

---

*Administrator's Handbook*

---

ARRIS® Embedded Software Version 9.1.4h0d51

## ARRIS® NVG599 VDSL2 Gateway



## **Copyright**

©ARRIS Enterprises, Inc. 2014 All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS Enterprises, Inc. ("ARRIS"). ARRIS reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

ARRIS and the ARRIS logo are all trademarks of ARRIS Enterprises, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and the names of their products. ARRIS disclaims proprietary interest in the marks and names of others. MOTOROLA and the Stylized M logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC. and are used by ARRIS under license. All other product or service names are the property of their respective owners.

ARRIS provides this guide without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. ARRIS may make improvements or changes in the product(s) described in this manual at any time.

The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.

EXCEPT AS INDICATED IN THE APPLICABLE SYSTEM PURCHASE AGREEMENT, THE SYSTEM, DOCUMENTATION AND SERVICES ARE PROVIDED "AS IS", AS AVAILABLE, WITHOUT WARRANTY OF ANY KIND. ARRIS GROUP, INC. ("ARRIS") DOES NOT WARRANT THAT THE SYSTEM WILL MEET CUSTOMER'S REQUIREMENTS, OR THAT THEIR OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ANY ERRORS CAN OR WILL BE FIXED. ARRIS HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ORAL OR WRITTEN, WITH RESPECT TO THE SYSTEM AND SERVICES INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, INTEGRATION, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND ALL WARRANTIES ARISING FROM ANY COURSE OF DEALING OR PERFORMANCE OR USAGE OF TRADE.

EXCEPT AS INDICATED IN THE APPLICABLE SYSTEM PURCHASE AGREEMENT, ARRIS SHALL NOT BE LIABLE CONCERNING THE SYSTEM OR SUBJECT MATTER OF THIS DOCUMENTATION, REGARDLESS OF THE FORM OF ANY CLAIM OR ACTION (WHETHER IN CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE), FOR ANY (A) MATTER BEYOND ITS REASONABLE CONTROL, (B) LOSS OR INACCURACY OF DATA, LOSS OR INTERRUPTION OF USE, OR COST OF PROCURING SUBSTITUTE TECHNOLOGY, GOODS OR SERVICES, (C) INDIRECT, PUNITIVE, INCIDENTAL, RELIANCE, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF BUSINESS, REVENUES, PROFITS OR GOODWILL, OR (D) DIRECT DAMAGES, IN THE AGGREGATE, IN EXCESS OF THE FEES PAID TO IT HEREUNDER FOR THE SYSTEM OR SERVICE GIVING RISE TO SUCH DAMAGES DURING THE 12-MONTH PERIOD PRIOR TO THE DATE THE CAUSE OF ACTION AROSE, EVEN IF COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS ARE INDEPENDENT FROM ALL OTHER PROVISIONS OF THIS AGREEMENT AND SHALL APPLY NOTWITHSTANDING THE FAILURE OF ANY REMEDY PROVIDED HEREIN.

All ARRIS products are furnished under a license agreement included with the product. If you are unable to locate a copy of the license agreement, please contact ARRIS.

Part Number

596491-001-00

V9.1.4h0d51

---

---

# Table of Contents

## **CHAPTER 1 - Introduction . . . . . 7**

About ARRIS Documentation . . . . .	7
Related Documentation . . . . .	7
Documentation Conventions . . . . .	8
General . . . . .	8
Internal Web Interface . . . . .	8
Command Line Interface . . . . .	8
Organization . . . . .	9
A Word About Example Screens . . . . .	9

## **CHAPTER 2 - Device Configuration . . . . . 11**

Important Safety Instructions . . . . .	12
POWER SUPPLY INSTALLATION . . . . .	12
TELECOMMUNICATION INSTALLATION . . . . .	12
COAX INSTALLATION . . . . .	12
PRODUCT VENTILATION . . . . .	12
Status Indicator Lights . . . . .	13
Battery Installation (optional) . . . . .	16
Battery Door Instructions . . . . .	17
Set up the ARRIS Gateway . . . . .	18
Microsoft Windows: . . . . .	18
Macintosh MacOS 8 or higher or Mac OS X: . . . . .	20
Accessing the Web Management Interface . . . . .	21
Broadband Network Redirect Pages . . . . .	22
IP Diagnostics Page Redirect . . . . .	23
Offline Troubleshooting . . . . .	23
Device Status Page . . . . .	24
Device Access Code . . . . .	24
Tab Bar . . . . .	27
Help . . . . .	27
Links Bar . . . . .	27
Device List . . . . .	28
System Information . . . . .	29
Access Code . . . . .	30
Remote Access . . . . .	31
Battery . . . . .	32
Restart Device . . . . .	33
Broadband Tab . . . . .	34
Broadband Status . . . . .	34
Configure . . . . .	37
IGMP Stats . . . . .	38

---

Home Network Tab .....	<b>39</b>
Configure .....	42
HPNA Configure .....	42
WiFi .....	43
Wireless Security .....	45
MAC Filtering .....	47
WiFi Scan .....	48
Subnets & DHCP .....	49
IP Allocation .....	50
HPNA .....	52
Voice .....	<b>54</b>
Line Details .....	55
Call Statistics .....	56
Firewall .....	<b>59</b>
Packet Filter .....	60
Working with Packet Filters .....	62
NAT/Gaming .....	67
Custom Services .....	68
IP Passthrough .....	72
Firewall Advanced .....	75
Diagnostics .....	<b>77</b>
Logs .....	80
Update .....	82
Resets .....	83
Syslog .....	84
Event Notifications .....	84
NAT Table .....	85

**CHAPTER 3 - Basic Troubleshooting .....** **87**

Status Indicator Lights .....	<b>88</b>
LED Function Summary Matrix .....	91
Factory Reset Switch .....	<b>95</b>
Log Event Messages .....	<b>96</b>

**CHAPTER 4 - Command Line Interface .....** **101**

Overview .....	<b>103</b>
Starting and Ending a CLI Session .....	<b>105</b>
Logging In .....	105
Ending a CLI Session .....	105
Using the CLI Help Facility .....	<b>106</b>
About SHELL Commands .....	<b>106</b>
SHELL Prompt .....	106
SHELL Command Shortcuts .....	106
SHELL Commands .....	<b>107</b>
Common Commands .....	107
WPS Commands .....	116

---

---

WAN Commands . . . . .	116
<b>About CONFIG Commands . . . . .</b>	<b>118</b>
CONFIG Mode Prompt . . . . .	118
Navigating the CONFIG Hierarchy . . . . .	118
Entering Commands in CONFIG Mode . . . . .	118
Guidelines: CONFIG Commands . . . . .	119
Displaying Current Gateway Settings . . . . .	119
Step Mode: A CLI Configuration Technique . . . . .	119
Validating Your Configuration . . . . .	120
<b>CONFIG Commands . . . . .</b>	<b>121</b>
Connection Commands . . . . .	121
Filter Set Commands . . . . .	124
Global Filter Set ("IPv6 Firewall") Commands . . . . .	128
Queue Commands . . . . .	129
IP Gateway Commands . . . . .	132
IPv6 Commands . . . . .	132
IP DNS Commands . . . . .	139
IP IGMP Commands . . . . .	139
NTP Commands . . . . .	142
Application Layer Gateway (ALG) Commands . . . . .	142
Dynamic DNS Commands . . . . .	143
Link Commands . . . . .	143
Management Commands . . . . .	146
Remote Access Commands . . . . .	148
Physical Interfaces Commands . . . . .	150
PPPoE Relay Commands . . . . .	157
NAT Pinhole Commands . . . . .	157
Security Stateful Packet Inspection (SPI) Commands . . . . .	158
VoIP Commands . . . . .	160
Targeted Ad Insertion Commands . . . . .	171
System Commands . . . . .	173
<b>Debug Commands . . . . .</b>	<b>178</b>
Disclaimer and Warning Text . . . . .	178
Commands . . . . .	178
TR-069 CLI CShell Commands (debug mode) . . . . .	178

## **CHAPTER 5 - Technical Specifications and Safety Information . . . . . 179**

Description . . . . .	<b>179</b>
Power Supply . . . . .	179
Environment . . . . .	179
Software and protocols . . . . .	179
Agency approvals . . . . .	<b>180</b>
Manufacturer's Declaration of Conformance . . . . .	<b>181</b>
Important Safety Instructions . . . . .	<b>183</b>
47 CFR Part 68 Information . . . . .	<b>184</b>
FCC Requirements . . . . .	184
FCC Statements . . . . .	184
RF Exposure Statement: . . . . .	<b>185</b>

---

Electrical Safety Advisory .....	185
Caring for the Environment by Recycling .....	186
Beskyttelse af miljøet med genbrug .....	186
Umweltschutz durch Recycling.....	186
Cuidar el medio ambiente mediante el reciclaje .....	186
Recyclage pour le respect de l'environnement.....	186
Milieubewust recycleren .....	187
DbáºoËç o Êrodowisko - recykling .....	187
Cuidando do meio ambiente através da reciclagem .....	187
Var rädd om miljön genom återvinning.....	187
Copyright Acknowledgments .....	189
Open Source Software Information .....	189

**Appendix A - ARRIS Gateway Captive Portal Implementation ..... 213**

Overview .....	214
Captive Portal RPC .....	215
X_00D09E_GetCaptivePortalParams RPC:.....	215
X_00D09E_SetCaptivePortalParams RPC:.....	216

**Appendix B - Quality of Service (QoS) Examples ..... 217**

Overview .....	218
Upstream QoS: Priority and Shaping .....	220
Downstream QoS: Ethernet Switch .....	221
Downstream QoS: Egress queues .....	221

**Index ..... 223**

---

# CHAPTER 1 Introduction

## About ARRIS Documentation

This guide describes the wide variety of features and functionality of the ARRIS NVG599 Gateway, when used in Router mode. The NVG599 device can also be delivered in Bridge mode. In Bridge mode, the NVG599 acts as a pass-through device and allows the workstations on your LAN to have public addresses directly on the Internet. Documentation for the NVG599 in Bridge mode is available for download.



---

**NOTE::**

For the purposes of this manual the “ARRIS NVG599 Gateway” will be referred to as the “NVG599.”

---

## Related Documentation

ARRIS provides a suite of technical documents for its family of intelligent enterprise and consumer gateways. This documentation consists of:

- ◆ Administrator’s Handbook (this document)
- ◆ Dedicated user manuals
- ◆ Specific white papers covering related technology

The documents are available in electronic form as Portable Document Format (PDF) files. They can be viewed (and printed) from Adobe Acrobat Reader, Exchange, or any other application that supports PDF files.

## Documentation Conventions

This manual uses the following conventions to present information.


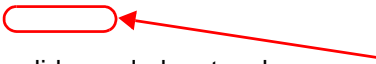
### General

The following typographic conventions are used in this guide.

Convention	Description
<b>bold sans serif</b>	Menu commands and button names
<u>underlined sans serif</u>	Web GUI page links
terminal	Computer display text
<b>bold terminal</b>	User-entered text
<i>italic</i>	The complete titles of manuals

### Internal Web Interface

The following graphic conventions are used when describing elements of the Web interface in this guide.

Convention (Graphics)	Description
 blue border	An excerpt from a Web page or the visual truncation of a Web page
 solid rounded rectangle with an arrow	An area of emphasis on a Web page

### Command Line Interface

Syntax conventions for the command line interface are as follows.

Convention	Description
[ ]	Optional command arguments are shown with straight brackets
{ }	Alternative values for an argument are presented in curly ({} ) brackets, with values separated by vertical bars ( ).
<b>bold</b>	User-entered text
<i>italic</i>	Variables for which you supply your own values



---

## Organization

This guide consists of five chapters, two appendixes, and an index. It is organized as follows:

- ◆ **Chapter 1, “Introduction”** — Describes the ARRIS® document suite and the purpose of, audience for, and structure of this guide. It includes a table of style conventions.
- ◆ **Chapter 2, “Device Configuration”** — Describes how to get up and running with your NVG599.
- ◆ **Chapter 3, “Basic Troubleshooting”** — Gives some simple suggestions for troubleshooting problems with the initial configuration of your NVG599.
- ◆ **Chapter 4, “Command Line Interface”** — Describes all the current text-based commands for both the SHELL and CONFIG modes. A summary table and individual command examples for each mode are provided.
- ◆ **Chapter 5, “Technical Specifications and Safety Information”** — Presents system and device specifications and important compliance and safety statements.
- ◆ **Appendix A, “ARRIS Gateway Captive Portal Implementation”** — Describes the ARRIS Gateway Captive Portal Implementation.
- ◆ **Appendix B, “Quality of Service (QoS) Examples”** — Describes the ARRIS Gateway Quality of Service (QoS) Implementation.

## A Word About Example Screens

This manual contains many example screen illustrations. Since ARRIS gateways offer a wide variety of features and functionality, the example screens shown may not exactly match the screens for your particular device or setup. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.



---

## CHAPTER 2      Device Configuration

Most users will find that the basic Quick Start configuration is sufficient to meet their needs. The Quick Start section may be all that you need to configure and use your ARRIS NVG599 Gateway. For more advanced users, a rich feature set is available. The following instructions cover installation in Router mode.

This chapter covers:

- ◆ [“Important Safety Instructions” on page 12](#)
- ◆ [“Status Indicator Lights” on page 13](#)
- ◆ [“Battery Installation \(optional\)” on page 16](#)
- ◆ [“Battery Door Instructions” on page 17](#)
- ◆ [“Set up the ARRIS Gateway” on page 18](#)
- ◆ [“Accessing the Web Management Interface” on page 21](#)
- ◆ [“Device Status Page” on page 24](#)
- ◆ [“Tab Bar” on page 27](#)
- ◆ [“Broadband Tab” on page 34](#)
- ◆ [“Home Network Tab” on page 39](#)
- ◆ [“WiFi” on page 43](#)
- ◆ [“Voice” on page 54](#)
- ◆ [“Firewall” on page 59](#)
- ◆ [“Diagnostics” on page 77](#)

## Important Safety Instructions

### POWER SUPPLY INSTALLATION

Connect the power supply cord to the power jack on the NVG599. Plug the power supply into an appropriate electrical outlet. There is no power (on / off) switch to power off the device.



**WARNING:**

The power supply must be connected to a mains outlet with a protective earth connection. Do not defeat the protective earth connection.

**CAUTION:**

Depending on the power supply provided with the product, either the direct plug-in power supply blades, power supply cord plug or the appliance coupler serves as the mains power disconnect. It is important that the direct plug-in power supply, socket-outlet or appliance coupler be located so it is readily accessible.

---

### TELECOMMUNICATION INSTALLATION

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury, including the following:

- ◆ This device is intended for indoor use only.



**RESTRICTIONS:**

- ◆ Do not install this device out doors.
- ◆ This device is restricted from transmitting in 5600-5650 MHz band.

**WARNING:**

- ◆ Installing and operating this device out doors is a violation of FCC rules.

- ◆ Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
  - ◆ Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
  - ◆ Do not use the telephone to report a gas leak in the vicinity of the leak.
  - ◆ **CAUTION:** The external phone should be UL listed, and the connections should be made in accordance with Article 800 of the NEC.
  - ◆ **CAUTION:** To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- 

### COAX INSTALLATION

Ensure that the outside coaxial cable system is grounded, so as to provide some protection against voltage surges and built-up static charges. Article 820-20 of the NEC (Section 54, Part I of the Canadian Electrical Code) provides guidelines for proper grounding and, in particular, specifies that the CATV cable ground be connected to the grounding system of the building, as close to the point of cable entry as practical.

### PRODUCT VENTILATION

The NVG599 is intended for use in a consumer's home. Ambient temperatures should not exceed 104 F (40 C). The NVG599 should not be used in locations exposed to outside heat radiation or where it is subject to trapping of its own heat. The product should have at least one inch of clearance on all sides except the bottom when properly installed and should not be placed inside tightly enclosed spaces unless proper ventilation is provided.



**WARNING:**

The battery used in this device may present a risk of fire or chemical burn if mistreated. Do not disassemble, heat above manufacturer's maximum temperature limit, or incinerate. Replace battery with ARRIS P/N 586185-002-00 only. Use of another battery may present a risk of fire or explosion.

Dispose of used battery promptly. Keep away from children. Do not disassemble and do not dispose of in fire.

---

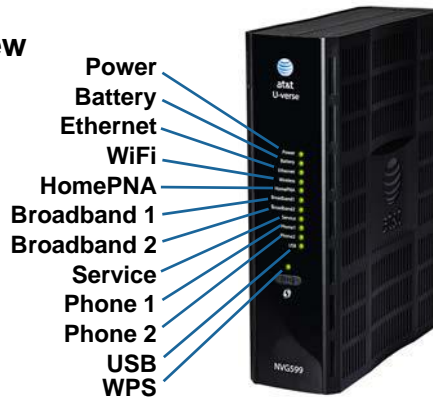
### SAVE THESE INSTRUCTIONS

## Status Indicator Lights

Colored LEDs on your NVG599 indicate the activity status of various ports.


### ARRIS NVG599 Status Indicator Lights

#### Side View

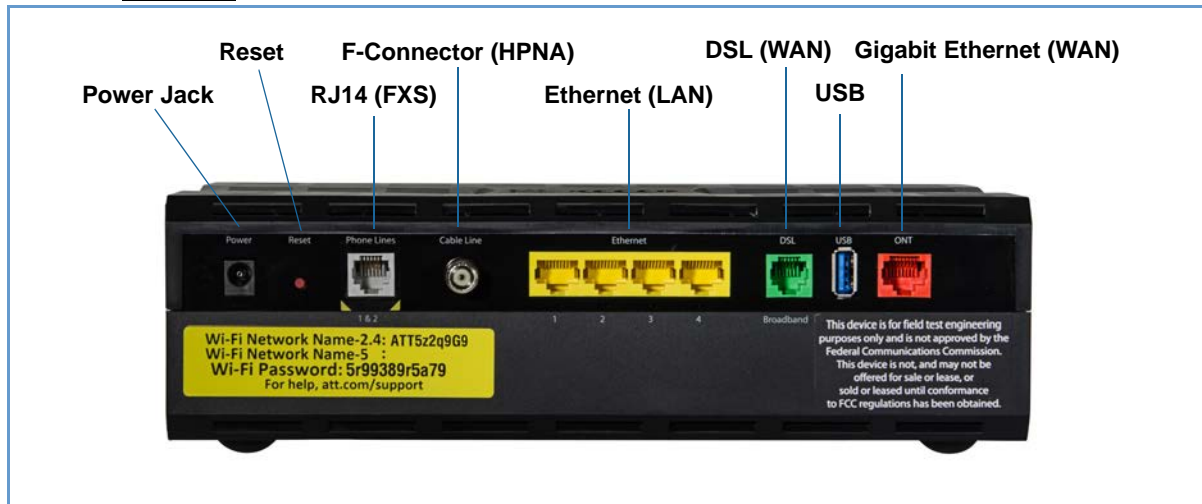


LED	Activity
<b>Power</b>	<p><b>Solid Green</b> = The device is powered.</p> <p><b>Flashing Green</b> = A power-on self-test (POST) is in progress</p> <p><b>Flashing Red</b> = A POST failure (not bootable) or device malfunction occurred.</p> <p><b>Flashing Amber</b> = Firmware upgrade in progress (see below)</p> <p>Off = The unit has no AC power. If the battery is in use, the Battery LED will indicate battery status, and all other LEDs will be off.</p>
<b>Power during Firmware Upgrade</b>	<p>During the software installation, you will lose Internet and phone service. The LEDs will function as follows:</p> <ol style="list-style-type: none"> <li>As firmware is being loaded into flash, the LEDs operate normally.</li> <li>During the firmware upgrade, which takes a few minutes, the Power LED will flash amber (flash writing to memory), and all other LEDs are off.</li> <li>The NVG599 restarts automatically. As the device reboots, the LEDs display power-on behavior.</li> </ol>
<b>All during Boot process</b>	<ul style="list-style-type: none"> <li>Power LED = <b>Flashing Green</b></li> <li>All other LEDs = Off</li> </ul> <p>If the device does not boot and fails its self-test or fails to perform initial load of the bootloader:</p> <ul style="list-style-type: none"> <li>Power LED = <b>Flashing Red</b></li> <li>ALL other LEDs = Off</li> </ul> <p>If the device boots and then detects a failure:</p> <p>Power LED = <b>Flashing Green</b> starting POST, and then all LEDs will <b>flash red</b>, including Power LED.</p>
<b>Battery</b>	<p><b>Solid Green</b> = Battery in place but not being used.</p> <p><b>Flashing Green</b> = Battery charging.</p> <p><b>Solid Red</b> = Battery backup mechanism has a fault.</p> <p><b>Flashing Red</b> = Battery needs to be replaced.</p> <p><b>Solid Amber</b> = Battery in use.</p> <p><b>Flashing Amber</b> = Low battery.</p> <p>Off = No battery, or battery has no charge.</p>

LED	Activity
Ethernet	<p><b>Solid Green</b> = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).</p> <p><b>Flickering Green</b> = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.</p> <p><b>Off</b> = The device is not powered, or no cable or no powered devices are connected to the associated ports.</p>
WiFi	<p><b>Solid Green</b> = Wi-Fi is powered.</p> <p><b>Flickering Green</b> = Activity seen from devices connected via Wi-Fi. The flickering of the light is synchronized to actual data traffic.</p> <p><b>Off</b> = The device is not powered, or no powered devices are connected to the associated ports.</p>
HomePNA	<p><b>Solid Green</b> = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).</p> <p><b>Flickering Green</b> = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.</p> <p><b>Off</b> = The device is not powered, or no cable or no powered devices are connected to the associated ports.</p>
Broadband 1**, 2	<p><b>Solid Green</b> = Good broadband connection (good DSL sync or Gigabit Ethernet).</p> <p><b>Flashing Green</b> = Attempting broadband connection (DSL attempting sync).</p> <p><b>Flashing Green and Red</b> = If, after three consecutive minutes, the broadband connection fails to be established, the LED switches to <b>Flashing Green</b> alternating with a five second steady <b>Red</b> while attempting or waiting to establish a broadband connection. This pattern continues until the broadband connection is successfully established.</p> <p><b>Flashing Red</b> = No DSL signal on the line. This display is not used during times of temporary 'no tone' during the training sequence.</p> <p><b>Off</b> = The device is not powered.</p> <p>** <b>Broadband 1 LED</b> is also the Gigabit Ethernet WAN LED when that is in play (and DSL is not).</p>
Service	<p><b>Solid Green</b> = IP connected. The device has a WAN IP address from DHCP or 802.1x authentication and the broadband connection is up.</p> <p><b>Flashing Green</b> = Attempting connection, attempting IEEE 802.1X authentication, or attempting to obtain DHCP information.</p> <p><b>Red</b> = Device attempted to become IP connected and failed (no DHCP response, 802.1x authentication failed, no IP address from IPCP, etc.). The <b>Red</b> state times out after two minutes, and the Service indicator light returns to the Off state.</p> <p><b>Off</b> = The device is not powered or the broadband connection is not present.</p>
Phone 1, 2	<p><b>Solid Green</b> = The associated VoIP line has been registered with a SIP proxy server.</p> <p><b>Flashing Green</b> = Indicates a telephone is off-hook on the associated VoIP line.</p> <p><b>Off</b> = VoIP not in use, line not registered, or gateway power off.</p>
USB	<p><b>Solid Green</b> = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to the Ethernet connection).</p> <p><b>Flickering Green</b> = Activity seen from devices associated with the port. The flickering of the light is synchronized to actual data traffic.</p> <p><b>Off</b> = The device is not powered, no cable or no powered devices connected to the associated ports.</p>

LED	Activity
<b>WPS</b> <b>(appears after using WPS button)</b> 	<b>Solid Green</b> = Wi-Fi Protected Setup has been completed successfully. LED should stay on for 5 minutes or until push button is pressed again. <b>Flashing Green</b> = Continues for 2 minutes, indicating when WPS is broadcasting. <b>Flashing Red</b> = Continues for 2 minutes, indicating a Session overlap was detected (possible security risk). <b>Solid Red</b> = Error unrelated to security, such as failure to find a partner, or WPS is disabled. LED should stay solid red for 5 minutes or until push button is pressed again. <b>Off</b> = The device is ready for WPS authentication.

**Rear View**



LED	Activity
<b>Ethernet</b> <b>1, 2, 3, 4</b>	<b>Flashing Amber</b> = A Gigabit Ethernet device is connected to each port. <b>Solid Green</b> = A 10/100 Ethernet device is connected. <b>Flickering Green</b> = Ethernet traffic activity. <b>Off</b> = The device is not powered, or no powered devices are connected to the associated ports.



**NOTE:**

The NVG599 supports two VoIP lines over one RJ14 (FXS) VoIP port. In order to connect two phone lines, the supplied inner/outer pair splitter adapters must be attached to the RJ14 (FXS) VoIP port in order to terminate both lines. This is a special-purpose splitter. You must use only the inner/outer pair splitter adapters supplied by AT&T.



## Battery Installation (optional)

The optional backup battery is located in a compartment on the bottom of the unit. Installing the battery door requires some care.



### CAUTION:

The battery used in this device may present a risk of fire or chemical burn if mistreated. Do not disassemble, heat above manufacturer's maximum temperature limit, or incinerate. Replace battery with ARRIS P/N 586185-002-00 only. Use of another battery may present a risk of fire or explosion.

Dispose of used battery promptly. Keep away from children. Do not disassemble and do not dispose of in fire.

1. Note the tab on the bottom of the battery.



2. Insert the battery into the compartment on the bottom of the unit, as shown, and press into place so that the battery contacts seat securely in the unit.



Battery Compartment Door

3. Close the compartment door. See [“Battery Door Instructions” on page 17.](#)



---

## Battery Door Instructions

1. Place NVG599 unit on a tabletop with the battery door side up.
2. Push in and upward to open the battery door as shown in Figure 1.



**Figure 1**



**Figure 2**



**Figure 3**

3. Swing back the battery door. See Figure 2.
4. Insert the battery in the compartment as shown in Figure 3.
5. Swing the door back down and snap closed.

## Set up the ARRIS Gateway

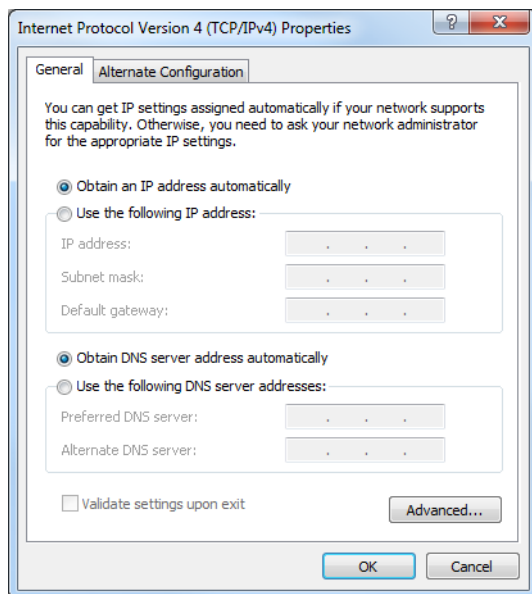
Refer to your Quick Start Guide for instructions on how to connect your NVG599 to your power source, PC, or local area network, and your Internet access point, whether it is a dedicated DSL outlet or a DSL or cable modem. Be sure to enable dynamic addressing on your PC. To set up the gateway, complete the following steps:

### Microsoft Windows:

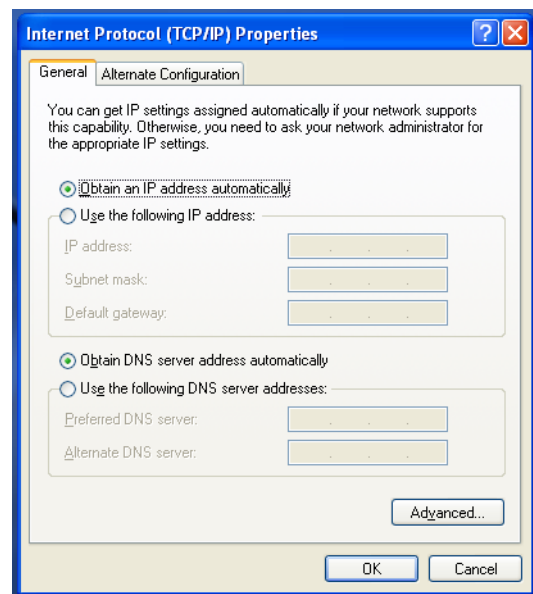
1. Navigate to the TCP/IP Properties control panel to configure the IP address using one of the suggested pathways that follow. Note that Windows Vista and Windows 7 obtain an IP address automatically by default. You may not need to configure it at all.

Windows 7 follows a path like this: **Start menu -> Control Panel -> Network and Sharing Center -> Change adapter settings -> Local Area Connection -> Change settings of this connection -> Local Area Connection Properties -> Internet Protocol (TCP/IP) -> Properties**

Windows XP follows a path like this: **Start menu -> Settings -> Control Panel -> Network Connections -> Local Area Connection -> Internet Protocol [TCP/IP] -> Properties**



Windows 7

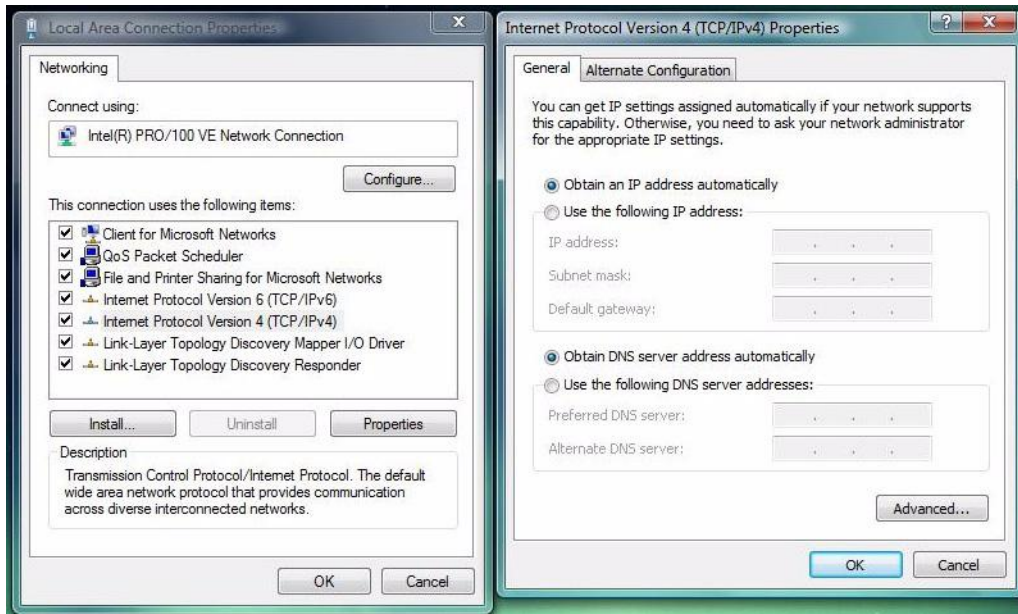


Windows XP

2. Select **Obtain an IP address automatically**.
3. Select **Obtain DNS server address automatically**, if available.
4. Remove any previously configured gateways, if available.
5. OK the settings. Restart if prompted.

To check:

1. Open the Networking control panel and select **Internet Protocol Version 4 (TCP/IPv4)**.
2. Click the **Properties** button. The Internet Protocol Version 4 (TCP/IPv4) Properties window should appear as shown.



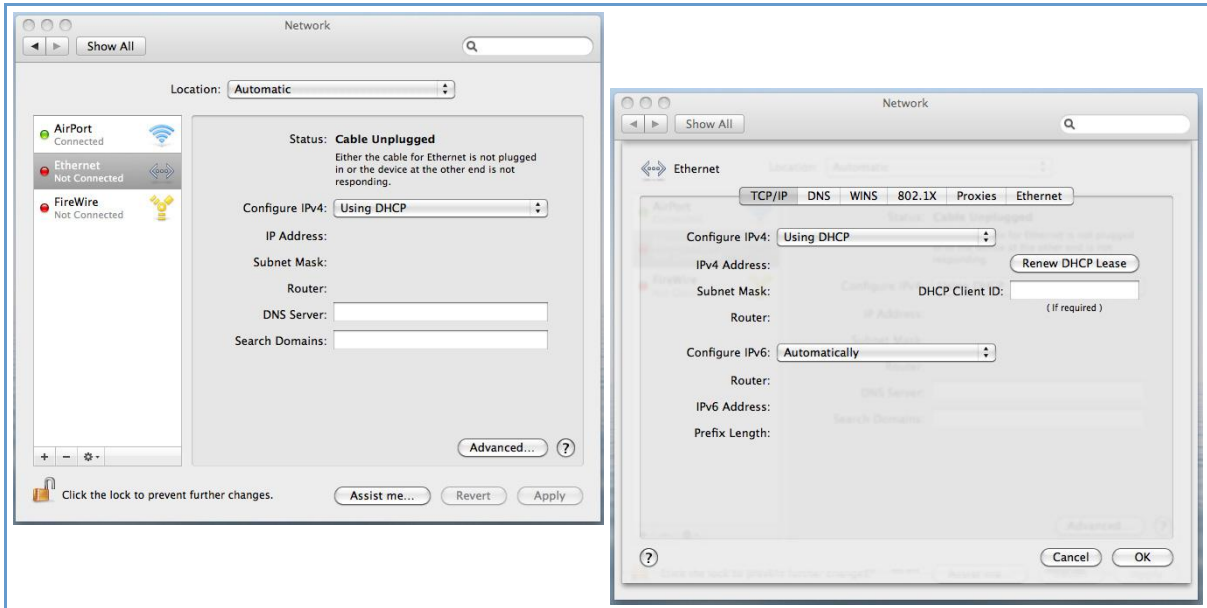
**Windows Vista**

3. Set the radio buttons to the values shown above, and click the **OK** button.

## Macintosh MacOS 8 or higher or Mac OS X:

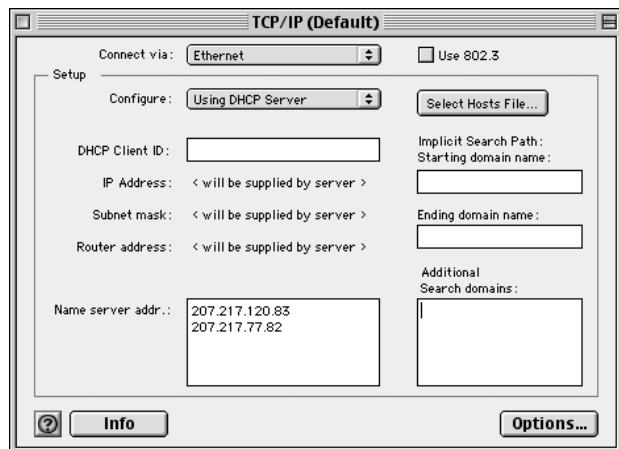
1. Access the **TCP/IP** or **Network** control panel.
  - ◆ Mac OS X follows a path like this:

Apple Menu -> **System Preferences** -> **Network**



- ◆ MacOS Classic follows a path like this:

Apple Menu -> **Control Panels** -> **TCP/IP Control Panel**

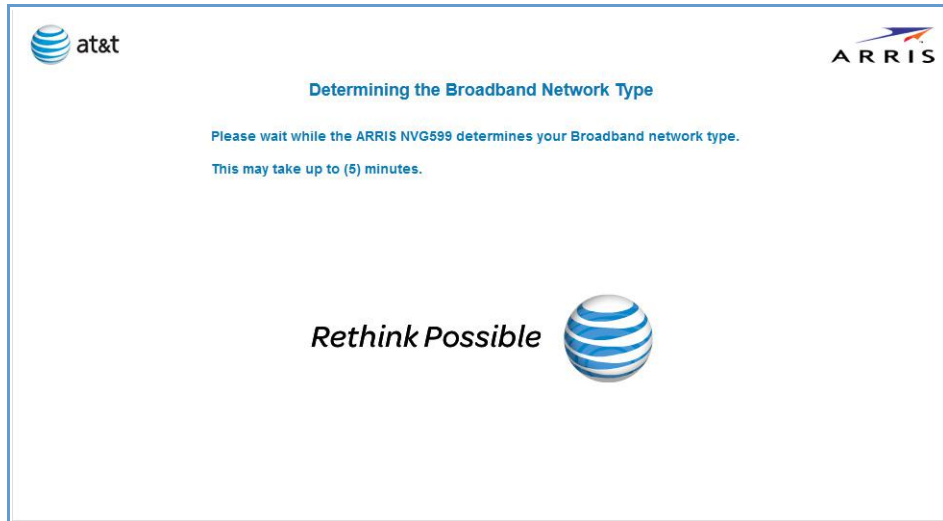


2. Select **Ethernet**.
3. Select **Configure Using DHCP**.
4. Close and save, if prompted.

Proceed to [“Accessing the Web Management Interface”](#) on page 21.

## Accessing the Web Management Interface

1. Run your Web browser application, such as Firefox or Microsoft Internet Explorer, from the computer connected to the NVG599 device.
2. Enter <http://192.168.1.254> in the Location text box.  
While the NVG599 is determining the broadband network type, the following screen appears.



The Device Status page appears.

The screenshot shows the "Device Status" page. At the top, there are navigation tabs: "Device", "Broadband", "Home Network", "Voice", "Firewall", and "Diagnostics". Below these are sub-tabs: "Status", "Device List", "System Information", "Access Code", "Remote Access", "Battery", and "Restart Device". The "Status" section is active and shows several components:

- Broadband Connection:** Status is "Up". A "Restart" button is visible.
- Battery:** Status is "Normal". A "More Info" button is visible.
- 2.4 Ghz Radio Status:** Status is "On". A "Restart" button is visible.
- Wi-Fi:** Two networks are listed:
  - Network Name (SSID): NVG599-TEST, Type: User, Authentication Type: WPA, Password: 1111111111, Status: Enabled.
  - Network Name (SSID): NVG599-TEST\_Guest, Type: Guest, Authentication Type: WPA, Password: (blank), Status: Disabled.
- 5 Ghz Radio Status:** Status is "On". A "Restart" button is visible.
- Coax to STB:** Status is "On". A "Restart" button is visible.
- Voice:** Two lines are listed, both with status "Down":
  - Line 1 Not Subscribed
  - Line 2 Not Subscribed

Below the status section is the "Common Tasks" area with several links: "Go to AT&T online support for troubleshooting and repair", "Modify your Wi-Fi security or settings", "Restart your device", "Find a computer on your home network", and "Adjust firewall settings for gaming and applications".

At the bottom, there is a "Home Network Devices" section with a "More Info" button. Below this is a table:

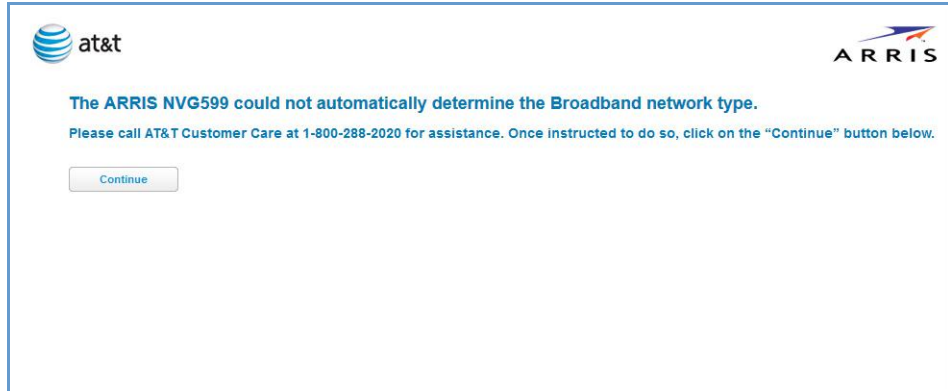
Device	IPv4 Address / Name	MAC Address	Status	Connection	Allocation
	192.168.1.145 / FTJPT4-02	70:5a:b6:b0:27:cd	on	Ethernet	dhcp

3. Check to make sure the Broadband and Service LEDs on your NVG599 device are lit **GREEN** to verify that the connection to the Internet is active.

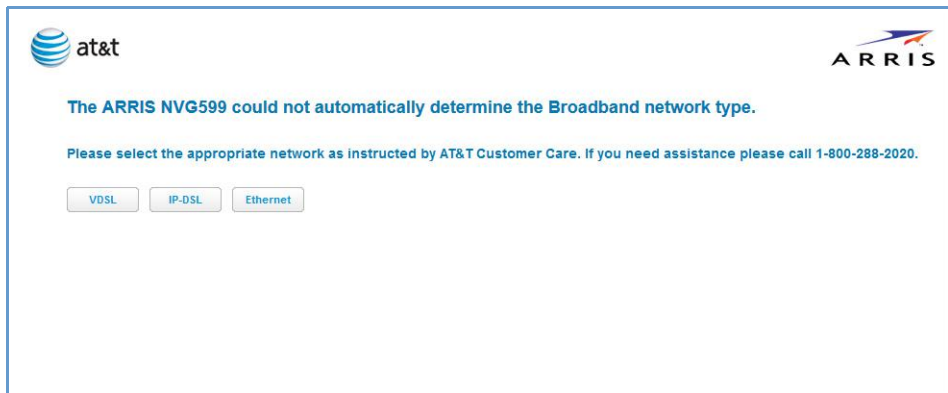
Congratulations! Your installation is complete. You can now surf to your favorite Web sites by typing a URL in your browser's location box or by selecting one of your favorite Internet bookmarks.

### **Broadband Network Redirect Pages**

After a few minutes, if the broadband network cannot be determined, the following screen appears. Contact AT&T Customer Care at the number shown on your screen for assistance.



If you click the **Continue** button, the following screen appears. Here you can manually select the broadband network type, if you know it.




---

## IP Diagnostics Page Redirect

In the event that your connection to the Internet fails, the Broadband LED on your NVG599 device flashes **RED** and you are redirected to the IP Diagnostics page.

Changes saved

### IP Diagnostics



**WARNING:** DSL Failed to Connect (Message ID: NAD-3304D)

The ARRIS NVG599 device does not currently detect a DSL signal.

To restore your broadband connection:

1. Check any recent changes to wires, splitters or faceplates as these sometimes block the DSL signal and you may need to undo these changes.
2. If your device is connected to a DSL phone filter, make sure it is connected to the filter jack labeled DSL and make sure the filter is connected using the green data cable to the device port labeled Broadband.
3. If your device is not connected to a DSL phone filter, verify that the telephone cable is still properly connected between a working wall jack and the device port labeled Broadband.
4. Make sure all phones, answering machines or other devices which connect to a phone jack have a DSL phone filter attached.
5. Check that the broadband connection setting in the device is set to Automatic.
6. If you are using another type of broadband connection, check that the broadband connection setting in the device is set to Automatic or specifically for that type of broadband connection.

After checking the above items, click on the "Check Connection" button to retry connection to your Broadband service.

If the problem persists, please contact the AT&T Help Desk at 1-800-288-2020.

[Check Connection](#)

Follow the on-screen troubleshooting suggestions.

For additional troubleshooting information, see [“Diagnostics” on page 77](#) and [“Basic Troubleshooting” on page 87](#).

When your connection is restored or the problem is resolved, the Broadband LED turns **GREEN**.



**NOTE:**

For AT&T this function is enabled by default. See the CLI command [“set management lan-redirect enable \[ off | on \]” on page 149](#).

---

## Offline Troubleshooting

If the WAN is down, the following information is displayed at the top of the page:

### Offline Troubleshooting

[Refresh](#)

If you have a problem with your device, perform the following steps, in order:

1. Click the "Restart" button next to each system below marked as "Down".
2. Restart your device using the button below.

[Restart...](#)

3. If this condition persists for more than 15 minutes, please contact the AT&T Help Desk at 1-800-288-2020.

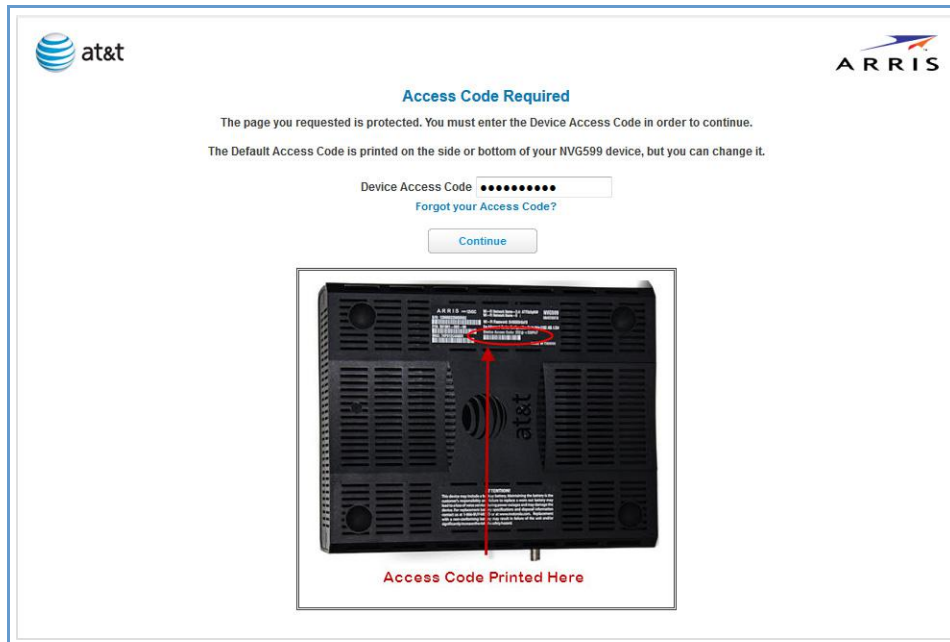
## Device Status Page

After you have performed the basic Easy Login configuration, any time you log in to your NVG599 you will access the NVG599 Home page.

To access the Home page, type `http://192.168.1.254` in your Web browser's location box.

## Device Access Code

On the Device Status page, you may be required to provide your device access code to access the Web management configuration pages. The device access code is unique to your device. It is printed on a label on the side of the NVG599.



Enter your device access code and click the [Continue](#) button.



The Device Status page appears.

The screenshot displays the AT&T Arris Device Status page. At the top, there are logos for AT&T and ARRIS. Below them is a navigation bar with tabs for Device, Broadband, Home Network, Voice, Firewall, and Diagnostics. Under the Device tab, there are sub-links for Status, Device List, System Information, Access Code, Remote Access, Battery, and Restart Device.

The main content area is divided into two columns. The left column, titled "Status", contains several status cards:

- Broadband Connection:** Status is "Up". Includes a "Restart" button.
- Battery:** Status is "Normal". Includes a "More Info" button.
- 2.4 Ghz Radio Status:** Status is "On". Includes a "Restart" button.
- Wi-Fi:** Shows two networks:
  - Network Name (SSID): NVG599-TEST, Type: User, Authentication Type: WPA, Password: 1111111111, Status: Enabled.
  - Network Name (SSID): NVG599-TEST\_Guest, Type: Guest, Authentication Type: WPA, Password: 1111111111, Status: Disabled.
- 5 Ghz Radio Status:** Status is "On". Includes a "Restart" button.
- Coax to STB:** Status is "On". Includes a "Restart" button.
- Voice:** Shows "Line 1 Not Subscribed" and "Line 2 Not Subscribed", both with a "Down" indicator and a "Restart" button.






The right column, titled "Common Tasks", contains several links for troubleshooting and support:

- [Go to AT&T online support for troubleshooting and repair »](#)
- [Modify your Wi-Fi security or settings »](#)
- [Restart your device »](#)
- [Find a computer on your home network »](#)
- [Adjust firewall settings for gaming and applications »](#)

At the bottom, there is a section for "Home Network Devices" with a "More Info" button. Below this is a table with the following data:

Device	IPv4 Address / Name	MAC Address	Status	Connection	Allocation
	192.168.1.145 / FTJP74-02	70:5a:b6:b0:27:cd	on	Ethernet	dhcp

The Device Status page displays the following information in the center section:

(icon)	Field	Description
 (Broadband)	Broadband Connection	Waiting for DSL is displayed while the NVG599 is training. This should change to Up within two minutes. Up is displayed when the ADSL line is synched and the session is established. Down indicates inability to establish a connection; possible line failure.
 (Battery)	Status	May display any of these values: Normal, Low Battery, Charging, Warning: No battery or battery has no charge or Warning: Battery backup mechanism has a fault.
 (WiFi)	Status	Your wireless signal may be On or Off.
	Network ID (SSID)	The name or ID that is displayed to a client scan. The default SSID for the NVG599 is attxxx where xxx is the last 3 digits of the serial number located on the side of the NVG599.
	Authentication Type	The type of wireless encryption security in use. May be Disabled, WPA, WEP, Default Key, or Manual.
 (Coax to STB)	Network Key	Wireless network encryption key in use.
	Status	Off or On.
 (Voice)	Line 1	Indication of VoIP or other phone connection.
	Line 2	Indication of VoIP or other phone connection.

Some fields may or may not be displayed, depending on your particular setup.

The [Diagnostics](#) button will connect you to the Troubleshoot page. See [“Diagnostics” on page 77](#).

The frame at right displays some links to commonly performed tasks for easy access.

**Common Tasks**

- [Go to AT&T online support for troubleshooting and repair »](#)
- [Modify your Wi-Fi security or settings »](#)
- [Restart your device »](#)
- [Find a computer on your home network »](#)
- [Adjust firewall settings for gaming and applications »](#)

- ◆ [Display additional troubleshooting steps »](#) - OR - [Go to AT&T online support for troubleshooting and repair](#)  
This link will connect you to the IP Diagnostics page with help for troubleshooting and the AT&T Help Desk information. See [“IP Diagnostics Page Redirect” on page 23](#).
- ◆ [Modify your WiFi security or settings »](#)  
This link will connect you to the WiFi page. See [“WiFi” on page 43](#).
- ◆ [Restart your device »](#)  
This link will connect you to the Restart Device page. See [“Restart Device” on page 33](#).
- ◆ [Find a computer on your home network »](#)  
This link will connect you to the Device List page. See [“Device List” on page 28](#).
- ◆ [Adjust firewall settings for gaming and applications »](#)  
This link will connect you to the NAT/Gaming page. See [“NAT/Gaming” on page 67](#).

---

## Tab Bar

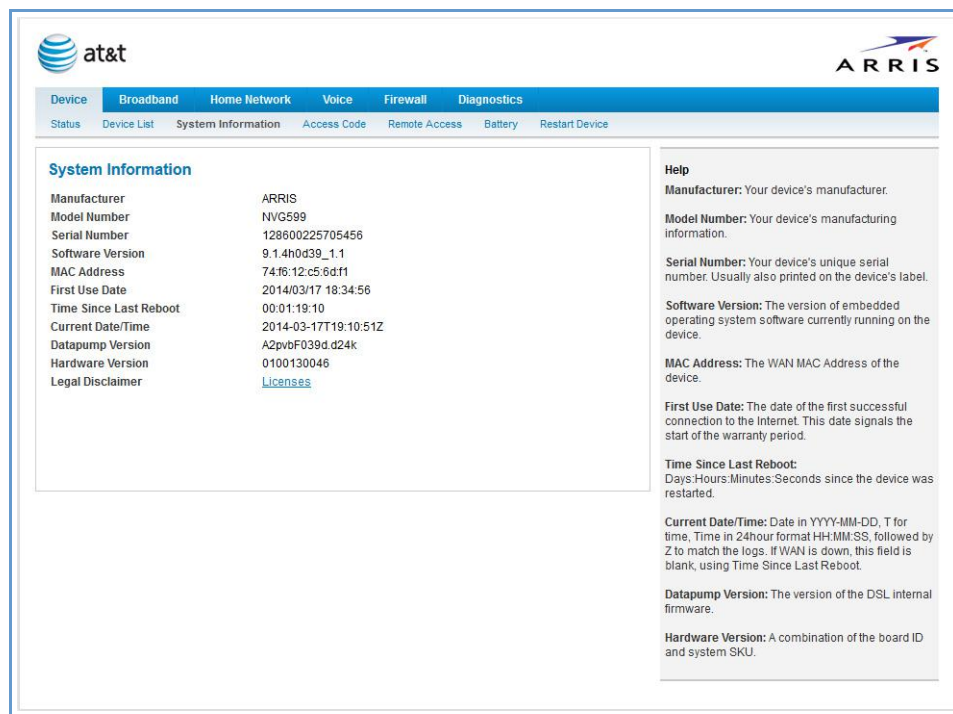
The tab bar is located at the top of every page, allowing you to move freely about the site.



The tabs reveal a succession of pages that allow you to manage or configure several features of your Gateway. Each tab is described in its own section.

## Help

Online Help for your device is available in the rightmost frame on every page in the Web interface. For example, the Help section at right is displayed on the System Information page.

A screenshot of the AT&T web interface. At the top left is the AT&T logo, and at the top right is the ARRIS logo. Below the logos is a navigation bar with tabs: "Device", "Broadband", "Home Network", "Voice", "Firewall", and "Diagnostics". Underneath this is a secondary navigation bar with links: "Status", "Device List", "System Information", "Access Code", "Remote Access", "Battery", and "Restart Device". The "System Information" link is selected. The main content area is split into two columns. The left column, titled "System Information", lists various device details: Manufacturer (ARRIS), Model Number (NVG599), Serial Number (128600225705456), Software Version (9.1.4h0d39\_1.1), MAC Address (74:f6:12:c5:6d:f1), First Use Date (2014/03/17 18:34:56), Time Since Last Reboot (00:01:19:10), Current Date/Time (2014-03-17T19:10:51Z), Datapump Version (A2pvbF039d.d24k), Hardware Version (0100130046), and Legal Disclaimer (with a link to Licenses). The right column, titled "Help", provides definitions for several of these fields: Manufacturer, Model Number, Serial Number, Software Version, MAC Address, First Use Date, Time Since Last Reboot, Current Date/Time, Datapump Version, and Hardware Version.

## Links Bar

The links bar appears at the top of each page, allowing you to configure aspects of the features displayed on the page. For example, the links bar on the Home Summary page is as shown below:



The links bar on the Device Status page includes the following links. For more information about each link, see the related section in this guide.

- ◆ **Status** (see [page 24](#))
- ◆ **Device List** (see [page 28](#))

- ◆ System Information (see [page 29](#))
- ◆ Access Code (see [page 30](#))
- ◆ Remote Access (see [page 31](#))
- ◆ Battery (see [page 32](#))
- ◆ Restart Device (see [page 33](#))

[Link: Device List](#)

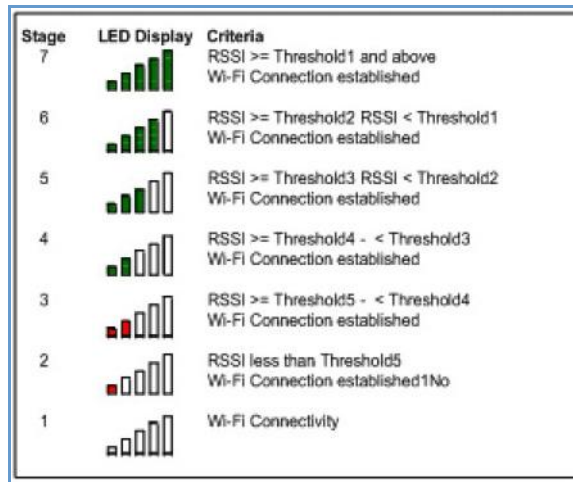
When you click the [Device List](#) link, the Device List page appears.



The page displays the following summary information for each home network device connected to the NVG599 device on your local area network: IPv4 address, network name, MAC address, and other status information.

Home Network Devices	
MAC Address	Client device's unique hardware address.
IPv4 Address / Name	Client device's IP address or device network name.
Last Activity	Date and time of last traffic for this client device.
Status	May be off or on.
Allocation	Type of IP address assignment, for example, static or DHCP.
Connection Type	Type of connection, for example, Ethernet or WiFi.

For WiFi client connections, the Device List page displays the familiar bars indicating signal strength, as follows:



- ◆ Click the [Clear Device List](#) button to update the Home Network Devices summary.
- ◆ Click the [Scan for Devices](#) button to seek out other devices that have been connected since the last Home Network Devices summary update.

### [Link: System Information](#)

When you click the [System Information](#) link, the System Information page appears.

System Information	
Manufacturer	ARRIS
Model Number	NVG599
Serial Number	128600225705456
Software Version	9.1.4h0d39_1.1
MAC Address	74:f6:12:c5:6d:f1
First Use Date	2014/03/17 18:34:56
Time Since Last Reboot	00:01:19:10
Current Date/Time	2014-03-17T19:10:51Z
Datapump Version	A2pvbF039d.d24k
Hardware Version	0100130046
Legal Disclaimer	<a href="#">Licenses</a>

The page displays the following information:

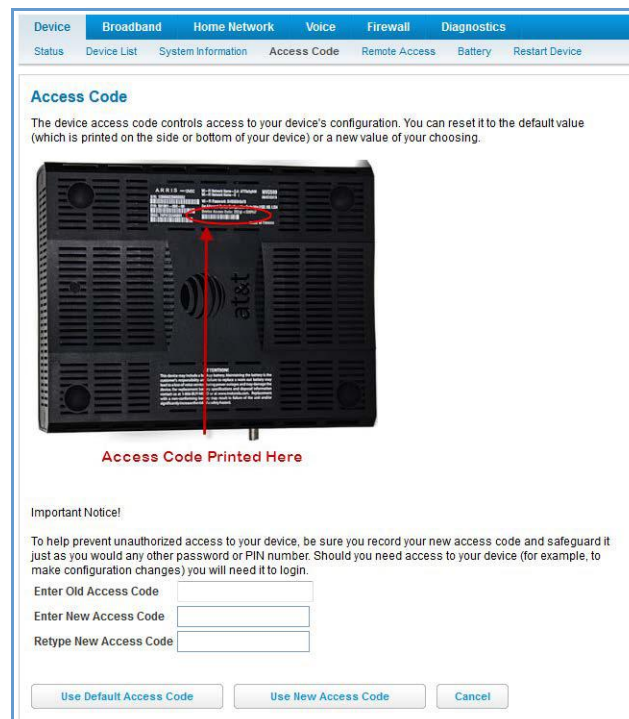
System Information	
Manufacturer	Manufacturer's identifier name.
Model Number	Manufacturer's model number.
Serial Number	Unique serial number of your device.
Software Version	Version number of the current embedded software in your device.
MAC Address	Unique hardware address of this NVG599 unit.
First Use Date	Date and time the NVG599 device is first used. This field changes to the current date and time after a reset to factory defaults.
Time Since Last Reboot	Elapsed time since last reboot of the device in days:hr:min:sec.
Current Date/Time	Current system date and time in days:hr:min:sec.
Datapump Version	Underlying operating system software datapump version.
Legal Disclaimer	Clicking the <a href="#">Licenses</a> link displays a listing of software copyright attributions, also shown in <a href="#">"Copyright Acknowledgments" on page 189</a> .

### Link: Access Code

When you click the Access Code link, the Access Code page appears and allows changes to the code that controls access to your device's configuration. Access to your NVG599 device is controlled through an account named *Admin*. The default Admin password for your device is the unique access code printed on the label on the side of your device.

As the Admin, you can change this password to one of your own choosing between 8 and 20 characters long. The new password must include two characters from any these categories: alpha, number, and special characters.

**Example:** "fru1tfl13s\_likeabanana"



---

Enter your old access code, your new access code, and click the [Use New Access Code](#) button. The new access code takes effect immediately.

You can always return to the original default password by clicking the [Use Default Access Code](#) button.

---

## Link: Remote Access

The Remote Access page lets you grant access to your NVG599 device to other users on the WAN. This function can be used for advanced troubleshooting or remote configuration.



### WARNING:

Enabling remote access allows anyone who knows or can determine the password, port ID, and URL (address) of your NVG599 device to view any configuration settings or change the operation of your gateway.

---

If remote access is not currently enabled, the Remote Access page will let you configure and enable it. If remote access has been enabled, the Remote Access page will indicate that, and provides a button to disable it.

The screenshot shows the 'Remote Access' configuration page. At the top, there are navigation tabs: Device, Broadband, Home Network, Voice, Firewall, and Diagnostics. Below these are sub-tabs: Status, Device List, System Information, Access Code, Remote Access (selected), Battery, and Restart Device. The main content area is titled 'Remote Access' and contains the following fields and options:

- User Name:** tech
- Password:** A text input field with a placeholder example: *e.g. mywanpass24#*
- Port to use:** A text input field with the value 41680 and a placeholder example: *e.g. 8080*
- Access Type:** Two radio buttons:  Read only access and  Update access
- URL:** https://10.13.211.51

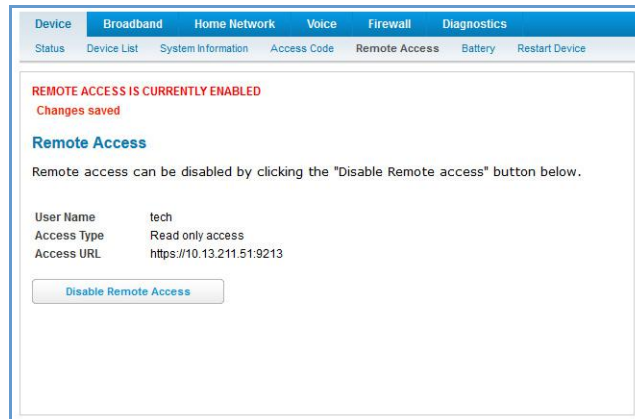
At the bottom of the form is a button labeled 'Enable Remote Access'.

To enable remote access:

1. Type a password in the **Password** field. This password must be at least 8 characters long, and must include at least two of the following types of characters:
  - ◆ Alphabetic (letter) characters
  - ◆ Numeric (number) characters
  - ◆ Special characters (! @ # \$ % ^ & \* , etc)
2. If necessary, set a custom port number for secure HTTP access to the NVG599 remote access session in the **Port Value** field.
3. Click the radio button that describes the type of remote access to allow:
  - ◆ Read only access - to allow the remote access session to view, but not change, the configuration and collected statistics of the gateway.
  - ◆ Update access - to allow the session to make changes to the gateway's configuration.
4. Click the [Enable Remote Access](#) button.

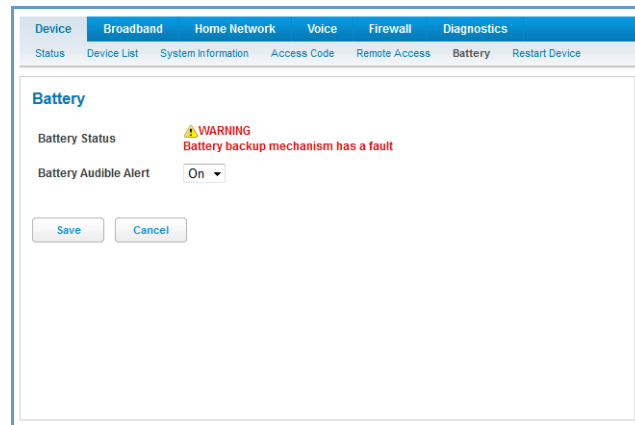
The NVG599 updates the Remote Access page and displays the current remote access settings, shows the URL that a remote access client must use to connect to the remote access session, and provides a button for ending the remote access session. The remote access client will need to connect to the URL shown on the Remote Access page, and will need to log in with the user name "tech" and with the password configured when access was enabled.

To end (disable) an existing remote access configuration, click the [Disable Remote Access](#) button, as shown below:



### [Link: Battery](#)

The Battery page shows the condition and status of the NVG599 internal battery, and provides control over the battery condition audible alarm.



The battery condition audible alarm provides an on-hook ringing signal on a connected telephone if the NVG599 battery needs recharging or replacing. This alarm uses a distinctive “splash” ring pattern and a battery notification message on phones with caller ID displays or announcers. Additionally, the NVG599 provides an off-hook voice notification to the subscriber if the NVG599 battery is low (and needs recharging) or faulty (and needs replacing). After playing the recorded voice notification, the NVG599 provides a dial tone.

The alarm is triggered when the NVG599 determines that the installed battery is:

- ◆ Below 35% charge and in need of recharging, or
- ◆ Unable to charge past 80% of capacity and in need of replacing.



#### **Note:**

A subscriber may interrupt the voice notification by dialing. The voice notification may be turned off by a subscriber phone dialing “\*#103”. This capability is included in the VOIP digit map with the parameter \*#103<:@C06>

To change the alarm setting, click the Battery Audible Alert drop-down menu, and select the setting (On or Off) for the alarm. Click the [Save](#) button to save the new settings, or [Cancel](#) to discard them.

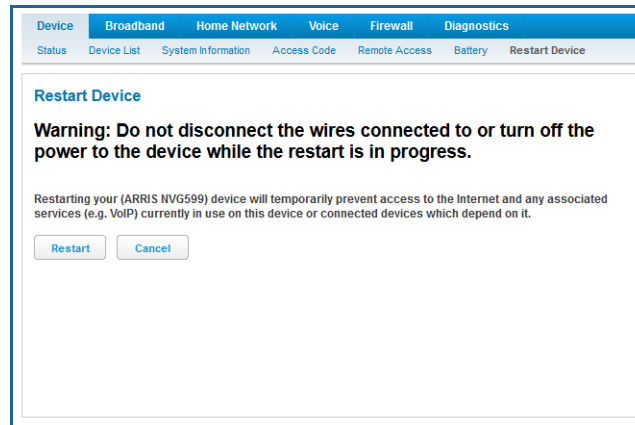


---

## [Link: Restart Device](#)

When the NVG599 is restarted, it will disconnect all users, initialize all its interfaces, and load the operating system software.

In some cases, when you make configuration changes, you may be required to restart for the changes to take effect.



## Broadband Tab

Links available on the Broadband tab provide access to pages that allow you to view information about the broadband connection and configure connection details.

### Link: Broadband Status

When you click the **Broadband** tab, the Broadband **Status** page is the first to appear.

Device
Broadband
Home Network
Voice
Firewall
Diagnostics

Status
Configure
IGMP Stats

### Broadband Status

Broadband Connection Source    DSL

Broadband Connection            Up

Broadband IPv4 Address        10.13.211.30

Gateway IPv4 Address         10.13.211.126

MAC Address                    74:16:12:c5:6d:f1

Primary DNS                    10.13.193.1

Secondary DNS                 10.14.40.1

Primary DNS Name

Secondary DNS Name

MTU                                1500

DSLAM Vendor ID                b5004244434da3db

### DSL Status

	Line 1	Line 2		
Line State	Up	Up		
Downstream Sync Rate (kbps)	51456	48982		
Upstream Sync Rate (kbps)	15955	15198		
Downstream Max Attainable Rate (kbps)	52200	50106		
Upstream Max Attainable Rate (kbps)	7292	15332		
Modulation	VDSL2	VDSL2		
Data Path	Fast	Fast		
	Downstream	Upstream	Downstream	Upstream
SN Margin (dB)	9.3	6.3	9.3	5.3
Line Attenuation (dB)	3.4	2.4	1.5	2.8
Output Power(dBm)	11.3	-25.9	11.3	-25.9
Errored Seconds	2	439	0	150
Loss of Signal	0	0	0	0
Loss of Frame	0	0	0	0
FEC Errors	34125	217473	0	1051882
CRC Errors	2	2114	0	1174

### Timed Statistics

	15 Min	Cur Day	Showtime	Last Showtime	Total
Errored Seconds (ES) Line 1	0	2	2	2	2
Errored Seconds (ES) Line 2	0	391	0	0	391
Severely Errored Seconds (SESL) Line 1	0	0	0	0	0
Severely Errored Seconds (SESL) Line 2	0	391	0	0	391
Unavailable Seconds (UASL) Line 1	0	83	0	0	83
Unavailable Seconds (UASL) Line 2	0	1774	0	0	1774
FEC Errors Line 1	0	34125	34125	34125	34125
FEC Errors Line 2	0	201	0	0	201
CRC Errors Line 1	0	2	2	2	2
CRC Errors Line 2	0	142687	0	0	142687
DSL Initialization Timeouts Line 1	0	0	0	0	0
DSL Initialization Timeouts Line 2	0	0	0	0	0

Aggregated Information	
Bonded Downstream Rate	100438
Bonded Upstream Rate	31153
IPv6	
Status	Unavailable
Global Unicast IPv6 Address	
Border Relay IPv4 Address	
IPv4 Statistics	
Transmit Packets	5701
Transmit Errors	0
Transmit Discards	0
Transmit Bytes	0
Receive Packets	6060
Receive Errors	0
Receive Discards	0
Receive Bytes	2661733
PTM Receive PDUs	6060
IPv6 Statistics	
Transmit Packets	0
Transmit Errors	0
Transmit Discards	0
<a href="#">Clear Statistics</a>	

The **Status** page displays information about the NVG599 device’s WAN connection(s) to the Internet.

### Broadband Status

Broadband Connection Source	The communications technology providing the NVG599 broadband uplink.
Broadband Connection	May be <b>Up</b> (connected) or <b>Down</b> (disconnected).
Broadband IPv4 Address	The public IP address of your device, whether dynamically or statically assigned.
Gateway IPv4 Address	Your ISP's gateway router IP address.
MAC Address	Your device’s unique hardware address identifier.
Primary DNS	The IP address of the primary Domain Name System (DNS) server.
Secondary DNS	The IP address of the backup DNS server, if available.
Primary DNS Name	The name of the primary DNS server.
Secondary DNS Name	The name of the backup DNS server, if available.
MTU	Maximum transmittable unit before packets are broken into multiple packets.

### DSL Status (for each line)

Line State	May be <b>Up</b> (connected) or <b>Down</b> (disconnected).
Downstream Sync Rate	The rate at which your connection can download (receive) data on your DSL line, in kilobits per second.
Upstream Sync Rate	The rate at which your connection can upload (send) data on your DSL line, in kilobits per second.
Modulation	Method of regulating the DSL signal. DMT (discrete multi-tone) allows connections to work better when certain radio transmitters are present.
Data Path	Type of path used by the device's processor.

### Downstream and Upstream Statistics (DSL WAN)

SN Margin (db)	Signal-to-noise margin, in decibels. Reflects the amount of unwanted noise on the DSL line.
Line Attenuation	Amount of reduction in signal strength on the DSL line, in decibels.
Output Power (dBm)	Measure of power output in decibels (dB) referenced to one milliwatt (mW).
Errored Seconds	The number of uncorrected seconds after being down for seven consecutive seconds.

Loss of Signal	The absence of any signal for any reason, such as a disconnected cable or loss of power.
Loss of Frame	A signal is detected but the device cannot sync with signal because of mismatched protocols, wrong ISP connection configuration, or faulty cable.
FEC Errors	Forwarded Error Correction errors. Count of received errored packets that were fixed successfully without a retry.
CRC Errors	Number of times data packets have had to be resent because of errors in transmission or reception.

**Ethernet Statistics (Ethernet WAN)**

Line State	Up or Down
Current Speed	Line speed
Current Duplex	Full- or half-duplex
Receive Packets	Number of packets received
Transmit Packets	Number of packets sent
Receive Bytes	Number of bytes received
Transmit Bytes	Number of bytes sent
Receive Unicast	Receive Unicast statistics
Transmit Unicast	Transmit Unicast statistics
Receive Multicast	Receive Multicast statistics
Transmit Multicast	Transmit Multicast statistics
Receive Drops	Received packets dropped
Transmit Drops	Sent packets dropped
Receive Errors	Count of received errored packets that were fixed successfully without a retry.
Transmit Errors	Number of times data packets have had to be resent due to errors in transmission.
Collisions	Count of packet collisions.

**Aggregated Information**

Bonded Downstream Rate	The bonded channel receive rate.
Bonded Upstream Rate	The bonded channel transmit rate.

**IPv6**

Status	May be Enabled or Unavailable.
Global Unicast IPv6 Address	The public IPv6 address of your device, whether dynamically or statically assigned.
Border Relay IPv4 Address	The public IPv4 address of your device.

**IPv4 Statistics**

Transmit Packets	IPv4 packets transmitted.
Transmit Errors	Errors on IPv4 packets transmitted.
Transmit Discards	IPv4 packets dropped.

**IPv6 Statistics**

Transmit Packets	IPv6 packets transmitted.
Transmit Errors	Errors on IPv6 packets transmitted.
Transmit Discards	IPv6 packets dropped.

---

## Link: Configure

When you click the [Configure](#) link, the Broadband **Configure** screen appears. Here you can reconfigure your type of broadband connection should it change in the future.

- ◆ **Broadband Source Override** - Auto (automatically detected), DSL - Line 1, DSL - Line 2, DSL - Line 1 / Line -2 (Bonded), or Ethernet WAN.  
If you switch from DSL to Ethernet or from Ethernet to DSL, the device will proceed to reconnect as in its initial connection to the Internet, as described earlier. See [“Accessing the Web Management Interface” on page 21.](#)
- ◆ The WAN connection is automatically configured. However, you can adjust the **Maximum allowable MTU** (maximum transmittable unit) value, if your service provider suggests it. The default 1500 is the maximum value, but some services require other values (1492 is common).

If you make any change here, click the [Save](#) button.

Link: IGMP Stats

When you click the [IGMP Stats](#) link, the **IGMP Stats** screen appears. The IGMP statistics screen reports IGMP proxy groups and multicast forwarding information. It also displays a packet counter.

The screenshot displays the IGMP Stats page with the following sections:

- IGMP Stats Multicast Configuration:**
  - IGMP Querier Version: 3
  - IGMP Robustness: 2
  - IGMP Query Interval: 125
  - IGMP Query Response Interval: 100
  - IGMP Unsolicited Report Interval: 10
  - IGMP Fast Leave Enable: on
  - IGMP Last Member Interval: 10
  - IGMP Last Member Count: 2
  - IGMP Maximum Group Memberships: 64
  - IGMP Default Forward Allow: on
  - IGMP Snooping Entry Time: 150
  - IGMP Snooping Unreg Mode: block
  - IGMP QoS To S: 0xc0
  - IGMP QoS P Bit: 6
  - IGMP QoS Marker: snoop|fwd
  - IGMP Proxy State: snoop|fwd
- IGMP Snooping Statistics:**

Port	Group	Source	Timeout
- Summary:**

	Fwd Grp Num	Grp Num	Query	V1 Responses	V2 Responses	V2 Leaves	V3 Responses	Other
Received	1	4	0	0	9	5	102	0
Transmitted	1	4	672	0	0	0	0	0
- Group Details Table:**

Group	Interface	Group Address	Uptime	Last Reporter Address	Last Reporter Time
Group	br2	224.0.0.2	00:23:15:13	0.0.0.0	
Group	br2	224.0.0.252	00:00:15:43	192.168.1.145	2014-03-18 17:34:20
Group	br2	239.255.255.250	00:23:15:07	192.168.1.145	2014-03-17 18:34:56
Group	br2	224.0.0.22	00:23:15:13	192.168.1.145	2014-03-17 18:34:50
- Multicast Group Hosts:**
  - Host IP Address: 192.168.1.145, Uptime: 00:00:15:38, Multicast Address: 224.0.0.252
 

	Query	V1 Responses	V2 Responses	V2 Leaves	V3 Responses	Other
Received	0	0	0	0	18	0
Transmitted	0	0	0	0	0	0
  - Host IP Address: 10.13.195.68, Uptime: 00:00:15:43, Multicast Address: 224.0.0.252
 

	Query	V1 Responses	V2 Responses	V2 Leaves	V3 Responses	Other
Received	0	0	0	0	4	0
Transmitted	0	0	0	0	0	0

## Home Network Tab

When you click the [Home Network](#) tab, the Home Network Status page appears.

### Home Network Status

Device IPv4 Address	192.168.1.254
DHCPv4 Netmask	255.255.255.0
DHCPv4 Start Address	192.168.1.64
DHCPv4 End Address	192.168.1.253
DHCP Leases Available	188
DHCP Leases Allocated	2
DHCP Primary Pool	Private
Secondary Subnet	Disabled
Public Subnet	
Cascaded Router Status	Disabled
IP Passthrough Status	Off (private IP address)

### Interfaces

Interface	Status	Active Devices	Inactive Devices
Ethernet	Enabled	1	0
Wi-Fi 2.4GHz	Enabled	0	1
Wi-Fi 5.0GHz	Disabled	0	0
HPNA	Enabled	0	0

### IPv6

Status	Unavailable
Global IPv6 Address	/
Unique Local IPv6 Address	
Link-Local IPv6 Address	
Router Advertisement Prefix	
IPv6 Delegated LAN Prefix	/64

### IPv4 Statistics

Transmit Packets	113474
Transmit Errors	0
Transmit Discards	0
Receive Packets	121910
Receive Errors	0
Receive Discards	0

### IPv6 Statistics

Transmit Packets	0
Transmit Errors	0
Transmit Discards	0

### Wi-Fi Status

	2.4 GHz Radio	5.0 GHz Radio
Wi-Fi Radio Status	Enabled	Disabled
Mode	B/G/N	AC
Bandwidth	20MHz	80MHz
Current Radio Channel	1	
Radio Channel Selection	automatic	automatic
MAC Address Filtering	Off	Off
Power Level	100%	100%
Home SSID	On	On
Network Name (SSID)	NVG599-TEST	NVG599-TEST
Hide Network Name	Off	Off
Security	WPA	WPA
Password	1111111111	1111111111
MAC Address	74:f6:12:c5:6d:f0	
Guest SSID	Off	
SSID Subnet		
Network Name (SSID)	NVG599-TEST_Guest	
Hide Network Name	Off	
Security	WPA	
Password		
MAC Address	76:f6:12:c5:6d:f1	

### Wi-Fi Network Statistics

	2.4 GHz Radio	5.0 GHz Radio
Transmit Bytes	4436083	0
Receive Bytes	47936	0
Transmit Packets	70838	0
Receive Packets	587	0
Transmit Error Packets	0	0
Receive Error Packets	0	0
Transmit Discard Packets	6067	0
Receive Discard Packets	15932832	0

### Wi-Fi Congestion

WARNING: Running the Congestion test will temporarily disconnect Wi-Fi users.

[Run Congestion Detection](#)

The Home Network Status page displays information about the NVG599 device's local area network.

If you click the [Run Congestion Detection](#) button, the device will generate statistics for each of the 11 channels available, displaying:

- ◆ Channel number
- ◆ AP (access point) count
- ◆ Congestion score (1 - 10) - Note that higher values mean lower congestion.

The wireless congestion feature provides simple data to the user to show the level of network congestion in each wireless channel. This data can be used to determine router placement or to determine which channels to avoid.

The display tells the user how many access points (APs) are active within each channel, and provides a score of 1 - 10 to indicate how clear the channel is. A higher score indicates less congestion in a channel; thus, a 10 indicates a channel extremely clear of wireless traffic and noise. Alternatively, a score of 1 indicates more severe congestion in a channel.

You can clear the current statistics information by clicking the [Clear Statistics](#) button.

### Wi-Fi Client Connection Statistics

[Clear Connection Statistics](#)

MAC Address	Authentication State	IP Address	Radio Channel	Access Point	Transmit Packets	Receive Packets	Transmit Bytes
dc:86:d8:e1:67:83	Disconnected	192.168.1.147	N/A	2.4 Radio: NVG599-TEST	0	0	0

### LAN Ethernet Statistics

	Port 1	Port 2	Port 3	Port 4
State	up	down	down	down
Transmit Speed	1000000000	0	0	0
Transmit Packets	23773	0	0	0
Transmit Bytes	8351951	0	0	0
Transmit Dropped	0	0	0	0
Transmit Errors	0	0	0	0
Receive Packets	19059	0	0	0
Receive Bytes	5640200	0	0	0
Receive Unicast	17786	0	0	0
Receive Multicast	913	0	0	0
Receive Dropped	0	0	0	0
Receive Errors	0	0	0	0

[Clear Statistics](#)

### Home Network Status

Device IPv4 Address	The NVG599 device's own IP address on the network.
DHCP Netmask	The device's own netmask on the network.
DHCPv4 Start Address	The starting IP address of the DHCP range served by the device.
DHCPv4 End Address	The ending IP address of the DHCP range served by the device.
DHCP Leases Available	The number of IP addresses of the DHCP range available to be served by the device.
DHCP Leases Allocated	The number of IP addresses of the DHCP range currently being served by the device.
DHCP Primary Pool	Source pool of the IP addresses served by the NVG599 device, Public or Private.

### IPv6

Status	May be <b>Enabled</b> or <b>Unavailable</b> .
Global IPv6 Address	The public IPv6 address of your device, whether dynamically or statically assigned.
Link-local IPv6 Address	The private IPv6 address of your device, whether dynamically or statically assigned.
Router Advertisement Prefix	The IPv6 prefix to include in router advertisements.
IPv6 Delegated LAN Prefix	The IPv6 network address prefix that identifies the NVG599 network.

### IPv4 Statistics

Transmit Packets	IPv4 packets transmitted.
Transmit Errors	Errors on IPv4 packets transmitted.
Transmit Discards	IPv4 packets dropped.

### IPv6 Statistics

Transmit Packets	IPv6 packets transmitted.
Transmit Errors	Errors on IPv6 packets transmitted.
Transmit Discards	IPv6 packets dropped.

### WiFi Status

WiFi Radio Status	Status of the Wi-Fi radio: <b>Enabled</b> or <b>Disabled</b> .
Mode	2.4 Ghz radio may be <b>802.11B</b> only, <b>802.11G</b> only, <b>802.11N</b> only, <b>802.11 B/G</b> or <b>802.11 B/G/N</b> . 5.0 Ghz radio may be <b>802.11A</b> , <b>802.11AC</b> only, <b>802.11N</b> only or <b>802.11AC</b> (i.e. <b>802.11N/AC</b> ) as well.
Bandwidth	The capacity of the wireless LAN to carry traffic in megahertz.
Current Radio Channel	The radio channel that your Wi-Fi network is broadcasting on.
Radio Channel Selection	May be set to <b>automatic</b> or manually selected.
MAC Address Filtering	May be either <b>On</b> or <b>Off</b> . If <b>On</b> , you can accept or block client devices from your WLAN based on their MAC address.
Power Level	May be adjusted up to 100%, lower if multiple wireless access points are in use, and might interfere with each other.
WiFi MAC Address	Shows the information of the MAC address of the wireless subsystem.
User SSID	May be either <b>On</b> or <b>Off</b> for either frequency.
Guest SSID	May be either <b>On</b> or <b>Off</b> for the 2.4 Ghz radio only.
Network Name (SSID)	The name or ID that is displayed to a client scan. The default SSID for the NVG599 is <b>attxxx</b> where <b>xxx</b> is the last 3 digits of the serial number located on the side of the NVG599 device.
Hide SSID	May be either <b>On</b> or <b>Off</b> . If <b>On</b> , your SSID will not appear in a client scan.



Wireless Security	The type of wireless encryption security in use. May be Disabled, WPA, WEP, Default Key, or Manual.
Password	Shows the information of the security encryption key in use.

#### WiFi Network Statistics

Transmit Bytes	Number of bytes transmitted on the Wi-Fi network.
Receive Bytes	Number of bytes received on the Wi-Fi network.
Transmit Packets	Number of packets transmitted on the Wi-Fi network.
Receive Packets	Number of packets received on the Wi-Fi network.
Transmit Error Packets	The number of errors on packets transmitted on the Wi-Fi network.
Receive Error Packets	The number of errors on packets received on the Wi-Fi network.
Transmit Discard Packets	The number of packets transmitted on the Wi-Fi network that were dropped.
Receive Discard Packets	The number of packets received on the Wi-Fi network that were dropped.

#### LAN Ethernet Statistics

State	May be Up or Down.
Transmit Speed	The maximum speed of which the port is capable.
Transmit Packets	The number of packets sent out from the port.
Transmit Bytes	The number of bytes sent out from the port.
Transmit Dropped	The number of packets sent out from the port that were dropped.
Transmit Errors	The number of errors on packets sent out from the port.
Receive Packets	The number of packets received on the port.
Receive Bytes	The number of bytes received on the port.
Receive Unicast	The number of unicast packets received on the port.
Receive Multicast	The number of multicast packets received on the port.
Receive Dropped	The number of packets received on the port that were dropped.
Receive Errors	The number of errors on packets received on the port.

The links at the top of the Home Network page provide access to a series of pages that allow you to configure and monitor features of your device.

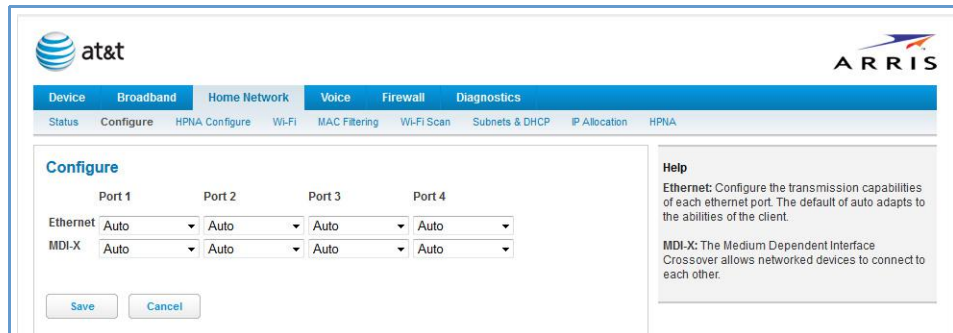


The links bar on the Home Network page includes the following links. For more information about each link, see the related section in this guide.

- ◆ **Configure** (see [page 42](#))
- ◆ **HPNA Configure** (see [page 42](#))
- ◆ **Wifi** (see [page 43](#))
- ◆ **MAC Filtering** (see [page 47](#))
- ◆ **Wireless Scan** (see [page 48](#))
- ◆ **Subnets & DHCP** (see [page 49](#))
- ◆ **IP Allocation** (see [page 50](#))
- ◆ **HPNA** (see [page 52](#))

[Link: Configure](#)

When you click the [Configure](#) link, the **Configure** page for the Ethernet LAN appears.



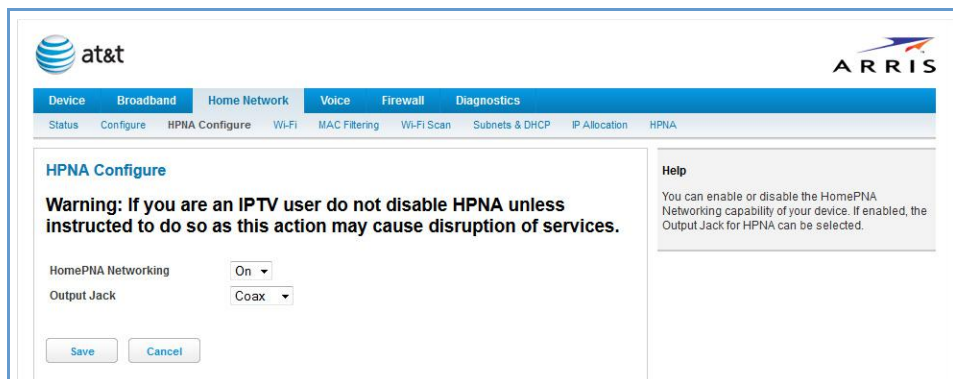
For each Ethernet Port, 1 through 4, you can select:

- ◆ **Ethernet – Auto** (the default self-sensing rate), **10M full- or half-duplex**, **100M full- or half-duplex**, or **1G full- or half-duplex**.
- ◆ **MDI-X – Auto** (the default self-sensing crossover setting), **Off**, or **On**.

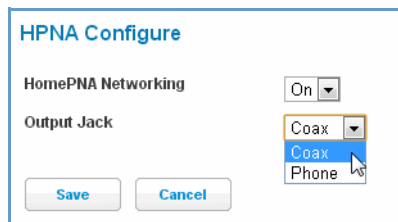
Click the [Save](#) button.

[Link: HPNA Configure](#)

When you click the [HPNA Configure](#) link, the **HPNA Configure** page for the HomePNA network appears.



Here you can set HomePNA Networking **On** or **Off**.



If desired, you can also set the Output Jack, as either the **Coax** jack or the **Phone** jack.

Click the [Save](#) button.

## Link: WiFi

When you click the [WiFi](#) link, the WiFi page appears. The WiFi page displays the status of your wireless LAN elements.

The screenshot shows the AT&T WiFi configuration page. The page is titled "at&t" and "ARRIS". It has a navigation bar with "Device", "Broadband", "Home Network", "Voice", "Firewall", and "Diagnostics". Under "Home Network", there are links for "Status", "Configure", "HPNA Configure", "Wi-Fi", "MAC Filtering", "Wi-Fi Scan", "Subnets & DHCP", "IP Allocation", and "HPNA". The main content area is divided into sections: "Wi-Fi", "Home SSID", "Guest SSID", "WPS PIN", and "WPS Virtual Pushbutton". The "Wi-Fi" section includes settings for Radio Selection (2.4 GHz Radio), Wi-Fi Operation (On), Mode (B/G/N), Bandwidth (20MHz), Channel (Automatic), and Power Level (100%). The "Home SSID" section includes Home SSID Enable (On), Network Name (SSID) (ATTXXX), Hide Network Name (Off), Security (WPA - Default Password), WPA Version (Both), WEP Password Length (10 characters), Password (1111111111), and Wi-Fi Protected Setup (WPS) (Off). The "Guest SSID" section includes Guest SSID Enable (Off), Guest SSID Subnet (192.168.2.0/24), Guest Network Name (ATTXXX\_Guest), Hide Network Name (Off), Security (WPA - PSK), WPA Version (Both), WEP Password Length (10 characters), and Password (1111111111). The "WPS PIN" section includes a text input for the PIN and a "Submit to Home SSID" button. The "WPS Virtual Pushbutton" section includes a "WPS Pushbutton to Home SSID" button. A "Help" section on the right provides detailed information about each setting.

The WiFi page center section contains a summary of the configuration settings and operational status for the wireless access point.

### Summary Information

Field	Status and/or Description
Radio Selection	Display the settings for either the 2.4 Ghz or the 5.0 Ghz frequency radio.
WiFi Operation	May be either On or Off.
Mode	Wireless transmission mode. For the 2.4 Ghz radio, may be 802.11B only, 802.11G only, 802.11N only, 802.11 B/G or 802.11 B/G/N. For the 5.0 Ghz radio, may be 802.11AC as well.
Bandwidth	The capacity of the wireless LAN to carry traffic in megahertz, <b>20</b> or <b>40</b> .
Channel	The radio channel on which your Wi-Fi network is broadcasting.
Power Level	May be adjusted up to 100%, lower if multiple wireless access points are in use, and might interfere with each other.

User SSID Enable	May be either <i>On</i> or <i>Off</i> for either frequency.
Guest SSID Enable	May be either <i>On</i> or <i>Off</i> for the 2.4 Ghz radio only.
Network Name (SSID)	The name or ID that is displayed to a client scan. The default SSID for the NVG599 is <b>attxxx</b> where xxx is the last 3 digits of the serial number located on the side of the device.
Hide SSID	May be either <i>Off</i> or <i>On</i> . If <i>On</i> , your SSID will not appear in a client scan.
Security	The type of wireless encryption security in use. May be <i>OFF-No Privacy</i> , <i>WPA-PSK</i> , <i>WEP</i> , <i>Default Key</i> or <i>Manual</i> .
WPA Version	If WPA is selected, may be <i>Both</i> , <i>WPA-1</i> , or <i>WPA-2</i> .
WEP Key Length	May be 10 characters for 40/64-bit, or 26 characters for 128-bit WP encryption.
Key	Here you can enter a manual encryption key.
WiFi Protected Setup (WPS)	May be either <i>On</i> or <i>Off</i> .

### General Information

- ◆ **WiFi Operation** – Automatically enabled by default. If you deselect the checkbox, the WiFi options are disabled, and the wireless access point will not provide or broadcast its wireless LAN services.
- ◆ **Mode** – The drop-down menu allows you to select and lock the NVG599 into the wireless transmission mode you want: **A/C**, **B/G/N**, **B-only**, **B/G**, **G-only**, or **N-only**.  
For compatibility with clients using 802.11b (up to 11 Mbps transmission), 802.11g (up to 20+ Mbps), 802.11a (up to 54 Mbit/s using the 5 GHz band), or 802.11n (from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz), select **B/G/N**. To limit your wireless LAN to one mode or the other, select the option that applies to your setup.



**NOTE:**

If you choose to limit the operating mode to 802.11b or 802.11g only, clients using the mode you excluded will not be able to connect.

- ◆ **Bandwidth** – Use a single 20-MHz channel (**20MHz** setting), or combine two 20-MHz channels (**40MHz** setting) to increase data speeds. The 40-MHz mode may only be selected if the **Mode** setting is 801.11 **B/G/N** or 802.11 **N-Only**. To prevent interference with lower bandwidth clients, the wireless network will revert to 20MHz operation if non-compatible (802.11**B**, 802.11**G**, or 20-MHz 802.11**N**) clients are detected.
- ◆ **Channel** – Channel (1 through 11, for North America) on which the network will broadcast. This is a frequency range within the 2.4-Ghz or 5.0-Ghz band. The **Automatic** setting allows the wireless access point to automatically determine the best channel for broadcast.
- ◆ **Power Level** – Sets the wireless transmit power, scaling down the wireless access point's wireless transmit coverage by lowering its radio power output. Default is **100%** power. Transmit power settings are useful in large venues with multiple wireless routers where you want to reuse channels. Since there are only three non-overlapping channels in the 802.11 spectrum, it helps to size the wireless access point cell to match the location. This allows you to install a router to cover a small "hole" without conflicting with other routers nearby.
- ◆ **Network Name (SSID)** – Preset to a number unique to your unit. You can either leave it as is, or change it by entering a freeform name of up to 32 characters, for example "Brian's Wireless LAN." In client PC software, this might also be called the wireless ID. The Network Name is used to identify this particular wireless LAN. Depending on their operating system or client wireless card, users must either:
  - Select from a list of available wireless LANs that appear in a scanned list on their client.
  - Enter this name on their clients in order to join this wireless LAN.
- ◆ **Hide SSID** – If enabled, this mode hides the wireless network from the scanning features of wireless client computers. Hiding the SSID prevents casual detection of your wireless network by unwanted neighbors and passers-by. The gateway WLAN will not appear when clients scan for access points. If Hide SSID is enabled, you must remember to enter your SSID when adding clients to the wireless LAN.



**NOTE:**

While hiding the SSID may prevent casual discovery of your wireless network, enabling security is the only true method of securing your network.

- ◆ **Security, WPA Version, WEP Key Length, Key** – See "[Wireless Security](#)" on page 45.

- ◆ **WiFi Protected Setup (WPS)** – Not a security protocol. WPS is an easier way to add and securely configure new clients to your WLAN. By default, Privacy is set to WiFi Protected Access (WPA-PSK) with a 12-character security key. WPS allows you to securely share your exact security configuration with a new client that you are adding to the WLAN, without needing to look up and type this security key. Clients can be added using the WPS button on the router, or by entering the client WPS PIN on this page. Not all client wireless devices support WPS. Refer to their documentation.

To add a client: Enter your **WPS PIN** and click the **Submit** button. Follow the instructions that came with your wireless client.

## Wireless Security

By default, wireless security is set to **WPA-PSK** with a pre-defined **WPA-Default Key**.

**Home SSID**

Home SSID Enable: On

Network Name (SSID): NVG599-TEST  
e.g. NVG599-TEST

Hide Network Name: Off

Security: WPA-PSK

WPA Version: WPA2

WEP Password Length: 10 characters (40/64 bits)

Password: 1111111111  
e.g. 1111111111

Wi-Fi Protected Setup (WPS): Off

**Save** **Cancel**

**WPS PIN**

Enter the Wi-Fi Client's all digit PIN, click the Submit button associated with the SSID you want to use, then follow the Wi-Fi client instructions.

WPS PIN:  **Submit to Home SSID**

**WPS Virtual Pushbutton**

Click the pushbutton associated with the SSID you want to use, then follow the Wi-Fi client instructions.

**WPS Pushbutton to Home SSID**

**Mode:** This option allows you to restrict the device to respond only to the LAN devices using the specified protocols. Do not change this setting unless you fully understand the implications of having your device ignore a given class of clients.

**Bandwidth:** Do not change this setting unless your Wi-Fi client requires it.

**Channel:** The device can transfer data on various channels. If a nearby Wi-Fi network is transmitting on the same channel, this interferes with data transfer. If you experience speed problems on your Wi-Fi network, test whether a particular choice of channel improves the data transfer. Choosing automatic causes the device to select the best operating channel for its environment.

**Power Level:** The device can operate at a reduced power level to cover a smaller area. For instance, in a densely populated setting, you might reduce the transmit power to reduce interference with other Wi-Fi transmitters.

**Home/Guest SSID:** A Wi-Fi client connected to a Home SSID may be able to communicate with other devices on that SSID and elsewhere on the LAN, as well as connect to the Internet. A Wi-Fi client connected to a Guest SSID can connect to the Internet, but cannot communicate with any other wireless devices or with the LAN.

**SSID Enable:** Each SSID, but especially the secondary SSIDs, may be enabled or disabled.

Other options are available from the **Security** drop-down menu:

- ◆ **WEP - Manual:** WEP security is a privacy option that is based on encryption between the router and any PCs (clients) you have with wireless cards. For WEP-Manual encryption to work, both your wireless access point and each client must share the same wireless ID (SSID), and both must be using the same encryption keys. See [“WEP-Manual” on page 46](#).

### NOTE:



WEP is a less current and less secure authentication method than WPA-PSK. It may be required if your wireless clients do not support WPA.

- ◆ **WPA-PSK:** Allows you to enter your own key, the most secure option for your wireless network. The key can be between 8 and 63 characters, but for best security it should be at least 20 characters. If you select **WPA-PSK** as your privacy setting, the **WPA Version** drop-down menu allows you to select the WPA version(s) that will be required for client connections. Choices are:

- **Both**, for maximum interoperability
- **WPA-1**, for backward compatibility
- **WPA-2**, for maximum security

All clients must support the version(s) selected in order to successfully connect. *Be sure that your Wi-Fi client adapter supports this option. Not all Wi-Fi clients support WPA-PSK.*

- ◆ **OFF - No Privacy:** Disables privacy on your network, allowing any wireless users to connect to your wireless LAN. Select this option if you are using alternative security measures such as VPN tunnels, or if your network is for public use.

Click the **Save** button.

## WEP-Manual

You can provide a level of data security by enabling WEP (Wired Equivalent Privacy) for encryption of network data. You can enable 40- or 128-bit WEP Encryption (depending on the capability of your client wireless card) for IP traffic on your LAN.



---

**NOTE:**

WEP is a less current and less secure authentication method than WPA-PSK. It may be required if your wireless clients do not support WPA.

---

**WEP - Manual** allows you to enter your own encryption keys manually. This is a difficult process, but only needs to be done once. Avoid the temptation to enter all the same characters.

**Key Length:** The drop-down menu selects the length of each encryption key. The longer the key, the stronger the encryption and the more difficult it is to break the encryption.

**Key:** You must enter a key using hexadecimal digits. For 40/64-bit encryption, you need ten digits; 26 digits for 128-bit WEP. Hexadecimal characters are 0 – 9, and a – f.

**Examples:**

- ◆ 40 bits: 02468ACE02
- ◆ 128 bits: 0123456789ABCDEF0123456789

Any WEP-enabled client must have an identical key of the same length as the router, in order to successfully receive and decrypt the traffic. Similarly, the client also has a default key that it uses to encrypt its transmissions. In order for the router to receive the client's data, it must likewise have the identical key of the same length.

Click the [Save](#) button.

---

## Link: MAC Filtering

When you click the [MAC Filtering](#) link the MAC Filtering page appears.

---



### NOTE:

5.0 Ghz Radio selection is reserved for future use.

---

**MAC Filtering**

2.4 GHz Radio  
Home SSID Filtering: Disabled  
Guest SSID Filtering: Disabled

5.0 GHz Radio  
Home SSID Filtering: Disabled

Save Cancel

**MAC Filter List**

MAC	IP Address/Name	2.4 GHz Home	2.4 GHz Guest	5.0 GHz Home	Delete MAC from All SSID Lists
00:08:24:23:44:21		allowed*	allowed*	allowed*	Delete
00:08:01:15:01:02		allowed	allowed*	allowed	Delete
00:08:06:16:65:48		allowed	allowed	allowed*	Delete

**MAC Filter Entry**

Please choose from the Device List or enter a MAC Address manually and click "Add"

MAC Address: Manual Entry  
Select from this list: e.g. 00:01:02:03:04:05

2.4 GHz Home:  2.4 GHz Guest:  5.0 GHz Home:

Add

**Help**

By enabling this feature you can limit Wi-Fi access to your device to a select group of Wi-Fi clients based on their unique Ethernet (MAC) addresses. This feature does not affect wired clients. You can create Filter Lists and enable Filtering on one or more SSIDs even if they are not currently enabled.

**MAC Filtering Type:** Selecting whitelist allows access to all clients in the MAC Filter List. Selecting blacklist denies access to all clients in the MAC Filter List.

**MAC Filter List:** The MACs in this list are the filtered MACs. The status of blocked or allowed makes the assumption that the SSID is enabled.

**MAC Filter Entry:** Choose from the list of MAC Addresses or enter the hardware MAC address directly in the Manual Entry field. The Manual Entry must be in xxxxxx (hexadecimal) format. Select one or more SSIDs on which to add this MAC filter entry.

MAC filtering allows you to specify which client PCs are allowed to join the wireless LAN by unique hardware (MAC) address.

- ◆ To enable this feature, select **Blacklist** or **Whitelist** from the **MAC Filtering Type** menu. **Blacklist** means that only MAC addresses you specify will be denied access; **Whitelist** means that only MAC addresses you specify will be allowed access.
- ◆ You add wireless clients that you want to whitelist or blacklist for your wireless LAN by selecting them from the **MAC Address** drop-down list or by entering the MAC addresses in the **Manual Entry** field provided.
- ◆ Click the **Add** button.

Your entries will be added to a list of clients that will be either authorized (whitelisted) or disallowed (blacklisted) depending on your selection.

**MAC Filter List**

MAC	IP Address/Name	2.4 GHz Home	2.4 GHz Guest	5.0 GHz Home	Delete MAC from All SSID Lists
00:08:24:23:44:21		allowed*	allowed*	allowed*	Delete
dc:86:d8:e1:67:83	192.168.1.147/Brians- iPhone	allowed*	allowed*	allowed*	Delete
00:08:01:15:01:02		allowed	allowed*	allowed	Delete
00:08:06:16:65:48		allowed	allowed	allowed*	Delete

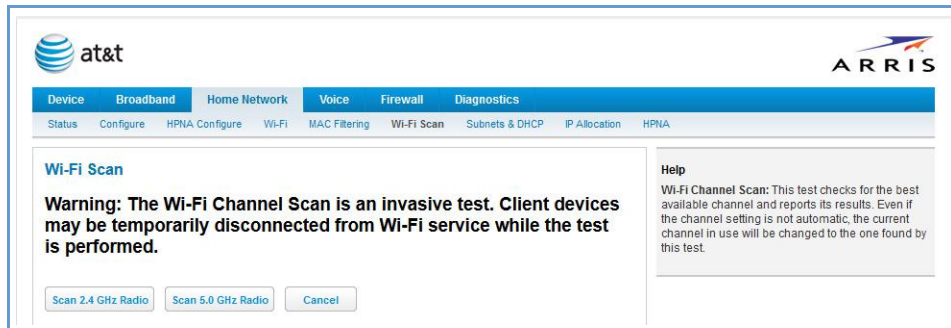
- ◆ Click the **Save** button.

You can add or delete any of your entries later by returning to this page.

---

[Link: WiFi Scan](#)

Your device automatically checks for the best channel to broadcast wireless services. However, in some cases it may be useful to switch to a different channel (1 through 11, for North America) on which the network will broadcast.



The scan covers a frequency range within the 2.4 Ghz or 5.0 Ghz band. Channel selection depends on government regulated radio frequencies that vary from region to region. Channel selection can have a significant impact on performance, depending on other wireless activity close to this device. You need not select a channel at any of the computers on your wireless network. They will automatically scan available channels seeking a wireless device broadcasting on the SSID for which they are configured.

This scan will disconnect any wireless client devices from the wireless network.

If you want to scan for a different channel on which the device will broadcast, click the [Continue](#) button.



---

## Link: Subnets & DHCP

When you click the [Subnets & DHCP](#) link, the Subnets & DHCP page appears.

The screenshot shows the AT&T NVG599 configuration interface for Subnets & DHCP. The page has a blue header with the AT&T logo and navigation tabs for Device, Broadband, Home Network, Voice, Firewall, and Diagnostics. The Subnets & DHCP tab is selected. The main content area is divided into four sections: Private LAN Subnet, DHCP Server, Public Subnet, and Cascaded Router. Each section contains input fields for various parameters. A Help sidebar on the right provides detailed explanations for each configuration option.

Section	Parameter	Value
Private LAN Subnet	Device IPv4 Address	192.168.1.254
	Subnet Mask	255.255.255.0
DHCP Server	DHCPv4 Start Address	192.168.1.64
	DHCPv4 End Address	192.168.1.253
	DHCP Lease (Days)	1
	DHCP Lease (Hours)	0
Public Subnet	Public Subnet Mode	Off
	Allow Inbound Traffic	Off
	Public IPv4 Address	
	Public Subnet Mask	255.255.255.0
	DHCPv4 Start Address	
	DHCPv4 End Address	
Cascaded Router	Cascaded Router Enable	Off
	Cascaded Router Address	
	Network Address	
	Subnet Mask	255.255.255.248

The server configuration determines the functionality of your DHCP settings. This functionality enables the NVG599 to assign your LAN computer(s) a “private” IP address and other parameters that allow network communication. This feature simplifies network administration because the NVG599 maintains a list of IP address assignments. Additional computers can be added to your LAN without the need to configure an IP address. This is the default mode for your NVG599 device.

### Private LAN Subnet

- ◆ **Device IPv4 Address:** The IP address of your device as seen from the LAN.
- ◆ **Subnet Mask:** Subnet mask of your LAN.

### DHCP

- ◆ **DHCPv4 Start Address:** First IP address in the range being served to your LAN by the NVG599 DHCP server.
- ◆ **DHCPv4 End Address:** Last IP address in the range being served to your LAN by the NVG599 DHCP server.
- ◆ **DHCP Lease:** Specifies the default length for DHCP leases issued by the router. Enter lease time in *dd:hh:mm:ss* (days/hours/minutes/seconds) format.

### Public Subnet

- ◆ **Public Subnet Enable:** If you select **On** from the drop-down menu, you can enable a second subnet to distribute public addresses to DHCP clients; this means that IP addresses assigned to LAN clients will be public addresses.
- ◆ **Public IPv4 Address:** The IP address of your NVG599 device as seen from the WAN.
- ◆ **Public Subnet Mask:** Public subnet mask.

- ◆ **DHCPv4 Start Address:** First IP address in the range being served from a DHCP public pool.
- ◆ **DHCPv4 End Address:** Last IP address in the range being served from a DHCP public pool.
- ◆ **Primary DHCP Pool:** Choose the source of the DHCP pool IP address assignment by selecting either **Private** (local to your LAN) or **Public** (assigned remotely).

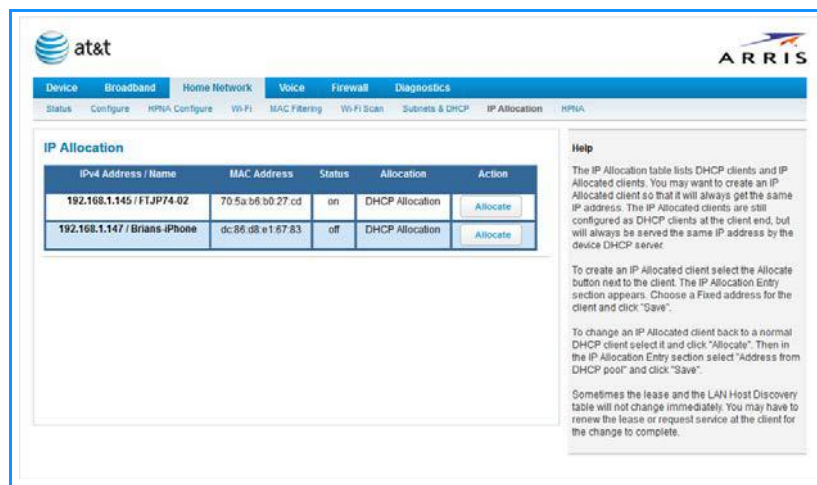
### Cascaded Router

- ◆ **Cascaded Router Enable:** If you have another router behind this device, choose **On** from the drop-down menu.
- ◆ **Cascaded Router Address:** If you chose **On** from the drop-down menu, enter the IP address of the router you are using behind this device in the LAN private IP subnet range.
- ◆ **Network Address:** If you chose **On** from the drop-down menu, enter the Network Address that defines the range of IP addresses available to clients of the router you are using behind this device.
- ◆ **Subnet Mask:** If you chose **On** from the drop-down menu, enter the subnet mask for the network address that defines the range of IP addresses available to clients of the router you are using behind this device.

If you make any changes here, click the **Save** button, and if prompted, restart the NVG599 device.

### Link: IP Allocation

When you click the [IP Allocation](#) link, the IP Allocation page appears.



**NOTE:**

IP Allocation functions require you to enter your NVG599 Gateway's access code. Information on the device code is provided in ["Device Access Code" on page 24](#)

The IP Allocation page lets you set aside or assign IP addresses to client devices on your network. With IP allocation, you can configure known devices to either use DHCP for dynamic IP address assignment, or set aside a specific IP address for a client device. When IP allocation is enabled for a client, that device is assigned a pre-determined IP address by the DHCP server of the NVG599. IP allocation lets you set up client devices as common DHCP systems, but ensures that they always receive the same IP address from the gateway.

The IP Allocation table shows a list of all identified and active client devices the NVG599 is serving.

To change the allocation method used by a client:

1. Locate the client in the IP Allocation table. The client may be identified by the *Name* value (in the *IPv4 Address/Name* column) or the device MAC address.
2. Click the **Allocate** button associated with the client entry.