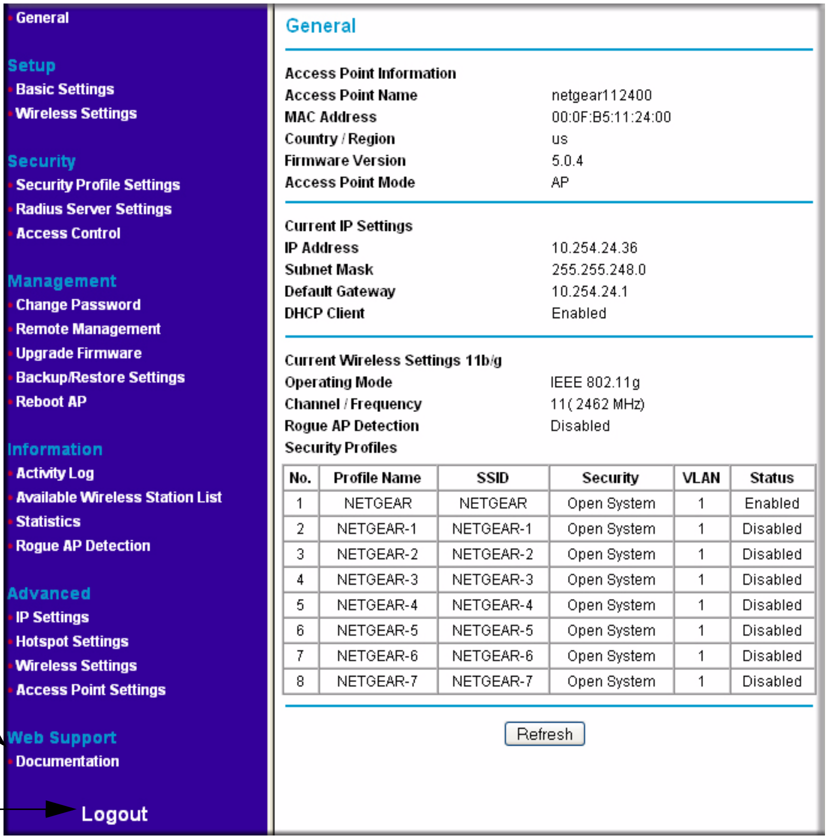
      – The LAN light of the wireless access point is lit when connected to a powered on computer.

2. Configure LAN and wireless access.

   a. Use your Web browser to connect to the WG302v2.

Enter **192.168.0.228** in the address field of your browser. The WG302v2 login screen appears. When prompted, enter **admin** for the user name, and **password** for the password, both in lower case letters. For more information, see "Logging in to the WG302v2 Using Its Default IP Address" on page 2-7.

The Web browser displays the WG302v2 main menu and General page, as Figure 2-1 shows.



General

Access Point Information
Access Point Name netgear112400
MAC Address 00:0F:B5:11:24:00
Country / Region us
Firmware Version 5.0.4
Access Point Mode AP

Current IP Settings
IP Address 10.254.24.36
Subnet Mask 255.255.248.0
Default Gateway 10.254.24.1
DHCP Client Enabled

Current Wireless Settings 11b/g
Operating Mode IEEE 802.11g
Channel / Frequency 11(2462 MHz)
Rogue AP Detection Disabled
Security Profiles

No.	Profile Name	SSID	Security	VLAN	Status
1	NETGEAR	NETGEAR	Open System	1	Enabled
2	NETGEAR-1	NETGEAR-1	Open System	1	Disabled
3	NETGEAR-2	NETGEAR-2	Open System	1	Disabled
4	NETGEAR-3	NETGEAR-3	Open System	1	Disabled
5	NETGEAR-4	NETGEAR-4	Open System	1	Disabled
6	NETGEAR-5	NETGEAR-5	Open System	1	Disabled
7	NETGEAR-6	NETGEAR-6	Open System	1	Disabled
8	NETGEAR-7	NETGEAR-7	Open System	1	Disabled

Click to view documentation

Click to log out. After five minutes with no activity, you are logged out automatically

Figure 2-1

For more information about the fields on the General page, see "Viewing General Information" on page 3-7.

b. Click the Basic Settings link in the Setup section of the main menu to view the Basic Settings menu.

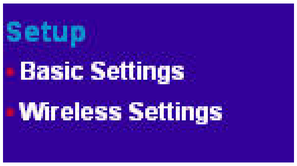


Figure 2-2

c. Configure the settings for your network and click **Apply**. See the online help or "Basic IP Settings" on page 2-8 for more information about how to configure the settings on this page.

d. Click Wireless Settings in the Setup section of the main menu to view the Wireless Settings menu.

e. Enter the wireless settings and click **Apply**. See the online help or "Wireless Settings" on page 2-10 for information about how to configure the settings on this page.

➡	**Note:** In the USA, the Region is preset according to regulatory requirements and cannot be changed. In other areas, you can and must set the Region. It may not be legal to operate the wireless access point in a region other than one of those identified in this field.

Now that you have finished the setup, you are ready to deploy the WG302v2 in your network. If needed, you can now reconfigure the computer you used for this process back to its original TCP/IP settings.

3. Deploy the wireless access point.

a. Disconnect the WG302v2 and put it where you will deploy it. The best location is elevated, such as wall mounted, or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices. For more information, see "Wireless Equipment Placement and Range Guidelines" on page 2-2

b. Lift the antenna on either side to be vertical.

c. Connect an Ethernet cable from your WG302v2 to a LAN port on your router, switch, or hub.

Note: By default, the DHCP client on the WG302v2 is disabled. If your network uses dynamic IP addresses, you must change this setting. To connect to the WG302v2 after the DHCP server on your network assigns it a new IP address, enter the access point name into your Web browser. The default access point name is netgearxxxxxx, where xxxxxx represents the last 6 bytes of the MAC address. The default name is printed on the bottom label of the WG302v2.

d. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The PWR, LAN, and WLAN lights should light up.

4. Verify wireless connectivity.

Using a computer with an 802.11b/g wireless adapter with the correct wireless settings needed to connect to the WG302v2 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Mozilla Firefox, Netscape, or Internet Explorer to browse the Internet, or check for file and printer access on your network.

Note: The default SSID is NETGEAR.The SSID of any wireless access adapters must match the SSID you configure in the ProSafe 802.11g Wireless Access Point. If they do not match, you will not get a wireless connection to the WG302v2.

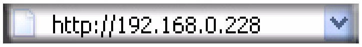
Note: If you are unable to connect to the WG302v2 with a wireless client, see Chapter 5, “Troubleshooting

Logging in to the WG302v2 Using Its Default IP Address

After you install the WG302v2, log in to it to configure the basic settings and the wireless settings. The WG302v2 is set, by default, with the IP address of 192.168.0.228 with DHCP disabled. You can log in to the WG302v2 by using the HTTP or HTTPS protocol.

➡ **Note:** Unless you change the IP address or enable the DHCP client on the WG302v2, the computer that you use to connect to the WG302v2 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

1. Open a Web browser such as Internet Explorer, Netscape Navigator, or Mozilla Firefox.
2. Connect to the WG302v2 by entering its default address of **http://192.168.0.228** into your browser.

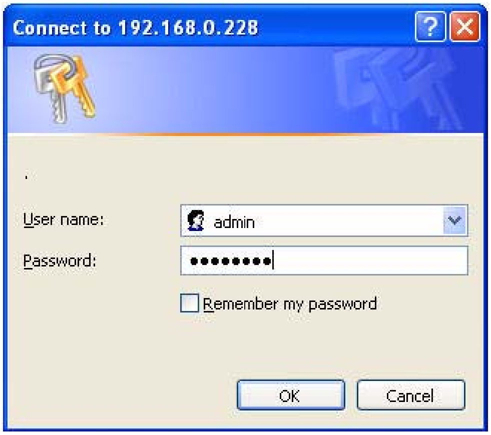


http://192.168.0.228

Figure 2-3

➡ **Note:** To use the HTTPS protocol, enter **https://192.168.0.228** into your browser and accept the certificate.

3. A login window like the one shown below opens:



Connect to 192.168.0.228

User name: admin

Password: ●●●●●●●●●

□ Remember my password

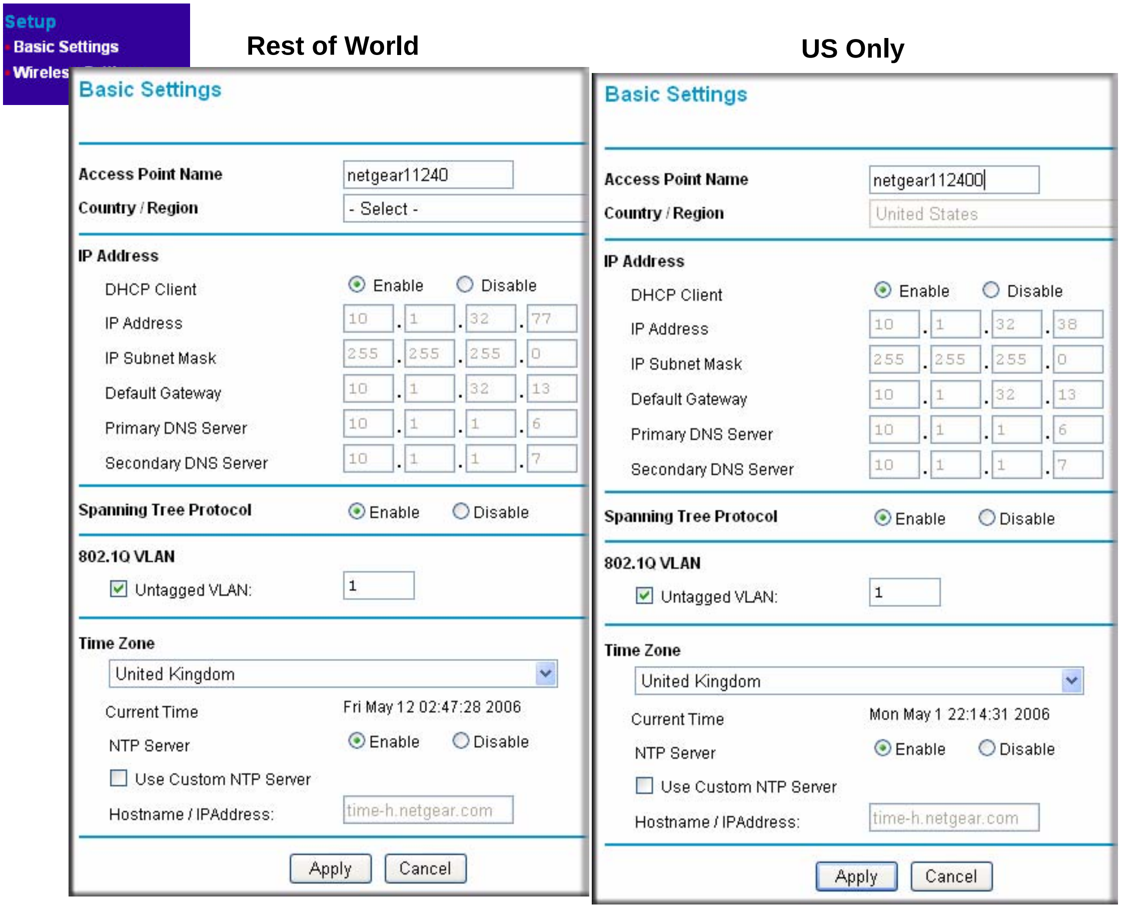
Figure 2-4

4. Log on by using the default user name of **admin** and default password of **password**.

   After you log on, the Web browser displays the General Information page as shown in Figure 2-1 on page 2-4.

Basic IP Settings

To configure the basic settings of your wireless access point, connect to the WG302v2 and click Basic Settings in the Setup section of the WG302v2 main menu. Figure 2-5 shows the Basic Settings page.



Rest of World

Basic Settings

Access Point Name: netgear11240
Country / Region: - Select -

IP Address
DHCP Client: ● Enable ○ Disable
IP Address: 10 . 1 . 32 . 77
IP Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 10 . 1 . 32 . 13
Primary DNS Server: 10 . 1 . 1 . 6
Secondary DNS Server: 10 . 1 . 1 . 7

Spanning Tree Protocol: ● Enable ○ Disable

802.1Q VLAN
☑ Untagged VLAN: 1

Time Zone
United Kingdom
Current Time: Fri May 12 02:47:28 2006
NTP Server: ● Enable ○ Disable
□ Use Custom NTP Server
Hostname / IPAddress: time-h.netgear.com

US Only

Basic Settings

Access Point Name: netgear112400
Country / Region: United States

IP Address
DHCP Client: ● Enable ○ Disable
IP Address: 10 . 1 . 32 . 38
IP Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 10 . 1 . 32 . 13
Primary DNS Server: 10 . 1 . 1 . 6
Secondary DNS Server: 10 . 1 . 1 . 7

Spanning Tree Protocol: ● Enable ○ Disable

802.1Q VLAN
☑ Untagged VLAN: 1

Time Zone
United Kingdom
Current Time: Mon May 1 22:14:31 2006
NTP Server: ● Enable ○ Disable
□ Use Custom NTP Server
Hostname / IPAddress: time-h.netgear.com

Figure 2-5

The Basic Settings default settings below work for most users and situations:

- **Access Point Name.** This unique name is the access point NetBIOS name. The default Access Point Name is on the bottom label of the WG302v2. The default name is netgearxxxxxx, where xxxxxx represents the last six hexadecimal digits of the WG302v2 MAC address. You can change the name to a unique name up to 15 characters long.
- **Country/Region.** This is the region where the WG302v2 can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. For products sold in the United States, the default country domain is preset. For products sold outside of the United States, you must select a country or region.
- **DHCP Client:** By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point get its IP address, subnet mask and default gateway settings automatically from the DHCP server on your network when you connect the WG302v2 to your LAN.

> **Note:** To connect to the WG302v2 after the DHCP server on your network assigns it a new IP address, enter the access point name into the address field of your Web browser. The default access point name is netgearxxxxxx, where xxxxxx represents the last 6 bytes of the MAC address. The default name is printed on the bottom label of the WG302v2.

- **IP Address.** The default IP address is 192.168.0.228. To change it, enter an unused IP address from the address range used on your LAN (factory default: 192.168.0.228); or enable DHCP.
- **IP Subnet Mask.** Enter the subnet mask value used on your LAN (factory default: 255.255.255.0).
- **Default Gateway.** Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected (factory default: 0.0.0.0).
- **DNS Server.** Enter the IP address of the Domain Name Server (DNS) you want to use (factory default: 0.0.0.0).
- **Spanning Tree Protocol.** Enable or disable spanning tree protocol (factory default: enabled). Spanning tree protocol provides network traffic optimization in settings with multiple ProSafe 802.11g devices.
- **Untagged VLAN.** You can use 802.1Q VLANs on the WG302v2 to logically separate traffic that is on the same physical network. VLAN tagging is always enabled so that the WG302v2 can process VLAN membership information.

By default all traffic on the WG302v2 uses VLAN 1, which is the default untagged VLAN. Therefore, all traffic is untagged until you change the untagged traffic VLAN ID or the VLAN ID for a specific Security Profile. Check the Untagged VLAN check box to transmit all frames on the specified VLAN as untagged. If you clear the box, all traffic is tagged with a VLAN ID.

- **Time Zone.** Select the Time Zone to match your location. If your location uses daylight saving, check the box Adjust for Daylight Saving Time.
- The Current Time, as used on the wireless access point, is displayed.

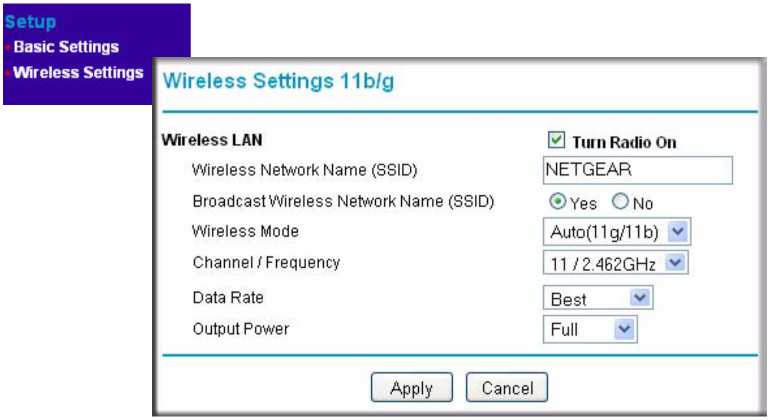
> **Note:** You must have an Internet connection to get the current time.

- **NTP Server.** Click Enable to use a network time protocol (NTP) server to synchronize the clock in your access point, or click Disable if you do not want to use an NTP server.
- **Use Custom NTP Server.** If you do not want to use the default NETGEAR NTP server, click this box and enter the hostname or IP address of the NTP server to use.

Wireless Settings

To configure the wireless settings, connect to the WG302v2 and click Wireless Settings in the Setup section of the WG302v2 main menu.

The Wireless Settings menu appears, as shown in Figure 2-6.



Wireless Settings 11b/g

Wireless LAN ☑ Turn Radio On

Wireless Network Name (SSID)	NETGEAR
Broadcast Wireless Network Name (SSID)	● Yes ○ No
Wireless Mode	Auto(11g/11b)
Channel / Frequency	11 / 2.462GHz
Data Rate	Best
Output Power	Full

Figure 2-6

The Wireless Settings page options are discussed below:

- **Turn Radio On.** On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use the SSID. The WG302v2 default SSID is **NETGEAR**. The following list contains additional information about SSIDs:
  - A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set (BSS).
  - Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).
  - A group of wireless stations and multiple access points, all using the same ID (ESSID), form an Extended Service Set (ESS).
  - Different access points within an ESS can use different channels. To reduce interference, it is recommended that adjacent access points *should* use different channels.
  - As wireless stations physically move through the area covered by an ESS, they will automatically change to the access point which has the least interference or best performance. This capability is called roaming.
- **Broadcast Wireless Network Name (SSID).** The default is Yes. If you choose No, then only stations that know the SSID can connect. Disabling the SSID broadcast might interfere with the wireless network “discovery” feature of some products.
- **Wireless Mode.** Select one of the following wireless operating modes:
  - Auto: Both 802.11b and 802.11g wireless stations can be used.
  - 802.11b Only: 802.11b wireless stations can be used.
- **Channel/Frequency.** This field sets the operating frequency to use. You should not need to change the channel unless you notice interference problems, or if you are setting up the WG302v2 near another access point. The wireless channel range is 1 to 11 for USA and Canada and 1 to 13 for Europe and Australia. The default is channel 11.
  - Access points use a fixed channel. You can select the channel to provide the least interference and best performance. In the USA and Canada, 11 channels are available.

  - If you use multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use channels 1 and 6, or 6 and 11).
  - In “Infrastructure” mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the access points use the same SSID.

  To learn more about wireless channels, see Appendix A, “Related Documents for information about online resources.

- **Data Rate.** Shows the available transmit data rate of the wireless network. The default is Best.
- **Output Power.** Set the transmit signal strength of the access point (AP). The options are Full, Half, Quarter, Eighth, and Min. Decrease the transmit power if two or more APs are close together and use the same channel frequency. The default is Full.

Understanding WG302v2 Wireless Security Options

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The ProSafe 802.11g provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WG302v2. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network ‘discovery’ feature of some products such as Windows XP, but the data is still fully exposed to a determined person using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **Use IEEE 802.1x.** IEEE 802.1x is the standard for passing the Extensible Authentication Protocol (EAP) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than Static WEP.

- **Use WPA, WPA-PSK, WPA2, or WPA2-PSK.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a newer standard than the other security options, wireless device driver and software availability may be limited.

Configuring Security Profiles

You can configure up to eight unique security settings on the WG302v2. Figure 2-7 shows the Security Profile Settings page.Use the following steps to configure a Security Profile.

1. Connect to the WG302v2.

In the address field of your Web browser, enter the default LAN address of **http://192.168.0.228**. Log in with the user name of **admin** and default password of **password**, or log in by using the LAN address and password that you configured.

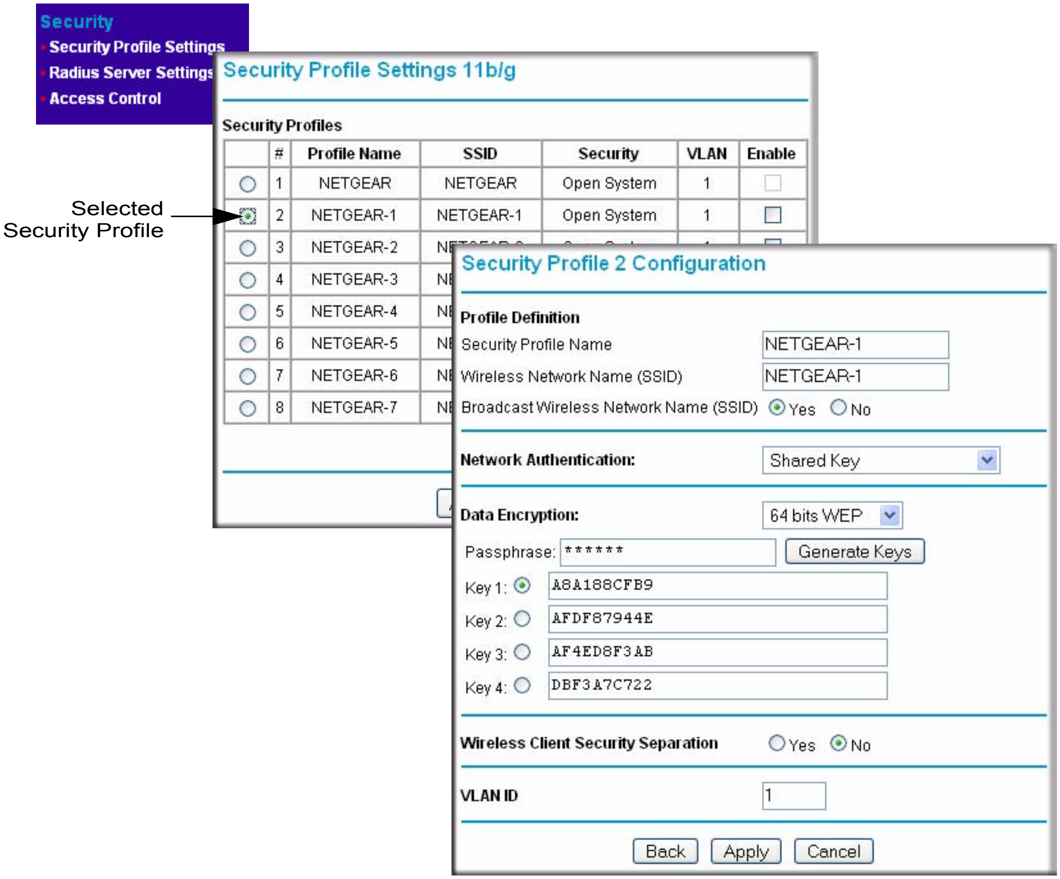
2. In the Security menu, click Security Profile Settings.

> **Note:** If you are using a RADIUS Server, configure the RADIUS settings first, as described in "Configuring the RADIUS Server Settings" on page 2-20.

The Security Profile Settings page appears and displays the current settings for the eight Security Profiles.

3. Select the Security Profile to configure and click Edit.

   The Security Profile Configuration page appears, as shown below.



Security Profile Settings 11b/g

Security Profiles

	#	Profile Name	SSID	Security	VLAN	Enable
○	1	NETGEAR	NETGEAR	Open System	1	□
●	2	NETGEAR-1	NETGEAR-1	Open System	1	□
○	3	NETGEAR-2	NE			
○	4	NETGEAR-3	NE			
○	5	NETGEAR-4	NE			
○	6	NETGEAR-5	NE			
○	7	NETGEAR-6	NE			
○	8	NETGEAR-7	NE			

Security Profile 2 Configuration

Profile Definition

Security Profile Name: NETGEAR-1

Wireless Network Name (SSID): NETGEAR-1

Broadcast Wireless Network Name (SSID) ● Yes ○ No

Network Authentication: Shared Key

Data Encryption: 64 bits WEP

Passphrase: ******

Key 1: ● A8A188CFB9

Key 2: ○ AFDF87944E

Key 3: ○ AF4ED8F3AB

Key 4: ○ DBF3A7C722

Wireless Client Security Separation ○ Yes ● No

VLAN ID 1

Figure 2-7

4. Enter the settings for the Security Profile, which are described on the following page.
5. To update the settings, click Apply.

> **Note:** If you use a wireless computer to configure Security Profile settings, and if your computer uses the Security Profile that you change, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired computer to make any further changes.

After the configuration changes are applied, the main Security Profile page displays.

6. If the Security Profile you configured is not already enabled, click the Enable check box associated with the Security Profile, and then click Apply.

   By default, only the first Security Profile (default name: NETGEAR) is enabled. To disable this Security Profile, you must disable the radio on the Wireless Settings page.

Profile Definition

The following settings are in the Profile Definition section on the Security Profile Configuration screen:

- **Security Profile Name.** Use a name that makes it easy to recognize the profile, and to tell profiles apart.
- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. The SSID separates network traffic from different wireless networks. For more information about the SSID, see Wireless Network Name (SSID) on page 2-11.
- **Broadcast Wireless Network Name (SSID).** This field lets you turn off the SSID broadcast. If you do so, then only stations that know the SSID can connect. Disabling the SSID broadcast might interfere with the wireless network “discovery” feature of some products. The default is to enable SSID broadcast.

Network Authentication

The ProSafe 802.11g is set by default as an open system with no authentication. When setting up Network Authentication, note the following information:

- If you are using Access Point mode, then all options are available. In other modes such as Repeater or Bridge, some options might be unavailable.
- Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions about configuring WPA2 settings.

You can configure the WG302v2 to use the types of network authentication shown in the table below in Table 2-1.

Table 2-1 Network Authentication Types

Authentication	Description
Open System	Can be used with WEP encryption or no encryption.
Shared Key	You must use WEP encryption and enter at least one shared key.
Legacy 802.1x	You must configure the RADIUS Server Settings to use this option.
WPA with RADIUS	You must configure the RADIUS Server Settings to use this option.
WPA2 with RADIUS	WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption and configure the RADIUS Server Settings.
WPA and WPA2 with RADIUS	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS Server Settings.
WPA-PSK	You must use TKIP encryption and enter the WPA passphrase (Network key).
WPA2-PSK	WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption and enter the WPA passphrase (Network key).
WPA-PSK and WPA2-PSK	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter the WPA passphrase (Network key).

Data Encryption

Select the data encryption that you want to use. The available options depend on the Network Authentication setting above (otherwise, the default is None). The Data Encryption settings are explained below:

Table 2-2 Data Encryption Settings

Settings	Description
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
152 bits WEP	Proprietary mode that will only work with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA.

Table 2-2 Data Encryption Settings (continued)

Settings	Description
AES	This is the standard encryption method for WPA2. Some clients may support AES with WPA, but this is not supported by this Access Point.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

The Passphrases and Keys are explained below:

- **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
- **Key 1, Key 2, Key 3, Key 4.** If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
- **WPA Pre-Shared Key.** If using WPA-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.

Note: Security Profiles that share the same type of network authentication must share the same passphrase or keys. Security Profiles that use WEP must share the same four keys, but they do not need to use the same default key.

Wireless Client Security Separation

If enabled, the associated wireless clients will not be able to communicate with each other. This feature is used for hotspots and other public access situations. The default is disabled.

VLAN ID

Enter a VLAN ID from 1-4094 to assign traffic from wireless clients to a VLAN. When a wireless client uses this Security Profile, the traffic is tagged with the VLAN ID you specify. To assign multiple Security Profiles to the same VLAN, enter the same VLAN ID for each profile. The default VLAN ID is 1. If you enter a VLAN ID that is not the default, make sure the VLAN ID matches the VLAN ID that switches and other network devices use on the LAN.

The VLAN assigned to the first Security Profile (default name: NETGEAR) is the management VLAN. By default all traffic on the WG302v2 uses VLAN 1, which is the default untagged VLAN. Therefore, all traffic is untagged until you change the untagged traffic VLAN ID on the Basic Settings page or assign a different VLAN ID to the Security Profile.

SSID and Wireless Security Settings Form

For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the person who set up or is responsible for the network can provide this information. Be sure to set the Regulatory Domain correctly as the first step. Store this information in a safe place.

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. You may customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: ____________________________________

  Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID.

- **Authentication**
  Circle one: Open System or Shared Key. Choose "Shared Key" for more security.

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key and have the same keys in the same positions as those in the WG302v2.

- **WEP Encryption Keys**
  For all four data encryption keys, choose the Key Size. Circle one: 64, 128, or 152 bits

  Key 1: ____________________________________

  Key 2: ____________________________________

  Key 3: ____________________________________

  Key 4: ____________________________________

- **WPA-PSK (Pre-Shared Key)WPA2-PSK (Pre-Shared Key)**
  Record the WPA-PSK key:Record the WPA2-PSK key:

  Key: ________________________________ Key: ________________________________

- **WPA RADIUS Settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary __________________ Secondary ___________________

  Port: ____________________________________

  Shared Secret: ____________________________________

- **WPA2 RADIUS Settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary __________________ Secondary ___________________

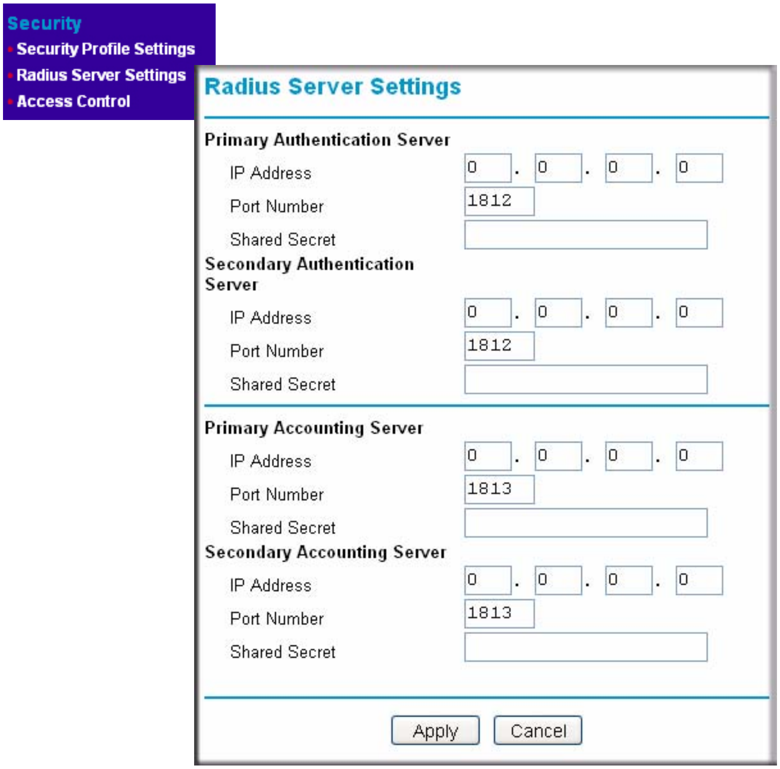
  Port: ____________________________________

  Shared Secret: ____________________________________

Configuring the RADIUS Server Settings

To view or change the RADIUS Server Settings:

1. Connect to the WG302v2.
2. In the address field of your Web browser, enter the default LAN address of **http://192.168.0.228**. Log in with the user name of **admin** and default password of **password**, or log in by using the LAN address and password that you configured.
3. In the Security menu, click RADIUS Server Settings.
4. Enter the settings for the primary RADIUS server and secondary RADIUS server (if available).
5. Click **Apply** to save your settings.



Radius Server Settings

Primary Authentication Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:

Secondary Authentication Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:

Primary Accounting Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1813

Shared Secret:

Secondary Accounting Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1813

Shared Secret:

Figure 2-8

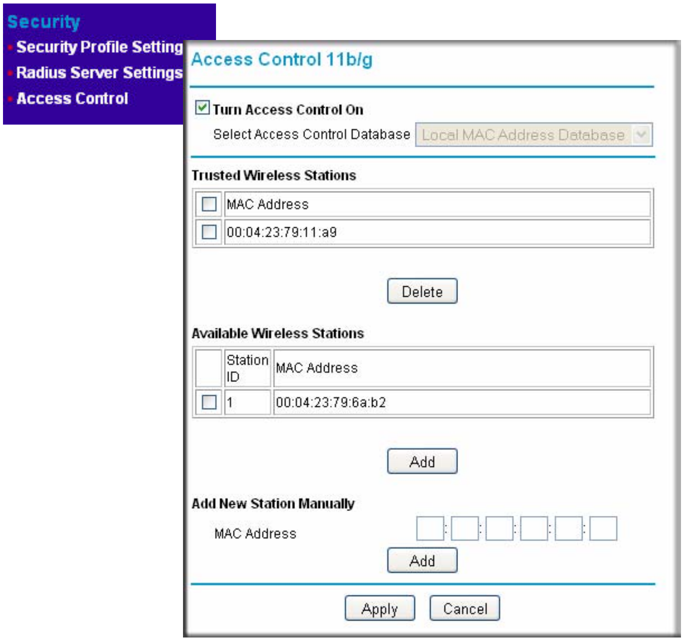
The following list describes the RADIUS Server Settings:

- **Authentication Server Configuration.** This configuration is required for authentication and access control using a RADIUS Server.The IP Address, Port Number and Shared Secret are required for communication with the RADIUS Server. You can configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.
- **IP Address.** The IP address of the RADIUS Server. The default is 0.0.0.0.
- **Port Number.** The port number of the RADIUS Server. The default is 1812.
- **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client). The shared secret can contain up to 63 standard alphanumeric and special characters. The shared secret is case sensitive.
- **Accounting Server Configuration.** This configuration is required for accounting using a RADIUS Server. The IP Address, Port Number and Shared Secret are required for communication with the RADIUS Server. You can configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.
- **IP Address.** The IP address of the RADIUS Server. The default is 0.0.0.0.
- **Port Number.** Port number of the RADIUS Server. The default is 1813.
- **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant.

Restricting Wireless Access by MAC Address

To restrict access based on MAC addresses, use the following steps:

1. Connect to the WG302v2 by entering the IP address of the WG302v2 into the address field of your Web browser.
2. From the Security menu, click the Access Control link to display the Access Control menu shown in Figure 2-9.



Security
- Security Profile Setting
- Radius Server Settings
- Access Control

Access Control 11b/g

☑ Turn Access Control On

Select Access Control Database: Local MAC Address Database

Trusted Wireless Stations

□	MAC Address
□	00:04:23:79:11:a9

Available Wireless Stations

	Station ID	MAC Address
□	1	00:04:23:79:6a:b2

Add New Station Manually

MAC Address □:□:□:□:□:□

Figure 2-9

3. Select the Turn Access Control On check box.

> **Note:** When configuring the WG302v2 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.

4. Either select from the list of available wireless stations the WG302v2 has found in your area, or enter the MAC address for a device you plan to use.

   You can usually find the MAC address of a wireless station printed on the wireless adapter. Click Add to add the wireless device to the access list. Repeat these steps for each additional device you want to add to the list.

5. Be sure to click **Apply** to save your wireless access control list settings.

Now, only devices on the MAC ACL will be allowed to wirelessly connect to the WG302v2.

Chapter 3
Management and Information

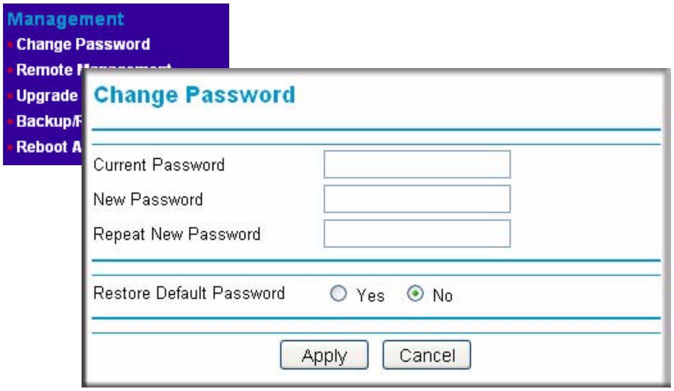
This chapter describes how to use the management and information features of your ProSafe 802.11g Wireless Access Point. To get to these features, connect to the WG302v2 as described in "Logging in to the WG302v2 Using Its Default IP Address" on page 2-7.

Changing the Administrator Password

The default password is **password**. NETGEAR recommends that you change this password to a more secure password. You cannot change the administrator login name.

To change the default password:

1. From the WG302v2 main menu, click Change Password to go to the menu shown below.Figure 3-1
2. Change the password by first entering the old password, and then enter the new password twice.
3. Click **Apply** to save your change.



Change Password

Current Password

New Password

Repeat New Password

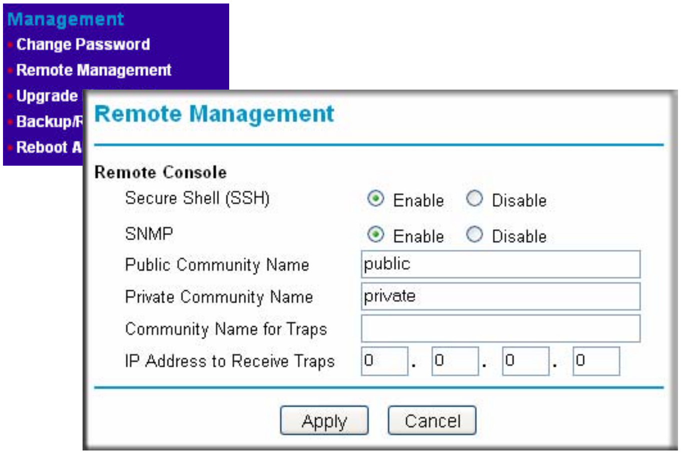
Restore Default Password ○ Yes ● No

Figure 3-1

Remote Management

To access the Remote Management screen:

1. Enter the LAN address of the WG302v2 into the address field of your browser.
2. After you log in, click Remote Management under Management on the main menu



Remote Management

Remote Console

Secure Shell (SSH) ● Enable ○ Disable

SNMP ● Enable ○ Disable

Public Community Name: public

Private Community Name: private

Community Name for Traps:

IP Address to Receive Traps: 0 . 0 . 0 . 0

Figure 3-2

3. Enter the Remote Management information.
   - **Secure Shell (SSH)**: If set to Enable, the Wireless Access Point will only allow remote access via Secure Shell and Secure Telnet. The default is Enable.
   - **SNMP**: Enable SNMP to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point via SNMPv1/v2 protocol.
   - **Public Community Name**: The community string to allow the SNMP manager to read the wireless access point's MIB objects. The default is public.
   - **Private Community Name**: The community string to allow the SNMP manager to read and write the wireless access point's MIB objects. The default is private.
   - **Community Name for Traps:** The community string associated with the IP address to Receive Traps. There is no default value.
   - **IP address to Receive Traps**: The IP address of the SNMP manager to receive traps sent from the wireless access point. The default is 0.0.0.0.
4. Click **Apply** to save your settings.

Using the Secure Telnet Interface

The WG302v2 includes a secure Telnet command line interface (CLI). You can access the CLI from a secure Telnet client over the Ethernet port or over the serial console port.

> **Note:** You must use a secure Telnet client such as PuTTY. Also, when you configure the client, use the SSH1, 3DES option. If you use the Telnet client to connect over the Ethernet port, use the IP address of the WG302v2 as the host name.

Accessing the CLI by Using the Console Port

1. Using a null-modem cable, connect a VT100/ANSI terminal or a workstation to the port labeled Console.

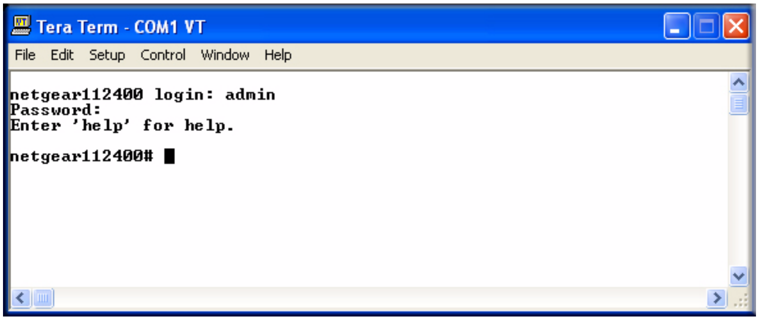
If you attached a PC, Apple Macintosh, or UNIX workstation, start a secure terminal-emulation program.

2. Configure the terminal-emulation program to use the following settings:

- Baud rate: 9600 bps
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

These settings appear below the connector on the back panel.

3. Press ENTER, and a screen similar to the one in Figure 3-3 should appear.



```
netgear112400 login: admin
Password:
Enter 'help' for help.

netgear112400#
```

Figure 3-3

The login name is **admin** and **password** is the default password.

After a successful login, the screen should show the command prompt, which is the name of the access point, by default. In this example, the prompt is *netgear112400#*.

Press TAB two times (TAB + TAB) to display the CLI command help.

CLI Commands

The CLI commands that correspond to the Web interface are explained in Appendix C, “Command Line Reference”.

Upgrading the Wireless Access Point Firmware

The ProSafe 802.11g firmware is stored in FLASH memory and can be upgraded as new firmware is released by NETGEAR. You can download the upgrade files from the NETGEAR Web site. You can upload the upgrade file (.TAR) to the wireless access point by using your Web browser.

> ⚠ **Warning:** When uploading firmware to the ProSafe 802.11g , do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the firmware, and render the WG302v2 completely inoperable.

You cannot upgrade the firmware from a computer that is connected to the WG302v2 with a wireless link. You must use a computer that is connected to the WG302v2 with an Ethernet cable. You cannot use the WG302v2 image to upgrade the WG302v1 software. When you upgrade the WG302v2 software, the configuration file is erased. After you upgrade the firmware, you must reconfigure the WG302v2. The previous configuration file might not be compatible with the new software.

> ➡ **Note:** The Web browser used to upload new firmware into the WG302v2 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

Use the following steps to upgrade the firmware:

1. Download the file from *http://kbserver.netgear.com/products/wg302.asp* and save it to your hard disk.
2. If you want to save your configuration settings, see “Backing up and Restoring the Configuration” on page 3-6.

3. From the main menu Management section, click the Upgrade Firmware link.
4. In the Upgrade Firmware menu, click the Browse button and browse to the location of the image (.tar) upgrade file.
5. Click Upload.

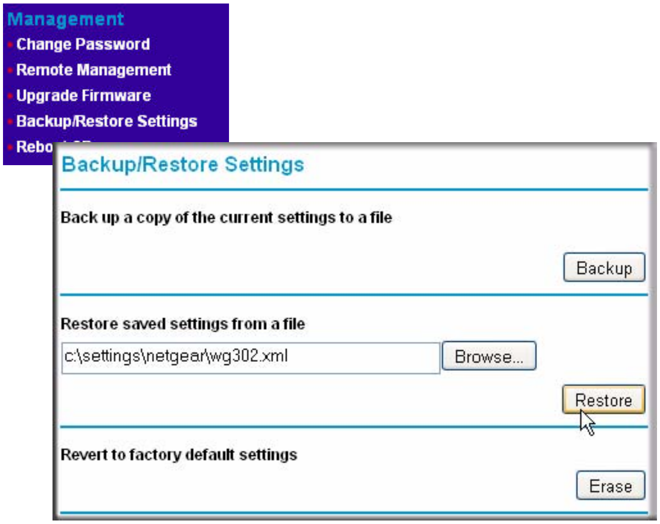
   When the upload completes, your wireless access point automatically restarts. The upgrade process typically takes about one minute.

In some cases, you may need to reconfigure the wireless access point after upgrading.

Configuration File Management

The ProSafe 802.11g settings are stored in the wireless access point in a configuration file. This file can be saved (backed up) to a computer, retrieved (restored) from a computer, or cleared to factory default settings.

Click Backup/Restore Settings under the Management heading to go to the page shown in Figure 3-4.



Backup/Restore Settings

Back up a copy of the current settings to a file

Restore saved settings from a file

c:\settings\netgear\wg302.xml

Revert to factory default settings

Figure 3-4

The following sections describes the options available on the Backup/Restore Settings page.

Backing up and Restoring the Configuration

To save your settings, click Backup. Your browser extracts the configuration file from the wireless access point and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as `WG302v2.xml`.

To restore your settings from a saved configuration file, enter the full path to the file on your computer or click the Browse button to locate the file. When you have located it, click the Restore button to upload the file. After completing the upload, the WG302v2 reboots automatically.

Erasing the Configuration

You can erase the wireless access point configurations and return to the factory default settings. After you erase the configurations, the wireless access point's password will be **password**, the SSID will be NETGEAR, the DHCP client will be disabled, the default LAN IP address will be 192.168.0.228, and the access point name is reset to the name printed on the label on the bottom of the unit.

Using the Reset Button to Restore Factory Default Settings

If you do not know the login password or IP address, you can still restore the factory default configuration settings with the Reset button. This button is on the rear panel of the wireless access point (see "Rear Panel" on page 1-6). To view a list of the factory default settings, see "Default Factory Settings" on page B-1.

The reset button has two functions:

- **Reboot.** When pressed and released, the Wireless Access Point reboots (restart).
- **Reset to Factory Defaults.** When pressed and held down, it clears all data and restores all settings to the factory default values.

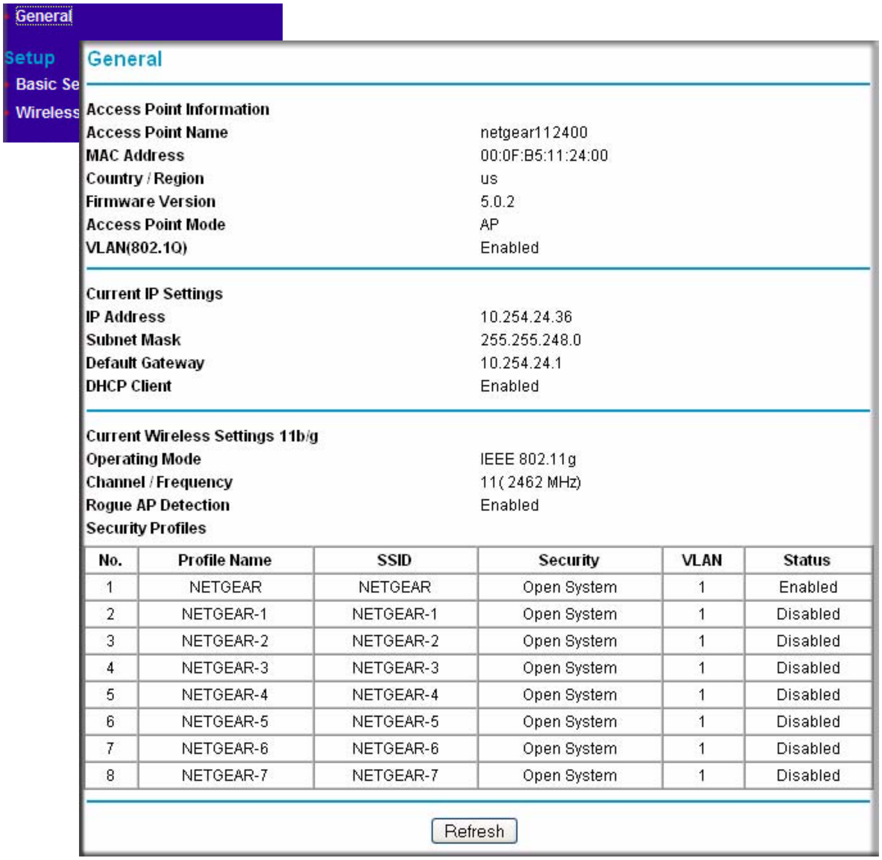
To clear all data and restore the factory default values:

1. Hold the Reset Button until the LEDs blink twice, usually more than five seconds.
2. Release the Reset Button.

The factory default configuration has now been restored, and the WG302v2 is ready for use.

Viewing General Information

The information on the General screen is a summary of the WG302v2 configuration settings. From the WG302v2 main menu, click General to view the screen shown below.



General

Access Point Information

Access Point Name	netgear112400
MAC Address	00:0F:B5:11:24:00
Country / Region	us
Firmware Version	5.0.2
Access Point Mode	AP
VLAN(802.1Q)	Enabled

Current IP Settings

IP Address	10.254.24.36
Subnet Mask	255.255.248.0
Default Gateway	10.254.24.1
DHCP Client	Enabled

Current Wireless Settings 11b/g

Operating Mode	IEEE 802.11g
Channel / Frequency	11(2462 MHz)
Rogue AP Detection	Enabled

Security Profiles

No.	Profile Name	SSID	Security	VLAN	Status
1	NETGEAR	NETGEAR	Open System	1	Enabled
2	NETGEAR-1	NETGEAR-1	Open System	1	Disabled
3	NETGEAR-2	NETGEAR-2	Open System	1	Disabled
4	NETGEAR-3	NETGEAR-3	Open System	1	Disabled
5	NETGEAR-4	NETGEAR-4	Open System	1	Disabled
6	NETGEAR-5	NETGEAR-5	Open System	1	Disabled
7	NETGEAR-6	NETGEAR-6	Open System	1	Disabled
8	NETGEAR-7	NETGEAR-7	Open System	1	Disabled

Figure 3-5

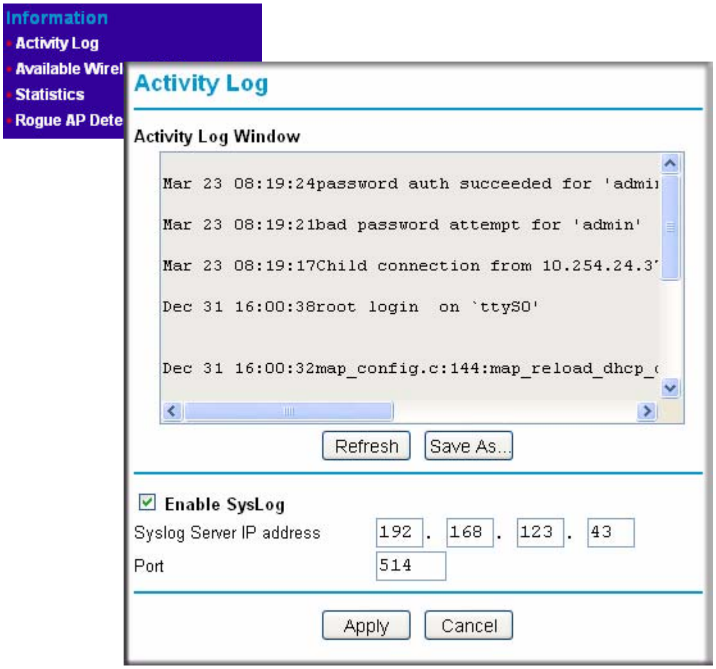
Table 3-1 describes the fields on the General Information page.

Table 3-1 General Information Fields

Field	Description
Access Point Information	
Access Point Name (NetBIOS name)	The name of the access point, which you can configure.
MAC Address	The Media Access Control address (MAC address) of the wireless access point's Ethernet port.
Country/Region	The domain or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Access Point Mode	The operating mode of the WG302v2: Access Point, Point-to-point bridge, Multi-point bridge or Repeater.
VLAN (802.1Q)	Indicates if VLAN support is enabled. The default is enabled.
Current IP Settings	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	If the DHCP Client is enabled, the current IP address was obtained from a DHCP server on your network. Disabled indicates a static IP configuration.
Current Wireless Settings	
Operating Mode	Shows the IEEE 802.11 wireless operating mode.
Channel/Frequency	The channel the wireless port uses. The default channel setting is 11. For the frequencies used on each channel, see the resources listed in Appendix A, "Related Documents.
Rogue AP Detection	Shows whether Rogue AP Detection is enabled.
Security Profiles	For each Security Profile, the following information is displayed: Profile Number, Profile Name, SSID, Security, VLAN, and Status.

Viewing the Activity Log

To access the Activity Log, connect to the WG302v2 and click Activity Log under the Information heading.



Activity Log Window

```
Mar 23 08:19:24password auth succeeded for 'admi

Mar 23 08:19:21bad password attempt for 'admin'

Mar 23 08:19:17Child connection from 10.254.24.3

Dec 31 16:00:38root login  on `ttyS0'


Dec 31 16:00:32map_config.c:144:map_reload_dhcp_
```

☑ Enable SysLog

Syslog Server IP address 192 . 168 . 123 . 43

Port 514

Figure 3-6

The Activity Log Window displays the Access Point system activity.

You can click Refresh to update the display. To save the log contents into a file on your PC, click Save As and save the file to a disk drive.

You can use a SysLog server to view the Activity Log. If you have a SysLog server on your LAN, then enable SysLog. If enabled, you must enter the IP address of your SysLog server and the port number that your SysLog server uses.

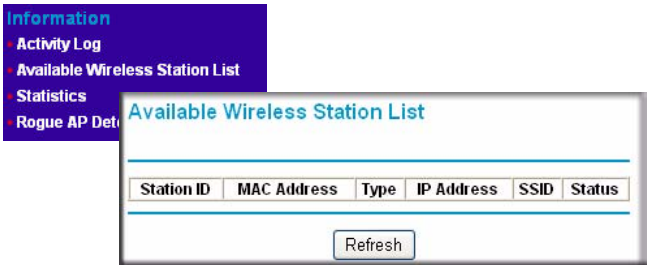
- **SysLog Server IP Address:** The access point sends all the SysLog messages to the specified IP address if SysLog option is enabled. Default: 0.0.0.0
- **Port:** The port number configured in the SysLog server on your LAN. The default is 514.

Viewing the Available Wireless Station List

The Available Wireless Station List contains a table of all IP devices associated with the wireless access point for the Wired Network Name (SSID)

From the WG302v2 main menu, under the Information heading, click Available Wireless Station List to view the list.

For each device, the Available Wireless Station List table shows the Station ID, MAC address, IP Address, and Status (whether the device is allowed to communicate with the wireless access point or not).


Information
Activity Log
Available Wireless Station List
Statistics
Rogue AP Det
Available Wireless Station List
Refresh

Station ID	MAC Address	Type	IP Address	SSID	Status

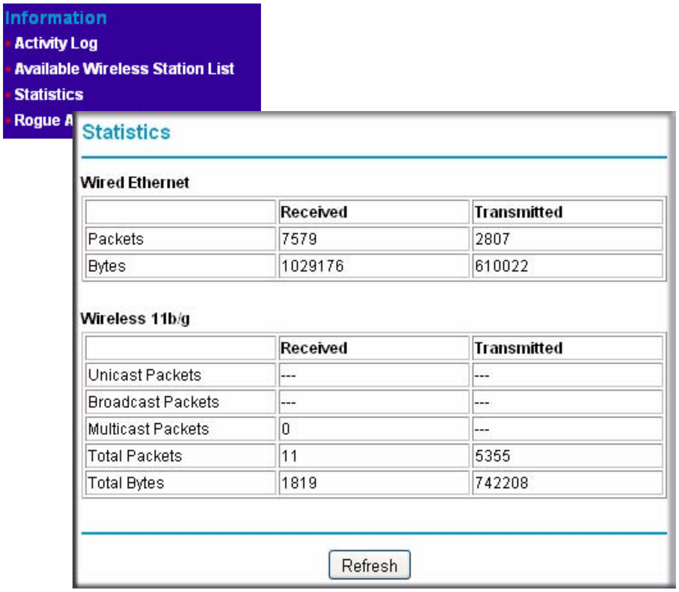
Figure 3-7

If the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click the Refresh button.

➡	**Note:** A wireless network can include multiple wireless access points that use the same network name (SSID). This extends the reach of the wireless network. Users can roam from one access point to another, providing seamless network connectivity. If this is the case, only the stations associated with this access point are shown in the Available Station List.

Viewing Statistics

The Statistics screen provides LAN and WLAN statistics. From the WG302v2 main menu, click Statistics under the Information heading to view the screen shown in Figure 3-8.



Statistics

Wired Ethernet

	Received	Transmitted
Packets	7579	2807
Bytes	1029176	610022

Wireless 11b/g

	Received	Transmitted
Unicast Packets	---	---
Broadcast Packets	---	---
Multicast Packets	0	---
Total Packets	11	5355
Total Bytes	1819	742208

Figure 3-8

Table 3-2 explains the fields on the Statistics page.

Table 3-2 Access Point Statistics

Field	Description
Wired Ethernet	Received/Transmitted
Packets	The number of packets sent since the WG302v2 was restarted.
Bytes	The number of bytes sent since the WG302v2 was restarted.

Table 3-2 Access Point Statistics

Field	Description
Wireless Interface	Received/Transmitted
Unicast Packets	The Unicast packets sent since the WG302v2 was restarted.
Broadcast Packets	The Broadcast packets sent since the WG302v2 was restarted.
Multicast Packets	The Multicast packets sent since the WG302v2 was restarted.
Total Packets	The Wireless packets sent since the WG302v2 was restarted.
Total Bytes	The Wireless bytes sent since the WG302v2 was restarted.
Refresh button	Click the Refresh button to update the statistics on this screen.

Rogue AP Detection

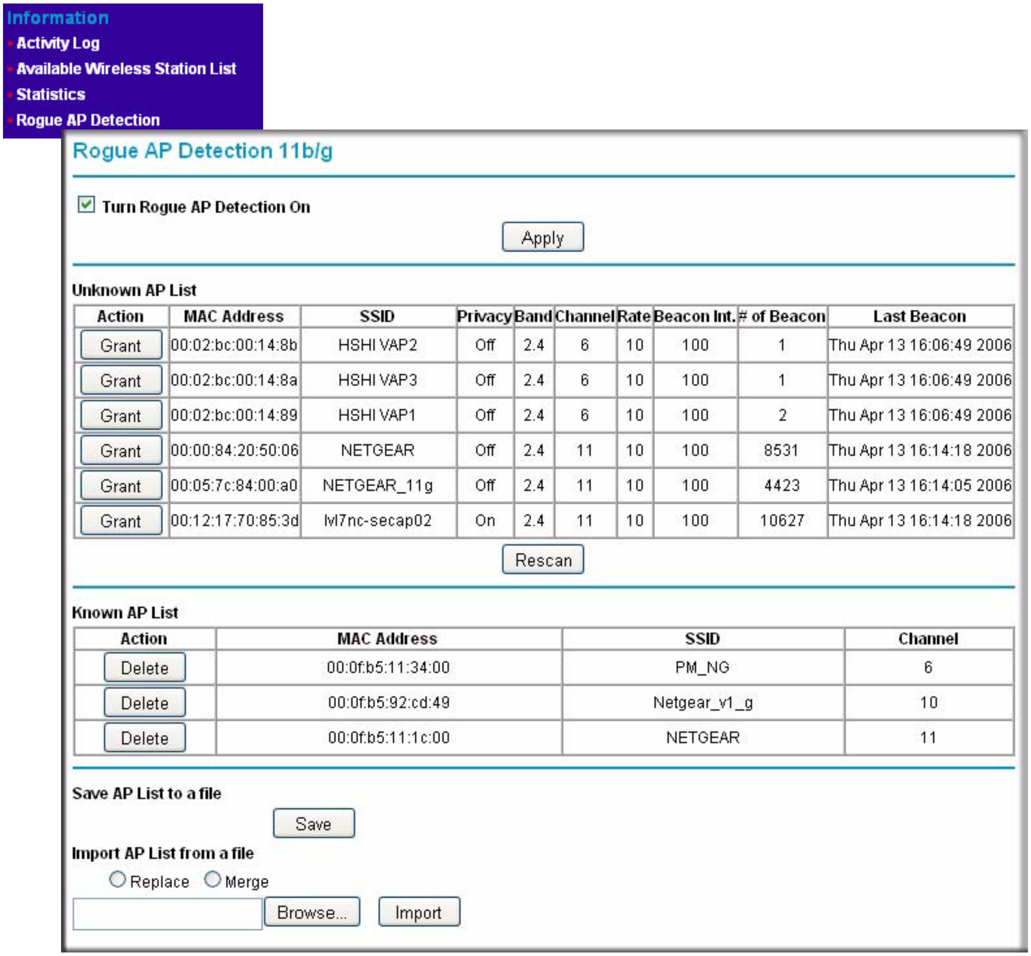
The WG302v2 can detect rogue APs and wireless stations and exclude them from connecting to the ProSafe 802.11g .

From the WG302v2 main menu:

1. Click **Rogue AP Detection** to view the page shown in Figure 3-9.

   If you enable Rogue AP Detection, the AP continuously scans the wireless network and collects information about all APs heard on its channel.

2. You can click **Rescan** to discover the APs.
3. Click **Grant** to add any AP to the Known AP List.
4. Click **Delete** to remove an AP from the list.
5. Click **Save** to export the list of known APs to a file. A window opens so you can browse to the location where you want to save the file. The default file name is WG302Rogue.cfg



Rogue AP Detection 11b/g

☑ Turn Rogue AP Detection On

Unknown AP List

Action	MAC Address	SSID	Privacy	Band	Channel	Rate	Beacon Int.	# of Beacon	Last Beacon
Grant	00:02:bc:00:14:8b	HSHI VAP2	Off	2.4	6	10	100	1	Thu Apr 13 16:06:49 2006
Grant	00:02:bc:00:14:8a	HSHI VAP3	Off	2.4	6	10	100	1	Thu Apr 13 16:06:49 2006
Grant	00:02:bc:00:14:89	HSHI VAP1	Off	2.4	6	10	100	2	Thu Apr 13 16:06:49 2006
Grant	00:00:84:20:50:06	NETGEAR	Off	2.4	11	10	100	8531	Thu Apr 13 16:14:18 2006
Grant	00:05:7c:84:00:a0	NETGEAR_11g	Off	2.4	11	10	100	4423	Thu Apr 13 16:14:05 2006
Grant	00:12:17:70:85:3d	lvl7nc-secap02	On	2.4	11	10	100	10627	Thu Apr 13 16:14:18 2006

Known AP List

Action	MAC Address	SSID	Channel
Delete	00:0f:b5:11:34:00	PM_NG	6
Delete	00:0f:b5:92:cd:49	Netgear_v1_g	10
Delete	00:0f:b5:11:1c:00	NETGEAR	11

Save AP List to a file

Import AP List from a file

○ Replace ○ Merge

Figure 3-9

To import a list of known APs, use the following steps:

1. Create a text file that contains the MAC address of each known AP, separated by a space.

   The following example shows a list of six known APs that an administrator might upload to the AP:

```
00:0c:41:d7:ee:a5 00:0f:b5:92:cd:49 00:12:17:70:85:3d
00:14:bf:ae:b1:e4 00:40:f4:f8:47:03 00:0c:41:d7:ee:b4
```

2. Check the Replace radio box to replace the existing list of known APs, check Merge to add the new MAC addresses to the existing list.

3. Click **Browse** and navigate to the location where you saved the text file.
4. Select the file and click **Open**.
5. Click **Import** to upload the list to the AP.

Chapter 4
Advanced Configuration

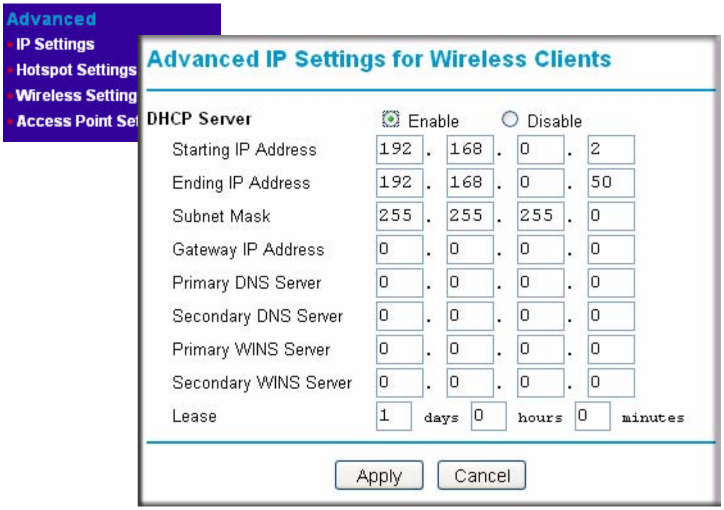
This chapter describes how to configure the advanced features of your ProSafe 802.11g Wireless Access Point. The following list describes the advanced features:

- **IP Settings:** Use the AP as a DHCP server for wireless clients.
- **Hotspot Settings:** Capture and redirect all HTTP (TCP, port 80) requests.
- **Wireless Settings:** Configure advanced wireless LAN parameters and Quality of Service (QoS).
- **Access Point Settings:** Enable wireless bridging and repeating.

To get to these features, connect to the WG302v2 as described in "Logging in to the WG302v2 Using Its Default IP Address" on page 2-7 and click the desired link under the Advanced menu heading.

Configuring Advanced IP Settings for Wireless Clients

The WG302v2 can act as a DHCP server gateway for wireless clients. After you log in, click IP Settings under the Advanced menu to view the Advanced IP Settings for Wireless Clients.



Advanced IP Settings for Wireless Clients

DHCP Server ● Enable ○ Disable

Starting IP Address	192	168	0	2
Ending IP Address	192	168	0	50
Subnet Mask	255	255	255	0
Gateway IP Address	0	0	0	0
Primary DNS Server	0	0	0	0
Secondary DNS Server	0	0	0	0
Primary WINS Server	0	0	0	0
Secondary WINS Server	0	0	0	0

Lease 1 days 0 hours 0 minutes

Figure 4-1

The following list provides information about how to configure DHCP settings:

- **Use AP as DHCP Server:** Turn on this option to allow the wireless access point to function as a DHCP Server for wireless clients. The WG302v2 provides the pre-configured TCP/IP configurations for wireless clients connected to this wireless access point. The default setting is disable.

> **Note:** The DHCP server only assigns network information to clients that connect to the WG302v2 through Security Profiles that are on the same VLAN as Security Profile 1. VLAN 1 is the default VLAN for all Security Profiles. If you typically use an existing DHCP server on your network to assign network information to hosts, you do not need to enable the DHCP server on the WG302v2.

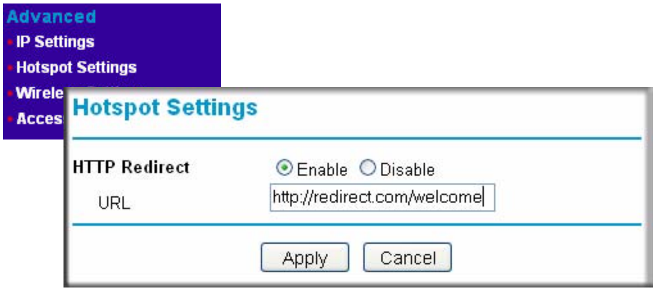
If you enable the WG302v2 DHCP server, you must configure the following TCP/IP configuration information that the wireless access point assigns to wireless clients that associate with it:

- **Starting IP Address:** Enter the starting IP address the DHCP server on this Access Point can assign wireless clients.The default starting IP address is 192.168.0.2.
- **Ending IP Address:** Enter the Ending IP address the DHCP server on this Access Point can assign wireless clients. The default ending IP address is 192.168.0.50.
- **Subnet Mask:** Enter a subnet mask for the DHCP server on the Access Point to assign wireless clients. The default subnet mask is 255.255.255.0.
- **Gateway Address:** Enter a Gateway Address for the DHCP server on the Access Point to assign wireless clients. The wireless clients will use this IP address as the default gateway for any traffic beyond the local network. By default, the gateway address is the IP address of the WG302v2.
- **Primary DNS Server:** Enter a Primary DNS Server IP address for the DHCP server on the Access Point to assign wireless clients. By default, the DNS server address is the IP address of the WG302v2. The WG302v2 relays requests from wireless clients to the DNS server configured on the **Basic Settings** page.
- **Secondary DNS Server:** Enter a Secondary DNS Server IP address for the DHCP server on the Access Point to assign wireless clients. There is no default server.
- **Primary WINS Server:** Enter a Primary WINS Server IP address for the DHCP server on the Access Point to assign wireless clients. There is no default server.
- **Secondary WINS Server:** Enter a Secondary WINS Server IP address for the DHCP server on the Access Point to assign wireless clients. There is no default server.

- **Lease:** Enter a lease time in days, hours and minutes. The wireless client must renew the IP address when the lease expires. The default lease time is one day.

Configuring Hotspot Settings

If you want the wireless access point to capture and redirect all HTTP (TCP, port 80) requests, use this feature. For example, a hotel might want all wireless connections to go to its server to show a branded splash screen.



HTTP Redirect ● Enable ○ Disable

URL http://redirect.com/welcome

Figure 4-2

Enter the URL of the Web server where you want to redirect HTTP requests.

Configuring Advanced Wireless Settings

The WG302v2 provides a bridge between Ethernet wired LANs and 802.11b/g compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

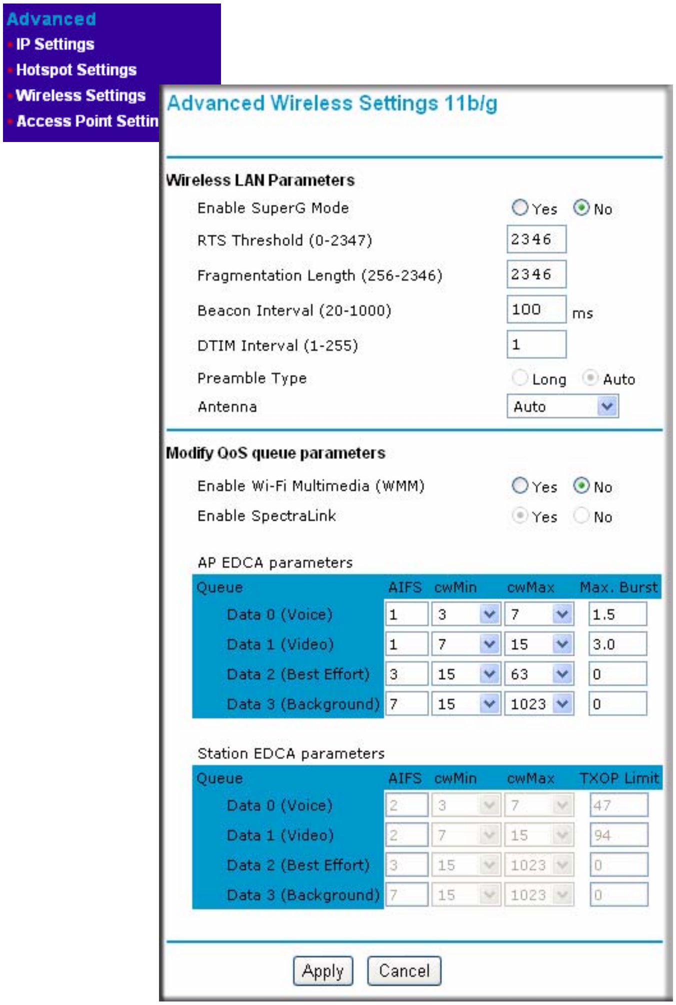
The WG302v2 also supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Roaming among access points on the same subnet

From the Advanced Wireless Settings menu, you can configure wireless LAN parameters and modify QoS queue settings, including Wi-Fi Multimedia (WMM).

Configuring Wireless LAN Parameters

Figure 4-3 shows the Advanced Wireless Settings screen that includes both the Wireless LAN Parameters section and the QoS Queue Parameters section. For most networks, the default Advanced Wireless LAN Parameter settings work well.



Advanced Wireless Settings 11b/g

Wireless LAN Parameters

Enable SuperG Mode ○ Yes ● No

RTS Threshold (0-2347) 2346

Fragmentation Length (256-2346) 2346

Beacon Interval (20-1000) 100 ms

DTIM Interval (1-255) 1

Preamble Type ○ Long ● Auto

Antenna Auto

Modify QoS queue parameters

Enable Wi-Fi Multimedia (WMM) ○ Yes ● No

Enable SpectraLink ● Yes ○ No

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

Figure 4-3

Table 4-1 describes the Advanced Wireless Parameters.

Table 4-1 Advanced Wireless LAN Parameters

Field	Description
Enable SuperG Mode	Click Enable to enable Super G Mode.
RTS Threshold	The packet size used to determine whether the access point should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission.
Fragmentation Length	This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.
Beacon Interval	Specifies the data beacon rate, which is between 20 and 1004.
DTIM Interval	The Delivery Traffic Indication Message specifies the data beacon rate, which is between 1 and 255.
Preamble Type	A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance.
Antenna	Select the antenna to use for transmitting and receiving. The antennas are labeled on the rear panel. The default is Auto.

Modifying QoS Queue Parameters

Figure 4-3 also shows the Quality of Service (QoS) queue section on the Advanced Wireless Settings page. For most networks, the default QoS queue parameter settings work well.Quality of Service provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data.

The QoS options on the WG302v2 are as follows:

- **Enable Wi-Fi Multimedia (WMM):** Select Yes or No as required on the Advanced Wireless Settings menu. The default is No.

  WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM. If WMM is disabled, you cannot configure Station EDCA parameters.

- **SpectraLink Enabled:** With SpectraLink enabled, SVP traffic takes priority over all other traffic. The default is always enabled.

SpectraLink Voice Priority (SVP) is a QoS approach for Wi-Fi deployments. SVP is an open specification that is compliant with the IEEE 802.11b standard. SVP minimizes delay and prioritizes voice packets over data packets on the Wireless LAN, thus increasing the probability of better network performance.

- **Modify AP EDCA Parameters.** Specify the AP EDCA parameters for different types of data transmitted from the WG302v2 to the wireless client.
- **Modify Station EDCA Parameters.** Specify the Station EDCA parameters for different types of data transmitted from the wireless client to the WG302v2. If WMM is disabled, you cannot configure Station EDCA parameters.

Table 4-2 describes the settings for QoS Queues.

Table 4-2 QoS Queues and Parameters

QoS Queue	Description
Data 0 (Voice)	High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
Data 1(Video)	High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
Data 2 (best effort)	Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
Data 3 (Background)	Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Arbitration Inter-Frame Space)	Specifies a wait time (in milliseconds) for data frames. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	Upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the “cwmin” are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMin must be lower than the value for cwMax.
cwMax (Maximum Contention Window)	Upper limit (in milliseconds) for the doubling of the random backoff value. Valid values for the “cwmax” are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMax must be higher than the value for cwMin.
Max. Burst Length	Specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0.0 through 999.9.

Wireless Bridging and Repeating

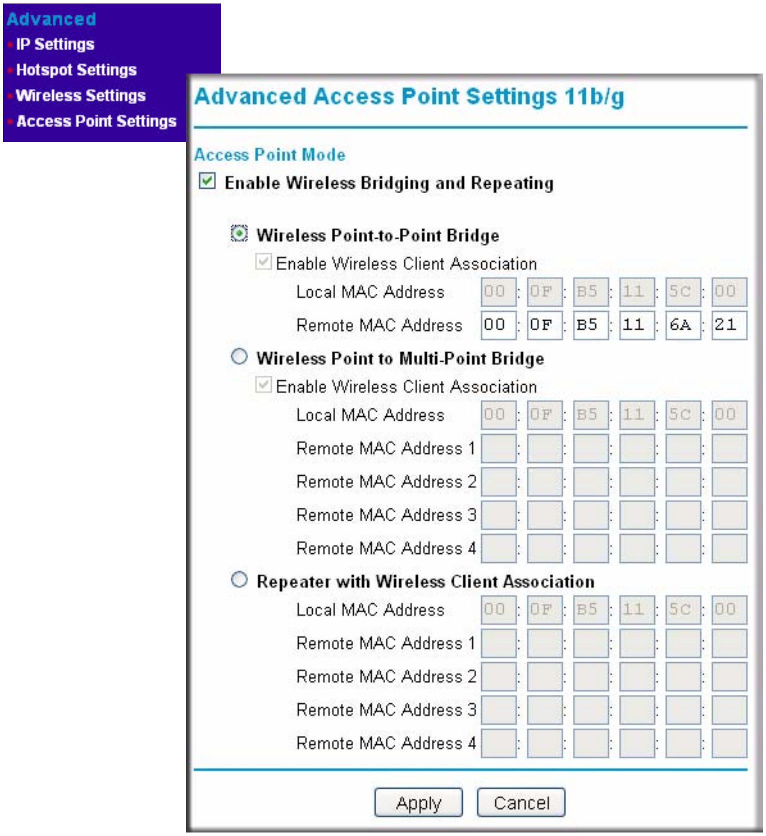
The ProSafe 802.11g lets you build large bridged wireless networks.

Examples of wireless bridged configurations are:

- **Point-to-Point Bridge.** The WG302v2 communicates with another bridge-mode wireless station. See "Point-to-Point Bridge Configuration" on page 4-9.
- **Multi-Point Bridge.** The WG302v2 is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this "master," rather than to other access points. See "Multi-Point Bridge Configuration" on page 4-10.
- **Repeater with Wireless Client Association.** Sends all traffic to the remote AP. See "Repeater with Wireless Client Association" on page 4-11.

➡ **Note:** The Wireless Bridging and Repeating feature uses the default Security Profile to send and receive traffic.

These configurations can be set up from the Advanced Access Point Settings page, shown in Figure 4-4 below.



Advanced Access Point Settings 11b/g

Access Point Mode

☑ Enable Wireless Bridging and Repeating

● Wireless Point-to-Point Bridge

☑ Enable Wireless Client Association

Local MAC Address 00 : 0F : B5 : 11 : 5C : 00

Remote MAC Address 00 : 0F : B5 : 11 : 6A : 21

○ Wireless Point to Multi-Point Bridge

☑ Enable Wireless Client Association

Local MAC Address 00 : 0F : B5 : 11 : 5C : 00

Remote MAC Address 1

Remote MAC Address 2

Remote MAC Address 3

Remote MAC Address 4

○ Repeater with Wireless Client Association

Local MAC Address 00 : 0F : B5 : 11 : 5C : 00

Remote MAC Address 1

Remote MAC Address 2

Remote MAC Address 3

Remote MAC Address 4

Figure 4-4

Point-to-Point Bridge Configuration

In Point-to-Point Bridge mode, the WG302v2 communicates with another bridge-mode wireless station. In addition, you can enable client associations with this WG302v2. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication. The figure below shows an example of Point-to-Point Bridge mode.

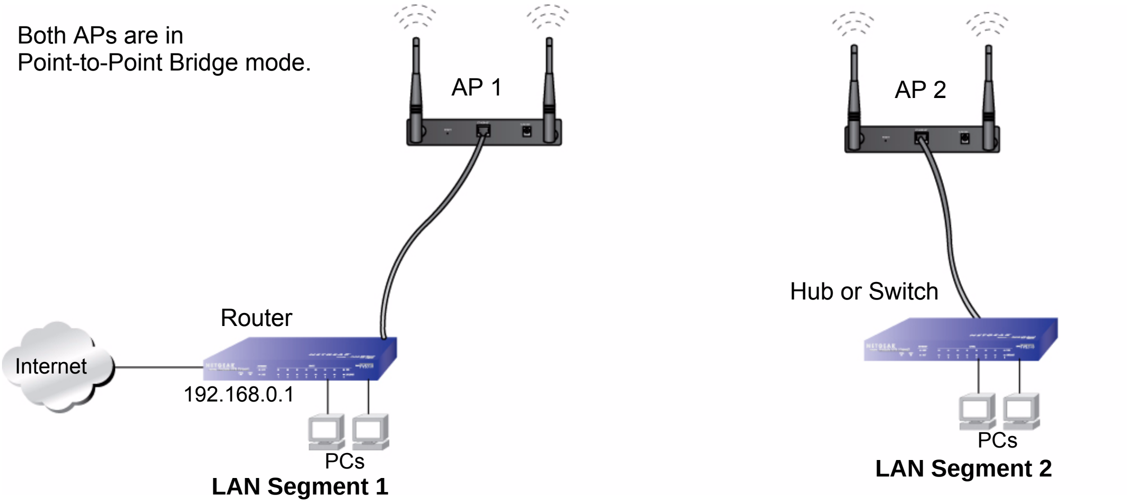


Figure 4-5

The following steps describe how to set up the Point-to-Point Bridge configuration in Figure 4-5.

1. Configure the WG302v2 (AP 1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the other access point (AP 2) on LAN Segment 2 in Point-to-Point Bridge mode.

   AP 1 must have AP 2's MAC address in its Remote MAC Address field, and AP 2 must have AP 1's MAC address in its Remote MAC Address field.
3. Configure and verify the following for both access points:
   - Verify the LAN network configuration of the access points. Both APs must be configured to operate in the same LAN network address range as the LAN devices.
   - Both APs must use the same SSID, Channel, authentication mode, if any, and security settings if security is in use.
4. Verify connectivity across the LAN 1 and LAN 2.

   A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Multi-Point Bridge Configuration

Multi-point bridge mode allows a wireless access point to bridge to multiple peer wireless access points simultaneously. In addition, you can enable client associations with this WG302v2. Multi-Point Bridge mode configuration includes the following steps:

- Enter the MAC addresses of the other access points in the fields provided.
- Set the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this WG302v2 as the Remote MAC Address.
- Use wireless security to protect this traffic.

The figure below shows an example of a Multi-Point Bridge mode configuration.

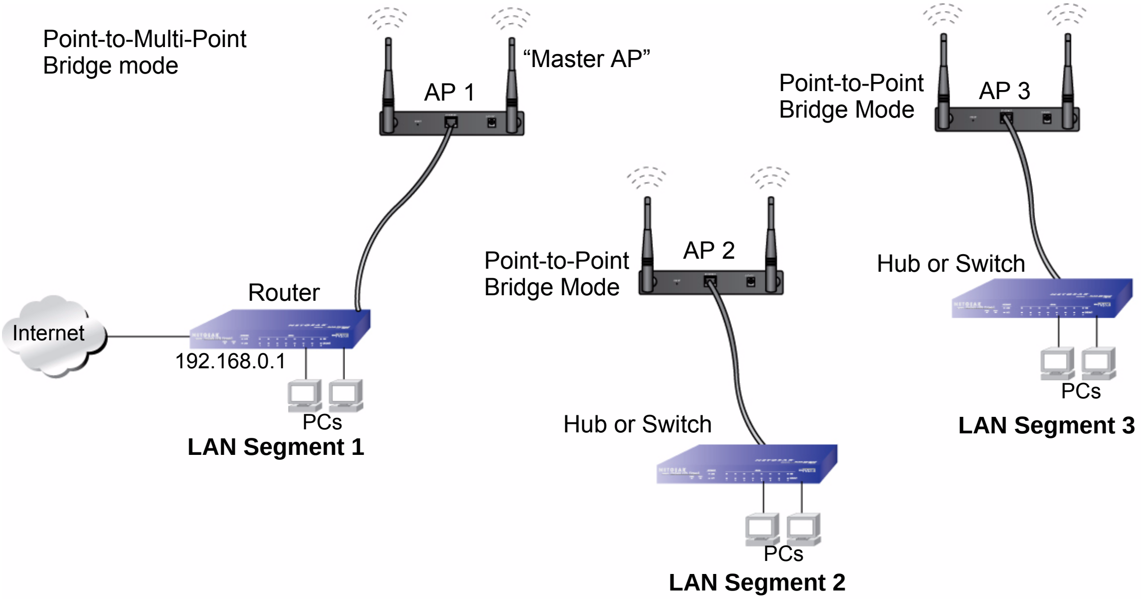


Figure 4-6

The following steps describe how to set up the Multi-Point Bridge configuration shown in Figure 4-6.

1. Configure the Operating Mode of the ProSafe 802.11g s.
   - Because it is in a central location, configure WG302v2 (AP 1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode and enter the MAC addresses of AP 2 and AP 3 in the Remote MAC Address 1 and Remote MAC Address 2 fields.

- Configure WG302v2 (AP 2) on LAN Segment 2 in Point-to-Point Bridge mode with the Remote MAC Address of AP 1.
- Configure the WG302v2 (AP 3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP 1.

2. Verify the following for all access points:

- The LAN network configuration of the ProSafe 802.11g s are configured to operate in the same LAN network address range as the LAN devices
- Only one AP is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
- All APs must be on the same LAN. That is, all the AP LAN IP addresses must be in the same network.
- If using DHCP, all ProSafe 802.11g s should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- All ProSafe 802.11g s must use the same SSID, Channel, authentication mode, if any, and encryption in use.
- All Point-to-Point APs must have the MAC address of AP 1 in the Remote AP MAC address field.

3. Verify connectivity across the LANs.

- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
- Wireless stations will not be able to connect to the ProSafe 802.11g s in Figure 4-6. If you require wireless stations to access any LAN segment, you can use additional ProSafe 802.11g s configured in Wireless Access Point mode to any LAN segment.

➡	**Note:** You can extend this multi-point bridging by adding additional WG302v2s configured in Point-to-Point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Repeater with Wireless Client Association

In this mode, the ProSafe 802.11g sends all traffic to the remote AP. For repeater mode, you must enter the MAC address of the remote “parent” access point. You can also enter the address of the “child” access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this WG302v2.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent/child AP pair.

The figure below shows an example of a Repeater Mode configuration.

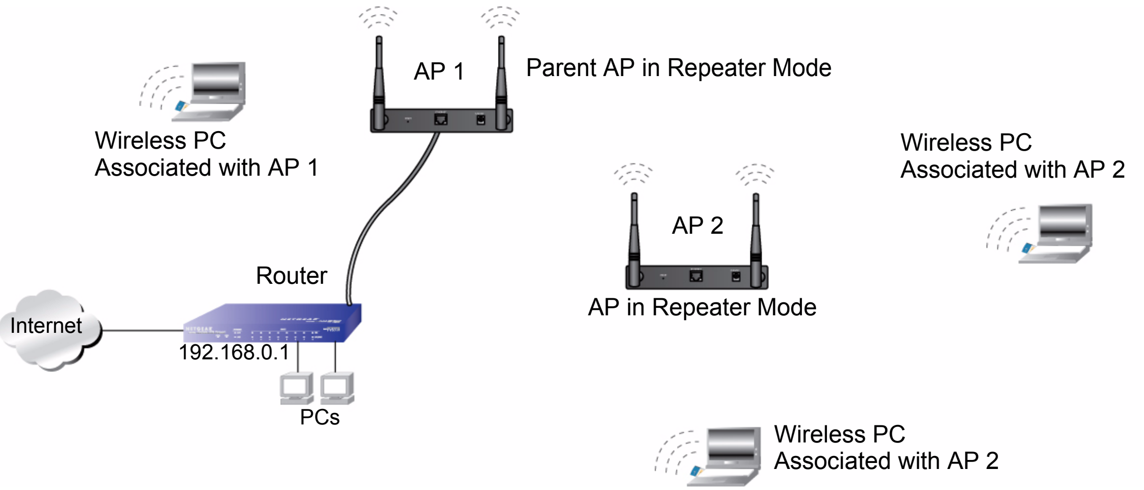


Figure 4-7

To set up a repeater with wireless client association, follow the steps below:

1. Configure the Operating Mode of the ProSafe 802.11g devices.
   - Configure AP 1 on LAN Segment 1 with the MAC address of AP 2 in the Remote MAC Address field.
   - Configure AP 2 with the MAC address of AP 1 in the Remote MAC Address field.
2. Verify the following for all access points:
   - The LAN network configuration of the ProSafe 802.11g devices are configured to operate in the same LAN network address range as the LAN devices
   - All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
   - If using DHCP, all ProSafe 802.11g devices should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.

- All ProSafe 802.11g devices use the same SSID, Channel, authentication mode, if any, and encryption in use.

3. Verify connectivity across the LANs.

A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

⇨	**Note:** You can extend this repeating by adding up to two more WG302v2s configured in repeater mode. However, since repeaters communicate in half-duplex mode, the bandwidth decreases as you add repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Chapter 5
Troubleshooting

This chapter provides information about troubleshooting your ProSafe 802.11g Wireless Access Point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WG302v2 on?

  Go to "Front Panel" on page 1-5.

- Have I connected the wireless access point correctly?

  Go to "Installing the ProSafe 802.11g Wireless Access Point" on page 2-3.

- I cannot remember the wireless access point's configuration password.

  Go to "Viewing the Activity Log" on page 3-9.

If you have trouble setting up your WG302v2, check the tips below.

No lights are lit on the access point.

It takes a few seconds for the power indicator to light up. Wait a minute and check the power light status on the access point.

If the access point has no power.

- Make sure the power cord is connected to the access point.
- Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure you are using the correct NETGEAR power adapter supplied with your access point.

The Wireless LAN activity light does not light up.

The access point's antennae are not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antennas are tightly connected to the WG302v2.
- Contact NETGEAR technical support if the Wireless LAN activity light remains off.

The LAN light is not lit.

There is a hardware connection problem. Check these items:

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

I cannot access the Internet or the LAN with a wireless capable computer.

There is a configuration problem. Check these items:

- You might not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to "Obtain an IP address automatically."
- The access point's default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.

I cannot connect to the WG302v2 to configure it.

Check these items:

- The WG302v2 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is on (amber indicating a 10 Mbps Ethernet connection or green indicating a 100 Mbps Ethernet connection) to verify that the Ethernet connection is OK.
- The default configuration of the WG302v2 is for a static IP address of 192.168.0.228 and a Mask of 255.255.255.0 with DHCP disabled. Make sure your network configuration settings are correct.
- If you are using the NetBIOS name of the WG302v2 to connect, ensure that your computer and the WG302v2 are on the same network segment or that there is a WINS server on your network.
- If your computer is set to “Obtain an IP Address automatically” (DHCP client), restart it.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WG302v2. The WG302v2 default IP Address is 192.168.0.228 and the default Subnet Mask is 255.255.255.0.

When I enter a URL or IP address I get a timeout error.

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WG302v2 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the WG302v2 is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.
- Try again.

I am unable to download files from some FTP sites.

If the IP address of the WG302v2 LAN interface is not on the same network as the IP addresses the DHCP server on the WG302v2 assigns to wireless clients, the WG302v2 performs automatic network address and port translation (NAPT). Some higher-layer protocols, such as FTP, might not work with the NAPT on the WG302v2.

To fix this issue, reconfigure the DHCP server settings (Advanced IP Settings) so that the wireless clients receive IP addresses that are on the same network as the WG302v2 Ethernet interface.

I need to restore factory default settings.

To restore the factory default settings, you can use the Reset button (see "Using the Reset Button to Restore Factory Default Settings" on page 3-6) or use the Backup/Restore Settings menu (see "Erasing the Configuration" on page 3-6). To view a list of the factory default settings, see "Default Factory Settings" on page B-1.

Appendix A
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications:	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access:	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN):	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary:	http://documentation.netgear.com/reference/enu/glossary/index.htm

Appendix B
Specifications

This appendix provides default factory settings and technical specifications for the ProSafe 802.11g Wireless Access Point.

Default Factory Settings

You can use the reset button located on the rear panel of your device to reset all settings to their factory defaults. This is called a hard reset. To perform a hard reset, push and hold the reset button for three seconds. Your device will return to the factory configuration settings shown in Table B-1.

Table B-1 Access Point Default Configuration Settings

Feature		Description
AP Login		
	User Login URL	192.168.0.228
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Ethernet Connection		
	Ethernet MAC Address	See bottom label.
	Port Speed	10/100
Basic Settings		
	AP Name	netgearxxxxxx, where xxxxxx are the last six digits of the wireless access point's MAC address
	Country / Region	United States (in North America; otherwise, varies by region)
	IP Address	192.168.0.228
	Subnet Mask	255.255.255.0
	DHCP Client	Disabled
	Spanning Tree Protocol	Enabled
	VLAN (802.1Q)	Enabled

Table B-1 Access Point Default Configuration Settings

Feature		**Description**
	Untagged Packet and VLAN Mapping	Disabled
	Untagged VLAN ID	1
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
Wireless Settings		
	Wireless Communication (Radio)	Enabled
	802.11g Network Name (SSID)	NETGEAR
	Broadcast SSID	Enabled
	802.11g Radio Frequency Channel	Channel 11
	Data Rate	Auto*
	Output Power	Full
Security Profile Settings		
	Profile Name	NETGEAR
	SSID	NETGEAR
	Security	Open System
	VLAN ID	1
	Status	Enabled (all other security profiles are disabled)
Radius Server Settings		
	Authentication Server IP Address	0.0.0.0
	Authentication Server Port	1812
	Accounting Server IP Address	0.0.0.0
	Accounting Server Port	1813

Table B-1 Access Point Default Configuration Settings

Feature		Description
Remote Management		
	SSH	Enabled
	SNMP	Enabled
	Public Community Name	public
	Private Community Name	private
	Community Name for Traps	NETGEAR WG302v2
	IP Address to Receive Traps	0.0.0.0
DHCP Server Settings		
	DHCP Server	Disabled
	Starting IP Address	192.168.0.2
	Ending IP Address	192.168.0.50
	Netmask	255.255.255.0
	Lease	86400 Seconds (1 Day)
Wireless LAN Parameters		
	Super-G Mode	Disabled
	RTS Threshold	2,346
	Fragmentation Length	2,346
	Beacon Interval	100
	DTIM Interval	1
	WMM Support	Disabled
	SpectraLink Support	Disabled
Other Settings		
	MAC Access Control	Disabled
	Rogue AP Detection	Disabled
	Activity Log	Disabled
	HTTP Redirect	Disabled
	Wireless Bridging and Repeating	Disabled

* Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Specifications for the WG302v2

The following table describes the WG302v2 technical specifications.

Table B-2 WG302v2 Technical Specifications

Parameter	ProSafe 802.11g Wireless Access Point
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; typically 30 to 70 nodes.
Status LEDs	Power/Ethernet LAN/Wireless LAN/Test
Power Adapter	12V DC, 1.2 A
Electromagnetic Compliance	FCC Part 15 Class B and Class E, CE and C-Tick
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing
Data Encoding:	802.11b: 1 and 2 Mbps, Direct Sequence Spread Spectrum (DSSS) 802.11b: 5.5 and 11 Mbps, Complementary Code Keying (CCK) 802.11g: All rates, Orthogonal Frequency Division Multiplexing (OFDM)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 10-40 nodes.
802.11b/g Radio Data Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable)
802.11b and g Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.412 ~ 2.484 GHz (Japan) 2.412 ~ 2.472 GHz (Europe ETSI) 2.457 ~ 2.462 GHz (Spain) 2.457 ~ 2.472 GHz (France)
802.11g Encryption	40-bits (also called 64-bits), 128- and 152-bits WEP data encryption
Antenna	Two (2) external 5 dBi 2.4 GHz detachable antennas

Appendix C
Command Line Reference

In addition to the Web-based user interface, the ProSafe 802.11g Wireless Access Point includes a command line interface (CLI) for administering the access point. The CLI lets you view and modify status and configuration information.The CLI is particularly useful if the network connection is not functioning because you can access the CLI through a serial port. To connect to the WG302v2 by using the CLI, see "Using the Secure Telnet Interface" on page 3-3 and "Accessing the CLI by Using the Console Port" on page 3-3.

The following topics provide an introduction to the class structure upon which the CLI is based, CLI commands, and examples of using the CLI to get or set configuration information on an access point:

- "Accessing CLI TAB Completion Help"
- "Keyboard Shortcuts"
- "Interface Naming Conventions"
- "Entering CLI Commands"
- "Using the CLI to Configure the ProSafe 802.11g"

Accessing CLI TAB Completion Help

Press the TAB key twice to show a list of available commands or keywords. You can also use TAB to complete a command after you enter enough characters to uniquely identify a command. If multiple completions exist, the system beeps. Type TAB again, and the CLI displays all keywords that match the characters you entered.

Example 1: At a blank command line, type TAB+TAB (press the TAB key twice) to get a list of all commands.

```
netgear115C00#
add                 Add an instance to the running configuration
config              Upload/Download the running configuration
factory-reset       Reset the system to factory defaults
firmware-upgrade    Upgrade the firmware
get                 Get property values of the running configuration
reboot              Reboot the system
```

```
remove                Remove instances in the running configuration
save-running          Save the running configuration
set                   Set property values of the running configuration
```

Example 2: Type “`get`” TAB+TAB to see a list of keywords for the `get` command.

```
netgear115C00# get
association           Associated station
basic-rate            Basic rates of radios
bridge-port           Bridge ports of bridge interfaces
....
vap                   Virtual Access Point
web-server            Web server
wme-queue             Transmission queue parameters for stations
```

Example 3: Type `get ssh s` TAB. This results in completion with the only matching keyword:

```
netgear115C00#
get ssh status
```

Press ENTER to display the output results of the command.

Keyboard Shortcuts

The CLI provides keyboard shortcuts to help you navigate the command line and build valid commands. Table C-1 describes the keyboard shortcuts available from the CLI.

Table C-1 Keyboard Shortcuts

Keyboard Shortcut	Action on CLI
Ctrl-a	Move the cursor to the beginning of the current line
Ctrl-e	Move the cursor to the end of the current line
Ctrl-b Left Arrow key	Move the cursor back on the current line, one character at a time
Ctrl-f Right Arrow Key	Move the cursor forward on the current line, one character at a time
Ctrl-c	Start over at a blank command prompt (abandons the input on the current line)
Ctrl-h Backspace	Remove one character on the current line.
Ctrl-w	Remove the last word in the current command. (Clears one word at a time from the current command line, always starting with the last word on the line.)

Table C-1 Keyboard Shortcuts (continued)

Keyboard Shortcut	Action on CLI
Ctrl-k	Remove characters starting from cursor location to end of the current line. (Clears the current line from the cursor forward.)
Ctrl-u	Remove all characters before the cursor. (Clears the current line from the cursor back to the CLI prompt.)
Ctrl-p Up Arrow key	Display previous command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.)
Ctrl-n Down Arrow key	Display next command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.)
Ctrl-d	Exit the CLI. (At a blank command prompt, typing Ctrl-d closes the CLI.) (Typing Ctrl-d within command text also removes characters, one at a time, at cursor location like Ctrl-h.)

Interface Naming Conventions

Table C-2 describes the interface naming conventions for the WG302v2.

⚠ **Warning:** The CLI uses specific interface names the Web UI does not use. Many `get` and `set` commands require that you enter interface names.

➡ **Note:** Use the `get interface` command to display common information on all interfaces, including IP addresses.

Table C-2 Interface Naming Convention

Interface	Description
brvlan1	The Internal bridge represents the internal interface for the access point. To Telnet or SSH into the access point, use the IP address for this interface. The brvlan1 interface consists of: • eth0 (or vlan <*vlanid*> if you have VLANs configured) • wlan0 •
brtrunk	Internal bridge trunk interface.

Table C-2 Interface Naming Convention (continued)

Interface	Description
lo	Local loopback for data meant for the access point itself.
eth0	The Ethernet interface connected to the Internal network.
vlan1	The VLAN interface associated with the default security profile.
wlan0	The default security profile for the Internal network.
wlan0vap*x*	The wireless interface for the *x* security profile.
wlan0wds*x*	A wireless distribution system (WDS) interface where *x* indicates the number of the WDS link. The WDS interface allows you to configure wireless bridging and repeating.

Entering CLI Commands

This section describes how to use CLI commands to configure the access point and how to view system settings and information.

Table C-3 shows the commands available at the blank CLI prompt. You can type TAB twice to display the list of commands. After you enter the command, press the TAB key twice to display a list of available keywords and variables.

Table C-3 Commands at the Blank Prompt

Command	Description
get	Gets the property values of existing instances of a class.
set	Sets the property values of existing instances of a class.
add	Adds a new instance or group of instances of a class.
remove	Removes an existing instance of a class.
config	Uploads or downloads the running configuration.
firmware-upgrade	Upgrades the firmware.
save-running	Saves the running configuration as the startup configuration.
reboot	Restarts the access point (a “soft” reboot).
factory-reset	Resets the AP to factory defaults and reboots.

Warning: Settings updated from the CLI (with `get`, `set`, `add`, and `remove` commands) will not be saved to the startup configuration unless you explicitly save them by issuing the `save-running` command.

The `get`, `set`, `add`, and `remove` commands are followed by one or more keywords and might be followed by one or more optional or required name-value pairs.

You can use CLI commands to view or configure most of the features that you can view and configure by using the Web UI.

Note: CLI commands are not available to merge, import, and export the known AP list for Rogue AP detection feature. Additionally, you cannot set the channel or frequency by using the CLI.

Using the CLI to Configure the ProSafe 802.11g

This section describes the commands you use to view and configure the WG302v2. The CLI commands correspond to tasks you can accomplish by using the Web-based user interface (UI). In some cases, the CLI `get` command provides additional details not available through the Web UI.

Viewing General Information

Table C-4 describes the commands you use to view some of the information that you see on the General page of the Web UI.

Table C-4 General Information

Task	Command
Access Point Information	
View Access Point Name	`get host id`
View the MAC Address for the Access Point	`get interface brvlan1 mac`
View the Country/Region	`get system country`
View the Firmware Version for the Access Point	`get system version`
View the Access Point Mode	`get interface brvlan1 type`
View the Untagged VLAN ID	`get untagged-vlan`
Current IP Settings	
View the IP Address	`get interface brvlan1`
View the Subnet Mask	`get interface brvlan1`
View the Default Gateway IP address	`get ip-route gateway`
View the DHCP Client status	`get management dhcp-client status`
Current Wireless Settings	
View the Operating Mode	`get radio all mode`
View the Channel / Frequency	`get radio all channel`
View whether Rogue AP Detection is enabled	`get radio all ap-detection`
View information about the Security Profiles	`get vap all detail`

The commands in the following table do not correspond to a specific Web page, but they can be helpful for viewing basic system information.

Table C-5 System Information

Task	Command
View hardware information	`get system`
View information about all interfaces	`get interface`
View information about the 802.11 radio	`get radio`
View information about the Security Profiles	`get vap`
View DNS settings	`get host`

Configuring Basic Settings

The commands in Table C-6 correspond to the Basic Settings page on the Web UI.

Table C-6 Basic Setting s

Task	Command

Set the Access Point Name	`set host id <name>`
	Example:
	`set host id LAB_AP`

Set the Country / Region	`set system country <2_letter_country_code>`
	Example:
	`set system country us`

Enable the DHCP Client	`set management dhcp-client status up`
Disable the DHCP Client	`set management dhcp-client status down`

Set a Static IP Address	`set interface brvlan1 static-ip <ip_address>`
	Example:
	`set interface brvlan1 static-ip 10.10.12.221`

Set a Subnet Mask	`set interface brvlan1 static-mask <netmask>`
	Example:
	`set interface brvlan1 static-mask 255.255.255.0`

Set the Default Gateway	`set static-ip-route gateway <ip_address>`
	Example:
	`set static-ip-route gateway 10.10.12.1`

Table C-6 Basic Setting (continued)s

Task	Command

Set the Primary DNS Server	`set host static-dns-1 <ip_address>`
	Example:
	`set host static-dns-1 10.10.3.10`

Set the Secondary DNS Server	`set host static-dns-2 <ip_address>`
Enable Spanning Tree Protocol	`set interface brvlan1 stp on`
Disable Spanning Tree Protocol	`set interface brvlan1 stp off`
Set the Management VLAN ID	`set management vlan-id <1-4096>`
Enable Untagged VLANs and set the VLAN ID	`set untagged-vlan untagged-vlan-id <1-4096>`
Set the Time Zone	`set ntp timezone <timezone>`
Enable the NTP Server	`set ntp status up`
Disable the NTP Server	`set ntp status down`
Use a custom NTP server	`set ntp use-default-servers off`
Use the default NTP server	`set ntp use-default-servers on`

Set the Hostname or IP Address for the custom NTP server
Note: You can set a primary and secondary NTP server.
	`set ntp-servers [primary | secondary] server [<hostname> | <ip_address>]`
	Example:
	`set ntp-serves primary ntp.foo.com`
	or
	`set ntp-servers primary server 192.168.1.10`

View the Current Time	`date`

Configuring Wireless Settings

The commands in Table C-7 correspond to the Wireless Settings page on the Web UI.

Table C-7 Wireless Setting s

Task	Command
Turn on the Radio	`set interface wlan0 status up`
Turn off the Radio	`set interface wlan0 status down`

Table C-7 Wireless Setting (continued)s

Task	Command

Configure the Wireless Network Name (SSID)	`set interface wlan0 ssid <ssid_name>`
	Example:
	`set interface wlan0 ssid test_lab`

Allow SSID Broadcasts	`set bss wlan0bssvap0 ignore-broadcast-ssid off`
Deny SSID Broadcasts	`set bss wlan0bssvap0 ignore-broadcast-ssid on`

Set the Wireless Mode	`set radio wlan0 mode g`
	`set radio wlan0 mode b`

Set the Channel/Frequency	Not permitted

Set the Data Rate	`get supported-rate wlan0`
	`add supported-rate wlan0 <rate>`
	`remove supported-rate wlan0 <rate>`

Set the Output Power	`set radio wlan0 tx-power <percent>`

Configuring Security Profile Settings

You can configure up to eight security profiles on the AP. Table C-8 maps the Web UI security profile for wlan0 to the profile name in the CLI.

Table C-8 Security Profile Interface Names

Web UI Security Profile	Default Profile Name	CLI Name
Profile 1	NETGEAR	vap0
Profile 2	NETGEAR-1	vap1
Profile 3	NETGEAR-2	vap2
Profile 4	NETGEAR-3	vap3
Profile 5	NETGEAR-4	vap4
Profile 6	NETGEAR-5	vap5
Profile 7	NETGEAR-6	vap6
Profile 8	NETGEAR-7	vap7

The commands in Table C-9 correspond to the Security Profile Settings page on the Web UI. The commands in this table show how to configure Security Profile 1, which is the default profile and has a default profile name of NETGEAR.

Note: The commands in Table C-9 configure the default security profile, which is vap0 on radio wlan0. To configure other security profiles, use `vapx`, where `x` is the VAP ID associated with the security profile.

Table C-9 Security Profile Settings

Task	Command
Enable a security profile	`set vap vap0 with radio wlan0 status up`
Disable a security profile	`set vap vap0 with radio wlan0 status down`
Set the security profile name	`set vap vap0 with radio wlan0 profile <name>`
Set the SSID of the security profile	`set interface wlan0vap0 ssid <ssid_name>`
Broadcast wireless network name.	`set bss wlan0bssvap0 ignore-broadcast-ssid off`
Do not broadcast wireless network name.	`set bss wlan0bssvap0 ignore-broadcast-ssid on`
Set Network Authentication to Open System	`set interface wlan0 security plain-text`
Set Network Authentication to Shared Key	`set interface wlan0 security static-wep`
Set the Data Encryption to 64-bit WEP	`set interface wlan0vap0 wep-key-length 40`
Set the Data Encryption to 128-bit WEP	`set interface wlan0vap0 wep-key-length 104`
Set the Key Type to ASCII	`set interface wlan0vap0 wep-key-ascii yes`
Set the Data Encryption to 152-bit WEP	`set interface wlan0vap0 wep-key-length 128`
Set the Key Type to Hex:	`set interface wlan0vap0 wep-key-ascii no`

Table C-9 Security Profile Settings (continued)

Task	Command

Set the WEP Keys	`set interface wlan0 wep-key-1 <key>`
	Note: For 64-bit WEP, use 5 ASCII characters or 10 Hex characters. For 128-bit WEP, use 13 ASCII characters or 26 Hex characters. For 152-bit WEP, use 32 hexadecimal or 16 ASCII characters.
	Example (64-bit WEP with ASCII):
	`set interface wlan0 wep-key-1 abcde`
	`set interface wlan0 wep-key-2 fghi`
	`set interface wlan0 wep-key-3 klmno`
	`set interface wlan0 wep-key-4 pqrst`

Set Network Authentication to 802.1X	`set interface wlan0 security dot1x`

Set Network Authentication to WPA	`set interface wlan0 security wpa-personal`
	`set bss wlan0bssvap0 wpa-allowed on`
	`set bss wlan0bssvap0 wpa2-allowed off`

Set Network Authentication to WPA2	`set interface wlan0 security wpa-personal`
	`set bss wlan0bssvap0 wpa-allowed off`
	`set bss wlan0bssvap0 wpa2-allowed on`

Set Network Authentication to WPA and WPA2	`set interface wlan0 security wpa-personal`
	`set bss wlan0bssvap0 wpa-allowed on`
	`set bss wlan0bssvap0 wpa2-allowed on`

Set the WPA Passphrase	`set interface wlan0 wpa-personal-key <key>`
	Example
	`set interface wlan0 wpa-personal-key “KeY!”`
	`or`
	`set interface wlan0 wpa-personal-key My!KeY`

Set Network Authentication to WPA with RADIUS	`set interface wlan0 security wpa-enterprise`
	`set bss wlan0bssvap0 wpa-allowed on`
	`set bss wlan0bssvap0 wpa2-allowed off`

Set Network Authentication to WPA2 with RADIUS	`set interface wlan0 security wpa-enterprise`
	`set bss wlan0bssvap0 wpa-allowed off`
	`set bss wlan0bssvap0 wpa2-allowed on`

Table C-9 Security Profile Settings (continued)

Task	Command

Set Network Authentication to WPA and WPA2 with RADIUS	`set interface wlan0 security wpa-enterprise`
	`set bss wlan0bssvap0 wpa-allowed on`
	`set bss wlan0bssvap0 wpa2-allowed on`

Enable Wireless Client Security Separation	`set radio wlan0 station-isolation on`
Disable Wireless Client Security Separation	`set radio wlan0 station-isolation off`
Set the VLAN ID for the Security Profile	`set vap vap0 with radio wlan0 vlan-id <1-4096>`

RADIUS Server Settings

The commands in Table C-10 correspond to the RADIUS Server Settings page on the Web UI.

Table C-10 RADIUS Server Settings

Task	Command
Set the IP Address of the Primary Authentication Server	`set radius-client primary-authentication-server <ip_address>`
Set the Port Number of the Primary Authentication Server	`set radius-client primary-authentication-port <port_number>`
Set the Shared Secret for the Primary Authentication Server	`set radius-client primary-authentication-key <value>`
Set the IP Address of the Secondary Authentication Server	`set radius-client secondary-authentication-server <ip_address>`
Set the Port Number of the Secondary Authentication Server	`set radius-client secondary-authentication-port <port_number>`
Set the Shared Secret for the Secondary Authentication Server	`set radius-client secondary-authentication-key <value>`
Set the IP Address of the Primary Accounting Server	`set radius-client primary-accounting-server <ip_address>`

Table C-10 RADIUS Server Settings (continued)

Task	Command
Set the Port Number of the Primary Accounting Server	`set radius-client primary-accounting-port <port_number>`
Set the Shared Secret for the Primary Accounting Server	`set radius-client primary-accounting-key <value>`
Set the IP Address of the Secondary Accounting Server	`set radius-client secondary-accounting-server <ip_address>`
Set the Port Number of the Secondary Accounting Server	`set radius-client secondary-accounting-port <port_number>`
Set the Shared Secret for the Secondary Accounting Server	`set radius-client secondary-accounting-key <value>`

Access Control

The commands in Table C-11 correspond to the Access Control page on the Web UI.

Table C-11 Access Control Settings

Task	Command
View a list of wireless clients by MAC address	`get association station`
Create a list of clients to permit access to the AP	`set bss wlan0bssvap0 mac-acl-mode accept-list`

Add a client to the Trusted Wireless Stations list	`add mac-acl wlan0bssvap0 mac <mac_address>`
	Example:
	`add mac-acl wlan0bssvap0 mac 00:01:02:03:04:05`
	`add mac-acl wlan0bssvap0 mac 00:01:02:03:04:06`

Remove a client from the Trusted Wireless Stations list	`remove mac-acl wlan0bssvap0 mac <mac_address>`
Disable MAC Access Control (remove all clients from the list)	`remove mac-acl all`

Viewing and Configuring Management Settings

The commands in Table C-12 correspond to the pages on the Web UI under the Management heading. This section includes commands for the following features:

- Change Password
- Remote Management
- Upgrade Firmware
- Backup and Restore
- Reboot the System.

Table C-12 AP Management

Task	Command
Set a password for admin access to the AP.	`set system password <password>`
Enable Remote CLI Access	`set ssh status up`
Disable Remote CLI Access	`set ssh status down`
Enable SNMP	`set snmp status up`
Disable SNMP	`set snmp status down`
Set a Public Community name	`set snmp ro-community <string>`
Set a Private Community name	`set snmp rw-community <string>`
Set an IP address to receive SNMP traps	`set traphost host <ip_address>`

Upgrade the firmware (requires a reboot)	`firmware-upgrade <url>`
	Example:
	`firmware-upgrade tftp://1.2.3.4/upgrade.tar`
	`firmware-upgrade file://1.2.3.4/tmp/upgrade.tar`

Backup the configuration file	`config download <url>`
	Example:
	`config download tftp://1.2.3.4/ defaultcfg.xml`

Restore the configuration file	`config upload <url>`
	Example:
	`config upload tftp://1.2.3.4/defaultcfg.xml`

Revert to factory default settings	`factory-reset`
Reboot the system	`reboot`

Viewing and Configuring System Information

The commands in Table C-12 correspond to the pages on the Web UI under the Information heading. This section includes commands for the following features:

- Activity Log
- Available Wireless Station List
- Statistics
- Rogue AP Detection

Table C-13 AP Information

Task	Command
View the SysLog activity log	`get log-entry`
View all SysLog server information	`get log detail`
Enable SysLog	`set log relay-enabled 1`
Disable SysLog	`set log relay-enabled 0`
Set the IP address of the SysLog server	`set log relay-host <ip_address>`
Set the port number configured in the SysLog server	`set log relay-port <port_number>`
View a list of wireless stations	`get association detail`

View interface statistics	`get interface all ip mac ssid`
	`tx-packets tx-bytes tx-errors`
	`rx-packets rx-bytes rx-errors`

Turn Rogue AP Detection On	`set radio wlan0 ap-detection on`
Turn Rogue AP Detection Off	`set radio wlan0 ap-detection off`
View a list of unknown APs	`get unknown-ap`
View a list of known APs	`get known-ap-config`
Add an AP to the Known AP list	`add known-ap-config <mac_address>`
Delete an AP from the Known AP list	`remove known-ap-config <mac_address>`
Delete all APs from the Known AP list	`remove known-ap-config all`

Table C-13 AP Information (continued)

Task	Command

Save the list of Known APs	`set known-ap-list action export config-file <file_name> config-server <tftp_server>`
	Example:
	`set known-ap-list action export config-file wg302Rogue3.cfg config-server tftp://192.168.24.10/ knownAP`

Import a list of known APs	`set known-ap-list action import config-file <file_name> config-server <tftp_server>`
	Example:
	`set known-ap-list action export config-file wg302Rogue3.cfg config-server tftp:// 192.168.24.10/knownAP`

Configuring Advanced IP Settings

The commands in Table C-14 correspond to the IP Settings page on the Web UI under the Advanced heading.

Table C-14 Advanced IP Setting s

Task	Command
View all DHCP server information	`get dhcp-server detail`
Enable the DHCP Server	`set dhcp-server status up`
Disable the DHCP Server	`set dhcp-server status down`
Set the Starting IP Address	`set dhcp-server ipstart <ip_address>`
Set the Ending IP Address	`set dhcp-server ipend <ip_address>`
Set the Subnet Mask	`set dhcp-server netmask <subnet_mask>`
Set the Gateway IP Address	`set dhcp-server gateway <ip_address>`
Set the Primary DNS Server	`set dhcp-server dns1 <ip_address>`

Table C-14 Advanced IP Setting (continued)s

Task	Command
Set the Secondary DNS Server	`set dhcp-server dns2 <ip_address>`
Set the Primary WINS Server	`set dhcp-server wins1 <ip_address>`
Set the Secondary WINS Server	`set dhcp-server wins1 <ip_address>`
Set the Lease	`set dhcp-server lease <seconds>`

Hotspot Settings

The commands in Table C-15 correspond to the Hotspot Settings page on the Web UI under the Advanced heading.

Table C-15 Hotspot Settings

Task	Command
View all HTTP redirect information	`get http-redirect`
Enable HTTP Redirect	`set http-redirect status up`
Disable HTTP Redirect	`set portal status down`
Set the URL for the redirect	`set http-redirect url <url>`

Advanced Wireless Settings

The commands in Table C-16 correspond to the Wireless Settings page on the Web UI under the Advanced heading. For information about the configuration options in this section, see "Configuring Advanced Wireless Settings" on page 4-3.

Table C-16 Advanced Wireless Settings

Task	Command
Enable Super-G Mode	`set radio wlan0 super-ag yes`
Disable Super-G Mode	`set radio wlan0 super-ag no`
Set the RTS Threshold	`set radio wlan0 rts-threshold <0-2347>`
Set the Fragmentation Length Threshold	`set radio wlan0 fragmentation-threshold <256-2346>`
Set the Beacon Interval	`set radio wlan0 beacon-interval <20-1000>`

Table C-16 Advanced Wireless Settings (continued)

Task	Command
Set the DTIM Interval	`set bss wlan0bssvap0 dtim-period <1-255>`
Enable Wi-Fi Multimedia (WMM)	`set radio wlan0 wme on`
Disable Wi-Fi Multimedia (WMM)	`set radio wlan0 wme off`
View QoS queue parameters	`get tx-queue`
AP EDCA parameters	

Set AIFS on AP-to-station traffic	`set tx-queue wlan0 with queue <Queue_Name> to aifs <AIFS_Value>`
	Example:
	`set tx-queue wlan0 with queue data0 to aifs 13`

Set cwMin and cwMax on AP-to-station traffic	`set tx-queue wlan0 with queue <Queue_Name> to cwmin <cwmin_Value> cwmax <cwmax_Value>`
	Example:
	`set tx-queue wlan0 with queue data1 cwmin 15 cwmax 31`

Set Max. Burst on AP-to-station traffic	`set tx-queue wlan0 with queue <Queue_Name> to burst <burst_Value>`
	Example:
	`set tx-queue wlan0 with queue data2 to burst 0.5`

Station EDCA parameters	

Set AIFS on station-to-AP traffic	`set wme-queue wlan0 with queue <Queue_Name> to aifs <AIFS_Value>`
	Example:
	`set wme-queue wlan0 with queue vo to aifs 14`

Set cwMin and cwMax on station-to-AP traffic	`set wme-queue wlan0 with queue <Queue_Name> to cwmin <cwmin_Value> cwmax <cwmax_Value>`
	Example:
	`set wme-queue wlan0 with queue vi cwmin 7 cwmax 15`

Set TXOP Limit on station-to-AP traffic	`set wme-queue wlan0 with queue <Queue_Name> to txop-limit <txop-limit_Value>`
	Example:
	`set wme-queue wlan0 with queue vo to txop-limit 49`

Advanced Access Point Settings

The commands in Table C-17 correspond to the Access Point Settings page on the Web UI under the Advanced heading.

Table C-17 Advanced Access Point Settings

Task	Command

Enable Wireless Bridging and Repeating	`set interface wlan0wds0 status up`
	`set interface wlan0wds0 radio wlan0`

Disable Wireless Bridging and Repeating	`set interface wlan0wds0 status down`
View the Local MAC Address for the Wireless Bridge or Repeater	`get interface wlan0wds0 mac`
Set the Remote MAC Address 1	`set interface wlan0wds0 remote-mac <remote_MAC_address>`
Set the Remote MAC Address 2	`set interface wlan0wds1 remote-mac <remote_MAC_address>`
Set the Remote MAC Address 3	`set interface wlan0wds2 remote-mac <remote_MAC_address>`
Set the Remote MAC Address 4	`set interface wlan0wds3 remote-mac <remote_MAC_address>`