

501 SE Columbia Shores Boulevard, Suite 500 Vancouver, Washington 98661 USA

+1 360 859 1780 / smartrg.com

## / Gateway User Manual

Model: SR501

Release 1.4

Firmware Version 2.6.2.5

July 2020



## **Table of Contents**

Welcome!	3
Purpose & Scope	
Intended Audience	
Getting Assistance	
	J
Copyright and Trademarks	3
Disclaimer	
Getting Familiar with your Gateway	
LED Status Indicators	5
Connections	
Buttons	
ON/OFF Switch	
Decet Dutter	0
Reset Button	6
Installing your SmartRG Gateway	7
Logging in to your SmartRG Gateway's UI	7
Device Info	8
Summary	
WAN	
Statistics	
LAN	
WAN Service	
xTM	11
xDSL	12
References	
Route	
ARP	
DHCP	
DHCPv6	
VPN	20
Advanced Setup	. 21
Layer2 Interface	
ATM Interface	
PTM Interface	
WAN Service	
PPP over Ethernet	
IP over Ethernet	
Bridging	45
LAN	49
IPv6 Autoconfig	
Ethernet Config	53
NAT	55
Virtual Servers	
Port Triggering	
DMZ Host	
Security	
IP Filtering - Outgoing	60
IP Filtering - Incoming	
MAC Filtering	63
Adding a MAC Filtering Rule	63
Parental Control	0J
Time Restriction	
URL Filter	
Quality Of Service	
QoS Config	67
QoS Config Supported DSCP Values	67
QoS Queue Config	68
QoS Classification	
QoS Port Shaping	
Routing	/4

Default Gateway	74
Static Route	75
Policy Routing	
RIP (Routing Information Protocol)	76
DNS	
DNS Server	70
Dynamic DNS	
Static DNS	
DSL	81
Advanced settings	
UPnP	85
DNS Proxy	
Interface Grouping	
IP Tunnel	89
IPv6inIPv4	
IPv4inIPv6	
IPSec	
Advanced IKE Settings	93
Certificate	94
Local	94
Trusted CA	96
Power Management	97
Multicast	98
Diagnostics	
Diagnostics	
Ethernet OAM	
Ping Host	104
Trace Route to Host	
Management	
Settings	106
Backup	
Update	106
Restore Default	
System Log	
Security Log	
Management Server	110
TR-069 Client	
STUN Config	113
Internet Time	
Access Control	
Accounts	
Add an Account	116
Modify or Delete an Account	119
Default Passwords	119
Services	120
Passwords	121
Access List	121
Logout Timer	
Update Software	122
Reboot	123
Logging Out	125
Appendix C: FCC Statements	
FCC - Part 68	126
REN (RINGER EQUIVALENT NUMBERS)	
STATEMENT	126
IC-CS03 statement	126
FCC Statement	
FCC Radiation Exposure Statement	127
ree Rudiation Exposure Statement	14/



## **Table of Contents**

Canada Statement	
Revision History	





## Welcome!

Thank you for purchasing this SmartRG product.

SmartRG offers solutions that simplify the complex Internet ecosystem. Our solutions include hardware, software, applications, enhanced network insights, and security delivered via a future-proof operating system. Based in the USA, SmartRG provides local, proactive software development and customer support. We proudly offer the best, most innovative broadband gateways available.

Learn more at www.SmartRG.com.

### Purpose & Scope

This User Manual provides SmartRG customers with installation, configuration and monitoring information for the SR501 gateway.

### Intended Audience

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

### Getting Assistance

Frequently asked questions are provided on the SmartRG Web site.

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

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

### Copyright and Trademarks

Copyright © 2020 by SmartRG, Inc., an ADTRAN company. Published by SmartRG, Inc. All rights reserved.

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.



### 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.





# Getting Familiar with your Gateway

This section contains descriptions of the SR501 gateway's lights, ports, and buttons.

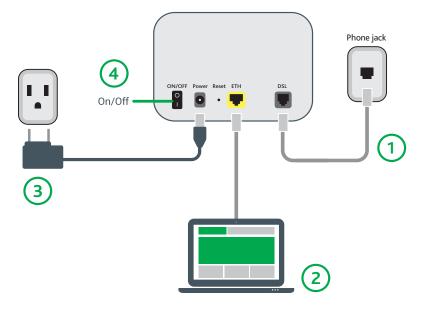
### LED Status Indicators

Your SR501 gateway has four indicator lights (LEDs) on the front. The following table describes the LEDs and their functions.

LED	Action	Description
Internet	•	Connected to Internet
	•	Authentication failed.
DSL	٢	Connecting to DSL
	•	Connected to DSL
	٢	Transferring data
LAN	٠	Connected to LAN
	٢	Transferring data
POWER	•	Unit is on

### Connections

Below is a diagram of how to install your SR501 gateway. This information is also in the Quick Start Guide enclosed with your gateway.



The ports depicted in this example are described below.





Port	Description
Power	Connect the power cord included with your gateway to this connector. Use only the power supply included with your gateway. Intended for indoor use only.
	The yellow RJ45 port on the back of your gateway is used to connect client devices such as computers and printers to your gateway
DSL	The grey RJ12 port labeled DSL is specifically intended for connection to an internet provider via a DSL (Digital Subscriber Line) service.

### **Buttons**

#### **ON/OFF Switch**

The ON/OFF toggle switch is located on the back of the gateway and turns the gateway on and off.

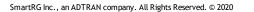
#### **Reset Button**

The Reset button is a small hole in the gateway's enclosure with the actual button mounted behind the surface. This style of pushbutton 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 back of the unit.

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

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





### Installing your SmartRG Gateway

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

- 1. Attach your computer's RJ45 connection to the SmartRG gateway's LAN port.
- 2. If your computer is not already set up to acquire IP addresses using DHCP, configure your computer's IP interface to do so. (For instructions on logging in to a SmartRG gateway configured for "bridge mode" operation, see the Note below.)

### Logging in to your SmartRG Gateway's UI

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

1. Open a browser and enter the gateway's default address: http://192.168.1.1 in the address bar. The Authentication Required dialog box appears.

	-	
0	A username and password are being requested by http://192.168.1.1. The site says: "Broadband	
	Router"	_
User Name:		
Password:		-
in the second		-
	OK Cancel	

2. Enter the default username and password: admin/admin, and click OK. The Device Info summary page appears.

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

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

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

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



## **Device Info**

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 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.

RG°				SR50
Device Info				
Board ID:		KD218C26A	Г	
Symmetric CPU Threa	ds:	2	1	
Build Timestamp:		200626_1023		
Software Version:		2.6.2.5	1	
Configuration File Orig	gin:	SmartRG		
Bootloader (CFE) Vers	ion:	1.0.38-118.3		
DSL PHY and Driver Ve	ersion:	A2pv1042r.d26u		
Uptime:		0D 0H 0M 54S		
System Base MAC Add	ress:	3c:90:66:4c:64:29		
Serial Number:		SR501AA0A6-000101	4	
LAN IPv4 Address: Default Gateway: WAN IPv4 Address Primary DNS Server:	192. 0.0.0	168.1.1 0.0 0.0	our WAN connection.	
	Board ID: Symmetric CPU Thread Build Timestamp: Software Version: Configuration File Orig Bootloader (CFE) Vers DSL PHY and Driver Ve Uptime: System Base MAC Add Serial Number: This information reflect LAN IPv4 Address: Default Gateway: WAN IPv4 Address Primary DNS Server:	Board ID:         Symmetric CPU Threads:         Build Timestamp:         Software Version:         Configuration File Origin:         Bootloader (CFE) Version:         DSL PHY and Driver Version:         Uptime:         System Base MAC Address:         Serial Number:         This information reflects the         LAN IPv4 Address:       192.         Default Gateway:          WAN IPv4 Address       0.0.0         Primary DNS Server:       0.0.0	Board ID:KD218C26ASymmetric CPU Threads:2Build Timestamp:200626_1023Software Version:2.6.2.5Configuration File Origin:SmartRGBootloader (CFE) Version:1.0.38-118.3DSL PHY and Driver Version:A2pv1042r.d26uUptime:0D 0H 0M 54SSystem Base MAC Address:3c:90:66:4c:64:29Serial Number:SR501AA0A6-000101This information reflects the current status of yoLAN IPv4 Address:192.168.1.1Default Gateway:.0.0.0	Board ID:KD218C26ASymmetric CPU Threads:2Build Timestamp:200626_1023Software Version:2.6.2.5Configuration File Origin:SmartRGBootloader (CFE) Version:1.0.38-118.3DSL PHY and Driver Version:A2pv1042r.d26uUptime:DD 0H 0M 545System Base MAC Address:3c:90:66:4c:64:29Serial Number:SR501AA0A6-0001014This information reflects the current status of your WAN connection.LAN IPv4 Address:192.168.1.1Default 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).



9

#### SMART/RG SR501 Device Info Summary WAN Info Summary WAN Statistics Route ARP DHCP DHCPv6 VPN Advanced Setup Diagnostics Management Interface lgmp Pxy gmp Src Enbl MLD Sr Enbl IPv4 Addres IPv6 ddre br\_0\_0\_35 Bridge Disabled Disabled 0.0.0.0 atm0.3 Disabled Disabled Disabled Disabled Disabled Disabled Unconfigured (null) ppp0.1 pppoe\_0\_0\_35 PPPoE Disabled Disabled Disabled Disabled Disabled Disabled Enabled Enabled Unconfigured Username autoconfig 0.0.0.0 (null) ppp1.2 pppoe\_0\_0\_35 PPPoE Disabled Disabled Disabled Disable Disabled Disabled Enabled Enabled Unconfigured Username autoconfig 0.0.0.0 (null) IPv4: Unconfigured IPv6: Unconfigured 0.0.0.0 IPoE Disabled Enabled ptm0 ipoe\_0\_0\_1 Enabled Disabled Disabled Disabled Disable Enabled (null) Management Logout

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

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.
Туре	The service type. Options are <b>PPPoE</b> , <b>IPoE</b> , and <b>Bridge</b> .
VlanMuxId	The VLAN ID. Options are <b>Disabled</b> or <b>0-4094</b> .
IPv6	The state of IPv6. Options are <b>Enabled</b> and <b>Disabled</b> .
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 <b>Enabled</b> and <b>Disabled</b> .
Firewall	The state of the Firewall. Options are <b>Enabled</b> and <b>Disabled</b> .
Status	The status of the WAN connection(s). Options are <b>Disconnected</b> , <b>Unconfigured</b> , <b>Con-</b> <b>necting</b> , and <b>Connected</b> .
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 and w10 (Wireless Interface) are included.

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

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

SMART/	RG°																SR501		
Device Info Summary	Statistics	LAN																	
WAN					F	Receive	ed		Transmitted										
Statistics	Interface		То	tal		Multicast Unicas		Unicast	ast Broadcast		Total			Multicast		Unicast	Broadcast		
LAN		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts		
WAN Service	LAN1	461137	2988	0	7	0	1762	1028	198	583493	6123	0	0	0	40	429	5654		
хTM																			
xDSL																			
Route	Reset Statist	ics																	
ARP																			
рнср																			

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

Field Name	Description
Interface	LAN interface.
Received & Tra	ansmitted 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.

SMART/I	KG																SR501
evice Info	Statistics W	AN															
Summary		Received Transmitted															
WAN	Service		То	tal		Multi	cast	Unicast	Broadcast		То	tal		Multi	cast	Unicas	Broadcast
Statistics	Description	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs				Pkts	Pkts
LAN	br_0_0_35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
WAN Service	pppoe_0_0_35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
хTМ	pppoe_0_0_35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
xDSL	ipoe_0_0_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Route																	
ARP																	
DHCP	Reset Statistics																
DHCPv6																	

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: <b>pppoe</b> , <b>ipoe</b> , and <b>bridge</b> .					
Received & Tra	nsmitted columns					
Bytes	Number of packets in bytes.					
Pkts	Number of packets.					
Errs	Number of error packets.					
Drops	Number of dropped packets.					

#### хТМ

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.



SMART/RC	0										SR501
Device Info Summary WAN	Port Number	ln Octets	Out Octets	In Packets	Inte Out Packets	rface Stat In OAM Cells	out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
Statistics LAN				-							
WAN Service xTM						Reset					
×DSL				~~~~~	محمد		~~~~~		man		

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.

	1			
Device Info	Statistics xDSL			
Summary				
WAN	Last Synchronized:	-		
Statistics	Retrain Count:		0	
LAN				
WAN Service	Mode:		1	
XTM	Traffic Type:	-		
xDSL	Status:		Disabled	
Route	Link Power State:	2		
ARP				
DHCP		Downstream	Upstream	
DHCPv6	Line Coding(Tretis):			
VPN	SNR Margin (0.1 dB):			
Idvanced Setup	Attenuation (0.1 dB):			
Diagnostics	Output Power (0.1 dBm) Attainable Rate (Kbps):			
Vanagement	Rate (Kbps):			
Logout	Rate (hups).	-		
oPoor	Super Frames:			
	Super Frame Errors:			
	R5 Words:			
	RS Correctable Errors:			
	RS Uncorrectable Errors	5		
	HEC Errors:			
	OCD Errors:			
	LCD Errors:			
	Total Cells:			
	Data Cels:			
	Bit Errors:			
	Total ES:			
	Total SES:			
	Total UAS:			

- 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.

ADSL BER Test - Result The ADSL BER test comp	leted successfully.				
Test Time (sec):	20				
Total Transferred Bits:	0x000000068FAA500				
Total Error Bits:	0x000000000000000000000000000000000000				
Error Ratio:	0.00e+00				
Ce	10				

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

Field Name	Description
Last Synchronized	The date and time that the gateway was last synchronized.
Retrain Count	The number of times the gateway was synchronized
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 Upstrea	am columns
Line Coding (Trellis)	State of theTrellis Coded Modulation. Options are <b>On</b> and <b>Off</b> .
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)	<ul> <li>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:</li> <li>Single frame bearer and single latency operation</li> </ul>
	<ul> <li>Signal-to-Noise Ratio Margin (SNRM) to be equal or above the SNR Target Margin</li> </ul>
	<ul> <li>BER not to exceed the highest BER configured for one (or more) latency paths</li> </ul>
	<ul> <li>Latency not to exceed the highest latency configured for one (or more) latency paths</li> </ul>



Field Name	Description
	<ul> <li>Accounting for all coding gains available (e.g., trellis coding, RS FEC) with latency bound</li> </ul>
	Accounting for the loop characteristics at the instant of measurement [2]
Output Power (0.1 Bm)	Transmit power from the gateway to the DSL loop relative to one Milliwatt (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
	<ul> <li>Latency not to exceed the highest latency configured for one (or more) latency paths</li> </ul>
	<ul> <li>Accounting for all coding gains available (e.g., trellis coding, RS FEC) with latency bound</li> </ul>
	Accounting for the loop characteristics at the instant of measurement [2]
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	n 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	
Super Frames	The number of xDSL OH Frames transmitted/received.

15



Field Name	Description
Super 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 trans- mitted/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 Code- words received.
RS Codewords Corrected	(Visible only for gateways connected via DSL) Total number of Reed-Solomon Code- words corrected.
RS Codewords Uncor- rected	(Visible only for gateways connected via DSL) Total number of Reed-Solomon Code- words 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] <u>ITU-T Recommendation G.992.1</u> (1999), Asymmetric digital subscriber line (ADSL) transceivers.

[2] ITU-T Recommendation G.992.3 (2005), Asymmetric digital subscriber line transceivers 2 (ADSL2).

[3] <u>ITU-T Recommendation G.997.1</u> (2006), Physical layer management for digital subscriber line (DSL) transceivers.



[4] ITU-T Recommendation I.432.1 (1999), B-ISDN user-network interface - Physical layer specification: General characteristics.

### Route

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

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

SMART/I	RG°							SR501
Device Info Summary WAN Statistics	Device Info Flags: U - up, D - dynamic (	! - reject,					state	
Route	Destination	Gateway	Subr	et Mask	Flag	Metric	Service	Interface
ARP DHCP	192.168.1.0	0.0.0.0	255.	255.255.0	U	0		br0
DHCPv6 VPN	IPv6 Route		-					
Advanced Setup Diagnostics Management	Flags: U - up, D - dynamic (						state	
Logout	Destination	Next Hop	Flag	Metric	Service	Interf	ace	
	fe80::/64		U	256		br0		
	fe80::/64		U	256		eth0		

Field Name	Description
Destination	Destination IP addresses.
Gateway	(For IPv4 only) Gateway IP address.
Next Hop	(For IPv6 only) Next hop IP address.
Subnet Mask	Subnet mask for the gateway.
Flag	Status of the flags. See detailed descriptions above the tables.
Metric	Number of hops required to reach the default gateway.



Field Name	Description
Service	Service type.
Interface	WAN/LAN interface.

### 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.

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

SMART/R	G°				SR501
Device Info Summary WAN	Device Info -	- ARP Flags	HW Address	Device	1
Statistics Route			c8:f7:50:b4:61:c1		

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: <b>Complete</b> , <b>Per-</b> manent, and <b>Published</b> .
HW Address	The hardware (MAC) address of the host.
Device	The system level interface by which the host is connected. Options are: <b>br(n)</b> , <b>atm(n)</b> , and <b>ptm(n)</b> .

### DHCP

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

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



SMART/	RG°			SR501
Device Info Summary	Device Info DHC	P Leases		
WAN	Hostname	MAC Address	IP Address	Expires In
Statistics	kdadamo7390w10	c8:f7:50:b4:61:c1	192.168.1.2	23 hours, 51 minutes, 48 seconds
Route				
ARP				
DHCP			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	

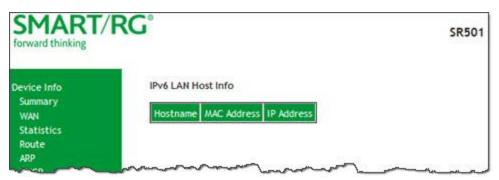
The fields on this page are explained in the following table.

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.

### DHCPv6

On this page, you can view the host name, the IP address assigned by the DHCPv6 server, and the MAC address corresponding to the IP address.

In the left navigation bar, select **Device Info > DHCPv6**. The following screen appears.





Field Name	Description
Hostname	Host name of each connected LAN device.
MAC Address	MAC address for each connected LAN device.
IP Address	IP address for each connected LAN device.

### VPN

On this page, you can view details about the IPSec tunnels configured for your gateway.

In the left navigation bar, select **Device Info** > VPN. The following screen appears.

SMART/RG	SR501
Device Info Summary WAN Statistics Route	Device Info IPSec Tunnels Tunnel Name Interface Remote Gateway LAN-side Addresses Remote-side Addresses Enabled Connection State

Field Name	Description
Tunnel Name	Name of the IPSec tunnel.
Interface	WAN interface used by the tunnel.
Remote Gateway	WAN IP address for the tunnel.
LAN-side Addresses	Acceptable IP addresses defined for the LAN side.
Remote-side Addresses	Acceptable IP addresses defined for the WAN side.
Enabled	Indicates whether the tunnel is enabled or disabled.
Connection State	Indicates whether the tunnel connection is active or inactive.



# **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.

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



SMART/R		SR5
Device Info	ATM PVC Configuration	
Advanced Setup		
Layer2 Interface	This screen allows you to con	figure a ATM PVC.
ATM Interface	Les augus	
PTM Interface	VPI: 0 [0-255]	
WAN Service	VCI: 35 [32-65535]	
LAN		
Ethernet Config	Select DSL Latency	
NAT	Path0 (Fast)	
Security	Path1 (Interleaved)	
Parental Control	La ratin (intercarea)	
Quality of Service	Select DSL Link Type (EoA is f	or PPPoE, IPoE, and Bridge.)
Routing	EoA	
DNS	O PPPOA	
DSL	O IPOA	
UPnP	C non	
DNS Proxy	Encapsulation Mode:	LLC/SNAP-BRIDGING 🤝
Interface Grouping		Provide the second seco
IP Tunnel	Service Category:	UBR Without PCR 🗸
IPSec	Minimum Cell Rate:	[.1 [cels/s] (-1 indicates no shaping)
Certificate	Minimum Ces Rate.	(i [cels/s] ( i indicates in shaping)
Power Management	Select Scheduler for Queues	of Equal Precedence as the Default Queue
Multicast	Weighted Round Robin	nen versionen anderen en e
Diagnostics	O Weighted Fair Queuing	
Management		
Logout	Default Queue Weight:	1 [1-63]
	Default Queue Precedence:	s [1-8] (lower value, higher priority)
	VC WRR Weight:	1 [1-63]
	VC Precedence:	a [1-8] (lower value, higher priority)
	For single queue VC, the defa	P among unequal precedence VC's and WRR among equal precedence VC's. sult queue precedence and weight will be used for arbitration. recedence and weight will be used for arbitration.
		Sack Apply/Save

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

Field Name	Description
VPI	Enter a Virtual Path Identifier. A VPI is an 8-bit identifier that uniquely identifies a net- work 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: <b>32-65535</b> .



Field Name	Description
Select DSL Latency	Select the level of DSL latency. Options are:
	<ul> <li>Path0 Fast: No error correction and can provide lower latency on error free lines.</li> <li>Path1 Interleaved: Error checking that provides error free data which increases latency.</li> </ul>
	If you are not certain which method is best, you can select both.
Select DSL Link Type	Select the linking protocol. <b>EoA</b> is the most popular with <b>PPPoA</b> a close second (used with many legacy ISPs). Options are:
	• 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:
	<ul> <li>LLC/ENCAPSULATION: (Available for PPOA only) Logical Link Control (LLC) encapsulation protocols used with multiple PVCs</li> </ul>
	<ul> <li>LLC/SNAP-BRIDGING: LLC used to carry multiple protocols in a single PVC.</li> <li>LLC/SNAP-ROUTING: (<i>Available for IPoA only</i>) LLC used to carry one protocol per PVC.</li> </ul>
	<ul> <li>VC/MUX: Virtual Circuit Multiplexer creates a virtual connection used to carry one protocol per PVC.</li> </ul>
Service Category	Select the bit rate protocol. Options are:
	• <b>UBR without PCR:</b> Unspecified Bit Rate with no Peak Cell Rate, flow control or time synchronization between the traffic source and destination. Commonly used with applications that can tolerate data / packet loss.
	• UBR with PCR: Same as above but with a Peak Cell Rate.
	• <b>CBR:</b> Constant Bit Rate relies on timing synchronization to make the network traffic predictable. Used commonly in Video and Audio traffic network applications.
	• 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.
	• <b>Realtime VBR:</b> Realtime Variable Bit Rate. Same as the above option but relies on timing and synchronization between the destination and source. This category is commonly used in networks with compressed video traffic.
Minimum Cell Rate	Minimum allowable rate (cells per second) at which cells can be sent on a ATM net-



Field Name	Description
	work. The default is <b>-1</b> (no shaping).
· ·	The algorithm used to schedule the queue behavior. VC scheduling is different than the default queues. Options are:
Default Queue	<ul> <li>Weighted Round Robin: Packets are accessed in a round robin style. Classes can be assigned.</li> </ul>
	Weighted Fair Queuing: Packets are assigned to a specific queue.
Default Queue Weight	Enter a default weight of the specified queue. Options are: 1-63.
Default Queue Pre- cedence	Enter a precedence for the specified queue. Options are: <b>1</b> - <b>8</b> .
VC WRR Weight	The weight of the specified virtual channel queue. Options are <b>1-63</b> .
VC Precedence	The priority of the specified virtual channel queue. Options are <b>1-8</b> .

#### **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.



SMART/R			SR50
Device Info	PTM Configuration		
Advanced Setup Layer2 Interface	This screen allows you to configur	e a PTA	A flow.
ATM Interface	Select DSL Latency		
PTM Interface	Path0 (Fast)		
WAN Service LAN	Path1 (Interleaved)		
Ethernet Config NAT	Select Scheduler for Queues of Eq Weighted Round Robin	ual Pred	cedence as the Default Queue
Security	O Weighted Fair Queuing		
Parental Control		_	1
Quality of Service	Default Queue Weight:	1	[1-63]
Routing	Default Queue Precedence:	8	[1-8] (lower value, higher priority)
DNS	Default Queue Minimum Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
DSL	Default Queue Shaping Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
UPnP DNS Proxy	Default Queue Shaping Burst Size:		[bytes] (shall be >=1600)
Interface Grouping	8	aok /	Apply/Save
IP Tunnel IPSec			

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

Field Name	Description
Select DSL Latency	Select the level of DSL latency. Options are:
	<ul> <li>Path0 Fast: No error correction and can provide lower latency on error free lines.</li> </ul>
	<ul> <li>Path1 Interleaved: Error checking that provides error free data which increases latency.</li> </ul>
	If you are not certain which method is best, you can select both.
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	Enter a default weight of the specified queue. Options are: 1-63.



Field Name	Description
Default Queue Pre- cedence 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 Rate	The shaping rate for the specified queue. Options are: <b>1-0</b> Kbps. The default is <b>-1</b> (no shaping).
Default Queue Shaping Burst Rate	The maximum rate at which traffic can pass through the queue. Options are <b>1600</b> or greater.



### 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.

SMART/RG®		SR501
Device Info	WAN Service Interface Configuration	
Advanced Setup Layer2 Interface WAN Service	Select a layer 2 interface for this service	
LAN Ethernet Config NAT	Note: For ATM interface, the descriptor string is (portId_vpi_vci) For PTM interface, the descriptor string is (portId_high_low) Where portId=0> DSL Latency PATH0 portId=1> DSL Latency PATH1	
Security Parental Control	portId=4> DSL Latency PATHO&1 low =0> Low PTM Priority not set low =1> Low PTM Priority set	
Quality of Service Routing DNS	high =0> High PTM Priority not set high =1> High PTM Priority set	
DSL UPnP DNF Proven	atm0/(0_0_35) ~	
DNS Proxy Interface Grouping IP Tunnel	Back Next	
upcoc	man man	



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

SMART/R	G°	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security	WAN Service Configuration Select WAN service type: PPP over Ethernet (PPPoE) IP over Ethernet Bridging	
Parental Control Quality of Service Routing DNS	Enter Service Description: pppor_0_0_35	
DSL UPnP DNS Proxy	For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.	
Interface Grouping IP Tunnel IPSec Certificate	Enter 802.1P Priority [0-7]: Enter 802.1Q VLAN ID [0-4094]: Select VLAN TPID:	-1 Select a TPID ↓
Power Management Multicast Diagnostics	Internet Protocol Selection:	
Management Logout	Back Next	

- 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.
	Options are <b>0</b> - <b>7</b> . The default is <b>0</b> .
ority	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.
Enter 802.1Q VLAN ID	Options are <b>0</b> - <b>4094</b> . The default is <b>-1</b> (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.



Field Name	Description
Select VLAN TPID	Select the TPID for this VLAN. Options are <b>0x8100</b> , <b>0x88A8</b> , and <b>0x9100</b> .
Internet Pro- tocol Selection	Select the IP version. Options are IPv4 Only, IPv4&IPv6 (Dual Stack), and IPv6 Only.



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

SMART/R forward thinking	SR501		
Device Info	PPP Username and Password		
Advanced Setup Layer2 Interface	PPP usually requires that you have a user name and password to establish your connection. In		
ATM Interface PTM Interface WAN Service LAN	PPP Username: autoconfig Use base MAC address as username PPP Password:  PPPoE Service Name:		
Ethernet Config NAT	Authentication Method: AUTO ~		
Security Parental Control Quality of Service	Link Control Protocol LCP Keepalive Period (s): 30		
Routing DNS DSL	LCP Retry Threshold:		
UPnP	PPP IP extension		
DNS Proxy Interface Grouping	Advanced DMZ		
IP Tunnel IPSec	Non DMZ         IP Address:         192.168.2.1           Non DMZ         Net Mask:         255.255.0		
Certificate Power Management	Use Static IPv4 Address		
Multicast			
Diagnostics Management Logout	Use Static IPv6 Address		
Logout	Enable IPv6 Unnumbered Model		
	Launch Dhcp6c for Address Assignment (IANA)		
	✓ Launch Dhcp6c for Prefix Delegation (IAPD)		
	Retry PPP password on authentication error		
	Max PPP authentication retries (1-65536): 65536 (use 65536 to retry forever)		
	Enable PPP Debug Mode		
	Bridge PPPoE Frames Between WAN and Local Ports		
	Enable Firewall		
	Enable SYN Flood rules     Enabling the SYN Flood rules can degrade TCP performance.		
	Network Address Translation Settings		
	Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).		
	Enable NAT		
	Enable Fullcone NAT		
	Enable SIP ALG		
	IGMP Multicast		
	Enable IGMP Multicast Proxy		
	Enable IGMP Multicast Source		
	MLD Multicast		
	Enable MLD Multicast Proxy     Enable MLD Multicast Source		
	MTU size [1370-1492]: 1492 Use Base MAC Address on this WAN interface (Note: only select this for one WAN interface (Note: only select this for one WAN		
	interface) Back Next		



#### 6. Modify the fields as needed.

Field Name	Description	
PPP Username	Enter the username required for authentication to the PPP server.	
	To use the gateway's MAC address as the user name, click the Use base MAC address as username checkbox.	
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:	
Method	• AUTO: Attempt to automatically detect handshake protocol (listed below)s.	
	• PAP: Password Authentication Protocol (plaintext passwords).	
	<ul> <li>CHAP: Challenge Handshake Authentication Protocol. (MD5 hashing scheme on passwords).</li> </ul>	
	<ul> <li>MSCHAP: Microsoft Challenge Handshake Authentication Protocol. (Microsoft encryp ted password authentication protocol).</li> </ul>	
Link Control Protoco	lsection	
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 declar- ing 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.	
Advanced DMZ	( <i>Available only when <b>PPP IP Extension</b> is selected</i> ) 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 b cast 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 gate- way. The default is <b>255.255.255.0</b> .	
Use Static IPv4 Address	Click the checkbox and then specify the IPv4 Address to apply for this WAN service.	
Use Static IPv6 Address	Click the checkbox and then specify the IPv6 Address to apply for this WAN service.	
Enable IPv6 Unnumbered Model		



Field Name	Description	
Launch Dhcp6c for Address Assignment (IANA)	(Available only when IPv4&IPv6 (Dual Stack) is selected for the Internet Protocol field Select to launch the dhcp6c client deamon to request and configure IPv6 addresses and host network configuration information.	
Launch Dhcp6c for Pre- fix Delegation (APD)	(Available only when <b>IPv4&amp;IPv6 (Dual Stack)</b> is selected for the <b>Internet Protocol</b> field) Select to enable your DHCPv6 server to allow your gateway to ask for an IPv6 prefix (sub- net) that it can then split up and delegate to the clients it serves. This option is selected by default.	
Retry PPP password	This option is selected by default. To disable it, click the checkbox to clear it.	
on authentication error	In the Max PPP authentication retries field, enter the maximum number of PPP authen- tication 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	This option is selected by default and <i>enables</i> functions in the <b>Security</b> sub-menu. To <i>dis-able</i> the firewall, click the checkbox to clear it.	
Enable SYN Flood rules	Select to enable rules for preventing SYN flood distributed denial of service attacks.	
Network Address Tran	slation Settings section	
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	( <i>Appears when Enable NAT is selected</i> ) Click to enable Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications.	
IGMP Multicast section		
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.	
MLD Multicast section		
Enable MLD Multicast	(Available only for IPv6 environments) Click to enable MLD multicast. Used by IPv4 hosts to	
Proxy	report multicast group memberships to any neighboring multicast routers.	



Field Name	Description
	( <i>Available only for IPv6 environments</i> ) Click to enable this service to act as an MLD mul- ticast source.
	Enter the MTU (Maximum Transmission Unit) size for SmartRG gateways supporting a gig- abit-capable WAN interface. Options are <b>1370</b> - <b>1492 bytes</b> . The default is <b>1492</b> bytes.
	Use the SmartRG Devices Base (Primary) MAC address. When unchecked, a unique MAC is assigned for each service.

7. Click Next. The following page appears.

SMART/R	G	SR501
Device Info Advanced Setup	Routing Default Gateway	
Layer2 Interface WAN Service LAN Ethernet Config NAT	default gateways but only one the higest and the last one the	can have multiple WAN interfaces served as system will be used according to the priority with the first being elowest priority if the WAN interface is connected. by removing all and adding them back in again.
Security Parental Control	Selected Default Gateway Interfaces	Available Routed WAN Interfaces
Quality of Service Routing DNS DSL UPnP DNS Proxy	ppp0.1	ppp1.2
Interface Grouping IP Tunnel IPSec	~	~
Certificate Power Management Multicast	IPv6: Select a preferred wan i	nterface as the system default IPv6 gateway.
Diagnostics Management Logout	Selected WAN Interface pppo	e_0_0_35/ppp1.2 🤍
		Back Next

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 D	NS Server settings.
----	-------------	--------------------	---------------	-------------------	---------------------

SMART/R forward thinking	G° SR501
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Management Logout	<section-header>         DYS Server Onfiguration         Sect DNS Server Interface from available WAN interfaces OR enter static DNS server for diddresses for the system. In ATM mode, if only a single PVC with IPoA or static DNS server IP addresses must be entered. DIS Server Interfaces can have multiple WAN interfaces served as system dns servers ab to the priority with the first being the higest and to the priority with the first being the higest and to the priority with the first being the higest and to the priority with the first being the higest and to the addresses must be entered. Priority order can be achieved by removing all and adding them back in again.         Image: Imag</section-header>
	IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.
	Obtain IPv6 DNS info from a WAN interface: WAN Interface selected: ipoe_0_0_1/ptm0      Use the following Static IPv6 DNS address: Primary IPv6 DNS server: Secondary IPv6 DNS server: Back Next

- 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.



- SMART/RG SR501 prward thinking Device Info WAN Setup - Summary Advanced Setup Make sure that the settings below match the settings provided by your ISP. Layer2 Interface WAN Service 0/0/35 LAN Connection Type: PPPoE Ethernet Config Service Name: NAT pppoe\_0\_0\_35 Service Category: UBR IP Address: Automatically Assigned Quality of Service Service State Enabled Routing Enabled NAT Full Cone NAT: Disabled UPhP Firewall: Enabled DNS Proxy Interface Grouping GMP Multicast Proxy: Disabled IGMP Multicast Source Enabled: Disabled IP Tunnel MLD Multicast Proxy: IPSec Disabled Certificate MLD Multicast Source Enabled: Disabled Power Management Quality Of Service: Disabled Multicast Diagnostics Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications. Vanagement Back Apply/Sale orout
- 12. Click Next. The summary page appears indicating that your PPPoE WAN setup is complete.

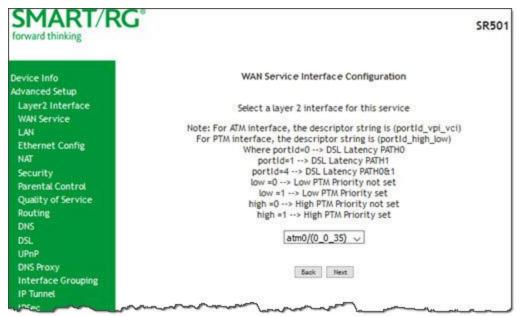
13. Review the summary and either click Apply/Save to commit your changes or click Back to step through the pages in reverse order to make any necessary alterations.

#### **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.

SMART/R	G°	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security	WAN Service Configuration Select WAN service type: O PPP over Ethernet (PPPoE) IP over Ethernet Bridging	
Security Parental Control Quality of Service Routing DNS DSL UPnP	Enter Service Description: ippe_0_0_35 For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.	
orm DNS Proxy Interface Grouping IP Tunnel IPSec Certificate		ct a TPID 🗸
Power Management Multicast Diagnostics Management Logout	Internet Protocol Selection: IPV4 Only ~ Back Next	



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

Field Name	Description
Enter Service Description	( <i>Optional</i> ) Enter a name to describe this configuration.
Enter 802.1P Pri- ority	Options are <b>0</b> - <b>7</b> . The default is <b>0</b> . For tagged service, enter values in this field and the <b>802.1Q VLAN ID</b> field. For untagged service, enter - <b>1</b> (disabled) in this field and the <b>802.1Q VLAN ID</b> field.
Enter 802.1Q VLAN ID	Options are <b>0</b> - <b>4094</b> . The default is <b>-1</b> (disabled). For tagged service, enter values in this field and the <b>802.1P Priority</b> field. For untagged service, enter <b>-1</b> (disabled) in this field and the <b>802.1P Priority</b> field.
Select VLAN TPID	Select the TPID for this VLAN. Options are <b>0x8100</b> , <b>0x88A8</b> , and <b>0x9100</b> .
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.

SMART/F	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics	WAN IP Settings         Enter information provided to you by your ISP to configure the WAN IP settings.         Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPOE mode.         If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway. <ul> <li>Obtain an IP address automatically</li> <li>Option 60 Vendor ID:</li> <li>Option 61 IAID:</li> <li>Option 61 DUID:</li> <li>(8 hexadecimal digits)</li> <li>Option 77 User ID:</li> <li>Option 125:</li> <li>Disable</li> <li>Enable</li> </ul> Option 50 Request IP         Address:         Option 51 Request         1800         Leased Time:         Option 54 Request Server         Address:         WAN Nubnet Mask:         WAN gateway IP         Address:
Logout	<ul> <li>Advanced DMZ</li> <li>Non DMZ IP Address: 192.168.2.1</li> <li>Non DMZ Net Mask: 255.255.255.0</li> </ul> Enter information provided to you by your ISP to configure the WAN IPv6 settings. Notice: If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface. If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64. ● Obtain an IPv6 address automatically □ Dhcpv6 Address Assignment (IANA) □ Dhcpv6 Prefix Delegation (IAPD) ○ Use the following Static IPv6 address: WAN IPv6 Address/Prefix Length: Specify the Next-Hop IPv6 address for this WAN interface. Num Next-Hop IPv6 Address: WAN Next-Hop IPv6 Address: WAN Next-Hop IPv6 Address: Wan Next-Hop IPv6 Address:



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

Field Name	Description	
Obtain an IP address auto- Select when you want the ISP to automatically assign the WAN IP to the gate matically		
Option 60 Vendor ID	(Optional) Broadcast a specific vendor ID for the DHCP server to accept the device.	
Option 61 IAID	( <i>Optional</i> ) Interface Association Identifier (IAID). A unique identifier for an IA, chosen by the client.	
Option 61 DUID	( <i>Optional</i> ) DHCP Unique Identifier (DUID) is used by the client to get an IP address from the DHCP server.	
Option 77 User ID	( <i>Optional</i> ) Enter the user class ID that should be used to filter traffic.	
Option 125	( <i>Optional</i> ) Select whether to enable local devices to automatically receive DHCP options from the server. This option is disabled by default. To enable it, click <b>Enabled</b>	
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	( <i>Optional</i> ) Select this option to enable Advanced DMZ on the WAN service. For more information, see the knowledgebase on SmartRG Support site.	
Non DMZ IP Address	If using the Advanced DMZ feature, you can enter a specific vendor ID that will be broadcast for the DHCP server to accept the device, 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 <b>255.255.255.0</b> .	
IPv6 settings	······	
The following fields and set	when either IPv6 Only or IPv4&IPv6 (Dual Stack) network protocols are selected on	



Field Name	Description		
the WAN Service Configura	the WAN Service Configuration page.		
Obtain IPv6 address auto- matically	ss auto- 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 Assign- ment (IANA)	Select this option for the CPE to receive WAN IP from ISP.		
Dhcpv6 Prefix Delegation (IAPD)	Select this option for the CPE to generate the WAN IP's prefix from the server's REST by MAC address.		
Use the following Static IPv6 address	Select this option to manually declare the v6 Static IP information provided by your ISP.		
WAN IPv6 Address/Prefix Length	If entering a static IP address, enter the IP address / prefix length. If you do not spe- cify a prefix length, the default of <b>/64</b> is used.		
WAN 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.

SMART/F	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Management Logout	Network Address Translation Settings         Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).         Enable NAT         Enable Fullcone NAT         Enable Firewall         Enable SYN Rood rules         Enable SYN Flood rules can degrade TCP performance.         Enable SIP ALG
	<ul> <li>Enable MLD Multicast Proxy</li> <li>Enable MLD Multicast Source</li> <li>Use Base MAC Address on this WAN interface (Note: only select this for one WAN interface)</li> </ul>

8. 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.



FIELD NAME	DESCRIPTION
Enable NAT	Enables 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.
	<b>Note:</b> 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 SYN Flood rules	Select to enable rules for preventing SYN flood distributed denial of service attacks.
Enable Firewall	Select to enable functions in the Security sub-menu.
Enable SIP ALG	( <i>Appears when Enable NAT is selected</i> ) Enables Session Initiation Protocol (SIP) pass- 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.
Enable MLD Multicast Proxy	(Available only for IPv6 environments) Click to enable MLD multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable MLD Multicast Source	(Available only for IPv6 environments) Click to enable this service to act as an MLD mul- ticast 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.



9. Click Next. The following page appears.

SMART/R	G°	SR501
Device Info Advanced Setup	Routing Default Gateway	
Layer2 Interface WAN Service LAN Ethernet Config NAT	default gateways but only one the higest and the last one th	t can have multiple WAN interfaces served as system will be used according to the priority with the first being e lowest priority if the WAN interface is connected. I by removing all and adding them back in again.
Security Parental Control	Selected Default Gateway Interfaces	Available Routed WAN Interfaces
Quality of Service Routing DNS DSL UPnP DNS Proxy	ppp0.1	ptm0 A ppp1.2
Interface Grouping IP Tunnel IPSec	~	~
Certificate Power Management Multicast Diagnostics	IPv6: Select a preferred wan	interface as the system default IPv6 gateway.
Management Logout	Selected WAN Interface ipoe	_0_0_1/ptm0 🧹
		Eack Hent

10. 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.



SMART/R	G SR5	01
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	DNS Server Configuration Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.	0420
Security Parental Control Quality of Service Routing DHS DSL UPNP DRS Proxy Interface Grouping IP Turnel IPSec Certificate Power Management Matricast Diagnotics Management Logout	Select DNS Server Interface from available WAN interfaces:   Select DNS Server   Available WAN Interfaces   ppp0.1   pp0.1   pp0.1   pp1.2 pp1.2 pp1.2 pp1.2 pp1.2 pp1.2 pp1.2 pp1.2 pp1.2 pp1.3 pp1.4 pp1.5 Secondary DNS server: Secondary DNS server: Primary DNS server: Secondary DNS server: Secondary DNS server:	
	Note that selecting a WAN Interface for IPv6 DNS server will enable DHCPv6 Client on that Interface.  Obtain IPv6 DNS info from a WAN Interface: WAN Interface selected:  iooe_0_1/ptm0  O Use the following Static IPv6 DNS address: Primary IPv6 DNS server: Secondary IPv6 DNS server:	

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

- 12. 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.
- 13. Alternatively, you can enter static DNS IP addresses in the Use the following Static DNS IP address section.
- 14. 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.



15. Click Next. The summary page appears.

en and an and			
Device Info Advanced Setup Layer2 Interface	WAN Setup - Summary Make sure that the settings below	match the settings prov	rided by your ISP.
WAN Service	PORT / VPI / VCI:	0/0/1	1
Ethernet Config	Connection Type:	IPoE	1
NAT	Service Name:	ipoe_0_0_1	1
Security	Service Category:	UBR	1
Parental Control	IP Address:	Automatically Assigned	1
Quality of Service Routing	Service State:	Enabled	1
DNS	NAT:	Enabled	1
DSL	Full Cone NAT:	Disabled	1
UPnP	Firewall:	Enabled	1
DNS Proxy Interface Grouping	IGMP Multicast Proxy:	Disabled	1
IP Tunnel	IGMP Multicast Source Enabled:	Disabled	1
IPSec	MLD Multicast Proxy:	Disabled	1
Certificate	MLD Multicast Source Enabled:	Disabled	1
Power Management	Quality Of Service:	Disabled	1

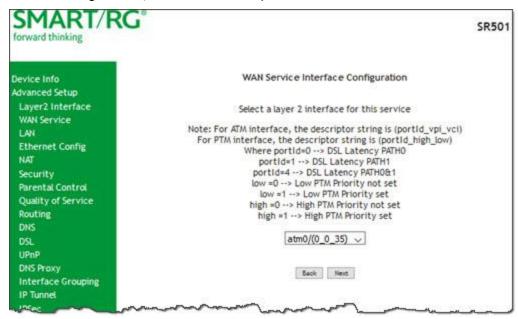
16. Review the summary and either click Apply/Save to commit your changes or click Back to step through the pages in reverse order to make any necessary alterations.

### 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.

SMART/R	G	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel	WAN Service Configuration         Select WAN service type:         PPP over Ethernet (PPPoE)         IP over Ethernet         Bridging         Allow as IGMP Multicast Source         Allow as MLD Multicast Source         Enter Service Description:         br.d.gsed service, enter valid 802.1P Priority and 802.1Q VLAN ID.         For tagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.         Enter 802.1P Priority [0-7]:	7
IPSec Certificate Power Management Multicast Diagnostics Management	Enter 802.1Q VLAN ID [0-4094]: -1 Select VLAN TPID: Select VLAN TPID:	kt a TPID 🗸
Logout	Back Next	

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 Descrip- tion	( <i>Optional</i> ) Enter a name to describe this configuration.
Enter 802.1P Priority	Options are <b>0</b> - <b>7</b> . The default is -1 (disabled). For tagged service, enter values in this field and the <b>802.1Q VLAN ID</b> field. For untagged service, accept the default of -1 in this field and in the <b>802.1Q VLAN ID</b> field.
Enter 802.1Q VLAN ID	Options are <b>0</b> - <b>4094</b> . The default is <b>-1</b> (disabled). For tagged service, enter values in this field and the <b>802.1P Priority</b> field. For untagged service, enter <b>-1</b> (disabled) in this field and in the <b>802.1P Priority</b> field.
Select VLAN TPID	(Optional) Select the TPID for this VLAN. Options are 0x8100, 0x88A8, and 0x9100.



47



- SMART/RG SR501 orward thinking Device Info WAN Setup - Summary Advanced Setup Make sure that the settings below match the settings provided by your ISP. Layer2 Interface WAN Service 0/0/35 PORT / VPI / VCI: LAN **Connection Type:** Bridge Ethernet Config Service Name: br\_0\_0\_35 Security Service Category: UBR Parental Control IP Address: Not Applicable Quality of Service Service State: Enabled Routing NAT: Disabled Full Cone NAT: Disabled UPnP Firewall: Disabled DNS Proxy Interface Grouping GMP Multicast Proxy: Not Applicable **IGMP Multicast Source Enable** Disabled IP Tunnel MLD Multicast Proxy: **IPSec** Not Applicable Certificate MLD Multicast Source Enabled: Disabled Power Management Quality Of Service: Disabled Multicast Diagnostics Click "Apply/Save" to have this interface to be effective. Click "Back" to make any Management modifications. Logout Back Apply/Save
- 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.

SMART/R	G° SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN IPv6 Autoconfig Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Management Logout	Local Area Network (LAN) Setup   Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default    P: Address:   P: Address:   P: Contable IGMP Snooping   Standard Mode   B: Bocking Mode <t< th=""></t<>
	Option 66:       (TFTP Server Name)         Option       (Comma-seperated list of TFTP Server IPv4         150:       (maximum 2 entries))         Option 43:       (Addess(es)
	□ Configure the second IP Address and Subnet Mask for LAN interface
	Appky/Save



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

Field Name	Description
GroupName	Select an interface group from the list of available groups (defined on the Interface Group- ing 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 listen ing to these conversations, the gateway maintains a map of which links need which IP mul- ticast 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 Fire- wall	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	( <i>Becomes editable when Enable DHCP Server is selected</i> ) Enter the beginning of the class C, IP address range to be assigned by the DHCP server.
End IP Address	( <i>Becomes editable when Enable DHCP Server is selected</i> ) Enter the end of the class C, IP address range to be assigned by the DHCP server.
Leased Time (hour)	( <i>Becomes editable when Enable DHCP Server is selected</i> ) 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.



Field Name	Description					
	<ol> <li>Click Add Entries.</li> <li>Enter the MAC address and IP address and click Apply/Save.</li> <li>Repeat these steps to create any additional entries that you need up to 32.</li> </ol>					
Automatically create static IP leases from the following OUIs	<ul> <li>For LAN hosts, IP addresses can be assigned manually or by using DHCP.</li> <li>1. Click Add OUI.</li> <li>2. Enter the OUI and click Apply/Save.</li> <li>3. Repeat these steps to create any additional entries that you need.</li> </ul>					
Static DNS Servers	(Optional) Enter the IP addresses for the <b>Primary</b> and <b>Secondary</b> DNS servers.					
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.					
Option 43	A Cisco proprietary methodology for providing the Cisco Aironet Controller address to your access point.					
Configure the second IP address and sub- net mask for LAN interface	When you select this option, the <b>IP Address</b> and <b>Subnet Mask</b> fields appear where you can enter a second IP address and Subnet mask to support a second, simultaneous LAN, i.e., the primary LAN might be defined as 192.168.0.1 and this secondary LAN defined as 192.168.2.1.					



### 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.

SMART/F	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN IPv6 Autoconfig Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Management Logout	IPv6 LAN Auto Configuration         Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe: Please enter "0:0:0:2" instead of "::2".         Static LAN IPv6 Address Configuration         Interface Address (prefix length is required):         IPv6 LAN Applications         Stateless         State ful         Stan in therace Advertisement         Rea

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

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 Application	ns section
Enable DHCP v6 Server	This option enables the DHCP v6 feature on the LAN.



Field Name	Description
Stateless	This option is <i>selected</i> by default. Click to <i>stop</i> inheriting IPV6 address assignments from the WAN IPV6 inter- face.
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 shorthand notation (::2). Options are:
	<ul> <li>Start interface ID: Enter the beginning IPv6 available addresses for DHCP to assign to LAN devices.</li> <li>End interface ID: Enter the ending IPv6 available addresses for DHCP to assign to LAN devices.</li> <li>Leased Time (hour): Amount of time before a new IPv6 lease is requested by the LAN client.</li> </ul>
Enable RADVD	( <i>Optional</i> ) This option is <i>enabled</i> 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) advert- isement 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	( <i>Optional</i> ) This option is <i>enabled</i> by default. It enables Multicast Listener Discovery (MLD) snooping to man- age IPV6 multicast traffic. Options are:
	• Standard Mode: Multicast traffic will flood to all bridge ports when no client subscribes to a mul- ticast group even if IGMP snooping is enabled.
	<ul> <li>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.</li> </ul>
Enable MLD LAN to LAN Multicast	( <i>Optional</i> ) This option is <i>enabled</i> by default. It enables LAN-to-LAN Multicast until the first WAN service is connected. Options are <b>Disable</b> and <b>Enable</b> .

# 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.

ß					SR50	)1
		Ethern	et Port Configurat	tion		
ſ	Port	Configure	Current Bit Rate	Duplex Mode	Status	
ĺ	eth0/LAN1	Auto ~	100	Full	Up	
L						
	* 114	ws configure	1000BaseT connec	tions with Aut	2	
	Atm	iys conjigure	rooodaser connect	cions with Add		
			Save/Apply			
	G	Port eth0/LAN1	Ethern Port Configure eth0/LAN1 Auto ~	Ethernet Port Configurat           Port         Configure         Current Bit Rate           eth0/LAN1         Auto         100	Ethernet Port Configuration         Port       Configure       Current Bit Rate       Duplex Mode         eth0/LAN1       Auto       100       Full         * Always configure       1000BaseT connections with Auto	Ethernet Port Configuration         Port Configure Current Bit Rate Duplex Mode Status         eth0/LAN1       Auto       100       Full       Up         * Always configure 1000BaseT connections with Auto.

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.

SMART/F	<b>SC</b> °								SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	Virtual S External required	irtual Serve erver allows port) to the only if the h the LAN si	you to dire Internal se external por	rver with prt needs to	private IP a be conver	ddress on t ted to a dif configured	the LAN side	e. The Inter	nal port is
Virtual Servers Port Triggering DMZ Host	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Security Parental Control									



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

SMART/F	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Virtual Servers Port Triggering DMZ Host Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Management Logout	<section-header></section-header>

- 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.

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



Field Name	Description
Address	
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 En	d 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.

SMART/RC		SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Virtual Servers Port Triggering DMZ Host Security Parental Control	NAT Port Triggering Some applications such as games, video conferencing, remote access applicat require that specific ports in the Router's firewall be opened for access by the can configure the port settings from this screen by selecting an existing appli your own (Custom application) and dick "Save/Apply" to add it. Remaining number of entries that can be configured:96 Use Interface [poe_0_0_1/ptm0 ~ Application Name: © Select an application: Select One ~ Custom application: Select One ~	e applications. You
Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics	Trigger Port Start       Trigger Port Cool       Open Port Start       Open Port End         TCP       TCP           TCP       TCP           TCP       TCP           TCP       TCP           TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            TCP            Save/Apply	TCP            TCP

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

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



Field Name	Description
Trigger Protocol	Select the protocol required by the application that will be using the ports in the specified range. Options are: <b>TCP</b> , <b>UDP</b> , and <b>TCP/UDP</b> .
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.

SMART/F	RG° SR501
Device Info	NAT DMZ Host
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	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. Enter the computer's IP address and click 'Apply' to activate the DMZ host.
Virtual Servers	Clear the IP address field and dick 'Apply' to deactivate the DMZ host.
Port Triggering DMZ Host Security Parental Control Quality of Service	DMZ Host IP Address:

- 2. Enter the DMZ Host IP Address.
- 3. Click Save/Apply 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.

SMART/R	₿ <b>G</b> °	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethemet Config NAT Security IP Filtering Outgoing Incoming MAC Filtering Parental Control Quality of Service Routing DNS	specifying a new filter name and at le	IPv4 ~ ~
DSL		man

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

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 <b>IPv4</b> and <b>IPv6</b> . The default is <b>IPv4</b> . If you select <b>IPV6</b> , both the Source and Destination IP address must be specified in IPV6 format. The following is an IPV6-compliant, hexadecimal address: 2001:0DB8:AC10:FE01:0000:0000:0001.



Field Name	Description
Protocol	Select the protocol profile for the filter you are defining. TCP/UDP is most commonly used. The options are <b>TCP/UDP</b> , <b>TCP</b> , <b>UDP</b> , and <b>ICMP</b> .
Source IP address [/prefix length]	Enter the source IP address of a LAN side host for which you wish to filter/block outgoing traffic for the specified protocol(s). <b>Note:</b> 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 protocols. <b>Note:</b> 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 reach- ing the otherwise intended destination(s), e.g., to block the traffic to those ports on, say, a com- puter 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.

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



SMART/R	G	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security IP Filtering	name and at least one condition below. All satisfied for the rule to take effect. Default behavior for Incoming filter rules is However, the DROP checkbox will create a for such purposes as restricting access to V will allow access from any source.	to identify incoming IP traffic by specifying a new filter of the specified conditions in this filter rule must be to <b>ACCEPT</b> packets meeting the specified conditions. ilter that will <b>DROP</b> packets. Dropping packets is useful rtual Servers, as the default condition for Virtual Servers be Service Ports of the Broadband Router itself (HTTP,
Outgoing Incoming MAC Filtering Parental Control		ess List' at Management-> Access Control-> Access List
Quality of Service Routing	Filter Name:	
DNS	IP Version: IPv4	~
DSL	Protocol:	~
UPnP	Source IP address[/prefix length]:	
DNS Proxy	Source Port (port or port:port):	
Interface Grouping	Destination IP address[/prefix length]: Destination Port (port or port:port):	
IP Tunnel	DROP:	
IPSec		
Certificate		e and with firewall enabled) and LAN Interfaces
Power Management	Select one or more WAN/LAN interfaces dis	played below to apply this rule.
Multicast		oe_0_0_35/ppp0.1
Diagnostics	Select All M 1poe_0_0_1/ptm0 M ppp	be_u_u_s5/ppp0.1 🗠 ppp0e_0_0_35/ppp1.2 🗠 br0/br0
Management		
Logout		
		Apply/Save

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

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).
DROP	Select this option to drop packets that meet this filter's requirements. The packets are deleted.
WAN Interfaces	Click to apply this rule to all WAN interfaces or only certain types. Options are <b>Select All</b> or the interfaces defined for your network. The default is <b>Select All</b> .



#### **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.

SMART/R	G° SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethermet Config NAT Security	MAC Filtering Setup MAC Filtering is only effective on WANs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. MAC Filtering Policy For Each Interface: WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new
IP Filtering MAC Filtering Parental Control Quality of Service Routing DNS	rules for the new policy.       Interface     Policy     Change       atm0.3     FORWARD
DSL UPnP DNS Proxy Interface Grouping IP Tunnel	Change Policy Choose Add or Remove to configure MAC filtering rules. Interface Protocol Destination MAC Source MAC Frame Direction Remove
IPSec Certificate Power Management	Add Remove

- 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.

SMART/F	<b>KG</b> °	SR501
Device Info	Add MAC Filter	
Advanced Setup Layer2 Interface WAN Service LAN		he MAC layer frames by specifying at least one e conditions are specified, all of them take effect. Click e the filter.
Ethernet Config	Protocol Type:	~ ·
NAT Security	Destination MAC Address: Source MAC Address:	
IP Filtering MAC Filtering	Frame Direction:	LAN<=>WAN ~
Parental Control Quality of Service	WAN Interfaces (Configured	in Bridge mode only)
Routing	br_0_0_35/atm0.3 >	
DNS		
DSL		Save/Apply
UPnP		
DNS Proxy		

- 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
	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.
	Enter the MAC address of the device that is originating requests intended for the device asso- ciated with the <b>Destination MAC Address</b> .
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.

SMART/RG® SR501		
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Time Restriction Url Filter Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate	Access Time Restriction         This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device, where the browser is running. To restrict other LAN device, dick the 'Other MAC Address' button and enter the MAC address of the other LAN device, To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".         User Name	

- 2. Fill in the fields using the information in the table below.
- 3. Click Apply/Save.

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.	
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 ( <b>00:00</b> - <b>24:00</b> ).	



#### **URL Filter**

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

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

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

SMART/F	ß	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Time Restriction Url Filter	Parental Control Enter the URL addre add the entry to the URL Address: Port Number:	ess and port number then dick "Apply/Save" to
Audity of Service		an and and an address and a second and a second and a second a s

- 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	( <i>Optional</i> ) Enter the port number associated with the URL. The default is <b>80</b> .

# Quality Of Service

Quality of Service (QoS) enables prioritization of Internet content to help ensure the best possible performance. This is particularly useful for streaming video and audio content with minimized potential for drop-outs. QoS becomes significant when the sum of all traffic (audio, vid<u>"QoS Classification"</u>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

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

SMART/R	G <sup>®</sup> SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service QoS Config QoS Queue Config QoS Queue Config QoS Classification QoS Port Shaping Routing DNS DSL	QoS Queue Management Configuration         If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.         Usage Notes:         If the Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.         The default DSCP mark is used to mark all egress packets that do not match any classification rules.         QoS and a non-default queue are highly recommended for PPP WAN services. Each time a PPP WAN service starts or resets, if a non-default queue does not exist, one will be created and QoS automatically enabled.         Image QoS
UPnP DNS Proxy Interface Grouping IP Tunnel	Select Default DSCP Mark No Change(-1) V
IPSec Certificate	والمراجع المراجع المراج

- 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.
  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)	CS7(111000)
AF11(001010)	AF33(011110)	AF41(100010)	

#### QoS Queue Config

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

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

SMART/R forward thinking	KG° SR	501
Device Info	QoS Configuration	
Advanced Setup Layer2 Interface WAN Service	This screen allows you to configure a QoS queue and add it to a selected layer2 interface.	
LAN Ethernet Config NAT	(Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.) Name:	
Security	Enable: Enable ~	
Parental Control		
Quality of Service	Interface:	
QoS Config		
QoS Queue Config		
Queue Configuration		
QoS Classification	A mathe of man	
QoS Port Shaping	Apply/Save	
Routing		
DNS	man and a second a	

- 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 once for each WAN configuration.
- 5. Click Apply/Save to save your settings.

Field Name	Description
Enable	Select to enable or disable this queue configured on the selected interface. This option is <i>enabled</i> by default.
	<b>Note:</b> Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.
Queue Priority settings	5
Precedence	Select the priority value to be associated with the new queue. Options vary by inter- face 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	( <i>Not applicable for ETH interfaces</i> ) Select an algorithm for applying queue data pri- ority. Options are:
	• Strict Priority: Applies weighting based on the Priority field value.
	• 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 dif- ferent 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	( <i>Applicable for PTM and Dynamic WAN interfaces only</i> ) Enter the minimum shaping rate for packets in QoS queues. Options are <b>1</b> - <b>1255</b> kbps.
	To specify no minimum rate, enter -1.
Shaping Rate	( <i>Applicable for PTM and Dynamic WAN interfaces only</i> ) Enter the shaping rate for pack- ets in QoS queues. Options are <b>1</b> - <b>1255</b> kbps.
	To specify no shaping, enter -1.
Shaping Burst Size	( <i>Applicable for PTM and Dynamic WAN interfaces only</i> ) Enter the shaping burst size to be applied to packets in the defined queue. Options are <b>1600 bytes</b> or greater.
PTM Priority	(Applicable for PTM and Dynamic WAN interfaces only) Select the priority for the PTM interface. Options are Low and High.



#### **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.

SMART/F	<b>≧G</b> °	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security	Add Network Traffic Class Rule This screen creates a traffic class and optionally mark the DSCP or I Click 'Apply/Save' to save and act Traffic Class Name: Rule Order: Rule Status:	ss rule to classify the ingress traffic into a priority queue Ethernet priority of the packet.
Parental Control Quality of Service QoS Config QoS Queue Config Queue Configuration QoS Classification QoS Port Shaping Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Wanagement Logout	Ingress Interface: Ether Type: Source MAC Address: Source MAC Address: Destination MAC Address: Destination MAC Address: Destination MAC Mask: <b>Specify Classification Results</b> (A Specify Egress Interface (Required): - Packets dassified into a queue is not specified to exist, will inst Mark Differentiated Service Code Mark 802.1p priority: - Class non-vlan packets egress to class rule p-bits. - Class vlan packets egress to a ni by the class rule p-bits. No additi - Class non-vlan packets egress to and the class rule p-bits.	):
	Set Rate Limit:	[Kbits/s]

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



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 <b>Last.</b>	
Rule Status	Select whether this rule is active or inactive. Options are <b>Disable</b> and <b>Enable</b> .The default is <b>Enable</b> .	
Specify Classification Cri	teria 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	( <i>For Ether Type of 8021Q only</i> ) 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	( <i>Not applicable for <b>Ether Type</b> of <b>8021Q</b>) Enter the source MAC Address and Source MAC Mask for this classification.</i>	
Destination MAC Address Destination MAC Mask	( <i>Not applicable for Ether Type of 8021Q</i> ) Enter the destination MAC Address and des- tination MAC Mask for this classification.	
Source IP Address[Mask]	(Not applicable for <b>Ether Type</b> of <b>8021Q</b> ) (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]	( <i>Optional</i> ) ( <i>Not applicable for Ether Type of 8021Q</i> ) Enter the destination IP address and subnet mask for this classification.	
Differentiated Service Code Point (DSCP) Check	( <i>Optional</i> ) ( <i>Not applicable for Ether Type of 8021Q</i> ) Select the desired DSCP code for marking incoming data.	
Protocol	( <i>Optional</i> ) ( <i>Not applicable for Ether Type of 8021Q</i> ) Enter the Protocol specified for this classification.	
Specify Class Queue	(Not applicable for <b>Ether Type</b> of <b>8021Q</b> ) Select from the available queues.	
	<b>Note:</b> 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.	



Field Name	Description
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.
	This value is inserted into the Ethernet frame and used to differentiate traffic. Lower values assign higher priorities. Options are: <b>1</b> - <b>7</b> .
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.

SMART/F	۶G°			SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN	If "Egress Sha be ignored.	haping Setup ping supports traffic rate l ping Rate" is set to "-1", si licing Rate" is set to "-1", p	haping will be disabled ar	
Ethernet Config NAT	Interface	Egress Shaping Rate (Kbps)	Egress Burst Size (bytes)	Ingress Policing Rate (Kbps)
Security Parental Control	eth0/LAN1	•1	0	•1
Quality of Service QoS Config QoS Queue Config	Apply/Save			

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

Field Name	Description
Interface	Each entry in this column represents one of the Ethernet LAN ports on the gateway.
Shaping Rate (Kbps)	Enter the data rate for packets on the specified Interface. Options are: <b>1</b> - <b>1,000,000</b> Kbps. The default is <b>-1</b> (no shaping).
Burst Size (bytes)	Enter the burst size to be applied to packets in the defined queue. Options are <b>1600 bytes</b> or greater.



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

SMART/F	<b>\G</b> °	SR501
Device Info Advanced Setup	Routing Default Gatewa	ау
Layer2 Interface WAN Service LAN Ethernet Config NAT Security	system default gateways I with the first being the h	e list can have multiple WAN interfaces served as out only one will be used according to the priority ighest and the last one the lowest priority if the ed. Priority order can be changed by removing all again.
Parental Control Quality of Service	Selected Default Gateway Interfaces	Available Routed WAN Interfaces
Routing Default Gateway	ppp0.1 ^	ptm0 ^ ppp1.2
Static Route Policy Routing RIP		٠
DNS DSL		<.
UPnP DNS Proxy	$\checkmark$	~
Interface Grouping IP Tunnel IPSec	Select a preferred wan in	terface as the system default IPv6 gateway.
Certificate Power Management Multicast	Selected WAN Interface [	ipoe_0_0_1/ptm0 ~
Multicast Diagnostics Management Logout		Apply/Save

- 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.
- 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.

SMART/R	₿ <b>G</b> °	SR501
Device Info Advanced Setup	<b>Routing Static Route Add</b> Enter the destination network address, su	bnet mask, gateway AND/OR
Layer2 Interface WAN Service LAN	available WAN interface then click "Apply/S routing table.	
Ethernet Config NAT Security	IP Version: Destination IP address/prefix length:	IPv4 ~
Parental Control Quality of Service	Interface: Gateway IP Address:	
Routing Default Gateway Static Route	(optional: metric number should be greater Metric: Apply/Save	
Policy Routing		A

- 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	( <i>Optional</i> ) 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.

SMART/F	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing Default Gateway Static Route Policy Routing RIP DNS	Policy Routing Settup         Enter the policy name, policies, and WAN interface then dick "Apply/Save" to add the entry to the policy routing table.         Note: Default gateway must be configured for IPoE connection that doesn't rely on DHCP.         Policy Name:         Source IP:         Use Interface         Ippe_0_0_1/ptm0         Default Gateway IP:
DSL	

- 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.	
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)

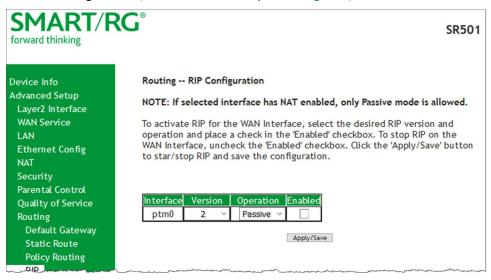
RIP is a type of distance-vector routing protocol, which leverages hop count as a metric for routing. RIP puts a limit on the number of hops (maximum of 15) allowed in order to prevent routing loops. This can sometimes limit the size of networks where RIP can be successfully employed.

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.

Field Name	Description
Interface	Displays a list of available WAN interfaces. Complete the line item(s) associated with the inter- face 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	<ul> <li>Select the operation mode. Options are:</li> <li>Active: This mode listens and advertises routes.</li> <li>Passive: This mode listens only. It does not advertise routes.</li> </ul>
Enabled	Select to employ RIP on the displayed interface.



# DNS

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

### **DNS Server**

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

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

SMART/RC	0	SR501
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 Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics Man agement Logout	<ul> <li>addresses for the system. In protocol is configured, Stati DNS Server Interfaces can honly one will be used accord one the lowest priority if the by removing all and adding the selected DNS Server Interfaces</li> <li>Select DNS Server Interfaces</li> <li>ppp0.1</li> <li>Use the following Stati Primary DNS server: Secondary DNS server: Select the configured WAN is static IPv6 DNS server Addres Note that selecting a WAN ir on that interface.</li> <li>Obtain IPv6 DNS info for the selection of the selec</li></ul>	rface from available WAN interfaces: Available WAN Interfaces ptm0 ppp1.2 c DNS IP address: Available WAN Interface for the IPv6 DNS server information OR enter the isses. Interface for the IPv6 DNS server will enable the DHCPv6 Client om a WAN interface: ipoe_0_0_1/ptm0 v

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 hostnames, addresses or other data. Often this update occurs in real time. On this page, you can configure the settings for this feature.

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

SMART/F	<b>\G</b> °	SR501
Device Info Advanced Setup	Add Dynamic DNS	
Layer2 Interface WAN Service	This page allows you to or no-ip.com.	o add a Dynamic DNS address from DynDNS.org, TZO,
LAN Ethernet Config	D-DNS provider	DynDNS.org ~
NAT Security Parental Control	Hostname Interface	ipoe_0_0_1/ptm0
Quality of Service Routing DNS	<b>DynDNS Settings</b> Username Password	
DNS Server Dynamic DNS Static DNS		
DSL UPnP		Apple/Exic
DNS Proxy Interface Grouping IP Tunnel		Apply/Save

- 2. Modify the settings, using the information provided in the following table.
- 3. Click Apply/Save to commit your changes.

Field Name	Description							
D-DNS provider	Select a dynamic Domain Name Server provider.							
Hostname	Enter the hostname of the dynamic DNS server.							



Field Name	Description					
Interface Select the gateway WAN interface whose traffic will be pointed at the specified Dyn provider.						
DynDNS.org sett	ings					
Username	Enter the username for the dynamic DNS server .					
Password	Enter the password for the dynamic DNS server.					
TZO and no-ip se	ettings					
Email	Enter the email use to access TZO.					
Кеу	Enter the key for your TZO account.					

## 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.

SMART/F	<b>G</b> °	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config	Static DNS Entry Enter the Host Name and IP address then dick "Apply/Save" . Host Name: IP Address:	
NAT Security Parental Control Quality of Service	Apply/Save	

- 2. Modify the settings, using the information provided in the following table.
- 3. Click Apply/Save to commit your changes.

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



# DSL

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

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

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

SMART/F	<b>RG</b> °	SR501
Device Info	DSL Settings	
Advanced Setup Layer2 Interface WAN Service		t the profile below.
LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP	✓ G.lite Enabled       ✓ 8b         ✓ T1.413 Enabled       ✓ 8c         ✓ ADSL2 Enabled       ✓ 8d         ✓ AnnexL Enabled       ✓ 12         ✓ ADSL2+ Enabled       ✓ 12	a Enabled 5 Enabled 6 Enabled 9 Enabled 2a Enabled 2b Enabled 7a Enabled
DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Diagnostics	<ul> <li>✓ VDSL2 Enabled</li> <li>US0</li> <li>✓ En</li> <li>Select the phone line pair below.</li> <li> <ul> <li>Inner pair</li> <li>Outer pair</li> </ul> </li> </ul>	nabled
Management Logout	Capability Bitswap Enable SRA Enable PhyR Enable ADSL PTM Mode Enable Stinger® Mode Enable Inventory Management Use board serial for EOC Serial Num	

2. Modify the settings as needed.



- 3. To configure advanced settings, see "Advanced settings".
- 4. 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 SmartRG gateways.

Parameter	8a	8b	8c	8d	12a	12b	17a
Max DS Tx Power (dBm)	+17.5	+20.5	+11.5			+14.5	5
Max US Tx Power (dBm)				+14.	5		
Min bidirectional net data rate		50M	bps		68	Mbps	100Mbps

Field Name	Description
Other Settings	
US0	This option is <i>enabled</i> by default. To <i>disable</i> it, click the checkbox to clear it.
Inner Pair/Outer Pai	The RJ11 connector has four contacts. The center pair of pins is DSL1. The outer pins are the con- tacts for DSL2. Select which pair should be used.



Field Name	Description
Capability	<ul> <li>Bitswap Enable: Enables adaptive handshaking functionality.</li> <li>SRA Enable: Enables Seamless Rate Adaptation.</li> <li>PhyR Enable: Enables Physical Layer Retransmission.</li> <li>ADSL PTM Mode Enable: Enables Asymmetric Digital Subscriber Line in Packet Transfer Mode.</li> <li>Stinger® Mode Enable: Enables communication with Stinger type equipment.</li> </ul>
-	Select whether to use the gateway serial number as the EOC serial number in your inventory man- agement database.

## Advanced settings

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

SMART/F	SR506n
Device Info Advanced Setup	DSL Advanced Settings Select the test mode below.
Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing	<ul> <li>Normal</li> <li>Reverb</li> <li>Medley</li> <li>No retrain</li> <li>L3</li> </ul>
DNS DSL UPnP	Apply Tone Selection

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



						10	pstrea	m Tone							
	1	2	23		15	126	17	⊠8	29	10	11	12	13	14	15
	17	18	19	20	21	22			25		27				
							wnstre			20					
32	☑ 33	☑ 34	35	⊠ 36	37		Contraction of the local distance of the loc	CONTRACTOR OF THE OWNER.	A10-10-0	242	₫43	244	₩45	☑ 46	247
Ø 48	249	250	251	252	₫ 53	254	255	1 56	157	1 58	₫ 59	100	161	162	163
164	165	266	67	1 68	269	70	71	72	₫73	74	75	76	277	78	79
280	281	282	83	284	285	286	87	288	289	290	291	292	293	294	295
296	297	298	299	100	101	102	103	104	105	106	107	108	109	110	211
10000		114	1000000				10.7	0	100000000	0.000			1000		
128	129	130	131	132	M 133	134	135	136	137	138	139	140	141	142	14
		146		0.000								1.1.1		1.	
		162			_										
		178									1000	0.000			
		194													
	1000	210						2000 0000		1000					
		226													
		242													
					Chec	k All	Clear Al	Ap	ply	Close					

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

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

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

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



# **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.

SMART/RG® forward thinking SR501			
Device Info Advanced Setup Layer2 Interface WAN Service	UPnP Configuration NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.		
LAN Ethernet Config NAT	✓ Enable UPnP		
Security Parental Control Quality of Service Routing	Apply/Save		

- 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.

SMART/F	RG°	SR501
Device Info	DNS Proxy Configuration	
Advanced Setup Layer2 Interface WAN Service	✓ Enable DNS Proxy	
LAN Ethernet Config NAT	Host name of the Broadband Router: ClearView Domain name of the LAN network: Home	
NAT Security Parental Control	Apply/Save	
Quality of Service		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

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



# Interface Grouping

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

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



ward thinking	G°	SR501			
ice Info	Interface grouping Configuration				
vanced Setup ayer2 Interface VAN Service	To create a new interface group: 1. Enter the Group name and the group (static) below:	name must be unique and select either 2. (dynamic) or 3.			
AN Ethernet Config IAT	2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.				
ecurity arental Control Quality of Service outing	3.Select interfaces from the available in	terface list and add it to the grouped interface list using the apping of the ports. <b>Note that these clients may obtain public</b>			
INS ISL	<ol> <li>If this interface is to share the WAN in WAN interface you select will be remove</li> </ol>	terface, dick the "shared WAN interface" box, otherwise the ed from any other interface groups.			
PnP NS Proxy Lterface Grouping	5. Click Apply/Save button to make the	changes effective immediately			
P Tunnel PSec Certificate	IMPORTANT If a vendor ID is configured attached to the modem to allow it to o	for a specific client device, please REBOOT the client device btain an appropriate IP address.			
ower Management	Group Name:				
ulticast gnostics	Shared WAN Interface:				
nagement	Grouped WAN Interfaces	Available WAN Interfaces			
	~	pppoe_0_0_35/pp1.2     No Interface/None     c.			
	Grouped LAN Interfaces	Available LAN Interfaces			
	^				
	~	~			
	Automatically Add Clients With the following DHCP Vendor IDs				
		and the second state and a second s			
hadren	have god to be				

- 2. To create a new interface group, enter a unique Group Name, then proceed with either step 3 (dynamic) or step 4 (static) below.
- 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 (on the right).
  - b. Add it to the **Grouped Interface** list (on the left) 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.
- 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 and then click Add. The following page appears.

SMART/F	RC°			SR501
Device Info	IP Tunneling 6in4 Tunnel Conf	iguration		
Advanced Setup Layer2 Interface	Currently, only 6rd configuration	is supported		
WAN Service	Tunnel Name			
LAN	Mechanism:		6RD	~
Ethernet Config	Associated WAN Interface:			~
NAT	Associated LAN Interface:		LAN/br0 ~	
Security	Manual O Automatic			
Parental Control				
Quality of Service	IPv4 Mask Length:			1
Routing	6rd Prefix with Prefix Length:			1
DNS	Border Relay IPv4 Address:			ĺ
DSL				
UPnP		Apply/Save		
DNS Proxy				
Interface Crowsing			m_mm_mm	



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 either 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.

SMART/RG <sup>®</sup> SR501			
Device Info	IP Tunneling 4in6 Tunnel Configu	uration	
Advanced Setup Layer2 Interface	Currently, only DS-Lite configuration	n is supported.	
WAN Service	Tunnel Name		
LAN	Mechanism:	DS-Lite 🗸	
Ethernet Config	Associated WAN Interface:	~	
NAT	Associated LAN Interface:	LAN/br0 V	
Security	Manual O Automatic		
Parental Control Quality of Service Routing DNS	AFTR:	Apply/Save	

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. Below 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. The following page appears.

SMART/Re	G°	SR501
Device Info Advanced Setup	IPSec Settings	new connection 🗌 NAT Traversal
Layer2 Interface WAN Service LAN	IP Version:	IPv4 ~
Ethernet Config NAT	Tunnel Mode	ESP 🗸
Security Parental Control	WAN Interface:	Select interface ~
Quality of Service Routing DNS	Remote Security Gateway	0.0.0.0 Anonymous
DSL UPnP DNS Proxy Interface Grouping IP Tunnel	LAN-side VPN IP Address Mask or Prefix Length Local ID Type	Subnet         V           0.0.0         255.255.0           Default         V
IPSec Certificate Power Management Multicast Diagnostics Management	Remote-side VPN IP Address Mask or Prefix Length Remote ID Type	Subnet         ~           0.0.0.0
Logout	Key Exchange Method Authentication Method Pre-Shared Key Perfect Forward Secrecy	Auto (IKE)       ~         Pre-Shared Key       ~         key
	Advanced IKE Settings	Show Advanced Settings
		Apply/Save

- 2. Complete the fields, using the information provided in the following table.
- If desired, click Advanced IKE Settings to select Phase 1 and Phase 2 specific parameters. For detailed information about these settings, see <u>"Advanced IKE Settings"</u>.
- 4. Click Apply/Save to commit your changes.



Field Name	Description
IPSec Connection Name	Enter a descriptive name for this connection.
NAT Transversal	Click to enable the NAT traversal protocol.
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:
	<ul> <li>AH: Use this mode to encapsulate a packet with AH and IP headers. For authentication, the entire packet is signed.</li> </ul>
	• 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.
WAN Interface	Select the WAN connection to be associated with this tunnel.
Remote Security Gateway	Enter the WAN IP for this tunnel.
	To allow anonymous connections, click the <b>Anonymous</b> checkbox.
LAN-side VPN	Select whether to allow access to the entire LAN or a single host for local IP addresses. Options are:
	• Subnet: Allows access to the entire LAN.
	• Single Address: For single host, select this option.
IP Address	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 <b>255.255.255.0</b> .
Local ID Type	Select the type of ID for the local VPN. Options are <b>Default, Domain</b> , and <b>E-Mail</b> . The default is <b>Default</b> .
	When you select <b>Domain</b> or <b>E-Mail</b> , enter the domain name or email address in the <b>ID Content</b> field.
Remote-side VPN	Select whether to allow access to the entire LAN or a single host for remote IP addresses. Options are:
	• Subnet: Allows access to the entire LAN.
	• Single Address: Allows access to a single host.
IP Address	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 <b>255.255.255.0</b> .
Remote ID Type	Select the type of ID for the remote VPN. Options are <b>Default, Domain</b> , and <b>E-</b> Mail. The default is <b>Default</b> .



Field Name	Description
	When you select <b>Domain</b> or <b>E-Mail</b> , enter the domain name or email address in the <b>ID Content</b> field.
Key Exchange Method	Select the key-exchange method to be used for IPSec. Options are:
	<ul> <li>Auto(IKE): This method uses the negotiated key-exchange method for IPSec. This is the default and recommended for best results.</li> <li>Manual: This method requires that you configure the details.</li> </ul>
Authentication Method	Select the method by which the remote end will authenticate.
	• <b>Pre-Shared Key:</b> A key is distributed to authorized users for logging into the system. Enter the key in the <b>Pre-Shared Key</b> field.
	<ul> <li>Certificate (X.509): A certificate is used for authentication. Select the certificate file in the Certificates field that appears.</li> </ul>
Pre-Shared Key	If you selected <b>Pre-Shared Key</b> in the <b>Authentication Method</b> field, enter the key here.
Perfect Forward Secrecy	Select whether a session key is derived from a set of long-term keys is com- promised if one of the long-term keys in the set is compromised.
	• Enable: Prevents long-term key from being compromised.
	• <b>Disable</b> : Permits long-term keys to be compromised.
The following fields appear b	elow Advanced Settings when Manual is selected in the Key Exchange Method field.
Encryption Algorithm	Select the encryption algorithm. Options are <b>3DES</b> and <b>AES</b> .
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 <b>3DES</b> , <b>AES -128</b> , <b>AES-192</b> , and <b>AES-256</b> .
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 <b>768bit</b> - <b>8192bit</b> . The default is <b>1024bit</b> .
Key Life Time	Enter the number of seconds that a key is valid. The default is <b>3600</b> seconds.

3. Click Apply/Save to commit your changes.

# Certificate

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.



SMART/F	۲G	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN		<b>quest</b> signing request you need to include Common Name, /Province Name, and the 2-letter Country Code for
Ethernet Config NAT Security Parental Control Quality of Service	Certificate Name: Common Name: Organization Name: State/Province Name: Country/Region Name:	US (United States)
Routing DNS DSL UPnP		Apply

- 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.
Organization Name	A free form text field. Typically, this is the name of the company creating the request.
State/Province Name	Enter the state or province where this certificate will be used.
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.



SMART/F	RG°		SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping	Import certificate Enter certificate nau Certificate Name: Certificate:	me, paste certificate content and private key.	
IP Tunnel IPSec Certificate Local Trusted CA Power Management Multicast Diagnostics Management Logout	Private Key:	BEGIN RSA PRIVATE KEY <insert here="" key="" private=""> END RSA PRIVATE KEY</insert>	<u></u>

- 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.



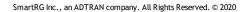
SMART/R	G°	SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL UPnP DNS Proxy	Import CA certificate Enter certificate name and paste certificate content. Certificate Name:BEGIN CERTIFICATE <insert certificate="" here="">END CERTIFICATE Certificate:</insert>	
Interface Grouping IP Tunnel IPSec Certificate	Apply	

- 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.

# Power Management

Note: This feature is not currently supported.





# 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.

SMART/RO	G°			SR501
Device Info Advanced Setup Layer2 Interface WAN Service LAN	Multicast Precedence Multicast Strict Grou Enforcement:		lower value, higher priority	
Ethernet Config NAT	IGMP Configuration			
Security Parental Control	Enter IGMP protocol	configuration fields	if you want modify default valu	ies shown below.
Quality of Service Routing DNS DSL UPnP DNS Proxy Interface Grouping IP Tunnel IPSec	Default Version: Query Interval: Query Response Inte Last Member Query Robustness Value: Maximum Multicast I Sources (for IGMPv3 Maximum Multicast I Members: Fast Leave Enable:	Interval: 10 2 Groups: 25 Data ): 10		
Certificate Power Management	IGMP Group Excepti			
Multicast	Group Address		Remove	
Diagnostics	224.0.0.0	255.255.255.0		
Management Logout	239.255.255.250 224.0.255.135	255.255.255.255 255.255.255.255	Add	
	Remove Checked Entries MLD Configuration Enter MLD protocol below. Default Version: Query Interval: 	2 125	figuration fields if you want mo	dify default values shown

- 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.

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.
	• <b>Disable:</b> IGMP packets are not prioritized. This is the default.
Multicast Strict Group- ing Enforcement	Select whether strict grouping is applied to IGMP packets. Options are <b>Enable</b> and <b>Dis</b> - able.
IGMP Configuration and	MLD Configuration sections
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 <b>125</b> .
	<b>Note:</b> 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 Inter- val	Upon receiving a query packet, a host begins counting down seconds, from a random num- ber. When the timer expires, the host sends its report. The default is <b>10</b> seconds.
	Enter the maximum number of seconds that a host can pick to count down from. The value must be greater than the <b>Query Interval</b> . If using IGMP v1, this value is fixed at <b>10</b> seconds.
Last Member Query Interval	Enter the maximum response time (in seconds) within which the host must respond to the Out of Sequence query from the router. The default is <b>10</b> 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 Groups	Enter the maximum number of groups allowed. The default is <b>25</b> .



Field Name	Description
Maximum Multicast Data Sources (for IGMPv3)	Enter the maximum number of data sources allowed. Options are <b>1</b> - <b>24</b> . The default is <b>10</b> .
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 <b>25</b> .
Fast Leave Enable	Select whether the IGMP proxy removes group members immediately without sending a query. Options are:
	<ul> <li>Enabled: Group members are removed immediately. This is the default.</li> <li>Disabled: Group members are removed after a query is sent and a response received.</li> </ul>



# 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.

SMART/R	₿ <b>G</b> °		SI	R501
Device Info Advanced Setup Diagnostics Diagnostics Ethernet OAM Ping Host Trace Route to Host Management Logout		status, to make ick "Help ovider	dick "Rerun sure the fail s	tatus
	Next Connection Test Test With OAM F	F4		

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.

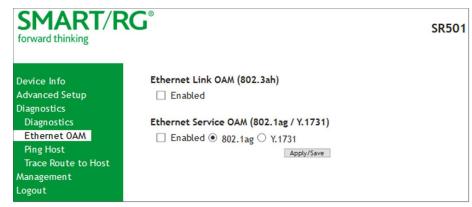
- 3. To test at the VP level instead of at an individual VC connection, click Test With OAM F4.
- 4. To test additional connections, click Next Connection. The page refreshes to show data for the next connection and the Previous Connection button appears. Repeat steps 2-4 for each connection.

# Ethernet OAM

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



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



- 2. To enable Ethernet Link OAM (802.3ah):
  - a. Click the **Enabled** checkbox. Additional fields appear.

Ethernet Link OAM (	302.3ah)	
WAN Interface:	atm0 ~	
OAM ID:	1	(positive integer)
Auto Event		
Variable Retrieval	e.	
Link Events		
Remote Loopbad	k	
Active Mode		

b. Modify the fields as needed, using the information in the Ethernet Link OAM (802.3ah) section of the table below.
3. To enable Ethernet Service OAM (802.1ag/Y.1731):

a. Click the **Enabled** checkbox. Additional fields appear showing values for 802.1ag. To configure Y.1731, click the Y.1731 radio button. The page refreshes.



Ethernet Service OA	M (802.1a	ag / Y.1731)
Enabled  802.	1ag O Y.17	731
WAN Interface:	atm0 ~	-
MD Level:	0 ~ [0-	-7]
MD Name:	Broadcom	[e.g. Broadcom]
MA ID:	BRCM	[e.g. BRCM]
Local MEP ID:	1	[1-8191]
Local MEP VLAN ID:	-1	[1-4094] (-1 means no VLAN tag)
CCM Transmission	n	
Remote MEP ID:	-1	[1-8191] (-1 means no Remote MEP)
Loopback and Linktra	ace Test	
Target MAC:		[e.g. 02:10:18:aa:bb:cc]
Linktrace TTL:	4	[1-255] (-1 means no max hop limit)
Loopback Result: N	/A	
Linktrace Result: N/	/Α	
		Send Loopback Send Linktrace
		Apply/Save

- b. Modify the fields, using the information provided in the Ethernet Service OAM (802.1ag/Y.1731) section of the table below.
- 4. Click Apply/Save to commit your changes.
- 5. To run a loopback test, enter a MAC address in the Target MAC field and click Send Loopback at the bottom of the page. The results appear in the Loopback Result row of the table.
- 6. To run a linktrace test, enter a MAC address in the Target MAC field and click Send Linktrace at the bottom of the page. The results appear in the Linktrace Result row of the table.

Field Name	Description
Ethernet Link OAM	(802.3ah) section
WAN Interface	Select the WAN interface that you want to test.
OAM ID	Enter the ID of this OAM configuration. Only positive numbers are allowed.
Auto Event	Click to enable automatic reporting of events.
Variable Retrieval	Click to enable on-demand link diagnostics, including bit-error-rate approximation.
Link Events	Click to enable reporting of critical conditions that may cause link failure.



Field Name	Description
Remote Loopback	Click to enable on-demand link diagnostics, including bit-error-rate approximation.
Active Mode	Click to enable this feature.
Ethernet Service OA	AM (802.1ag/Y.1731) section
WAN Interface	Select the WAN interface that you want to test.
MD Level	(Appears for the 802.1ag option only) Select the domain level for this maintenance domain. Options are <b>0</b> - <b>7</b> . The larger the domain, the higher the value you should select.
MD Name	(Appears for the 802.1ag option only) Enter the name of the maintenance domain, e.g., Broadcom.
MA ID	(Appears for the 802.1ag option only) Enter the maintenance association ID, e.g., BRCM.
MEG Level	(Appears for the Y.1731 option only) Enter the level of the maintenance entity group.
MEG ID	(Appears for the Y.1731 option only) Enter the ID of the MEG.
Local MEP ID	Enter the ID of the local maintenance entity group end point Options are <b>1</b> - <b>8191</b> . The default is <b>1</b> .
Local MEP VLAN ID	Enter the VLAN ID of the local MEP. Options are 1 - 4094. The default is -1 (no VLAN tag).
CCM Transmission	Click to enable continuity check message transmission.
Remote MEP ID	Enter the ID of the remote MEP. Options are 1 - 8191. The default is -1 (no remote MEP).
Loopback and Linkt	race Test section
Target MAC	Enter the MAC address for the test, e.g., 02:10:18:aa:bb:cc.
Linktrace TTL	Enter the maximum number of hops allowed. Optinons are 1-233. The default is -1 (no limit).
Loopback Result	Displays the results of the loopback test.
Linktrace Result	Displays the results of the linktrace test.

# Ping Host

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

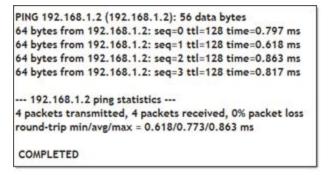
1. In the left navigation menu, click **Diagnostics Tools** > **Ping Host**. The following page appears.

SMART/F	SR501
Device Info Advanced Setup	Ping Host
Diagnostics Diagnostics	Enter the IP address of the device that you wish to ping. The results will take a few moments (up to 15 seconds) to appear.
Ethernet OAM Ping Host	Target Host Address: Ping Host
Trace Route to Host Management Logout	

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.

SMART/F	SR501
Device Info Advanced Setup Diagnostics Diagnostics Ethernet OAM Ping Host Trace Route to Host Management Logout	Trace Route to Host Enter the IP address of the device that you wish to trace. The results will take a few moments (up to 15 seconds) to appear. Target Host Address: Trace Route to Host

- 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.

traceroute to 192.168.1.2 (192.168.1.2), 10 hops max, 38 byte packets
1**
2**
3**
4**
5**
6**
7**
8**
9**
10**
COMPLETED

17



# Management

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

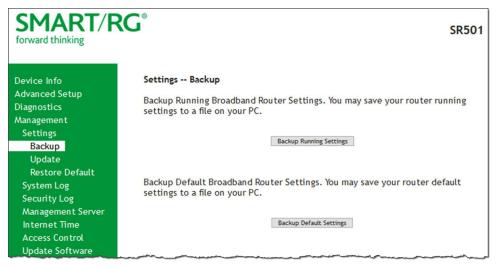
# Settings

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

## Backup

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

1. In the left navigation bar, click Management. 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.

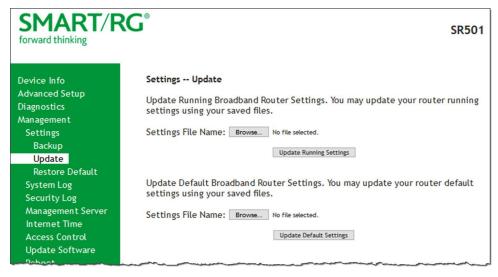
**Note:** If you plan to create backups frequently, you may want to rename the backup files by appending dates to the file name. Otherwise, every new backup file overwrites the existing backup file.

## 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.
- 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.

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

SMART/F	SR501
Device Info Advanced Setup Diagnostics Management Settings Backup Update Restore Default	Settings Restore Default Restore Broadband Router setting to the defaults. Restore Default Settings

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.

System Log			
Date/Time	Facility	Severity	Message
Jan 1 00:00:28	daemon	err	syslog: caTmBik:Time Blocking: Shutting down, sig -1
Jan 1 00:00:29	daemon	crit	kernet: eth3 (switch port: 4) Link UP 1000 mbps full duplex
Jan 1 00:00:59	daemon	err	syslog: CDM:caCdmPolForMessages: unrecognized msg 0x10000250
Jan 1 00:10:44	daemon	err	syslog: httpd:644.295:cgiValidateSessionKey:2356:failed session key check. Got 2135380610, expected 658209780, age=0 max=600000
Jan 1 00:13:10	daemon	err	syslog: httpd:790.530:cgiValidateSessionKey:2356:failed session key check. Got 685698293, expected 1511422544, age=0 max=600000
Jan 1 00:15:59	daemon	crit	kernel: Line 1: xDSL G.994 training
Jan 1 00:16:02	daemon	crit	kernet: Line 1: ADSL link down
Jan 1 00:26:14	daemon	crit	kernel: Line 0: xD5L G.994 training

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.

SMART/R	G° SR501
Device Info Advanced Setup Diagnostics Management Settings System Log Security Log Management Server Internet Time Access Control Update Software Reboot Logout	System Log Configuration         If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to be specified IP address and UDP port of the remote systeg server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.         Select the desired values and dick 'Apply/Save' to configure the system log options.         Log       Optionsble C Enable         Log Level:       Debugging ~         Display Level:       Error ~         Mode:       Local ~

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 <b>Disable</b> .		
Logging Level	Select <b>Error</b> unless actively troubleshooting a situation with a subscriber for which increased log detail is required. Options are <b>Emergency</b> , <b>Alert</b> , <b>Critical</b> , <b>Error</b> , <b>Notice</b> , <b>Warning</b> , <b>Informational</b> , and <b>Debugging</b> . The options are listed in top-down order. The default is <b>Debugging</b> .		
Display Level	Select <b>Error</b> unless actively troubleshooting a situation with a subscriber for which increased detail is required. This field has the same options as the <b>Logging Level</b> field. The default is <b>Error</b> .		
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 <b>Remote</b> or <b>Both</b> .		
	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
- Security lockout added/removed
- Authorized/unauthorized resource access
- Software update
- 1. In the left menu, click Management > Security Log. The following page appears.

SMART/F	SR501
Device Info	Security Log
Advanced Setup Diagnostics	The Security Log dialog allows you to view the Security Log.
Management	Click "View" to view the Security Log.
Settings System Log	Click "Reset" to clear and reset the Security Log.
Security Log	Right-dick here to save Security Log to a file.
Management Server	
Internet Time Access Control	View Reset
Update Software	
Reboot	
Logout	

- 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.

### Management Server

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

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

#### TR-069 Client

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

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

SmartRG products can accommodate several ACS products, including:



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

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

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

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

SMART/F	RG°	SR501
Device Info Advanced Setup Diagnostics Management Settings System Log	auto-configuration, provision, collec	allows a Auto-Configuration Server (ACS) to perform tion, and diagnostics to this device. Apply/Save" to configure the TR-069 dient options.
Security Log Management Server	OUI-Serial	● MAC ○ Serial Number
TR-069 Client STUN Config	TR-069 Client	⊖ Disable ●Enable
Internet Time Access Control	ACS URL from DHCP:	Enabled
Update Software Reboot Logout	Inform Interval: ACS URL: ACS User Name: ACS Password: TR-069 Client Port: WAN Interface used by TR-069 client	3600           https://acs.smartrg.com           (mil)           00005           120005
	Connection Request Authentica	tion
	Connection Request User Name: Connection Request Password: Connection Request URL:	admin ••••• (null)
	Α	pply/Save GetRPCMethods

- 2. Modify the fields as needed, following the instructions from your ACS platform vendor. Information about specific fields is provided in the table below.
- 3. Click Apply/Save to commit your changes.

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

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

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



Field Name	Description
OUI-Serial	Select whether to use the base MAC address or the serial number of your gateway when con- necting to the ACS. This value may display in an ACS user interface when looking at the device details of a particular gateway.
	<ul> <li>Serial Number: Select for SmartRG gateways using firmware version 2.5.0.2 and above.</li> <li>MAC: This is the most typical scenario. This is the default. For firmware versions prior to 2.5.0.2, MAC is the only available option.</li> </ul>
TR-069 Client	Enable or disable the TR-069 client on the CPE. You can disable the TR-069 WAN Management Cli- ent if no ACS is employed.
	<b>Note:</b> If you may want to add an ACS to your infrastructure in the future, it is recommended to leave this option enabled. When this feature is disabled, every gateway deployed with this setting must be manually/locally re-configured to enable this client if needed later.
ACS URL from DHCP	Click the <b>Enabled</b> checkbox to enable your gateway to obtain the ACS URL via DHCP. The default is disabled.
Inform Interval	The frequency (in seconds) with which the CPE (gateway) checks in with the ACS to sync and exchange data. A typical production environment entails CPEs in the field informing to the ACS once/day or every 86,400 seconds. The default is <b>300</b> 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 certificatebased 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 <b>30005</b> .
ACS User Name	Enter the user name by which this gateway logs in to the ACS. The default username is typically <b>admin</b> .
ACS Password	Enter the password to authenticate the above user name. The default password is typically <b>admin</b> .
TR-069 Client Port	Enter the TR-069 port number.
WAN Interface used by TR-069 client	Select any WAN, LAN, Loop back or a configured connection to declare how this gateway will con- nect to the ACS. The default is <b>Any_WAN - IPv4</b> .

4. (*Optional*) You can configure the gatway's client Connection Request mechanism which is used by your ACS for communication with subscriber gateways.



Field Name	Description
Connection Request Authentication	Select if your ACS requires authenticated connection requests. Complete the additional credential fields that are exposed. The default condition is enabled.
Connection Request Username	Enter the user name by which this gateway authenticates the ACS. Contact your ACS pro- vider for this information. The default username is typically <b>admin</b> .
Connection Request Password	Enter the password by which this gateway will authenticate to the ACS. Contact your ACS provider for this information. The default password is typically <b>admin</b> .
Connection Request URL	If a WAN service has been configured, the URL appears in this field.

- 5. To force the gateway to attempt to sync with the ACS, click the GetRPCMethods button. This will assist you in verifying the TR-069 parameters entered above.
- 6. If you made any further changes, click Apply/Save to commit them.

#### **STUN Config**

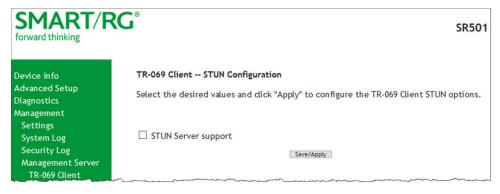
STUN stands for "Simple Traversal of UDP through NATs". STUN enables a device to find out its public IP address and the type of NAT service it is sitting behind.

STUN is most commonly used with older modems under ACS management connected via a NAT gateway. NAT accommodates a LANside 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. Additional fields appear.

SMART/Re	G°	SR501
Device Info Advanced Setup	TR-069 Client STUN Configuration	n
Diagnostics	Select the desired values and dick "	Apply" to configure the TR-069 Client STUN options.
Management		
Settings System Log	STUN Server support	
Security Log	STUN Server Address:	
Management Server	STUN Server Port:	3478
TR-069 Client STUN Config	STUN Server User Name: STUN Server Password:	
Internet Time	STUN Server Maximum Keep Alive	4
Access Control	Period: STUN Server Minimum Keep Alive	
Update Software	Period:	0
Reboot		Save/Apply
Logout		Second dependence

- 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. Con- sult your ACS vendor for implementation options and also TR-069 protocol doc- umentation, 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.



Field Name	Description
	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 <b>0</b> .

\* 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.

SMART/F	<b>R</b> G°	SR501
Device Info Advanced Setup Diagnostics Management Settings System Log Security Log Management Server Internet Time Access Control Update Software Reboot Logout	Time settings This page allows you to change the modem's time configuration.	
	Apply/Save	



2. Click Automatically synchronize with Internet time servers. Additional fields appear.

SMART/R	G°		SR501
Device Info Advanced Setup Diagnostics	<b>Time settings</b> This page allows you to	change the modem's time configuration.	
Management Settings		ronize with Internet time servers	
System Log Security Log Management Server	First NTP time server: Second NTP time server:	time.nist.gov ~ ntp1.tummy.com ~	
Internet Time Access Control	Third NTP time server: Fourth NTP time server:	None  V None V	
Update Software Reboot	Fifth NTP time server:	None ~	
Logout	offset:	0) Pacific Time, Tijuana	~
		Apply/Save	

- 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.

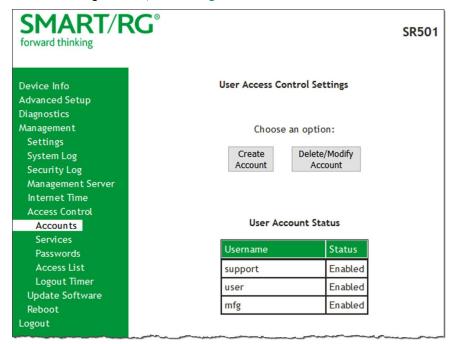
#### Accounts

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.

Add an Account



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





SMART/RO	<b>-</b>		SR501
Device Info Advanced Setup Diagnostics Wanagement Settings System Log Security Log Management Server Internet Time Access Control Accounts Services Passwords Access List Logout Timer Update Software Reboot Logout	Username: Password: Password: Device Info Summary WAN Statistics Route ARP DHCP Advanced Setup Layer 2 Interface WAN Service 4G LTE Settings Ethernet Config LAN NAT Security Parential Control Quality of Service Routing DNS	eate Account	
	DSL DSL Bonding UPnP DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Multicast	Management Server Internet Time Access Control Update Software Reboot Support Tools Port Mirroring Factory reset	
	Network	Access Type (Required)	
	Back	Save Account	

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

SMART/RG	SR501
Device Info Advanced Setup Diagnostics Management Settings System Log Security Log Management Server Internet Time	Delete/Edit Account Select an account : support Enable/Disable account:  Enable O Disable Username: support Privileges for 'support','user' and 'mfg' accounts cannot be customized.
Access Control Accounts Services Passwords Access List	Back Update Account Delete Account

- 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**

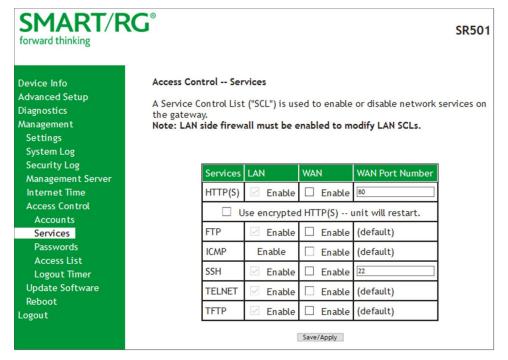
USER	PASSWORD
admin	admin
support	support
user	user
mfg	IDH7iw@ibRsPOIBa



#### 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 <b>FTP</b> , <b>HTTP</b> , <b>ICMP</b> , <b>SNMP</b> , <b>SSH</b> , <b>TELNET</b> , and <b>TFTP</b> .
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	If a WAN service is configured for your gateway, select the services enabled on the WAN



Field Name	Description	
	side firewall. If no WAN service is configured, this column does not appear.	
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.	

#### 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.

SMART/R	G <sup>®</sup> SR501
Device Info	Access Control Passwords
Advanced Setup Diagnostics Management	Access to your Router is controlled through three user accounts: admin, support, and user.
Settings System Log	The user name "admin" has unrestricted access to change and view configuration of your Router.
Security Log Management Server	The user name "support" is used to allow an ISP technician to access your Router for maintenance and to run diagnostics.
Internet Time Access Control Accounts	The user name "user" can access the Router, view configuration settings and statistics, as well as update the router's software.
Services Passwords	Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.
Access List Logout Timer	User Name:
Update Software Reboot	New Password: Confirm Password:
Logout	Apply/Save

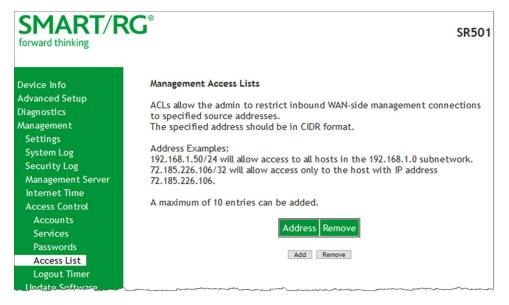
- 2. Enter your user name and current passwor.
- 3. In the New Password and Confirm Password fields, enter the new password.
- 4. Click Apply/Save to implement the change.

#### 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.

SMART/R	<b>G</b> °	SR501
Device Info	Management Access Li	st
Advanced Setup		
Diagnostics	Restrict inbound manag	gement connections to specified source address
Management		
Settings	Source Address:	
System Log		
Security Log		Apply/Save
Management Server		
Internet Time		
Access Control		

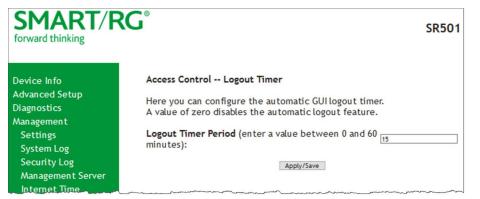
- b. Enter the address for which you want to restrict access.
- c. Click Apply/Save. You are returned to the Management Access Lists page.
- d. To add up to 9 more addresses, repeat steps 2a 2c.
- 3. To remove an address, click the **Remove** checkbox next to it and then click **Remove**. The list is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

SMART/F	SR501
Device Info	Update Software
Advanced Setup Diagnostics	Step 1: Obtain an updated software image file from your ISP.
Management Settings	Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
System Log Security Log	Step 3: Click the "Update Software" button once to upload the new image file.
Management Server Internet Time Access Control	NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Update Software Reboot	Software File Name: Browse No file selected.
Logout	Update Software

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.

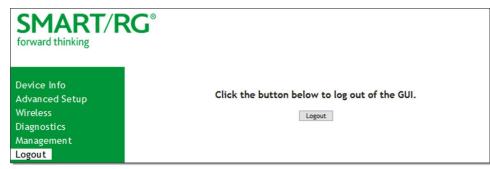


2. Click Reboot. Your gateway is rebooted and you must log in again if you want to make further changes.



# 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.



# **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: VW7DL01ASR501, 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 specifications techniques applicables d'Industrie Canada.

IC-CS03 statement



This product meets the applicable Industry Canada technical specifications. / Le présent matériel est conforme aux specifications 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 telephone 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 installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

- -Increase the separation between the equipment and receiver.
- -Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

#### 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 (VW7DL01ASR506N) 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
1.4	July 2020	Updated for SmartRG firmware release 2.6.2.5.
1.3	March 2020	Updated for SmartRG firmware release 2.6.2.4.
1.2	September 2019	Updated for firmware release 2.6.2.3.
1.1	September 2019	Updated for firmware release 2.6.2.2.
1.0	December 2016	Initial release of document.