SMART/RG

/ GATEWAY USER MANUAL

Model: SR506n

Release 1.0

November 2016

TABLE OF CONTENTS

SMART/RG

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

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.

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. 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.

FCC Information

See Appendix C: FCC_Statements.

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 inter-operable 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.

Purpose & Scope

The purpose and scope of this document is to provide SmartRG customers with installation, configuration and monitoring information for the SR506n CPE.

Intended Audience

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 descriptions of the SR506n gateway's lights, ports, and buttons.

LED Status Indicators

Your SmartRG gateway has several indicator lights (LEDs) on its exterior. The LED indicators are described below (from left to right).

INDICATOR	ACTION	DESCRIPTION
Power	●	Device is powered on and operating normally.
	☀	Software is syncing.
	○	The device is powered off.
DSL	●	DSL link is established.
	☀	The DSL line is training.
	○	The device is powered off.
Internet	●	Internet link is established.
	☀	Data is being transmitted.
	○	Internet interface is disconnected.
	●	Authentication has failed.
LAN 1-4	●	Ethernet interface is connected.
	☀	Data is being transmitted.
	○	Ethernet interface is disconnected.
USB	●	The connection of 3G or USB flash disk has established. !!! TW: Bug RB-2380 open on this LED's function. Check for resolution before publishing.
	☀	Data is being transmitted.
	○	No signal is detected.

Connections

Below is an illustration of the connectors located on the back of the SR506n gateway.
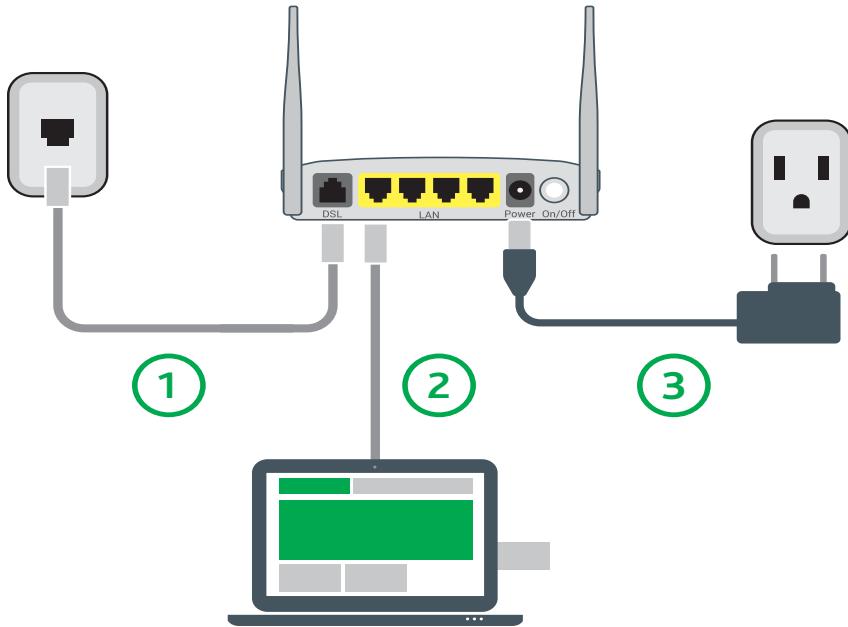
The buttons and ports located on the gateway are described below.

Feature	Description
Top	
WiFi	Button used for enabling or disabling the 5 GHz wireless function.
WPS	Button used for enabling or disabling the 2.4 GHz wireless function.
Rear panel	
DSL	The grey RJ11 port is used to connect your gateway to an Internet provider via a DSL service.
LAN 1 - 4	The yellow RJ45 ports can be used to connect client devices such as computers and printers to your gateway.
Power	Use only the power supply included with your gateway. Intended for indoor use only.
On/Off	Power switch.
Left side	
USB	Can transfer data, act as a printer interface, and handle a 3G accessory.
Reset	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 **Reset** button is located on the left side of the unit. Press the button for at least 1 second and release. The factory default settings are restored.

Buttons

On/Off Button

The On/Off button is located on the back of the gateway and turns the gateway on and off.

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 Reset button is located on the backleft 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 **Reboot** function in the gateway software.
6-20 seconds	Performs the software equivalent to the **Restore Defaults** 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.

WPS Button

The WPS button is located on the top of the unit. It 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 Wireless section of this manual.

WiFi Button

The WiFi button is located on the top of the unit and toggles the WiFi radio on and off.

To activate the WiFi radio, press and hold the WiFi button for 3-5 seconds and then release. Repeat this step to deactivate the WiFi radio.

INSTALLING YOUR SR506N GATEWAY

1. Plug the power adapter into the wall outlet and then connect the other end to the Power port of the gateway.
2. Connect the LAN port of the gateway to the network card of the PC using an Ethernet cable.
3. Turn on the unit by pressing the On/Off button on the side of the gateway.

Note: If you use 3G WAN service, connect the 3G USB data card to a USB port of the gateway. If you use the Ethernet uplink, connect to the WAN interface using an Ethernet cable. You cannot use the xDSL uplink, 3G WAN service, and Ethernet uplink all at the same time.

Your gateway is now automatically being set up to connect to the Internet. This process may take a few minutes to complete before you can begin using your Internet applications (browser, email, etc.).

If you are unable to connect to the Internet, confirm that all cable connections are in place and the router's power is turned on.

LOGGING IN TO YOUR GATEWAY'S UI

To manually configure the SmartRG SR555acSR655ac gateway, access the gateway's embedded UI.

1. Open a Web browser on your computer.
2. Enter http://192.168.1.1 (the default IP address of the DSL gateway) in the address bar. The login page appears where you can access the gateway's GUI or view the system log. For more information about configuring system logs, see the System Log topic in this User Manual.
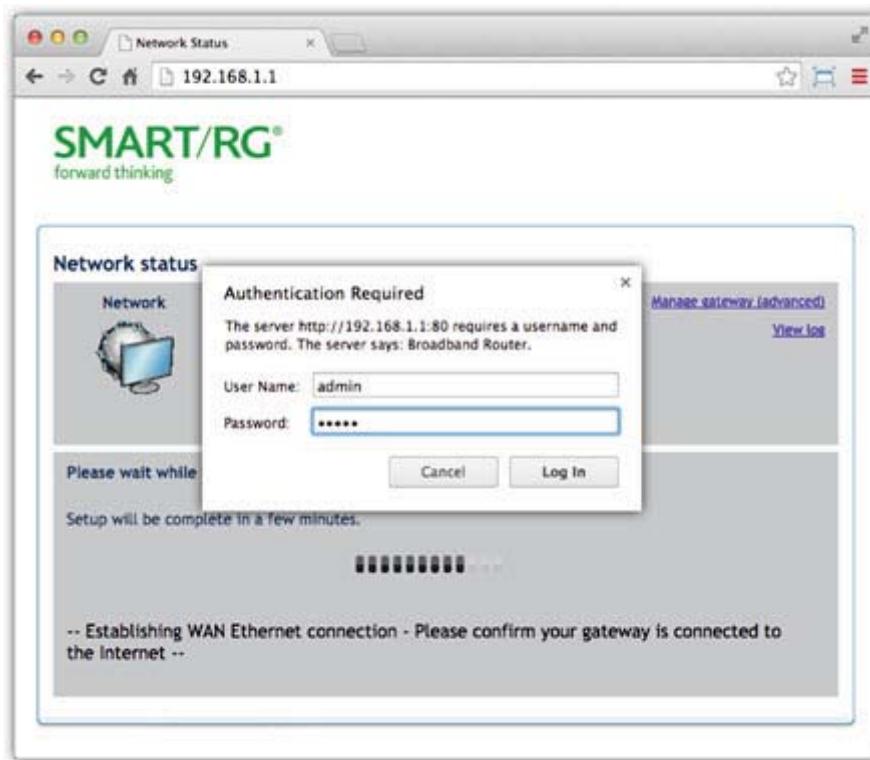
3. Click the **Manage gateway (advanced)** link at the top right of the page.
4. Enter the admin user name and password. The default admin username/password are admin/admin. The default username/password of the common user are user/user. It is recommended that you change these default values after logging in to the DSL gateway for the first time.
5. Click **OK**. The gateway interface appears, showing the Device Info summary page.

DEVICE INFO

In this section, you can view information about your gateway's setup, status or nature of its connection with the provider and with LAN devices. You cannot interact with or change the settings in this section.

Summary

When you log into the gateway interface, the **Device Info** summary page appears. 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.

SMART/RG
forward thinking

Device Info

Device Info
  Summary
  WAN
  Statistics
  Route
  ARP
  DHCP
Advanced Setup
Wireless
Diagnostics
Management
Logout

Board ID:	963381REF1
Symmetric CPU Threads:	2
Build Timestamp:	161013_1533
Software Version:	2.6.1.2016:10:13:13:37:22
Configuration File Origin:	SmartRG
Bootloader (CFE) Version:	1.0.38-118.3
DSL PHY and Driver Version:	A2pvl042j1.d26k1
Wireless Driver Version:	7.14.131.1608.cpe4.16L05.0-kdb
Uptime:	0D 2H 6M 47S
System Base MAC Address:	00:23:6a:d8:9d:86
Serial Number:	SR506NA086-9000001

This information reflects the current status of your WAN connection.

B0 Traffic Type:	PTM
B0 Line Rate - Upstream (Kbps):	41091
B0 Line Rate - Downstream (Kbps):	100016
B1 Traffic Type:	Inactive
B1 Line Rate - Upstream (Kbps):	0
B1 Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	ppp0
WAN IPv4 Address	10.101.2.16
Primary DNS Server:	8.8.8.8
Secondary DNS Server:	8.8.4.4
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).

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

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 **PPPoE**, **IPoE**, and **Bridge.**
VlanMuxId	The VLAN ID. Options are **Disabled** or **0-4094.**
IPv6	The state of IPv6. Options are **Enabled** and **Disabled.**
Igmp Pxy	The IGMP proxy.
Igmp Src Enbl	The IGMP source option is enabled for this connection.
MLD Pxy	The MLD proxy.
MLD Src Enbl	The MLD source option is enabled for this connection.
NAT	The state of NAT. Options are **Enabled** and **Disabled.**
Firewall	The state of the Firewall. Options are **Enabled** and **Disabled.**
Status	The status of the WAN connection. Options are **Disconnected**, **Unconfigured**, **Connecting**, and **Connected.**
IPv4 Address	The obtained IPv4 address.
IPv6 Address	The obtained IPv6 address.

Statistics

In this section, you can view network interface information for LAN, WAN Service, xTM and xDSL. All data is updated in 15-minute intervals.

LAN

On this page, you can view the received and transmitted bytes, packets, errors and drops for each LAN interface configured on your gateway. Data is provided for the total bytes, packets, errors and drops as well as bytes and packets for multicast transmissions, and packets for unicast and broadcast transmission. 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.

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

Field Name	Description
Interface	Available LAN interfaces. The only avalable option is LAN 1.Options are **LAN1** - **LAN4**, **WAN** (if configured on your device), **Wireless**, and **2.4 Ghz** and **5 Ghz**.
Received & **Transmitted** columns	
Bytes	Number of packets in bytes.
Pkts	Number of packets.
Errs	Number of error packets.
Drops	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. Data is provided for the total bytes, packets, errors and drops as well as bytes and packets for multicast transmissions, and packets for unicast and broadcast transmission. 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: **atm**, **ptm**, and **eth**.
Description	Service description. Options are: **pppoe**, **ipoe**, and **bridge**.
Received & **Transmitted** columns	
Bytes	Number of packets in bytes.
Pkts	Number of packets.
Errs	Number of error packets.
Drops	Number of dropped packets.

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** near the bottom of the page.
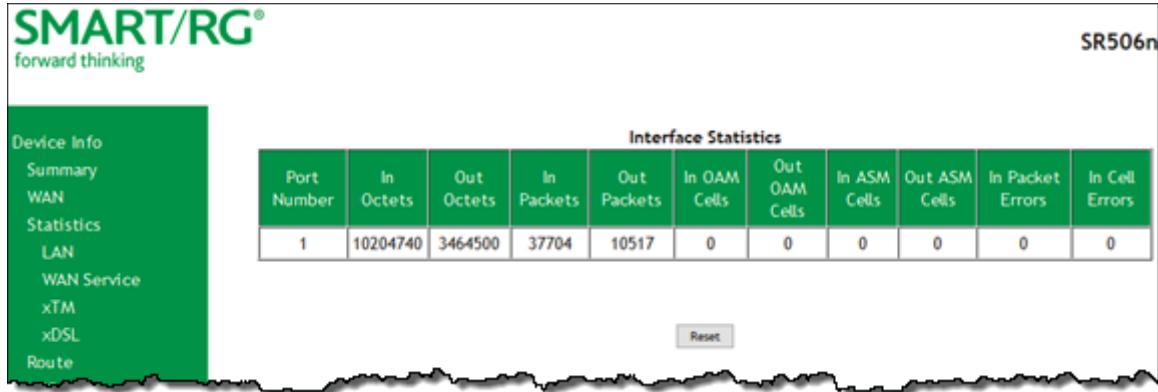
The fields on this page are explained in the following table.

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.

2. 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 default is **20** 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 in the dialog box.
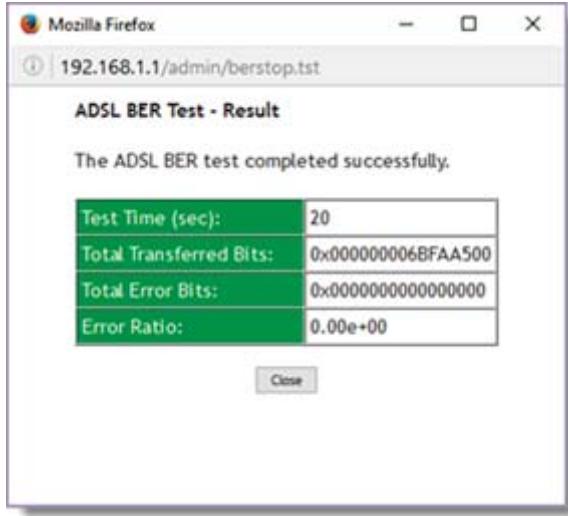
3. To reset the counters, click **Reset Statistics** at the bottom of the page.

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: **ATM** and **PTM**.
Status	Status of the connection. Options are: **Up**, **Disabled**, **NoSignal**, and **Initializing**.
Link Power State	Current link power management state (e.g., L0, L2, L3).
Downstream and **Upstream** columns	
Line Coding (Trellis)	State of theTrellis Coded Modulation. Options are **On** and **Off**.
SNR Margin (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 (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 (dBm)	Transmission 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: • Single frame bearer and single latency operation • Signal-to-Noise Ratio Margin (SNRM) to be equal or above the SNR Target Margin • BER not to exceed the highest BER configured for one (or more) latency paths • Latency not to exceed the highest latency configured for one (or more) latency paths • Accounting for all coding gains available (e.g., trellis coding, RS FEC) with latency bound

Field Name	Description
	• Accounting for the loop characteristics at the instant of measurement [2]
PhyR Status	Physical Layer Retransmission feature status. Options are **Inactive** and **Active**.
G.inp Status	The status of video data retrieval from the buffer. Options are **Inactive** and **Active**.
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]
Downstream and **Upstream** 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.
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, used to manager error correction.
I (interleaver block size in bytes)	The block sizeused for interleaving data transmissions.
N (RS codeword size)	The size of the Reed-Solomon (RS) codeword used for managing error correction.
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.
(End of DSL-specific field group)	
OH Frames	The number of xDSL OH Frames transmitted/received.
OH Frame Errors	The number of xDSL OH 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	*(Visible only for gateways connected via DSL)* Total number of Reed-Solomon Codewords received.
RS Codewords Corrected	*(Visible only for gateways connected via DSL)* Total number of Reed-Solomon Codewords corrected.

Field Name	Description
RS Codewords Uncorrected	*(Visible only for gateways connected via DSL)* 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, a1-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]
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.

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

Field Name	Description
IPv4 & IPv6 route fields	
Destination (Including IPv6 Route)	Destination IP addresses.
Gateway	Gateway IP address.
Subnet Mask	Subnet mask for the gateway.
Flag (Including IPv6 Route)	Status of the flags. See detailed descriptions above the tables.
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.
IPv6 Route only fields	

Field Name	Description
Destination	Destination IP addresses.
Next Hop	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 is marked with one of these flags. Options are: **Complete**, **Permanent**, and **Published.**
HW Address	The hardware (MAC) address of the host.
Device	The system level interface by which the host is connected. Options are: **br(n)**, **atm(n)**, and **ptm(n).**

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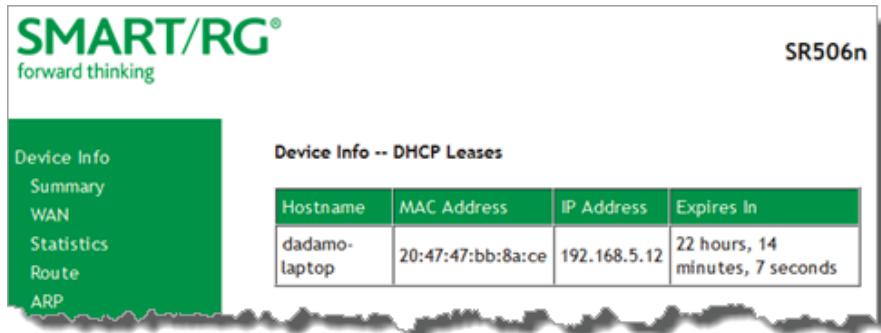
The fields on this page are explained in the following table.

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 and PTM 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.

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: **0-255**.
VCI	Enter a Virtual Channel Identifier. A VCI is a 16-bit identifier that has a unique channel. Options are: **32-65535**.

| Field Name	Description
Select DSL Latency	Select the level of DSL latency. Options are: • **Path0 Fast:** No error correction and can provide lower latency on error free lines. • **Path1 Interleaved:** Error checking that provides error free data which increases latency. • **Path0** and **Path1:** If you are not certain which method is best, you can select both.
Select Link Type	Select the linking protocol. **EoA** is the most popular with **PPPoA** a close second (used with many legacy ISPs). Options are: • **EoA:** Ethernet over ATM. • **PPPoA:** Point-to-Point Protocol over ATM. • **IPoA:** Internet Protocol over ATM.
Encapsulation Mode	Select whether multiple protocols or only one protocol is carried per PVC (Permanent Virtual Circuit). Options are: • **LLC/ENCAPSULATION**: (*Available for PPOA only*) Logical Link Control (LLC) encapsulation protocols used with multiple PVCs • **LLC/SNAP-BRIDGING:** LLC used to carry multiple protocols in a single PVC. • **LLC/SNAP-ROUTING**: (*Available for IPoA only*) LLC used to carry one protocol per PVC. • **VC/MUX:** Virtual Circuit Multiplexer creates a virtual connection used to carry one protocol per PVC.
Service Category	Select the bit rate protocol. Options are: • **UBR without PCR:** 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. • **UBR with PCR:** Same as above but with a Peak Cell Rate. • **CBR:** Constant Bit Rate relies on timing synchronization to make the network traffic predictable. Used commonly in Video and Audio traffic network applications. • **Non Realtime VBR:** 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. • **Realtime VBR:** 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.

Field Name	Description
Minimum Cell Rate	Minimum allowable rate (cells per second) at which cells can be sent on a ATM network. The default is **-1** (no shaping).
Scheduler for Queues of Equal Precedence as the Default Queue	The algorithm used to schedule the queue behavior. VC scheduling is different than the default queues. Options are: • **Weighted Round Robin:** Packets are accessed in a round robin style. Classes can be assigned. • **Weighted Fair Queuing:** Packets are assigned to a specific queue. • **Default Queue Weight:** The default weight of the specified queue. Options are **1**-**63**. • **Default Queue Precedence:** The precedence of the specified group. Options are **1**-**8**. • **VC WRR Weight**: The weight of the specified virtual channel queue. Options are **1**-**63**. • **VC Precedence**: The priority of the specified virtual channel queue. Options are **1**-**8**.

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, handling 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: **1**-**63**.
Default Queue Precedence	Enter a precedence for the specified queue. Options are: **1**-**8**.
Default Queue Minimum Rate	The default minimum rate at which traffic can pass through the queue. For no shaping, enter **-1** (disabled). Options are: **1**-**0** Kbps.
Default Queue Shaping	The shaping rate for the specified queue. Options are: **1**-**0** Kbps. The default is **-1** (no

Field Name	Description
Rate	shaping).
Default Queue Shaping Burst Rate	The maximum rate at which traffic can pass through the queue. Options are **1600** or greater.

ETH Interface

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

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

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.

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"
- Bridging

Instructions are 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.
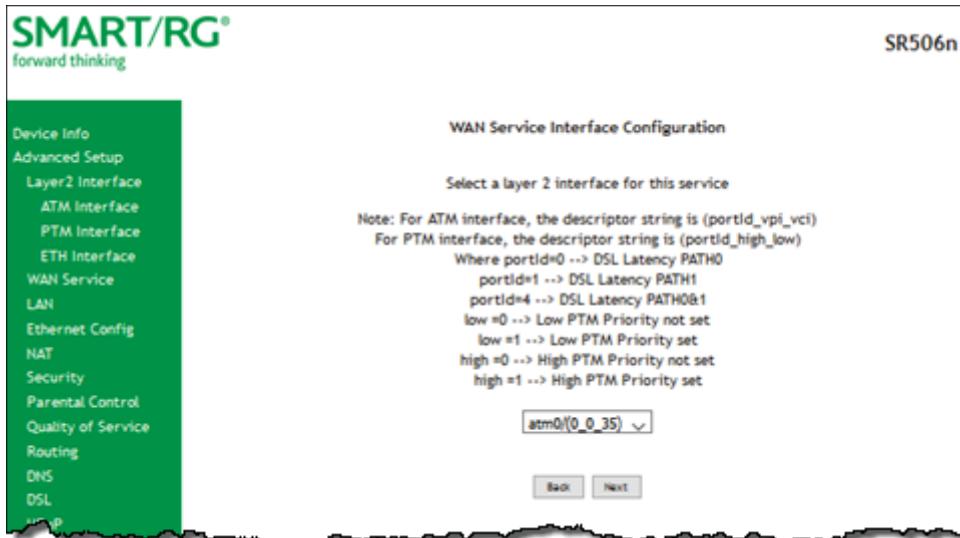
2. Select the Layer2 interface to use for the WAN service and click **Next**. The following page appears.
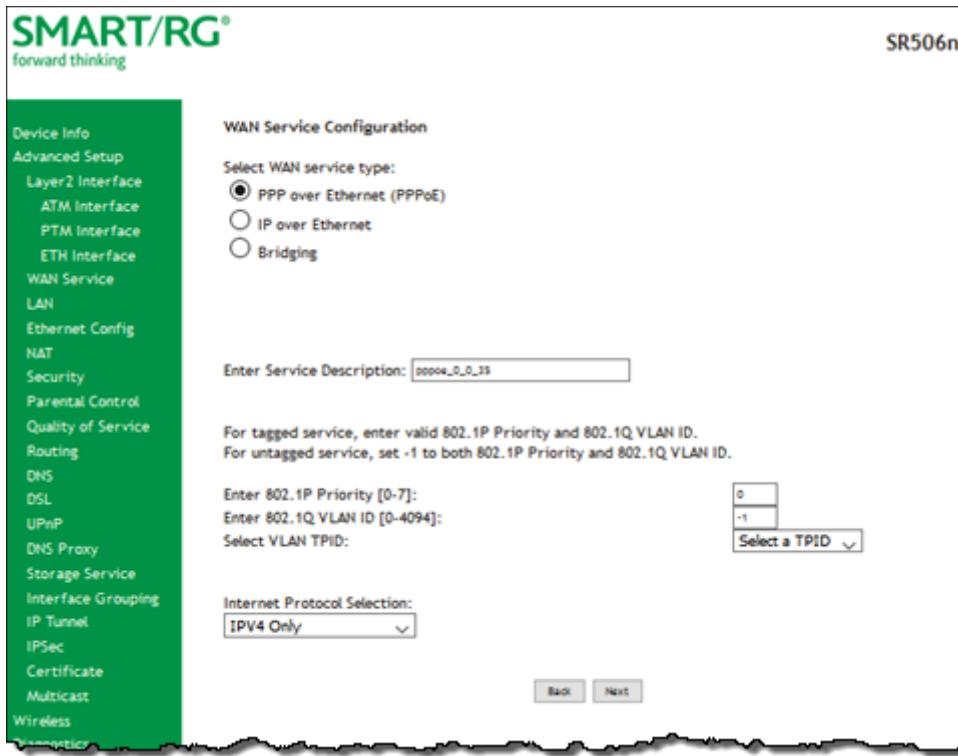
3. Select the **PPP over Ethernet (PPPoE)** WAN service type.
4. Modify the other settings as needed, using the information in the following table.

Field Name	Description
Enter Service Description	Enter a name to describe this configuration.
Internet Protocol Selection	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 **IPv4 Only**, **IPv4&IPv6** (Dual Stack), and **IPv6 Only**. **Note:** When you select **IPV4&IPV6** or **IPV6**, the subsequent options presented will change accordingly.
Enter 802.1P Priority	Options are **0** - **7**. The default is **0**. For tagged service, enter values in this field and the **802.1Q VLAN ID** field. For untagged service, enter **-1** (disabled) in this field and the **802.1Q VLAN ID** field.

Field Name	Description
Enter 802.1Q VLAN ID	Options are **0 - 4094**. The default is **-1** (disabled).
	For tagged service, enter values in this field and the **802.1P Priority** field.
	For untagged service, enter **-1** (disabled) in this field and the **802.1P Priority** field.
Select VLAN TPID	Select the TPID for this VLAN. Options are **0x8100**, **0x88A8**, and **0x9100**.
Internet Protocol Selection	Select the IP version. Options are **IPv4 Only**, **IPv4&IPv6 (Dual Stack)**, and **IPv6 Only**.

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

6. 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	(*Optional*) Enter a description for this service.
Authentication Method	Select a means for authentication. Options are: **AUTO**: Attempt to automatically detect handshake protocol (listed below)s. **PAP**: Password Authentication Protocol (plaintext passwords). **CHAP**: Challenge Handshake Authentication Protocol. (MD5 hashing scheme on passwords). **MSCHAP**: Microsoft Challenge Handshake Authentication Protocol. (Microsoft encrypted password authentication protocol).
LCP 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.
PPP IP Extension	Select whether to forward all traffic to the advanced DMZ IP specified in the next field. When you select this option, the NAT fields are hidden.

Field Name	Description
Advanced DMZ	Specify the IP address and mask to which PPPoE traffic is forwarded.
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, 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**.
Use Static IPv4 Address	Specify the IPv4 Address to apply for this WAN service.
Use Static IPv6 Address	Specify the IPv6 Address to apply for this WAN service.
Enable IPv6 Unnumbered Model	(*Available only when **IPv4&IPv6 (Dual Stack)** is selected for the **Interned Protocol** field*) Select to allow your gateway to process IP packets without configuring a unique IP address. This works by "borrowing" an IP address from another interface.
Launch Dhcp6c for Address Assignment (IANA)	(*Available only when **IPv4&IPv6 (Dual Stack)** is selected for the **Interned Protocol** field*) Select to launch the dhcp6c client deamon to request and configure IPv6 addresses and host network configuration information.
Launch Dhcp6c for Prefix Deleg- ation (APD)	(*Available only when **IPv4&IPv6 (Dual Stack)** is selected for the **Interned Protocol** field*) Select to enable your DHCPv6 server to allow your gateway to ask for an IPv6 prefix (subnet) that it can then split up and delegate to the clients it serves. This option is selected by default.
Retry PPP pass- word on authen- tication 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 **Security** sub-menu.
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	(*Appears when **Enable NAT** is selected*) Click to enable what is known as one-to-one NAT.
Enable SIP ALG	(*Appears when **Enable NAT** is selected*) Click to enable Session Initiation Protocol (SIP) pass-

Field Name	Description
	through NAT. Used for Voice over IP (VOIP) applications.
Enable IGMP Multicast Proxy	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	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 **1370 - 1492 bytes**. The default is **1492** bytes. 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	(*Appears when* **Use Base MAC Address** *is deselected*) Enter the MAC address to be used as the close address.

7. Click **Next**. The following page appears.
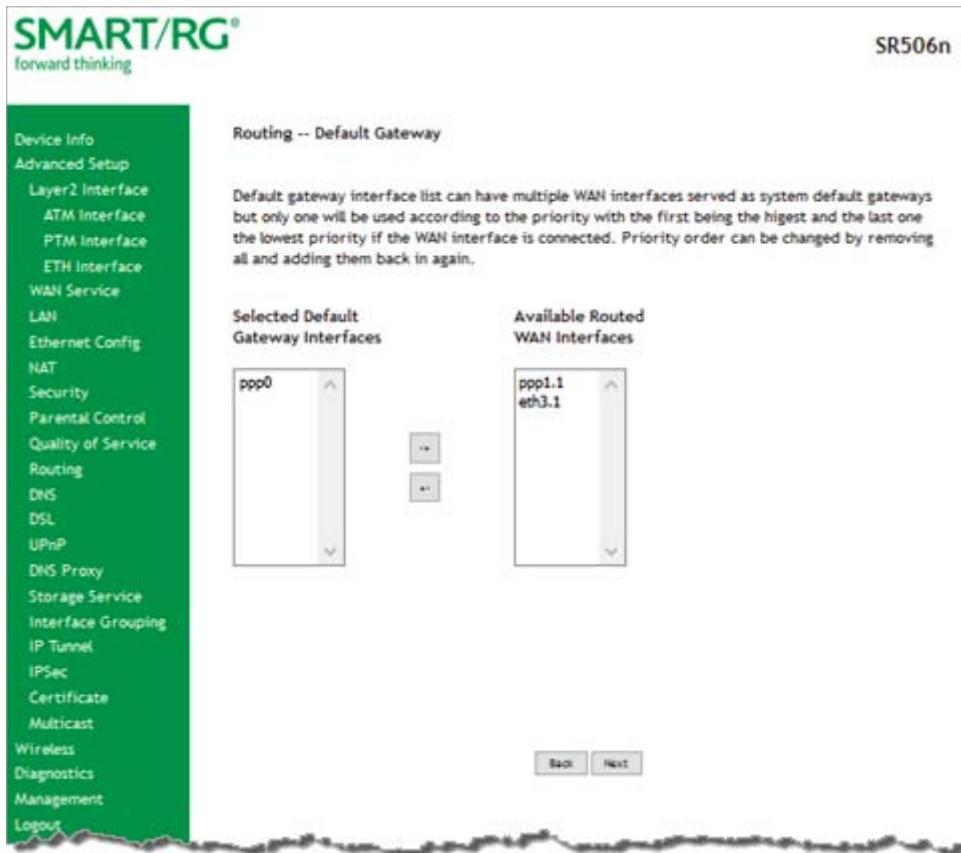
8. Select the interface used as a default gateway for the PPP service being created and click the **arrows** to move your selection from left to right or from right to left.

9. Click **Next**. The following page appears where you will select DNS Server settings.
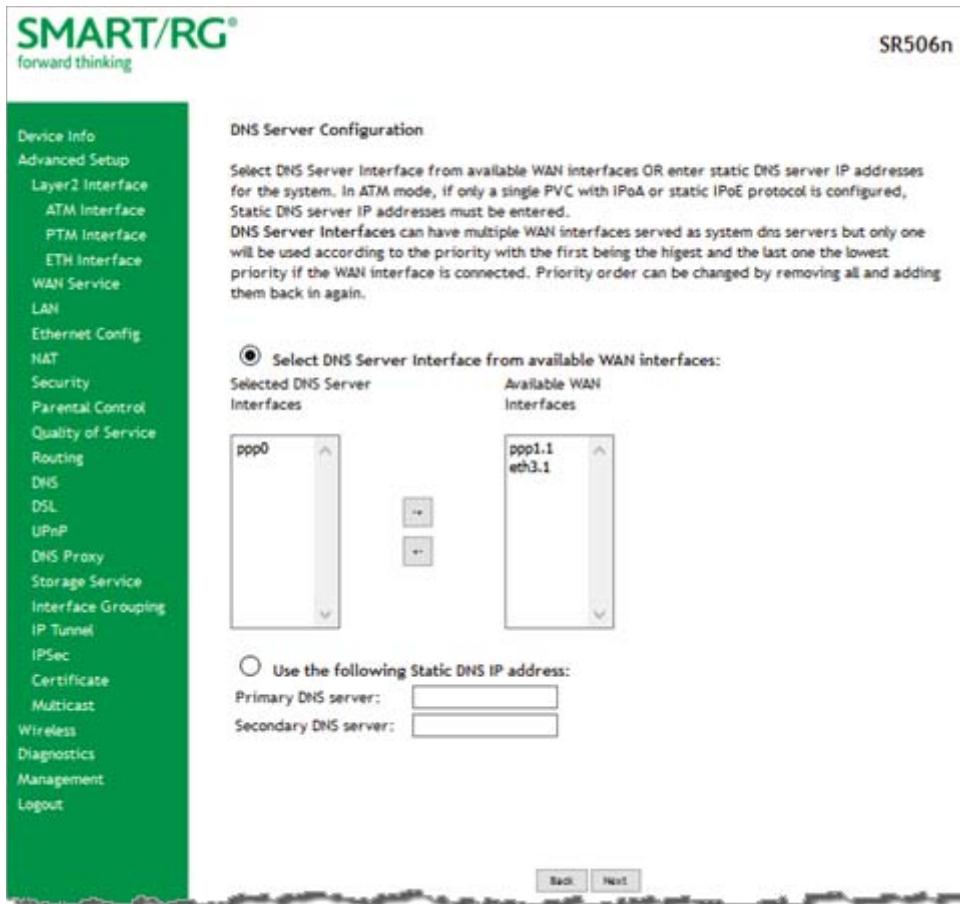
10. Select the DNS Server Interface from Available WAN interfaces and click the **arrows** to move your selection from left to right or from right to left.
11. Alternatively, you can enter static DNS IP addresses in the **Use the following Static DNS IP address** section.

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

13. 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.

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	(*Optional*) Enter a name to describe this configuration.
Enter 802.1P Priority	Options are **0** - **7**. The default is **-1** (disabled). For tagged service, enter values in this field and the **802.1Q VLAN ID** field. For untagged service, accept the default of **-1** in this field and inthe **802.1Q VLAN ID** 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 **802.1P Priority** field.

Field Name	Description
	For untagged service, accept the default of **-1** in this field and in the **802.1P Priority** field.
Select VLAN TPID	Select the TPID for this VLAN. Options are **0x8100**, **0x88A8**, and **0x9100**.
Internet 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 **IPv4 Only**, **IPv4&IPv6 (Dual Stack)**, and **IPv6 Only**. The default is **IPv4 Only**. **Note:** When selecting **IPV4&IPV6** or **IPV6**, the subsequent options presented will change accordingly.

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

6. Enter the relevant WAN IP Settings, using the information provided in the following table.

Field Name	Description
Obtain an IP address automatically	Select when you want 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.

Field Name	Description
Option 61 DUID	(*Optional*) DHCP Unique Identifier (DUID) is used by the client to get an IP address from the DHCP server.
Option 77 User ID	(*Optional*) Enter the user class ID that should be used to filter traffic.
Option 125	(*Optional*) Select whether to enable local devices to automatically receive DHCP options from the server.This option is disabled by default. To enable it, click **Enabled**.
Option 50 Request IP Address	Select to request a specific IP address when sending messages. If the address is not available, the DHCP server assigns the next allowed IP address.
Option 51 Request Leased Time	Select to request the maximum lease time defined for the client.
Option 54 Request Server Address	Select to request the IP address of the source server.
Use the following Static IP address	Select when you want to manually declare the static IP information provided by your ISP. The WAN address fields become available.
WAN IP Address	Enter the static WAN IPV4 Address.
WAN Subnet Mask	Enter the static subnet mask.
WAN gateway IP Address	Enter the static gateway IP address.
Advanced DMZ	(*Optional*) 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, 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**.
IPv6 settings	
The following fields appear when either **IPv6 Only** or **IPv4&IPv6 (Dual Stack)** network protocols are selected on the WAN Service Configuration page.	
Obtain 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	Select this option for the CPE to generate the WAN IP's prefix from the server's REST

Field Name	Description
(IAPD)	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.

7. Click **Next**. The **NAT settings** page appears.

8. Click **Next**.
9. 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. **Note:** This option and its related options are not available when IPv6 is selected as the Internet protocol.
Enable Fullcone NAT	(*Appears when **Enable NAT** is selected*) Enables what is known as one-to-one NAT.
Enable SIP ALG	(*Appears when **Enable NAT is selected***) Enables Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications.
Enable Firewall	Select to enable functions in the **Security** sub-menu.
Enable IGMP Multicast Proxy	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	Select to enable this service to act as an IGMP multicast source.
Use Base MAC Address on this WAN interface	Use SmartRG Devices Base (Primary) MAC address. When unchecked, a unique MAC per service is assigned.

10. Click **Next**. The following page appears.
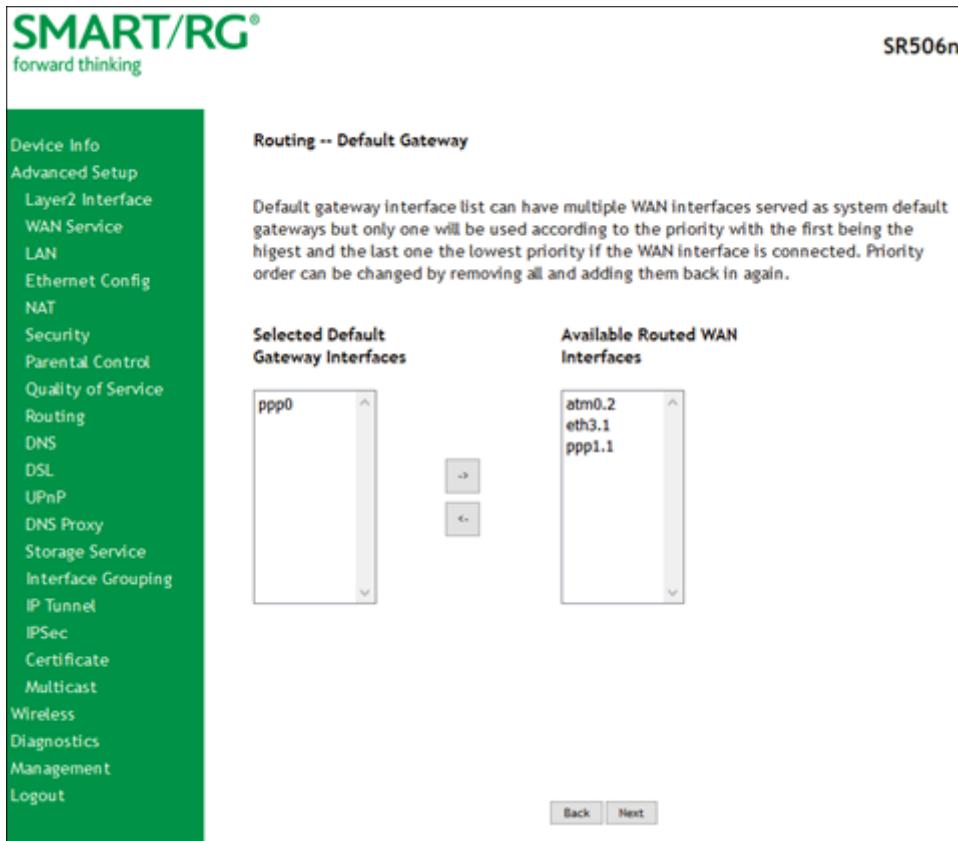
11. Select the interface used as a default gateway for the PPP service being created and click the **arrows** to move your selection from left to right or from right to left.

12. Click **Next**. The following page appears where you will select DNS Server settings.
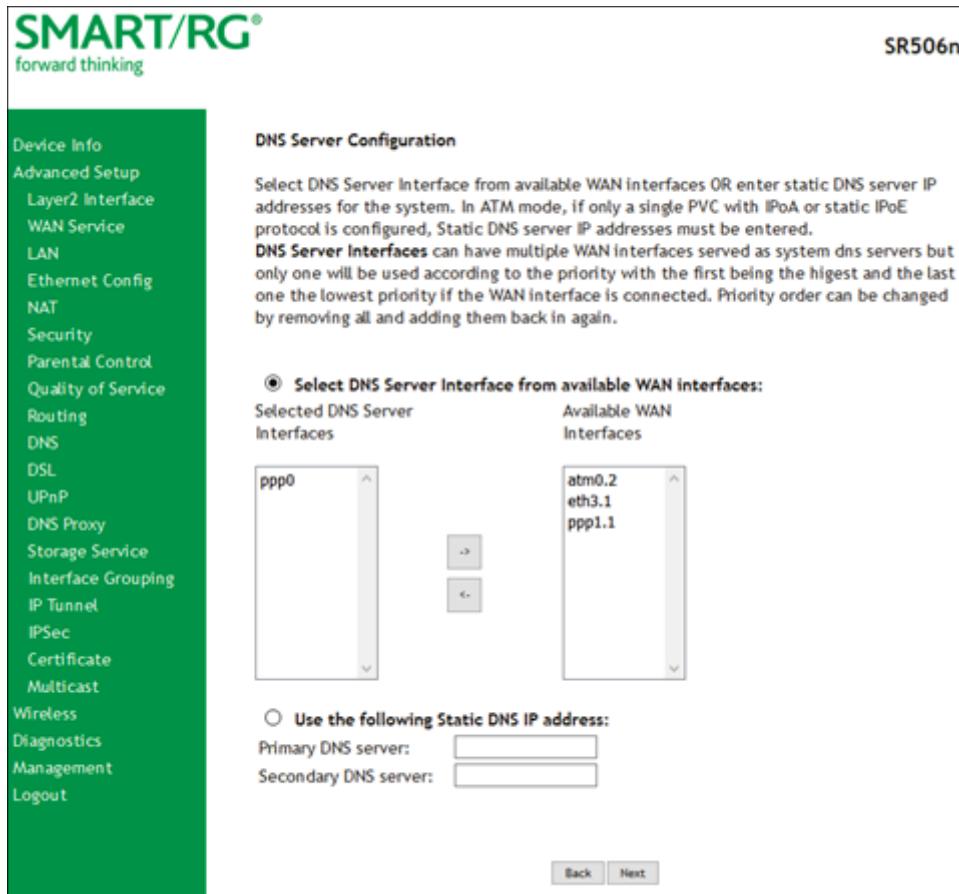
13. Select the DNS Server Interface from available WAN interfaces and click the **arrows** to move your selection from left to right or from right to left.

14. Alternatively, you can enter static DNS IP addresses in the **Use the following Static DNS IP address** section.

15. If you selected IPv6 as the Internet protocol earlier, you can configure the same DNS server information in the following fields:

- **Obtain IPv6 DNS info from a WAN interface**: Select a **WAN Interface**.

- **Use the following Static IPv6 DNS address**: Enter the **Primary IPv6 DNS server** address and, if desired, enter a **Secondary IPv6 DNS server** address.

16. Click **Next**. The summary page appears.

17. 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.

Bridging

Before you can configure a bridge WAN service, you must create the related ATM interface.

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

2. Select an ATM interface for the WAN service and then click **Next**. The following page appears.
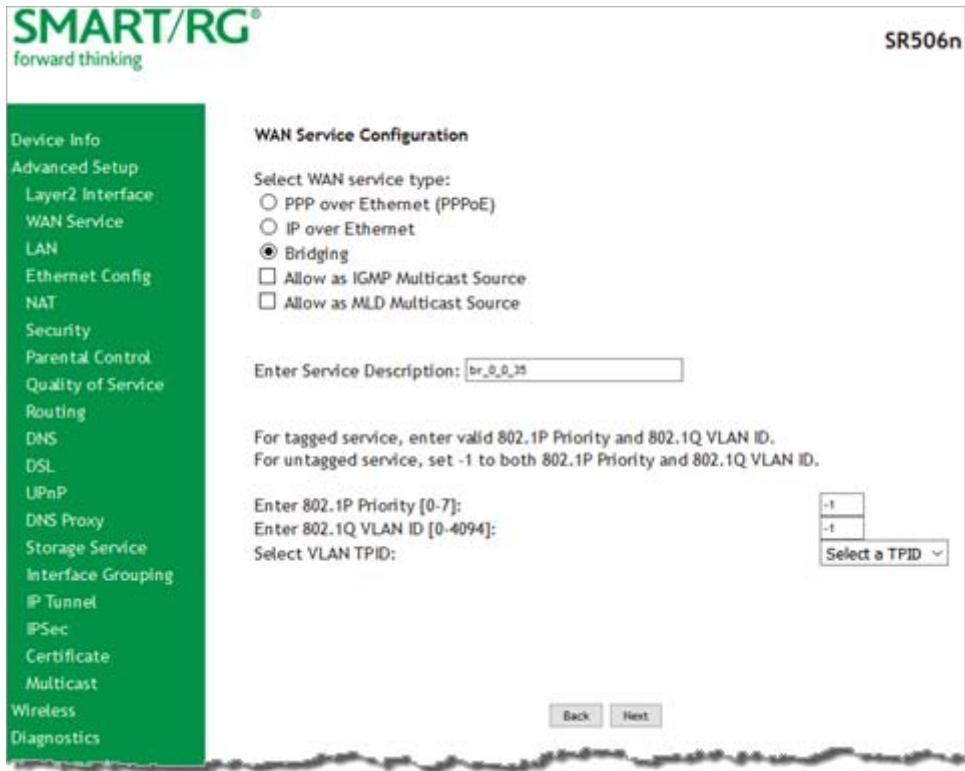
3. Select **Bridging**. The Multicast Source fields appear.
4. Modify the other fields as needed, using the information in the following table.

Field Name	Description
Allow as IGMP Multicast Source	Select to enable this service to act as an IGMP multicast source.
Allow as MLD Multicast Source	Select to enable this service to act as an MLD multicast source.
Enter Service Description	(*Optional*) Enter a name to describe this configuration.
Enter 802.1P Priority	Options are **0** - **7**. The default is **-1** (disabled). For tagged service, enter values in this field and the **802.1Q VLAN ID** field. For untagged service, accept the default of **-1** in this field and in the **802.1Q VLAN ID** field.

Field Name	Description
Enter 802.1Q VLAN ID	Options are **0** - **4094**. The default is **-1** (disabled).
	For tagged service, enter values in this field and the **802.1P Priority** field.
	For untagged service, enter **-1** (disabled) in this field and in the **802.1P Priority** field.
Select VLAN TPID	(*Optional*) Select the TPID for this VLAN. Options are **0x8100**, **0x88A8**, and **0x9100**.

5. Click **Next**. The summary page appears indicating that your Bridging WAN setup is complete.

6. 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.

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	Select an interface group from the list of available groups (defined on the Interface Grouping page).
IP Address	Enter the LAN IP address by which LAN devices will connect to this gateway.
Subnet Mask	Enter the Subnet mask to be used by LAN devices connecting to this gateway.
Enable IGMP Snooping	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	Allows multicast traffic between LANs.
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 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	(*Becomes editable when* **Enable DHCP Server** *is selected*) Enter the beginning of the class C, IP address range to be assigned by the DHCP server.
End IP Address	(*Becomes editable when* **Enable DHCP Server** *is selected*) Enter the end of the class C, IP address range to be assigned by the DHCP server.
Leased Time (hour)	(*Becomes editable when* **Enable DHCP Server** *is selected*) Enter the number of hours for which an IP address will be leased.
Static IP Lease List	Specify a literal, static IP address to be associated with a specific MAC Address of one of your LAN host devices. 1. Click **Add Entries**. 2. Enter the MAC address and IP address and click **Apply/Save**. 3. Repeat this step to create any additional entries that you need up to 32.

Field Name	Description
Automatically create static IP leases from the following OUIs	For LAN hosts, IP addresses can be assigned manually or by using DHCP. Click **Add OUI**. Enter the OUI and click **Apply/Save**. Repeat these steps to create any additional entries that you need.
Configure DHCP Options section	
Option 66	For devices that 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 150	A Cisco proprietary methodology for pointing to one or two TFTP servers.
Configure the second IP address and sub-net mask for LAN interface	When you select this option, the **IP Address** and **Subnet Mask** 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.

IPv6 Autoconfig

On this page, you can configure your gateway's IPv6 environment.

1. In the left navigation bar, click **Advanced Setup** > **LAN** > **IPv6 Autoconfig** . The following page appears.

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

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

Field Name	Description
Interface Address	IPV6 address to assign as the gateways Local LAN IPV6 address and prefix length. Prefix length is required.
IPv6 LAN Applications section	
Enable DHCP v6 Server	Enable the DHCP v6 feature on the LAN.

Field Name	Description
Enable DHCP Server - Stateless	This option is selected by default. Click to stop inheriting IPV6 address assignments from the WAN IPV6 interface.
Enable DHCP Server - Stateful	DHCPv6 server given by the LAN IPV6 network as configured with additional options. Zero compression is not supported. Make sure to enter zeros between the colons, that is, do not use short-hand notation (::2). Options are: • **Start interface ID**: Enter the beginning IPv6 available addresses for DHCP to assign to LAN devices. • **End interface ID**: Enter the ending IPv6 available addresses for DHCP to assign to LAN devices. • **Leased Time (hour):** Amount of time before a new IPv6 lease is requested by the LAN client.
Enable RADVD	(*Optional*) This option is enabled by default. It enables Router Advertisement Daemon (RADVD) service that sends router advertisements to LAN clients. Clear the check box to disable RADVD. Options are: • **Enable ULA Prefix Advertisement:** Check this option to enable unique local address (ULA) advertisement on the LAN. When you select this option, the **Randomly Generate** option is selected and the gateway can generate a random IPv6 prefix. • **Statically Configure Prefix:** Select this option to configure the IPv6 prefix, and enter values in the **Preferred Life Time** and **Valid Life Time** fields (in hours). The default value for these fields is **-1** (no limit).
Enable MLD Snooping	(*Optional*) This option is enabled by default. It enables Multicast Listener Discovery (MLD) snooping to manage IPV6 multicast traffic. Options are: • **Standard Mode:** Multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if IGMP snooping is enabled. • **Blocking Mode:** The multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group. This is the default.
Enable MLD LAN to LAN Multicast	(*Optional*) This option is enabled by default. It enables LAN-to-LAN Multicast until the first WAN service is connected. Options are **Disable** and **Enable**.

Ethernet Config

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

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

2. In the **Configure** column, select an option (**Auto**, **100 Full**, **100 Half**, **10 Full** or **10 Half**) for the Ethernet port 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: For 1000 BaseT connections, always select **Auto**.

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

NAT

In this 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. To add a virtual server, click Add. The following page appears.

3. Customize the fields to create your port forwarding entry, using the information provided in the table below.
4. 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 **Select a Service** list, you can enter a unique name for the application in this field.

Field Name	Description
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: **TCP**, **UDP**, or **TCP/UDP**.
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.
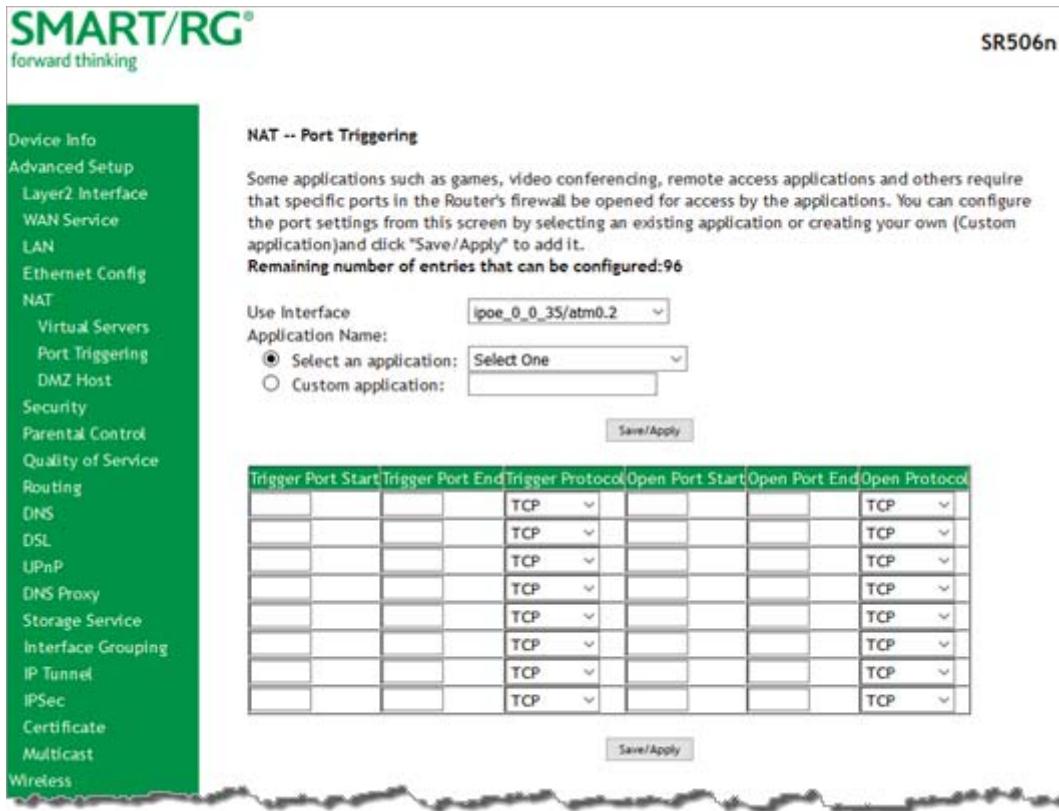
2. Customize the fields as needed for the firewall pinholes you wish to establish. A maximum 96 entries can be configured.
3. Click **Apply/Save** to commit your changes. If the selected service configures multiple servers, the same number of entries are added to the table of the NAT - Virtual Servers Setup page.

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 a Service	Select the application which requires a port trigger entry. The starting and ending IP addresses and port numbers that are configured for the service are populated into the table at the bottom of the page.
Custom Service	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**.

Field Name	Description
Trigger Port End	Enter the end number of the range of available outgoing trigger ports. Options are: **1** - **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.
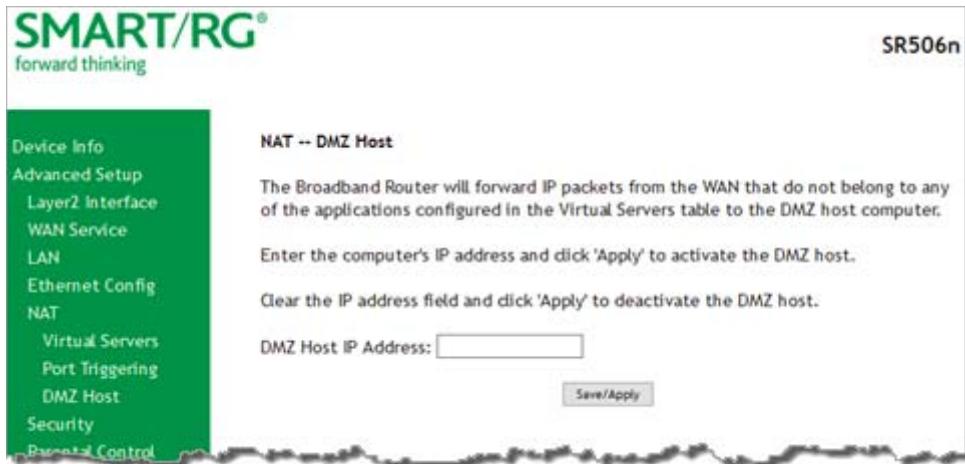
2. Enter the **DMZ Host IP Address**.
3. Click **Apply/Save** to commit your change.

Security

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

IP Filtering - Outgoing

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

1. In the left navigation bar, click **Advanced Setup** > **Security** > **IP Filtering** 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 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.
IP Version	For the filter to be configured and effective for IPV6 , the gateway must be installed on a net-work that is either a IPV6-only network (with that protocol enabled) or is both IPV4 and IPV6 dual protocol enabled/configured. Options are **IPv4** and **IPv6**. The default is **IPv4**. If you select **IPV6**, 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 **TCP/UDP**, **TCP**, **UDP**, and **ICMP**.

Field Name	Description
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).
	Note: This address can be a particular address or a block of IP addresses on a 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.
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	Enter the destination IP address of a LAN side host for which you wish to filter/block outgoing traffic for the specified protocol(s).
	Note: This address can be a particular address or a block of IP address on a 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.
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.

IP Filtering - Incoming

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

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	Enter a descriptive name for this filter.
IP Version	Select the IP version for this filter. Options are **IPv4** and **IPv6**. The default is **IPv4**.
Protocol	Select the protocol to be associated with this incoming filter. Options are: **TCP/UDP**, **TCP**, **UDP**, or **ICMP**.
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).
WAN Interfaces	Click to apply this rule to all WAN interfaces or only certain types. Options are **Select All** or the interfaces defined for your 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 **FORWARD** and **BLOCKED**.

Adding 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 **Save/Apply** 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 **PPPoE**, **IPv4**, **IPv6**, **AppleTalk**, **IPX**, **NetBEUI**, and **IGMP**.
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. Options are **LAN<=>WAN**, **WAN=>LAN**, and **LAN-N=>WAN**. The default is **LAN<=>WAN**.
WAN Interfaces	Select the interface to which the filter should be applied.

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** 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.
Browser's MAC Address	This option is selected by default. The MAC address of the connected device is shown.
Other MAC Address	Select this option to restrict access to another device. Enter the MAC address of that device. **Note:** You can view a list of the connected devices and MAC addresses on the **Device Info** > **ARP** page.

Field Name	Description
Days of the week	Select the days (**Mon** - **Sun**) for which the restrictions apply.
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 (**00:00** - **24:00**).

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. Next to **URL List Type**, select **Exclude**.
    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, next to **URL List Type**, 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 **80**.

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.

Note: Before proceeding, make sure that the necessary WAN service has been configured with the appropriate Priority setting.

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) 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. If the **Enable QoS** checkbox is *not* checked, click it to select it.
    Warning: If this option is already enabled and you clear the checkbox, QoS will be disabled for ALL interfaces.
3. In the **Select Default DSCP Mark** field, select the Differentiated Services Code Point (DSCP) Mark classification value to be used. The default is **No Change(-1)**. For a list of supported values, see "Supported DSCP Values".
4. 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 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. In the **Name** field, type a descriptive name for this queue.
3. In the **Interface** field, select the Layer 2 interface to be associated for this queue. Additional fields appear.
4. Fill in the fields, using the information provided in the table below.
   Note: For Dynamic WAN interfaces, the **Queue Priority** settings appear twice - once for ATM WAN QoS configuration and once for PTM WAN QoS configuration.
5. Click **Apply/Save** to save your settings.

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

Field Name	Description
Enable	Select to enable or disable this queue configured on the selected interface. This option is enabled by default. **Note:** Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.
Queue Priority settings	
Queue Pre-cedence/ Precedence	Select the priority value to be associated with the new queue. Options vary by interface type and include **1(SP - 4(SP)**, **1(WRR/WFQ) - 7(WRR/WFQ)**, and **8(WRR)**. **Note:** The lower the value, the higher the priority.
Scheduler Algorithm	(*Not applicable for ETH interfaces*) Select an algorithm for applying queue data priority. Options are: • **Weighted Round Robin:** Applies a fair round robin scheme weighting that is effective for networks with fixed packet sizes, e.g., ATM networks. • **Weighted Fair Queuing:** Applies a fair queue weighting scheme by allowing different sessions to have different service shares for improved data packet flow in networks with variable packet sizes, e.g., PTM/IP networks.
Queue Weight	(*Not applicable for ETH interfaces*) Enter a weight for prioritizing this queue. Options are **1 - 63**.
Minimum Rate	(*Applicable for PTM and Dynamic WAN interfaces only*) Enter the minimum shaping rate for packets in QoS queues. Options are **1 - 100000** Kbps. To specify no minimum rate, enter **-1**.
Shaping Rate	(*Applicable for PTM and Dynamic WAN interfaces only*) Enter the shaping rate for packets in QoS queues. Options are **1 - 100000** Kbps. To specify no shaping, enter **-1** .
Shaping Burst Size	(*Applicable for PTM and Dynamic WAN interfaces only*) Enter the shaping burst size to be applied to packets in the defined queue. Options are **1600 bytes** or greater.
PTM Priority	(*Applicable for PTM and Dynamic WAN interfaces only*) Select the priority for the PTM inter-face. Options are **Low** and **High**.
DSL Latency atm, ptm	(*Not applicable for ETH or Dynamic WAN interfaces*) Select the level of DSL latency. Options are: • **Path0 (Fast):** No error correction and can provide lower latency on error free lines. • **Path1 (Interleaved):** Error checking that provides error free data which increases latency. **Note:** If you are not sure which option to select, you can select both.

Wlan Queue

On this page, you can view the WLAN queues defined for your network.

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

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 last in the list of classification rules. The only option is **Last.**
Rule Status	Select whether this rule is active or inactive. Options are **Disable** and **Enable.**The

Field Name	Description
	default is **Enable**.
Specify Classification Criteria section	
Ingress Interface	Select an interface for incoming data. Options are **LAN**, **WAN**, **Local** and any interface already configured for your gateway.
Ether Type	Select the Ethernet interface type for this classification. Options are **IP**, **ARP**, **IPV6**, **PPPoE_DISC**, **pPPoE_SES**, **8865**, **8866**, and **8021Q.**
802.1P priority	(*For **Ether Type** of **8021Q** only*) This value is inserted into the Ethernet frame and used to differentiate traffic. Lower values assign higher priorities. Options are: **1** - **7.**
Source MAC Address Source MAC Mask	(*Not applicable for **Ether Type** of **8021Q***) Enter the source MAC Address and Source MAC Mask for this classification.
Destination MAC Address Destination MAC Mask	(*Not applicable for **Ether Type** of **8021Q***) Enter the destination MAC Address and des-tination MAC Mask for this classification.
Source IP Address[Mask]	(*Not applicable for **Ether Type** of **8021Q***) (Optional) Enter the source IP address and subnet mask for this classification, or select a DHCP option from the drop-down list and enter the address and mask for that server.
Destination IP Address [Mask]	(*Optional*) (*Not applicable for **Ether Type** of **8021Q***) Enter the destination IP address and subnet mask for this classification.
Differentiated Service Code Point (DSCP) Check	(*Optional*) (*Not applicable for **Ether Type** of **8021Q***) Select the desired DSCP code for marking incoming data.
Protocol	(*Optional*) (*Not applicable for **Ether Type** of **8021Q***) Enter the Protocol specified for this classification.
Specify Class Queue	(*Not applicable for **Ether Type** of **8021Q***) Select from the available queues. **Note:** Make sure to select a queue that is configured for the interface that you selec-ted. 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.
Specify Classification Results section	
Specify Egress Interface	Select the egress interface for this rule. Options are the interfaces already configured.
Specify Egress Queue	Select the egress queue for this rule. Options are the queues already configured.
Mark Applied Dif-ferentiated Service Code Point	Select the desired DSCP code for marking classification results.

Field Name	Description
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**.
Set Rate Limit	Enter the data traffic rate limit (in Kbps) applied for this classification.

QoS Port Shaping

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

1. In the left navigation bar, click **Advanced Setup** > **Quality Of Service** > **QoS Port Shaping**. 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	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)	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)	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 **Shaping Rate** field, the value in this field is ignored.
Egress Shaping Rate (Kbps)	Enter the data rate for packets on the specified Interface. Options are: **1 - 1,000,000** Kbps. The default is **-1** (no shaping).

Field Name	Description
Egress Burst Size (bytes)	Enter the burst size to be applied to packets in the defined queue. Options are **1600 bytes** or greater. The default is **0** (no size limit). If you enter a value of **-1** (disabled) in the **Egress Shaping Rate** field, the value in this field is ignored.
Ingress Policing Rate (Kbps)	Enter data rate for policing incoming packets in the defined queue. The default is **-1** (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.

Note: You must configure the IPv6 interface before attempting to assign it as the default gateway interface.

1. In the left navigation bar, select **Advanced Setup** > **Routing**. The following page appears.
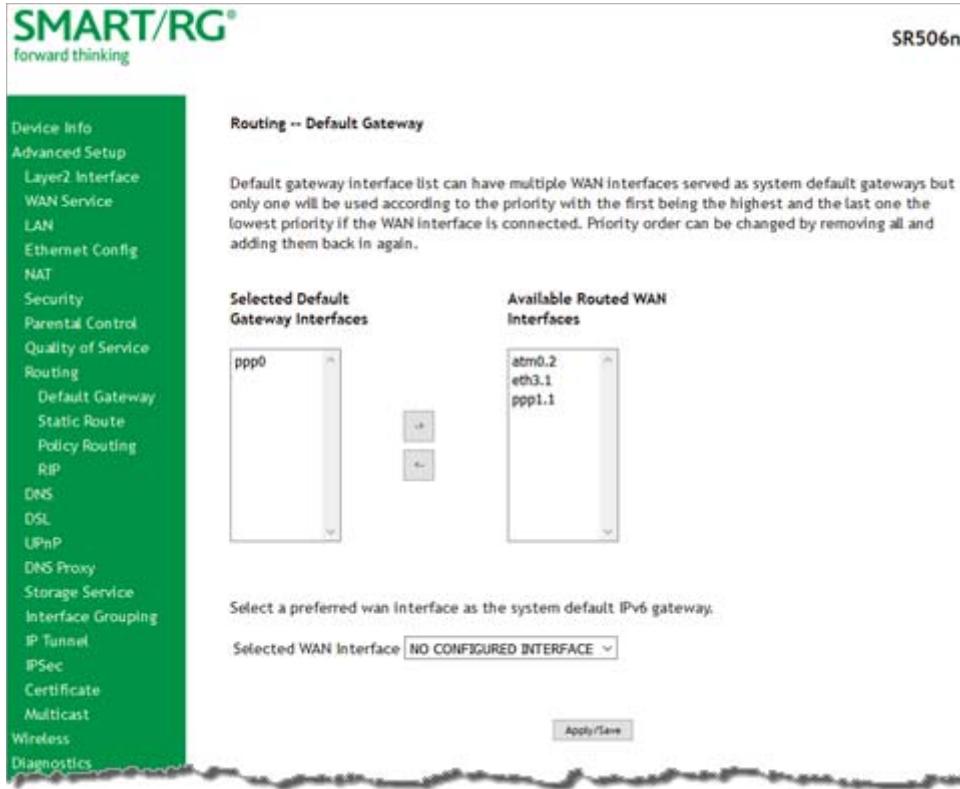
2. Select the interfaces that you want used as default gateway interfaces. Click the **arrows** to move your selection between the columns. Move the highest priority interface first, followed by the next highest priority interface, and so on.
3. (*Optional*) In the **Selected WAN Interface** field, select an IPv6 interface. 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: **IPv4** and **IPv6**.
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.
Physical LAN Port	Select a physical port on the gateway.
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.

Note: This feature applies only to IPoE configurations.

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: • **Active:** This mode listens and advertises routes. • **Passive:** This mode listens only. It does not advertise routes.
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**. The following page appears.

2. (*Optional*) Select DNS Server interfaces by moving them from left to right or right to left by clicking the **arrows**. The options for obtaining the DNS information from a WAN interface are selected by default.
3. To use a static DNS IP address, click **Use the following Static DNS IP address** and enter the primary DNS IP address. If applicable, enter a secondary DNS IP address.

4. (*Optional*) In the **WAN Interface selected** field, select a different WAN interface.
   The **Obtain IPv6 DNS info from a WAN interface** option is selected by default.
5. To use a static DNS IPv6 address, click **Use the following Static IPv6 DNS address** and enter the primary DNS IP address. If applicable, enter a secondary DNS IP address.
6. Click **Apply/Save** to commit changes.

Dynamic DNS

Dynamic DNS (DDNS) automatically updates a name server in the DNS with the active DNS configuration of its configured host-names, 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.

2. Modify the settings, 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
D-DNS provider	Select a dynamic Domain Name Server provider.
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

Field Name	Description
	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. Modify the settings, 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
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.

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

The modulation settings are described in the table below.

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 pins are the contacts for DSL2. Select which pair should be used.
Capability	**Bitswap Enable**: Enables adaptive handshaking functionality. **SRA Enable**: Enables Seamless Rate Adaptation. **PhyR Enable**: Enables Physical Layer Retransmission. **ADSL PTM Mode Enable**: Enables Asymmetric Digital Subscriber Line in Packet Transfer Mode. **Stinger® Mode Enable**: Enables communication with Stinger type equipment.
Inventory Management	Select whether to use the gateway serial number as the EOC serial number in your inventory management database.

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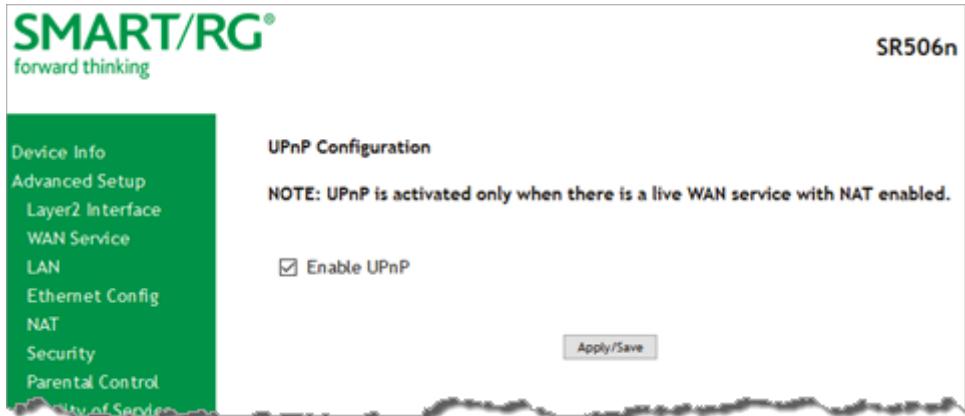
2. To disable this option, click **Enable UPnP** to clear the box.
3. Click **Apply/Save** to commit your changes.

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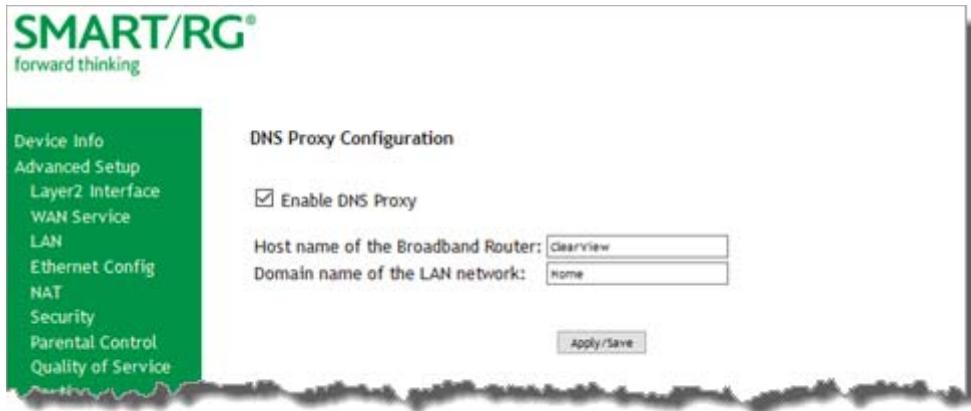
2. If not already selected, click **Enable DNS Proxy**.
   The **Host name** and **Domain Name** fields appear.
3. Enter the host name of the broadband router and the domain name of the LAN network.
4. Click **Apply/Save** to commit your changes.

Storage Service

In this section, you can view information about the storage devices connected to the gateway and manage the user accounts that can access them.

Storage Device Info

On this page, you can view information about storage devices that connect to the gateway and manage the related user accounts.

In the left navigation menu, click **Advanced Setup** > **Storage Service**. The following page appears, showing information about the connected storage device.

User Accounts

On this page, you can manage user accounts for the storage devices.

1. In the left navigation menu, click **Advanced Setup** > **Storage Service** > **User Accounts**. The following page appears.

2. To add a new account:
   a. Click **Add**. the following page appears.

   b. Enter a user name and enter the password twice. Spaces are not allowed in the password.
      Note: The **volumeName** field is not currently used.
   c. Click **Apply/Save** to save your settings. You are returned to the User Accounts page.
3. To remove a user account, click the **Remove** checkbox next to the account entry and then click the **Remove** button. The list refreshes to show your changes were applied.

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.

SMART/RG®
forward thinking

SR506n

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

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

Group Name:

Shared WAN Interface: ☐

Grouped WAN Interfaces

Available WAN Interfaces

ipoe_0_0_35/atm0.2
br_0_0_35.7/atm0.3
ipoe_eth3/eth3.1
pppoe_0_0_35.5/ppp1.1
pppoe_0_0_35/ppp2.4
pppoe_0_0_1/ppp0
No Interface/None

Grouped LAN Interfaces

Available LAN Interfaces

LAN1
LAN2
LAN3
Wireless
Wireless Guest|wl0.1
Wireless Guest|wl0.2
Wireless Guest|wl0.3

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

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, on the Interface Grouping list page, 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 IPv6inIP4 settings.

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

2. Enter a descriptive **Tunnel Name**.

   Skip the **Mechanism** field. Currently, only the **6RD** mechanism is supported.

3. Select the **WAN** and **LAN** interfaces associated with the tunnel you wish to establish.
4. Do one of the following:
     a. To configure the LAN interface settings manually, enter values located below the **Manual** button.
        - **IPv4 Mask Length**: Options are 0 - 32.
        - **6rd Prefix with Prefix Length**: prefix/length, such as: 2002::/64.
        - **Border Relay IPv4 Address**: Enter the IP address for the IPv6 relay server.
     b. To configure these settings automatically, select **Automatic**. The fields below the buttons are hidden.
5. Click **Apply/Save** to commit your changes.

IPv4inIPv6

On this page, you can configure the IPv4inIP6 settings.

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

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

2. Enter a descriptive **Tunnel Name**.
3. Select the **LAN** and **WAN** interfaces associated with the tunnel you wish to establish.
4. Under **Associated LAN Interface**, enter the appropriate value for **AFTR** (Address Family Transition Router). To configure this setting automatically, select **Automatic**. The **AFTR** field is hidden.
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 IPSec 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.

2. Complete the fields, using the information provided in the following table.
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	Enter a descriptive name for this connection
IP Version	Select the IP version associated with your infrastructure. Options are **IPv4** and **IPv6**.
Tunnel Mode	Select the encapsulation method to be used. Options are: • **AH**: Use this mode to encapsulate a packet with AH and IP headers. For authentication, the entire packet is signed. • **ESP**: Use this mode to encapsulate a packet with ESP and IP headers. An ESP trailer is added to the packet for authentication and integrity.
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: • **Subnet**: Allows access to the entire LAN. • **Single Address**: For single host, select this option.
IP Address for VPN	Enter the IP address used for local access.
Mask or Prefix Length	Enter the subnet mask or prefix length for IP address entered for local access. The default is **255.255.255.0**.
Tunnel Access From Remote IP Addresses	Select IP information for site A and B. Options are: • **Subnet**: Allows access to the entire LAN. • **Single Address**: Allows access to a single host.
IP Address for VPN	Enter the IP address used for remote access.
Mask or Prefix Length	Enter the subnet mask or prefix length for IP address entered for remote access. The default is **255.255.255.0**.
Key Exchange Method	Select the key-exchange method to be used for IPSec. Options are: • **Auto(IKE)**: This method uses the negotiated key-exchange method for IPSec. This is the default and recommended for best results. • **Manual**: This method requires that you configure the details.
Authentication Method	Select the method by which the remote end will authenticate. • **Pre-Shared Key**: A key is distributed to authorized users for logging into the system. Enter the key in the **Pre-Shared Key** field. • **Certificate (X.509)**: A certificate is used for authentication. Select the certificate file in the **Certificates** field that appears.
Perfect Forward Secrecy	Select whether a session key is derived from a set of long-term keys is com-

Field Name	Description
	promised if one of the long-term keys in the set is compromised.
	• **Enable**: Prevents long-term key from being compromised.
	• **Disable**: Permits long-term keys to be compromised.
The following fields appear below **Advanced Settings** when **Manual** is selected in the **Key Exchange Method** field.	
Encryption Algorithm	Select the encryption algorithm. Options are **DES**, **3DES** and **AES**.
Encryption Key	Enter the hex value for the selected encryption algorithm.
Authentication Algorithm	Select the authentication algorithm. Options are **MD5** and **SHA1**.
Authentication Key	Enter the hex value for the selected authentication algorithm.
SPI	Enter the hex value for the service provider interface (SPI). The default is **101**.

Advanced IKE Settings

You can configure advanced IKE settings if desired.

1. On the IPSec Settings page, click **Show Advanced 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 **Main** and **Aggressive**.
Encryption Algorithm	Select the encryption algorithm. Options are **DES**, **3DES** , **AES -128**, **AES-192**, and **AES-256**.
Integrity Algorithm	Select the integrity algorithm. Options are **MD5** and **SHA1**.
Select Diffie-Hellman Group for Key Exchange	Select the D-H group. Options are **768bit** - **8192bit**. The default is **1024bit**.
Key Life Time	Enter the number of seconds that a key is valid. The default is **3600** seconds.

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

Certificate

In this section, 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 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. Complete the fields, using the information in the table below. For more information about certificates, refer to the ITU X.509 standard.
3. Click **Apply** to complete the request.

Field Name	Description
Certificate Name	Enter a description of 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.

Field Name	Description
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.

4. To import a certificate and the corresponding private key, on the Advanced Setup > Local Certificates page, click **Import Certificate**. The following page appears.

5. In the **Certificate Name** field, type "cpecert".

6. Paste the **Certificate** details between the **BEGIN** and **END** markers.
7. Paste the **Private Key** information between the **BEGIN** and **END** markers.
8. 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.

1. In the left navigation bar, click **Advanced Setup > Certificate > Trusted CA** and then click **Import Certificate**. The following page appears.
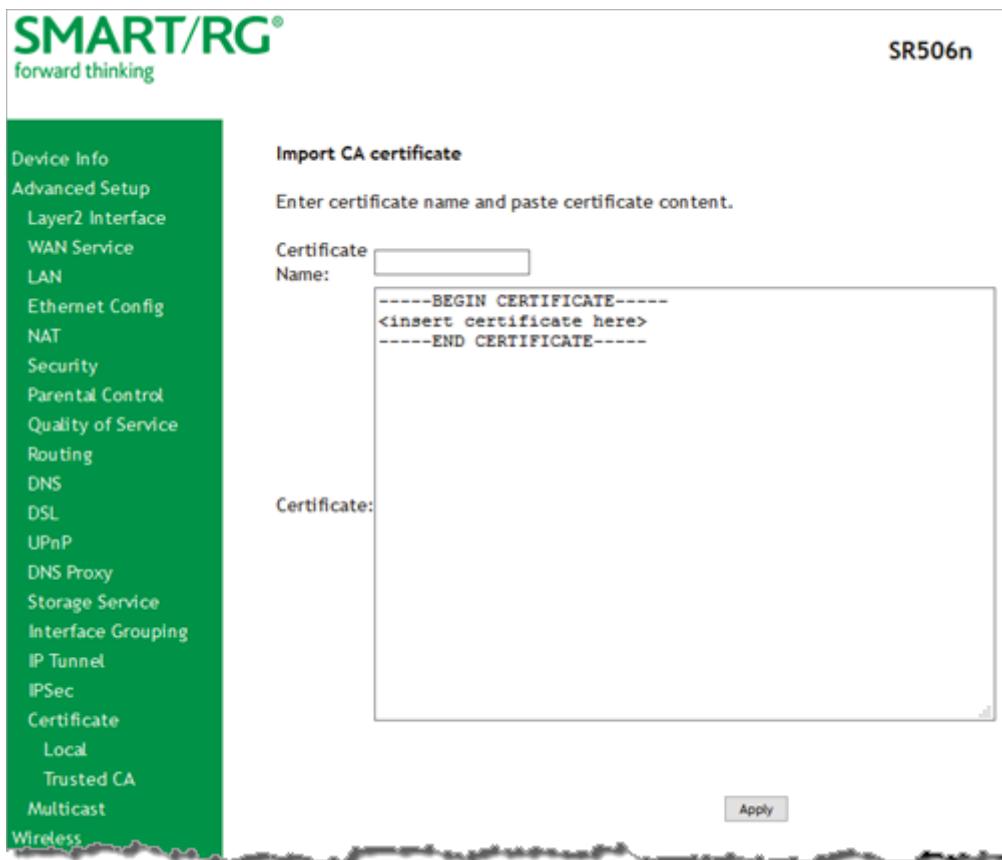
2. In the **Certificate Name** field, type "acscert"
3. Paste the **Certificate** details between the **BEGIN** and **END** markers.
4. Click **Apply** to commit this certificate.

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. Modify the settings as needed, using the information in the table below. The same fields are provided for both IGMP and MLD configuration.
3. To add addresses to the exception lists, in the **Group Exception List** tables, enter any additional address and mask information and then click **Add**.

Note: For the IGMP list, the **Group Address** must be between 244.x.x.x and 239.x.x.x. For the MLD table, the **Group Address** must be a valid IPv6 address.

4. To remove addresses from the exception lists, click the checkbox in the **Remove** column next to the address(es) and then click **Remove Checked Entries**. The list refreshes immediately.
5. 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. Options are: **1 - 4:** 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. **Disable:** IGMP packets are not prioritized. This is the default.
Multicast Strict Grouping Enforcement	Select whether strict grouping is applied to IGMP packets. Options are **Enable** and **Disable**.
IGMP Configuration section	
Default Version	Select the supported IGMP version. Options are **1 - 3**.
Query Interval	Enter the interval (in seconds) at which the multicast router sends a query messages to hosts. the default is **125**. **Note:** 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. The default is **10** seconds. Enter the maximum number of seconds that a host can pick to count down from. The value must be greater than the **Query Interval**. If using IGMP v1, this value is fixed at **10** seconds.
Last Member Query Interval	Enter the maximum response time (in seconds) within which the host must respond to the Out of Sequence query from the router. The default is **10** seconds. 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 **2 - 7**. The default is **2**.
Maximum Multicast	Enter the maximum number of groups allowed. The default is **25**.

Field Name	Description
Groups	
Maximum Multicast Data Sources (for IGMPv3)	Enter the maximum number of data sources allowed. Options are **1** - **24**. The default is **10**.
Maximum Multicast Group Members	Enter the maximum number of multicast groups that can be joined on a port or group of ports. The default is **25**.
Fast Leave Enable	Select whether the IGMP proxy removes group members immediately without sending a query. Options are: ● **Enabled:** Group members are removed immediately. This is the default. ● **Disabled:** Group members are removed after a query is sent and a response received.

WIRELESS

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

Basic

On this page, you can configure basic features of the WiFi LAN interface. You can enable or disable the WiFi LAN interface, hide the network from active scans, set the WiFi 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.

2. Modify the settings as desired, using the information provided in the table below.
3. (*Optional*) Define up to three virtual access points for guest use using the information from the **Wireless - Guest/Virtual Access Points** section of the table below.
4. Click **Apply/Save** to commit your settings.

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

Field Name	Description
Enable Wireless	Select to enable the gateway's WiFi radio.
Enable WiFi Button	Select to enable the gateway's WiFi button functionality.
Enable Wireless Hotspot 2.0	Select whether to enable wireless Hotspot 2.0. (WPA2 is required.) Hotspot 2.0 enables 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. Options are **Enabled** and **Disabled**.
Hide Access Point	Select to hide the access point SSID from end users and passive scanning.
Clients Isolation	Select to prevent LAN client devices from communicating with one another on the wireless network.
Disable WMM Advertise	Select to stop the wireless from advertising Wireless Multimedia (WMM) functionality. Selecting this option can improve transmission performance for voice and video data.
Enable Wireless Multicast Forwarding	Select to disable Wireless Multicast Forwarding (WMF). Multicast traffic is forwarded across wireless clients. Selecting this option can improve the quality of video services such as IPTV.
SSID	Enter the WiFi SSID. For security purposes, this identifier should be unique for your system.
BSSID	Displays the Basic Service Set Identifier (BSSID), the MAC address, assigned to the wireless router.
Country	Select the country in which the gateway is deployed. The wireless channel will adjust to the frequency provision for the selected country.
Country RegRev	Enter the revision number of the registration for the selected country.
Max Clients	Enter the maximum number of clients that can access the route wirelessly. Options are **1** through to the value set in the **Global Max Clients** field on the Wireless > Advanced page. **Note:** Before you can change this setting, you must change the **Global Max Clients** setting.
Wireless - Guest/Virtual Access Points table	
Enabled	Select to enable a virtual wireless access point for guest access.
SSID	Enter the wireless SSID for guests to use.
Hidden	Select to hide the SSID from being broadcast publicly.
Isolate Clients	Select to prevent client PCs from communicating with one another.
Enable WMM Advertise	Select to stop the wireless from advertising Wireless Multimedia (WMM) functionality.

Field Name	Description
Enable WMF	Select to enable Wireless Multicast Forwarding (WMF).
Enable HSPOT	Select to enable Hotspot 2.0 access.
Max Clients	Enter the maximum number of clients that can connect to this access point.
BSSID	Displays the Basic Service Set Identifier or **"N/A"**.

Security

On this page, you can configure network security settings of a wireless LAN interface, either by using the WiFi Protected Setup (WPS) method or by setting the network authentication mode. For WiFi Protected Setup, the following methods are supported:

- PIN entry, a mandatory method of setup for all WPS-certified devices. Options are:
  - **Enter STA PIN**: You must enter the (input) station PIN from the client.
  - **Use AP PIN**: AP generates the device PIN.
- PBC (Push button configuration): Uses a simulated push button in the software. (This is an optional method on wireless clients.)

To use the PIN method, you need a Registrar (access point/wireless gateway) to initiate the registration between a new device and an active access point/wireless gateway.

Note: The PBC method may also need a Registrar when the PIN is all zeros.

Seven types of network authentication modes are supported: Open, Shared, 802.1X, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

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

2. Modify the settings as needed, using the information provided in the field description table below and in the sections that explain each authentication method.

    The fields in the **WPS Setup** section are described in the following table.

Field Name	Description
Enable WPS	Select to enable WiFi Protected Setup. Options are: **Enabled** and **Disabled**. The default is **Disabled**.
Add Client	(*Available for **WPA-PSK**, **WPA2-PSK** and **Open Network Authentication** methods*) Select the method for generating the WPS PIN. Options are: **Enter STA PIN** and **Use AP PIN**. If you select **Enter STA PIN**, type the PIN in the field below the radio button. If you select **Use AP PIN**, the entry field and the **Set Authorized Station MAC** field disappear. To add an enrollee station, click **Add Enrollee**. **Note:** If the **PIN** and **Set Authorized Station MAC** fields are left blank, the **PBC** (push-button) mode is automatically made active.
Set Authorized Station MAC	(*Available only when **Enter STA PIN** is selected*) Enter the MAC address of the authorized (input) station.
Set WPS AP Mode	Select how security is assigned to clients. • **Configured**: The gateway assigns security settings to clients. This is the default. • **Unconfigured**: An external client assigns security settings to the gateway.
Device PIN	This value is generated by the access point.

3. In the **Manual Setup AP** section, select the SSID for the device that you want to configure.
4. Select the **Network Authentication** method and then fill in the fields that appear. The default method is **Mixed WPA2 / WPA-PSK**. Detailed instructions are provided for each method in the following sections:

   - "Open and Shared Network Authentication"
   - "802.1X Network Authentication"
   - "WPA2-PSK and Mixed WPA2/WPA-PSK Network Authentication"
   - "WPA2 and Mixed WPA2/WPA Network Authentication"

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

Open and Shared Network Authentication

The same configuration fields apply for both **Shared** and **Open** authentication types except that **WEP Encryption** is enabled by default for the **Shared** method.

The following fields appear when you select **Open** or **Shared** in the **Network Authentication** field.

Modify the fields as needed and then click **Apply/Save**.

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

Field Name	Description
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are **Enabled** and **Disabled**. The default is **Disabled** for **Open** authentication and **Enabled** for **Shared** authentication.
Encryption Strength	(*Appears when WEP Encryption is set to Enabled*) Select the length of the encryption method. Options are **128-bit** and **64-bit**. **128-bit** is the default and is the more robust option for security.
Current Network Key	(*Appears when WEP Encryption is set to Enabled*) Select which of the four keys is presently in effect.
Network Key 1-4	(*Appear when WEP Encryption is set to Enabled*) Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength.

802.1X Network Authentication

The following fields appear when you select **802.1X** in the **Network Authentication** field. WPS is disabled for this method.

Modify the fields as needed, using the information provided in the table below, and then click **Apply/Save**.

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 server is used to authenticate the hosts on the wireless network.
RADIUS Port	Enter the port number for the RADIUS server. Port 1812 is the default and the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port 1645. Options are **1 - 65535**.
RADIUS Key	(*Optional*) Enter the encryption key (if required) needed to authenticate to the specified RADIUS server.
WEP Encryption	This option is set to **Enabled** by default. It enables WEP (Wired Equivalent Privacy) mode.
Encryption Strength	(*Appears when* **WEP Encryption** *is set to* **Enabled**) Select the length of the encryption method. Options are **128-bit** and **64-bit**. **128-bit** is the default and is the more robust option

Field Name	Description
	for security.
Current Network Key	(*Appears when **WEP Encryption** is set to **Enabled***) Select which of the four keys is presently in effect.
Network Key 1-4	(*Appear when **WEP Encryption** is set to **Enabled***) Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength.

WPA2 and Mixed WPA2/WPA Network Authentication

The following fields appear when you select **WPA2** or **Mixed WPA2/WPA** in the **Network Authentication** field.

Manual Setup AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify
the encryption strength.
Click 'Apply/Save' when done.

Select SSID:	SmartRG-b8ef-5G
Network Authentication:	WPA2
Protected Management Frames:	Disabled
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

Apply/Save

Modify the fields as needed and then click **Apply/Save**.

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

Field Name	Description
Protected Management Frames	Select whether management frames are protected. Options are **Disabled**, **Capable**, and **Required**. The default is **Disabled**.
WPA2 Preauthentication	Select whether clients can pre-authenticate with the gateway while still connected to another AP. Options are **Enabled** and **Disabled**. The default is **Disabled**.
Network Re-Auth Interval	Enter the interval at which the client must re-authenticate with the gateway. The default is **36000** seconds (10 hours).
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: **0** - **65535** seconds. The default is **0**.
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 **1812** is the default and is the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port **1645**. Options are **1** - **65535**.
RADIUS Key	(*Optional*) Enter the encryption key needed to authenticate to specified RADIUS Server.
WPA/WAPI Encryption	Select the encryption standard. This field is displays the option most compatible with the selected network authentication method. Options are: • **AES**: Advanced Encryption Standard. This is the default. • **TKIP+AES**: AES combined with TKIP (Temporary Key Integrity Protocol) allows access by either standard.
WEP Encryption	This option is set to **Disabled** and cannot be changed. It enables Wired Equivalent Privacy (WEP) mode.

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

The following fields appear when you select **WPA2-PSK** or **Mixed WPA2/WPA-PSK** in the **Network Authentication** field.

Modify the fields as needed and then click **Apply/Save**.

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

Field Name	Description
Protected Management Frames	Select whether management frames are protected. Options are **Disabled**, **Capable**, and **Required**. The default is **Disabled**.
WPA passphrase	Enter the security password to be used by this security configuration.
Use base MAC address as default WPA passphrase	Select to use the gateway's MAC address as the passphrase for wireless security.
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 is displays the option most compatible with the selected network authentication method. Options are: • **AES**: Advanced Encryption Standard. • **TKIP+AES**: AES combined with TKIP (Temporary Key Integrity Protocol).
WEP Encryption	This option is set to **Disabled** and cannot be changed. It disables WEP (Wired Equivalent Privacy) mode.

MAC Filter

On this page, you can configure whether wireless clients are allowed to access the wireless network of the wireless gateway.

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

2. In the **Select SSID** field, select the access point that you want to configure.
3. Select the **MAC Restrict Mode**. Options are:
   - **Disabled**: Disable wireless MAC address filtering.
   - **Allow**: Allow the wireless clients in the **MAC Address** list to access the wireless network.

     Note: For this option to work, you must add at least one MAC address to this page.

   - **Deny**: Reject the wireless clients in the **MAC Address** list to access the wireless network.

4. To add a **MAC Address** to the filter list:
    a. Click **Add**. The following page appears.

    b. Enter the **MAC address** of the wireless client.
    c. Click **Apply/Save** to save the address to the list.
5. To remove a MAC address from the list, click the **Remove** check box next to it and then click the **Remove** button. The list refreshes.

Wireless Bridge

On this page, you can configure the wireless bridge features of the wireless LAN interface.

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

2. Modify the fields as needed, using the information provided in the field description table below.

Field Name	Description
Bridge Restrict	Enable or disable the bridge restrict function for MAC addresses in the Remote Bridges MAC Address field. Options are: • **Disabled**: Disable the wireless MAC address filtering function. Any wireless bridge can access the wireless LAN. • **Enabled** and **Enabled (Scan)**: Allow only those bridges selected in the Remote Bridges MAC Address table to access the wireless LAN. This is the default.
Remote Bridges MAC Address	Enter up to four MAC addresses for the remote bridges that are allowed to access the wireless LAN.

3. Click **Apply/Save** to save your settings.

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.

Note: The default settings work for most environments. It is recommended that only experienced users change settings on this page.

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

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	The only option for this field is **2.4GHz**.
Channel	Select the WiFi channel you want to use. This gateway supports auto-channeling. The default is **Auto**. The current channel number displays to the right of the field. All devices in your wireless network must use the same channel in order to work correctly.
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: **0** - **65535** minutes. The default is **15** minutes.
MIMO-OFDM	Select whether to enable this standard. Options are **Auto** and **Disabled**. The default is **Auto**.
Bandwidth	Select the operating bandwidth. Options are **20 MHz**, **40 MHz**, and **80 MHz**. The current bandwidth setting displays to the right of the field.
Control Sideband	This field is disabled.
MIMO Data rate	Select the desired physical transmission rate. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds (**1** - **15**), or you can select **Auto** to have the gateway automatically use the fastest possible data rate and enable the **Auto-Fallback** feature. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client. The default is **Auto**.
RTS/CTS Protection	Select whether to enable 802.11n and legacy clients to both work effectively on the network. Options are: • **Auto**: Provides maximum security but produces 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. This is the default. • **Off**: Provides better throughput.
Support MIMO Clients Only	Select whether to restrict non-MIMO clients from accessing the gateway. Options are **On** and **Off**. The default is **Off**.
RIFS Advertisement	RIFS (Reduced InterFrame Speed) is the time in micro seconds by which the multiple transmissions from a single station is separated. This option Improves performance by reducing dead time required between OFDM transmission. Options are **Off** and **Auto**. The default is **Auto**.
OBSS Co-Existence	Coexistence of Overlapping Basic Service Sets (OBSS) prevents overlapping in the 20 MHz

| Field Name	Description
	and 40 MHz frequencies. Options are: • **Enable**: 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. This is the default. • **Disable:** The gateway advertises and operates in 40 MHz mode regardless of what other networks are configured nearby.
RX Chain Power Save	Select whether to turn on power-save mode. Options are **Disable** and **Enable**. **Note:** Before setting this parameter, set **MIMO-OFDM** to **Auto**.
RX Chain Power Save Quiet Time	Enter the number of minutes that will elapse before quiet time begins. The default is **10**.
RX Chain Power Save PPS	Enter the number of seconds for the throughput threshold for when the router engages power save mode after the quiet time seconds have elapsed. The default is **10**.
54g Rate	This option is set to **1 Mbps** and cannot be changed.
Multicast Rate	Select the multicast transmission rate for the network according to the speed of your wireless network. Select from a range of transmission speeds or select **Auto** to have the gateway automatically use the fastest possible data rate and enable the **Auto-Fallback** feature. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client. Options are **Auto** and **1** - **54** Mbps. The default is **Auto**.
Basic Rate	Select the basic transmission rate ability for the AP. Options are **Default, All, 1 & 2 Mbps**, and **1 & 2 & 5.5 & 6 & 11 & 12 & 24 Mbps**. The default is **Default**.
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 **256** - **2346** bytes. The default is **2346** bytes. **Note:** A high packet error rate is an indication that a slightly increased fragmentation threshold is needed. When possible, the default value of **2346** bytes should be maintained. Poor throughput is a likely result of setting this threshold too low.
RTS Threshold	The gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. If a packet is smaller than this setting, the WLAN client hardware does not invoke its RTS/CTS mechanism. Options are **256** - **2347** bytes. The default value (**2347**, disabled) should be left in place unless you encounter inconsistent data flow. In that case, make minor reductions to this value until the issue is

Field Name	Description
	resolved.
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 **1** - **255**. The default is **1**.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is the period of time (sent with the beacon) that the device waits before sending the beacon again. Enter the time interval (in milliseconds) between beacon transmissions. Options are **1** - **65535** ms. The default is **100** ms, which is recommended.
Global Max Clients	Enter the maximum number of clients that can assess this wireless network at one time. The maximum for 5 GHZ is 80; the maximum for 2.4 GHZ is 128. The default is **128**. **Note**: You must change this field before you can change the **Max Clients** on the Wireless > Basic. page.
Xpress™ Technology	Select whether to enable Xpress Technology. This is a special accelerating technology for IEEE802.11g. Options are **Enabled** and **Disabled**.
Transmit Power	Select the transmission power level. Options are **20%** - **100%**. The default is **100%**.
WMM (WiFi Multimedia)	Select whether to enable this technology. It allows multimedia services (audio, video and voice packets) to get higher priority for transmission. Options are **Auto**, **Enabled**, and **Disabled**. The default is **Enabled**. Warning: If you disable this option, all QoS queues and classifications defined for the wireless network are also disabled.
WMM No Acknowledgment	The acknowledge policy used at the MAC level. Enabling this option allows better throughput but, in a noisy RF environment, higher -963error rates may result. The default is **Disabled**, meaning that an acknowledgement packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. Disabling the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree. Options are **Enabled** and **Disabled**. The default is **Disabled**.
WMM APSD	APSD (Automatic Power Save Delivery) is an automatic power saving feature. Enabling ensures very low power consumption. WMM Power Save is an improvement to the 802.11e amendment, adding advanced power management functionality to WMM. Options are **Enabled** and **Disabled**. The default is **Enabled**.
Band Steering	Select whether to detect if the client has the ability to use two bands. When enabled,

Field Name	Description
	the less-congested 5GHz network is selected (by blocking the client's 2.4GHz network). Options are **Disabled** and **Enabled**. The default is **Disabled**.
Enable Traffic Scheduler	Select whether to enable scheduling of traffic to improve efficiency and increase usable bandwidth for some types of packets by delaying other types. Options are **Disable** and **Enable**. The default is **Disable**.
Airtime Fairness	Select how the gateway will manage the receiving signal with other devices. Options are **Disable** and **Enable**. The default is **Enable**.

Station Info

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

In the left navigation menu, click **Wireless** > **Station Info**. The following page appears.

To update the data, click **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 connections.

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

2. To refresh the displayed data, 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.

3. To test at the VP level instead of at an individual VC connection, click **Test With OAM F4**.

4. To test additional connections, click **Next Connection**. The page refreshes to show data for the next connection and the **Previous Connection** button appears. Repeat steps 2-4 for each connection.

Ping Host

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

1. In the left navigation menu, click **Diagnostics Tools** > **Ping Host**. The following page appears.
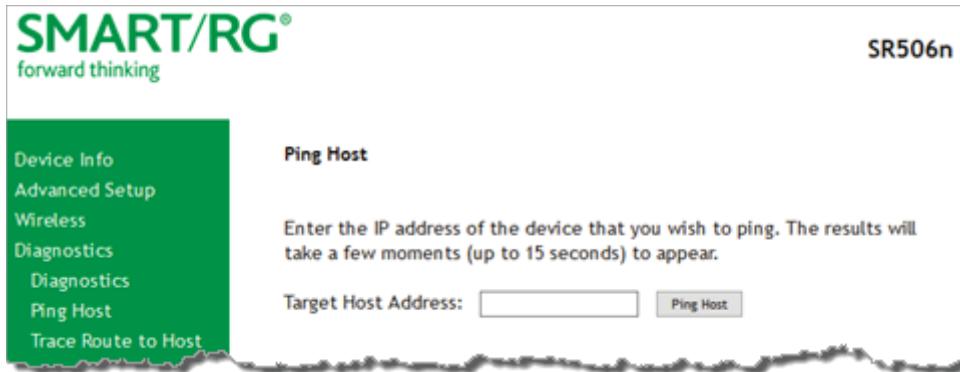
2. Enter the host name or IP address.

3. Click **Submit**. The details of the ping appear on the page.
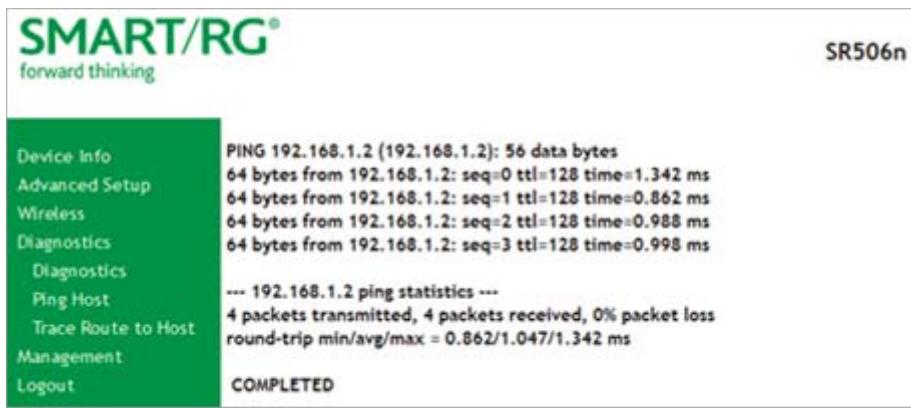
Trace Route to Host

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.
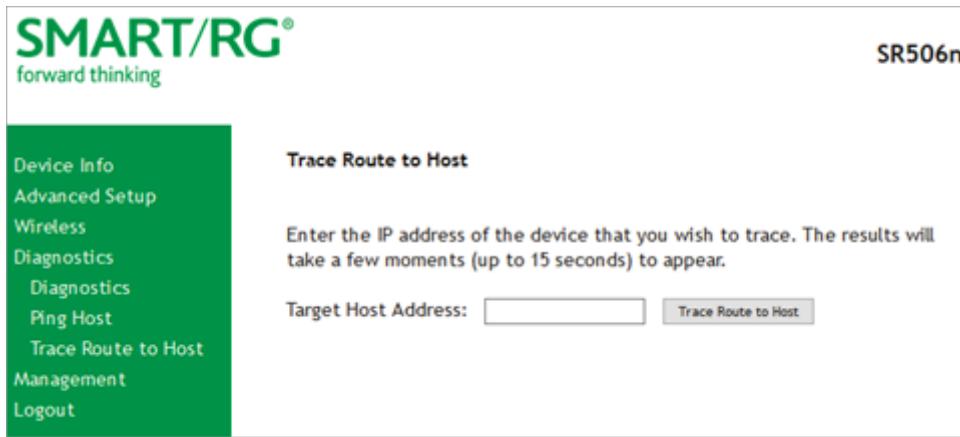
2. Enter the host name or IP address that you want to trace.
3. Click **Trace Route to Host**. The details of the trace appear on the page.
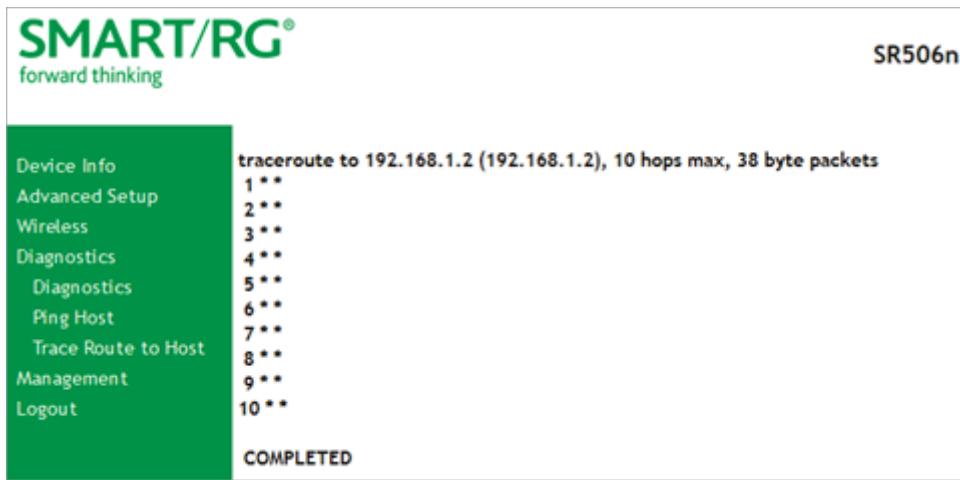
Settings

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**. The following page appears.
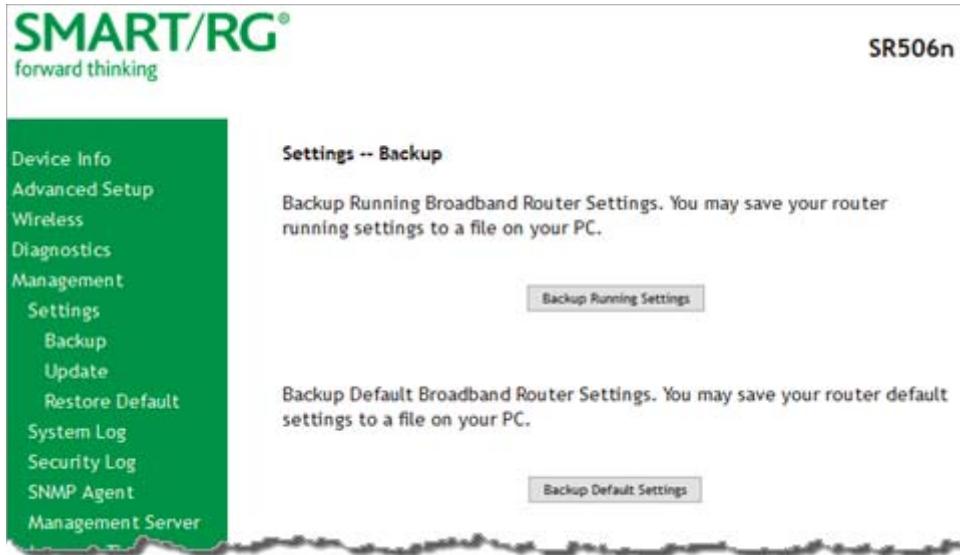

2. To save a backup file of the currently running settings to a local drive, click **Backup Running Settings**. The File Upload dialog box appears. Click **OK**. The backupsettings.conf file is created in your default download location.
3. To save a backup file of the default settings to a local drive,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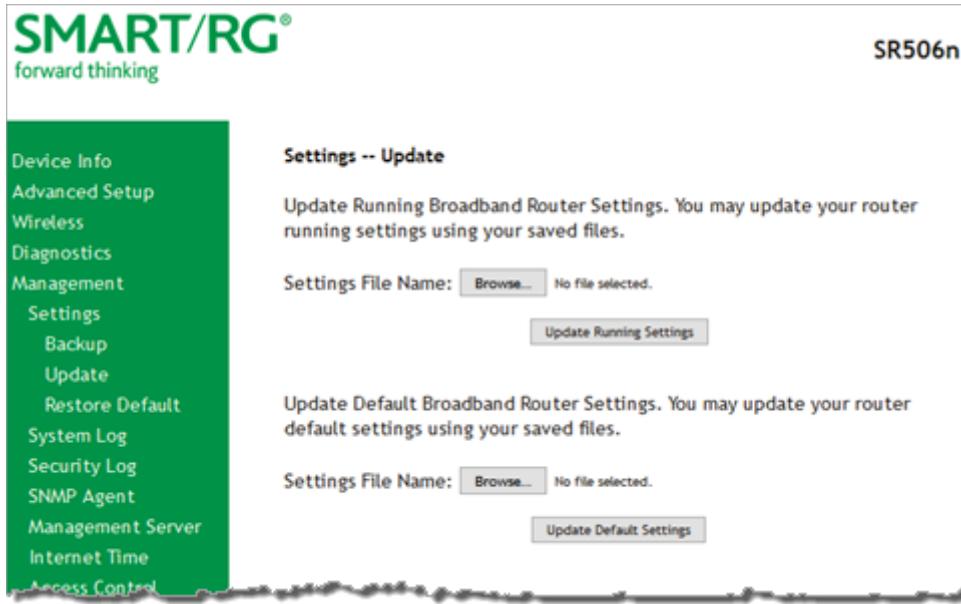

2. Click the **Browse** button for the type of setting you wish to restore.
3. Locate the desired .conf file on your local system and click **Open**.
4. Click the appropriate **Update** button.
   The gateway reboots when the update has completed.

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 and the default settings overwrite the previous settings.

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.

2. To view the contents of the system log, click **View System Log**. The System Log details page appears.

3. To update the displayed entries, click **Refresh**.

4. To modify the system log settings:
    a. Click **Configure System Log**. The System Log - Configuration page appears.
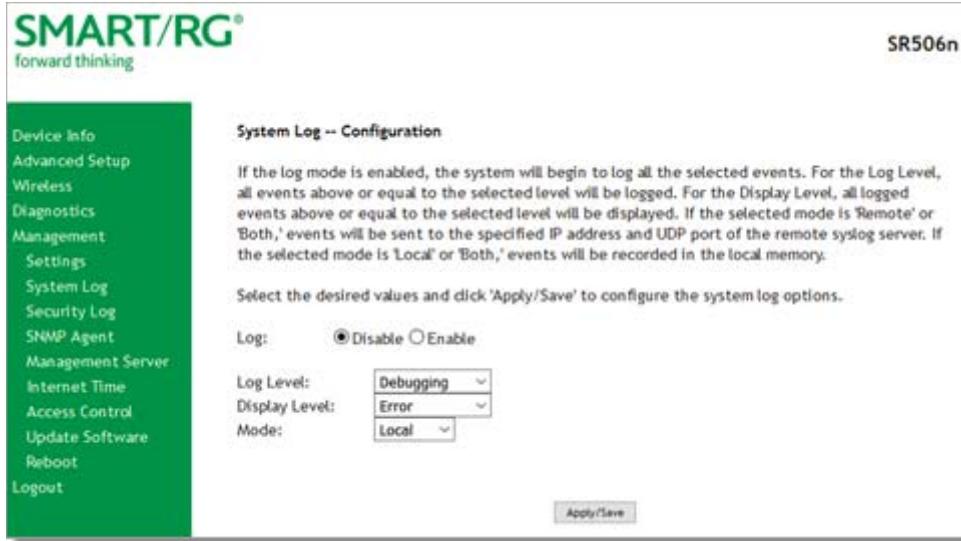
    b. Modify the settings as needed, using the information provided in the following table.

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

    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/failure
- Authorized login success/failure
- Authorized user logged out
- Security lockout added/removed
- Authorized/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 it 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 **public**.
Set Community	The options are public and private. The default is **private**.
System Name	The name of the system.
System Location	(*Optional*) 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

SmartRG gateways support TR-069 based standards for remote management, including STUN server configuration. In this section, you can configure the gateway with details about the management ACS (Auto Configuration Server) to which this gateway will be linked.

TR-069

The TR-069 client screen contains default connection parameters and generally only needs to be enabled, pointed to the ACS URL, and any required ACS Username and ACS Password entered. This manual does not cover the setup of your ACS. If you need to modify the default settings, consult the materials provided by your ACS vendor to determine the appropriate parameters and server settings.

SmartRG products can accommodate several ACS products, including:

- Device Manager by SmartRG
- Cisco Prime Home
- Calix Consumer ACS

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

2. Complete the necessary fields per the instructions from your ACS platform vendor.

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

Field Name	Description
Inform	Select whether to disable this function.
Inform Interval	Enter the frequency (in seconds) at which the CPE (gateway) checks in with the ACS to sync and exchange data. A typical production environment has CPEs informing to the ACS once/day or every 86,400 seconds.
ACS URL	Enter the URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST 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 certificate-based authentication. You can include a port specification suffix if your ACS platform requires it, e.g., http://customer.acs.wanmanagmentservices.com:30005 where 30005 is the port number. The default port is **30005**.
ACS User Name	Enter the user name by which this gateway logs in to the ACS. This is usually "admin".
ACS Password	Enter the password to authenticate the above user name. This is usually "admin".
WAN Interface used by TR-069 client	Select any WAN, LAN, Loopback or configured connection to identify how this gateway will connect to the ACS.
Display SOAP messages on serial console	Select whether to enable the display of messages on consoles.

3. (*Optional*) To configure the modem client Connection Request mechanism used by your ACS for communication with subscriber gateways, click **Connection Request Authentication**. Additional fields appear.
Note: Consult with your ACS vendor for any specific connection request requirement impacted by the following settings.

Field Name	Description
Connection Request Username	Enter the user name by which this gateway authenticates the ACS. For example, many ACS platforms use "admin" or "tr069".
Connection Request Password	Enter the password by which this gateway will authenticate to the ACS.
Connection Request Port / URL	There is typically no need to set the Connection Request URL as it is normally established automatically based on the effective WAN IP. The port can be configured if needed. An example value might be "http://xxx.xxx.xxx.xxx:30005/" where the xxx values are specific WAN IP octet numbers.

Field Name	Description
	The default port value is **30005**.

4. 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.
5. Click **Apply/Save** to commit your changes.

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 STUN Configuration page appears.
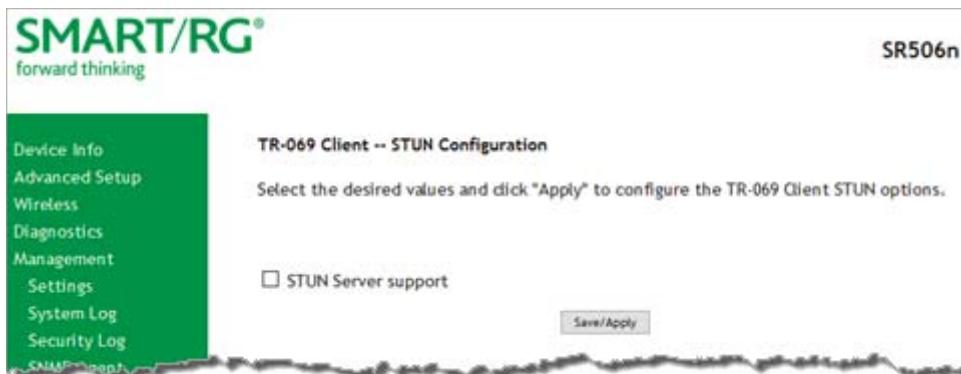
2. To view the required STUN settings, click **STUN Server Support**.
3. Complete the fields in accordance with the implementation specifics of your server. Information about the fields is provided in the table below.
4. Click **Save/Apply** to commit your changes.

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.
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 hidden.
STUN Server Maximum Keep Alive Period *	Enter the maximum keepalive time in seconds. Options are any integer. The default is **-1** (no maximum time).
STUN Server Minimum Keep Alive Period *	Enter the maximum keepalive time in seconds. Options are any integer. The default is **0**.

* 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.

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

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 allows for coordinated refresh on the bindings for mappings it uses. For further information, review STUN-related RFCs.

Internet Time

On this page, you can configure the gateway to synchronize its time with the Internet time servers. This feature is enabled by default.

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

2. Click **Automatically synchronize with Internet time servers**. Additional fields appears.
3. Select the desired time servers.
4. Select the **Time zone offset**.
5. Click **Apply/Save** to save and apply your settings.
6. To disable this feature, click the **Automatically synchronize with Internet time servers** check box to clear it.
7. Click **Apply/Save**.

Access Control

In this section, you can manage access to your gateway and network. You can configure passwords, accounts, services, the logout timer, and access lists.

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.** The following page appears.

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 category, the subordinate boxes are also selected. For example, if you select **Support Tools**, **Port Mirroring** and **Factory Reset** are selected as well.
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 delete the default user accounts (Admin, Support, MFG, or User) but you can disable all but the Admin accounts. The default passwords for the default user accounts are listed in the "Default Passwords" section of this topic.

1. Make sure you are logged into the gateway as an Admin or Support user.
2. In the left navigation bar, click **Management** > **Access Control** > **Accounts** and then click **Delete/Modify Account**. The Delete/Edit Account page appears.

3. In the **Select an account** field, select the account you wish to modify or delete.
4. Do one of the following:
    a. To disable or enable the account, click the appropriate **Enable/Disable account** button and then click **Update Account** (at the borrom of the page).
    b. To modify the account, check or clear the check boxes for the privileges as needed, and then click **Update Account** to commit your changes.
    c. To delete the account, click **Delete Account**. A confirming message appears. Click **OK**.

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.

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

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

Field Name	Description
Services	Select the SCL services that you want to be enabled. Options are **FTP**, **HTTP**, **ICMP**, **SNMP**, **SSH**, **TELNET**, and **TFTP**.
Use encrypted HTTP (S)	Click this checkbox to implement secured HTTP. **Warning:** When you click this option, the gateway reboots.
LAN	Select the services enabled on LAN side firewall. Depending on configuration settings made elsewhere in the GUI, this column may be read-only. **Note:** ICMP is an always-enabled service by default and has no checkbox.
WAN	Select the services enabled on the WAN side firewall.

Field Name	Description
WAN Port Number	Enter the port to which the access control applies on the WAN side for the given service. Except where noted below, the service ports are the default ports for the WAN.
Service port options	
FTP	FTP service access.
HTTP	HTTP Service access. (This is in association with the specified port.) The default port is **80**.
ICMP	ICMP service access.
SNMP	SNMP service access.
SSH	SSH service access. (This is in association with the specified port) The port default is **22**.
TELNET	TELNET service access.
TFTP	TFTP service access.

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. In the **New Password** and **Confirm Password** fields, enter the new password.
3. Click **Apply/Save** to implement the change.

Access List

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

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**. The following page appears.

    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.

1. In the left navigation bar, click **Management** > **Access Control** > **Logout Timer**. The following page appears.
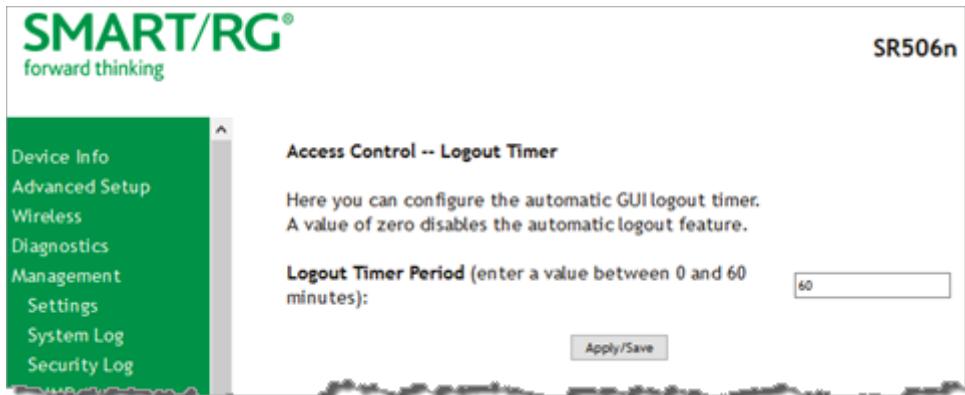
2. In the **Logout Timer Period** field, type the number of minutes after which a session will be ended. Options are **0** - **60** minutes. The default is **15** minutes. To disable this feature, enter a zero (**0**) in the field.

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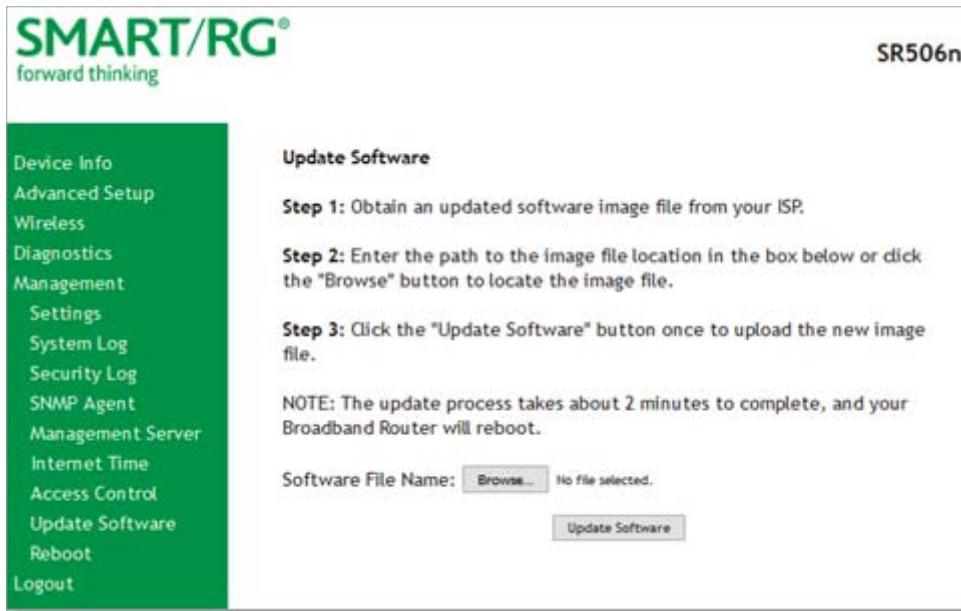
2. Follow the on-page instructions. When the update has completed, the gateway reboots.

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.

LOGGING OUT

1. To log out of your gateway, click **Logout** in the left navigation menu. The logout page appears.
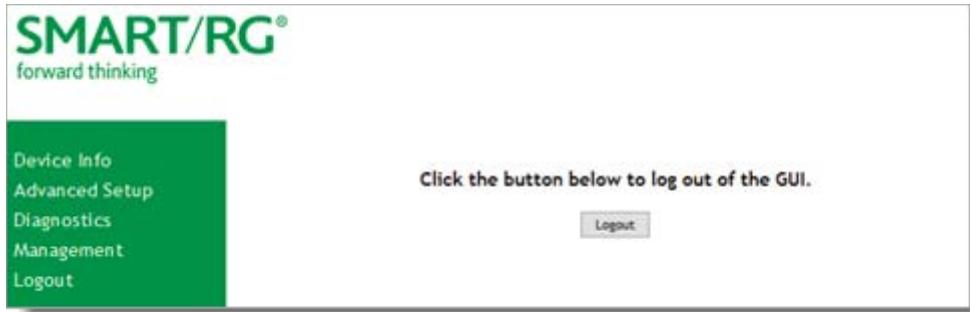
2. Click the **Logout** button. A success message appears.

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 anincorrect 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

APPENDIX A: ADVANCED FEATURES

This appendix outlines the advanced feature set for SmartRG brand home gateway products.

Connect-and-Surf (Automatic Broadband Connection Configuration)

Connect-and-Surf 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.

Notes

- If you prefer to configure your SmartRG's WAN interface manually, connect a laptop to any of the LAN ports and follow the instructions in the "LOGGING IN TO YOUR GATEWAY'S UI" 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. SmartRG Inc. maintains an activation server that associates a device's MAC address with its service provider's ACS settings. The MAC addresses are entered into the activation server prior to delivery. Gateways contact the activation server to have their ACS settings modified upon 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.

TR-069 Remote Management: Automated Configuration Server 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. SmartRG gateways provide maximum remote manageability and the highest level of visibility into the connected home yielding:

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

SmartRG works closely with TR-069 automated configuration server (ACS) solutions providers to ensure "plug-n-play" interoperability. See the following table for examples.

Device Manager by SmartRG	**Device Manager by SmartRG** Device Manager is a robust TR-069 ACS management platform which utilizes a secure cloud-based deployment designed to be repeatable and portable. For more information, go to the Device Manager page on the SmartRG web site.
	Calix Compass/Consumer Connect ACS 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.
AFFINEGY	**Affinegy ACS** SmartRG gateways have been tested to confirm maximum interoperability with the Affinegy ACS solution.
CISCO	**Cisco Prime Home™ ACS** SmartRG gateways have a long history of Prime Home (formerly ClearVision) ACS interoperability.

APPENDIX B: GATEWAY FEATURE COMPARISON

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. For more information, contact SmartRG Support.

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	✓	✓	Dual-band concurrent 802.11ac	✓	✓	✓
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	✓	✓	✓
SR506n	ADSL2+, Ethernet	4 FE	✓	✓	802.11n	✓	✓	✓
SR505n	Tri-mode: ADSL2+, VDSL2, GigE	3 FE + 1 GE	✓	✓	802.11n	✓	✓	✓
SR501	ADSL2+, Ethernet	1 FE	✓	✓				
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+	1 FE	✓	✓	802.11n	✓	✓	✓

Model	Broadband Con-nection	LAN ports	LAN Device Dis-covery	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	✓	✓				

APPENDIX C: FCC STATEMENTS

This appendix includes the FCC statements that apply to the products described in this User Manual.

FCC - PART 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom case of this equipment is a label that contains, among other information, a product identifier in the format US: VW7DL01ASR506N, and REN: NAN for this equipment.

This equipment uses the following USOC jacks: RJ-11/RJ45/USB/Power Jacks!

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

REN (RINGER EQUIVALENT NUMBERS) STATEMENT

REN=0.1A

Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

If this equipment VW7DL01ASR506N causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment VW7DL01ASR506N , for repair or warranty information, please contact SmartRG,Inc.. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this VW7DL01ASR506N does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

This product meets the applicable Industry Canada technical specifications. / Le présent matériel est conforme aux spe-cifications techniques applicables d'Industrie Canada.

IC-CS03 statement

This product meets the applicable Industry Canada technical specifications. / Le présent matériel est conforme aux spe-cifications techniques applicables d'Industrie Canada

The Ringer Equivalence Number (REN) is an indication of the maximum number of devices allowed to be connected to a tele-phone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five. / L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

FCC Statement

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 install-ation. 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 inter-ference 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 inter-ference 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.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

Canada Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The device meets the exemption from the routine evaluation limits in section 2.5 of RSS 102 and compliance with RSS-102 RF exposure, users can obtain Canadian information on RF exposure and compliance.

Le dispositif rencontre l'exemption des limites courantes d'évaluation dans la section 2.5 de RSS 102 et la conformité à l'exposition de RSS-102 rf, utilisateurs peut obtenir l'information canadienne sur l'exposition et la conformité de rf.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Cet émetteur ne doit pas être Co-placé ou ne fonctionnant en même temps qu'aucune autre antenne ou émetteur. Cet équipement devrait être installé et actionné avec une distance minimum de 20 centimètres entre le radiateur et votre corps.

This radio transmitter (11130A–SR506N) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (identifier le dispositif par son numéro de certification ou son numéro de modèle s'il fait partie du matériel de catégorie I) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	Nov 2016	Initial release of document.