

**SMART/RG<sup>®</sup>**  
forward thinking

## / GATEWAY USER MANUAL

For all Broadcom Chipset-based models including:

ADSL 3xx series

VDSL 5xx series

Release 3.5

June 2016

## Table of Contents

<b>Table of Contents</b> .....	<b>1</b>
<b>Disclaimer</b> .....	<b>3</b>
<b>Copyright and Trademarks</b> .....	<b>3</b>
<b>FCC Interference Statement</b> .....	<b>3</b>
<b>FCC Caution</b> .....	<b>3</b>
<b>Safety Warnings</b> .....	<b>4</b>
<b>Welcome!</b> .....	<b>5</b>
Purpose & Scope .....	5
Intended Audience .....	5
Getting Assistance .....	5
<b>GETTING FAMILIAR WITH YOUR GATEWAY</b> .....	<b>6</b>
LED Status Indicators .....	6
Connections .....	6
External Buttons .....	8
Installing your SmartRG Gateway .....	9
Logging in to your SmartRG Gateway's UI .....	9
<b>Device Info</b> .....	<b>11</b>
Summary .....	11
WAN .....	12
Statistics .....	14
Statistics - WAN Page for SR515ac Gateway	16
References .....	21
Route .....	21
ARP .....	22
DHCP .....	23
<b>ADVANCED SETUP</b> .....	<b>24</b>
Layer2 Interface .....	24
WAN Service .....	30
Ethernet Config .....	44
MoCA .....	45
LAN .....	47
NAT .....	50
Security .....	55

Add a MAC Filtering Rule .....	59
Parental Control .....	60
Quality Of Service .....	62
Supported DSCP Values .....	64
Routing .....	73
DNS .....	77
DSL .....	81
DSL Bonding .....	84
UPnP .....	86
DNS Proxy .....	87
Interface Grouping .....	88
IP Tunnel .....	89
IPSec .....	92
Certificate .....	94
Multicast .....	98
<b>WIRELESS</b> .....	<b>100</b>
Basic .....	100
Security .....	103
MAC Filter .....	112
Wireless Bridge .....	113
Advanced .....	114
Station Info .....	118
<b>DIAGNOSTICS</b> .....	<b>118</b>
Diagnostics .....	118
Fault Management .....	119
Ethernet OAM .....	120
Ping .....	122
Trace Route to Host .....	122
<b>Management</b> .....	<b>123</b>
Settings .....	123

---

System Log .....	127
Security Log .....	129
SNMP Agent .....	130
Management Server .....	131
Internet Time .....	136
Access Control .....	137
Add an Account .....	137
Modify or Delete an Account .....	138
Default Passwords .....	140
Update Software .....	144
Reboot .....	144
<b>APPENDIX A: ADVANCED FEATURES .....</b>	<b>146</b>
Connect-and-Surf (Automatic Broadband Con- nection Configuration) .....	146
Activation (Automatic ACS Connection Con- figuration) .....	146
TR-069 Remote Management: ACS Support .....	146
<b>APPENDIX B: FEATURE COMPARISON MATRIX .....</b>	<b>148</b>
<b>Q&amp;A .....</b>	<b>150</b>
<b>REVISION HISTORY .....</b>	<b>150</b>

## Disclaimer

SmartRG does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor patent rights of others. SmartRG further reserves the right to make changes to any products described herein without notice. This publication is subject to change without notice.

Any trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Copyright and Trademarks

Copyright © 2016 by SmartRG, Inc.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of SmartRG, Inc.

Published by SmartRG, Inc. All rights reserved.

## FCC Interference Statement

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions:

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

This Class B digital apparatus complies with Canadian ICES-003.

*Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.*

## FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement:

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
- This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adapter to the correct supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas, or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust, or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

## Welcome!

Thank you for purchasing this SmartRG product.

SmartRG proudly brings you the best, most innovative broadband gateways available. SmartRG enables service providers to monitor, manage, and monetize the connected home through the design and production of reliable and highly interoperable hardware and software solutions.

As an early innovator in TR-069 remote management technology, SmartRG offers the finest in managed broadband and home networking solutions. Our products leverage various broadband access technologies and are outfitted with highly customizable software, meeting diverse service provider requirements. Based in the USA, SmartRG provides local, proactive software development and customer support. In the rapidly evolving broadband market, SmartRG helps service providers keep their businesses on the cutting edge through its laser-focused product line, leveraging the very latest in broadband access and home networking technologies. SmartRG solutions enable service providers to improve their bottom line by reducing service costs and increasing customer satisfaction.

Learn more at [www.SmartRG.com](http://www.SmartRG.com).

## *Purpose & Scope*

The purpose and scope of this document is to provide SmartRG customers with installation, configuration and monitoring information for the SR300x and SR500x CPE platforms.

## *Intended Audience*

The information in this document is intended for Network Architects, NOC Administrators, Field Service Technicians, and other networking professionals responsible for deploying and managing broadband access networks. Readers of this manual are assumed to have a basic understanding of desktop computer operating systems, networking concepts and telecommunications.

## *Getting Assistance*

**Subscribers:** If you require help with this product, please contact your service provider.

**Service providers:** if you require help with this product, please open a support request.

## GETTING FAMILIAR WITH YOUR GATEWAY

This section contains a quick description of the Gateway's lights, ports, and buttons. SmartRG produces several models that vary slightly in capabilities (See Appendix B for details) but the basic scheme of lights, ports and buttons represented in this section exists on each model.

### LED Status Indicators

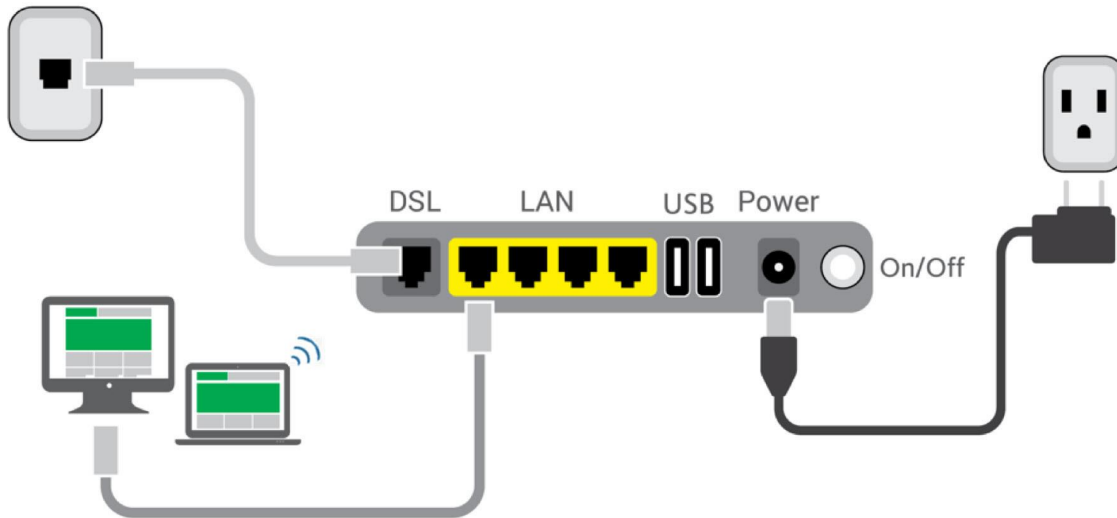
Your SmartRG gateway has several indicator lights (LEDs) on its exterior. The number and type of ports vary from model to model. The following table illustrates a comprehensive set of LEDs to cover the indicators available on all models.

	POWER	WAN	LAN 1-4	WLAN	WPS	DSL 1 or 2	INTERNET
Power up test failure	●						
DSL sync acquired and gateway online	●					●	●
No sync to DSL line	●					○	
DSL sync in progress	●					⚙	
Modem authentication in progress	●					●	⚙
DSL sync acquired and gateway online	●					●	●
Gateway online and data transfer in progress	●					●	⚙
IP connection failure	●						○
Connection dropped – attempting re-authentication	●	○				○	●
LAN device on network connected	●		●				
Wi-Fi enabled on modem	●			●			
PC / network activity / data transfer	●	●/⚙	●/⚙	●/⚙			●/⚙
WPS Setup procedure in progress	●			●	⚙		
Failure to find any partner with which to pair	●				●		
Session overlap detected. Possible security risk	●				⚙		
WPS Connection completed successfully	●			●	●		

● : On    ○ : Off    ⚙ : Blinking / active

### Connections

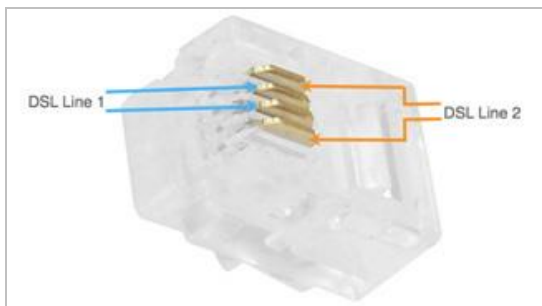
Below is a generic representation of a SmartRG gateway. Your specific model may have more or fewer ports and controls across the back of the unit. Refer to the Quick Start Guide enclosed with your gateway for specifics regarding installation of your particular model.



The ports depicted in this example are described below.

## DSL

The grey RJ12 port labeled DSL is specifically intended for connection to an internet provider via a DSL (Digital Subscriber Line) service. The center pair carries the first DSL line. For models like the SR550n equipped with two DSL ports and bonded DSL capability, the outer pair carries the second line.



## WAN

A stand-alone RJ45 port labeled WAN enables your SmartRG gateway to be hard-wired to another network device with a RJ45/Ethernet output such as a cable, fiber, or DSL modem.

For models with a stand-alone, RJ45, WAN port and a DSL port, the WAN port can be re-purposed to function as an additional LAN port when your internet connection is via DSL.

For instructions to enable this SmartPort™ feature, see the [Ethernet Configuration section](#) in this manual.



## LAN

The four (yellow) RJ45 ports across the back of your gateway labeled LAN1, LAN2, LAN3, LAN4 are the means to connect client devices such as computers and printers to your gateway.

On some models, one of these four ports may be labeled as WAN indicating SmartPort™ support. SmartPort allows a LAN port to be re-purposed to function as an Ethernet WAN port (described above). When this port is serving as a LAN port, the corresponding LED on the face of the unit is labeled "WAN"

For instructions to enable this SmartPort™ feature, see the [Ethernet Configuration section](#) in this manual.

## USB

USB ports on SmartRG products currently provide +5 DC volts.

## POWER

Use only the power supply included with your gateway. Intended for indoor use only.

## *External Buttons*

Smart RG gateways provide push-button controls on the exterior for critical features. These buttons provide a convenient way to trigger WPS mode, toggle the WiFi radio on and off, or reset the gateway. Their presence and locations vary by model.

The following describes each of these controls.

### **WPS Button**

The WPS button triggers WPS (Wi-Fi Protected Setup™) mode. WPS is a standard means for creating a secure connection between your gateway and various wireless client devices. It is designed to simplify the pairing process between devices.

If you have client devices that support WPS, use this button to automatically configure wireless security for your network.

For specific instructions, refer to the Quick Start Guide included with your gateway. Also see the "Basic" section of this manual.

WPS configures one client device at a time. You can repeat the steps as necessary for each additional WPS-compliant device you wish to connect.

The location of the WPS button varies by model:

- For SR360n models, the button is located on the top of the unit.
- For SR510n, SR550n, SR515ac, and SR552n models, the button is located on the left side of the unit.

For other models, an exterior button is not present. However, WPS is supported via the on-board software.

For specific instructions, refer to the Quick Start Guide included with your gateway.

### **WiFi or WLAN Button**

The button labeled WiFi or WLAN (depending on model) toggles the WiFi radio on and off. The WLAN LED indicator on the gateway displays the current state of the WiFi radio.

The location of the WLAN button varies by model:

- For SR360n models, the button is located on the top of the unit.
- For SR510n, SR512nm, SR550n, and SR552n models, the button is located on the left side of the unit.

For other models, an exterior button is not present. However, WiFi is supported via the on-board software.

For specific instructions, refer to the Quick Start Guide included with your gateway.

To activate the WiFi radio, press and hold the WiFi (WLAN) button for 3-5 seconds and then release. Expect a 1-3 second delay before the WiFi (WLAN) LED turns on. Repeat this step to deactivate the WiFi radio.

## Reset Button

The Reset button is a small hole in the gateway's enclosure with the actual button mounted behind the surface. This style of push-button prevents the gateway from being inadvertently reset during handling. Reset must be actuated with a paper clip or similar implement.

The location of the Reset button varies by model:

- For SR5xx and SR630n models, the button is located on the rear of the unit.
- For SR350n models, the button is located on the bottom of the unit.
- For SR360n models, the button is located on the left side of the unit.

This pin-hole sized reset button has three functions. The duration for which the button is held dictates which function is carried out.

Hold Duration	Effect
Less than 6 seconds	Performs a modem reset that is equivalent to the <b>Reboot</b> function in the gateway software.
6-20 seconds	Performs the software equivalent to the <b>Restore Defaults</b> function in the gateway software.
20 or more seconds	Changes the POWER LED to red and the gateway enters CFE mode which is a state associated with performing firmware updates via Internet browser.

## Installing your SmartRG Gateway

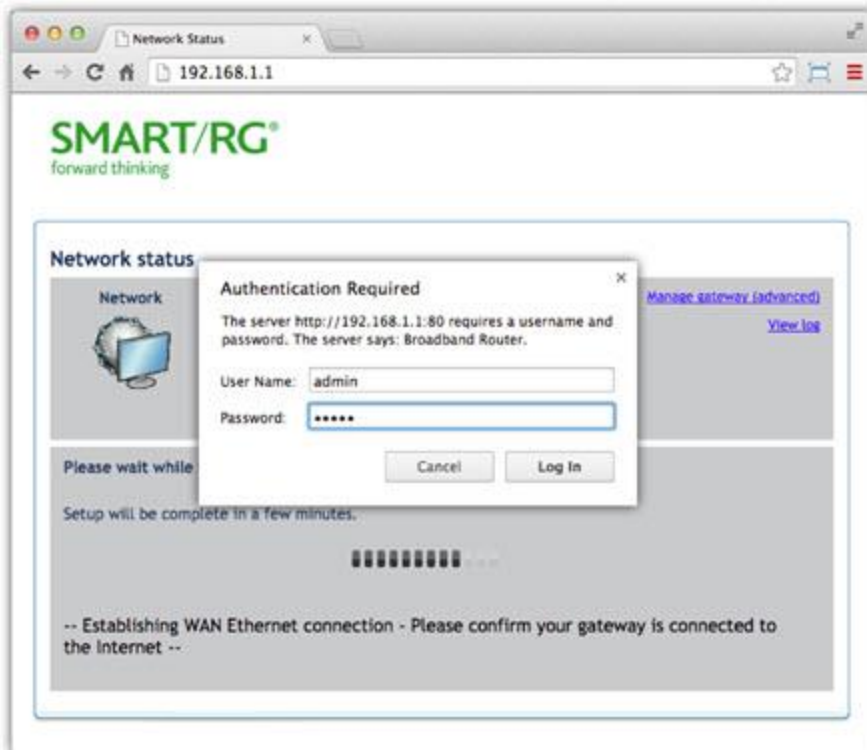
The following instructions explain all connection types offered for SmartRG gateways. For instructions specific to your gateway, follow the instructions in the Quick Start Guide included in the box.

1. Attach your computer's RJ45 connection to any of the SmartRG gateway's LAN ports (1-4).
2. Configure your computer's IP interface to acquire an IP address using DHCP. (For instructions on logging in to a SmartRG gateway configured for "bridge mode" operation, see the Note below.)

## Logging in to your SmartRG Gateway's UI

To manually configure the SmartRG Gateway, you can access the gateway's embedded web UI.

1. Open a browser and enter the gateway's default address (usually <http://192.168.1.1>; may also be <http://192.168.0.1>) in the address bar.
2. For some models, the Network status page appears. If so, click the [Manage gateway \(advanced\)](#) link (usually located in the upper right corner). The Authentication Required dialog box appears.



3. For all models, enter the default username and password (usually: admin/admin) and click **Login** or **OK** to display the default landing page. For many models, this is the Device Info page.

Note: The gateway's UI can be accessed via the WAN connection by entering the WAN IP address in your browser's address bar and entering the default username and password: support/support. WAN HTTP access control MUST be enabled to access the gateway's UI via the WAN connection. For more information, see the [Management Access Control](#) section.

If your SmartRG gateway is configured for "bridge mode" (modem) operation, your PC will NOT be able to acquire an address via CPE DHCP. Instead, manually configure your PC's interface with an IP address on the default network (e.g., 192.168.1.100).

The remainder of this guide is dedicated to a sequential walk-through of the gateway user interface. Screen captures are provided along with descriptions of the options available on the pictured page. Where applicable, valid values are provided.

For in-depth "how-to" information for specific scenarios, look at the knowledge base found on our support web site. Access to this site is restricted to SmartRG customers and partners. Do not share links to this site with your subscribers.

## Device Info

There are several selections under Device Info in the left navigation bar. Each of them shows a different element of the gateway's setup, status or nature of its connection with the provider and also with LAN devices. Device Info pages are read-only. You cannot interact with or change the settings in this section.

### *Summary*

When you log into the gateway interface, the **Device Info** is the first page to appear. This page displays details about the hardware and software associated with your gateway. In addition, the current status of the WAN connection (if present) is shown.

**Note:** The following variations exist:

- For the SR3xxn models, the **Symmetric CPU Threads** field and **Aggregate Line Rate** fields are not applicable.
- For the SR505n and SR510n models, the **Aggregate Line Rate** fields are not applicable. The **B0 Traffic** & **B1 Traffic** fields are unique to these two models and are not shown below.
- For the SR515ac model, the **Traffic Type** and **Aggregate Line Rate** fields are not applicable.

The screenshot shows the SMART/RG web interface. On the left is a navigation menu with 'Device Info' selected. The main content area is titled 'Device Info' and contains two tables. The first table lists hardware and software details. Below it is a note: 'This information reflects the current status of your WAN connection.' The second table shows WAN connection parameters, with 'Traffic Type' set to 'Inactive'.

**SMART/RG®**  
forward thinking

**Device Info**

Board ID:	SR552n
Symmetric CPU Threads:	2
Build Timestamp:	141223_1913
Software Version:	2.5.0.6
Configuration File Origin:	ClearAccess
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	A2pvbF039j.d25d
Wireless Driver Version:	6.30.163.23.cpe4.12L08.1
Uptime:	00 0H 59M 13S
System Base MAC Address:	00:23:6a:5d:bd:a9
Serial Number:	SR552NA084-0004464

This information reflects the current status of your WAN connection.

Traffic Type:	Inactive
Aggregate Line Rate - Upstream (Kbps):	0
Aggregate Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
WAN IPv4 Address:	0.0.0.0
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	

## WAN

On this page, you can view information about the connection between your ISP and your gateway. The WAN interface can be DSL or Ethernet and supports a number of Layer 2 and above configuration options (explained later in this document). Some features are supported only on specific SmartRG models. Those exceptions are specified in this guide.

In the left navigation bar, click **Device Info** > **WAN**. The following page appears.

WAN Info											
Interface	Description	Type	VlanMuxId	IPv6	Icmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ppp0	pppoe_0_0_1	PPPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Unconfigured	0.0.0.0	(null)

The fields on this page are explained in the following table.

Field Name	Description
Interface	The connection interface (Layer 2 interface) through which the gateway handles the traffic.
Description	The service description such ipoe_0_0_1, showing the type of WAN and its ID..
Type	The service type. Options are <b>PPPoE</b> , <b>IPoE</b> , and <b>Bridge</b> .
VlanMuxId	The VLAN ID. Options are <b>Disabled</b> or <b>0-4094</b> .
IPv6	The state of IPv6. Options are <b>Enabled</b> and <b>Disabled</b> .
Icmp	<i>(Not available on SR515ac gateways)</i> The state of IGMP. Options are <b>Enabled</b> and <b>Disabled</b> .
Icmp Pxy	<i>(Applies to SR515ac gateways only)</i> The IGMP proxy.
Icmp Src Enbl	<i>(Applies to SR515ac gateways only)</i> The IGMP source option is enabled for this connection.
MLD	<i>(Not available on SR515ac gateways)</i> The state of MLD. Options are <b>Enabled</b> and <b>Disabled</b> .
MLD Pxy	<i>(Applies to SR515ac gateways only)</i> The MLD proxy.
MLD Src Enbl	<i>(Applies to SR515ac gateways only)</i> The MLD source option is enabled for this connection.
NAT	The state of NAT. Options are <b>Enabled</b> and <b>Disabled</b> .
Firewall	The state of the Firewall. Options are <b>Enabled</b> and <b>Disabled</b> .
Status	The status of the WAN connection. Options are <b>Disconnected</b> , <b>Unconfigured</b> , <b>Connecting</b> , and <b>Connected</b> .
IPv4 Address	The obtained IPv4 address.
IPv6 Address	The obtained IPv6 address.

## Statistics

The Statistic pages provide network interface information for LAN, WAN Service, xTM and xDSL. All data is updated in 15-minute intervals.

### Notes:

- For SR512nm models, statistics are also provided for MoCA connections.
- For SR515ac models, statistics are also provided for the 2.4 Ghz and 5 Ghz wireless connections.

## LAN

On this page, you can view the received and transmitted bytes, packets, errors and drops for each LAN interface configured on your gateway. All local LAN Ethernet ports, Ethernet WAN ports and w10 (Wireless Interface) are included.

In the left navigation bar, click [Device Info](#) > [Statistics](#). The Statistics - LAN page appears where you can view detailed information about the status of your LAN.

To reset the counters, click [Reset Statistics](#) near the bottom of the page.

**SMART/RG®**  
forward thinking

Device Info  
Summary  
WAN  
Statistics  
LAN  
WAN Service  
xTM  
xDSL  
Route  
ARP  
DHCP  
Advanced Setup  
Wireless  
Diagnostics

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN1	735907	7373	0	0	881198	4051	0	0
LAN2	0	0	0	0	0	0	0	0
LAN3	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0
WAN	6386003	61584	0	0	3909821	20855	0	0
w10	0	0	0	0	0	0	0	0

[Reset Statistics](#)

**Note:** Only the SR360n and SR5xx models support the SmartPort feature where a LAN port can be re-purposed to function as a WAN port (as shown in the [Interface](#) column).

The fields on this page are explained in the following table.

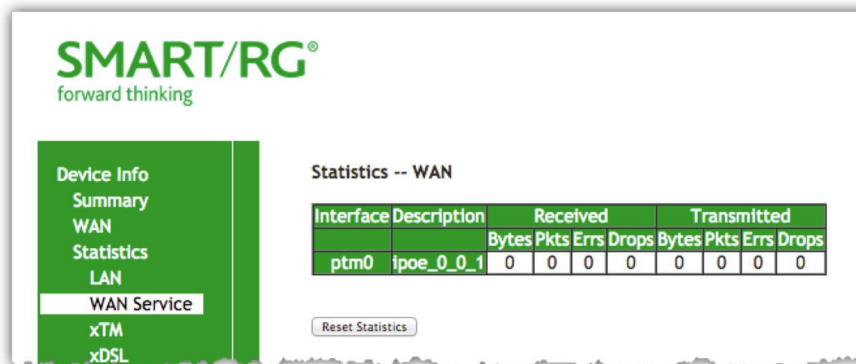
Field Name	Description
Interface	Available LAN interfaces. Options are <b>LAN1 - LAN4</b> , <b>WAN</b> (if configured on your device), and <b>WLO</b> (Wireless LAN-side interface), and <b>2.4 Ghz</b> and <b>5 Ghz</b> (SR515ac only).
<b>Received &amp; Transmitted</b> columns	
Bytes	Total number of packets in bytes.
Pkts	Total number of packets.
Errs	Total number of error packets.
Drops	Total number of dropped packets.

## WAN Service

On this page, you can view the received and transmitted bytes, packets, errors and drops for each WAN interface for your SmartRG Gateway. All WAN interfaces configured for your gateway are included.

In the left navigation bar, click **Device Info** > **Statistics** > **WAN Service**. The Statistics - WAN page appears where you can view detailed information about the status of your WAN.

To reset the counters, click **Reset Statistics** near the bottom of the page.



The fields on this page are explained in the following table.

Field Name	Description
Interface	Available WAN interfaces. Options are: <b>atm</b> , <b>ptm</b> , and <b>eth</b> .
Description	Service description. Options are: <b>pppoe</b> , <b>ipoe</b> , and <b>b</b> .
<b>Received &amp; Transmitted</b> columns	
Bytes	Total quantity of packets in bytes.
Pkts	Total quantity of packets.
Errs	Total quantity of error packets.
Drops	Total quantity of dropped packets.



## Statistics - WAN Page for SR515ac Gateway

The Statistics - WAN page for the SR515ac gateway is shown below. Statistics are provided for Multicast, Unicast, Broadcast, and total packets received and sent.

The columns labeled **Interface** and **Description** for the other gateway models are combined into the **Service Description** column on the SR515ac page.

Service Description	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
br_0_0_35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
pppoe_0_0_35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
lpoeth4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

## xTM

On this page, you can view the ATM/PTM statistics for your gateway. All WAN interfaces configured for your SmartRG gateway are included.

In the left navigation bar, click **Device Info** > **Statistics** > **xTM**. The Interface Statistics page appears.

To reset these counters, click **Reset Statistics** near the bottom of the page.

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
Reset										

The fields on this page are explained in the following table.

Field Name	Description
Port Number	Statistics for Port 1, or both ports if Bonded.
In Octets	Total quantity of received octets.
Out Octets	Total quantity of transmitted octets.
In Packets	Total quantity of received packets.
Out Packets	Total quantity of transmitted packets.
In OAM Cells	Total quantity of received OAM cells.
Out OAM Cells	Total quantity of transmitted OAM cells.
In ASM Cells	Total quantity of received ASM cells.
Out ASM Cells	Total quantity of transmitted ASM cells.
In Packet Errors	Total quantity of received packet errors.
In Cell Errors	Total quantity of received cell errors.

## xDSL

On this page, you can view the DSL statistics for your gateway. All xDSL (VDSL or ADSL) interfaces configured for your SmartRG gateway are included. The terms and their explanations are derived from the relevant ITU-T standards and referenced accordingly.

1. In the left navigation bar, click **Device Info** > **Statistics** > **xDSL**. The Statistics - xDSL page appears.

**SMART/RG**  
forward thinking

Device Info  
Summary  
WAN  
Statistics  
LAN  
WAN Service  
xTM  
xDSL  
Route  
ARP  
DHCP  
Advanced Setup  
Wireless  
Diagnostics  
Management  
Logout

Statistics -- xDSL

Bonding Line Selection

Mode:		
Traffic Type:		
Status:		
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

2. In the **Bonding Line Selection** field, select the line for which you want to view the statistics.  
**Note:** For the SR350n, SR360n, and SR505n models, the **Bonding Line Selection** field does not appear.
3. To run an xDSL Bit Error Rate (BER) test which determines the quality of the xDSL connection:
  - a. Scroll to the bottom of the page and click **xDSL BER Test**. The ADSL BER Test dialog box appears.
  - b. In the **Tested Time** field, select the duration in seconds and click **Start**. Options range from **1** second to **360** seconds. The test transfers idle cells containing a known pattern and compares the received data with this known pattern. Comparison errors are tabulated and displayed.
4. To reset the counters, click **Reset Statistics** at the bottom of the page.

The fields on this page are explained in the following table.

Field Name	Description
Mode	xDSL mode that the modem has trained under, such as ADSL2+, G.DMT, etc.
Traffic Type	Connection type. Options are: <b>ATM</b> , <b>PTM</b> and <b>ETH</b> .
Status	Status of the connection. Options are: <b>Up</b> , <b>Disabled</b> , <b>NoSignal</b> , and <b>Initializing</b> .
Link Power State	Current link power management state (e.g., L0, L2, L3).
<b>Downstream</b> and <b>Upstream</b> columns	
Line Coding (Trellis)	State of the Trellis Coded Modulation. Options are <b>On</b> and <b>Off</b> .
SNR Margin (0.1 db)	The signal-to-noise ration margin (SNRM) is the maximum increase (in dB) of the received noise power, such that the modem can still meet all of the target BERs over all the frame bearers. [2]
Attenuation (0.1 db)	The signal attenuation is defined as the difference in dB between the power received at the near-end and that transmitted from the far-end. [2]
Output Power (0.1 dBm)	Transmit power from the gateway to the DSL loop relative to one Milliwat (dBm).
Attainable Rate (Kbps)	The typically obtainable sync rate, i.e., the attainable net data rate that the receive PMS-TC and PMD functions are designed to support under the following conditions: <ul style="list-style-type: none"> <li>• Single frame bearer and single latency operation</li> <li>• Signal-to-Noise Ratio Margin (SNRM) to be equal or above the SNR Target Margin</li> <li>• BER not to exceed the highest BER configured for one (or more) latency paths</li> <li>• Latency not to exceed the highest latency configured for one (or more) latency paths</li> <li>• Accounting for all coding gains available (e.g., trellis coding, RS FEC) with latency bound</li> <li>• Accounting for the loop characteristics at the instant of measurement [2]</li> </ul>
PhyR Status	<i>(Visible only for gateways connected via DSL)</i> Physical Layer Retransmission feature status. Options are <b>Inactive</b> and <b>Active</b> .
G. inp Status	<i>(Visible only for gateways connected via DSL)</i> The status of video data retrieval from the buffer. Options are <b>Inactive</b> and <b>Active</b> .
Rate (Kbps)	The current net data rate of the xDSL link. Net data rate is defined as the sum of all frame bearer data rates over all latency paths. [2]
<b>Downstream</b> and <b>Upstream</b> columns for DSL-specific fields only	
B (# of bytes in Mux Data Frame)	The nominal number of bytes from frame bearer #n per Mux Data Frame at Reference Point A in the current latency path.
M (# of Mux Data Frames in FEC Data Frame)	The number of Mux Data Frames per FEC Data Frame in the current latency path.
T (Mux Data Frames over sync bytes)	The ratio of the number of Mux Data Frames to the number of sync bytes in the current latency path.
R (# of check bytes in FEC Data Frame)	The number of Reed Solomon redundancy bytes per codeword in the current latency path. This is also the number of redundancy bytes per FEC Data Frame in the current latency path.

Field Name	Description
S (ratio of FEC over PMD Data Frame length)	The ratio of FEC over PMD Data Frame length.
L (# of bits in PMD Data Frame)	The number of bits from the latency path included per PMD.
D (interleaver depth)	The interleaving depth in the current latency path.
Delay (msec)	The PMS-TC delay in milliseconds of the current latency path (or the lowest latency path when running dual-latency paths).
INP (DMT symbol)	The input level for DMT-managed DSL environments.
OH Frames	The number of xDSL OH Frames transmitted/received.
OH Frame Errors	The number of xDSL OH Frames transmitted/received with errors.
<i>(End of DSL-specific field group)</i>	
Super Frames	The number of xDSL Super Frames transmitted/received.
Super Frame Errors	The number of xDSL Super Frames transmitted/received with errors.
RS Words	The number of Reed-Solomon-based Forward Error Correction (FEC) codewords transmitted/received.
RS Correctable Errors	The number of Reed-Solomon-based FEC codewords received with errors that have been corrected.
RS Uncorrectable Errors	The number of Reed-Solomon-based FEC codewords received with errors that were not correctable.
RS Codewords Received	<i>(Visible only for gateways connected via DSL)</i> Total number of Reed-Solomon Codewords received.
RS Codewords Corrected	<i>(Visible only for gateways connected via DSL)</i> Total number of Reed-Solomon Codewords corrected.
RS Codewords Uncorrected	<i>(Visible only for gateways connected via DSL)</i> Total number of Reed-Solomon Codewords Uncorrected
HEC Errors	A count of ATM HEC errors detected. As per ITU-T G.992.1 and G.992.3, a 1-byte HEC is generated for each ATM cell header. Error detection is implemented as defined in ITU-T I.432.1 with the exception that any HEC error shall be considered as a multiple bit error, and therefore, HEC Error Correction is not performed. [1],[2]
OCD Errors	Total number of Out-of-Cell Delineation errors. ATM Cell delineation is the process which allows identification of the cell boundaries. The HEC field is used to achieve cell delineation. [4] An OCD Error is counted when the cell delineation process transitions from the SYNC state to the HUNT state. [2]
LCD Errors	Total number of Loss of Cell Delineation errors. An LCD Error is counted when at least one OCD error is present in each of four consecutive overhead channel periods and SEF (Severely Errored Frame) defect is present. [2]
Total Cells	The total number of cells (OAM and Data cells) transmitted/received.
Data Cells	The total number of data cells transmitted/received.
Bit Errors	The total number of Idle Cell Bit Errors in the ATM Data Path. [3]
Total ES	Total number of Errored Seconds. This parameter is a count of 1-second intervals with one or more CRC-8 anomalies. [4]

Field Name	Description
Total SES	Total number of Severely Errored Seconds. An SES is declared if, during a 1-second interval, there are 18 or more CRC-8 anomalies in one or more of the received bearer channels, or one or more LOS (Loss of Signal) defects, or one or more SEF (Severely Errored Frame) defects, or one or more LPR (Loss of Power) defects. [4]
Total UAS	Total number of Unavailable Seconds. This parameter is a count of 1-second intervals for which the xDSL line is unavailable. The xDSL line becomes unavailable at the onset of 10 contiguous SESs. These 10 SES's shall be included in the unavailable time. Once unavailable, the xDSL line becomes available at the onset of 10 contiguous seconds with no SESs. These 10 seconds with no SES's shall be excluded from unavailable time. [4]

## References

- [1] [ITU-T Recommendation G.992.1](#) (1999), Asymmetric digital subscriber line (ADSL) transceivers.
- [2] [ITU-T Recommendation G.992.3](#) (2005), Asymmetric digital subscriber line transceivers 2 (ADSL2).
- [3] [ITU-T Recommendation G.997.1](#) (2006), Physical layer management for digital subscriber line (DSL) transceivers.
- [4] [ITU-T Recommendation I.432.1](#) (1999), B-ISDN user-network interface – Physical layer specification: General characteristics.

## Route

On this page, you can view the LAN and WAN route table information configured in your SmartRG Gateway for both IPv4 and IPv6 implementation.

In the left navigation bar, click **Device Info** > **Route**. The following page appears.

**SMART/RG®**  
forward thinking

**Device Info -- Route**

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

**IPv6 Route**

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

Destination	Next Hop	Flag	Metric	Service	Interface
/64	::	U	256		br0
fe80::/64	::	U	256		eth4
fe80::/64	::	U	256		eth3

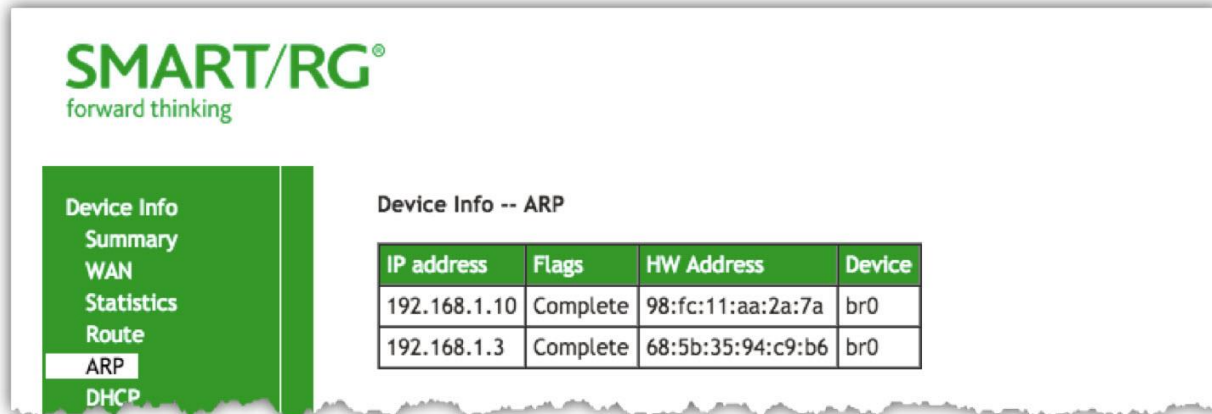
The fields on this page are explained in the following table.

Field Name	Description
Destination (Including IPv6 Route)	Destination IP addresses.
Gateway	Gateway IP address.
Subnet Mask	Subnet Masks.
Flag (Including IPv6 Route)	Status of the flags.
Metric (Including IPv6 Route)	Number of hops required to reach the default gateway.
Service (Including IPv6 Route)	Service type.
Interface (Including IPv6 Route)	WAN/LAN interface.
Next Hop (IPv6 Route only)	Next hop IP address.

## ARP

On this page, you can view the host IP addresses and their hardware (MAC) addresses for each LAN Client connected to the gateway via a LAN Ethernet port or wireless LAN.

In the left navigation bar, click **Device Info** > **ARP**. The following page appears.



The fields on this page are explained in the following table.

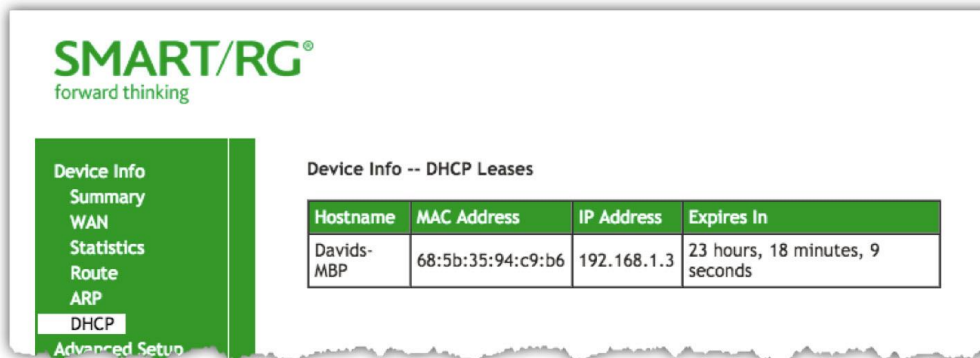
Field Name	Description
IP address	The IP address of the host.
Flags	Each entry in the ARP cache will be marked with one of these flags. Options are: <b>Complete</b> , <b>Permanent</b> , and <b>Published</b> .
HW Address	The hardware (MAC) address of the host.
Device	The system level interface by which the host is connected. Options are: <b>br(n)</b> , <b>atm(n)</b> , <b>eth(n)</b> , and <b>atm(n)</b> .

## DHCP

The DHCP page displays a list of locally connected LAN hosts and their DHCP lease status, which are directly connected to the SmartRG Gateway via a LAN Ethernet port or Wireless LAN.

In the left navigation bar, select **Device Info** > **DHCP**. The following page appears.





The fields on this page are explained in the following table.

Field Name	Description
Hostname	The host name of each connected LAN device.
MAC Address	The MAC Address for each connected LAN device.
IP Address	The IP Address for each connected LAN device.
Expires In	The time until the DHCP lease expires for each LAN device.

## ADVANCED SETUP

In this section, you can configure network interfaces, security, quality of service settings, and many other settings for your gateway and network.

### Layer2 Interface

In this section, you can configure interfaces for ATM, PTM and Ethernet interfaces. Generally you can accept the settings configured by default. If your network is highly customized, you may need to modify some of the settings, such as **Username** and **Password**.

### ATM Interface

On this page, you can configure Asynchronous Transfer Mode / Permanent Virtual Conduit (ATM/PVC) settings for your gateway. You can customize latency options, link type, encapsulation mode and more.

**Note:** Devices (routers) on both ends of the connection must support ATM / PVC.

1. In the left navigation bar, click **Advanced Setup > Layer2 Interface > ATM Interface** and then click **Add**. The following page appears.

**SMART/RG®**  
forward thinking

**Device Info**  
Advanced Setup  
Layer2 Interface  
WAN Service  
4G LTE Settings  
Ethernet Config  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
UPnP  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
Diagnostics  
Management  
Logout

**ATM PVC Configuration**

This screen allows you to configure a ATM PVC.

VPI:  [0-255]  
VCI:  [32-65535]

Select DSL Latency  
 Path0 (Fast)  
 Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)  
 EoA  
 PPPoA  
 IPoA

Encapsulation Mode:

Service Category:

Minimum Cell Rate:  [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue  
 Weighted Round Robin  
 Weighted Fair Queuing

Default Queue Weight:  [1-63]  
Default Queue Precedence:  [1-8] (lower value, higher priority)

VC WRR Weight:  [1-63]  
VC Precedence:  [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's. For single queue VC, the default queue precedence and weight will be used for arbitration. For multi-queue VC, its VC precedence and weight will be used for arbitration.

2. Modify the settings as desired, using the information provided in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
VPI	Enter a Virtual Path Identifier. A VPI is an 8-bit identifier that uniquely identifies a network path for ATM cell packets to reach its destination. A unique VPI number is required for each ATM path. This setting works with the VCI. Each individual DSL circuit must have a unique VPI/VCI combination. String limits are: <b>0-255</b> .
VCI	Enter a Virtual Channel Identifier. A VCI is a 16-bit identifier that has a unique channel.

Field Name	Description
	Options are: <b>32-65535</b> .
Select DSL Latency	Select the level of DSL latency. Options are: <ul style="list-style-type: none"> <li>• <b>Path0 Fast:</b> No error correction and can provide lower latency on error free lines.</li> <li>• <b>Path1 Interleaved:</b> Error checking that provides error free data which increases latency.</li> <li>• <b>Path0&amp;1 Both:</b> Fast &amp; Interleaved.</li> </ul>
Select Link Type	Select the linking protocol. <b>EoA</b> is the most popular with <b>PPPoA</b> a close second (used with many legacy ISPs). Options are: <ul style="list-style-type: none"> <li>• <b>EoA:</b> Ethernet over ATM.</li> <li>• <b>PPPoA:</b> Point-to-Point Protocol over ATM.</li> <li>• <b>IPoA:</b> Internet Protocol over ATM.</li> </ul>
Encapsulation Mode	Select whether multiple protocols or only one protocol is carried per PVC (Permanent Virtual Circuit). Options are: <ul style="list-style-type: none"> <li>• <b>LLC/SNAP-BRIDGING:</b> Logical Link Control used to carry multiple protocols in a single PVC.</li> <li>• <b>VC/MUX:</b> Virtual Circuit Multiplexer creates a virtual connection used to carry one protocol per PVC.</li> </ul>
Service Category	Select the bit rate protocol. Options are: <ul style="list-style-type: none"> <li>• <b>UBR without PCR:</b> Unspecified Bit Rate with no Peak Cell Rate, flow control or time synchronization between the traffic source and destination. Commonly used with applications that can tolerate data / packet loss.</li> <li>• <b>UBR with PCR:</b> Same as above but with a Peak Cell Rate.</li> <li>• <b>CBR:</b> Constant Bit Rate relies on timing synchronization to make the network traffic predictable. Used commonly in Video and Audio traffic network applications.</li> <li>• <b>NON Realtime VBR:</b> Non Realtime Variable Bit Rate used for connections that transport traffic at a Variable Rate. This category requires a guaranteed bandwidth and latency. It does not rely on timing synchronization between the destination and source.</li> <li>• <b>Realtime VBR:</b> Realtime Variable Bit Rate. Same as the above option but relies on timing and synchronization between the destination and source. This category is commonly used in networks with compressed video traffic.</li> </ul>
Minimum Cell Rate	Minimum allowable rate (cells per second) at which cells can be sent on a ATM network. For no shaping, enter -1.
Scheduler for Queues of Equal	The algorithm used to schedule the queue behavior. VC scheduling is unique from Default Queues. Options are:

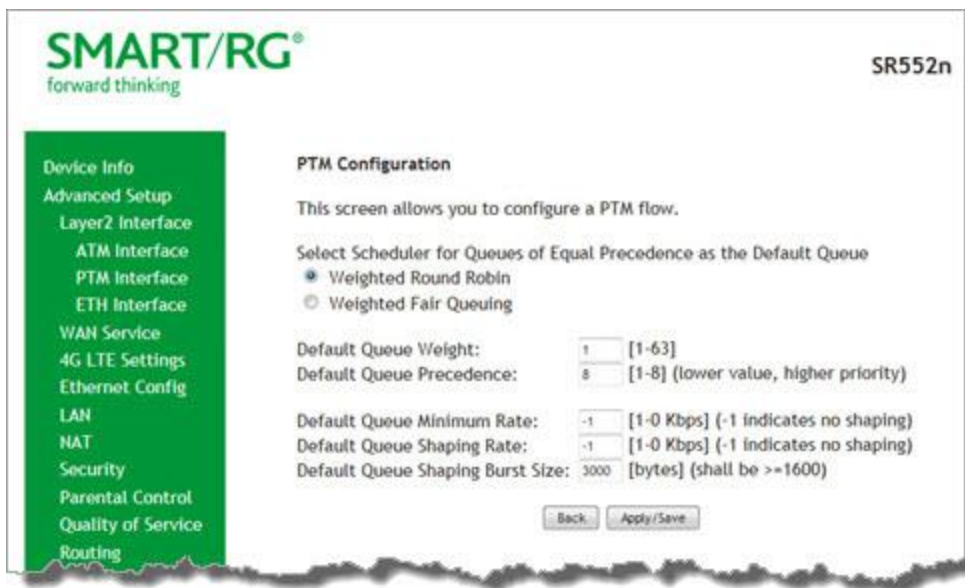
Field Name	Description
Precedence as the Default Queue	<ul style="list-style-type: none"> <li>• <b>WRR:</b> Weighted Round Robin packets are accessed in a round robin style and classes can be given.</li> <li>• <b>WFQ:</b> Weighted Fair Queuing packets are assigned in a specific queue.</li> <li>• <b>Default Queue Weight:</b> The default weight of the specified queue. Options are: 1-63.</li> <li>• <b>Default Queue Precedence:</b> The precedence of the specified group. Options are: 1-8</li> </ul>

## PTM Interface

The SmartRG gateway's VDSL2 standards support Packet Transfer Mode (PTM). An alternative to ATM mode, PTM transports packets (IP, PPP, Ethernet, MPLS, and others) over DSL links. For more information, refer to the IEEE802.3ah standard for Ethernet in the First Mile (EFM). Some 500 series gateways have a PTM interface configured by default.

On this page, you can configure a PTM interface for your gateway.

1. In the left navigation bar, click **Advanced Setup** > **Layer2 Interface** > **PTM Interface** and then click **Add**. The following page appears.



2. Modify the settings as desired.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Weighted Round Robin	Time slices are assigned to each process in equal portions and in circular order, hand-

Field Name	Description
	ling all processes without priority (also known as cyclic executive).
Weighted Fair Queuing	A data packet scheduling technique allowing different scheduling priorities to be assigned to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (that sent larger packets or more packets per second than the others since it became active) will only affect itself and not other sessions.
Default Queue Weight	Enter a default weight of the specified queue. Options are: <b>1-63</b> .
Default Queue Precedence	Enter a precedence for the specified queue. Options are: <b>1-8</b> .
Default Queue Minimum Rate	<i>(Does not appear for SR350n models)</i> The default minimum rate at which traffic can pass through the queue. For no shaping, enter -1 (disabled). Options are: <b>1-0</b> Kbps.
Default Queue Shaping Rate	<i>(Does not appear for SR350n models)</i> The shaping rate for the specified queue. For no shaping, enter -1 (disabled). Options are: <b>1-0</b> Kbps.
Default Queue Shaping Burst Rate	<i>(Does not appear for SR350n models)</i> The maximum rate at which traffic can pass through the queue. Options are <b>1600</b> or greater.

## ETH Interface

If you are using a gateway that is Ethernet-specific (non-DSL), you may want to configure an ETH interface to manage communication. Most models support Ethernet and can be configured for Ethernet and DSL at the same time. Your gateway has four LAN ports. One of them can be re-purposed to become an RJ45 WAN port when needed.

On this page, you can configure an Ethernet interface for your gateway.

1. In the left navigation bar, click **Advanced Setup > Layer2 Interface > ETH Interface**. If no WAN port is configured, the following page appears.



2. Click **Add**.
3. If a WAN port is already configured or you clicked **Add**, the following page appears.



**Note:** If a WAN port it is already configured, you must remove it before you can define a new one. Before you can remove the existing port, you must first modify or delete any WAN service that uses it. The **Add** button does not appear until the existing port is removed. Click the **Remove** checkbox and then click the **Remove** button.

4. Select the LAN port you wish to act as a WAN port.
5. Click **Apply/Save** to commit your changes.

## WAN Service

In this section, you can configure WAN services for:

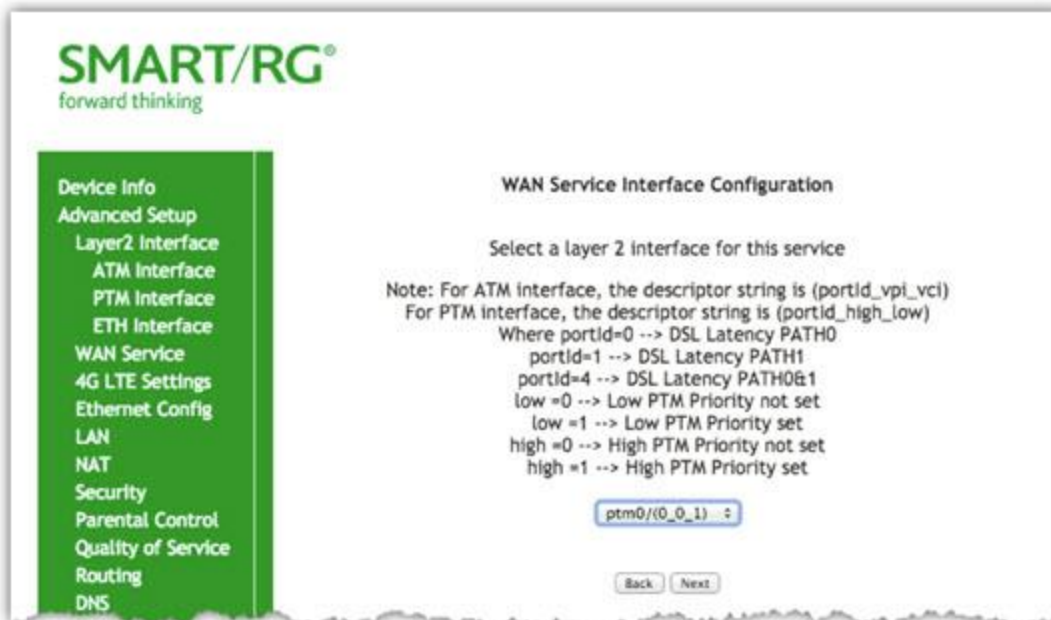
- ["PPP over Ethernet"](#)
- ["IP over Ethernet"](#)

A sample configuration scenario is provided for each variation.

### PPP over Ethernet

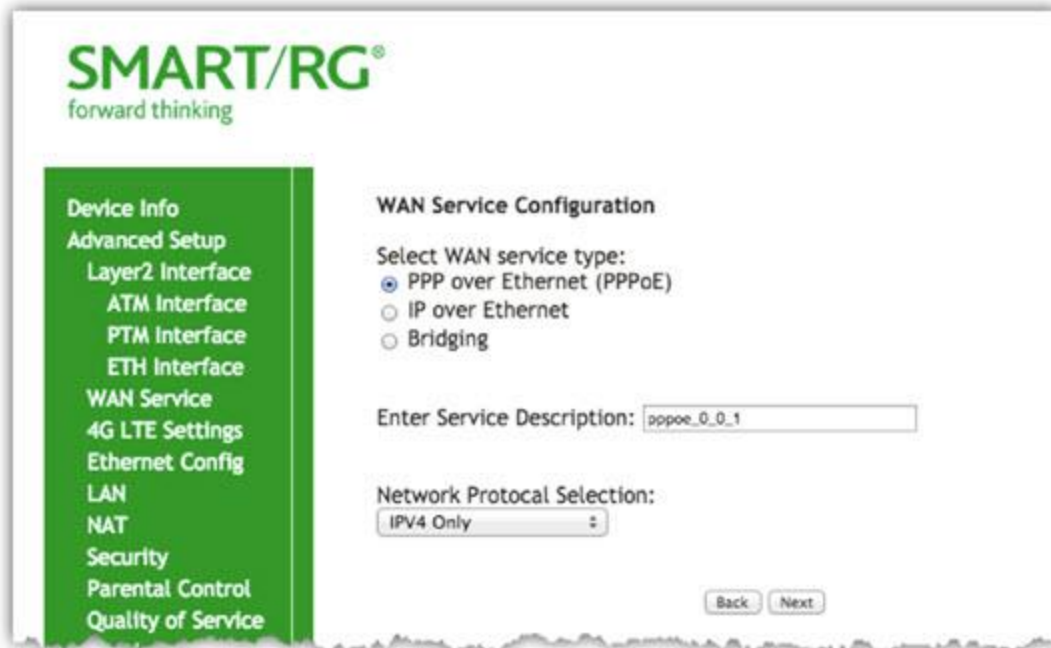
There are several parts to configuring a PPP over Ethernet WAN service. You will progress through several pages to complete the configuration.

1. In the left navigation bar, click **Advanced Setup** > **WAN Service** and then click **Add**. The following page appears.



2. Select the Layer2 interface to use for the WAN service.

3. Click **Next**. The following page appears.



4. Select the **PPP over Ethernet (PPPoE)** WAN service type.
5. Modify the other settings as needed.


The fields on this page are explained in the following table.

Field Name	Description
Enter Service Description	Enter a name to describe this configuration.
Network Protocol Selection	<p>(For SR515ac models, this field is named <b>Internet Protocol Selection</b>) Different scheduling priorities can be applied to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (which has sent larger packets or more packets per second than the others) will only punish itself and not other sessions. Options are <b>IPv4 Only</b>, <b>IPv4&amp;IPv6</b> (Dual Stack), and <b>IPv6 Only</b>.</p> <p><b>Note:</b> When you select <b>IPv4&amp;IPv6</b> or <b>IPv6</b>, the subsequent options presented will change accordingly.</p>
Enter 802.1P Priority	<p>(Available for SR515ac models only) Options are <b>0 - 7</b>. The default is <b>0</b>.</p> <p>For tagged service, enter values in this field and the <b>802.1Q VLAN ID</b> field.</p> <p>For untagged service, enter <b>-1</b> (disabled) in this field and the <b>802.1Q VLAN ID</b> field.</p>
Enter 802.1Q VLAN ID	<p>(Available for SR515ac models only) Options are <b>0 - 4094</b>. The default is <b>-1</b> (disabled).</p> <p>For tagged service, enter values in this field and the <b>802.1P Priority</b> field.</p>



Field Name	Description
	For untagged service, enter -1 (disabled) in this field and the <b>802.1P Priority</b> field.
Select VLAN TPID	(Available for SR515ac models only) Select the TPID for this VLAN. Options are <b>0x8100</b> , <b>0x88A8</b> , and <b>0x9100</b> .

6. Click **Next**. The following page appears where you will configure the PPP Username, Password and related information.



- Device Info
- Advanced Setup
- Layer2 Interface
- ATM Interface
- PTM Interface
- ETH Interface
- WAN Service
- 4G LTE Settings
- Ethernet Config
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- DSL Bonding
- UPnP
- DNS Proxy
- Interface Grouping
- IP Tunnel
- IPSec
- Certificate
- Multicast
- Wireless
- Diagnostics
- Management
- Logout

### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:   
 PPP Password:   
 PPPoE Service Name:   
 Authentication Method:

### Link Control Protocol

LCP Keepalive Period (s):   
 LCP Retry Threshold:

PPP IP extension  
 Advanced DMZ  
 Non DMZ IP Address:   
 Non DMZ Net Mask:

Use Static IPv4 Address  
 IPv4 Address:

Retry PPP password on authentication error  
 Max PPP authentication retries (1-65536):  (use 65536 to retry forever)

Enable PPP Debug Mode  
 Bridge PPPoE Frames Between WAN and Local Ports  
 Enable Firewall

### Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT  
 Enable Fullcone NAT  
 Enable SIP ALG

### Multicast Proxy

Enable IGMP Multicast Proxy  
 No Multicast VLAN Filter

MTU size [1370-1492]:

Use Base MAC Address on this WAN interface (Note: only select this for one WAN interface)

7. Modify the fields as needed.

The fields on this page are explained in the following table.

Field Name	Description
PPP Username	Enter the username required for authentication to the PPP server.
PPP Password	Enter the password required for authentication to the PPP server.
PPPoE Service Name	<i>(Optional)</i> Enter a description for this service.
Authentication Method	Select a means for authentication. Options are: <ul style="list-style-type: none"> <li>• <b>AUTO</b>: Attempt to automatically detect handshake protocol (listed below).</li> <li>• <b>PAP</b>: Password Authentication Protocol (plaintext passwords).</li> <li>• <b>CHAP</b>: Challenge Handshake Authentication Protocol. (MD5 hashing scheme on passwords).</li> <li>• <b>MSCHAP</b>: Microsoft Challenge Handshake Authentication Protocol. (Microsoft encrypted password authentication protocol).</li> </ul>
CP Keepalive Period	The frequency with which the keepalive packet is sent by the gateway to the PPP server.
LCP Retry Threshold	Enter the number of additional attempted packets that the gateway will send (in the event that the PPP server does not respond to the Keepalive) before giving up and declaring the connection as Failed.
Dial on Demand	Enables Inactivity Timeout (minutes). Enter the number of minutes before timeout kicks in. Options are 0 - 4320. The default is zero (0) which equals not applicable.  Connection automatically starts when there is outbound traffic to the Internet. It automatically terminates if the connection is idle, based on the value in the <b>Idle Timeout</b> setting.
PPP IP Extension	Select whether to forward all traffic to the advanced DMZ IP specified in the next field.
Advanced DMZ	<i>(Applies only when <b>PPP IP Extension</b> is selected)</i> Specify the IP address to which PPPoE traffic is forwarded.
Use Static IPv4 Address	Specify the IPv4 Address to apply for this WAN service.
Retry PPP password on authentication error	Enter the maximum number of PPP authentication retries on failure. Options are 1 - 65536. Entering 65536 sets the maximum to unlimited.
Enable PPP Debug Mode	Select to have the system put more PPP connection information into the system log of the device. This is for debugging errors and not for normal usage.
Bridge PPPoE Frames Between WAN and Local Ports	Select to enable PPPoE passthrough to relay PPPoE connections from behind the modem. Also known as Half-Bridged mode.
Enable Firewall	Select to enable functions in the <b>Security</b> sub-menu.

Field Name	Description
Enable NAT	Select to enable sharing the WAN interface across multiple devices on the LAN. Additional NAT and PPPoE NAT features appear.
Enable Fullcone NAT	<i>(Appears when <b>Enable NAT</b> is selected)</i> Click to enable what is known as one-to-one NAT.
Enable SIP	<i>(Appears when <b>Enable NAT</b> is selected)</i> Click to enable Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications.
Enable IGMP Multicast Proxy	<i>(Appears when <b>Enable NAT</b> is selected)</i> Click to enable Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
No Multicast VLAN Filter	<i>(Not available for SR515ac models)</i> Disables multicast filtering between WAN and LAN (VlanMux) network.
Enable IGMP Multicast Source	<i>(Available for SR515ac models only)</i> Select to enable this service to act as an IGMP multicast source.
MTU sizes	Enter the MTU (Maximum Transmission Unit) size for SmartRG gateways supporting a gigabit-capable WAN interface. Options are <b>1370 - 1492 bytes</b> . The default is <b>1492 bytes</b> . This feature is supported by SmartRG models SR500n, SR505n, SR510n, SR550n and SR552n. Firmware v2.5.0.7 or later is required.
Use Base MAC Address on this WAN interface	Use the SmartRG Devices Base (Primary) MAC address. When unchecked, a unique MAC is assigned for each service.
Enable MAC Clone	<i>(Appears when <b>Use Base MAC Address</b> is deselected)</i> Enter the MAC address to be used as the clone address.
Additional options for IPV6	Select options as needed. Options are: <ul style="list-style-type: none"> <li>• <b>Enable IPv6 Unnumbered Model</b></li> <li>• <b>Enable IPv6 Unnumbered Model</b></li> <li>• <b>Launch Dhcp6c for Address Assignment (IANA)</b></li> <li>• <b>Launch Dhcp6c for Prefix Delegation (IAPD)</b></li> <li>• <b>Enable MLD Multicast Proxy</b></li> </ul>

- Click **Next**. The following page appears where you will select the interface used as a default gateway used for the PPP service being created.

**SMART/RG®**  
forward thinking

**Device Info**  
Advanced Setup  
Layer2 Interface  
ATM Interface  
PTM Interface  
ETH Interface  
WAN Service  
4G LTE Settings  
Ethernet Config  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
UPnP  
DNS Proxy  
Interface Grouping

### Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Selected Default Gateway Interfaces**

ppp0

**Available Routed WAN Interfaces**

[->]  
[-<]

Back Next

9. Click the **arrows** to move your selection from left to right or from right to left.

- Click **Next**. The following page appears where you will select DNS Server settings.

**SMART/RG®**  
forward thinking

**Device Info**  
Advanced Setup  
Layer2 Interface  
ATM Interface  
PTM Interface  
ETH Interface  
WAN Service  
4G LTE Settings  
Ethernet Config  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
UPnP  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
Diagnostics  
Management  
Logout

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.  
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces	Available WAN Interfaces
ppp0	

Use the following Static DNS IP address:

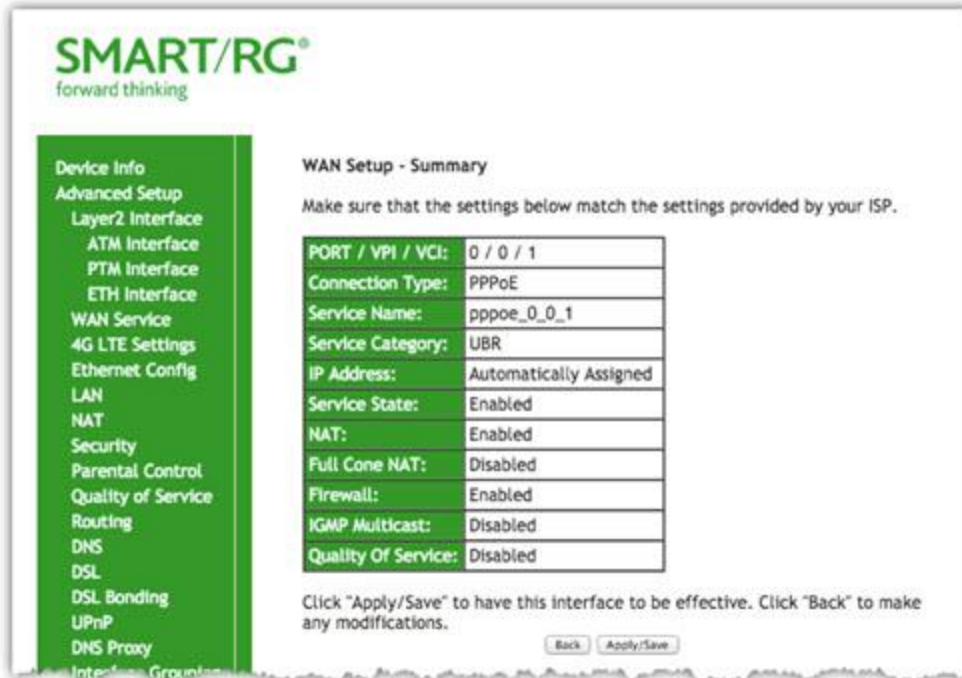
Primary DNS server:

Secondary DNS server:

Back Next

- Select the DNS Server Interface from available WAN interfaces.
- Click the **arrows** to move your selection from left to right or from right to left.
- Alternatively, you can enter static DNS IP addresses in the **Use the following Static DNS IP address** section.

- Click **Next**. The summary page appears indicating that your PPPoE WAN setup is complete.



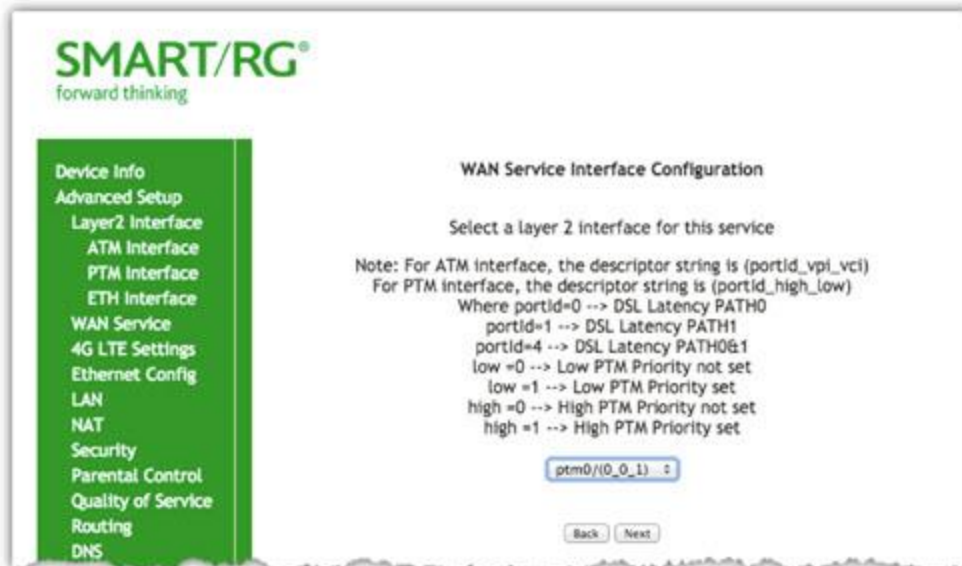
- Review the summary and either click **Apply/Save** to commit your changes or click **Back** to step through the pages in reverse order to make any necessary alterations.

**Note:** For the SR515ac model, additional fields are listed for IGMP Multicast and MLD Multicast settings.

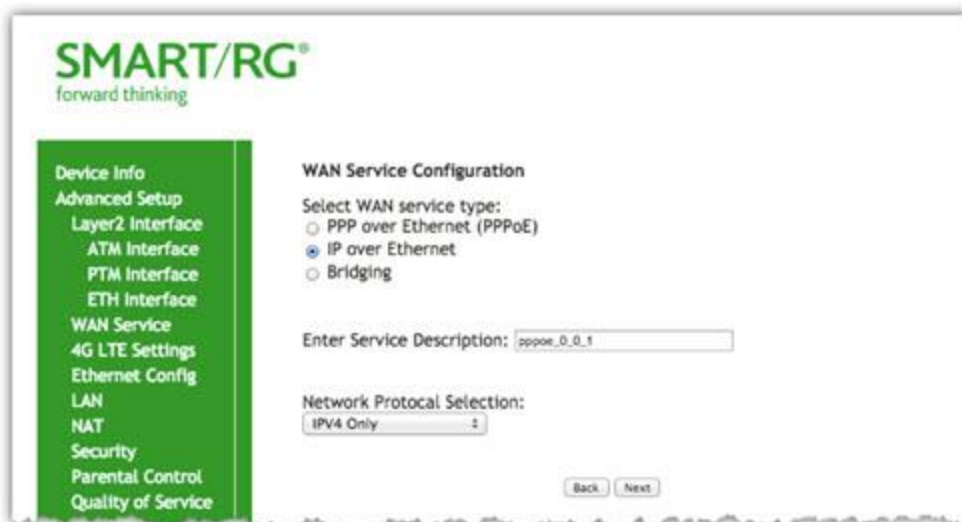
## IP over Ethernet

There are several parts to configuring a IP over Ethernet WAN service. You will progress through several pages to complete the configuration.

1. In the left navigation bar, click **Advanced Setup** > **WAN Service** and then click **Add**. The following page appears.



2. Select the Layer2 interface to use for the WAN service and click **Next**. The following page appears.



3. Select the **IP over Ethernet** WAN service type.
4. Modify the fields as needed.

The fields on this page are explained in the following table.



Field Name	Description
Enter Service Description	<i>(Optional)</i> Enter a name to describe this configuration.
Enter 802.1P Priority	Options are 0 - 7. The default is 0.  For tagged service, enter values in this field and the <b>802.1Q VLAN ID</b> field.  For untagged service, enter -1 (disabled) in this field and the <b>802.1Q VLAN ID</b> field.
Enter 802.1Q VLAN ID	Options are 0 - 4094. The default is -1 (disabled).  For tagged service, enter values in this field and the <b>802.1P Priority</b> field.  For untagged service, enter -1 (disabled) in this field and the <b>802.1P Priority</b> field.
Network Protocol Selection	This data packet scheduling technique allows different scheduling priorities to be applied to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (which has sent larger packets or more packets per second than the others since it became active) will only punish itself and not other sessions. Options are <b>IPv4 Only</b> , <b>IPv4&amp;IPv6</b> (Dual Stack), and <b>IPv6 Only</b> . The default is <b>IPv4 Only</b> .  <b>Note:</b> When selecting <b>IPv4&amp;IPv6</b> or <b>IPv6</b> , the subsequent options presented will change accordingly.

5. Click **Next**. The following page appears.

**SMART/RG®**  
forward thinking

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.  
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.  
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:  (8 hexadecimal digits)

Option 61 IAID:  (hexadecimal digit)

Option 61 DUID:  (hexadecimal digit)

Option 125:  Disable  Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Advanced DMZ

Non DMZ IP Address:  192.168.2.1

Non DMZ Net Mask:  255.255.255.0

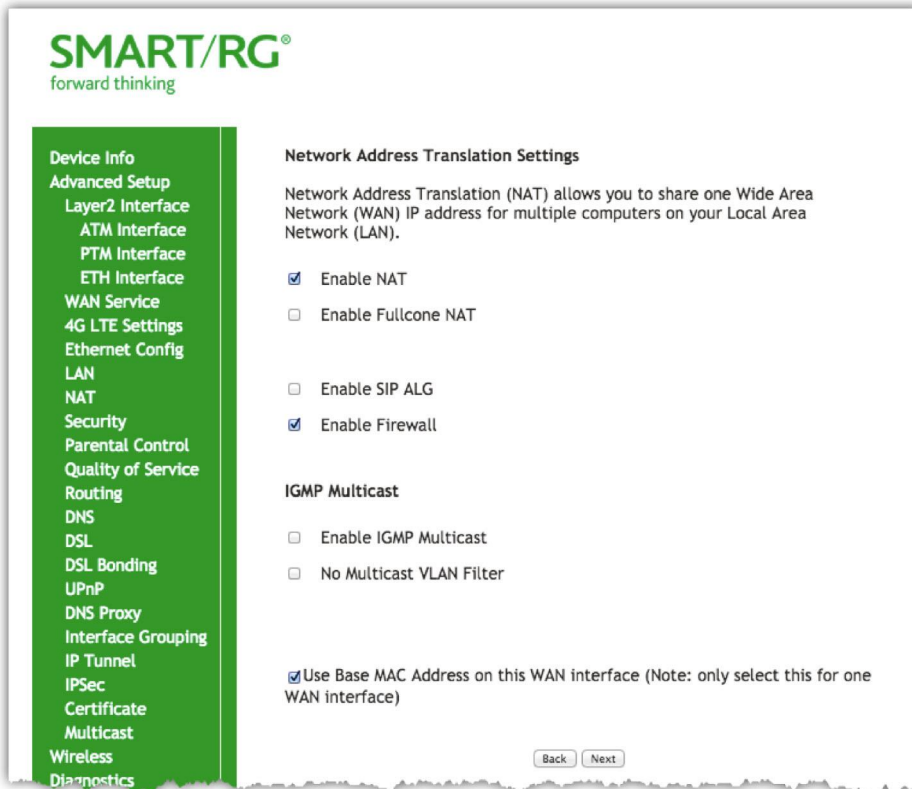
6. Enter the relevant WAN IP Settings.

The fields on this page are explained in the following table.

Field Name	Description
Obtain an IP address automatically	When you wish the ISP to automatically assign the WAN IP to the gateway.
Option 60 Vendor ID	(Optional) Broadcast a specific vendor ID for the DHCP server to accept the device.
Option 61 IAID	(Optional) Interface Association Identifier (IAID). A unique identifier for an IA, chosen by the client.
Option 61 DUID	(Optional) DHCP Unique Identifier (DUID) is used by the client to get an IP address from the DHCP server.
Use the following Static IP address	Use this section to manually declare the static IP information provided by your ISP.
WAN IP Address	If using a static IP address, enter the static WAN IPV4 Address.

Field Name	Description
WAN Subnet Mask	If using a static IP address, enter the static Subnet Mask.
WAN gateway IP Address	If using a static IP address, enter the static Gateway IP address.
Advanced DMZ	<i>(Optional)</i> Select this option to enable Advanced DMZ on the WAN service. For more information, see the knowledgebase on SmartRG Support site.
Non DMZ IP Address	If using the Advanced DMZ feature, you can enter a specific vendor ID that will be broadcast for the DHCP server to accept the device, y. e.g., 192.168.2.1.
Non DMZ Net Mask	If using the Advanced DMZ feature, you can enter a secondary LAN IP address for the gateway. The default is 255.255.255.0.
<b>IPv6 settings</b>	
The following fields appear when either <b>IPv6 Only</b> or <b>IPv4&amp;IPv6 (Dual Stack)</b> network protocols are selected on the WAN Service Configuration page.	
Obtain an IPv6 address automatically	Enables the DHCPv6 Client on this WAN interface. Select this option when you want the ISP to automatically assign the WAN IP to the gateway.
Dhcpv6 Address Assignment (IANA)	Select this option for the CPE to receive WAN IP from ISP.
Dhcpv6 Prefix Delegation (IAPD)	Select this option for the CPE to generate the WAN IP's prefix from the server's REST by MAC address.
Use the following Static IPv6 address	Select this option to manually declare the v6 Static IP information provided by your ISP.
WAN IPv6 Address/Prefix Length	If entering a static IP address, enter the IP address / prefix length. If you do not specify a prefix length, the default of /64 is used.
Specify the Next-Hop IPv6 address	Enter the IP address of the next WAN in the group. This address can be either a local link or a global unicast IPv6 address.

- Click **Next**. The **NAT settings** appears.



- Modify the settings if desired. All settings are optional. Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN). If you do not want to enable NAT (atypical) and wish the user of this gateway to access the Internet normally, you need to add a route on the uplink equipment. Failure to do so will cause access to the Internet to fail.

The fields on this page are explained in the following table.

FIELD NAME	DESCRIPTION
Enable NAT	Enable sharing the WAN interface across multiple devices on the LAN. Also enables the functions in the NAT sub-menu and addition PPPoE NAT features to select.
Enable Fullcone NAT	<i>(Appears when <b>Enable NAT</b> is selected)</i> Enables what is known as one-to-one NAT.
Enable SIP ALG	<i>(Appears when <b>Enable NAT</b> is selected)</i> Enables Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications.
Enable Firewall	Enables functions in the <b>Security</b> sub-menu

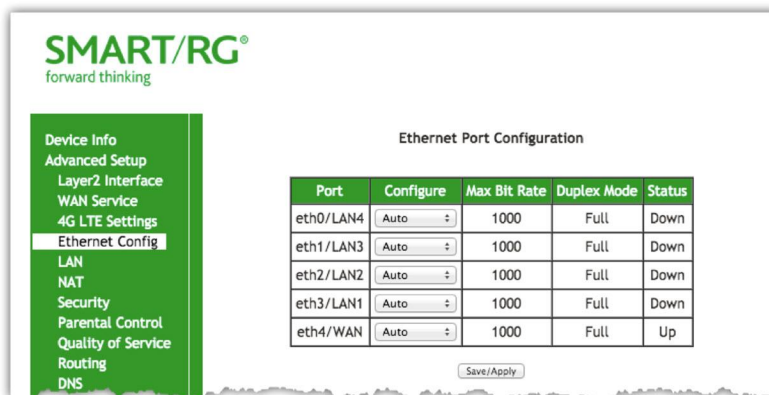
FIELD NAME	DESCRIPTION
Enable IGMP Multicast	<i>(Not available for SR515ac models)</i> Enables Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable IGMP Multicast Proxy	<i>(Available for SR515ac models only)</i> Click to enable Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable IGMP Multicast Source	<i>(Available for SR515ac models only)</i> Select to enable this service to act as an IGMP multicast source.
No Multicast VLAN Filter	<i>(Not available for SR515ac models)</i> Disables multicast filtering between WAN and LAN (VlanMux) network.
Use Base MAC Address on this WAN interface	Use SmartRG Devices Base (Primary) MAC address. When unchecked, a unique MAC per service is assigned.
Enable MAC Clone	<i>(Appears when <b>Use Base MAC Address</b> is deselected)</i> Enter the MAC address to be used as the clone address.

- For the remaining WAN Service configuration pages, use the instructions provided in the [default gateway step](#) in the *PPP over Ethernet* section.

## Ethernet Config

On the Ethernet Port Configuration page, you can set the speed and duplex mode for each of the Ethernet ports.

- In the left navigation bar, click **Advanced Setup > Ethernet Config**. The following page appears.



- In the **Configure** column, select an option (**Auto**, **100 Full**, **100 Half**, **10 Full** or **10 Half**) for each of the four Ethernet ports on your gateway.

These options represent 100 megabits or 10 megabits using half or full duplex transmission protocols. When you have a specific device with a known limited transmission speed capability, select one of the latter four options. If you select **Auto**, your gateway will automatically select an appropriate setting based on Ethernet auto negotiation with the NIC of the LAN host.

**Note:** Always select **Auto** for 1000 BaseT connections.

The following are the variations for the 500 series of gateways:

- For the SR510 and SR552n models, the fourth port is shown on this page as eth3/LAN1 and the ports are listed in reverse order. The eth4/WAN interface is also present on these models.
- SR505n v2.5.0.x and later has an additional option of **1000 Full** for the LAN1/WAN port.
- SR552n v2.5.0.6 and later has an additional option of **1000 Full** for all Ethernet interfaces.

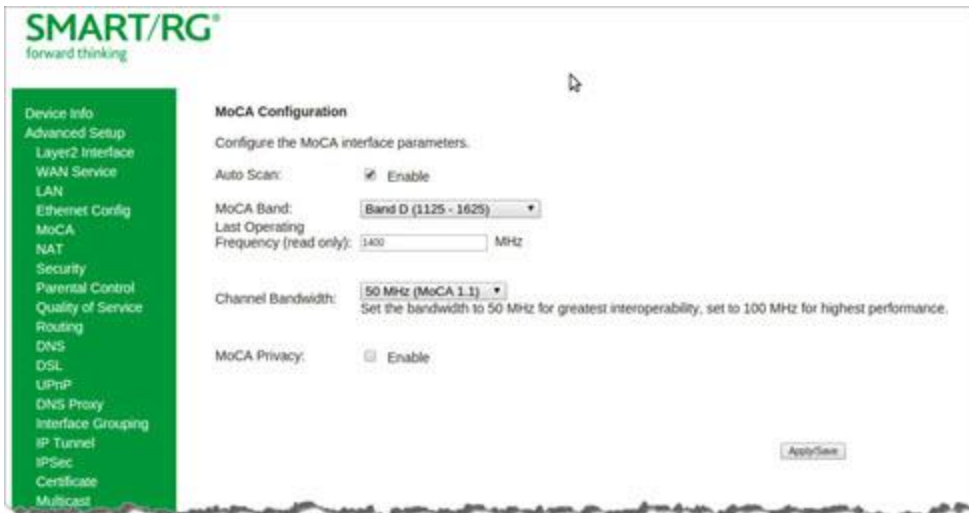
3. Click **Apply/Save** to commit your changes.

## MoCA

On this page, you can configure MoCA settings. The MoCA (Multimedia over Coax) protocol enables distribution of content over existing in-home coaxial TV cabling at the same speed delivered by Ethernet networks.

**Note:** This feature is available only on the SR512nm model.

1. In the left navigation bar, click **Advanced Setup > MoCA**. The following page appears.



2. Update or complete the necessary fields.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Auto Scan	Allows your gateway to scan automatically for the best connection to your provider. This option is enabled by default.
MoCA Band	Select the operating band for this gateway. The default is <b>Band D (1125-1625)</b> .
Last Operating Frequency	Displays the most recent operating frequency in Megahertz.
Channel Bandwidth	Select the bandwidth for your connection. Select <b>50 MHz</b> for better interoperability or select <b>100 MHz</b> for better performance.
MoCA Privacy	To activate privacy mode, click the <b>Enable</b> checkbox.
Privacy Password	<i>(Appears when <b>MoCA Privacy</b> is set to <b>Enabled</b>)</i> Enter the MoCA password for this gateway.

## LAN

On the Local Area Network (LAN) Setup page, you can configure the router's local IP addresses, subnet mask, DHCP behavior and other related LAN side settings for your gateway.

1. In the left navigation bar, click **Advanced Setup > LAN**. The following page appears.

2. Customize the fields as desired.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.



Field Name	Description
Groupname	<i>(Available on SR515ac models only)</i> Select an interface group from the list of available groups (defined on the Interface Grouping page).
IP Address	<i>(Available on SR515ac models only)</i> Enter the LAN IP address by which LAN devices will connect to this gateway.
Subnet Mask	<i>(Available on SR515ac models only)</i> Enter the Subnet mask to be used by LAN devices connecting to this gateway.
Enable IGMP Snooping	<i>(Available on SR515ac models only)</i> Enables your gateway to listen to IGMP network traffic between hosts and routers. By listening to these conversations, the gateway maintains a map of which links need which IP multicast streams.
Standard Mode	Allows multicast traffic will flood to all bridge ports when there is no client subscribed to any multicast group.
Blocking Mode	Blocks multicast data traffic, preventing it from flooding to all bridge ports when no client subscriptions to a multicast group are present.
Enable IGMP LAN to LAN Multicast	<i>(Available on SR515ac models only)</i> Allows multicast traffic between LANs. This option is enabled by default.
Enable LAN Side Firewall	Enables the restriction of traffic between LAN hosts.
Disable DHCP Server	Prevents the DHCP functionality of your gateway from automatically assigning LAN IP addresses to host devices as they connect with the gateway.
Enable / Disable DHCP Server	Allows the DHCP functionality of your gateway to automatically assign LAN IP addresses to host devices as they connect with the gateway. Fill in the next three fields to configure this action.
Start IP Address	<i>(Becomes editable when <b>Enable DHCP Server</b> is selected)</i> Enter the beginning of the class C, IP address range to be assigned by the DHCP server.
End IP Address	<i>(Becomes editable when <b>Enable DHCP Server</b> is selected)</i> Enter the end of the class C, IP address range to be assigned by the DHCP server.
Leased Time (hour)	<i>(Becomes editable when <b>Enable DHCP Server</b> is selected)</i> Enter the number of hours for which an IP address will be leased.
Static IP Lease List	Specify a literal, static, <b>IP address</b> to be associated with a <b>specific MAC Address</b> of one of your LAN host devices. Click <b>Add Entries</b> . Enter the MAC address and IP address and click <b>Apply/Save</b> . Repeat this step to create any additional entries that you need.
Automatically create static IP leases from the following OUIs	For LAN hosts, IP addresses can be assigned manually or by using DHCP. Click <b>Add OUI</b> . Enter the OUI and click <b>Apply/Save</b> . Repeat this setp to create any additional entries that you need.

Field Name	Description
Option 66	For some devices that also require access to a TFTP server (device configuration name files are in .cnf file format), which enables the device to communicate with other infrastructure, select this option to specify the name of the TFTP server. Option 66 is an IEEE standard.
Option 150	A Cisco proprietary methodology for pointing to one or two TFTP servers.
Enable DHCP Server Relay	<i>(Not available on SR515ac models )</i> The DHCP relay agent operates as the interface between DHCP clients and the server. It listens for client requests and adds vital configuration data, such as the client's link information, which is needed by the server to allocate the address for the client. When the DHCP server responds, the DHCP relay agent forwards the reply back to the DHCP client.
DHCP Server IP Address	<i>(Not available on SR515ac models )</i> Set the IP address to which LAN clients must connect to receive DHCP services.
Configure the second IP address and subnet mask for LAN interface	When you select this option, the <b>IP Address</b> and <b>Subnet Mask</b> fields appear where you can enter a second IP address and Subnet mask to support a second, simultaneous LAN, i.e., the primary LAN might be defined as 192.168.0.1 and this secondary LAN defined as 192.168.2.1.

## NAT

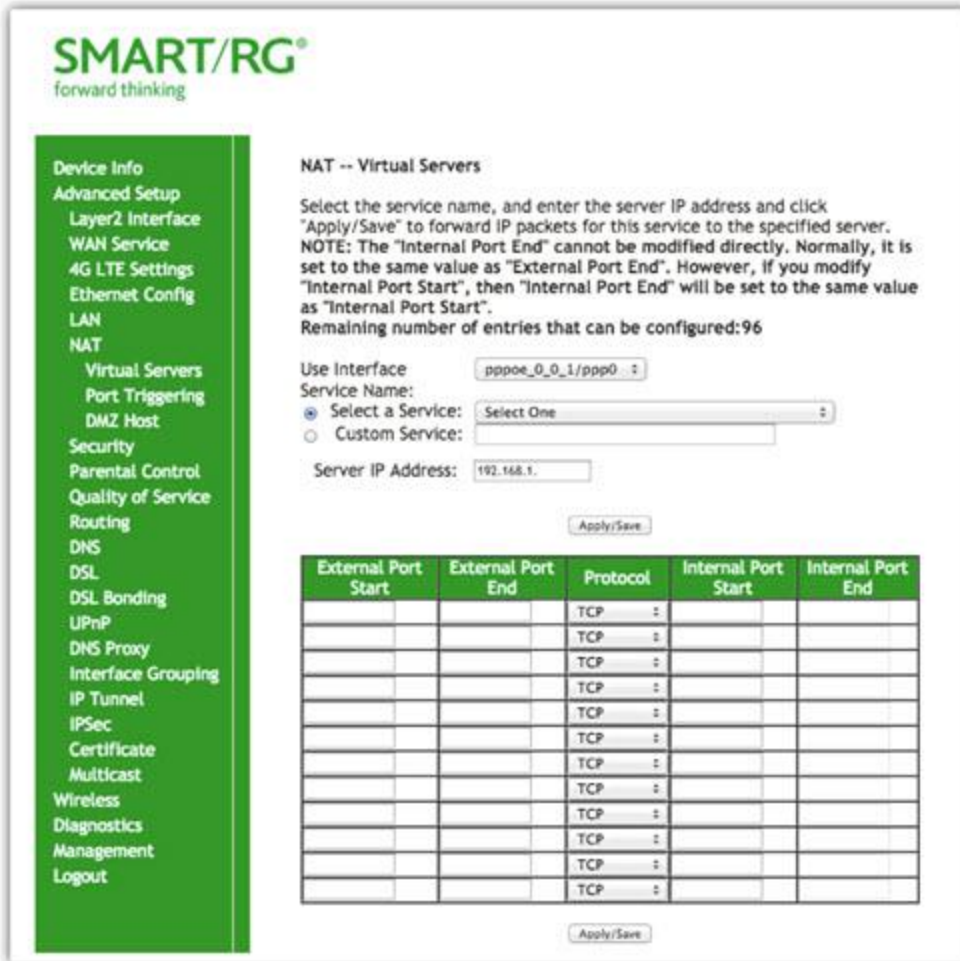
In the NAT section you can configure the settings for Network Address Translation including setting up virtual servers, port triggering and DMZ host. There is seldom need to customize these settings as the default settings manage the related features sufficiently for most environments.

### Virtual Servers

Virtual Servers (more commonly known as Port Forwards) is a technique used to facilitate communications by external hosts with services provided within a private local area network.

On this page, you can configure the virtual server settings for your gateway.

1. In the left navigation bar, select **Advanced Setup > NAT**. The following page appears.



2. Customize the fields to create your port forwarding entry.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Use Interface	Select the WAN interface to which this NAT rule will apply.
Select a Service	Select from a list of application that typically require port forwards configured. The port ranges and protocol fields will be pre-populated.
Custom Service	If your application does not appear in the <b>Select a Service</b> list, you can enter a unique name

Field Name	Description
	for the application in this field.
Server IP Address	Enter the IP address of the LAN client where the service is hosted.
External Port Start	Enter the first external port for this server.
External Port End	Enter the last external port for this server.
Protocol	Select the protocol to be used with this range of ports. Options are: <b>TCP, UDP, or TCP/UDP.</b>
Internal Port Start	Enter the first internal port for this server.
Internal Port End	Enter the last internal port for this server.

## Port Triggering

Some applications require that specific ports in the gateway's firewall be opened for access by remote parties. The Port Trigger feature dynamically opens up the open ports in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the triggering ports. The gateway allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the Open Ports.

1. In the left navigation bar, click **Advanced Setup > NAT > Port Triggering** and then click **Add**. The following page appears.



2. Customize the fields as needed for the firewall pinholes you wish to establish. A maximum 96 entries can be configured.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

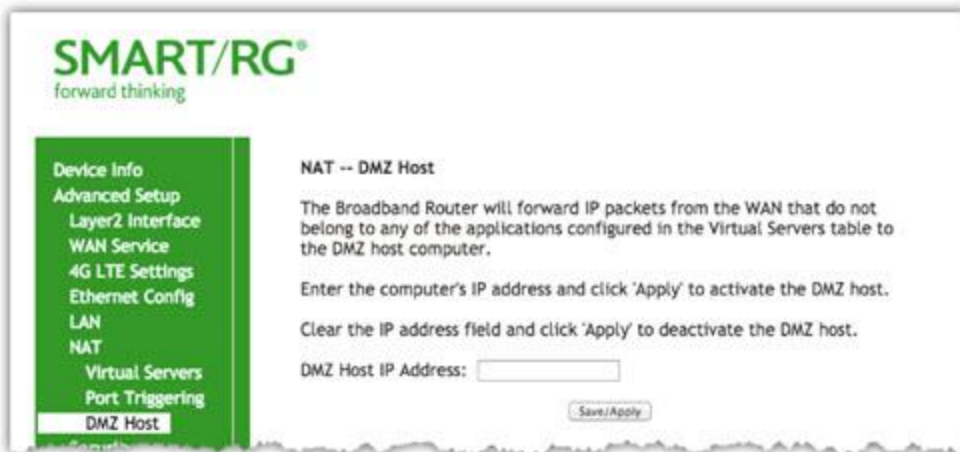
Field Name	Description
Use Interface	Select the interface for which the port triggering rule will apply.
Select an Application	Select the application which requires a port trigger entry.
Custom Application	If the application you want does not appear in the selection list, enter a unique name for the application for which you are creating a port trigger entry. This is a free-form text field.
Trigger Port Start	Enter the starting number of the range of available outgoing trigger ports. Options are: 1 - 65535.
Trigger Port End	Enter the end number of the range of available outgoing trigger ports. Options are: 1

Field Name	Description
	- 65535.
Trigger Protocol	Select the protocol required by the application that will be using the ports in the specified range. Options are: TCP, UDP, and TCP/UDP.
Open Port Start	Enter the starting number of the range of available incoming ports. Options are: 1 - 65535.
Open Port End	Enter the end number of the range of available incoming ports. Options are: 1 - 65535.
Open Protocol	Select the protocol for the open port. Options are: TCP, UDP, and TCP/UDP.

## DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer. If you want to route all internet traffic to a specific LAN device with no filtering or security, add the IP address of that device to this page.

1. In the left navigation bar, click **Advanced Setup > NAT > DMZ Host**. The following page appears.



2. Enter the **DMZ Host IP Address**.
3. Click **Apply/Save** to commit the new or changed address.

## Security

In this section, you can configure filtering for IP and MAC.

### IP Filtering - Incoming

On this page, you can add an incoming filter when refusal of data from the WAN to the LAN is desired.

**Note:** This option is not available in the SR515ac model.

1. In the left navigation bar, click **Advanced Setup** > **Security** > **IP Filtering** > **Incoming** and then click **Add**. The following page appears.

2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Filter Name	A free-form text field. Enter a descriptive name for this filter.



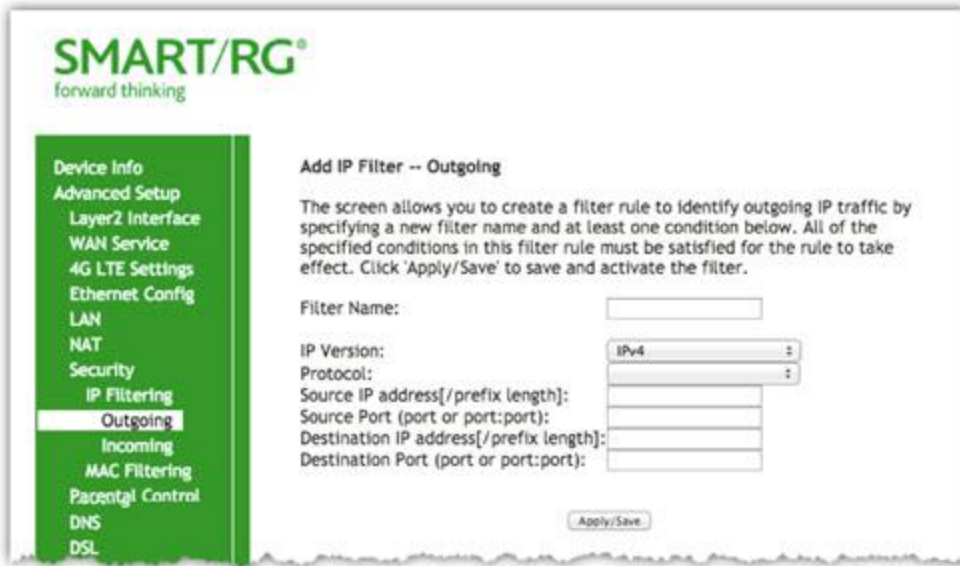
Field Name	Description
IP Version	Select the IP version for this filter. Options are <b>IPv4</b> and <b>IPv6</b> . The default is <b>IPv4</b> .
Protocol	Select the protocol to be associated with this incoming filter. Options are: <b>TCP/UDP, TCP, UDP, or ICMP</b> .
Source IP address [/prefix length]	Enter the source IP address for rule. For IPv6, enter the prefix as well.
Source Port (port or port:-port)	Enter source port number or range (xxxxx:yyyyy).
Destination IP address [/prefix length]	Enter the destination IP address for rule. For IPv6, enter the prefix as well.
Destination Port (port or port:port)	Enter destination port number or range (xxxxx:yyyyy).
Select All	Click to apply this rule to all WAN interfaces or only certain types. Options are <b>Select All</b> or the types defined for your network.
First WAN interface Last WAN interface	Click the applicable options to apply this rule on specific WAN interfaces. The WAN interfaces display that you configured for your network in <a href="#">Routing</a> and that have a firewall enabled.
First LAN interface Second LAN interface	Click the applicable options to apply this rule on specific LAN interfaces.
Bridged Interface	Click the applicable options to apply this rule on specific bridged interfaces.

## IP Filtering - Outgoing

On this page, you can add an outgoing filter when refusal of data from the LAN to the WAN is desired.

1. In the left navigation bar, click **Advanced Setup** > **Security** > **IP Filtering** > **Outgoing** and then click **Add**. The following page appears.

**Note:** For SR515ac models, click **Advanced Setup** > **Security** to access this page.



2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit the completed entry.

The fields on this page are explained in the following table.

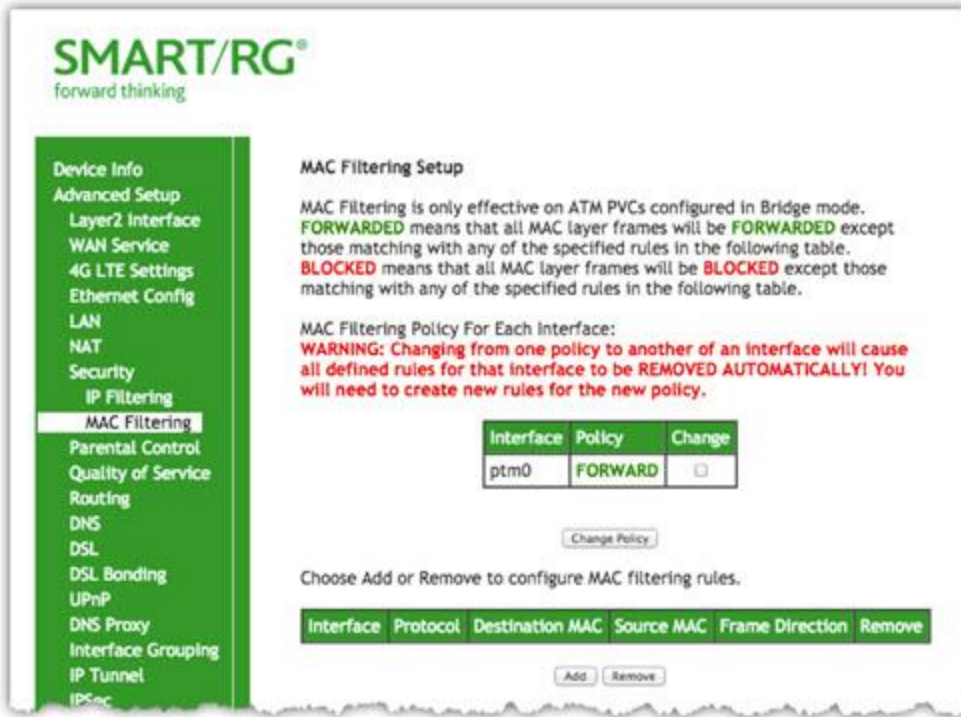
Field Name	Description
Filter Name	Enter a descriptive name for this filter. This is a free-form text field.
IP Version	For the filter to be configured and effective for IPV6 , the gateway must be installed on a network that is either a pure IPV6 network (with that protocol enabled) or is both IPV4 and IPV6 dual protocol enabled/configured. Options are <b>IPv4</b> and <b>IPv6</b> . The default is <b>IPv4</b> .  If you select <b>IPv6</b> , both the Source and Destination IP address must be specified in IPV6 format. The following is an IPV6-compliant, hexadecimal address: 2001:0DB8:AC10:FE01:0000:0000:0000:0001.
Protocol	Select the protocol profile for the filter you are defining. TCP/UDP is most commonly used. The options are <b>TCP/UDP</b> , <b>TCP</b> , <b>UDP</b> , and <b>ICMP</b> ].
Source IP address [/prefix length]	Enter the source IP address of a LAN side host for which you wish to filter/block outgoing traffic for the specified protocol(s).  <b>Note:</b> The address specified here can be a particular address or a block of IP addresses on a given network subnet. This is done by appending the associated routing "/prefix" length decimal value (preceded with the slash) to the addresses. A valid decimal routing prefix is required for defining the subnet mask per CIDR notation.

Field Name	Description
Source Port (port or port:port)	Set the outgoing host port (or range of ports) for the above host (or range of hosts defined by optional routing "/prefix" subnet mask) to define the ports profile for which egress traffic will be filtered from reaching the specified destination(s).
Destination IP address	<p>Enter the destination IP address of a LAN side host for which you wish to filter/block outgoing traffic for the specified protocol(s).</p> <p><b>Note:</b> The address specified here can be a particular address or a block of IP address on a given network subnet. This is done through appending the address with the routing " /prefix " length decimal value (preceded with the slash) associated. A valid decimal routing prefix is required for defining the subnet mask per CIDR notation.</p>
Destination Port (port or port:port)	Set the destination host port (or range of ports) for the above host (or range of hosts) to define the destination port profile for which the filtered host egress traffic will be filtered from reaching the otherwise intended destination(s), e.g., to block the traffic to those ports on, say, a computer external to the local network.

## MAC Filtering

Your SmartRG gateway can block or forward packets based on the originating device. This MAC filtering feature is available only in Bridge mode. For other modes, similar functionality is available via IP Filtering. On this page, you can manage MAC filtering for your gateway.

1. In the left navigation bar, click **Advanced Setup > Security > MAC Filtering**. The following page appears.



2. To modify policy settings:
  - a. Review the information on the page.
  - b. Once you understand the consequences of changing the policy, click the **Change** checkbox, and then click **Change Policy**. The policy is switched to **FORWARD** or **BLOCKED**.
3. To add a rule, follow the instructions in "[MAC Filtering](#)".
4. To remove a rule, click the **Remove** checkbox next to the rule and click the **Remove** button.
5. When your changes are completed, click **Apply/Save** to commit your changes.

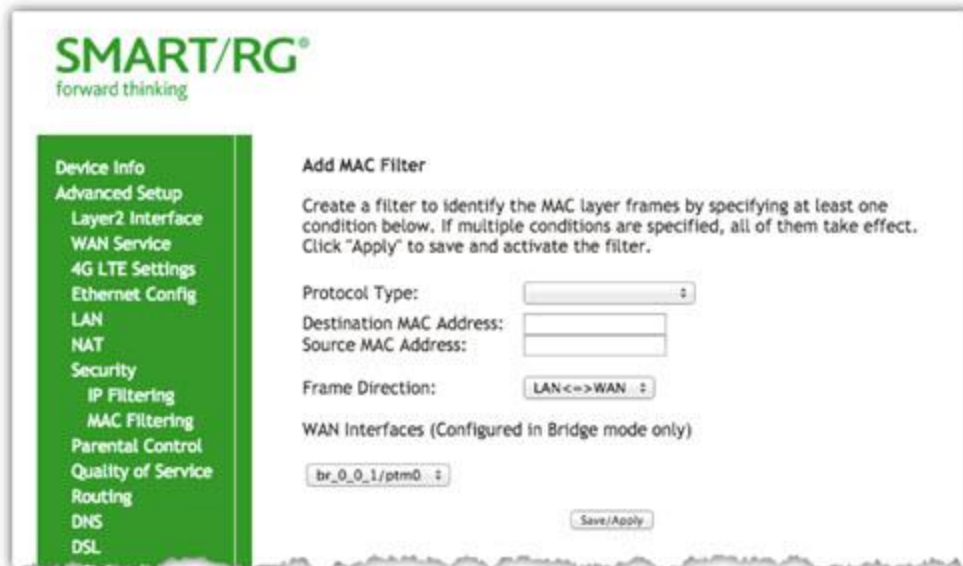
The fields on this page are explained in the following table.

Field Name	Description
Interface	The interface associated with an established policy rule.
Policy	The current/active policy type that is in place. Options are <b>FORWARD</b> and <b>BLOCKED</b> .

## Add a MAC Filtering Rule

You cannot edit rules but you can add new ones and then remove the obsolete ones.

1. On the MAC Filtering page, click **Add**. The following page appears.



2. Fill in the fields, using the information provided in the following table..
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Protocol Type	Select the protocol associated with the device at the destination MAC address. Options are <b>PPPoE, IPv4/IPv6, AppleTalk, IPX, NetBEUI, and IGMP</b> .
Destination MAC Address	Enter the MAC address of the hardware you wish to associate with this filter.
Source MAC Address	Enter the MAC address of the device that is originating requests intended for the device associated with the Destination MAC address.
Frame Direction	Select the incoming/outgoing packet interface.
WAN Interfaces	Applies the filter to the selected interface(s).

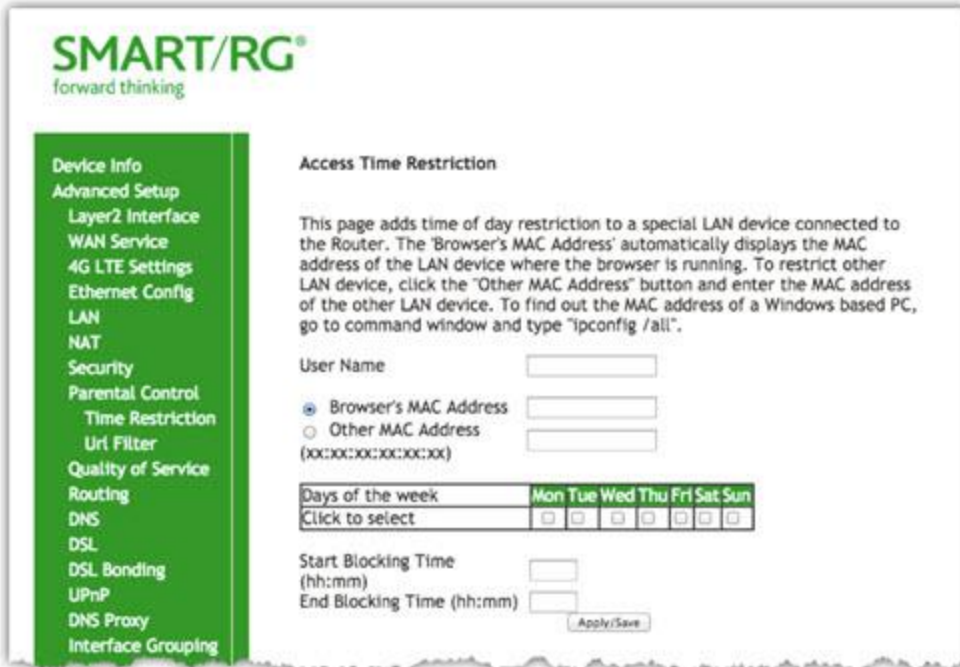
## Parental Control

In this section, you can configure the Parental Control features of your SmartRG gateway to restrict Internet access to certain hours and to certain URLs.

## Time Restriction

On this page, you can restrict Internet access to particular days and specific times for each device that accesses your gateway.

1. In the left navigation bar, click [Advanced Setup](#) > [Parental Control](#) > [Time Restriction](#) and then click [Add](#). The following page appears.



2. Fill in the fields using the information in the table below.
3. Click [Apply/Save](#).

The fields on this page are explained in the following table.

Field Name	Description
User Name	Enter a descriptive name for this restriction. This is a free-form text field.
Browser's MAC Address	The MAC address of the connected device. This option is selected by default.
Other MAC Address	Select this option to restrict access to another device. You can view a list of the connected devices and MAC addresses on the <a href="#">Device Info</a> > <a href="#">ARP</a> page.
Days of the week	Select the days ( <b>Mon - Sun</b> ) for which the restrictions apply.

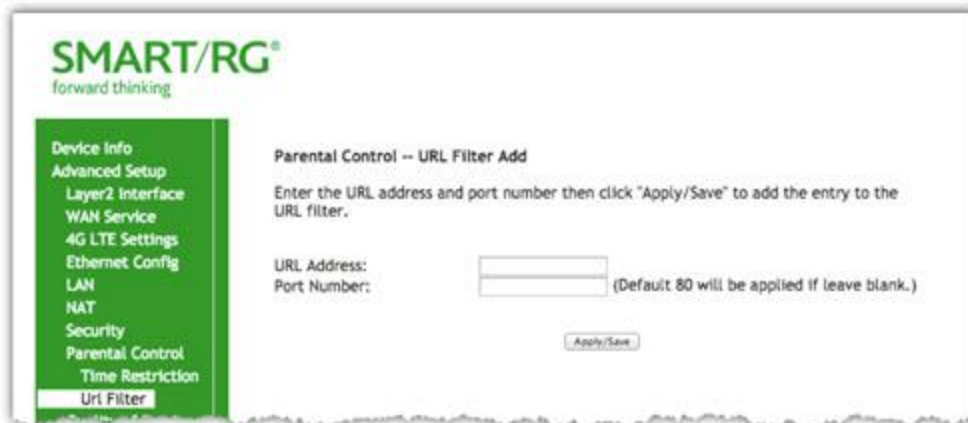
Field Name	Description
Start Time Blocking / End Time Blocking	Enter the range of time that the devices listed above are restricted from access to the Internet. Use 24-hour clock notation ( <b>00:00 - 24:00</b> ).

## URL Filter

The other side of the Parental Controls coin is URL filtering. On this page, you can exclude and include URLs as desired. Each list can include up to 100 addresses.

**Note:** Only one **Exclude** list and one **Include** list are supported for each gateway. Unique lists are not supported for connecting devices.

1. In the left navigation bar, click **Advanced Setup > Parental Control > Url Filter**.
2. To block a URL:
  - a. Select **Exclude List**.
  - b. Click **Add**. The following page appears.



- c. Click **Apply/Save** to save your settings. You are returned to the Url Filter page.
3. To create a list of URLs to allow, select **Include** and repeat the above steps.

The fields on this page are explained in the following table.

Field Name	Description
URL Address	Enter the URL address to be included in the list.
Port Number	(Optional) Enter the port number associated with the URL. The default is <b>80</b> .

## Quality Of Service

Quality of Service (QoS) enables prioritization of Internet content to help ensure the best possible performance. This is particularly useful for streaming video and audio content with minimized potential for drop-outs. QoS becomes significant when the sum of all traffic (audio, vid"[QoS Classification](#)", data) exceeds the capacity of the line.

In this section, you can configure QoS settings including traffic queues, classifications (rules) and port shaping.

## QoS Config

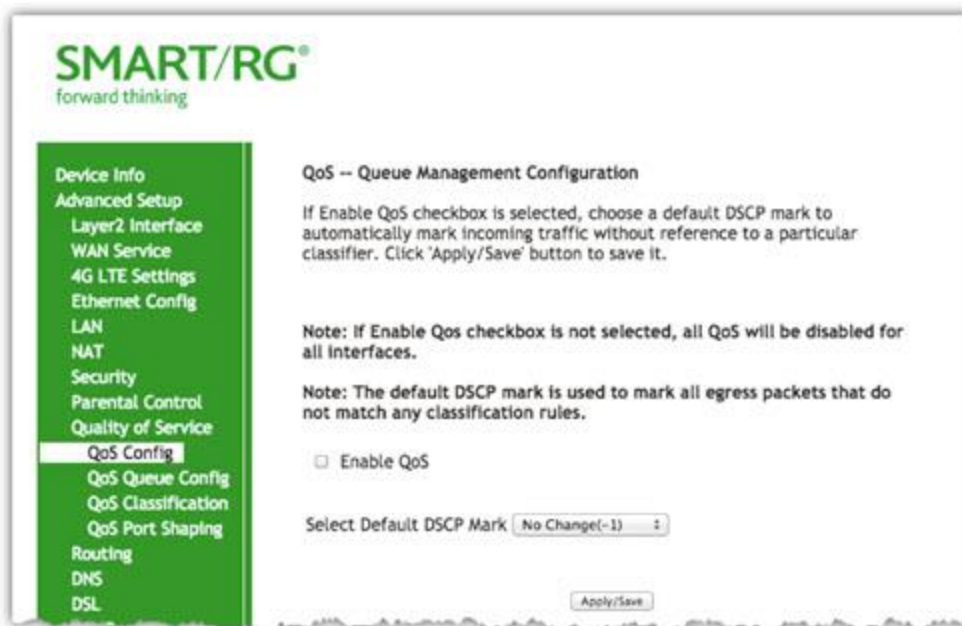
On this page, you can enable QoS and set the DSCP Mark classification.

The maximum number of queues that can be configured vary by mode, as shown below.

Mode	Maximum # of queues
ATM	16
Ethernet	4 per interface
PTM	8

**Note:** Queues for Wireless (e.g., WMM Voice Priority for wlan0 interface) are shown only when wireless is enabled. If the **WMM Advertise** function on the Wireless Basic Setup page is disabled, assigning classifications to wireless traffic has no effect.

1. In the left navigation bar, click **Advanced Setup** > **Quality Of Service** > **QoS Config**. The following page appears.



2. Click **Enable QoS**.  
The **QoS Queue Management Configuration** field appears where you can select the default Differentiated Services Code Point (DSCP) Mark classification value to be used. For a list of supported values, see ["Supported DSCP Values"](#).  
**Note:** If this option was already enabled and you clear the checkbox, QoS will be disabled for ALL interfaces.
3. Click **Apply/Save** to save your settings.



## Supported DSCP Values

The DSCP marking QoS Queue Management Configuration marking on ingress packets is based on the selection you make in the **Select Default DSCP Mark** field. The selected default marking is applied automatically to all incoming packets without reference to a particular classification.

**Note:** A default DSCP mark value of **Default(000000)** will mark all egress packets that do NOT match any classification.

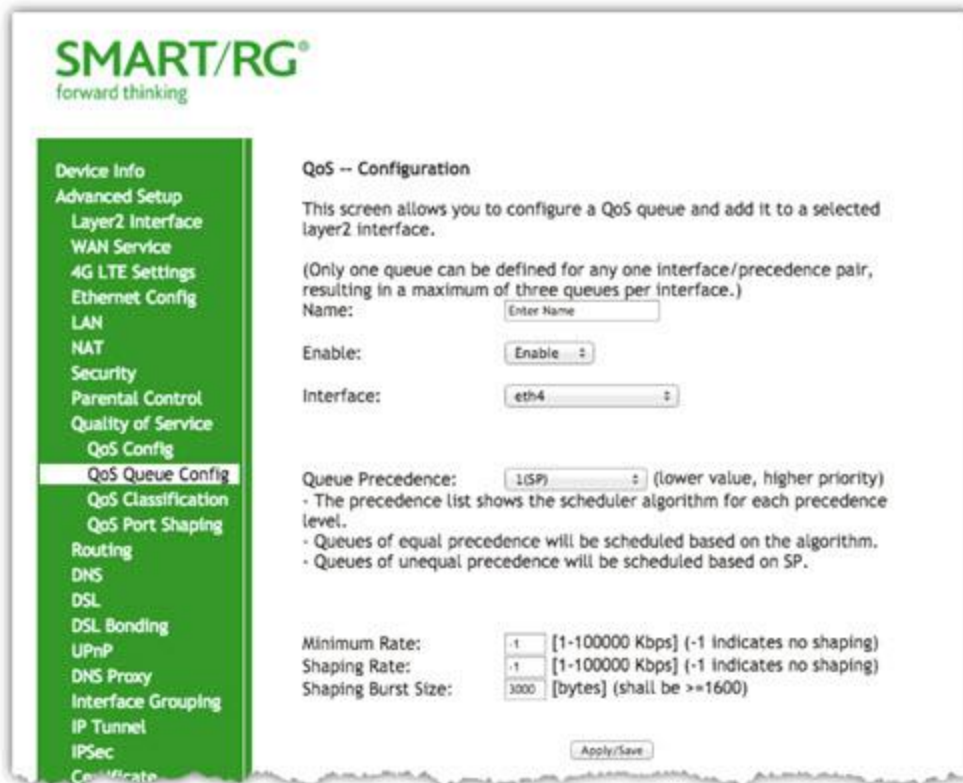
The following values are supported. For more information about commonly used DSCP values, refer to RFC 2475.

No Change(-1)	CS1(001000)	AF32(011100)	CS4 (100000)
Auto Marking(-2)	AF23(010110)	AF31(011010)	EF (101110)
Default(000000)	AF22(010100)	CS3(011000)	CS5 (101000)
AF13(001110)	AF21(010010)	AF43(100110)	CS6 (110000)
AF12(001100)	CS2(010000)	AF42(100100)	
AF11(001010)	AF33(011110)	AF41(100010)	

## QoS Queue Config

On this page you can configure a queue and add it to a selected Layer2 interface.

1. In the left navigation bar, click **Advanced Setup > Quality Of Service > QoS Queue Config** and then click **Add**. The following page appears.



2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to save your settings.

The fields on this page are explained in the following table.

Field Name	Description
Name	Enter a descriptive name for this configuration. This is a free-form text field.
Enable	Select to enable or disable a given QoS queue configured on the selected interface.  <b>Note:</b> Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.
Interface	Select the Layer 2 interface to be associated with the defined QoS queue, e.g., eth0 or eth4.
Queue Precedence	<i>(Appears when you select an interface)</i> Select the priority value to be associated with QoS queue defined. Options include levels for SP and SP WRR WFQ.

Field Name	Description
	<b>Note:</b> Lower value = higher priority.
Scheduler Algorithm	<p>(Appears when you select SP WRR WFQ in the <b>Queue Precedence</b> field)</p> <p>Select an algorithm for data priority in queues. Options are:</p> <p><b>Strict Priority:</b> Allows shaping of rate and burst size for packets in queue.</p> <p><b>Weighted Round Robin:</b> Applies a fair round robin scheme weighting that is effective for networks with fixed packet sizes, e.g., ATM networks.</p> <p><b>Weighted Fair Queuing:</b> Applies a fair queuing weighting scheme via allowing different sessions to have different service shares for improved data packets flow in networks with variable packet size, e.g., PTM/IP networks.</p>
<p>The following options appear only when the <b>Queue Precedence</b> field is set to SP WRR WFQ and the <b>Scheduler Algorithm</b> field is set to <b>Strict Priority</b>. These options do not appear in the SR3xxn models.</p>	
Minimum Rate	<p>Enter the minimum shaping rate for packets in QoS queues. Options are 1 - 100000 Kbps.</p> <p>To specify no minimum shaping, enter -1 .</p>
Shaping Rate	<p>Enter the shaping rate for packets in QoS queues. Options are 1 - 100000 Kbps.</p> <p>To specify no minimum shaping, enter -1 .</p>
Shaping Burst Size	<p>Enter the shaping burst size to be applied to packets in the defined queue. Options are 1600 bytes or greater.</p>
Minimum Rate	<p>(Appears when you select either <b>Weighted</b> algorithm option in the <b>Scheduler Algorithm</b> field) Enter the minimum shaping rate defined for packets in QoS queues. Options are: 1 - 100000 kbps.</p> <p>To specify no minimum shaping, enter -1 .</p>
Shaping Rate	<p>(Appears when you select either <b>Weighted</b> algorithm option in the <b>Scheduler Algorithm</b> field) Enter the shaping rate for packets in QoS queues. Options are: 1 - 100000 Kbps.</p> <p>To specify no minimum shaping, enter -1 .</p>
Queue Weight	<p>(Appears for the SR515ac model when you select either of the <b>Weighted</b> algorithm options in the <b>Scheduler Algorithm</b> field) Enter a weight for prioritizing this queue. Options are 1 - 63.</p>

## WLAN Queue

**Note:** This options is available for the SR515ac gateway only.

On this page, you can view the wireless queues and classifications.

**Note:** The WMM Advertise option must be enabled before these classifications will function. This option is enabled by default. If you have disabled it, go to the Wireless > Basic page and clear the **Disable WMM Advertise** checkbox.

In the left navigation bar, click **Advanced Setup > Quality Of Service > QoS Queue Config > Wlan Queue**. The following page appears.

**SMART/RG**  
forward thinking

SR515ac

QoS -- Wlan Queue Setup

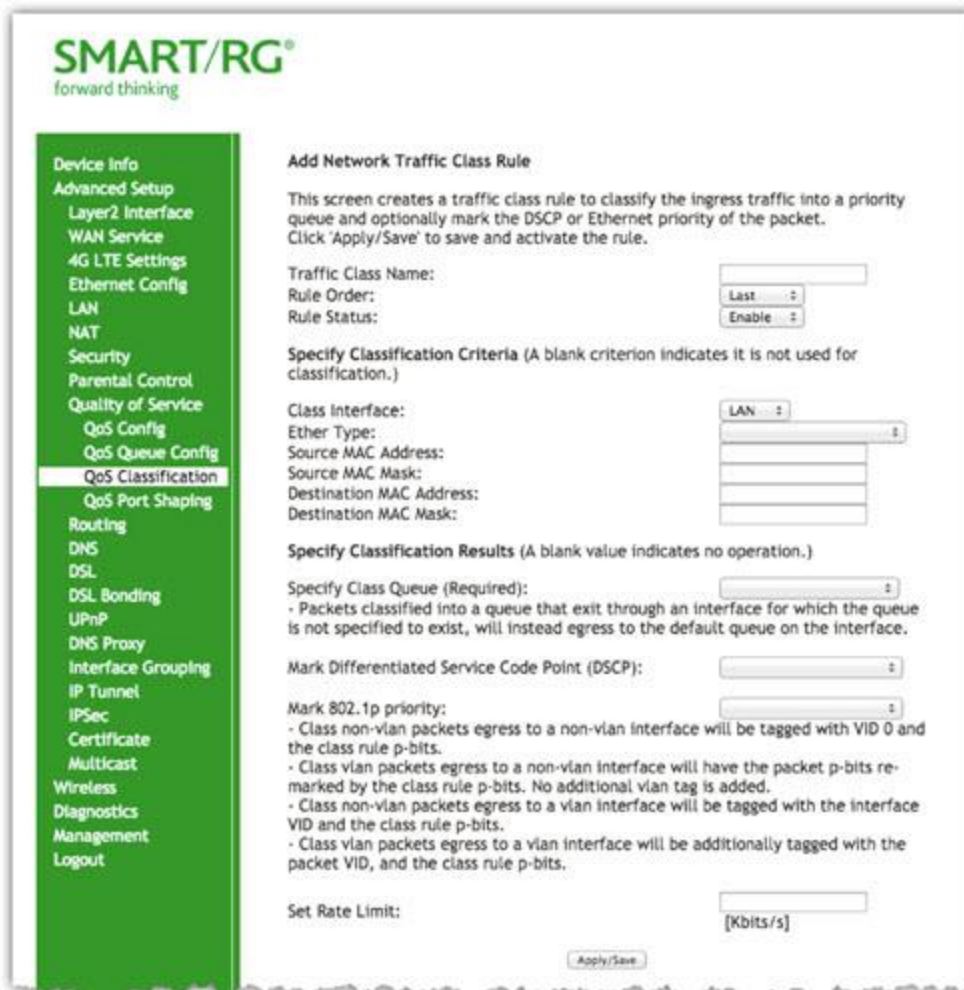
**Usage Note:**  
Wireless queues and classifications have no effect if WMM Advertise is disabled. The WMM Advertise function is located on the Wireless Basic Setup page.

Name	Key	Interface	Qid	Prec / Ag / Wght	Enable
WMM Voice Priority	1	wl0	8	1/SP	Enabled
WMM Voice Priority	2	wl0	7	2/SP	Enabled
WMM Video Priority	3	wl0	6	3/SP	Enabled
WMM Video Priority	4	wl0	5	4/SP	Enabled
WMM Best Effort	5	wl0	4	5/SP	Enabled
WMM Background	6	wl0	3	6/SP	Enabled
WMM Background	7	wl0	2	7/SP	Enabled
WMM Best Effort	8	wl0	1	8/SP	Enabled
WMM Voice Priority	33	wl1	8	1/SP	Enabled
WMM Voice Priority	34	wl1	7	2/SP	Enabled
WMM Video Priority	35	wl1	6	3/SP	Enabled
WMM Video Priority	36	wl1	5	4/SP	Enabled
WMM Best Effort	37	wl1	4	5/SP	Enabled
WMM Background	38	wl1	3	6/SP	Enabled
WMM Background	39	wl1	2	7/SP	Enabled
WMM Best Effort	40	wl1	1	8/SP	Enabled

## QoS Classification

On this page, you can create traffic class rules for classifying the ingress traffic into a priority queue. You can also mark the DSCP or Ethernet priority of the packet.

1. In the left navigation bar, click **Advanced Setup > Quality Of Service > QoS Classification** and then click **Add**. The following page appears. A maximum of 32 entries can be configured.



2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Traffic Class Name	Enter a descriptive name for this rule. This is a free-form text field.
Rule Order	Select whether this rule is processed next or last in the list of classification rules. Options are: <ul style="list-style-type: none"> <li>• <b>Last:</b> Sets this rule as the very last classification rule to be processed.</li> <li>• <b>Null:</b> Sets this rule as the next classification rule to be processed.</li> </ul>

Field Name	Description
Rule Status	Select whether this rule is active or inactive. Options are: <b>Enable</b> and <b>Disable</b> .
<b>Specify Classification Criteria</b> section	
Class Interface	<i>(Not applicable for SR515ac models )</i> Select an interface. Options are: <b>local</b> , <b>eth0 - eth4</b> , and <b>wl0</b> .
Ingress Interface	<i>(Available for SR515ac models only)</i> Select an interface. Options are <b>LAN</b> , <b>WAN</b> and any interface already configured for your gateway.
Ether Type	Select the Ethernet interface type for this classification. Options include: <b>IP</b> , <b>ARP</b> , and <b>IPV6</b> for most models, and additional options for the SR515ac model.
Source MAC Address	Enter the source MAC Address and Source MAC Mask for this classification.
Source MAC Mask	
Destination MAC Address	Enter the destination MAC Address and destination MAC Mask for this classification.
Destination MAC Mask	
Source IP Address/Mask	Enter the source IP Address and Source IP Mask for this classification.
Protocol	<i>(Optional)</i> Enter the Protocol specified for this classification.
UDP/TCP Source Port	<i>(Optional)</i> Enter the Source Port applicable for this classification. You can enter a range (port:port) or a single port.
UDP/TCP Destination Port	<i>(Optional)</i> Enter the destination port applicable for this classification. You can enter a range (port:port) or a single port.
Specify Class Queue	<p><i>(Not applicable for SR515ac models )</i> Select from the available queues.</p> <p><b>Note:</b> Make sure to select a queue that is configured for the interface that you selected. If you select a queue that is not configured for the selected interface, any packets classified into that queue are processed by the default queue for the interface.</p>
<b>Specify Classification Results</b> section <i>(Available for SR515ac models only)</i>	
Egress Interface	<i>(Available for SR515ac models only)</i> Select the egress interface for this rule. Options are the interfaces already configured.
Egress Queue	<i>Available for SR515ac models only)</i> Select the egress queue for this rule. Options are the queues already configured.
Mark Applied Differentiated Service Code	Select the desired DSCP code.

Field Name	Description
Point	
802.1P priority	This value is inserted into the Ethernet frame and used to differentiate traffic. Lower values assign higher priorities. Options are: 1 - 7.
Rate Limit (Kbps)	Enter the data traffic rate limit applied for this classification. For SR515ac models, this field is labeled <b>Set Rate Limit</b> .

## QoS Port Shaping

QoS Port Shaping facilitates setting a fixed rate (Kbps) for each of the Ethernet ports.

**Note:** This feature is not available for the SR3xxn model.

1. In the left navigation bar, click **Advanced Setup** > **Quality Of Service** > **QoS Port Shaping**. The following page appears.

**QoS Port Shaping Setup**

QoS port shaping supports traffic shaping of Ethernet interface.  
 If "Egress Shaping Rate" is set to "-1", it means no shaping is applied and "Egress Burst Size" will be ignored.  
 If "Ingress Policing Rate" is set to "-1", no policing (aka rate limiting) is applied.

Interface	Type	Egress Shaping Rate (Kbps)	Egress Burst Size (bytes)	Ingress Policing Rate (Kbps)
eth3	LAN	-1	0	-1
eth2	LAN	-1	0	-1
eth1	LAN	-1	0	-1
eth0	LAN	-1	0	-1
eth4	LAN	-1	0	-1

Apply/Save

2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Interface	Each entry in this column represents one of the Ethernet LAN ports on the gateway.
Type	Each entry in this column identifies the function for which each physical port is configured on the gateway.
Shaping Rate (Kbps)	(Not applicable for SR515ac models ) Enter the data rate for packets on the specified Interface. Options are: 1 - 1,000,000 Kbps. The default is -1 (no shaping).
Burst Size (bytes)	(Not applicable for SR515ac models ) Enter the burst size to be applied to packets in the defined queue. Options are 1600 bytes or greater.  If you enter a value of -1 (disabled) in the <b>Shaping Rate</b> field, the value in this field is



Field Name	Description
	ignored.
Egress Shaping Rate (Kbps)	<i>(Available for SR515ac models only)</i> Enter the data rate for packets on the specified Interface. Options are: <b>1 - 1,000,000</b> Kbps. The default is <b>-1</b> (no shaping).
Egress Burst Size (bytes)	<i>(Available for SR515ac models only)</i> Enter the burst size to be applied to packets in the defined queue. Options are <b>1600 bytes</b> or greater. The default is <b>0</b> (no size limit).  If you enter a value of <b>-1</b> (disabled) in the <b>Egress Shaping Rate</b> field, the value in this field is ignored.
Ingress Policing Rate (Kbps)	<i>(Available for SR515ac models only)</i> Enter data rate for policing incoming packets in the defined queue. The default is <b>-1</b> (no policing).

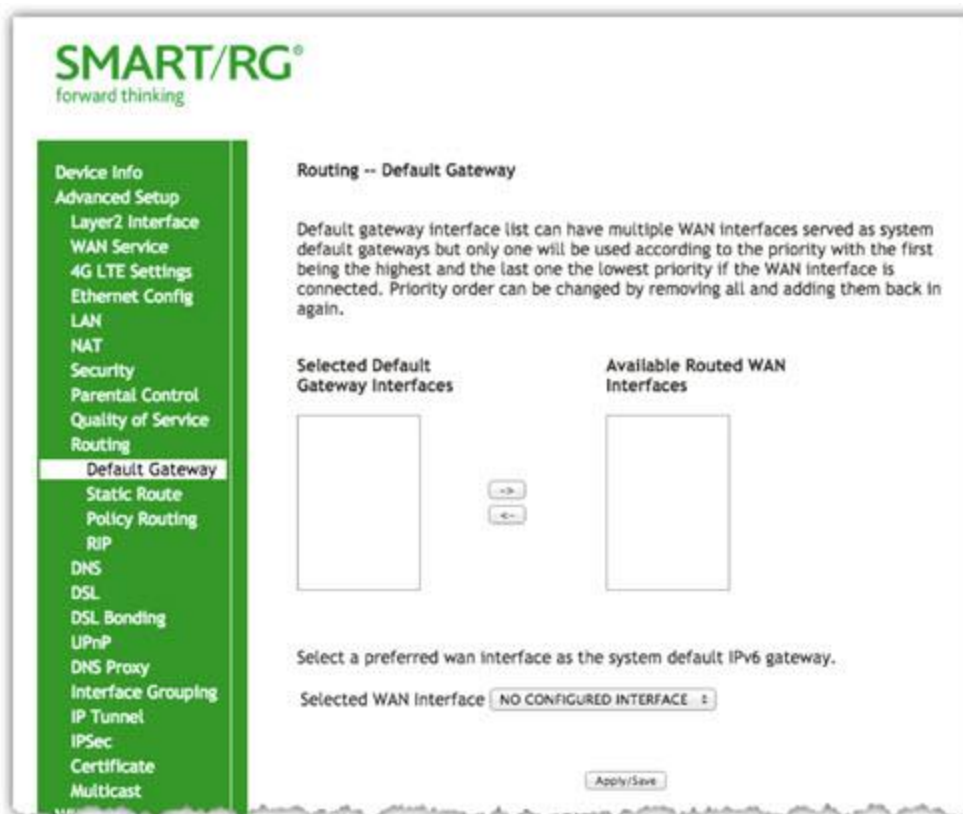
## Routing

In this section, you can configure default gateways, static routing, policy routing and RIP settings.

### Default Gateway

On this page, you can configure the default gateway interface list to establish access priority, that is, interfaces are accessed in the order listed in the **Selected Default Gateway Interfaces** column.

1. In the left navigation bar, select **Advanced Setup > Routing > Default Gateway**. The following page appears.

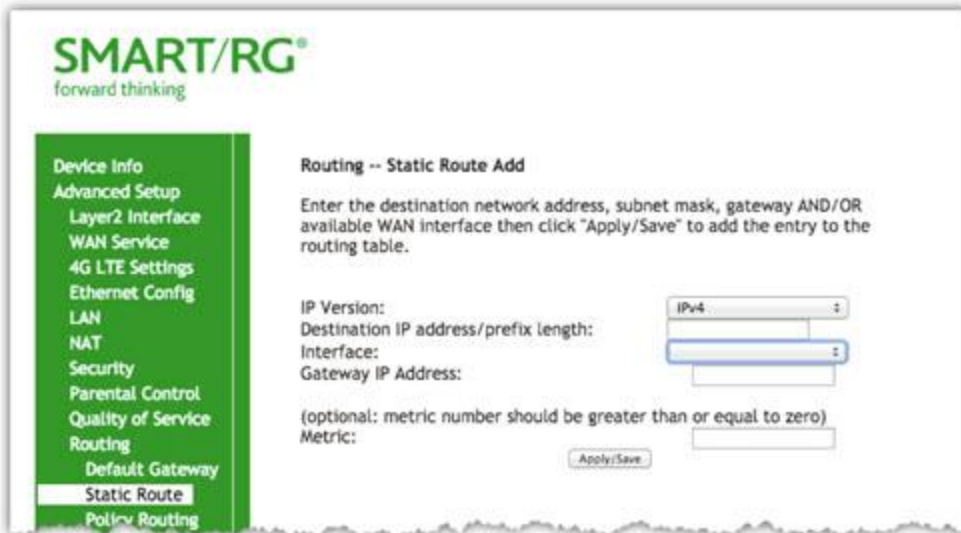


2. Select the interfaces that you want used as default gateway interfaces. Click the arrows to move your selection between the columns. Move the highest priority interface first, followed by the next highest priority interface, and so on.
3. (Optional) In the **Selected WAN Interface** field, select an IPv6 interface. You must configure the IPv6 interface before it appears in this field. The default is **NO CONFIGURED INTERFACE**.
4. Click **Apply/Save** to commit your changes.

### Static Route

On this page, you can configure static routes for your network. A static route is a manually configured, fixed route for IP data. You can enter a maximum of 32 entries.

1. In the left navigation bar, click **Advanced Setup** > **Routing** > **Static Route** and then click **Add**. The following page appears.



2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

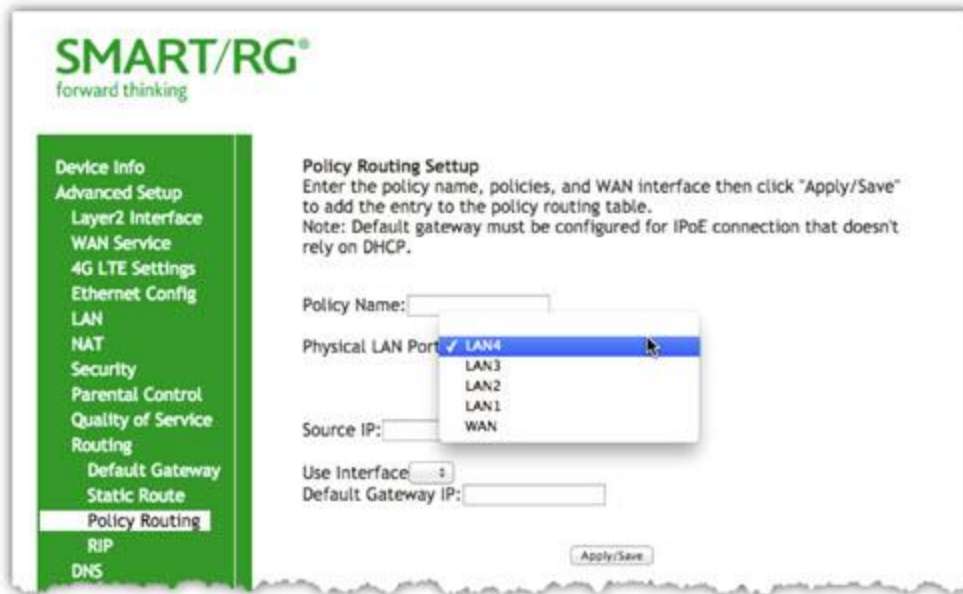
Field Name	Description
IP Version	Select the IP version associated with the static route you wish to create. Options are: <b>IPv4</b> and <b>IPv6</b> .
Destination IP address/- prefix length	Enter the destination network address / subnet mask for route.
Interface	Select the WAN Interface for this route. This list filtered by the selected IP version.
Gateway IP Address	Enter the destination IP address for this route. If needed, include the /prefix length.
Metric	(Optional) Establishes traffic priority/weighting. Must be equal to or greater than zero ( $\geq 0$ ).

## Policy Routing

Policy routing makes somewhat automated routing choices based on policies defined by a network administrator. For example, a network administrator might want to deviate from standard routing based on destination markers in the packet and, instead, forward a packet based on the source address.

On this page, you can configure similar policies.

1. In the left navigation bar, click **Advanced Setup > Routing > Policy Routing** and then click **Add**. The following page appears.



2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

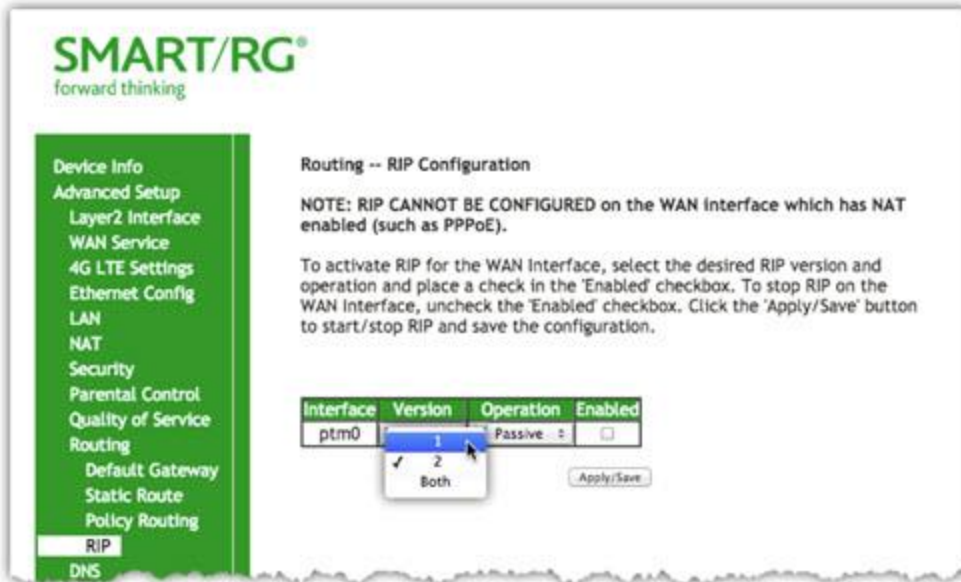
Field Name	Description
Policy Name	Enter a descriptive name for this entry to the policy routing table. This is a free-form text field.
Physical LAN Port	Select a physical LAN interface for the policy route.
Source IP	Enter the IP address for the source of this policy route.
Use Interface	Select the WAN Interface for this policy route
Default Gateway IP	Enter the IP address of the default gateway.

## RIP (Routing Information Protocol)

RIP is a type of distance-vector routing protocol, which leverages hop count as a metric for routing. RIP puts a limit on the number of hops (maximum of 15) allowed in order to prevent routing loops. This can sometimes limit the size of networks where RIP can be successfully employed.

On this page, you can configure the RIP settings.

1. In the left navigation bar, click **Advanced Setup** > **Routing** > **RIP**, and then click **Add**. The following page appears.



2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Interface	Displays a list of available WAN interfaces. Complete the line item(s) associated with the interface where you wish to employ RIP.
Version	Select the version of Routing Interface Protocol you desire. Reference RFC 1058 and RFC 1453 for detailed information on RIP versions. Options are: 1, 2, and Both.
Operation	Select the operation mode. Options are: <ul style="list-style-type: none"> <li>• <b>Active:</b> This mode listens and advertises routes.</li> <li>• <b>Passive:</b> This mode listens only. It does not advertise routes.</li> </ul>
Enabled	Select to employ RIP on the displayed interface.

## *DNS*

In this section, you can configure a DNS server, dynamic DNS and static DNS.

### **DNS Server**

On this page, you can input the Domain Name Server (DNS) information supplied by your service provider.

1. In the left navigation bar, click **Advanced Setup > DNS > DNS Server**. The following page appears.

**SMART/RG®**  
forward thinking

**Device Info**  
Advanced Setup  
Layer2 Interface  
WAN Service  
4G LTE Settings  
Ethernet Config  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
**DNS Server**  
Dynamic DNS  
Static DNS  
DSL  
DSL Bonding  
UPnP  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
Diagnostics  
Management  
Logout

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.  
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces	Available WAN Interfaces
<div style="border: 1px solid black; height: 80px; width: 100%;"></div>	<div style="border: 1px solid black; height: 80px; width: 100%;"></div>

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Select the configured WAN interface for the IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.  
Note that selecting a WAN interface for the IPv6 DNS server will enable the DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

2. Enter your desired settings. Click **Apply/Save** to commit changes.

The fields on this page are explained in the following table.

Field Name	Description
Selected DNS Server Interfaces	WAN service(s) selected to be your primary DNS server.

Field Name	Description
Available Wan Interfaces	WAN services available to be selected for the DNS server.
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	Enter the IP address of the secondary DNS server.
WAN Interface Selected	Alter this field only for IPv6 environments.
Primary IPv6 DNS Server	Enter the IP address of the primary IPv6 primary DNS.
Secondary IPv6 DNS Server	Enter the IP address of the primary IPv6 primary DNS.

## Dynamic DNS

Dynamic DNS (DDNS) automatically updates a name server in the DNS with the active DNS configuration of its configured hostnames, addresses or other data. Often this update occurs in real time. On this page, you can configure the settings for this feature.

1. In the left navigation bar, click **Advanced Setup > DNS > Dynamic DNS** and then click **Add**. The following page appears.

The screenshot shows the SMART/RG web interface. On the left is a green navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 4G LTE Settings, Ethernet Config, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DNS Server, and Dynamic DNS (which is highlighted). The main content area is titled 'Add Dynamic DNS'. Below the title is a paragraph: 'This page allows you to add a Dynamic DNS address from DynDNS.org or TZO or noip.com.' The form contains the following fields: 'D-DNS provider' (a dropdown menu currently showing 'DynDNS.org'), 'Hostname' (a text input field), 'Interface' (a dropdown menu), 'DynDNS Settings' (a section header), 'Username' (a text input field), and 'Password' (a text input field). At the bottom of the form is an 'Apply/Save' button.

2. Enter your desired settings.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
D-DNS provider	Select a dynamic Domain Name Server provider.



Field Name	Description
Hostname	Enter the hostname of the dynamic DNS server.
Interface	Select the gateway WAN interface whose traffic will be pointed at the specified Dynamic DNS provider.
Username	Enter the username for the dynamic DNS server .
Password	Enter the password for the dynamic DNS server.

## Static DNS

The Static DNS service allows you to resolve DNS queries on the Broadband Router by adding a static host name to the IP Address mappings. On this page, you can configure up to 10 static DNS entries.

1. In the left navigation bar, click **Advanced Setup > DNS > Static DNS** and then click **Add**. The following page appears.



2. Enter your desired settings.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Hostname	Enter the hostname of the client computer.
Interface	Enter the IP address of the DNS server client uses to assist in resolving domain names.

## DSL

On this page, you can configure settings for the DSL interface.

**Caution:** Altering these settings unnecessarily can result in the gateway being unable to attain DSL synchronization.

1. In the left navigation bar, click **Advanced Setup** -> **DSL**. The following page appears.

**SMART/RG®**  
forward thinking

**Device Info**  
Advanced Setup  
Layer2 Interface  
WAN Service  
4G LTE Settings  
Ethernet Config  
LAN  
NAT  
Security  
Parental Control  
Quality of Service  
Routing  
DNS  
**DSL**  
DSL Bonding  
UPnP  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
Diagnostics  
Management  
Logout

**DSL Settings**

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled
- VDSL2 Enabled

Select the profile below.

- 8a Enabled
- 8b Enabled
- 8c Enabled
- 8d Enabled
- 12a Enabled
- 12b Enabled
- 17a Enabled

US0

- Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable
- PhyR Enable
- ADSL PTM Mode Enable

Inventory Management

- Use board serial for EOC Serial Number

Apply/Save    Advanced Settings

2. Enter your desired settings.
3. To configure advanced settings, see ["Advanced settings"](#).
4. Click **Apply/Save** to commit your changes.

**Note:** For the SR3xxn models, the following fields are not available: **VDSL2** modulation, profile options, and **USO** checkbox.

The fields on this page are explained in the following table.

Modulation	Data Transmission Rate	Max Downstream (Mbps)	Max Upstream (Mbps)
G.Dmt	ITU-T G.992.1 standard.	12	1.3
G.lite	ITU-T G.991.2 standard.	4	0.5
T1.413	ANSI T1.413 Issue 2 standard.	8	1.0
ADSL2	ITU-T G.992.3 standard.	12	1.0
AnnexL	Annex L of ITU-T G.992.3 standard which supports longer loops but with reduced transmission rates.		
ADSL2+	ITU-T G.992.5 standard.	28	1.0
AnnexM	Annex L of ITU-T G.992.5 standard which supports extended upstream bandwidth.	24	3
VDSL2	ITU-T G.993.2 standard.	100	60

The following table explains the maximum transaction power for each profile supported for SRG gateways.

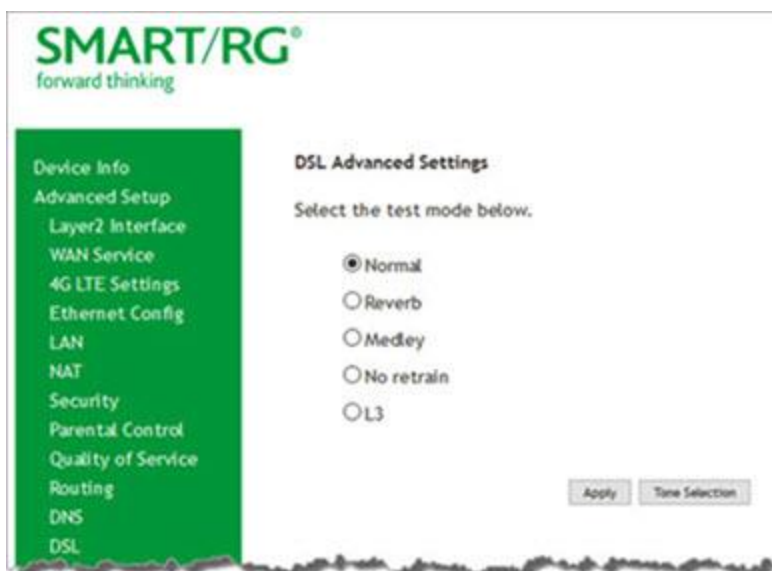
Parameter	8a	8b	8c	8d	12a	12b	17a
Max DS Tx Power (dBm)	+17.5	+20.5	+11.5				+14.5
Max US Tx Power (dBm)				+14.5			
Min bidirectional net data rate		50Mbps			68Mbps		100Mbps

Other Settings	
Field Name	Description
Inner Pair/Outer Pair	The RJ11 connector has four contacts. The center pair of pins is DSL1. The outer pair pins are the contacts for DSL2. Select which pair should be used.

Other Settings	
Field Name	Description
Capability	<ul style="list-style-type: none"> <li>• <b>Bitswap Enable:</b> Enables adaptive handshaking functionality.</li> <li>• <b>SRA Enable:</b> Enables Seamless Rate Adaptation.</li> <li>• <b>PhyR Enable:</b> Enables Physical Layer Retransmission.</li> <li>• <b>ADSL PTM Mode Enable:</b> Enables Asymmetric Digital Subscriber Line in Packet Transfer Mode.</li> </ul>
Inventory Management	Select whether to use the gateway serial number as the EOC serial number in your inventory management database.

## Advanced settings

1. To configure the test mode, click **Advanced Settings** on the **Advanced > DSL** page. The following page appears.



2. Click **Apply** to place the gateway in test mode.

- To view the ADSL tone settings, click **Tone Selection**. TADSL Tone Settings page appears.

**Caution:** Do not modify the tones selected unless under explicit instruction from a telecommunications professional.

- Click **Apply** to commit your changes or **Close** to return to the previous page.

The fields on this page are explained in the following table.

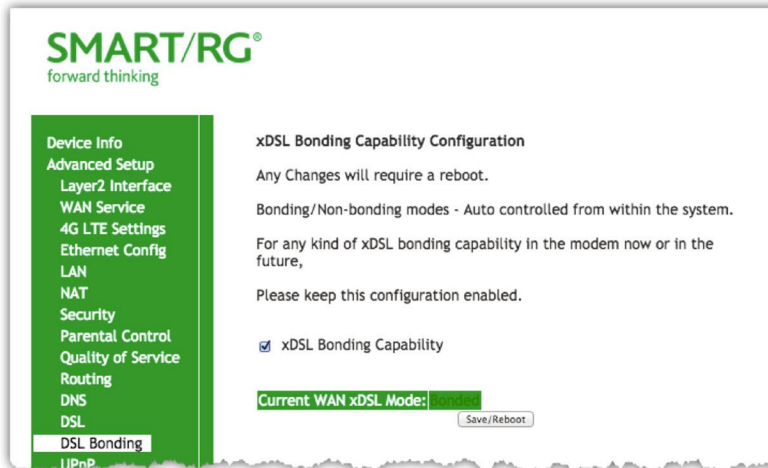
Mode	Description
Normal	Puts the DSL PHY in test mode, sending only a Normal signal.
Reverb	Puts the DSL PHY in test mode, sending only a REVERB signal.
Medley	Puts the DSL PHY in test mode, sending only a MEDLEY signal.
No Retrain	The DSL PHY attempts to establish a connection as in Normal mode, but once the connection is up, it does not retrain even if the signal is lost.
L3	Puts the DSL modem in the L3 power state.

## DSL Bonding

**Note:** This feature is supported only on the SR550n and SR552n models.

Bonding enables two DSL lines to feed the same modem and leveraging the bandwidth of both lines. Once bonded, the lines behave as a single, higher bandwidth connection.

1. In the left navigation bar, click **Advanced Setup** > **DSL Bonding**. The following page appears.



2. To enable bonding, click **xDSL Bonding Capability**.
3. Click **Save/Reboot** to commit your changes. Your gateway is rebooted.

## UPnP

On this page, you can enable UPnP when 3rd party devices on your LAN support this Universal Plug and Play standard. Common client devices include gaming consoles, IP cameras, printers and others. This feature is enabled by default.

1. In the left navigation bar, select **Advanced Setup > UPnP**. The following page appears.

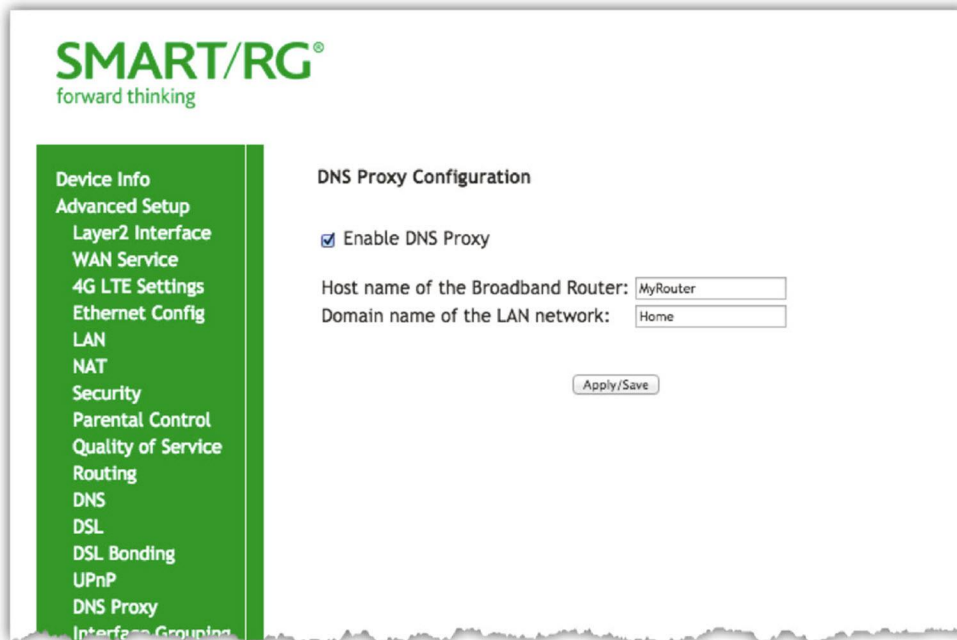


2. To disable this option, click **Enable UPnP** to clear the box.
3. Click **Apply/Save** to commit your changes.

## DNS Proxy

On this page, you can configure the DNS proxy settings. A DNS proxy improves domain look-up performance for clients by creating a historical cache of look-ups.

1. In the left navigation bar, click **Advanced Setup > DNS Proxy**. The following page appears.



2. If not already selected, click **Enable DNS Proxy**.  
The **Host name** and **Domain Name** fields appear.
3. Enter the host name of the broadband router and the domain name of the LAN network.
4. Click **Apply/Save** to commit your changes.



## Interface Grouping

You can create an interface group to map local interfaces to WAN interfaces. A typical application for this feature is assigning IPTV STBs to a WAN interface.

1. In the left navigation bar, click **Advanced Setup > Interface Grouping** and then click **Add** (below the table). The following page appears.

The screenshot shows the SMART/RG web interface for the 'Interface Grouping' configuration page. The left navigation bar is green and contains the following menu items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 4G LTE Settings, Ethernet Config, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, DSL Bonding, UPnP, DNS Proxy, **Interface Grouping** (highlighted), IP Tunnel, IPSec, Certificate, Multicast, Wireless, Diagnostics, Management, and Logout. The main content area has a white background and contains the following fields and sections:

- Group Name:** A text input field.
- Shared WAN Interface:** A checkbox.
- Grouped WAN Interfaces:** An empty box.
- Available WAN Interfaces:** A box containing 'br\_0\_0\_1/ptm0' and 'No Interface/None'.
- Grouped LAN Interfaces:** An empty box.
- Available LAN Interfaces:** A box containing 'LAN4', 'LAN3', 'LAN2', 'LAN1', and 'WAN'.
- Automatically Add Clients With the following DHCP Vendor IDs:** Two empty text input fields.
- Apply/Save:** A button at the bottom right.

2. To create a new interface group, enter a unique **Group Name**, then proceed with either step 3 (dynamic) or step 4 (static) below.

3. If this new grouped interface is to share the WAN interface, click **Shared WAN Interface**. *Not* selecting this option this will cause the WAN interface you select to be removed from any other interface groups.  
**Important:** If a vendor ID is configured for a specific client device, make sure to reboot the client device attached to the gateway to allow it to obtain an appropriate IP address.
4. Map the ports for the WAN or LAN interface:
  - a. Select an interface from the applicable **Available Interface** list.
  - b. Add it to the **Grouped Interface** list by clicking the arrow to create the required mapping of the ports. Hold down the Shift key to select multiple interfaces.  
**Note:** Depending on the WAN interface configuration, these clients may obtain public IP addresses.
5. To automatically add LAN clients (such as set-top boxes) to a WAN Interface in the new group, enter the **DHCP vendor ID** string. You can add up to 16 vendor IDs.  
When you configure a DHCP vendor ID string, any DHCP client request that includes this vendor ID is denied an IP address from the local DHCP server (DHCP option 60).
6. Click **Apply/Save**. Your changes take effect immediately.
7. To remove a grouping, select the grouping and click **Remove**. You can only remove groupings that you create.

## IP Tunnel

IP Tunneling is typically used as a means to establish a path between two independent networks. Your SmartRG gateway supports connecting islands of IPv6 networks across the IPv4 internet or IPv4 in IPv6 as well.

On this page, you can configure IP tunnel settings.

**Note:** For IPv6inIPv4, only 6rd configuration is supported. For IPv4inIPv6, only DS-Lite configuration is supported.

### IPv6inIPv4

On this page, you can configure the IPv6inIPv4 settings.

1. In the left navigation bar, click **Advanced Setup** > **IP Tunnel** > **IPv6inIPv4** and then click **Add**. The following page appears.

The screenshot shows the SMART/RG web interface for configuring an IPv6inIPv4 tunnel. The left navigation bar is green and contains the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 4G LTE Settings, Ethernet Config, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, DSL Bonding, UPnP, DNS Proxy, Interface Grouping, IP Tunnel, **IPv6inIPv4**, IPv4inIPv6, and IPS. The main content area is titled "IP Tunneling -- 6in4 Tunnel Configuration" and includes the following fields and options:

- Tunnel Name:** MyTunnel
- Mechanism:** 6RD
- Associated WAN Interface:** (Dropdown menu)
- Associated LAN Interface:** LAN/br0
- Manual/Automatic:** Manual (selected), Automatic
- IPv4 Mask Length:** (Input field)
- 6rd Prefix with Prefix Length:** (Input field)
- Border Relay IPv4 Address:** (Input field)
- Apply/Save:** (Button)

2. Enter a **Tunnel Name**.
3. Select the WAN and LAN interfaces associated with the tunnel you wish to establish.
4. **IPv4 Mask Length**, **6rd Prefix with Prefix Length** and **Border Relay IPv4 Address** can be configured automatically. To configure these settings manually, select **Manual** under **Associated LAN Interface** and enter the appropriate values.
5. Click **Apply/Save** to commit your changes.

## IPv4inIPv6

On this page, you can configure the IPv4inIPv6 settings.

1. In the left navigation bar, click **Advanced Setup** > **IP Tunnel** > **IPv6inIPv4** and then click **Add**. The following page appears.

**SMART/RG®**  
forward thinking

**IP Tunneling -- 4in6 Tunnel Configuration**

Currently, only DS-Lite configuration is supported.

Tunnel Name: My Tunnel

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

Manual  Automatic

AFTR:

Apply/Save

**Note:** Currently, only the DS-Lite Mechanism is supported. Consult RFC6333 for further information regarding DS-Lite.

2. Enter a **Tunnel Name**
3. Select the **LAN** and **WAN** interfaces associated with the tunnel you wish to establish.
4. **AFTR** (Address Family Transition Router) may be configured automatically. To configure **AFTR** manually, select **Manual** under **Associated LAN Interface** and enter the appropriate values.
5. Click **Apply/Save** to commit your changes.

## IPSec

Internet Protocol Security is a protocol for securing communications by packet level encryption and authentication.

On this page, you can enable and remove connections, or edit existing connections.

1. In the left navigation bar, click **Advanced Setup** > **IP Sec** and then click **Add New Connection**. The following page appears.

The screenshot shows the SMART/RG web interface for configuring IPSec settings. The left navigation bar is green and contains the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 4G LTE Settings, Ethernet Config, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, DSL Bonding, UPnP, DNS Proxy, Interface Grouping, IP Tunnel, IPv6InIPv4, IPv4InIPv6, IPSec, Certificate, Multicast, Wireless, Diagnostics, Management, and Logout. The main content area is white and contains the following settings:

- IPSec Settings**
- IPSec Connection Name:
- IP Version:
- Tunnel Mode:
- Local Gateway Interface:
- Remote IPSec Gateway Address:
- Tunnel access from local IP addresses:
- IP Address for VPN:
- Mask or Prefix Length:
- Tunnel access from remote IP addresses:
- IP Address for VPN:
- Mask or Prefix Length:
- Key Exchange Method:
- Authentication Method:
- Pre-Shared Key:
- Perfect Forward Secrecy:
- Advanced IKE Settings:
- 

2. Enter your connection details by completing the appropriate fields.
3. If desired, click **Advanced IKE Settings** to select Phase 1 and Phase 2 specific parameters. For detailed information about these settings, see ["Advanced IKE Settings"](#).
4. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
IPSec Connection Name	A free form text field. Enter a descriptive name for this connection
IP Version	Select the IP version environment associated with your infrastructure. Options are <b>IPv4</b> and <b>IPv6</b> .
Tunnel Mode	Select the encapsulation method to be used. Options are: <ul style="list-style-type: none"> <li>• <b>AH</b>: Use this mode to encapsulate a packet with AH and IP headers. For authentication, the entire packet is signed.</li> <li>• <b>ESP</b>: Use this mode to encapsulate a packet with ESP and IP headers. An ESP trailer is added to the packet for authentication and integrity.</li> </ul>
Local Gateway Interface	Select the WAN connection to be associated with this tunnel.
Remote IPSec Gateway Address	Enter the WAN IP for this tunnel.
Tunnel Access From Local IP Addresses	Select IP information for site A and B. Options are: <ul style="list-style-type: none"> <li>• <b>Subnet</b>: Allows access to the entire LAN.</li> <li>• <b>Single Address</b>: For single host, select this option.</li> </ul>
IP Address for VPN	Enter the IP address for local access.
Mask or Prefix Length	Enter the subnet mask or prefix length for IP address entered for local access, e.g., 255.255.255.0.
Tunnel Access From Remote IP Addresses	Select IP information for site A and B. Options are: <ul style="list-style-type: none"> <li>• <b>Subnet</b>: Allows access to the entire LAN.</li> <li>• <b>Single Address</b>: For single host, select this option.</li> </ul>
IP Address for VPN	Enter the IP address for remote access.
Mask or Prefix Length	Enter the subnet mask or prefix length for IP address entered for remote access, e.g., 255.255.255.0.
Key Exchange Method	The key-exchange method to be used for IPSec. Options are: <ul style="list-style-type: none"> <li>• <b>Auto(IKE)</b>: This method uses the negotiated key-exchange method for IPSec. This is the default and recommended for best results.</li> <li>• <b>Manual</b>: This method requires that you configure the details.</li> </ul>
Authentication Method	Select the method by which the remote end will authenticate. <ul style="list-style-type: none"> <li>• <b>Pre-Shared Key</b>: A key is distributed to authorized users for logging into the system. Enter the key in the <b>Pre-shared Key</b> field.</li> <li>• <b>Certificate (x.509)</b>: A certificate is used for authentication. Select the certificate file in the <b>Certificate</b> field that appears.</li> </ul>
Perfect forwarding Secrecy	This setting determines whether a session key derived from a set of long-term keys is compromised if one of the long-term keys in the set is compromised. <ul style="list-style-type: none"> <li>• <b>Enable</b>: Prevents long-term key from being compromised.</li> </ul>

Field Name	Description
	<ul style="list-style-type: none"> <li>• <b>Disable:</b> Permits long-term keys to be compromised.</li> </ul>

## Advanced IKE Settings

You can configure advanced IKE settings if desired.

1. On the IPSec Settings page, click **Show Advanced IKE Settings** to display the Phase 1 and Phase 2 fields.
2. Fill in the fields, using the information in the table below.

Field Name	Description
Mode	Select a mode. Options are <b>Main</b> and <b>Aggressive</b> .
Encryption Algorithm	Select the encryption algorithm. Options are <b>3DES</b> , <b>AES - 128</b> , <b>AES-192</b> , and <b>AES-256</b> .
Integrity Algorithm	Select the integrity algorithm. Options are <b>MD5</b> and <b>SHA1</b> .
Select Diffie-Hellman Group for Key Exchange	Select the D-H group. Options are <b>768bit - 8192bit</b> . The default is <b>1024bit</b> .
Key Life Time	Enter the number of seconds that a key is valid. The default is <b>3600</b> seconds.

3. Click **Apply/Save** to commit your changes.

## Certificate

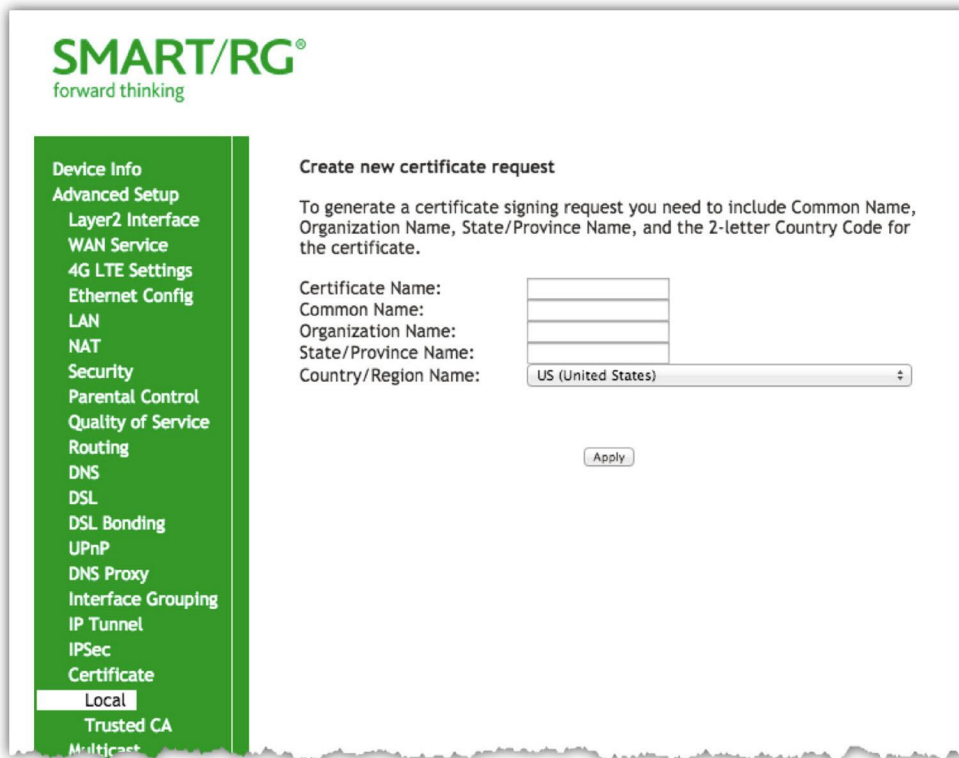
On this page, you can configure certificates for the gateway. You can use Local and Trusted CA certificates on this gateway.

### Local

Local certificates are used to identify the gateway to other users. On this page, you can create a new certificate request locally and have it signed by a certificate authority, or you can import an existing certificate.

For additional info regarding Public Key Infrastructure (PKI), refer to ITU-T X.509.

1. In the left navigation bar, click **Advanced Setup > Certificate > Local** and then click **Create Certificate Request**. The following page appears.



2. Enter your connection details by completing the appropriate fields. For more information about certificates, refer to the ITU X.509 standard.
3. Click **Apply** to complete the request.

The fields on this page are explained in the following table.

Field Name	Description
Certificate Name	A free-form text field used to describe the intended use of the certificate.
Common Name	Enter the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address is for identification purposes and is a free-form text field.
Organization Name	A free form text field. Typically, this is the name of the company creating the request.
Country/Region	Select the country or region in which this certificate will be employed.



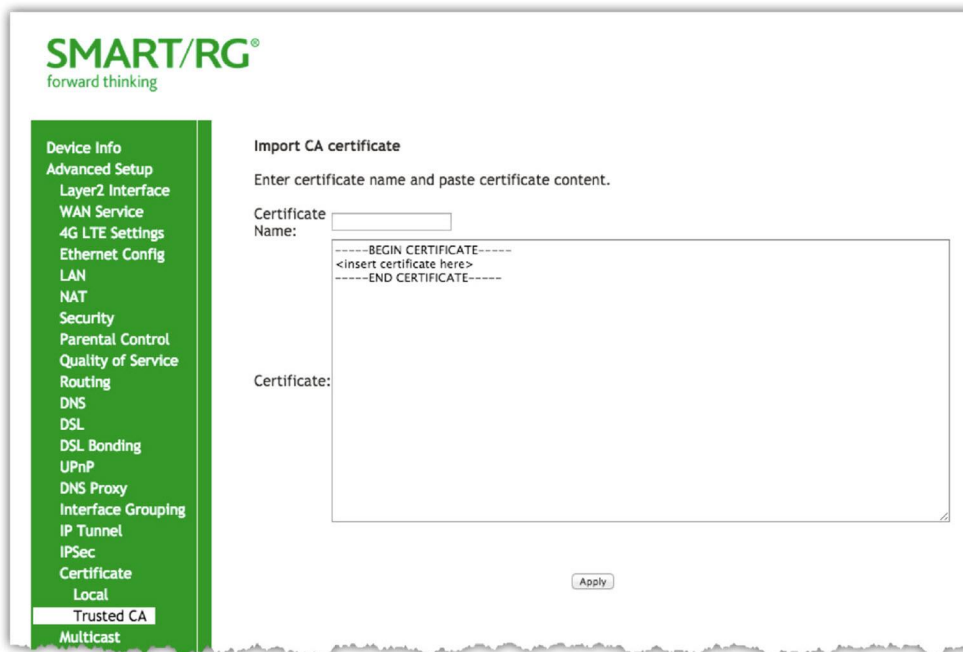
- To import a certificate and the corresponding private key, click **Import Certificate**. The following page appears.

- In the **Certificate Name** field, type "cpecert".
- Paste the **Certificate** details between the **BEGIN** and **END** markers.
- Paste the **Private Key** information between the **BEGIN** and **END** markers.
- Click **Apply** to implement this certificate.

## Trusted CA

On this page you import and store up to four trusted certificates. Trusted Certificates are used to identity other gateways to your gateway as a trusted source.

- In the left navigation bar, click **Advanced Setup > Certificate > Trusted CA** and then click **Import Certificate**. The following page appears.



2. In the **Certificate Name** field, type "acscert", and then paste the certificate details between the **BEGIN** and **END** markers.
3. Click **Apply** to commit this certificate.

After you add one certificate, a **Remove** button appears on the **Trusted CA** landing page. Click this button to remove the current certificate and replace it with a new one.

## Multicast

Multicast methodology is used for applications shipping information simultaneously to multiple destinations. The most common scenario is Internet television and other streaming media. In IP Multicast, the implementation occurs at the IP routing level, where routers create the most efficient distribution paths for packets sent to a destination.

On this page, you can configure the multicast settings.

1. In the left navigation bar, select **Advanced Setup > Multicast**. The following page appears.

2. Update or complete the necessary fields. The same fields are provided for both IGMP and MLD configuration.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Multicast Precedence	Select whether IGMP packets are given priority handling and at what level.

Field Name	Description
	Options are: <ul style="list-style-type: none"> <li>• <b>Enable:</b> IGMP packets are prioritized using the multicast precedence value. The lower the multicast precedence value, the higher that IGMP packets will be placed in the queue.</li> <li>• <b>Disable:</b> IGMP packets are not prioritized.</li> </ul>
Multicast Strict Grouping Enforcement	<i>(Available for SR515ac models only)</i> Select whether strict grouping is applied to IGMP packets. Options are <b>Enable</b> and <b>Disable</b> .
Default Version	Enter the supported IGMP version. Options are: <b>1 - 3</b> .
Query Interval	The interval at which the multicast router sends a query messages to hosts, expressed in seconds.  If you enter a number below 128, the value is used directly. If you enter a number 128, it is interpreted as an exponent and mantissa.
Query Response Interval	Upon receiving a query packet, a host begins counting down seconds, from a random number. When the timer expires, the host sends its report.  Enter the maximum number of seconds that a host can pick to count down from. The value must be greater than the <b>Query Interval</b> . If using IGMP v1, this value is fixed at <b>10</b> seconds.
Last Member Query Interval	Enter the maximum response time within which the host must respond to the Out of Sequence query from the router. The default is <b>1000ms</b> .  IGMP uses this value when the router receives an IGMPv2 Leave report indicating at least one host wants to leave the group. Upon receiving the Leave report, the router verifies whether the interface is configured for IGMP Immediate Leave. If not, the router sends the out-of-sequence query.
Robustness Value	Enter the value representing the complexity of the query. The greater the value, the more robust the query. Options are: <b>2 - 7</b> .
Maximum Multicast Groups	Enter the maximum number of groups allowed.
Maximum Multicast Data Sources (for IGMP v3)	Enter the maximum number of data sources allowed. Options are: <b>1 - 24</b> .
Maximum Multicast Group Members	Enter the maximum number of multicast groups that can be joined on a port or group of ports.
Fast leave	Select whether the IGMP proxy removes group members immediately without

Field Name	Description
	<p>sending a query. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> Group members are removed immediately.</li> <li>• <b>Disabled:</b> Group members are removed after a query is sent and a response received..</li> </ul>
LAN to LAN (Intra LAN) Multicast	<i>(Not applicable for SR515ac models)</i> Click to permit a multicast data source on the LAN side and enable IGMP snooping.
Membership Join Immediate (IPTV)	<p>Select whether clients should send join reports. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> No join report is sent; join is faster by a few milliseconds.</li> <li>• <b>Disabled:</b> The client sends a join report.</li> </ul>

## WIRELESS

In this section, you can configure the wireless interface settings for your gateway, including basic and advanced settings, MAC filtering, and wireless bridging.

**Note:** For the SR515ac model, the pages in this section are provided for both wireless bands, once for the 2.4 Ghz band and once for the 5 Ghz band. The fields are the same for both bands.

### Basic

On this page, you can configure basic features of the Wi-Fi LAN interface. You can enable or disable the Wi-Fi LAN interface, hide the network from active scans, set the Wi-Fi network name (also known as SSID) and restrict the channel set based on country requirements.

1. In the left navigation bar, click **Wireless > Basic**. The following page appears.

**SMART/RG**  
forward thinking

**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

- Enable WiFi Button
- Enable Wireless
- Enable Wireless Hotspot2.0 [WPA2 is required!]
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Max Clients:

**Wireless - Guest/Virtual Access Points:**

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Enable HSPOT	Max Clients	BSSID
<input type="checkbox"/>	Guest	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox" value="[wpa2]"/>	<input type="text" value="128"/>	N/A
<input type="checkbox"/>	Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox" value="[wpa2]"/>	<input type="text" value="128"/>	N/A
<input type="checkbox"/>	Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox" value="[wpa2]"/>	<input type="text" value="128"/>	N/A

2. Modify the settings as desired, using the information provided in the table below. The table at the bottom of the page lists the guest/virtual access points defined for your gateway. If desired, you can define up to three virtual access points for guest use.
3. Click **Apply/Save** to commit your settings.

The fields on this page are explained in the following table.

Field Name	Description
Enable Wi Fi Button	(Not applicable to the SR350n model) Click to enable the gateway's Wi-Fi button.
Enable Wireless	Click to enable the gateway's Wi-Fi radio.
Enable Wireless Hotspot2.0	Click to enable wireless Hotspot2.0. (WPA2 is required!)

Field Name	Description
	Hotspot 2.0 is focused on enabling a mobile device to automatically discover Wi-Fi access points that have a roaming arrangement with the user's home network and then connect securely.
Hide Access Point	Click to hide the access point SSID from end users.
Client Isolation	Click to prevent LAN client devices from communicating with one another on the wireless network.
Disable WMM Advertise	Click to stop the wireless from advertising Wireless Multimedia (WMM) functionality. WMM provides basic Quality of Service (QOS) for applications.
Enable Wireless Multicast Forwarding	Click to enable Wireless Multicast Forwarding (WMF). Multicast traffic is forwarded across wireless clients.
SSID	Enter the Wi-Fi SSID.
BSSID	Enter the Basic Service Set Identifier (BSSID) to provide the MAC address assigned to the wireless router.
Country	Select the country in which the gateway is deployed.
Country RegRev	<i>(Available on SR515ac models only)</i> Enter the revision number of the regulations being followed for the selected country. The default is 0.
Max Clients	Enter the maximum number of clients that can access the route wirelessly. Options are 1 - 16.
<b>Wireless - Guest/Virtual Access Points</b> table	
Enabled	Click to enable a virtual wireless access point for guest access.
SSID	Enter your wireless SSID.
Hidden	Click to hide the SSID from being broadcast publicly.
Isolate Clients	Click to prevent client PCs from communicating with one another.
Disable WMM Advertise	Click to stop the wireless from advertising Wireless Multimedia (WMM) functionality.
Enable WMF	Click to enable Wireless Multicast Forwarding (WMF).
Enable HSPOT	Click to enable wireless Hotspot2.0

Field Name	Description
BSSID	Displays the Basic Service Set Identifier or <b>N/A</b> .

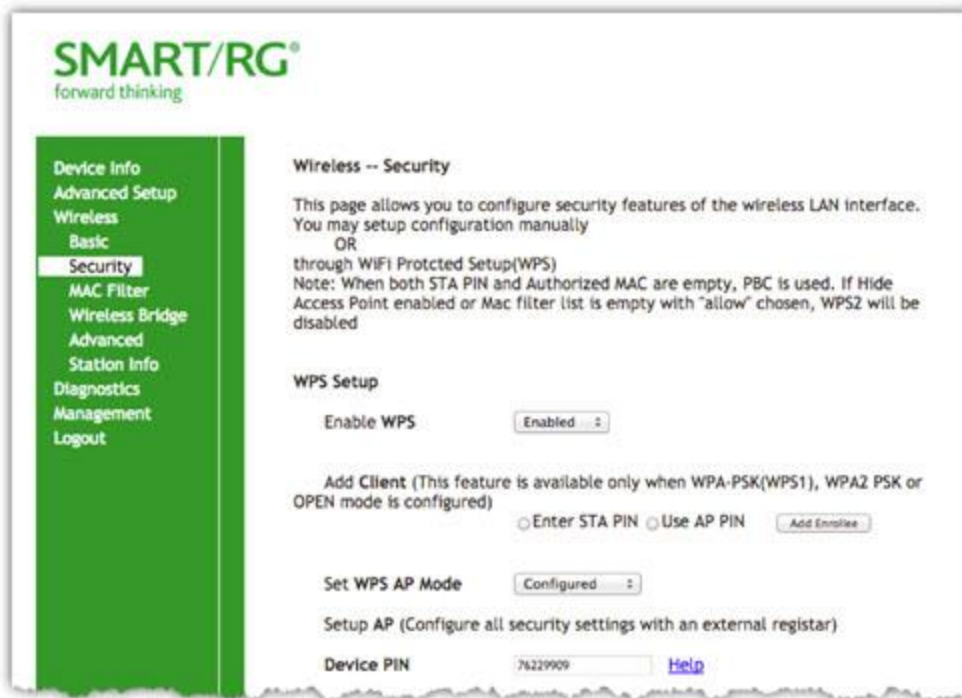
## Security

On this page, you can configure security features of the wireless LAN interface, either manually or via Wi-Fi Protected Setup (WPS).

**Note:** When WPS is enabled, the **STA PIN** and **Authorized MAC** fields appear. If both of these fields are empty, **PBC** becomes the default value. If **Hide Access Point** is enabled or the MAC filter list is empty with "Allow" chosen WPS2 will be disabled.

1. In the left navigation bar, click **Wireless > Security**. The following page appears.

**Note:** For SR515ac models, go to the **Wireless > 2.4 Ghz Band** or **5 Ghz Band** pages.



2. Modify the settings as needed, using the information provided in the field description table.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Enable WPS	Select to enable Wi-Fi Protected Setup. Options are: <b>Enabled</b> and <b>Disabled</b> .



Field Name	Description
Add Client	<p><i>(Not applicable for SR515ac models)</i> Select the method for generating the WPS PIN. Options are: <b>Enter STA PIN</b> and <b>Use AP PIN</b>.</p> <p>To add an enrollee station, click <b>Add Enrollee</b>.</p> <p><b>Note:</b> If the <b>PIN</b> and <b>Set Authorized Station MAC</b> fields are left blank, the <b>PBC</b> (push-button) mode is automatically made active.</p>
Set Authorized Station MAC	<p><i>(Not applicable for SR515ac models)</i> When manually pairing via WPS, enter the MAC address of the client device you are trying to connect.</p>
Set WPS AP Mode	<p>Select how security is assigned to clients.</p> <ul style="list-style-type: none"> <li>• <b>Configured:</b> The gateway assigns security settings to clients.</li> <li>• <b>Unconfigured:</b> An external client assigns security settings to the gateway.</li> </ul>
Device PIN	<p><i>(Not applicable for SR515ac models)</i> This value is generated by the access point.</p>
<b>Manual Setup AP</b> section	
Select SSID	<p>Select the SSID of the wireless network to which this security configuration will apply.</p>
Network Authentication	<p>Select the desired network security authentication type. Options are: <b>Open</b>, <b>Shared</b>, <b>802.1X</b>, <b>WPA</b>, <b>WPA-PSK</b>, <b>WPA2</b>, <b>WPA2-PSK</b>, <b>Mixed WPA2/WPA</b>, and <b>Mixed WPA2/WPA-PSK</b>.</p>

The fields shown in the **Manual Setup AP** section of the page vary based on the network authentication method that you select. The variations are explained in the following sections:

- ["Open and Shared Network Authentication"](#)
- ["802.1X Network Authentication"](#)
- ["WPA Network Authentication"](#)
- ["WPA-PSK Network Authentication"](#)
- ["WPA2 and Mixed WPA2/WPA Network Authentication"](#)
- ["WPA2-PSK and Mixed WPA2/WPA-PSK Network Authentication"](#)

## Open and Shared Network Authentication

The same configuration fields apply for both **Open** and **Shared** authentication types. However, WPS may not be used with the **Shared** method.

1. On the Wireless > Security page, select **Open** or **Shared** in the **Network Authentication** field. The following fields appear.

**Note:** For SR515ac models, go to the Wireless > 2.4 Ghz Band or 5 Ghz Band pages.



2. Fill in the fields, using the information in the field description table below.
3. Click **Apply/Save** to save the settings.

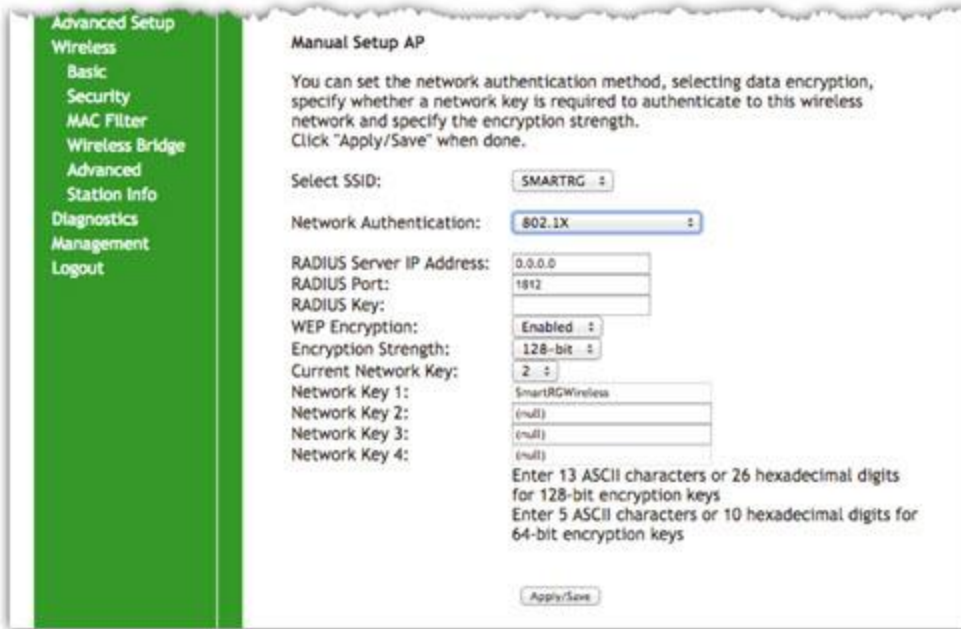
The fields on this page are explained in the following table.

Field Name	Description
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are <b>Enabled</b> and <b>Disabled</b> .
Encryption Strength	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select the length of the encryption method. Options are <b>128-bit</b> and <b>64-bit</b> . 128-bit is the more robust option for security.
Current Network Key	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select which of the four keys is presently in effect.
Network Key 1-4	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128-bit or 64-bit).

## 802.1X Network Authentication

1. On the Wireless > Security page, select **802.1X** in the **Network Authentication** field. The fields shown below appear.

**Note:** For SR515ac models, go to the **Wireless > 2.4 Ghz Band** or **5 Ghz Band** pages.



2. Fill in the fields, using the information in the field description table below.
3. Click **Apply/Save** to save the settings.

The fields on this page are explained in the following table.

Field Name	Description
RADIUS Server IP address	Enter the IP address of the RADIUS (Remote Authentication Dial In User Service) server associated with your network.
RADIUS Port	Enter the port number for the RADIUS server. Port <b>1812</b> is the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port <b>1645</b> . Options are <b>1 - 65535</b> .
RADIUS Key	<i>(Optional)</i> Enter the encryption key (if required) needed to authenticate to the specified RADIUS Server.
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are <b>Enabled</b> and <b>Disabled</b> .
Encryption Strength	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select the length of the encryption method. Options are <b>128-bit</b> and <b>64-bit</b> . 128-bit is the more robust option for security.
Current Network Key	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select which of the four keys is presently in effect.

Field Name	Description
Network Key 1-4	(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b> ) Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128-bit or 64-bit).

## WPA Network Authentication

WPA authentication requires the same set of parameters as the 802.1X authentication method plus two additional parameters: **WPA Group Rekey Interval** and **WEP Encryption**.

**Note:** This option is not available on SR515ac models.

1. On the Wireless > Security page, select **WPA** in the **Network Authentication** field. The fields shown below appear.



2. Fill in the fields, using the information in the field description table below and in ["802.1X Network Authentication"](#).
3. Click **Apply/Save** to save the settings.

The fields on this page are explained in the following table.

Field Name	Description
WPA Group Rekey Interval	The frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are: 1 - <b>65535</b> seconds.
WPA/WAPI Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are: <ul style="list-style-type: none"> <li>• <b>AES</b>: Advanced Encryption Standard.</li> <li>• <b>TKIP+AES</b>: AES combined with TKIP (Temporary Key Integrity Protocol).</li> </ul>

## WPA-PSK Network Authentication

**Note:** This option is not available on SR515ac models.

1. On the Wireless > Security page, select **WPA2-PSK** in the **Network Authentication** field. The following fields appear.



2. Fill in the fields, using the information in the field description table below.
3. Click **Apply/Save** to save the settings.

The fields on this page are explained in the following table.

Field Name	Description
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
WPA/WAPI passphrase	Enter the security password to be used by this security configuration.
Use base MAC address as WAP/WAPI Passphrase	Select whether to allow the base MAC address to be substituted for the password (in lieu of manually entering a password). When this box is checked, the <b>WPA/WAPI passphrase</b> field is ignored.
WPA Group Rekey Interval	The frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are: <b>1 - 65535</b> seconds.
WPA/WAPI Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are: <ul style="list-style-type: none"> <li>• <b>AES:</b> Advanced Encryption Standard.</li> <li>• <b>TKIP+AES:</b> AES combined with TKIP (Temporary Key Integrity Protocol).</li> </ul>
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are <b>Enabled</b> and <b>Disabled</b> .
Encryption Strength	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select the length of the encryption method. Options are <b>128-bit</b> and <b>64-bit</b> . 128-bit is the more robust option for security.

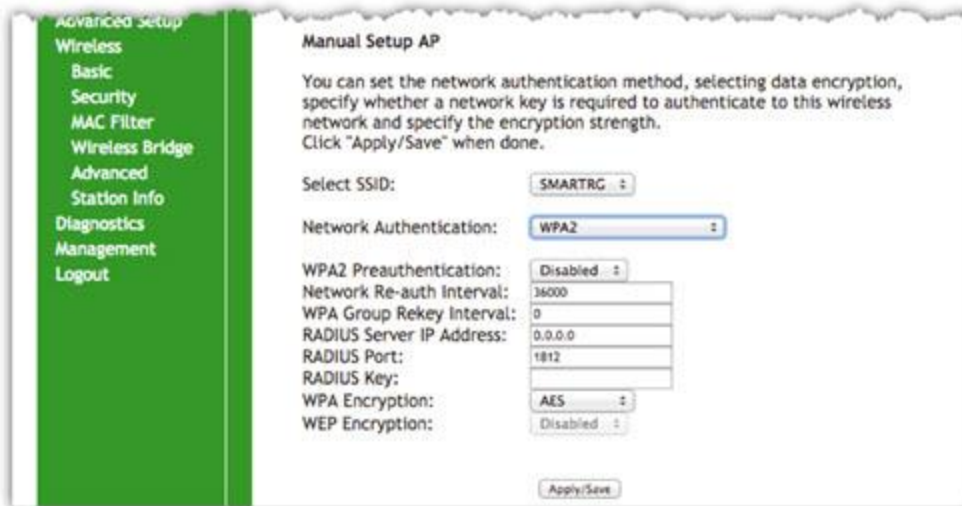
Field Name	Description
Current Network Key	(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b> ) Select which of the four keys is presently in effect.
Network Key 1-4	(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b> ) Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128-bit or 64-bit).

## WPA2 and Mixed WPA2/WPA Network Authentication

The same configuration fields apply for both WPA2 and Mixed WPA2/WPA authentication methods.

1. On the Wireless > Security page, select **WPA2** or **Mixed WPA2/WPA** in the **Network Authentication** field. The following fields appear.

**Note:** For SR515ac models, go to the Wireless > 2.4 Ghz Band or 5 Ghz Band> pages.



2. Fill in the fields, using the information in the field description table below.
3. Click **Apply/Save** to save the settings.

The fields on this page are explained in the following table.

Field Name	Description
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
Protected Management Frames	(Available for SR515ac models only) Select whether to enable this option. Options are <b>Enabled</b> and <b>Disabled</b> . The default is <b>Disabled</b> .
WPA2 Preauthentication	Select whether clients can pre-authenticate with the gateway while still connected to another AP. Options are <b>Enabled</b> and <b>Disabled</b> .

Field Name	Description
Network Re-Auth Interval	Enter the interval at which the client must re-authenticate with the gateway. Options are: <b>0-2,147,483</b> , and <b>647</b> seconds.
WPA Group Rekey Interval	The frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are: <b>1 - 65535</b> seconds.
RADIUS Server IP address	Enter the IP address of the RADIUS (Remote Authentication Dial In User Service) server associated with your network.
RADIUS Port	Enter the port number for the RADIUS server. Port <b>1812</b> is the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port <b>1645</b> . Options are <b>1 - 65535</b> .
RADIUS Key	<i>(Optional)</i> Enter the encryption key (if required) needed to authenticate to the specified RADIUS Server.
WPA/WAPI Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are: <ul style="list-style-type: none"> <li>• <b>AES</b>: Advanced Encryption Standard.</li> <li>• <b>TKIP+AES</b>: AES combined with TKIP (Temporary Key Integrity Protocol).</li> </ul>
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are <b>Enabled</b> and <b>Disabled</b> .
Encryption Strength	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select the length of the encryption method. Options are <b>128-bit</b> and <b>64-bit</b> . 128-bit is the more robust option for security.
Current Network Key	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select which of the four keys is presently in effect.
Network Key 1-4	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128-bit or 64-bit).

## WPA2-PSK and Mixed WPA2/WPA-PSK Network Authentication

The same configuration fields apply for both WPA2-PSK and Mixed WPA2/WPA-PSK authentication methods.

1. On the Wireless > Security page, select **WPA2-PSK** or **Mixed WPA2/WPA-PSK** in the **Network Authentication** field. The fields shown below appear.

**Note:** For SR515ac models, go to the Wireless > 2.4 Ghz Band or 5 Ghz Band pages.



2. Fill in the fields, using the information in the field description table below.
3. Click **Apply/Save** to save the settings.

The fields on this page are explained in the following table.

Field Name	Description
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
Protected Management Frames	<i>(Available for SR515ac models only)</i> Select whether to enable this option. Options are <b>Enabled</b> and <b>Disabled</b> . The default is <b>Disabled</b> .
WPA/WAPI passphrase	Enter the security password to be used by this security configuration.
Use base MAC address as WAP/WAPI Passphrase	Select whether to allow the base MAC address to be substituted for the password (in lieu of manually entering a password). When this box is checked, the <b>WPA/WAPI passphrase</b> field is ignored.
WPA Group Rekey Interval	The frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are: 1 - 65535 seconds.
WPA/WAPI Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are: <ul style="list-style-type: none"> <li>• <b>AES</b>: Advanced Encryption Standard.</li> <li>• <b>TKIP+AES</b>: AES combined with TKIP (Temporary Key Integrity Protocol).</li> </ul>
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are <b>Enabled</b> and <b>Disabled</b> .
Encryption Strength	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select the length of the encryption method. Options are <b>128-bit</b> and <b>64-bit</b> . 128-bit is the more robust option for security.
Current Network Key	<i>(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b>)</i> Select which of the four keys is presently in effect.

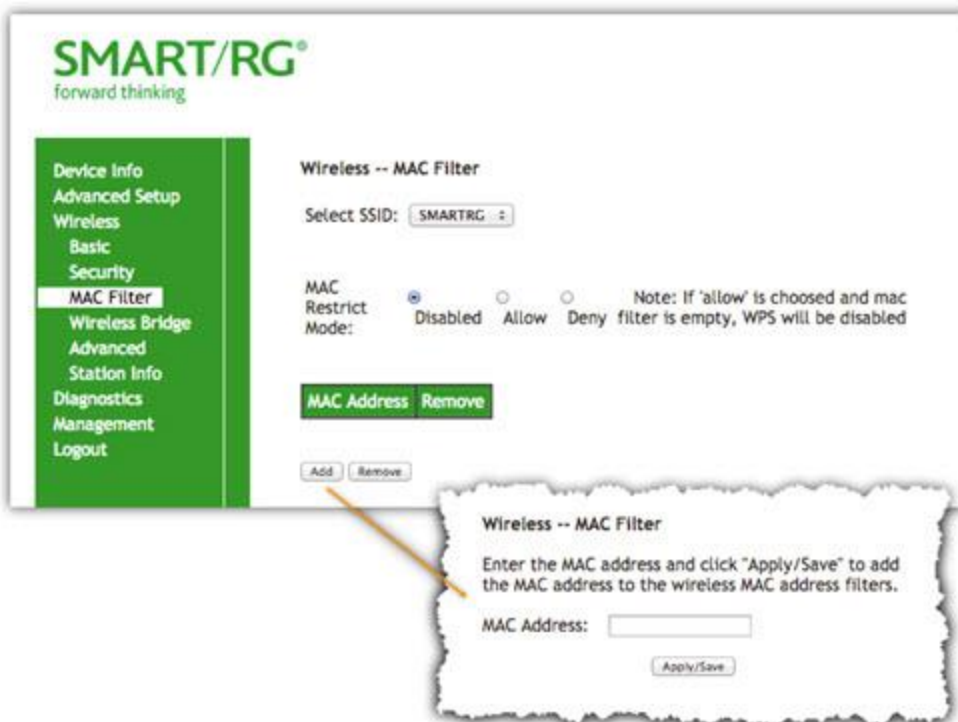


Field Name	Description
Network Key 1-4	(Appears when <b>WEP Encryption</b> is set to <b>Enabled</b> ) Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128-bit or 64-bit).

## MAC Filter

MAC Filtering refers to an access control methodology whereby the 48-bit address assigned to each LAN host NIC is used to determine access to the network. It is also known as Layer 2 address filtering.

1. In the left navigation bar, click **Wireless > MAC Filter**. The following page appears.



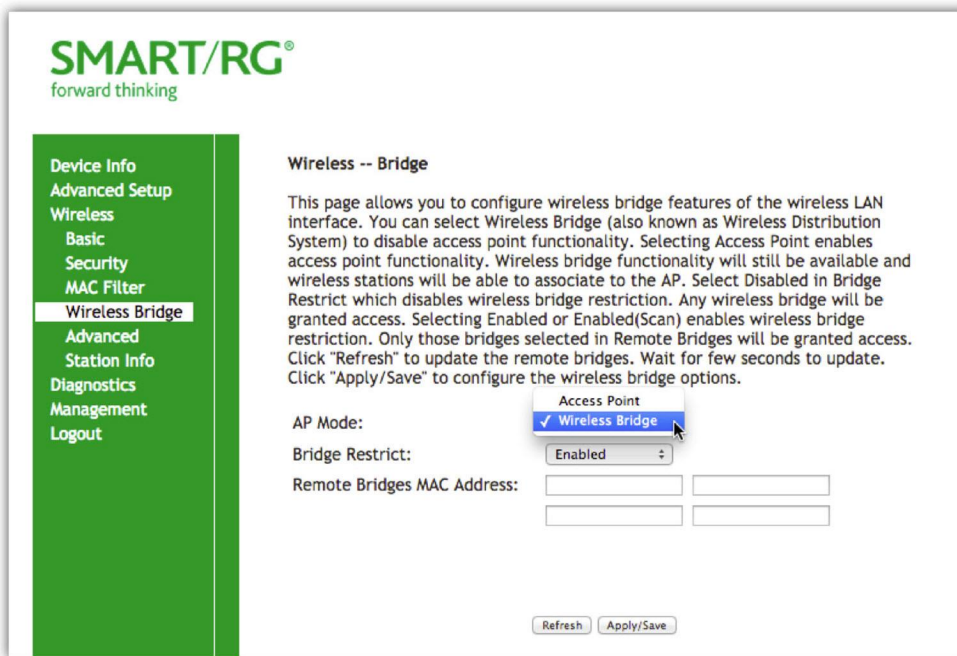
2. Select an SSID to which this MAC filter rule should apply.
3. In the **MAC Restrict Mode** field, select whether to apply MAC filtering. Options are:
  - **Disabled:** MAC filtering is off.
  - **Allow:** For specified MAC address, access is permitted.
  - **Deny:** Access for the specified MAC address is rejected.
4. To add a MAC address to the filter list:
  - a. Click **Add**.
  - b. Enter the MAC address.
  - c. Click **Apply/Save**.  
You are returned to the main MAC filtering page.

5. Click **Apply/Save** to commit your changes.

## Wireless Bridge

On this page, you can configure the wireless bridge features of the wireless LAN interface. Wireless Bridge is also known as Wireless Distribution System.

1. In the left navigation bar, click **Wireless > Wireless Bridge**. The following page appears.



2. Modify the settings as needed, using the information in the field description table.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
AP Mode	Select whether to enable or disable access point (AP) functionality. Options are: <ul style="list-style-type: none"> <li>• <b>Wireless Bridge</b>: Disables AP functionality.</li> <li>• <b>Access Point</b>: Enables AP functionality. Wireless bridge functionality is still available and wireless stations can associate to the AP.</li> </ul>
Bridge Restrict	<i>(Optional)</i> Select to enable or disable wireless bridge restriction. Options are: <ul style="list-style-type: none"> <li>• <b>Enabled or Enabled(Scan)</b>: Enables wireless bridge restriction. Only bridges specified in</li> </ul>

Field Name	Description
	<p>the <b>Remote Bridge MAC Address</b> field are granted access. Click <b>Refresh</b> to update the station list. The list takes a few seconds to update.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Disables wireless bridge restriction. Any wireless bridge is granted access.</li> </ul>
Remote Bridge MAC Address	Enter the MAC address(es) of the remote bridges to be allowed access.

## Advanced

On this page, you can configure the advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a desired speed, set the fragmentation threshold, the RTS threshold, the wakeup interval for clients in power-save mode, and more.

1. In the left navigation bar, click **Wireless > Advanced**. The following page appears.

**SMART/RG**  
forward thinking

**Wireless -- Advanced**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band: 2.4GHz  
 Channel: Auto  
 Auto Channel Timer(min): 5  
 802.11n/EWC: Auto  
 Bandwidth: 20MHz  
 Control Sideband: Lower  
 802.11n Rate: Auto  
 802.11n Protection: Auto  
 Support 802.11n Client Only: Off  
 RIFS Advertisement: Auto  
 OBSS Coexistence: Enable  
 RX Chain Power Save: Disable  
 RX Chain Power Save Quiet Time: 10  
 RX Chain Power Save PPS: 10  
 54g Rate: 1 Mbps  
 Multicast Rate: Auto  
 Basic Rate: Default  
 Fragmentation Threshold: 2346  
 RTS Threshold: 2347  
 DTIM Interval: 1  
 Beacon Interval: 100  
 Global Max Clients: 128  
 XPress™ Technology: Enabled  
 Transmit Power: 100%  
 WMM(Wi-Fi Multimedia): Enabled  
 WMM No Acknowledgement: Disabled  
 WMM APSD: Enabled

Current: 1 (interference: acceptable)  
 Current: 20MHz  
 Current: N/A  
 Power Save status: Full Power

Apply/Save

2. Modify the fields as needed, using the information in the field description table.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Band	Pre-set at 2.4 GHz for compatibility with IEEE 802.11x standards.
Channel	Select the Wi-Fi channel you want to use. Options are <b>Auto</b> and <b>1 - 11</b> . It is recommended to use only non-overlapping channels which are: <b>1, 6</b> and <b>11</b> .
Auto Channel Timer (min)	Enter the frequency (in minutes) at which the gateway scans channels for interference. If a threshold of inference is detected, a new channel will be selected automatically. Options are: <b>0 - 65535</b> minutes.
802.11n/EWC	Select whether to enable this standard. Options are <b>Auto</b> and <b>Disabled</b> . For detailed information about this standard, refer to IEEE 802.11n Draft 2.0.  Note: For SR515ac models, this field is labeled <b>802.11n</b> .
Bandwidth	Select the operating bandwidth. Options are: <ul style="list-style-type: none"> <li>• <b>20MHz</b>: This option utilizes only one 20MHz band.</li> <li>• <b>40MHz</b>: This option provides better throughput by taking advantage of two, adjacent 20MHz bands.</li> </ul>
Control Sideband	<i>(Applies only to 40 MHz, 802.11n operation)</i> The control sideband is the 20 MHz channel on which the network is advertised, where client devices will find beacons. Options are: <ul style="list-style-type: none"> <li>• <b>Lower</b>: The additional 20 MHz of bandwidth for data will be positioned <i>above</i> the control channel.</li> <li>• <b>Upper</b>: The additional 20 MHz of bandwidth for data will be positioned <i>below</i> the control channel. Also, selecting this option changes the channel choices displayed.</li> </ul>
802.11n rate	Select the desired physical transmission rate.
802.11n protection	Selects whether to enable 802.11n and legacy clients to both work effectively on the network. Options are: <ul style="list-style-type: none"> <li>• <b>Auto</b>: Provides maximum security but there is a noticeable impact on throughput. With this option, RTS/CTS behavior permits legacy clients to become aware of 802.11n transmit times, but decreases overall throughput of the system.</li> <li>• <b>Off</b>: Provides better throughput.</li> </ul>

Field Name	Description
Support 802.11n client only	Select whether to restrict 802.11b/g clients from accessing the gateway. Options are <b>On</b> and <b>Off</b> .
RIFS Advertisement	Reduced Inter-Frame Space (RIFS). Improves performance by reducing dead time required between OFDM transmissions. Options are <b>Auto</b> and <b>Off</b> .  Recommended primarily for "greenfield" deployments that include only 802.11n clients, and no legacy clients.
OBSS Coexistence	Coexistence of Overlapping Basic Service Sets (OBSS) prevents overlapping in the 20 MHz and 40 MHz frequencies. Options are: <ul style="list-style-type: none"> <li>• <b>Enable</b>: The gateway automatically reverts to 20 MHz channel bandwidth when another WiFi network within 2 channels of its own channel is detected or when a client device with its 40 MHz Intolerant bit set is detected.</li> <li>• <b>Disable</b>: The gateway advertises and operates in 40 MHz mode regardless of what other networks are configured nearby.</li> </ul>
RX power chain save	Select whether to turn on power-save mode. Options are <b>Enable</b> and <b>Disable</b> .  <b>Note</b> : Before setting this parameter, set <b>802.11n/EWC</b> to <b>Auto</b> .
RX power chain save quiet time	Sets the delay time (in seconds) between when system activity ceases and power-save mode engages. Options are: <b>0 - 2147483647</b> seconds.  <b>Note</b> : Before setting this parameter, set <b>802.11n/EWC</b> to <b>Auto</b> and to <b>Enable</b> .
RX power chain save PPS	Sets a throughput threshold (in seconds) for when the router engages power-save mode after the quiet time seconds have elapsed. Options are: <b>0 - 2147483647</b> packets per second.  <b>Note</b> : Before setting this parameter, set <b>802.11n/EWC</b> to <b>Auto</b> and to <b>Enable</b> .
54g™ rate	(Optional) Select a fixed data rate if desired. Options are <b>Auto</b> , <b>1 Mbps</b> , <b>2 Mbps</b> , <b>5.5 Mbps</b> , and <b>11 Mbps</b> .  <b>The Auto setting uses 11 Mbps</b> when possible but drops (based on signal strength) when necessary.
Multicast rate	Enter the desired packet transmit rate for multicast. Options are <b>1 - 54 Mbps</b> .
Basic Rate Fragmentation Threshold	Enter the size at which packets will be fragmented into smaller units. The primary consideration for this setting is the size/capability of the circuit. Options are <b>256 - 2346</b> bytes. The default is <b>2346</b> bytes.

Field Name	Description
	A high packet error rate is an indication that a slightly increased fragmentation threshold is needed. When possible, the default value of <b>2346</b> bytes should be maintained. Poor throughput is a likely result of setting this threshold too low.
RTS Threshold	Enter the RTS (Request to Send) packet size beyond which the WLAN client hardware invokes its RTS/CTS mechanism. Smaller packets will otherwise be sent not using RTS/CTS. Options are <b>256 - 2347</b> bytes. The default is <b>2347</b> (disabled).
DTIM Interval	Enter the Delivery Traffic Indication Message (DTIM or Beacon rate) countdown variable used to indicate when the next window is available to client devices for listening to buffered broadcast and multicast messages. Options are <b>1</b> and <b>65535</b> . The default is <b>1</b> .
Beacon Interval	Enter the time interval (in milliseconds) between beacon transmissions. Beacon transmissions make known the presence of an access point and convey to wireless NICs when to awake from power save mode to check for buffered frames at the access point. Options are <b>1</b> and <b>65535</b> ms. The default is <b>100</b> ms.
Global Max Clients	Enter the maximum number of client devices that can connect to the router. Options are <b>1 - 255</b> .
Xpress™ Technology	Select whether to enable Xpress Technology. This technology is compliant with draft specifications of two planned wireless industry standards. Options are <b>Enabled</b> and <b>Disabled</b> .
Regulatory Mode	<i>(Available for SR515ac models only)</i> Select whether to enable support for <b>802.11h</b> or <b>802.11d</b> regulations. The default is <b>Disabled</b> .
Pre-Network Radar Check	<i>(Available for SR515ac models only)</i> The radar check parameter setting for traffic trying to access your gateway from outside the network. The displayed value is <b>-1</b> .
In-Network Radar Check	<i>(Available for SR515ac models only)</i> The radar check setting for traffic trying to access your gateway from inside your network. The displayed value is <b>-1</b> .
TPC Mitigation(db)	<i>(Available for SR515ac models only)</i> The TPC mitigation value in db. The default is <b>0 (off)</b> .
Transmit Power	Enter the desired output power (by percentage).
WMM (Wi-Fi Multimedia)	Select whether to enable this technology. It allows multimedia services (audio, video and voice packets) to get higher priority for transmission. Options are <b>Auto</b> , <b>Enabled</b> , and <b>Disabled</b> .
WMM No Acknowledgement	Select whether acknowledgements are sent (applied at the MAC level). Enabling this option allows better throughput but, in a noisy RF environment, higher error rates may result. Options are <b>Enabled</b> and <b>Disabled</b> .

Field Name	Description
WMM APSD	Select whether to enable Automatic Power Save Delivery, a power consumption saving feature. Options are <b>Enabled</b> and <b>Disabled</b> .
Beamforming Transmission (BFR)	<i>(Available for SR515ac models only)</i> Select to concentrate the transmission signal at the gateway location. This results in a better signal and potentially better throughput. Options are <b>Enabled</b> and <b>Disabled</b> .
Beamforming Reception (BFE)	<i>(Available for SR515ac models only)</i> Select to concentrate the transmission signal at the gateway location. Options are <b>Enabled</b> and <b>Disabled</b> .

## Station Info

On this page, you can view authenticated wireless stations and their status.

In the left navigation bar, select **Wireless** > **Station Info**. The following page appears.

Click **Refresh** to update the information.

**SMART/RG®**  
forward thinking

Device Info  
Advanced Setup  
Wireless  
Basic  
Security  
MAC Filter  
Wireless Bridge  
Advanced  
**Station Info**  
Diagnostics

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
E4:8B:7F:52:EF:61	Yes		SMARTRG	wl0

Refresh

## DIAGNOSTICS

In this section, you can run line performance tests. Three legs of the data path are included in the available tests: LAN connectivity, DSL connectivity and Internet connectivity tests.

You can also ping a host or trace a connection.

### Diagnostics

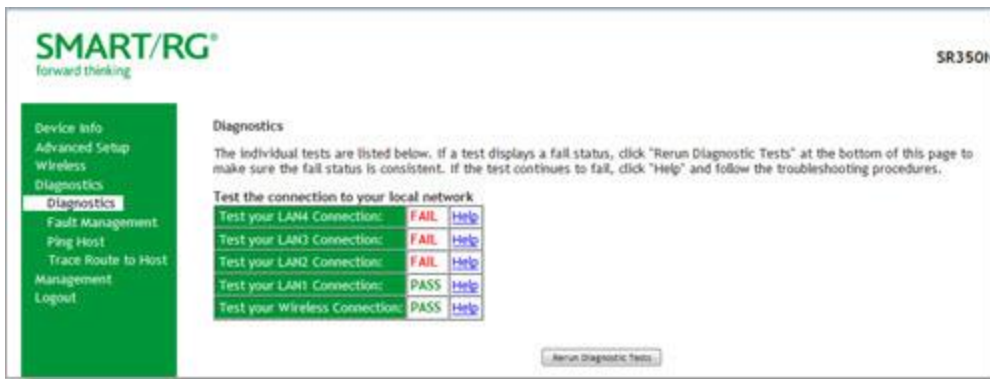
On this page, you can view information about your DSL connection.

In the left navigation bar, click [Diagnostics](#) > [Diagnostics](#) and then click [Test](#) at the bottom of the page. The normal test method is initiated, utilizing OAM F5 loopback cells.

The table is updated with fresh diagnostic information about connection integrity. To learn more about what is being tested and what actions to take in the event that a particular test should fail, click the [Help](#) link at the far right of each line item.

To test at the VP level in lieu of at an individual VC connection, click [Test With OAM F4](#).

**Note:** For SR515ac models, status is shown for both wireless bands in the [Test your Wireless Connection](#) row.



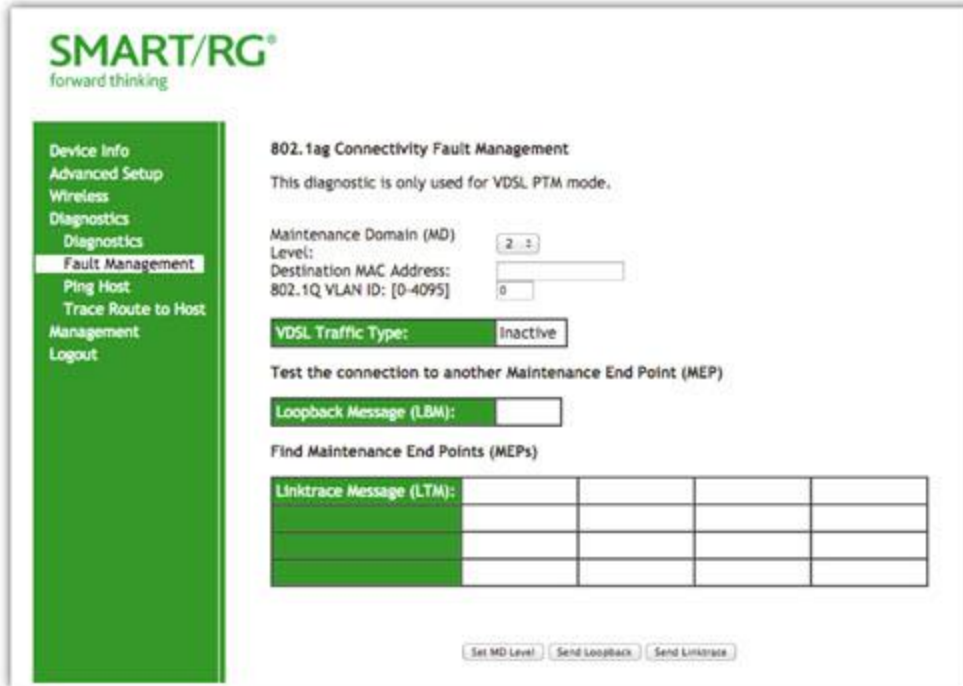
## Fault Management

On this page, you can view diagnostics regarding your VDSL PTM or Ethernet WAN connection. Fault Management is compliant with IEEE 802.1ag for Connectivity Fault Management.

**Note:** This option is not available for SR515ac models.



1. In the left navigation bar, click **Diagnostics > Fault Management**. The following page appears.



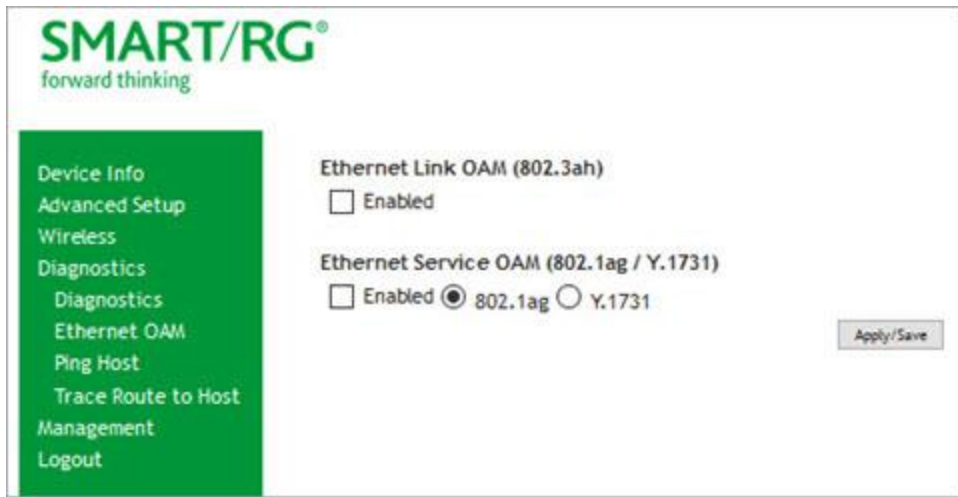
2. In the **Maintenance Domain (MD) Level** field, select the domain level that you want to view and then click **Set MD Level**. Maintenance Domains are management spaces on a network, typically owned and operated by a single entity. MDs are configured with names and levels and a hierarchical relationship exists between domains based on levels. Options are 0 - 7. The larger the domain, the higher the value you should select.
3. Enter the **Destination MAC Address**.
4. Enter any applicable **802.1Q VLAN IDs**. Options are 0 - 4095.

## Ethernet OAM

On this page, you can view diagnostics regarding your VDSL PTM or Ethernet WAN connection. Fault Management is compliant with IEEE 802.1ag for Connectivity Fault Management.

**Note:** This feature is available only for SR515ac models.

1. In the left navigation bar, click **Diagnostics > Ethernet OAM**. The following page appears.



2. Modify the fields as needed, using the information in the table below.
3. Click **Apply/Save** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
<b>Ethernet Link OAM (802.3ah) section</b>	
Ethernet Link OAM (802.3ah)	Click the <b>Enabled</b> checkbox to set options for this protocol. Additional fields appear.
WAN Interface	Select the WAN interface that you want tested.
OAM ID	Enter the ID of this OAM configuration. Only positive numbers are allowed..
Auto Event	Select whether to create event log entries automatically.
Variable Retrieval	Select to enable on-demand link diagnostics, including bit-error-rate approximation.
Link Events	Select to enable reporting of critical conditions that may cause link failure.
Remote Loopback	Select to enable on-demand link diagnostics, including bit-error-rate approximation.
Active Mode	Click to enable this feature.
<b>Ethernet Service OAM (802.1ag/Y.1731) section</b>	
Ethernet Service OAM (802.1ag/Y.1731)	Click the <b>Enabled</b> checkbox and then click <b>802.1ag</b> or <b>Y.1731</b> to set options for this protocol. Additional fields appear.
WAN Interface	Select the WAN interface that you want tested.
MD Level	<i>(Appears for the 802.1ag option only)</i> Select the domain level for this maintenance domain. Options are <b>0 - 7</b> . The larger the domain, the higher the value you should select.

Field Name	Description
MD Name	(Appears for the 802.1ag option only) Enter the name of the maintenance domain, e.g., Broadcom.
MA ID	(Appears for the 802.1ag option only) Enter the MA ID, e.g., BRCM.
MEG Level	(Appears for the Y.1731 option only) Enter the MEG level for this service.
MEG ID	(Appears for the Y.1731 option only) Enter the MEG ID for this service.
Local MEP ID	Enter the ID of the local MEP. Options are <b>1 - 8191</b> .
Local MEP VLAN ID	Enter the ID of the VLAN for the local MEP. Options are <b>1 - 4094</b> . The default is <b>-1</b> (no VLAN tag).
CCM Transmission	Select to enable CCM transmission.
Remote MEP ID	Enter the ID of the remote MEP. Options are <b>1 - 8191</b> . The default is <b>-1</b> (no remote MEP).
<b>Loopback and Linktrace Test</b> section	
Target MAC	Enter the MAC address for the test, e.g., 02:10:18:aa:bb:cc.
Linktrace TTL	Enter the maximum number of hops allowed. Options are <b>1- 233</b> . The default is <b>-1</b> (no hop limit).
Loopback Result	The results of the loopback test.
Linktrace Result	The results of the linktrace test.

## Ping

On this page you can ping a server by host name or IP address.

1. In the left navigation menu, click **Diagnostics Tools > Ping**. The following page appears.



2. Enter the host name or IP address.
3. Click **Submit**. The details of the ping appear on the page.

## Trace Route to Host

On this page, you can use the Trace Route utility to trace a connection.

1. In the left navigation menu, click **Diagnostics Tools > Trace Route to Host**. The following page appears.



2. Enter the host name or IP address that you want to trace.
3. Click **Submit** (or for the SR515ac, click **Trace Route to Host**). The details of the trace appear on the page.

## Management

In this section, you can manage configuration files, access control, management server configurations, SNMP Agent settings, and work with event logs.

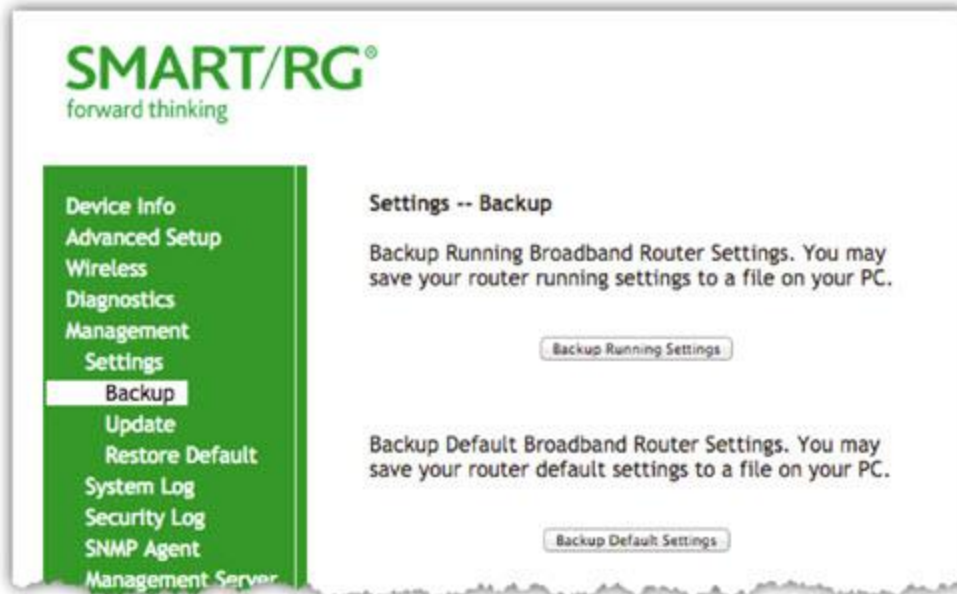
### Settings

In this section, you can back up the current settings, restore saved settings, or reset the gateway to default settings.

### Backup

You can back up the current settings for your gateway to a file stored on your computer.

1. In the left navigation bar, click **Management > Settings > Backup**. The following page appears.



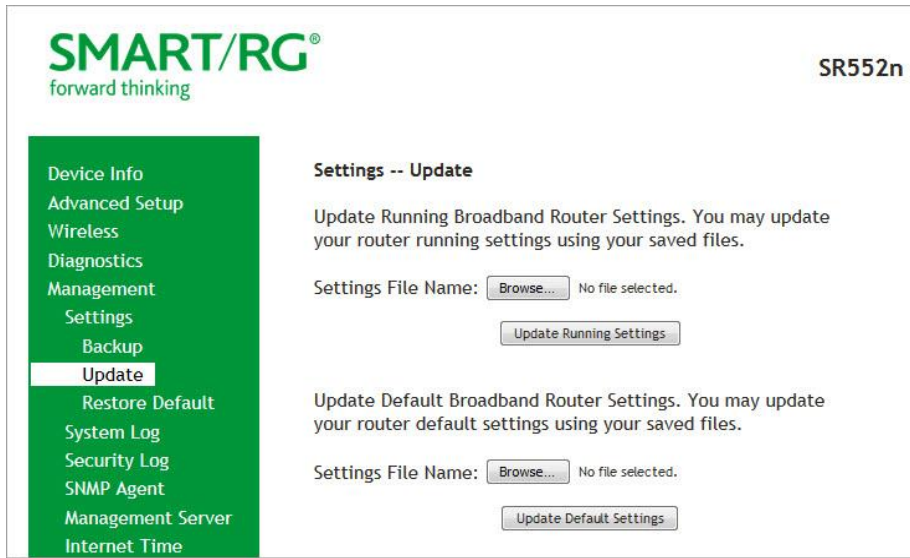
2. To save a backup file of the currently running settings to a local drive, click **Backup Running Settings**. The open/save dialog box appears. Click **OK**. The backupsettings.conf file is created in your default download location.
3. To save a backup file of the default settings to a local drive, click **Backup Default Settings**. The open/save dialog box appears. Click **OK**. The backupdefaultsettings.conf file is created in your default download location.

**Note:** If you plan to create backups frequently, you may want to rename the backup files by appending dates to the filename. Otherwise, every new backup file overwrites the existing backup file.

## Update

On this page, you can restore previously backed-up gateway settings. Both Current and Default settings can be managed here.

1. In the left navigation bar, click **Management > Settings > Update**. The following page appears.

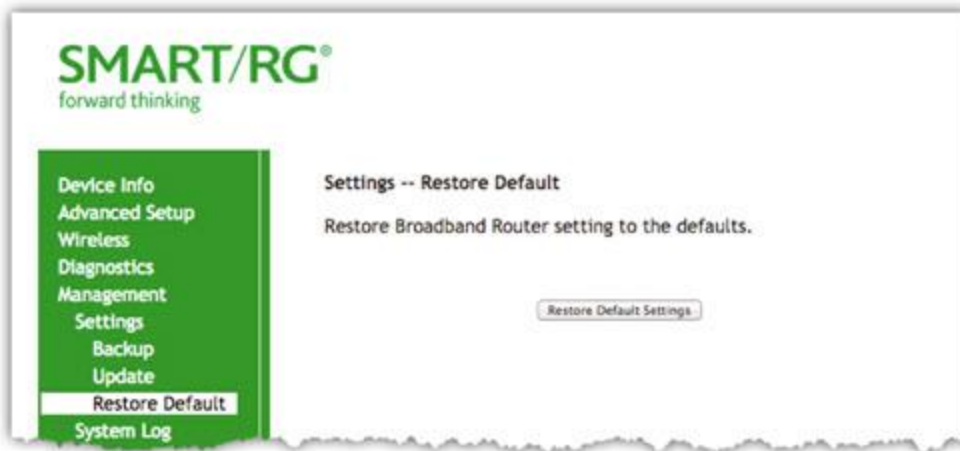


2. Click the **Browse** button for the type of setting you wish to restore.
3. Locate the desired .conf file on your local system and click **Open**.
4. Click the appropriate **Update** button.  
The gateway reboots when the update has completed.

## Restore Default

On this page, you can reset the gateway to its default settings which can be the factory defaults or defaults that you customized and stored. For details, see "[Restore Default](#)" and "[Restore Default](#)" sections above.

1. In the left navigation bar, click **Management > Settings > Restore Default**. The following page appears.
2. Click **Restore Default Settings**. The gateway is rebooted.



## System Log

On this page you can view and configure the system log generated for your gateway.

1. In the left navigation bar, click **Management** > **System Log**. The following page appears.





- To view the contents of the system log, click [View System Log](#). The System Log details page appears.

Date/Time	Facility	Severity	Message
Jan 1 00:00:28	daemon	err	syslog: caTmBlk:Time Blocking: Shutting down, sig -1
Jan 1 00:00:29	daemon	crit	kernel: eth3 (switch port: 4) Link UP 1000 mbps full duplex
Jan 1 00:00:59	daemon	err	syslog: CDM:caCdmPolForMessages: unrecognized msg 0x10000250
Jan 1 00:10:44	daemon	err	syslog: httpd:644.295:cgiValidateSessionKey:2356:failed session key check. Got 2135380610, expected 658209780, age=0 max=600000
Jan 1 00:13:10	daemon	err	syslog: httpd:790.530:cgiValidateSessionKey:2356:failed session key check. Got 685698293, expected 1511422544, age=0 max=600000
Jan 1 00:15:59	daemon	crit	kernel: Line 1: xDSL G.994 training
Jan 1 00:16:02	daemon	crit	kernel: Line 1: ADSL link down
Jan 1 00:26:14	daemon	crit	kernel: Line 0: xDSL G.994 training

- To update the displayed entries, click [Refresh](#).
- To modify the system log settings:
  - Click [Configure System Log](#). The System Log - Configuration page appears.

**SMART/RG®**  
forward thinking

SR552n

**System Log -- Configuration**

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

b. Modify the settings as needed.

The following table describes the options for configuration of the system log.

Action	Description
Enable/Disable	Select to turn logging off or on.
Logging Level	Select <b>Error</b> unless actively troubleshooting a situation with a subscriber for which increased log detail is required. Options are <b>Emergency</b> , <b>Alert</b> , <b>Critical</b> , <b>Error</b> , <b>Notice</b> , <b>Warning</b> , <b>Informational</b> , and <b>Debugging</b> . The options are listed in top-down order. The default is <b>Debugging</b> .
Display Level	Select <b>Error</b> unless actively troubleshooting a situation with a subscriber for which increased detail is required. This field has the same options as the <b>Logging Level</b> field.
Mode	Controls where log events will be sent.  To send logs to the specified IP address and UDP port of a remote syslog server, select <b>Remote</b> or <b>Both</b> .  To record events in the local memory of your SmartRG gateway, select <b>Local</b> or <b>Both</b> .

c. Click **Apply/Save** to save your changes.

## Security Log

The security log contains a history of events related to sensitive access to the gateway. Logged events include:

- Password change success
- Password change failure
- Authorized login success
- Authorized login fail
- Authorized user logged out
- Security lockout added
- Security lockout removed
- Authorized resource access
- Unauthorized resource access
- Software update

1. In the left navigation bar, click **Management > Security Log**. The following page appears.



2. Do any of the following:
  - To view the log, click **View**.
  - To purge the log entries and start fresh, click **Reset**. A confirmation message appears. Click **Close**.
  - To export the log to a local drive, click the **here** link in the last line of the instructions on the page. The log appears in the browser window. You can save the page or select all of the log text, paste into a Notepad window and save the file.

## *SNMP Agent*

On this page, you can configure the SNMP (Simple Network Management Protocol) settings to retrieve statistics from the SNMP agent for the gateway. You can enable or disable the SNMP agent and set parameters such as the read community, system name and trap manager IP.

1. In the left navigation bar, click **Management > SNMP Agent**. The following page appears.



2. Modify the fields as needed.
3. Click **Save/Apply** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
Read Community	The options are public and private. The default is <b>public</b> .
Set Community	The options are public and private. The default is <b>private</b> .
System Name	The name of the system.
System Location	<i>(Optional)</i> The location of the system.
System Contact	The contact for the system.
Trap Manager IP	The IP address where the trap manager is installed.

## Management Server

A management server is an Auto Configuration Server (ACS) such as Cisco Prime Home which offers significant advantages in terms of automation and productivity when managing subscriber devices in the field.

In this section, you can configure ACS settings for the TR-069 client and configure STUN server settings.

### TR-069 Client

On this page, you can configure the gateway with details about the management ACS to which this gateway will be linked.

SmartRG gateways support TR-069-based standards for remote management. The TR-069 client page is preset with default connection parameters and generally only needs to be enabled, pointed to the ACS URL, and any required ACS credentials entered.

SmartRG products can accommodate several ACS products, including:

- Cisco Prime Home
- ClearVision
- Calix Consumer ACS

A minimum firmware level of v2.5.0.x is required.

If you need to modify the request defaults, consult the ACS manufacturer's documentation.

1. In the left navigation bar, click **Management > Management Server > TR-069 Management**. The following page appears.

2. Update or complete the necessary fields per the instructions from your ACS platform vendor.
3. Click **Apply/Save** to commit your changes.

**Note:** This manual does not cover the setup of your ACS. Consult the materials provided by your ACS vendor to determine the appropriate parameters and server settings for configuring remote WAN side management via an ACS using the TR-069 Protocol.

The fields on this page are explained in the following table.

**Note:** Please consult with your ACS vendor for any specific connection request requirements impacted by the following settings.

Field Name	Description
OUI-Serial	<p>Select whether to use the base MAC address or the serial number of your gateway when connecting to the ACS. This value may display in an ACS user interface when looking at the device details of a particular gateway.</p> <p><i>(Optional)</i> For SmartRG gateways using firmware version 2.5.0.2 and above, select <b>Serial Number</b>.</p> <p><b>MAC</b> (MAC address) is the default for this field and the most typical scenario. For firmware versions prior to 2.5.0.2, MAC is the only available option.</p>
TR-069 Client	<p>Enable or disable the TR-069 client on the CPE. You can disable the TR-069 WAN Management Client if no ACS is employed.</p> <p><b>Note:</b> If you may want to add an ACS to your infrastructure in the future, it is recommended to leave this option enabled. When this feature is disabled, every gateway deployed with this setting must be manually/locally re-configured to enable this client if needed later.</p>
ACS URL from DHCP	<p><i>(Available for SR515ac models only)</i> Click the <b>Enabled</b> checkbox to enable your gateway to obtain the ACS URL via DHCP.</p>
Inform Interval	<p>The frequency (in seconds) with which the CPE (gateway) checks in with the ACS to sync and exchange data. A typical production environment entails CPEs in the field informing to the ACS once/day or every 86,400 seconds.</p>
ACS URL	<p>Enter the URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter <b>MUST</b> be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificatebased authentication.</p> <p>You can include a port specification suffix if your ACS platform requires it, e.g., http://customer.acs.wanmanagementservices.com:30005 where 30005 is the port number. The default port is <b>30005</b>.</p> <p>A minimum firmware level of v2.5.0.x is required.</p>
ACS User Name	<p>Enter the user name by which this gateway logs in to the ACS. The default username is typically admin.</p>

Field Name	Description
ACS Password	Enter the password to authenticate the above user name. The default password is typically admin.
TR-069 Client Port	<i>(Available for SR515ac models only)</i> Enter the TR-069 port number.
WAN Interface used by TR-069 client	Select any WAN, LAN, Loop back or a configured connection to declare how this gateway will connect to the ACS.

4. (Optional) You can configure the modem client Connection Request mechanism used by your ACS for communication with subscriber gateways.

Field Name	Description
Connection Request Authentication	Select this option if your ACS requires authenticated connection requests. Complete the additional credential fields that are exposed.
Connection Request Username	Enter the user name by which this gateway authenticates the ACS. Contact your ACS provider for this information.
Connection Request Password	Enter the password by which this gateway will authenticate to the ACS. Contact your ACS provider for this information.
Connection Request URL	There is typically no need to set the Connection Request URL as it is normally established automatically based on the effective WAN IP. In some cases, the port can be configured as needed. An example value for this field might be "http://xxx.xxx.xxx.xxx:30005/" where the xxx values are specific WAN IP octet numbers.  <b>Note:</b> The default port value is 30005.  This may need to be configured for interoperability with your ACS vendor. If so, consult with SmartRG.

5. To force the gateway to attempt to sync with the ACS, click the **GetRPCMethods** button. This will assist you in verifying the TR-069 parameters entered above.

## STUN Config

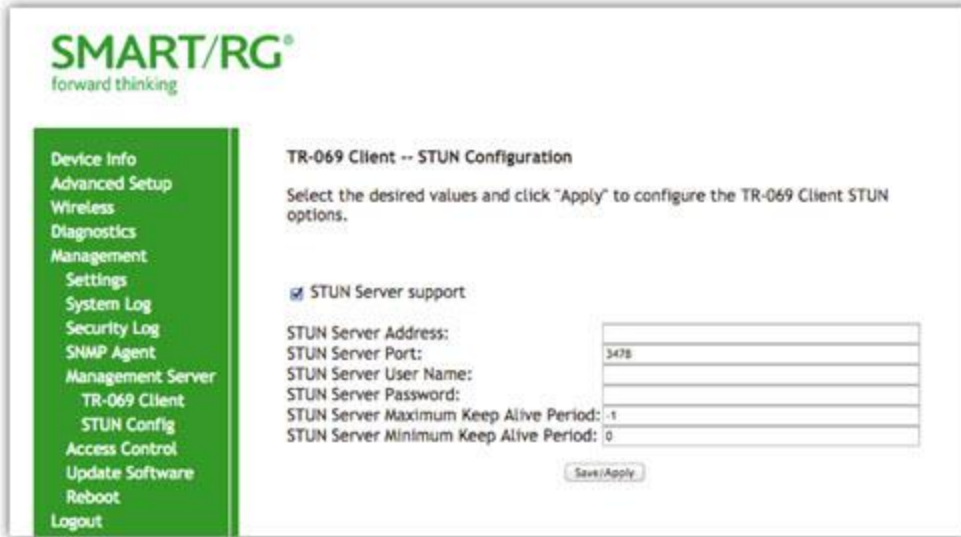
STUN stands for "Simple Traversal of UDP through NATs". STUN enables a device to find out its public IP address and the type of NAT service it is sitting behind.

STUN is most commonly used with older modems under ACS management connected via a NAT gateway. NAT accommodates a LAN-side device that has been allocated a Private IP address such as a CPE device on a private network behind an ONT. In this instance, the regular CWMP Connection Request mechanism to talk to the modem gateway cannot be used to initiate a session with that ACS.

A STUN server receives STUN requests and sends STUN responses. STUN servers are generally attached to the public Internet.

On this page, when a STUN server is present within the infrastructure of the Service Provider, you can configure this gateway with the connectivity specifics for that server.

1. In the left navigation bar, click **Management** > **Management Server** > **STUN Config**. The following page appears.



2. To view the required STUN settings, click **STUN Server Support**.
3. Complete each field in accordance with the implementation specifics of your server.
4. Click **Save/Apply** to commit your changes.

The fields on this page are explained in the following table.

Field Name	Description
STUN Server Address	The physical STUN server's assigned network address. An invalid address will produce an immediate on-page error message from the gateway. You can enter a maximum of 256 characters  An ACS server may also have STUN functionality running on the same physical box. Consult your ACS vendor for implementation options and also TR-069 protocol documentation, if necessary.
STUN Server Port	Set the port number associated with your STUN server infrastructure. Options are 0 - 64435. The default is 3478.
STUN Server User Name	The username by which the gateway accesses the STUN infrastructure. Maximum length is 256 characters. Special characters are valid. The value will be hidden.
STUN Server Password	The password by which the modem authenticates the above username to the STUN infrastructure. Maximum length is 256 characters. Special characters are valid. The value will be



Field Name	Description
	hidden.
STUN Server Maximum Keep Alive Period *	[0-Unlimited] Value is time in seconds. Default = -1 which specifies that there will be NO keep-alive period maximum limit.
STUN Server Minimum Keep Alive Period *	[0-Unlimited] Value is time in seconds. Default = 0 seconds.

\* This mechanism is used in coordination with the refreshing of NAT bindings. Specifically, in conjunction with use of Restricted Cone NAT or Port Restricted Cone NAT (as may be configured in some gateways). A device's internal address / port mappings, which the STUN protocol is allowed to make use of, can have keep alive values attributed. These minimum and maximum keep alive times define respectively, the minimum time to retain the mapping information STUN has discovered, and the maximum time to retain that information, before refreshing it through forced re-discovery.

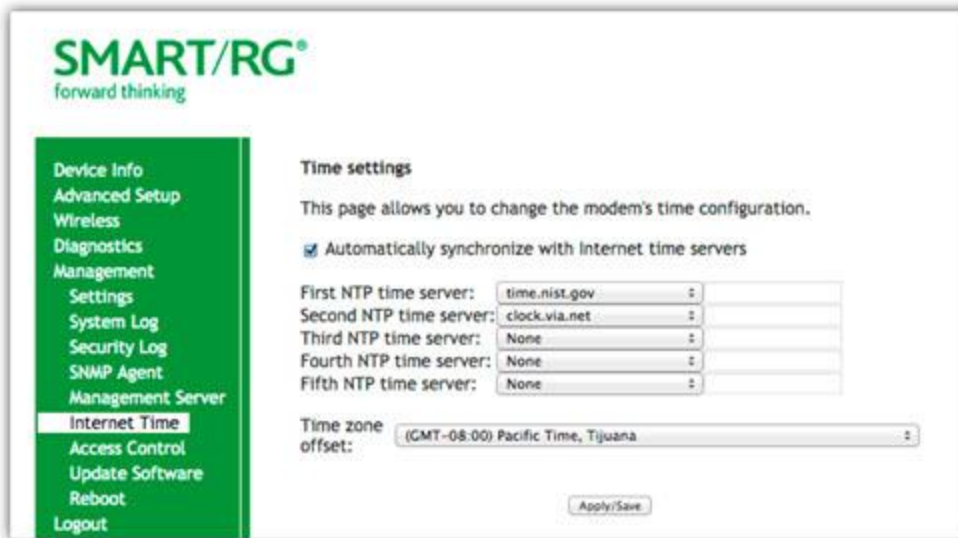
With the above-mentioned NAT schemes, it is possible the network address translation initially established may not be used after a specified elapsed time. Such internal mapping is dropped. The gateway will then assign a different address mapping. This mechanism within the STUN protocol allows for coordinated refresh on the bindings for mappings it uses. For further information, review STUN-related RFCs.

Selecting appropriate values for these two fields are influenced by a variety of environmental factors including devices types deployed, services employed and NAT configuration options enabled within the topology.

## *Internet Time*

On this page, you can synchronize the clock in your gateway with reliable external clocking servers available on the Internet.

1. In the left navigation bar, click **Management > Internet Time**. The following page appears.



2. Click **Automatically synchronize with Internet time server**. A list of server fields and the Time Zone offset field appear.
3. Select servers from the list or enter your own NTP servers.
4. Select the desired time zone for the gateway.
5. Click **Apply/Save** to commit your settings.

## Access Control

On this page you can manage access to your gateway and network. Depending on the model, you may be able to configure passwords, accounts, services, the logout timer, and/or access lists. Not all features are available on all models.

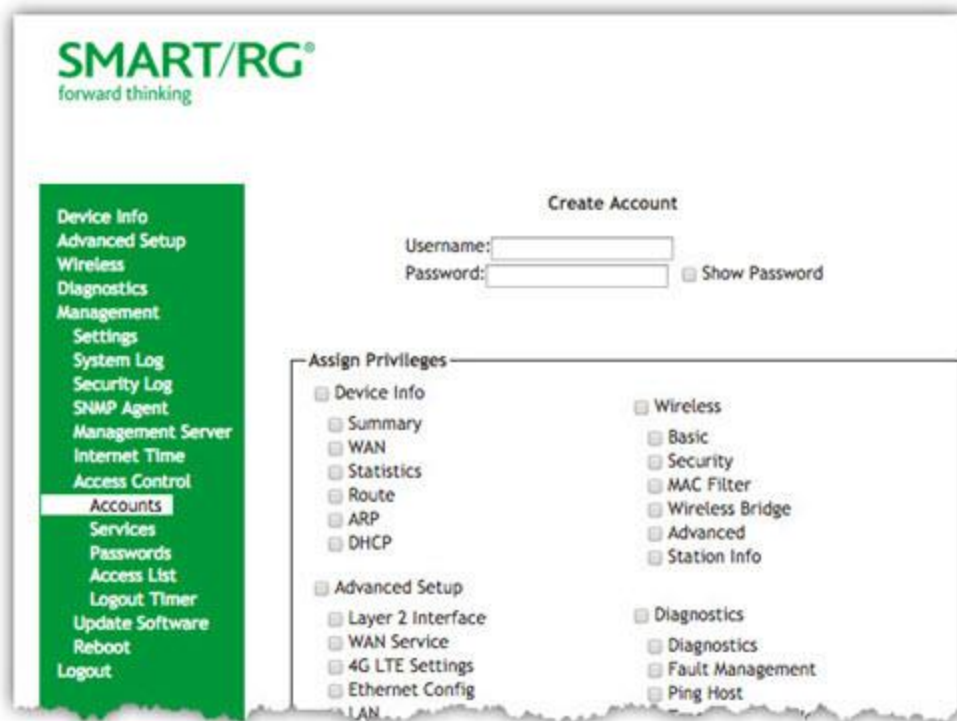
### Accounts

On this page, you can create and manage user accounts for your gateway. Your gateway can support multiple login accounts for its on-board user interface. Each account can be customized to grant access privileges to specific pages in the interface. This is particularly useful when an ISP wishes to limit access for subscribers, yet grant full access for technical support and on-site installation personnel.

**Note:** This feature requires firmware v2.5.0.7 or later.

#### Add an Account

1. In the left navigation bar, click **Management > Access Control > Accounts**.
2. To set up a new user, click **Create Account**. The following page appears.



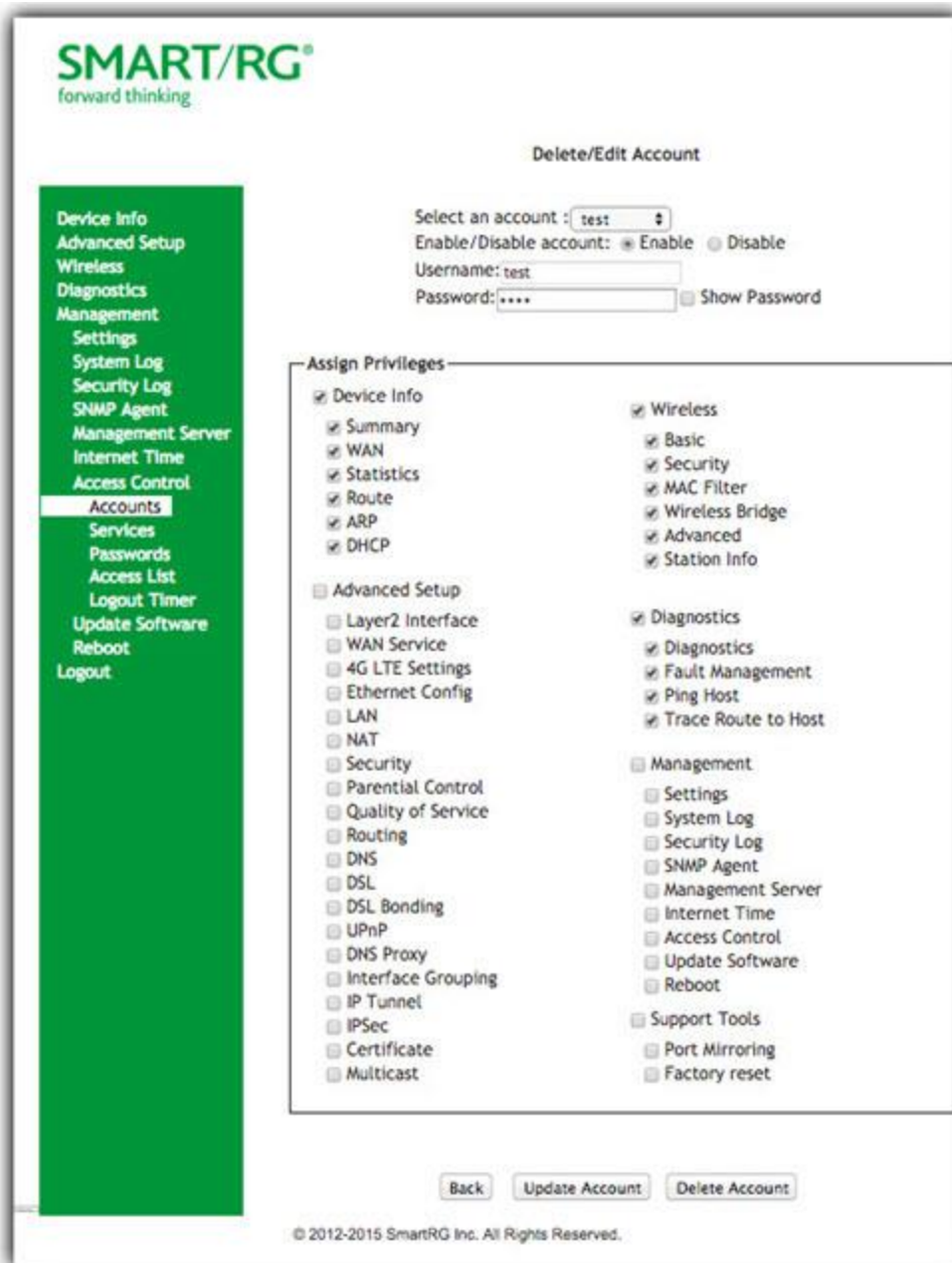
3. Enter a **Username** and **Password** for the new account.
4. Select the features that you want this user to access. If you select a subcategory, the subordinate boxes are also selected.
5. Click **Save Account** to commit your changes. The new account is created. To test the account credentials, log out of the interface and then log back in using the new account.

## Modify or Delete an Account

**Note:** You can NOT modify or delete the default user accounts (Admin, Support, MFG, or User) but you can disable the **Support**, **MFG**, or **User** accounts.

You must be logged into the gateway as the Admin or Support user to modify or delete any accounts.

1. In the left navigation bar, click **Management > Access Control > Accounts** and then click, **Delete/Modify Account**. The Delete/Edit Account page appears.



2. In the **Select an account** field, select the account you wish to modify or delete.
3. Do one of the following:
  - a. To modify an account, check or clear the desired boxes and then click **Update Account** to commit your changes.
  - b. To delete an account, scroll to the bottom of the page and click **Delete Account** to remove the account.
  - c. To disable or enable an account, click the **Enable/Disable account** buttons.

Your changes are implemented immediately.

## Default Passwords

USER	PASSWORD
admin	admin
support	support
user	user
mfg	IDH7iw@ibRsPOIBa

## Services

On this page, you can define a Service Control List to control which services (FTP, HTTP, Telnet, etc.) are restricted on the LAN.

1. In the left navigation bar, click **Management > Access Control > Services**. The following page appears.

**SMART/RG®**  
forward thinking

Device Info  
Advanced Setup  
Wireless  
Diagnostics  
Management  
Settings  
System Log  
Security Log  
SNMP Agent  
Management Server  
Access Control  
**Services**  
Passwords  
Access List  
Logout Timer  
Update Software  
Reboot  
Logout

**Access Control -- Services**

A Service Control List ("SCL") is used to enable or disable network services on the gateway.  
Note: LAN side firewall must be enabled to modify LAN SCLs.

Services	LAN
HTTP(S)	<input checked="" type="checkbox"/> Enable
<input type="checkbox"/> Use encrypted HTTP(S) -- unit will restart.	
FTP	<input checked="" type="checkbox"/> Enable
ICMP	Enable
SNMP	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable

Save/Apply

2. Modify settings as desired.
3. Click **Save/Apply** to commit your settings.

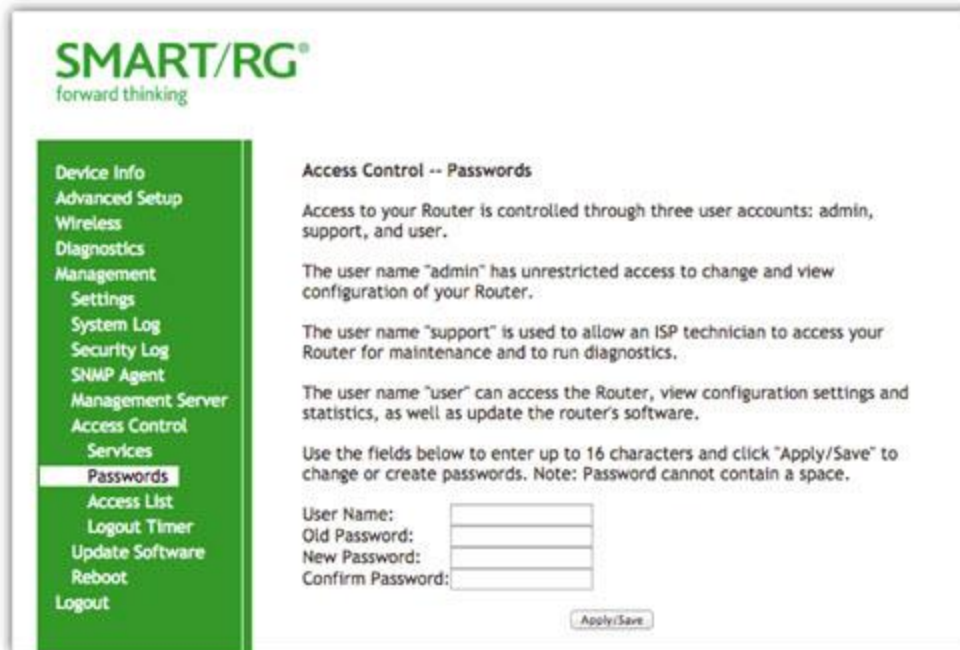
The fields on this page are explained in the following table.

Field Name	Description
Services	This column identifies the SCL services that can be enabled or disabled. Options are: <b>FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP.</b>
Use encrypted HTTP(S)	Click this checkbox to implement secured HTTP.  <b>Warning:</b> When you click this option, the gateway reboots.
LAN	Select the service enabled on LAN side firewall. Depending on configuration settings made elsewhere in the GUI, this column may be read-only.  <b>Note:</b> ICMP is an always-enabled service by default and has no checkbox.
WAN	Select the service enabled on the WAN side firewall.
WAN Port Number	The port the access control applies to on the WAN side for the given service. See port information below.
<b>Service port</b> options	
FTP	FTP Service access (For WAN, this is default port).
HTTP	HTTP Service access (For WAN, this is in association with specified port (default is port 80).
ICMP	ICMP Service access (For WAN, this is default port).
SNMP	SNMP Service access (For WAN, this is default port).
SSH	SSH Service access (For WAN, this is in association with specified port (default is port 22).
TELNET	TELNET Service access (For WAN, this is default port).
TFTP	TFTP Service Access (as with default port)!!! ASKSME to review contenet in parentheses.

## Passwords

On this page, you can create or change passwords associated with access to the gateway. Three accounts are available to manage: Admin, Support and User.

1. In the left navigation bar, click **Management > Access Control > Passwords**. The following page appears.



2. Enter the information for the logged-in account.
3. Click **Apply/Save** to commit your settings.

The fields on this page are explained in the following table.

Field Name	Description
User Name	Specifies name of account to be configured. Options are <b>admin</b> , <b>support</b> , <b>user</b> .
Old Password	Enter the current password for the entered User Name.
New Password	Enter the new password for the entered User Name. A maximum of 16 characters is allowed.
Confirm Password	Re-enter the new password.

## Access List

On this page, you can create and manage access control lists to control inbound access to specific IP addresses.

**Note:** This feature is available only for SR515ac models.

1. In the left navigation bar, click **Management > Access Control > Access List**. The following page appears showing any addresses already configured for managed access.



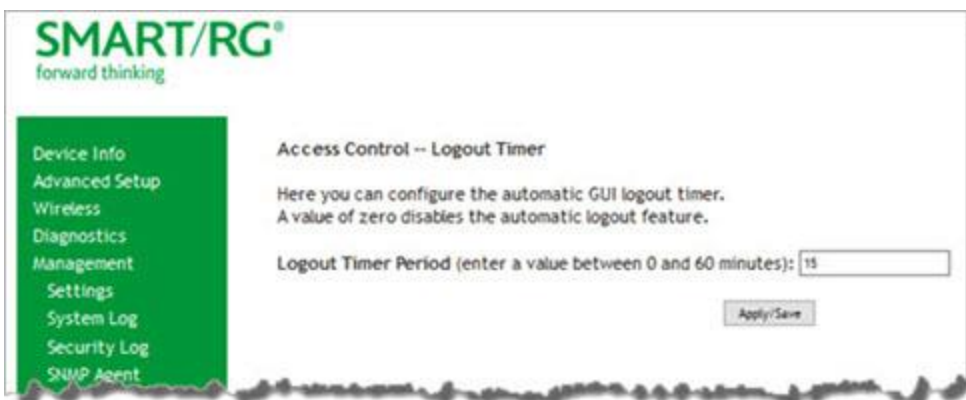
2. To add an address:
  - a. Click **Add**.
  - b. Enter the address for which you want to restrict access.
  - c. Click **Apply/Save**. You are returned to the Management Access Lists page.
  - d. To add up to 9 more addresses, repeat steps 2a - 2c.
3. To remove an address, click the **Remove** checkbox next to it and then click **Remove**. The list is updated.

## Logout Timer

On this page, you can define the maximum time that a session can remain open before the gateway logs out.

**Note:** This feature is available only for SR515ac models.

1. In the left navigation bar, click **Management > Access Control > Logout Timer**. The following page appears.



2. In the **Logout Timer Period** field, type the number of minutes after which a session will be ended. Options are **0 - 60** minutes. The default is **15** minutes. To disable this feature, enter a zero (**0**) in the field.



## Update Software

On this page, you can update the firmware of your SmartRG gateway. Software updates for SmartRG products are available for download by direct customers of SmartRG via the SmartRG Customer Portal.

1. In the left navigation bar, click **Management > Update Software**. The following page appears.

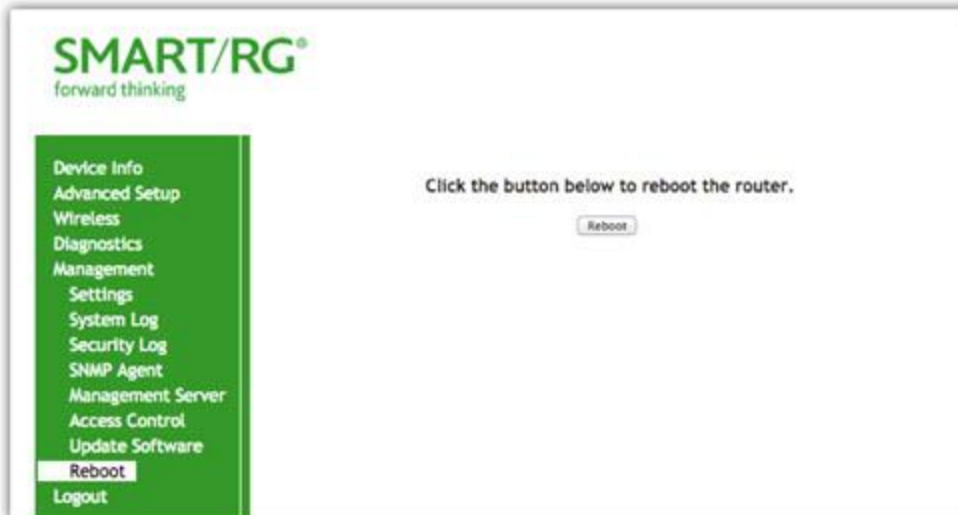


2. Follow the on-page instructions. When the update has completed, the gateway reboots.

## Reboot

Occasionally, troubleshooting measures may require that the gateway be rebooted. On this page, you can reboot your gateway.

1. In the left navigation bar, select **Management** > **Reboot**. The following page appears.



2. Click **Reboot**. Your gateway is rebooted and you must log in again if you want to make further changes.

## APPENDIX A: ADVANCED FEATURES

This appendix outlines the advanced features of SmartRG brand home gateway products.

### *Connect-and-Surf (Automatic Broadband Connection Configuration)*

The Connect-and-Surf feature automatically establishes a WAN connection for default-configured gateways obviating the need for manual or custom configurations. The active physical layer is detected (ADSL, VDSL or GigE) and layer 3 connectivity is established using PPP authentication or DHCP.

**Note:** If you prefer to configure your gateway's WAN interface manually, connect a laptop to any of the LAN ports and follow the instructions in the [Logging in to Your SmartRG Gateway](#) and [Management Server](#) sections of this User Manual. Do not connect the WAN interface cable until after the configuration is completed.

### *Activation (Automatic ACS Connection Configuration)*

SmartRG gateways are designed to discover their service provider-specific ACS management settings without custom firmware. We maintain an activation server that associates a device's MAC address with its service provider's ACS settings. Our gateways contact the activation server to have their ACS settings modified on initial power up (or after being reset to factory default settings).



**Note:** Activation server support is provided for ALL SmartRG gateways at no additional cost. SmartRG Inc. enters gateway MAC addresses into the activation server prior to shipment.

### *TR-069 Remote Management: ACS Support*


With a rich TR-069 heritage and a strong commitment to standards based, remote management, SmartRG gateways are designed for maximum interoperability with industry leading, TR-069-based remote management systems. Our gateways provide maximum remote manageability and the highest level of visibility into the connected home yielding:

- Shorter integration times
- Improved customer support
- Lower system integration costs
- Reduced operational expenses

SmartRG works closely with industry-leading, TR-069 automated configuration server (ACS) solution providers (such as those shown below) to ensure "plug-n-play" interoperability

	<p>Calix Compass/ Consumer Connect ACS</p>	<p>In addition to being Calix physical layer certified (to ensure Calix access equipment compatibility), SmartRG gateways have been tested to confirm maximum interoperability with the Calix Compass/Consumer Connect ACS solution.</p>
	<p>Affinegy ACS</p>	<p>SmartRG gateways have been tested to confirm maximum interoperability with the Affinegy</p>

# SMART/RG

		ACS solution.
	Cisco Prime Home™ ACS	SmartRG gateways have a long history of Prime Home (formerly ClearVision) ACS interoperability.

## APPENDIX B: FEATURE COMPARISON MATRIX

SmartRG residential gateways combine WAN connectivity with a firewall-protected router and industry-leading TR-069 remote management support. Most variants provide 802.11n Wi-Fi connectivity, as well. See the model-specific details below.

Model	Broadband Connection	LAN ports	LAN Device Discovery	Managed Firewall	Managed Wi-Fi	Wi-Fi Signal Monitor	IPv6	IPTV Ready
SR552n	Tri-mode: ADSL2+, VDSL2, GigE	5 GE	✓	✓	802.11n	✓	✓	✓
SR550n	Tri-mode: ADSL2+, VDSL2, GigE	3 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR515ac	Tri-mode: ADSL2+, VDSL2, GigE	4 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR512nm	Tri-mode: ADSL2+, VDSL2, GigE	4 FE + 1 GE + Coax	✓	✓	802.11n	✓	✓	✓
SR510n	Tri-mode: ADSL2+, VDSL2, GigE	4 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR505n	Tri-mode: ADSL2+, VDSL2, GigE	3 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR500n	Tri-mode: ADSL2+, VDSL2, GigE	4 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR400ac	Gigabit Ethernet	5 GE	✓	✓	Dual-band concurrent 802.11ac	✓	✓	✓
SR360n	ADSL2+, Ethernet	4 FE	✓	✓	802.11n	✓	✓	✓
SR350N	ADSL2+	4 FE	✓	✓	802.11n	✓	✓	✓

Model	Broadband Connection	LAN ports	LAN Device Discovery	Managed Firewall	Managed Wi-Fi	Wi-Fi Signal Monitor	IPv6	IPTV Ready
SR350NE	Ethernet	4 FE	✓	✓	802.11n	✓	✓	✓
SR100	ADSL2+	4 FE	✓	✓				
SR10	ADSL2+	1 FE	✓	✓				

For more information, contact SmartRG Support.

## Q&A

Q: Why are all the indicators off?

A: Check the following:

- The connection between the power adapter and the power socket.
- The status of the power switch.

Q: Why is the LAN indicator off?

A: Check the following:

- The connection between the ADSL gateway and your computer, hub, or switch.
- The running status of your PC, hub, or switch.

Q: Why is the DSL indicator off?

A: Check the connection between the "DSL" port of gateway and the wall jack.

Q: Why does Internet access fail while the DSL indicator is on?

A: Check whether the VPI, VCI, user name, and password are correctly entered.

Q: Why can't I access the web configuration page of the DSL gateway?

A: Choose Start > Run from the desktop, and ping 192.168.1.1 (IP address of the DSL gateway). If the DSL gateway is not reachable, check the type of the network cable, the connection between the DSL gateway and the PC, and the TCP/IP configuration of the PC.

Q: How can I reload the default settings after an incorrect configuration?

A: To restore the factory default settings, turn on the device, and press the reset button for about 1 second, and then release it. The default IP address and the subnet mask of the DSL gateway are 192.168.1.1 and 255.255.255.0, respectively.

- User/password of super user: admin/admin
- User/password of common user: user/user

## REVISION HISTORY

REV	DATE	CHANGES
3.5	6/28/2016	<ul style="list-style-type: none"> <li>Update FCC information; no substantive changes to content.</li> </ul>
3.5	4/26/2016	<ul style="list-style-type: none"> <li>Added information about SR512nm gateway (MoCA feature) and the SR515ac gateway.</li> <li>Updated screen captures and related descriptions.</li> <li>Further standardized wording &amp; formatting.</li> </ul>
3.4	6/20/2015	<ul style="list-style-type: none"> <li>Updated behavior description for the reset button for FW v2.5.0.7</li> <li>Clarified WLAN button operation with press and hold durations</li> <li>Expanded the field definitions for xDSL Statistics page</li> <li>Expanded the definition for the MTU Size field added to the PPP Usernam and Password page</li> <li>Added section for Access Control (new feature in FW v2.5.0.7)</li> <li>Corrected the table content for the fields seen on the NAT page found in the IPoE WAN interface workflow</li> <li>Miscellaneous formatting and content corrections</li> <li>Implemented image compression to reduce .pdf file size</li> </ul>
3.3	1/28/2015	<ul style="list-style-type: none"> <li>Cosmetic enhancements.</li> <li>Replaced page shots with new UI color scheme and logos.</li> <li>Expanded coverage of Advanced Setup &gt; WAN Service</li> <li>General edit</li> </ul>
3.2	10/20/2014	<ul style="list-style-type: none"> <li>Visual overhaul. New colors, logo and layout</li> <li>Added missing sections for Ethernet Config and LAN</li> <li>Expanded chapters for Management Server and STUN</li> </ul>
3.0	6/26/2014	<ul style="list-style-type: none"> <li>Complete re-write with new layout</li> <li>Authored complete field-by-field descriptions for each page</li> <li>Complete compendium of page-shots for each feature</li> <li>Migrated use cases to on-line knowledge base. (See the SmartRG Customer Portal.)</li> </ul>