Chapter 5
Advanced Configuration

This chapter describes how to configure the advanced features of your NETGEAR WG102 ProSafe 802.11g Wireless Access Point. These features can be found under the Advanced heading in the main menu.

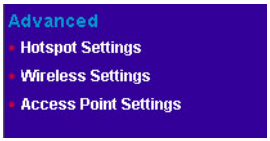

Figure 5-1

The following features are explained:

- Hotspot Settings: Redirect HTTP requests.
- Advanced Wireless Settings: Set up advanced wireless LAN parameters.
- Access Point Settings: Enable wireless bridging and repeating.

Hotspot Settings

If you want the access point (AP) 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 start a billing transaction.

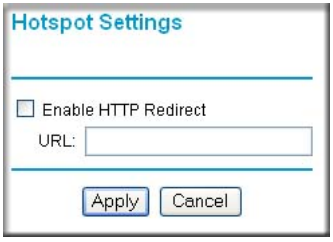

Figure 5-2

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

Advanced Wireless Settings

You can use the Advanced Wireless Settings menu to configure the following:

- AutoCell RF management
- Advanced wireless parameters

These options are discussed below.

AutoCell Overview

AutoCell provides advanced RF wireless management features that improve performance and enhance security.

Table 5-1. What does AutoCell do?

Problem	AutoCell Settings
Erosion of privacy	You can enable these two settings: • Enhanced RF Security (Default: Disable): Makes your Wi-Fi network nearly undetectable by neighbors and hackers. • Rogue Device Detection (Default: Disable): Blocks rogue wireless devices from connecting to your network.
Diminishing performance from multiple APs installed in one area.	The Auto RF Management feature (Default: Enabled) manages APs and clients load-balance traffic across underutilized APs.
Complexity of installation	With the Auto RF Management feature (Default: Enabled), the APs can be put in any convenient location and in any density.
Increasing interference	The Auto RF Management feature (Default: Enabled) lets clients and APs avoid interference from neighbors and other unexpected sources.

AutoCell's self-organizing micro cells provide an additional level of privacy for enterprises. AutoCell clients are highly-recommended for Enhanced RF Security.

AutoCell AP/Client Interaction

AutoCell's self-organizing micro cells provide performance benefits and an additional level of privacy for enterprises.

- **Automatic Transmit Power Control.** An AP with AutoCell enabled coordinates the RF transmit power level of AutoCell-enabled clients. This creates client micro-cells and reduces co-channel interference with other clients and APs on the same frequency. It also improves overall throughput and performance.
- **Automatic Load-Balancing.** An AutoCell-enabled client seeks out and associates with the lightest loaded AutoCell-enabled AP available.
- **Rapid Roaming.** An AutoCell-enabled client quickly distinguishes movement from RF anomalies such as arbitrary and momentary changes in the surrounding RF domain. When it detects true movement, the client immediately seeks the best available AP at the highest data rate possible instead of waiting for the data rate to decline. (Does not Require AutoCell-enabled APs.)

Additional AutoCell View Management Options

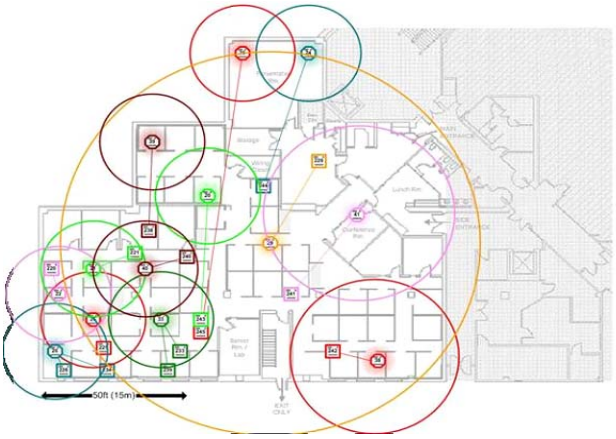

Figure 5-3

AutoCell View is a management tool that provides sophisticated views of your wireless network so that you can manage the wireless communications easily from a simple console.

AutoCell Configuration Options

There are three AutoCell configuration setting choices:

- Auto RF Management: Enabled by default.
- Enhanced RF Security: Disabled by default.
- Rogue Device Detection: Disabled by default.

These options are discussed below.

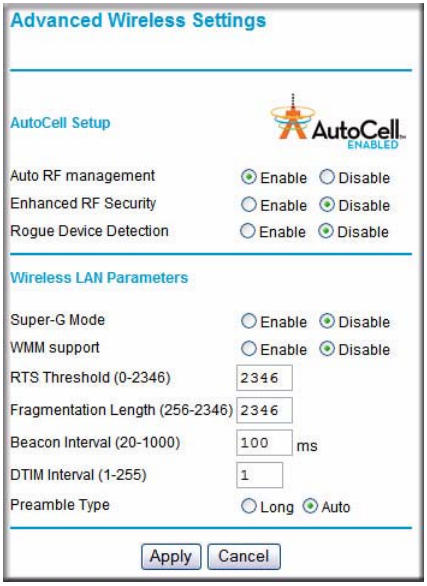

Figure 5-4

Auto RF Management

Note: Channel selection and power management is automatically adjusted by the AutoCell Auto RF Management option. The Auto RF Management option is enabled by default.

In this mode, AutoCell APs and clients load-balance traffic across underutilized APs. This mode avoids interference from neighbors, clients, APs, and other unexpected sources.

Enhanced RF Security

	Note: Broadcast Wireless Network Name (SSID) is automatically turned off when you select the AutoCell Enhanced RF Security option.

In this mode, AutoCell shrinks the size of coverage to the minimum to reach clients but also shrinks the size of the beacons that access points use to announce their presence. This mode makes an enterprise wireless LAN nearly invisible to users outside an office building.

Rogue Device Detection

The AutoCell Rogue Device Detection feature lets you identify and block wireless devices that should never be given access to the wireless network.

Configuring Advanced Wireless LAN Settings

The default advanced wireless LAN settings usually work well. If you want the AP to operate in Super-G mode, use this feature.

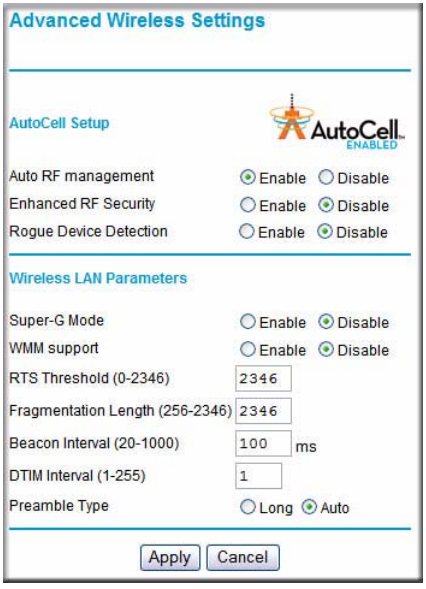

Figure 5-5

The advanced wireless settings normally do not need to be changed.

- **Super-G Mode.** Super-G Mode is a proprietary extension to the 802.11g standard, which can double the throughput to 108Mbps. Only compatible wireless stations can use this mode. The default is Disable.
- **WMM support.** WMM (Wireless Multimedia) 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, have a higher priority than normal traffic. For WMM to work correctly, wireless clients must also support WMM. The default is Disable.
- **RTS Threshold.** Request to Send Threshold. The packet size that is used to determine if it should use the Carrier Sense Multiple Access with Collision Detection mechanism (CSMA/CD) or the CSMA/CA mechanism for packet transmission. With CSMA/CD, the transmitting station sends the packet as soon as it has waited for the silence period. With CSMA/CA, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a Clear to Send (CTS) packet before sending the packet data. The default is 2346.
- **Fragmentation Length.** This is the maximum packet size used for fragmentation. Packets larger than this size will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval.** The interval time (between 20ms and 1000ms) for each beacon transmission. The default is 100.
- **DTIM Interval.** The Delivery Traffic Indication Message (DTIM) specifies the data beacon rate between 1 and 255. The default is 1.
- **Preamble Type.** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto automatically handles both long and short preambles. The default is Auto.

Wireless Bridging and Repeating

The WG102 Access Point lets you build large bridged wireless networks.

	**Note:** All bridge mode options are not available when AutoCell Auto RF Management is enabled (the default setting).

Examples of wireless bridged configurations are:

- Point-to-Point Bridge. The WG102 communicates with another bridge-mode wireless station. See “Point-to-Point Bridge Configuration” on page 5-8.
- Multi-Point Bridge. The WG102 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 5-9.
- Repeater with Wireless Client Association. Sends all traffic to the remote AP. See “Repeater with Wireless Client Association” on page 5-11.

These configurations can be set up from the Advanced Access Point Settings menu, shown to the right.

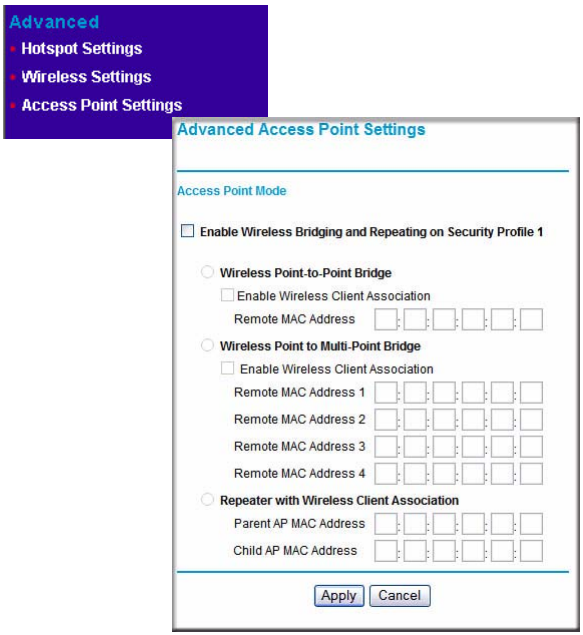

Figure 5-6

Point-to-Point Bridge Configuration

In Point-to-Point Bridge mode, the WG102 communicates with another bridge-mode wireless station. In addition, you can enable client associations with this WG102. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use WEP to protect this communication. The figure below shows an example of Point-to-Point Bridge mode.

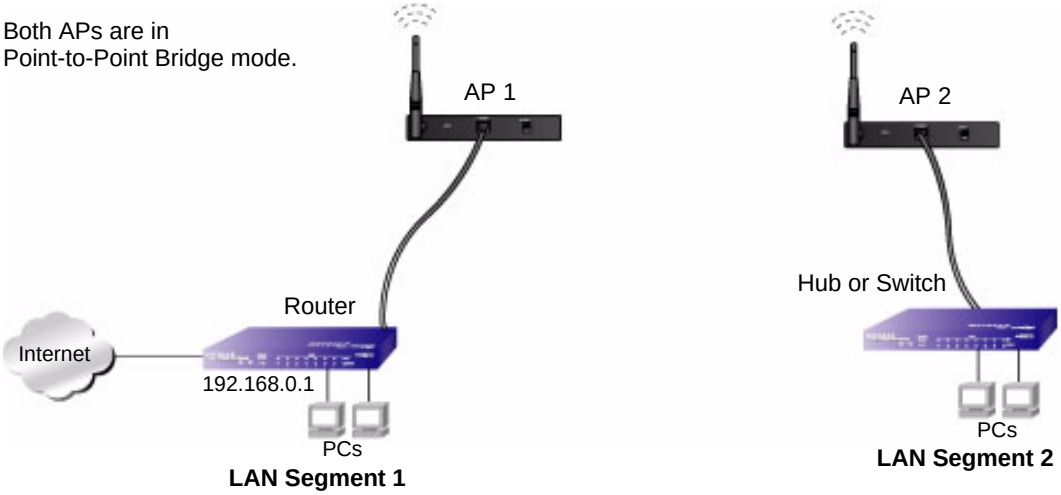

Figure 5-7

Follow the steps below to set up a Point-to-Point Bridge configuration.

1. Configure the WG102 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the other access point (AP2) 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 must be configured to operate in the same LAN network address range as the LAN devices
   - Both APs must use the same ESSID, 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

Set up a Multi-Point Bridge only if this WG102 is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this "master," rather than to the other access points. In addition, you can enable client associations with this WG102.

- You must enter the MAC addresses of the other access points in the fields provided.
- The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using the MAC address of this WG102 as the Remote MAC Address.
- Use WEP to protect this traffic.

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

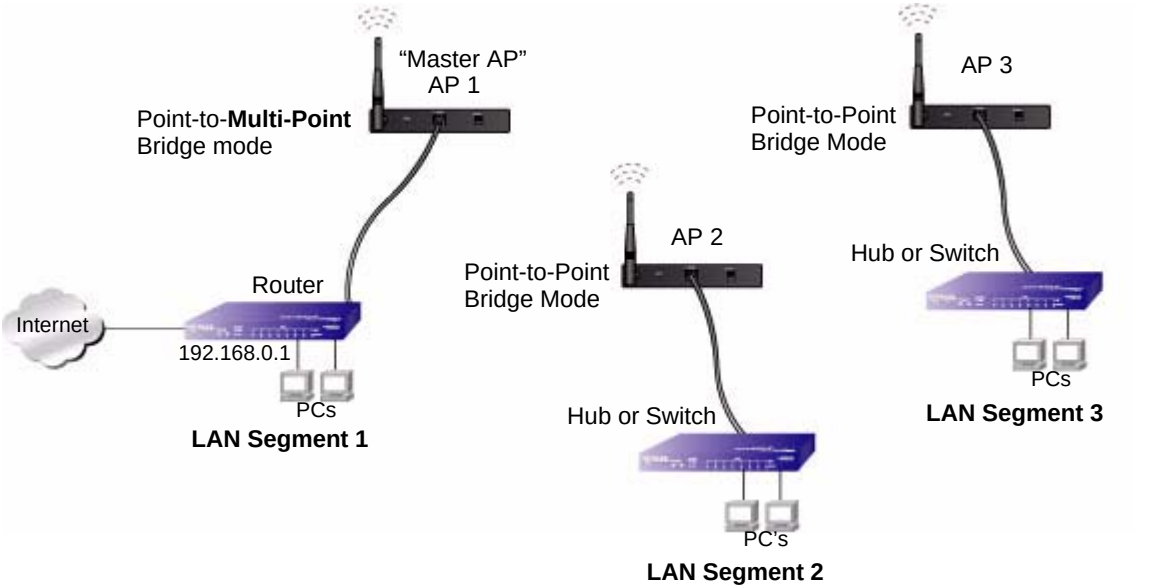

Figure 5-8

Follow the steps below to set up the Multi-Point Bridge configuration.

1. Configure the Operating Mode of the WG102 Access Points.
    - Because it is in the central location, configure WG102 (AP 1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode. The MAC addresses of AP2 and AP3 are required in AP1.
    - Configure WG102 (AP 2) on LAN Segment 2 in Point-to-Point Bridge mode with the Remote MAC Address of AP1.

- Configure the WG102 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP1.

2. Verify the following for all access points:
   - The LAN network configuration of the WG102 Access Points 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 APs LAN IP address must be in the same network.
   - If using DHCP, all WG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
   - All WG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
   - All Point-to-Point APs must have AP2’s MAC address in its 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 WG102 Access Points in the illustration above. If you require wireless stations to access any LAN segment, you can use additional WG102 Access Points configured in Wireless Access Point mode to any LAN segment.

	**Note:** You can extend this multi-point bridging by adding additional WG102s 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 WG102 Access Point 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 WG102.
- 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.

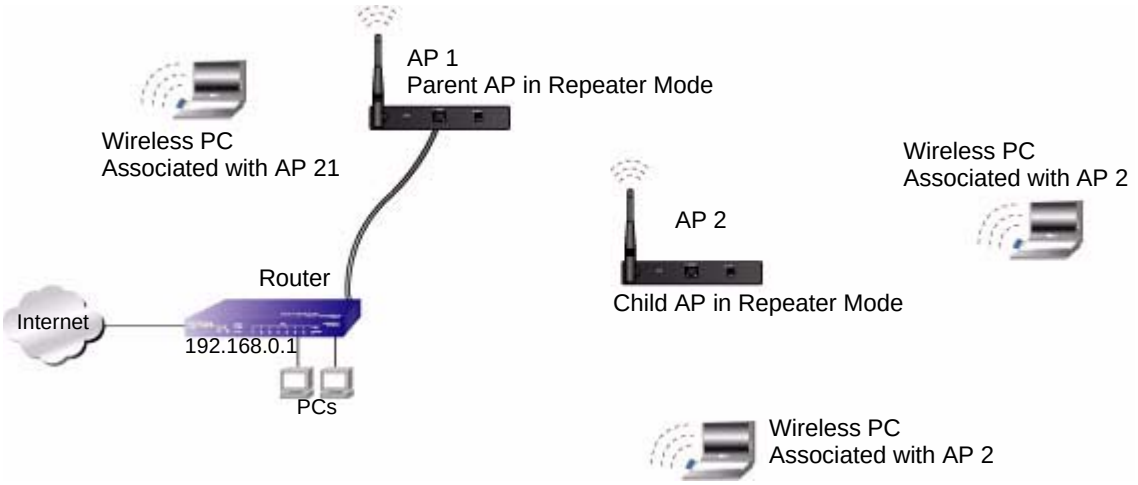

Figure 5-9

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

1. Configure the Operating Mode of the WG102 Access Points.
    - Configure AP 1 on LAN Segment 1 as the Parent in Repeater mode with the its own MAC address in the Parent AP MAC Address field, and the MAC Address of the ‘downstream’ AP (AP 2) in the Child AP MAC Address field.
    - Configure AP 2 in the Child Repeater mode with its MAC addresses as in the Child AP MAC Address field and the MAC address of the ‘upstream’ AP (AP 1) in the Parent MAC Address field.
2. Verify the following for all access points:
    - The LAN network configuration of the WG102 Access Points 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 WG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- All WG102 Access Points 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 WG102s 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.