

501 SE Columbia Shores Boulevard, Suite 500 Vancouver, Washington 98661 USA +1 360 859 1780 / smartrg.com

/ Gateway User Manual

For all Broadcom Chipset-based models including: ADSL 3xx series VDSL 5xx series

Firmware Versions: 2.6.1.6

Document Version 4.1

June 2018



Table of Contents

SMART/RG

Welcome!	3
Purpose & Scope	. 3
Intended Audience	3
Cotting Assistance	
Getting Assistance	
Copyright and Trademarks	
Disclaimer	
Getting Familiar with your Gateway	. 4
LED Status Indicators	. 4
Connections	
DSL	
WAN	
LAN	
USB	. 6
POWER	. 6
External Buttons	. 6
WPS Button	. 6
WiFi or WLAN Button	. 7
	• 4
Reset Button	. 7
Logging into your Gateway's UI	. 7
Device Info	. 9
Summary	. 9
WAN	
Statistics	
LAN	
WAN Service	.12
xTM	.13
xDSL	15
References	
Route	
ARP	
DHCP	. 20
VPN	.21
CPU & Memory	21
Advanced Setup	
Layer2 Interface	
ATM Interface	
PTM Interface	
ETH Interface	. 26
WAN Service	28
PPP over Ethernet	
IP over Ethernet	
Bridging	
LAN	
IPv6 Autoconfig	. 51
Ethernet Config	. 53
NAT	55
Virtual Servers	
Port Triggering	
	- 50
DMZ Host	
Security	. 59
IP Filtering - Outgoing	. 59
IP Filtering - Incoming	.60
MAC Filtering	62
Add a MAC Filtering Rule	62
Auu a MACTILLETING RULE	دں ۔ ۸ ۷
Parental Control	
Time Restriction	
URL Filter	
Quality Of Service	.67

QoS Config	67
Supported DSCP Values	68
QoS Queue Config	
WLAN Queue	70
QoS Classification	
QoS Port Shaping	
Routing	76
Default Gateway	
Static Route	77
Policy Routing	
RIP (Routing Information Protocol)	79
DNS	
DNS Server	
Dynamic DNS	
Static DNS	
DSL	
Advanced settings	
DSL Bonding	
UPnP	
DNS Proxy	
Storage Service	
Storage Device Info	90
User Accounts	
Interface Grouping	
IP Tunnel	
IPv6inIPv4	
IPv4inIPv6	
IPSec	
Advanced IKE Settings	
Certificate	
Local	
Trusted CA	. 103
Power Management	104
Multicast	. 105
Wireless	
Basic	
Security	
Open & Shared Authentication	112
802.1X Authentication	
WPA2 & Mixed WPA2/WPA Authentication	
WPA2-PSK & Mixed WPA2/WPA-PSK Authentic-	
ation	116
MAC Filter	
Wireless Bridge	
Advanced	
Station Info	124
Station Info Wifi Insight	. 124
Station Info Wifi Insight Site Survey	. 124 . 126
Station Info Wifi Insight Site Survey Channel Statistics	124 126 127
Station Info Wifi Insight Site Survey Channel Statistics Metrics	124 126 127 127
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics	. 124 . 126 . 127 . 127 . 127 . 128
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics Diagnostics	124 126 127 127 . 127 . 128 128
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics Diagnostics Ethernet OAM	124 126 127 .127 .127 .128 128 129
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics Ethernet OAM Ping	124 126 127 .127 .127 .128 128 129 .133
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics Ethernet OAM Ping Trace Route to Host	. 124 . 126 . 127 . 127 . 128 . 128 . 128 . 129 . 133 . 134
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics Ethernet OAM Ping Trace Route to Host Management	. 124 . 126 . 127 . 127 . 128 . 128 . 128 . 129 . 133 . 134 . 134
Station Info Wifi Insight Site Survey Channel Statistics Metrics Diagnostics Ethernet OAM Ping Trace Route to Host	124 126 127 . 127 . 128 128 129 . 133 134 134 134

SMARTRG INC. PROPRIETARY AND CONFIDENTIAL. ALL RIGHTS RESERVED. © 2018

Table of Contents

SMART/RG

Restore Default 136 System Log 137 Security Log 139 SNMP Agent 140 Management Server 141 TR-069 Client 141 STUN Config 144 Internet Time 147 Access Control 148 Accounts 148 Add an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 FCC Statements 156 FCC Radiation Exposure Statement 157 Ringer Equivalency Number Statement 157 IC CS-03 statement 158 Canada Statement 158 SGHz 159 Revision History 160	Update	
System Log 137 Security Log 139 SNMP Agent 140 Management Server 141 TR-069 Client 141 STUN Config 144 Internet Time 147 Access Control 148 Accounts 144 Modify or Delete an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 Logout 156 FCC Statements 156 FCC Radiation Exposure Statement 157 Ringer Equivalency Number Statement 157 IC CS-03 statement 158 Canada Statement 158 SGHz 159		
Security Log 139 SNMP Agent 140 Management Server 141 TR-069 Client 141 STUN Config 144 Internet Time 147 Access Control 148 Accounts 148 Accounts 148 Add an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 Logout 156 FCC Statements 156 FCC Interference Statement 156 FCC PART 68 157 Ringer Equivalency Number Statement 157 IC CS-03 statement 158 SGHz 159		
SNMP Agent 140 Management Server 141 TR-069 Client 141 STUN Config 144 Internet Time 147 Access Control 148 Accounts 148 Add an Account 148 Modify or Delete an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 Logout 156 FCC Statements 156 FCC Radiation Exposure Statement 157 Ringer Equivalency Number Statement 157 IC CS-03 statement 158 Canada Statement 158 SGHz 159		
Management Server 141 TR-069 Client 141 STUN Config 144 Internet Time 147 Access Control 148 Accounts 148 Accounts 148 Add an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 Logout 156 FCC Statements 156 FCC Radiation Exposure Statement 157 Ringer Equivalency Number Statement 157 IC CS-03 statement 158 SGHz 159		
TR-069 Client 141 STUN Config 144 Internet Time 147 Access Control 148 Accounts 148 Accounts 148 Add an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 Logout 156 FCC Statements 156 FCC Radiation Exposure Statement 157 Ringer Equivalency Number Statement 157 IC CS-03 statement 158 Canada Statement 158 SGHz 159		
STUN Config 144 Internet Time 147 Access Control 148 Accounts 148 Add an Account 148 Add an Account 148 Modify or Delete an Account 150 Default Passwords 150 Services 151 Passwords 152 Access List 153 Logout Timer 154 Update Software 155 Reboot 155 Cogout 156 FCC Statements 156 FCC Radiation Exposure Statement 157 Ringer Equivalency Number Statement 157 Ringer Equivalency Number Statement 158 Canada Statement 158 5GHz 159	TR-069 Client	141
Access Control148Accounts148Add an Account148Modify or Delete an Account150Default Passwords150Services151Passwords152Access List153Logout Timer154Update Software155Reboot155FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157Ringer Equivalency Number Statement158Canada Statement1585GHz159		
Accounts148Add an Account148Modify or Delete an Account150Default Passwords150Services151Passwords152Access List153Logout Timer154Update Software155Reboot155FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157Ringer Equivalency Number Statement158Canada Statement158SGHz159	Internet Time	
Add an Account148Modify or Delete an Account150Default Passwords150Services151Passwords152Access List153Logout Timer154Update Software155Reboot155Cogout156FCC Statements156FCC Radiation Exposure Statement157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159		
Add an Account148Modify or Delete an Account150Default Passwords150Services151Passwords152Access List153Logout Timer154Update Software155Reboot155Cogout156FCC Statements156FCC Radiation Exposure Statement157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Accounts	148
Default Passwords150Services151Passwords152Access List153Logout Timer154Update Software155Reboot155Logout156FCC Statements156FCC Radiation Exposure Statement157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Add an Account	
Default Passwords150Services151Passwords152Access List153Logout Timer154Update Software155Reboot155Logout156FCC Statements156FCC Radiation Exposure Statement157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Modify or Delete an Account	150
Passwords152Access List153Logout Timer154Update Software155Reboot155Logout156FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement158Canada Statement1585GHz159		
Access List153Logout Timer154Update Software155Reboot155Logout156FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Services	151
Logout Timer154Update Software155Reboot155Logout156FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Passwords	152
Update Software155Reboot155Logout156FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Access List	
Reboot155Logout156FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Logout Timer	154
Logout156FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Update Software	
FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Reboot	155
FCC Statements156FCC Interference Statement156FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	Logout	156
FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	FCC Statements	156
FCC Radiation Exposure Statement157FCC - PART 68157Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159	FCC Interference Statement	156
Ringer Equivalency Number Statement157IC CS-03 statement158Canada Statement1585GHz159		
IC CS-03 statement	FCC - PART 68	157
Canada Statement	Ringer Equivalency Number Statement	
5GHz	IC CS-03 statement	
•••.=		
	5GHz	
	Revision History	160



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 their 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 at the bottom of the Support page of 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

© 2018 by SmartRG, Inc. 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 a quick description of the Gateway's lights, ports, and buttons. SmartRG produces several models that vary slightly in capabilities (See Appendix B for details) but the basic scheme of lights, ports and buttons represented in this section exists on each model.

LED Status Indicators

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

	POWER	WAN	LAN 1-4	WLAN	WPS	DSL 1 or 2	INTERNE
Power up test failure	•						
DSL sync acquired and gateway online	•					۲	۲
No sync to DSL line						0	
DSL sync in progress	•					٢	
Mode m authenticatio n in progres s							()
DSL sync acquired and gateway online							
Gateway online and data transfer in progress	٠						٢
IP connec tion failure							0
Connec tion dropped – attempting		0				0	
re-authentication							
LAN device on network connected							
Wi-Fi enable d on modem				•			
PC / network activity / data transfer	•	•/	•/{	•/🔅			•/{
WPS Setup procedur e in progres s				•	()		
Failure to find any partner with which to pair					•		
ession overlap detected. Possible securit y risk	•				()		
WPS Connec tion complet ed successfully							

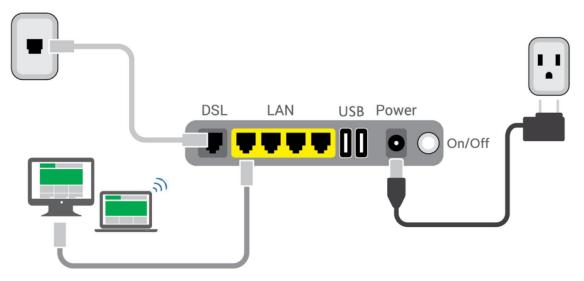
: On O: Off Slinking / active





Connections

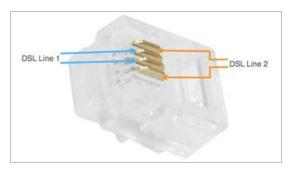
Below is a generic representation of a SmartRG gateway, Your specific model may have more or fewer ports and controls. Refer to the Quick Start Guide enclosed with your gateway for specifics regarding installation of your particular model.



The ports depicted in this example are described below.

DSL

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



WAN

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

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

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

LAN

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

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

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

USB

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

POWER

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

External Buttons

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

The following describes each of these controls. To identify the buttons that appear on your gateway model, refer to the Quick Start Guide for that model.

WPS Button

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

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

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

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

The location of the WPS button varies by model:

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

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

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

WiFi or WLAN Button

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

The location of the WLAN button varies by model:

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

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

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

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

Reset Button

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

The location of the Reset button varies by model:

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

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

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

Logging into your Gateway's UI

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

1. Open a browser and enter the gateway's default address (usually http://192.168.1.1; may also be http://192.168.0.1) in the address bar.

2. For some models, the Network status page appears. If so, click the Manage gateway (advanced) link (usually located in the upper right corner). The Authentication Required dialog box appears.

Network status	password. The User Name:	//192.168. ierver says: dmin		x username and er.	Manage sateway (advanced) View.log
Please wait while	Password:		Cancel	Log In	
Setup will be compl	lete in a few min	ites.			
Setup will be compl	lete in a rew min				

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

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

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

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

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

Device Info

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

Summary

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

Note: The following variations exist:

- For the SR3xxn models, the Symmetric CPU Threads field and Aggregate Line Rate fields are not applicable.
- For the SR505n and SR510n models, the Aggregate Line Rate fields are not applicable. The BO Traffic & B1 Traffic fields are used in these models and are not shown below.
- For the SR515ac model, the Traffic Type and Aggregate Line Rate fields are not applicable. Instead, the BO Traffic Type, BO Line Rate Upstream, BO Line Rate Downstream, B1 Traffic Type, B1 Line Rate Upstream, and B1 Line Rate Downstream appear.



forward thinking				SR552r			
Device Info	Device Info						
Advanced Setup Wireless	Board ID:	SR552n		1			
Diagnostics	Symmetric CPU Threads:	2					
Management	Build Timestamp:	Build Timestamp: 180619_1938					
ogout	Software Version:	Software Version: 2.6.1.2018:06					
	Configuration File Origin:	Configuration File Origin: ClearAccess					
	Bootloader (CFE) Version:	Bootloader (CFE) Version: 1.0.38-118.3					
	DSL PHY and Driver Version:	d26u					
	Wireless Driver Version:	Wireless Driver Version: 7.14.164.23.cpc					
	Uptime:	Uptime: 0D 0H 12M 20S					
	System Base MAC Address:	System Base MAC Address: 00:23:6a:a0:9f:1b					
	Serial Number:	SR552NA025-0	010870	-			
	This information reflects the Traffic Type:		of your WAN of PTM 60014	onnection.			
	the second s						
	Aggregate Line Rate - Down	stream (kops):	192.168.1.1				
	Default Gateway: WAN IPv4 Address		ppp0 10.101.2.4				
	Primary DNS Server:		8.8.8.8				
			8.8.4.4				
	Secondary DNS Server:		0.0.4.4				
	DAIN INVO OLA ADDRESS:						

WAN

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

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

ward thinking													SR	552n
ice Info								WAN	Info					
atistics	Interface	Description	Туре	VlanMuxid	Pv6	lgmp Pxy	lgmp Src Enbk	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address
Nute Sp HCP	ppp0	pppoe_0_0_1	PPPoE	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected Username autoconfig	10.101.2.4	(null)

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

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

Statistics

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

Notes:

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



LAN

On this page, you can view the received and transmitted bytes, packets, errors and drops for each LAN interface configured on your gateway. All local LAN Ethernet ports, Ethernet WAN ports and wireless Interfaces are included. For some models, statistics are provided for multicast, unicast and broadcast traffic.

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.

evice Info Summary	Statistics	LAN																
WAN		Received										Transmitted						
tatistics	Interface	Total				Multicast		Unicast	cast Broadcast	Total				Multicast		Unicast	Broadcas	
LAN		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Ems	Drops	Bytes	Pkts	Pkts	Pkts	
WAN Service	LANT	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
xTM	LAN2	13356956	18862	0	1	0	1571	17245	46	16794649	35315	0	0	0	1575	22400	11340	
x090	LAN3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
oute	LANA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
RP	WAN	7676070	8037	0	29	0	1193	6811	33	1518165	15154	0	0	0	1949	1853	11352	
HCP PN	Wheeless	0	Ô	0	9	0	0	0	0	0	0	0	0	0	0	0	0	

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

Field Name	Description
Interface	Available LAN interfaces. Options are LAN1 - LAN4, WAN (if configured on your device), WI0 (Wire- less LAN-side interface)(<i>not applicable for SR515ac</i>), Wireless, and 2.4 GHz and 5 GHz (<i>SR515ac only</i>).
Received & T	ransmitted columns
Bytes	Total number of packets in bytes.
Pkts	Total number of packets.
Errs	Total number of error packets.
Drops	Total number of dropped packets.

WAN Service

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



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

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

SMART/R	ß														SR	552n
Device Info Summary	Statistics W	VAN										*				
WAN	Service			eceived Multicast UnicastBroadcast					Multicast UnicastBroade			Broadcas				
Statistics	Description	Bytes	Pkts Er	TS Drop	-			Pkts	Bytes	and the second se	ms	Drops	de constituiones		Pkts	Pkts
LAN WAN Service	pppoe_0_0_1				0	0	14655	0	12243098	the second s	_	0	0	0	14012	0
xTM xDSL	Reset Statistics	1														
Route		_				~	_		~	-			~	ينج		

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

Field Name	Description
Service Descrip- tion	Service description. Options are: pppoe , ipoe , and b .
Received & Trans	mitted columns
Bytes	Total quantity of packets in bytes.
Pkts	Total quantity of packets.
Errs	Total quantity of error packets.
Drops	Total quantity of dropped packets.

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 Statistics** near the bottom of the page.

evice Info					Inter	face Stati	stics		_		
Summary WAN	Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
itatistics	1	10304710	13433680	28550	14282	0	0	0	0	0	0
LAN WAN Service xTM xDSL oute						Reset					

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

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

xDSL

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

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

RG°				S		
Statistics xDSL						
and a start of a start of a start of the						
Bonding Une Selection Ine G 🕤						
Entertaine Westmen L		00 (H 16M 1				
Last Synchronized: Retzain Count:		00 011 16/01	13			
and the second		1	-			
Made:		VOSL2	20			
Traffic Type: States:		PTM				
Unk Power State:		Lip L0	-			
	10.000					
	Downstream	nUpstream				
Une Coding(Trellis):	On	On				
SNR Margin (dB): Attenuation (dB):	11.9	9.2				
Attenuation (dll): Output Power (dBm):	4.2	11.1	-			
Attainable Rate (Rbps):	156714	62887	1			
PhyR Status:	inactive	Inactive.				
G.inp Status:	biactive .	Inactive				
	Path 0	1	Path 1			
	Downstream	nUpstream	Downstre	am Upstream		
Sate (Kbps):	100014	60014	þ	<u>jo</u>		
8 (# of bytes in Mux Data Frame):	79	207	þ	þ		
M (If of Mux Data Frames in an R5 codeword):	1	1	0	p.		
T (# of Mex Data Frames in an OH sub-frame):	59	22	0	0		
R [# of redundancy bytes in the RS codeword]: 5 [# of data symbols over which the RS code word spans	0.0255	0.1103	0	0		
	29544	15959	0	80		
L (# of bits transmitted in each data symbol): D (interleaver depth):	661	337	0	0		
1 (Interleaver block size in bytes):	94	110	0	0		
N (RS codeword size):	94	220	0	8		
Delay (miec): MP (DMT symbol):	4	5 0.50	0.00	0.00		
the form standard	1.00	p. 14	10.00	9.00		
OH Frames:	864047	534800	0	10		
OH Frame Errors:	0	058	0	ø		
RS Words: RS Correctable Errons:	152780549	05438546	0	0		
RS Lorrectable Errors: RS Uncorrectable Errors:	0	0	0	0		
RS Codewords Received:	0	6	6	0		
RS Codewords Corrected:	0	0	0	10		
RS Codewords Uncorrected:	0	0	0	þ		
HEC Errors:	6	6	0	10		
OCD Erron:	0	0	0	10		
LCD Emini	0	0	6	10		
Yotal Cells:	187910253	0	0	0		
Outa Cels:	160369	0	0	0		
Bit Enviro	0	þ	þ	þ		
Total ESc	Total ESc. 0 50					
Total SES:	0	p	2			
Tetal UAS:	115	115	<u>.</u>			
405, 803 Test Asset Statistics						

- 2. In the **Bonding Line Selection** field, select the line for which you want to view the statistics.
- Note: For the SR350n, SR360n, SR505n, and SR515ac models, the Bonding Line Selection field does not appear.
- 3. To run an xDSL Bit Error Rate (BER) test (to determine the quality of the xDSL connection):
 - a. Scroll to the bottom of the page and click xDSL BER Test. The ADSL BER Test Start dialog box appears.
 - b. In the Tested Time field, select the duration in seconds and click Start. Options range from 1 second to 360 seconds. The test transfers idle cells containing a known pattern and compares the received data with this known pattern. Comparison errors are tabulated and displayed. To stop the test, click Stop.
- 4. To reset the counters, click Reset Statistics at the bottom of the page.

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

Field Name	Description
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, PTM and ETH.
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 Upst	ream columns
Line Coding (Trellis)	State of theTrellis Coded Modulation. Options are On and Off .
SNR Margin (0.1 dB)	The signal-to-noise ration margin (SNRM) is the maximum increase (in dB) of the received noise power, such that the modem can still meet all of the target BERs over all the frame bearers. [2]
Attenuation (0.1 dB)	The signal attenuation is defined as the difference in dB between the power received at the near-end and that transmitted from the far-end. [2]
Output Power (0.1 dBm)	Transmit power from the gateway to the DSL loop relative to one 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 Mar- gin
	• BER not to exceed the highest BER configured for one (or more) latency paths
	 Latency not to exceed the highest latency configured for one (or more) latency paths
	 Accounting for all coding gains available (e.g., trellis coding, RS FEC) with latency bound
	Accounting for the loop characteristics at the instant of measurement [2]
PhyR Status	(<i>Visible only for gateways connected via DSL</i>) Physical Layer Retransmission fea- ture status. Options are Inactive and Active .
G. inp Status	(<i>Visible only for gateways connected via DSL</i>) The status of video data retrieval from the buffer. Options are Inactive and Active .
Rate (Kbps)	The current net data rate of the xDSL link. Net data rate is defined as the sum of all frame bearer data rates over all latency paths. [2]

Field Name	Description
Downstream and Upst	ream 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 Refer- ence 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 cur- rent 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 (# of data symbols over which the RS code word spans)	The number of data symbols over which the RS code word spans.
L (# of bits transmitted in each data symbol)	The number of bits transmitted in each data symbol.
D (interleaver depth)	The interleaving depth in the current latency path.
I (Interleaver block size in bytes)	(Available for SR515ac models only) The block size used for interleaving data trans- missions.
N (RS codeword size)	(<i>Available for SR515ac models only</i>) 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.
OH Frames	The number of xDSL OH Frames transmitted/received.
OH Frame Errors	The number of xDSL OH Frames transmitted/received with errors.
(End of DSL-specific fie	eld group)
Super Frames	(<i>Not applicable for SR515ac models</i>) The number of xDSL Super Frames trans- mitted/received.
Super Frame Errors	(<i>Not applicable for SR515ac models</i>) The number of xDSL Super Frames trans- mitted/received with errors.
RS Words	The number of Reed-Solomon-based Forward Error Correction (FEC) codewords transmitted/received.
RS Correctable Errors	The number of Reed-Solomon-based FEC codewords received with errors that have been corrected.
RS Uncorrectable Errors	The number of Reed-Solomon-based FEC codewords received with errors that were not correctable.
RS Codewords Received	(Visible only for gateways connected via DSL) Total number of Reed-Solomon Code- words received.
RS Codewords Cor- rected	(Visible only for gateways connected via DSL) Total number of Reed-Solomon Code- words corrected.
	(Visible only for gateways connected via DSL) Total number of Reed-Solomon Code- words Uncorrected

Field Name	Description
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 peri- ods 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 inter- vals for which the xDSL line is unavailable. The xDSL line becomes unavailable at the onset of 10 contiguous SES's. These 10 SES's shall be included in the unavail- able time. Once unavailable, the xDSL line becomes available at the onset of 10 con- tiguous seconds with no SES's. These 10 seconds with no SES's shall be excluded from unavailable time. [4]

References

[1] ITU-T Recommendation G.992.1 (1999), Asymmetric digital subscriber line (ADSL) transceivers.

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

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

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

Route

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

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

Device Info -	Route								
Flags: U - up, D - dynamic (tate			
Destination	Gateway	Subne	t Mask	Flag	Metric	Servi	ce	Interfac	æ
0.0.0.0	0.0.0.0	0.0.0.0	0	U	0	pppo	e_0_0_1	ppp0	
10.101.2.1	0.0.0.0	255.25	5.255.255	UH	0	pppo	e_0_0_1	ppp0	
y 192.168.1.0	0.0.0.0	255.25	5.255.0	U	0		-	br0	
IPv6 Route Rags: U - up, D - dynamic (M - moo	dified (red						
Rags: U - up, D - dynamic (Destination	redirect), /	M - moc	dified (red Next Hop	irect)		Flag	Metric	Service	Interface
Rags: U - up, D - dynamic (redirect), /	M - moc	dified (red Next Hop	irect)		Flag	Metric 0	Service	Interface ptm0
Rags: U - up, D - dynamic (Destination	redirect), /	M - moo	dified (red Next Hop	irect)		Flag	and the second second	Service	Contraction of the
Flags: U - up, D - dynamic (Destination fe80::223:6a	redirect), /	M - moc	dified (red Next Hop fe80::223:	irect)		Rag	0	Service	ptm0
Flags: U - up, D - dynamic (Destination fe80::223:6a fe80::264	redirect), /	M - mod	dified (red Next Hop fe80::223: ::	irect)		Plag U U	0	Service	ptm0 br0

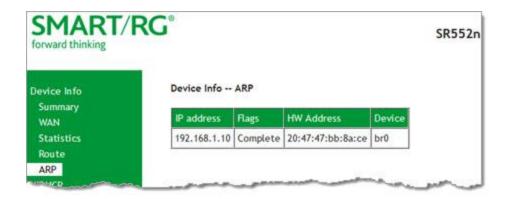
The fields on this page are explained in the following table.

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

ARP

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

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



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

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

DHCP

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

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

SMART/R	G°	SR552n
Device Info Summary	Device Info DHCP Leases Hostname MAC Address IP Address Expires In	
WAN Statistics Route		

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.

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°						SR552
Device Info Summary	Device In	fo IPSec	Tunnels				
WAN Statistics	Tunnel Name	Interface	Remote Gateway	LAN-side Addresses	Remote-side Addresses	Enabled	Connection State
Route ARP						n	~~~~

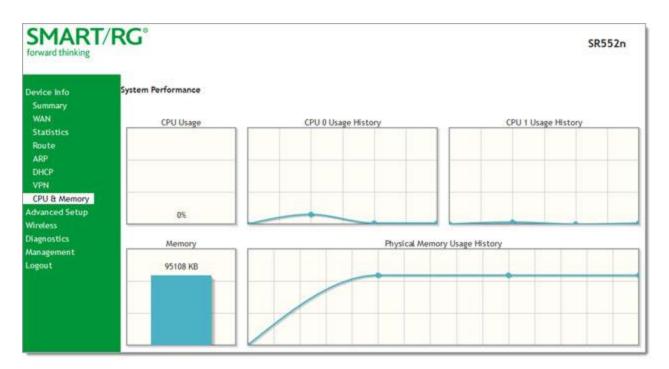
The fields on this page are explained in the following table.

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.

CPU & Memory

On this page, you can view the CPU and memory data for the gateway.

In the left navigation bar, click **Device Info > CPU & Memory**. The following page appears, showing the current usage and history. The information refreshes automatically.



Advanced Setup

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

Layer2 Interface

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

ATM Interface

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

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

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

SMART/R	G°	SR5	52n
Device Info	ATM PVC Configuration		
Advanced Setup		Annual March Party	
Layer2 Interface	This screen allows you to cor	ingure a AIM PVC.	
ATM Interface	VPI: 0 [0-255]		
PTM Interface	VCI: 15 [32-65535]		
ETH Interface	ver. [3 [32-05555]		
WAN Service	Select DSL Latency		
LAN	STATES FILS FOR THE MAIL		
Ethemet Config	Path0 (Fast)		
NAT	Path1 (Interleaved)		
Security	Colore DCL Link Tone (Cold in		
Parental Control	Select DSL Link Type (EoA is	for PPPoE, iPoE, and Bridge.)	
Quality of Service	O PPPoA		
Routing	O IPoA		
DNS			
DSI,	Encapsulation Mode:	LLC/SNAP-BRIDGING ~	
DSL Bonding			
UPnP	Service Category:	UBR Without PCR Y	
DNS Proxy	Minimum Cell Rate:	-1 [cells/s] (-1 indicates no shaping)	
Storage Service	Menimum Cea Rate:	teasys1(-rimocates no snaping)	
Interface Grouping	Select Scheduler for Queues	of Equal Precedence as the Default Queue	
IP Tunnel	Weighted Round Robin	M. 8	
IPSec	O Weighted Fair Queuing		
Certificate			
Multicast	Default Queue Weight:	1 [1-63]	
Wireless	Default Queue Precedence:	[8] [1-8] (lower value, higher priority)	
Diagnostics	VC WRR Weight:	1 [1-63]	
Management	VC Precedence:	 [1-8] (lower value, higher priority) 	
Logout	Note: VC scheduling will be S precedence VC's.	P among unequal precedence VC's and WRR among equal	
		ault queue precedence and weight will be used for arbitrat recedence and weight will be used for arbitration.	ion.
		Back Apply/Save	

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

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

Field Name	Description
VPI	Enter a Virtual Path Identifier. A VPI is an 8-bit identifier that uniquely identifies a network path for ATM cell packets to reach its destination. A unique VPI number is required for each ATM path. This setting works with the VCI. Each individual DSL circuit must have a unique VPI/VCI combination. Options are: 0-255 . The default is 0 .
VCI	Enter a Virtual Channel Identifier. A VCI is a 16-bit identifier that has a unique chan- nel. Options are: 32-65535 . The default is 35 .

Field Name	Description
Select DSL Latency	Select the level of DSL latency. Options are:
	 Path0 Fast: No error correction and can provide lower latency on error free lines. Path1 Interleaved: Error checking that provides error free data which increases latency.
Select DSL Link Type	Select the linking protocol. 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 (Per- manent Virtual Circuit). Options are:
	• LLC/ENCAPSULATION: (Available when PPPoA is selected as the Link <i>Type</i>) Logical Link Control (LLC) encapsulation protocols used with multiple PVCs.
	• LLC/SNAP-BRIDGING: (Available when EoA is selected as the Link Type) LLC used to carry multiple protocols in a single PVC.
	 LLC/SNAP-ROUTING: (Available when IPoA is selected as the Link Type) LLC used to carry one protocol per PVC.
	 VC/MUX: Virtual Circuit Multiplexer creates a virtual connection used to carry one protocol per PVC.
Service Category	Select the bit rate protocol. Options are:
	 UBR without PCR: Unspecified Bit Rate with no Peak Cell Rate, flow control or time synchronization between the traffic source and destination. Commonly used with applications that can tolerate data / packet loss. UBR with PCR: Same as above but with a Peak Cell Rate.
	 CBR: Constant Bit Rate relies on timing synchronization to make the net- work traffic predictable. Used commonly in Video and Audio traffic network applications.
	• NON Realtime VBR: Non Realtime Variable Bit Rate used for connections that transport traffic at a Variable Rate. This category requires a guaranteed bandwidth and latency. It does not rely on timing synchronization between the destination and source.
	• Realtime VBR: Realtime Variable Bit Rate. Same as the above option but relies on timing and synchronization between the destination and source. This category is commonly used in networks with compressed video traffic.
Minimum Cell Rate	Minimum allowable rate (cells per second) at which cells can be sent on a ATM net- work. For no shaping, enter -1 .

Field Name	Description
Scheduler for Queues of Equal Precedence as the Default Queue	The algorithm used to schedule the queue behavior. VC scheduling is unique from Default Queues. Options are:
	• Weighted Round Robin: Packets are accessed in a round robin style and classes can be assigned.
	• Weighted Fair Queuing: Packets are assigned in a specific queue.
Default Queue Weight	The default weight of the specified queue. Options are: 1-63. The default is 1.
Default Queue Pre- cedence	The precedence of the specified group. Options are: 1-8 . The default is 8 .
VC WRR Weight	Enter the weight of the VC queue. Options are: 1-63. The default is 1.
VC Precedence	Enter the precedence of the VC group. The lower the value, the higher the priority. Options are: 1-8 . The default is 8 .

PTM Interface

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

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

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

SMART/R	G°		SR552r
Device Info	PTM Configuration		
Advanced Setup	This screen allows you to configur	P	TAL Form
Layer2 Interface	This screen atows you to configur	e ar	I'M NOW.
ATM Interface	Select DSL Latency		
PTM Interface	Path0 (Fast)		
ETH Interface	Path1 (Interleaved)		
WAN Service	Educt Eduction for Ocean of Ed	10	and a set of the Defende Original
LAN	Select Scheduler for Queues of Eq Weighted Round Robin	uat P	recedence as the behaut Queue
Ethernet Config NAT	O Weighted Fair Queuing		
Security	Default Queue Weight:	1	[1-63]
Parental Control	Default Queue Precedence:	8	[1-8] (lower value, higher priority)
Quality of Service	STATES AND STATES	_	Accession researchers in the second
Routing	Default Queue Minimum Rate:	-1.	[1-60014 Kbps] (-1 indicates no shaping)
DNS	Default Queue Shaping Rate: Default Queue Shaping Burst Size:	-1	[1-60014 Kbps] (-1 indicates no shaping) [bytes] (shall be >=1600)
DSL.	Default Queue snaping burst size:	1000	_[oyces] (snar be >= 1600)
DSL Bonding UPnP	D	Back	Apply/Save
DNS Proxy			

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

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

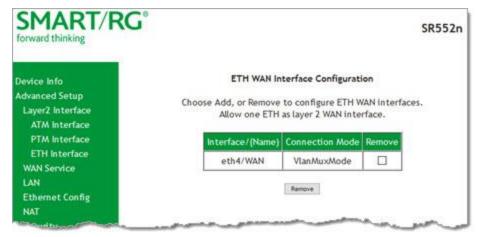
Field Name	Description	
Select DSL Latency	Select the level of DSL latency. Options are:	
	 Path0 Fast: No error correction and can provide lower latency on error-free lines. Path1 Interleaved: Error checking that provides error-free data which increases latency. 	
Select Scheduler for Queues of Equal Pre-	Select an algorithm for applying queue data priority. Options are:	
cedence as the Default Queue	• Weighted Round Robin: Time slices are assigned to each process in equal portions and in circular order, handling all processes without priority (also known as cyclic executive).	
	• Weighted Fair Queuing: A data packet scheduling technique allow- ing different scheduling priorities to be assigned to statistically mul- tiplexed data flows. Since each data flow has its own queue, an ill- behaved flow (that sent larger packets or more packets per second than the others since it became active) will only affect itself and not other sessions.	
Default Queue Weight	Enter a default weight of the specified queue. Options are: 1-63 .	
Default Queue Pre- cedence	Enter a precedence for the specified queue. Options are: 1-8 .	
Default Queue Minimum Rate	m (Does not appear for SR350n models) 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	(<i>Does not appear for SR350n models</i>) The shaping rate for the specified queue. For no shaping, enter -1 (disabled). Options are: 1-0 Kbps.	
Default Queue Shaping Burst Rate	(<i>Does not appear for SR350n models</i>) The maximum rate at which traffic can pass through the queue. Options are 1600 or greater.	

ETH Interface

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

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

- 1. In the left navigation bar, click Advanced Setup > Layer2 Interface > ETH Interface.
- 2. If no WAN port is configured, the Add button appears. Click Add.
- 3. If a WAN port is already configured or you clicked Add, the following page appears.



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

- 4. Select the LAN port you wish to act as a WAN port.
- 5. Click Apply/Save to commit your changes.
- 6. To remove the WAN interface, click the **Remove** checkbox and then click the **Remove** button.

WAN Service

In this section, you can configure WAN services for:

- "PPP over Ethernet"
- "IP over Ethernet"
- "Bridging"

A sample configuration scenario is provided for each variation.

PPP over Ethernet

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

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

SMART/RG [®]		SR552n
Device info	WAN Service Interface Configuration	
Advanced Setup Layer2 Interface WAN Service	Select a layer 2 interface for this service	
WAR Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS	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=4> DSL Latency PATH1 low =0> Low PTM Priority not set low =1> Low PTM Priority set high =0> High PTM Priority set	
DSL.	atm0/(0_0_35) ~	
DSL Bonding UPnP DNS Proxy	Back SHELT	
Storage Service		-

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

3. Click Next. The following page appears.

SMART/R	G°	SR552n
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 DSL DSL Bonding	Enter Service Description: Desc	
UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel	Enter 802.1P Priority [0-7]: Enter 802.1Q VLAN ID [0-4094]: Select VLAN TPID:	a ⊴ Select a TPID ⇒
PSec Certificate Multicast Wireless Diagnostics Management Logout	Internet Protocol Selection: IPV4 Only ~ Eack Peert	

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

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

Field Name	Description
Enter Service Description	Enter a name to describe this configuration.
Enter 802.1P Priority	Options are 0 - 7 . The default is -1 (disabled).
	For tagged service, enter values in this field and the 802.1Q VLAN ID field.
	For untagged service, enter -1 (disabled) in this field and the 802.1Q VLAN ID field.
Enter 802.1Q VLAN ID	Options are 0 - 4094 . The default is -1 (disabled).
	For tagged service, enter values in this field and the 802.1P Priority field.
	For untagged service, enter -1 (disabled) in this field and the 802.1P Priority field.
Select VLAN TPID	(Optional) Select the TPID for this VLAN. Options are: 0x8100, 0x88A8, and 0x9100.
Selection	Different scheduling priorities can be applied to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (which has sent larger packets or more packets per second than the others) will only punish itself and not other sessions. Options are IPv4 Only ,

Field Name	Description
	IPv4&IPv6 (Dual Stack), and IPv6 Only.
	Note: When you select IPV4&IPV6 or IPV6, the subsequent options presented will change accord-
	ingly.

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

MART/R		SR552	
ice info	PPP Username and Password		
anoed Setup yer2 Interface		ave a user name and password to establish your connection. In	
UN Service	ure poxes below, enter the use	r name and password that your ISP has provided to you.	
N	200222330007383	LUse base MAC address as	
ernet Config T	PPP Username: substr	username	
writy.	PPP Password:	444	
ental Control	Authentication Auto	· · · ·	
dity of Service ting	Method:		
	Link Control Protocol		
Bonding	LCP Keepalive Period (s):		
0	LCP Retry Threshold:		
Proxy			
rage Service	PPP IP extension		
rface Grouping Uncel			
ĸ	Advanced DMZ Non DMZ #		
tificate	Address:		
ticast	Non OW2 Net Mask: IIIA.IIA.IM		
ess ostics	Use Static IPv4 Address		
gements			
a.			
	Use Static IPv6 Address		
	Enable IPv6 Unnumbered Model		
	Launch Dhopisc for Address	Assignment (IANA)	
	E Launch Dhopsic for Prefix I	elegation (UPO)	
	Retry PPP password on aut		
	Max PPP authentication retries		
	1월 23일 이 일종가 물망이 가슴 것이다.	(recently line of the entry mean interior	
	Enable PPP Debug Mode		
	Eridge PPPoE Frames Beby	een 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 Fulicone NAT		
	Enable SP ALG		
	IGMP Multicast		
	Enable IGMP Multicast Proxy		
	Enable IGMP Multicast Sou	rce	
	MLD Multicast		
	Enable MLD Multicast Prox	,	
	Enable MLD Multicast Sour		
	MTU size [1370-1492]: 1+40		
	the state of the s	his WAN Interface (Note: only select this for one WAN Interface)	
		and a second s	

7. Modify the fields as needed.

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

Field Name	Description	
PPP Username and Pa	ssword section	
PPP Username	Enter the username required for authentication to the PPP server.	
Use base MAC address as username	Click this checkbox to use the base MAC address of the gateway as the PPP user name.	
PPP Password	Enter the password required for authentication to the PPP server.	
PPPoE Service Name	(Optional) Enter a description for this service.	
Authentication Method	Select a means for authentication. Options are:	
	 AUTO: Attempt to automatically detect handshake protocol. This is the default. 	
	• PAP: Password Authentication Protocol (plaintext passwords).	
	 CHAP: Challenge Handshake Authentication Protocol. (MD5 hashing scheme on passwords). 	
	MSCHAP: Microsoft Challenge Handshake Authentication Protocol.	
	(Microsoft encrypted password authentication protocol).	
Link Control Protocol s	ection	
LCP Keepalive Period (s)	The frequency with which the keepalive packet is sent by the gateway to the PPP server. The default is ${f 30}$.	
LCP Retry Threshold	Enter the number of additional attempted packets that the gateway will send (in the event that the PPP server does not respond to the Keepalive) before giving up and declaring the connection as Failed. The default is 3 .	
PPP IP Extension	Select whether to forward all traffic to the specified advanced DMZ IP. When you select this option, the Advanced DMZ checkbox becomes available.	
Advanced DMZ	(Available only when PPP IP Extension is selected) Specify the IP address and net mask to which PPPoE traffic is forwarded.	
Use Static IPv4 Address	Click to use a static IPv4 address for this WAN service. The IPv4 Address field appears. Enter the static IPv4 address for this WAN service.	
Use Static IPv6 Address	Click to use a static IPv6 address for this WAN service. The IPv6 Address field appears. Enter the static IPv6 address for this WAN service.	
Enable IPv6 Unnumbered Model	(<i>Available only for IPv6 environments</i>) Click to enable IP processing on a serial interface without assigning it an explicit IP address. The IP address of another interface can "borrow" the IP address of another interface already configured on the router, which conserves network and address space.	
Launch Dhcp6c for Address Assignment	(Available only for IPv6 environments) Click to enable the gateway to receive the WAN IP from the ISP.	

Field Name	Description
(IANA)	
Launch Dhcp6c for Prefix Delegation (IAPD)	(<i>Available only for IPv6 environments</i>) This option is enabled by default and enables the gateway to generate the WAN IP's prefix from the server's REST by MAC address. To <i>disable</i> this options, clear the checkbox.
Retry PPP password on authentication error	In the Max PPP authentication retries field, enter the maximum number of PPP authentication retries on failure. Options are 1 - 65536 . Entering 65536 sets the maximum to unlimited.
Enable PPP Debug Mode	Select to have the system put more PPP connection information into the sys- tem 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 enabled by default. To disable functions in the Security sub- menu, click the checkbox to clear it.
Enable SYN Flood rules	Click to enable SYN flood rules. Enabling this feature may degrade TCP per- formance.
Network Address Trans	slation settings
Enable NAT	Select to enable sharing the WAN interface across multiple devices on the LAN. Additional NAT and PPPoE NAT features appear.
Enable Fullcone NAT	(<i>Appears when Enable NAT is selected</i>) 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.
Port Control Protocol Mode	(<i>Available for SR515ac models only</i>) This option is disabled by default. Select a protocol to allow the PCP server to control how incoming packets are processed for NAT or packet filtering. Options are DS-Lite and NAT444 .
PCP Server	(<i>Available for SR515ac models only</i>) Enter the server IP address for the port control protocol.
IGMP Multicast section	
Enable IGMP Multicast Proxy	(<i>Appears when Enable NAT is selected</i>) Click to enable Internet Group Mem- bership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable IGMP Multicast Source MLD Multicast section	(<i>Available for SR515ac models onl</i> y) Select to enable this service to act as an IGMP multicast source.

Field Name	Description
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.
	(<i>Available only for IPv6 environments</i>) Click to enable this service to act as an MLD multicast source.
	Enter the MTU (Maximum Transmission Unit) size for SmartRG gateways sup- porting a gigabit-capable WAN interface. Options are 1370 - 1492 bytes . The default is 1492 bytes. This feature is supported by SmartRG models SR500n, SR505n, SR510n, SR515ac, SR550n and SR552n. Firmware v2.5.0.7 or later is required.
	Use the SmartRG Devices Base (Primary) MAC address. When unchecked, a unique MAC is assigned for each service.

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

SMART/R	G°	SR552n
Device Info Advanced Setup	Routing Default Gateway	
Layer2 interface WAN Service LAN Ethernet Config NAT	Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the 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.	
Security Parental Control	Selected Default Gateway Interfaces	Available Routed WAN Interfaces
Quality of Service Routing DNS DSL DSL Bonding UPmP	ppp0 ^	ppp2.1 ppp1.1
DNS Proxy Storage Service Interface Grouping IP Tunnel	. v	~
IPSec Certificate Multicast Wireless Diagnostics	IPv6: Select a preferred wan Selected WAN Interface ppp	interface as the system default IPv6 gateway. oe_0_0_35/ppp1.1 ~
Management Logout		Sack Nest

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

SMART/R		SR552	
Device Info	DNS Server Configuration		
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security	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.		
Parental Control Quality of Service Routing DNS	Select DNS Server Interface from available Selected DNS Server Available Interfaces Interface	ble WAN	
DSL DSL Bonding UPnP	ppp0 ^ ppp2.		
DNS Proxy Storage Service Interface Grouping IP Junnel	9. 60		
IPSec Certificate Multicast	~		
Vireless	O Use the following Static DNS IP address	ss:	
liagnostics	Primary DNS server:		
Management Logout	Secondary DNS server:		
	IPv6: Select the configured WAN interface fo static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 that interface.		
	Obtain IPv6 DNS info from a WAN interf WAN interface selected: pppoe 0.0_35/		
	Use the following Static IPv6 DNS addre Primary IPv6 DNS server:	a laboration and	
	Secondary IPv6 DNS server:		
	Tack		

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

- 11. Select the DNS Server Interface from available WAN interfaces.
- 12. 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.

Device Info	WAN Setup - Summary		
Advanced Setup	Make sure that the settings belo	w match the settings pro	vided by your ISP.
Layer2 Interface	mane pare unit die seconds een	in million and sections pro-	
WAN Service	PORT / VPI / VCI:	None	
Ethernet Config	Connection Type:	PPPoE	1
NAT	Service Name:	pppoe_eth4	
Security	Service Category:	UBR	
Parental Control	IP Address:	Automatically Assigned	
Quality of Service	Service State:	Enabled	
Routing	NAT:	Enabled	
DNS	Full Cone NAT:	Disabled	
DSL.	Firewall:	Enabled	·
DSL Bonding UPnP	A CARLEN AND A CAR		
DNS Proxy	IGMP Multicast Proxy:	Disabled	
Storage Service	IGMP Multicast Source Enabled:	222000	
Interface Grouping	MLD Multicast Proxy:	Disabled	
IP Tunnel	MLD Multicast Source Enabled:	Disabled	
IPSec	Quality Of Service:	Disabled	
Certificate			
Multicast	Click "Apply/Save" to have this i modifications.	nterface to be effective.	Click "Back" to make any
Wireless Diagnostics	modificacions.	Back Apply/Save	

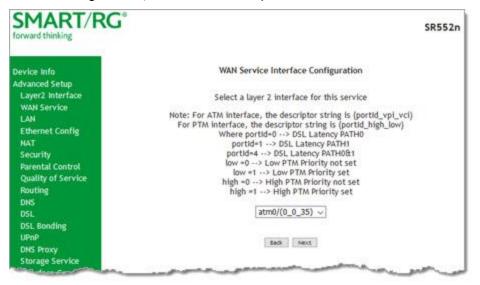
14. Click Next. The summary page appears indicating that your PPPoE WAN setup is complete.

15. 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°	SR552n
Device Info	WAN Service Configuration	
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	Select WAN service type: PPP over Ethernet (PPPoE) P over Ethernet Bridging	
Security Parental Control Quality of Service Routing	Enter Service Description: pppoe_0_0_35	
DNS DSL DSL Bonding UPnP	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.	
DNS Proxy Storage Service Interface Grouping	Enter 802.1P Priority [0-7]: Enter 802.1Q VLAN ID [0-4094]: Select VLAN TPID:	-1 -1 Select a TPID ~
IP Tunnel IPSec Certificate Multicast	Internet Protocol Selection:	
Wireless Diagnostics	Eack Nent	
Management Logout		

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

Field Name	Description
Enter Service Description	(<i>Optional</i>) Enter a name to describe this configuration.
	Options are 0 - 7 . The default is 0 .
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	Options are 0 - 4094 . The default is -1 (disabled).

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

MART/R	SR552/
-	DDb library and Descripted
ice linfo anced Setup	PPP Username and Password
ayer2 interface	PPP usually requires that you have a user name and password to establish your connection. In the
AN Service	boxes below; enter the user name and password that your ISP has provided to you.
AND IN CONTRACTOR	PPP Username: Autourtg Use base MAC address as username
thermet Config AT	PPPoE Service Name:
ounity	Authentication Method: AUTO v
rental Control	
utity of Service	Link Control Protocol
uting S	LCP Keepative Period (s): [30
	LCP Retry Threshold: 1
L Bonding	PPP IP extension
S Proxy rage Service	Advanced DMZ Non DMZ IP
erface Grouping	Address:
Looel	Non DMZ Net Mask: 298.288.2
ec rtificate	Use Static IPve Address
Aticast	
dess	C the first for attend
nostics	Use Static IPv6 Address
gement	Enable IPv6 Unnumbered Model
ut	
	Launch Dhop6c for Address Assignment (IANA)
	Launch Dhopóc for Prefix Delegation (IAPD)
	Retry PPP password on authentication error
	Max PPP authentication retries (1-65536): (H134 (use 65536 to retry forever)
	Enable PPP Debug Mode
	Bridge PPPoE Frames Between WAN and Local Ports
	2 Enable Firewall
	Enable SYN Flood rules
	Enabling the SYN Flood rules can degrade TCP performance.
	and the state of the
	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 SP ALG
	IGMP Multicast
	Enable IGMP Multicast Proxy
	Enable IGNP Multicast Source
	MLD Multicast
	Enable MLD Multicast Provy
	Enable MLD Multicast Source
	MTU size [1370-1492]: [ven
	EOUse Base MAC Address on this WAN interface (Note: only select this for one WAN interface)
	test rest

6. Enter the relevant WAN IP Settings.

Field Name	Description
Obtain an IP address auto- matically	When you wish the ISP to automatically assign the WAN IP to the gateway.
Option 60 Vendor ID	(<i>Optional</i>) 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 iden- tifier 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	Enter the user class ID that should be used to filter traffic.
Option 125	(<i>Optional</i>) Select whether to enable local devices to auto- matically receive DHCP options from the server.
Option 50 Request IP Address	Select to request a specific IP address when sending mes- sages. 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	Use this section to manually declare the static IP information provided by your ISP.
WAN IP Address	If using a static IP address, enter the static WAN IPV4 Address.
WAN Subnet Mask	If using a static IP address, enter the static Subnet Mask.
WAN gateway IP Address	If using a static IP address, enter the static Gateway IP address.
Advanced DMZ	(<i>Optional</i>) Select this option to enable Advanced DMZ on the WAN service. Enter the IP address and net mask to which PPPoE traffic is forwarded.
IPv6 settings section	

Field Name	Description	
The following fields appear when either IPv6 Only or IPv4&IPv6 (Dual Stack) network pro- tocol values is selected on the WAN Service Configuration page.		
Obtain an IPv6 address automatically	Enables the DHCPv6 Client on this WAN interface. Select this option when you want the ISP to automatically assign the WAN IP to the gateway.	
Dhcpv6 Address 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 inform- ation provided by your ISP.	
WAN IPv6 Address/Prefix Length	If entering a static IP address, enter the IP address / prefix length. If you do not specify a prefix length, the default of /64 is used.	
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 following page appears.

SMART/R	G	SR552r
Device Info Advanced Setup	Routing Default Gateway	
Layer2 Interface WAN Service LAN Ethernet Config NAT	default gateways but only on the higest and the last one th	t can have multiple WAN interfaces served as system e will be used according to the priority with the first being he 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 DSL Bonding UPnP	ppp0 ~	ppp2.2 ^ ppp1.1
DNS Proxy Storage Service Interface Grouping IP Tunnel		w.
IPSec Certificate	IPv6: Select a preferred wan	interface as the system default IPv6 gateway.
Multicast Wireless Diagnostics	Selected WAN Interface ppp	oe_0_0_35/ppp1.1 v
Management Logout		Eack Henrit

8. Click the **arrows** to move your selections from left to right or from right to left.

9. Click Next. The following page appears.

SMART/Re	SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing	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 higgest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again. Select DNS Server Interface from available WAN interfaces: Selected DNS Server Available WAN
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service interface Grouping IP Tunnel IPSec Certificate Multicast Wireless Diagnostics Management Logout	Interfaces
	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: [pppe_0_0_35/ppp1.1 v] Use the following Static IPv6 DNS address: Primary IPv6 DNS server: Secondary IPv6 DNS server: Interface interface inte

- 10. Do one of the following to configure the DNS:
 - Select the DNS server interface: Select interface entries and click the arrows to move the entries right or left.
 - Define a static DNS IP address: Click Use the following Static DNS IP address and enter the DNS server IP addresses.
 - Obtain IPv6 DNS info from a WAN interface: In the Obtain IPv6 DNS info from a WAN interface field, select a WAN interface.
 - Define a static IPv6 DNS IP address: Click Use the following Static IPv6 DNS address and enter the DNS server IP addresses.

11. Click Next. The following page appears.

SMART/Re			SR552
Device Info Advanced Setup Layer2 Interface	WAN Setup - Summary Make sure that the settings belo	w match the settings provid	led by your ISP.
WAN Service	PORT / VPI / VCI:	0/0/35	
LAN Ethernet Config	Connection Type:	PPPoE	
NAT	Service Name:	pppoe_0_0_35	
Security	Service Category:	UBR	
Parental Control	IP Address:	Automatically Assigned	
Quality of Service	Service State:	Enabled	
Routing	NAT:	Enabled	
DNS DSL	Full Cone NAT:	Disabled	
DSL Bonding	Firewall:	Enabled	
UPnP	IGMP Multicast Proxy:	Disabled	
DNS Proxy	IGMP Multicast Source Enabled:	Disabled	
Storage Service	MLD Multicast Proxy:	Disabled	
Interface Grouping IP Tunnel	MLD Multicast Source Enabled:	Disabled	
IP lunnet IPSec	Quality Of Service:	Disabled	
Certificate			
Multicast Wireless Diagnostics	Click "Apply/Save" to have this i modifications.	Iterface to be effective. Cli	ick "Back" to make any
Management Logout			

Bridging

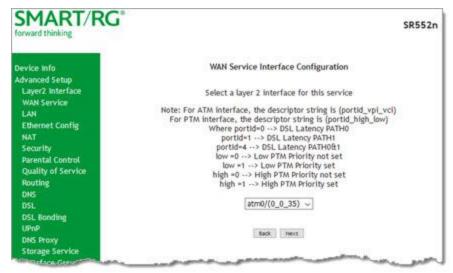
Before you can configure a bridge WAN service, you must create the related ATM interface.

Note: This feature is available for SR515ac models only.





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.

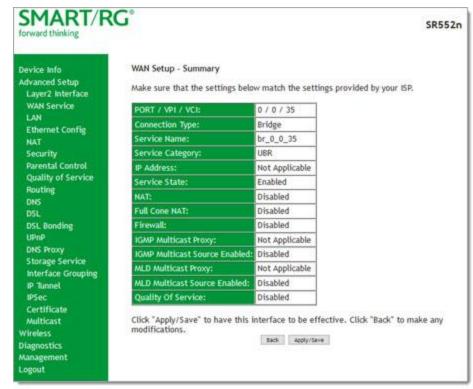
SMART/R	G°	SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel IPSec Certificate Multicast	WAN Service Configuration Select WAN service type: PPP over Ethernet (PPPoE) For ethernet Configuration For agged service, enter valid 802.1P Priority and 80 For untagged service, set -1 to both 802.1P Priority and 1D. Enter 802.1P Priority [0-7]: Enter 802.1Q VLAN ID [0-4094]: Select VLAN TPID:	
Mutocast Wireless Diagnostics Management Logout	Eack Next	

3. Select Bridging. The Multicast Source fields appear.

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





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

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

LAN

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

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

MART/R	6	SR552
evice Info	Local Area Networ	k (LAN) Setup
Ivanced Setup	Configure the Pres	dband Router IP Address and Subnet Mask for LAN interface.
Layer2 Interface WAN Service	GroupName Default	
LAN		192.168.1.1
States and a second	IP Address: Subnet Mask:	295.255.255.0
Pv6 Autoconfig	Subnet Mask:	233.235.235.0
themet Config IAT	Enable IGMP Se	nooping
lecurity		
arental Control		
Juality of Service	Enable LAN sid	le firewall
INS	O Disable DHCP 9	
1999 (March 1997)	Enable DHCP S	
SL.	Start IP Addres	
SL Bonding	End IP Address	Bedrass of the second se
PnP	Leased Time (h	
INS Proxy		List: (A maximum 32 entries can be configured)
torage Service		and for manual of energy on an energy of
nterface Grouping	MAC Address IP A	ddress Remove
P Tunnel		Remove Entries
PSec	ADD DID HIS	Receive Encryes
ertificate	Automatically	create static IP leases for the following OUIs:
Nulticast	OUI Remove	
reless	Statement in the second s	
gnostics	Add OUI R	lenove OUI
nagement		
jout	Configure DHC	P Options:
	Option 66:	(TFTP Server Name)
	10	(Comma-seperated list of TFTP Server IPv4
	Option 150:	Addess(es) (maximum 2 entries))
	Option 43:	(ASCII format) O (Hex format)
	Configure the se	econd IP Address and Subnet Mask for LAN interface
		Apply/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 Inter- face Grouping page).
IP Address	(<i>Optional</i>) Enter the LAN IP address by which LAN devices will connect to this gateway.
Subnet Mask	(<i>Optional</i>) Enter the subnet mask to be used by LAN devices connecting to this gateway.
Enable IGMP Snooping	Click to enable your gateway to listen to IGMP network traffic between hosts and routers. Additional fields appear. By listening to these conversations, the gateway maintains a map of which links need which IP multicast streams.
Standard Mode	(<i>Available when Enable IGMP Snooping is selected</i>) Allows multicast traffic will flood to all bridge ports when there is no client subscribed to any multicast group.
Blocking Mode	(<i>Available when Enable IGMP Snooping is selected</i>) Blocks multicast data traffic, preventing it from flooding to all bridge ports when no client sub-scriptions to a multicast group are present.
Enable IGMP LAN to LAN Multicast	(<i>Available when Enable IGMP Snooping is selected</i>) Allows multicast traffic between LANs. This option is enabled by default.
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 / Disable DHCP Server	Allows the DHCP functionality of your gateway to automatically assign LAN IP addresses to host devices as they connect with the gateway. Fill in the next three fields to configure this action.
Start IP Address	(Available when Enable DHCP Server is selected) Enter the beginning of the class C, IP address range to be assigned by the DHCP server.
End IP Address	(<i>Available 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>Available 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. Click Add Entries. Enter the MAC address and IP address and click Apply/Save. Repeat this step to create

Field Name	Description
	any additional entries that you need.
Automatically create static IP leases from the following OUIs	For LAN hosts, IP addresses can be assigned manually or by using DHCP. Click Add OUI. Enter the OUI and click Apply/Save. Repeat this step to create any additional entries that you need.
Option 66	For some devices that also require access to a TFTP server (device con- figuration name files are in .cnf file format), which enables the device to com- municate with other infrastructure, select this option to specify the name of the TFTP server. Option 66 is an IEEE standard.
Option 150	A Cisco proprietary methodology for pointing to one or two TFTP servers.
Option 43	A Cisco proprietary methodology for providing the Cisco Aironet Wireless Con- troller address to your access point.
Configure the second IP address and subnet mask for LAN interface	When you select this option, the IP Address and Subnet Mask fields appear where you can enter a second IP address and Subnet mask to support a second, simultaneous LAN, i.e., the primary LAN might be defined as 192.168.0.1 and this secondary LAN defined as 192.168.2.1.

IPv6 Autoconfig

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

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

SMART/R	G° SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN IPv6 Autoconfig	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):
Ethernet Config NAT	IPv6 LAN Applications
Security Parental Control Quality of Service Routing DNS DSL	Stateless Stateless Stateless Stateless Stateless End interface ID: Leased Time (hour):
DSL Bonding	Enable RADVD
UPnP DNS Proxy Storage Service Interface Grouping	Enable ULA Prefix Advertisement Randomly Generate Statically Configure Prefix:
IP Tunnel	Preferred Life Time (hour): -1
IPSec Certificate	Valid Life Time (hour): -1
Multicast Wireless	Enable MLD Snooping
Diagnostics Management	 Standard Mode Blocking Mode
Logout	Enable MLD LAN to LAN Multicast: (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)
	Save/Apply

- 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	s section
Enable DHCPv6 Server	This option is selected by default. Click to <i>disable</i> the DHCP v6 feature on the LAN.

Field Name	Description
Stateless	This option is selected by default. Click to stop inheriting IPV6 address assignments from the WAN IPV6 inter- face.
Stateful	Identifies the DHCPv6 server given by the LAN IPV6 network as configured with additional options. Zero com- pression is not supported. Make sure to enter zeros between the colons, that is, do not use shorthand nota- tion (::2). Options are:
	 Start interface ID: Enter the beginning IPv6 available addresses for DHCP to assign to LAN devices. End interface ID: Enter the ending IPv6 available addresses for DHCP to assign to LAN devices. Leased Time (hour): Amount of time before a new IPv6 lease is requested by the LAN client.
Enable RADVD	(<i>Optional</i>) This option is enabled by default. It enables Router Advertisement Daemon (RADVD) service that sends router advertisements to LAN clients. Clear the check box to disable RADVD. Options are:
	• Enable ULA Prefix Advertisement: Check this option to enable unique local address (ULA) 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 Snoop- ing	(<i>Optional</i>) This option is enabled by default. It enables Multicast Listener Discovery (MLD) snooping to manage IPV6 multicast traffic. Options are:
	• Standard Mode: Multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if IGMP snooping is enabled.
	• Blocking Mode: The multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group. This is the default.
Enable MLD LAN to LAN Multicast	(<i>Optional</i>) This option is enabled by default. It enables LAN-to-LAN Multicast until the first WAN service is con- nected. Options are Disable and Enable .

Ethernet Config

On this page, you can set the speed and duplex mode for the Ethernet ports and the WAN port, if configured,

forward thinking					
Device Info		Ethern	et Port Configural	tion	
Advanced Setup					
Layer2 Interface WAN Service	Port	Configure	Current Bit Rate	Duplex Mode	Status
LAN	eth0/LAN4	Auto ~	Auto	Auto	Down
Ethernet Config	eth1/LAN3	Auto ~	Auto	Auto	Down
NAT Security	eth2/LAN2	Auto ~	1000	Full	Up
Parental Control	eth3/LAN1	Auto ~	Auto	Auto	Down
Quality of Service Routing	eth4/WAN	Auto ~	1000	Full	Up
DNS DSL DSL Bonding	* Alwo	ys configure	1000BaseT connect	tions with Auto	o.
UPnP DNS Proxy			Save/Apply		

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

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

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

Note: Always select Auto for 1000 BaseT connections.

3. Click Apply/Save 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 a 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 and then click Add. The following page appears.

Device Info	NAT Virtual Servers	i i i		
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	forward IP packets for End" cannot be modif "External Port End". I Port End" will be set I	e, and enter the server this service to the speci ied directly. Normally, fowever, if you modify to the same value as "In entries that can be con	fied server. NOT it is set to the si "Internal Port St ternal Port Star	E: The "Internal Port ame value as tart", then "Internal
Virtual Servers Port Triggering	Use Interface Service Name:	ipoe_0_0_35/atm0.4	-	
DMZ Host	Select a Service:	Select One		~
Security Parental Control	O Custom Service:			2
Routing				
DNS DSL	External Port Start Ext	Apply/Save	1	itart internal Port End
DNS DSL DSL Bonding	External Port Start Ext	10000	1	Start Internal Port End
DNS DSL DSL Bonding UPnP	External Port StartExt	ernal Port End Protocol	Internal Port S	itarținternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy	External Port StartExt	ernal Port End Protocol	Internal Port S	itart internal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping	External Port Start Ext	ernal Port End Protocol TCP TCP	internal Port S	itartinternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnet	External Port Start Ext	emal Port End Protocol TCP TCP TCP	internal Port S	itartinternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel IPSec	External Port Start Ext	ernal Port End Protocol TCP TCP TCP TCP TCP	Internal Port S	itartinternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping InFinnet IP Tunnet IPSec Certificate	External Port Start Ext	ernal Port End Protocol TCP TCP TCP TCP TCP TCP	internal Port S	itartinternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnet IP Sec Certificate Multicast	External Port Start Ext	ernal Port End Protocol TCP TCP TCP TCP TCP TCP TCP TCP	Internal Port S	itartinternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnet IPSec Certificate Multicast ireless	External Port Start Ext	ernal Port End Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP	Internal Port S	itartinternal Port End
DNS DSL DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnet IPSec Certificate Multicast fireless iagnostics	External Port Start Ext	ernal Port End Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Internal Port S Intern	itartinternal Port End
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel IPSec Certificate	External Port Start Ext	ernal Port End Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Internal Port S Intern	itartinternal Port End

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

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

Field Name	Description
Use Interface	Select the WAN interface to which this NAT rule will apply.
Service Name	Select or enter the service for which you want to forward IP packets. Options are:
	 Select a Service: Select from services defined for your network. The port table at the bottom of the page is updated with the default port ID defined for the service.
	• Custom Service: Enter a new service name to establish a user service type. You must enter the ports and select a protocol in the table at the bottom of the page.
Custom Service	If your application does not appear in the Select a Service list, you can enter a unique name for the application in this field.
Server IP Address	Enter the final octet of the IP address of the LAN client where the service is hosted.
External Port Start External Port End	When you select a service, the external port start and end numbers display auto- matically. Modify them if necessary.
Protocol	Select the protocol to be used with this range of ports. Options are: TCP , UDP , or TCP/UDP . The default is TCP .
Internal Port Start Internal Port End	When you select a service, the internal port start and end numbers display auto- matically. Modify them if necessary.

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/R						SR	552r
Device Info	NAT Port Tri	ggering					
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	others require t applications. Yo existing applica to add it.	that specific p u can configu ation or creati	ames, video con ports in the Rout ore the port setti ing your own (Cu os that can be c	er's firewall be ings from this stom application	opened for a screen by sele on)and click "	ecting an	the
Virtual Servers Port Triggering	Use Interface Application Nan	50°	ipoe_0_0_35/at	tm0.4 v			
DMZ Host Security	Select an application: Custom application:		Select One	~			
Parental Control Quality of Service	Custome	ppication	Save/A	ppky	4		
				and the second se	Open Port	Ope	0
Routing DNS	Trigger Port Start	Trigger Port End		Open Port Start			
DNS DSL	Trigger Port Start	Trigger Port End	TCP V	Open Port Start	End	Proto	
DNS DSL DSL Bonding	Trigger Port Start		Protocol			Proto	col
DNS DSL DSL Bonding UPnP	Trigger Port Start		Protocol TCP ~			Proto TCP	col
DNS DSL DSL Banding UPnP DNS Proxy	Trigger Port Start		Protocol TCP ~ TCP ~			TCP TCP	col V V
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service	Trigger Port Start		Protocol TCP ~ TCP ~ TCP ~			Proto TCP TCP TCP	col V V
DNS DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping	Trigger Port Start		TCP ~ TCP ~ TCP ~ TCP ~ TCP ~			Proto TCP TCP TCP TCP	
DNS DSL DSL Banding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel	Trigger Port Start		TCP ~ TCP ~ TCP ~ TCP ~ TCP ~ TCP ~			Proto TCP TCP TCP TCP TCP	
Straight Market Straight Strai	Trigger Port Start		Protocol TOP ~ TOP ~			Proto TCP TCP TCP TCP 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 Apply/Save to commit your changes.

Field Name	Description	
Use Interface	Select the interface for which the port triggering rule will apply.	
Application Name	Select or enter the application that requires a port trigger. Options are:	
	• Select an Application: Select an available application. The Port and Protocol table is populated with the related values.	
	• Custom Application: Enter a unique name for the application for which you are creating a port trigger entry. You must enter the ports and select a protocol in the table at the bottom of the page.	
Trigger Port Start Trigger Port End	Enter the starting and ending numbers of the range of available outgoing trigger ports. Options are 1 - 65535 .	

Field Name	Description
	Note: You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.
Trigger Protocol	Select the protocol required by the application that will be using the ports in the spe- cified range. Options are TCP , UDP , and TCP/UDP . The default is TCP .
Open Port Start Open Port End	Enter the starting and ending numbers 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 . The default is TCP .

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/R	G	SR552n
Device Info	NAT DMZ Host	
Advanced Setup Layer2 Interface WAN Service	The Broadband Router will forward IP pac belong to any of the applications configu to the DMZ host computer.	
LAN Ethernet Config NAT	Enter the computer's IP address and click host.	k 'Apply' to activate the DMZ
Virtual Servers	Clear the IP address field and click 'Apply	/ to deactivate the DMZ host.
Port Triggering DMZ Host Security	DMZ Host IP Address:	
Parental Control Quality of Service	Save/Apply	
Routing DNS		

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

Security

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

IP Filtering - Outgoing

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

You can define up to 32 outgoing IP filters.

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

SMART/R	G°		SR552n
Device Info Advanced Setup Layer2 Interface WAN Service	Add IP Filter Outgoing The screen allows you to create a filter by specifying a new filter name and at the specified conditions in this filter n	least one cond	ition below. All of
LAN	take effect. Click 'Apply/Save' to save		
Ethernet Config NAT	Filter Name:	[
Security IP Filtering MAC Filtering	IP Version: Protocol: Source IP address[/prefix length]:	IPv4	×
Parental Control Quality of Service Routing	Source Port (port or port:port): Destination IP address[/prefix length]: Destination Port (port or port:port):		
DNS DSL DSL Bonding UPnP	Apply/S	118	

- 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. This is a free-form text field.
	For the filter to be configured and effective for IPV6, the gateway must be installed on a net- work that is either a pure IPV6 network (with that protocol enabled) or is both IPV4 and IPV6 dual protocol enabled/configured. Options are IPv4 and IPv6 . The default is IPv4 . If you select IPV6 , both the Source and Destination IP address must be specified in IPV6 format. The following is an IPV6-compliant, hexadecimal address: 2001:0DB8:AC10:FE01:0000:0000:0001.
Protocol	Select the protocol profile for the filter you are defining. TCP/UDP is most commonly used. The

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

IP Filtering - Incoming

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

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

SMART/R	u	SR552
Device Info	Add IP Filter Incoming	
Advanced Setup Layer2 Interface WAN Service	The screen allows you to create a filter specifying a new filter name and at lea conditions in this filter rule must be sa	st one condition below. All of the specified
LAN Ethernet Config NAT Security IP Filtering	DROP packets. Dropping packets is use	les is to ACCEPT packets meeting the DP checkbox will create a filter that will eful for such purposes as restricting access ition for Virtual Servers will allow access
Outgoing Incoming MAC Filtering	Incoming filters will not restrict access Router itself (HTTP, FTP, Telnet, etc). Management-> Access Control-> Acce	
Parental Control Quality of Service	Click 'Apply/Save' to save and activate	the filter.
Routing	Filter Name:	
DSL	IP Version:	1Pv4 ×
DSL Bonding	Protocol:	~
UPnP	Source IP address[/prefix length]:	
DNS Proxy	Source Port (port or port:port):	
Storage Service	Destination IP address[/prefix length]:	
Interface Grouping	Destination Port (port or port:port):	
IP Tunnel	DROP:	
IPSec Certificate Multicast	WAN Interfaces (Configured in Routin LAN Interfaces Select one or more WAN/LAN interface	ng mode and with firewall enabled) and as displayed below to apply this rule.
Wireless Diagnostics Management	Select All D ipoe_0_0_35/atm0.4 pppoe_0_0_35/ppp2.2 D pppoe_0_0	4☑ pppoe_0_0_35/ppp1.1☑
Logout		
	22	oly/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	A free-form text field. Enter a descriptive name for this filter.
	Select the IP version for this filter. Options are IPv4 and IPv6 . The default is IPv4 .
	Select the protocol to be associated with this incoming filter. Options are: TCP/UDP, TCP, UDP, or ICMP.
Source IP address [/pre- fix length]	Enter the source IP address for rule. For IPv6, enter the prefix as well.

Field Name	Description
Source Port (port or port: port)	Enter source port number or range (xxxxx:yyyyy).
Destination IP address [/prefix length]	Enter the destination IP address for rule. For IPv6, enter the prefix as well.
Destination Port (port or port:port)	Enter destination port number or range (xxxxx:yyyyy).
WAN Interfaces	Click to apply this rule to all WAN interfaces or only certain types. Options are Select All or the types defined for your network.

MAC Filtering

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

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

SMART/R	G° SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security IP Filtering MAC Filtering	MAC Filtering Setup MAC Filtering is only effective on ATM PVCs 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 rules for the new policy.
Parental Control Quality of Service Routing DNS DSL DSL Bonding	Interface Policy Change atm0.3 FORWARD
UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel	Choose Add or Remove to configure MAC filtering rules. Interface Protocol Destination MAC Source MAC Frame Direction Remove
IPSec Certificate 	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.

Add a MAC Filtering Rule

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

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

SMART/R	G°	SR552n
Device Info Advanced Setup Layer2 Interface WAN Service	Add MAC Filter Create a filter to identify the MAC layer frames by one condition below. If multiple conditions are spe	ecified, all of them
LAN Ethernet Config	take effect. Click "Apply" to save and activate the	v filter.
NAT Security	Destination MAC Address:	
IP Filtering MAC Filtering	Frame Direction:	
Parental Control Quality of Service	WAN Interfaces (Configured in Bridge mode only)	
Routing DNS	br_0_0_35/atm0.3 v	
DSL DSL Bonding	Save / Apply	
UPnP DNS Proxy		

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

Field Name	Description
Protocol Type	Select the protocol associated with the device at the destination MAC address. Options are PPPoE , IPv4/IPv6 , AppleTalk , IPX , NetBEUI , and IGMP .
Destination MAC Address	Enter the MAC address of the hardware you wish to associate with this filter.
Source MAC Address	Enter the MAC address of the device that originates requests intended for the device

Field Name	Description	
	associated with the Destination MAC address.	
Frame Direction	Select the incoming/outgoing packet interface. Options are LAN<=>WAN, WAN- N=>LAN, and LAN=>WAN. The default is LAN<=>WAN (both directions).	
WAN Interfaces	Select the WAN interface(s) for which the filter should apply. Only interfaces con- figured for Bridge mode are available.	

Parental Control

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

Time Restriction

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

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



SMART/R		SR552r
Device Info	Access Time Restriction	
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Time Restriction Url Filter Quality of Service Routing DNS	to the Router. The Browse MAC address of the LAN o other LAN device, click th MAC address of the other	ay restriction to a special LAN device connected er's MAC Address' automatically displays the device where the browser is running. To restrict te "Other MAC Address" button and enter the LAN device. To find out the MAC address of a command window and type "ipconfig /all".
DSL	Days of the week	Mon Tue Wed Thu Fri Sat Sun
DSL Bonding	Click to select	
DNS Proxy Storage Service Interface Grouping IP Tunnel IPSec Certificate	Start Blocking Time (hh:mm) End Blocking Time (hh:mm)	apply/Save

- 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. This is a free-form text field.
Browser's MAC Address	The MAC address of the connected device. This option is selected by default.
Other MAC Address	Select this option to restrict access to another device. You can view a list of the connected devices and MAC addresses on the 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 (00:00 - 24:00).

URL Filter

The other side of Parental Controls 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 and then click Add. The following page appears.



- 2. Select whether to exclude or include the URLs in the list you are going to create. If you select Exclude, users cannot access the URLs in the list. If you select Include, users can access the URLs in the list.
- 3. To create the list of URLs, click Add. The following page appears.

SMART/R forward thinking	G°		SR552n
Device Info	Parental Control	URL Filter Add	
Advanced Setup Layer2 Interface WAN Service	Enter the URL addre the entry to the URL	ss and port number then click , filter.	"Apply/Save" to add
LAN Ethernet Config	URL Address:		(Oxfords on ull be
NAT Security	Port Number:	applied if leave blank.	Oefault 80 will be .)
Parental Control Time Restriction Url Filter		Apply/Save	
Quality of Service			

4. Enter the URL address and its corresponding port number. For example, enter http://www.google.com as the URL address



and 80 as the port number. If you leave the Port Number field blank, the default port number of 80 is used.

5. Click Apply/Save to save your changes. You are returned to the Parental Control > URL Filter page

Quality Of Service

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

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

QoS Config

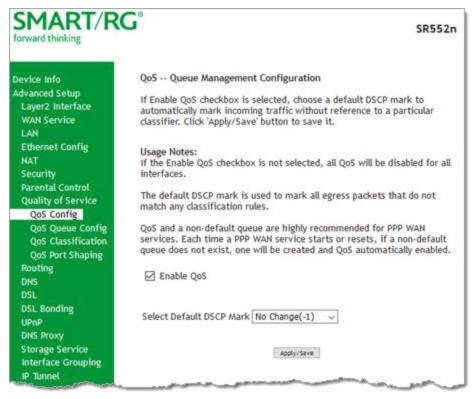
On this page, you can enable QoS and set the DSCP Mark classification.

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

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

Note: Queues for Wireless (e.g., WMM Voice Priority for wl0 interface) are shown only when wireless is enabled. If the WMM Advertise function on the Wireless Basic Setup page is disabled, assigning classifications to wireless traffic has no effect.

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



- 2. If not already selected, click **Enable QoS**.
- (Optional) In the Select Default DSCP Mark field, select the default Differentiated Services Code Point (DSCP) Mark classification value to be used. For a list of supported values, see "Supported DSCP Values".
- Warning: If this option was already enabled and you clear the checkbox, QoS will be disabled for ALL interfaces.
- 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) (for SR515ac models only)
AF11(001010)	AF33(011110)	AF41(100010)	

QoS Queue Config

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

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

SMART/Re	<u> </u>	SR552n
Device Info	QoS Configuration	
Advanced Setup Layer2 Interface WAN Service	This screen allows you to co layer2 interface.	configure a QoS queue and add it to a selected
LAN Ethernet Config NAT		fined for any one interface/precedence pair, three queues per interface.)
Security Parental Control	Enable: Enable:	inable 🗸
Quality of Service QoS Config QoS Queue Config Queue Configuration	Interface:	~
Wlan Queue QoS Classification QoS Port Shaping Routing		1001//Tave

- Fill in the fields, using the information in the table below.
 Note: For Dynamic WAN interfaces, the Queue Priority settings appear twice once for ATM WAN QoS configuration and once for PTM WAN QoS configuration.
- 3. Click Apply/Save to save your settings.

Field Name	Description
	Enter a descriptive name for this configuration. This is a free-form text field.
Enable	Select to enable or disable a given QoS queue configured on the selec-

Field Name	Description
	ted interface.
	Note: Only one queue can be defined for any one interface/precedence pair, resulting in a maximum of three queues per interface.
Interface	Select the Layer 2 interface to be associated with the defined QoS queue, e.g., eth0 or eth4.
Queue Precedence	(<i>Appears when you select an interface</i>) Select the priority value to be associated with QoS queue defined. Options include levels for SP and SP WRR WFQ .
	Note: Lower value = higher priority.
Scheduler Algorithm	(<i>Appears when you select SP</i> /WRR/WFQ in the Queue Precedence field) Select an algorithm for data priority in queues. Options are:
	• Strict Priority: Allows shaping of rate and burst size for packets in queue.
	• 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 queuing weighting scheme via allowing different sessions to have different service shares for improved data packets flow in networks with variable packet size, e.g., PTM/IP networks.
	appear only when the Queue Precedence field is set to SP WRR WFQ and m field is set to Strict Priority . These options are do not appear in the
Minimum Rate	Enter the minimum shaping rate for packets in QoS queues. Options are 1 - 100000 Kbps.
	To specify no minimum shaping, enter -1 .
Shaping Rate	Enter the shaping rate for packets in QoS queues. Options are 1 - 100000 Kbps.
	To specify no minimum shaping, enter -1 .
Shaping Burst Size	Enter the shaping burst size to be applied to packets in the defined queue. Options are 1600 bytes or greater.

WLAN Queue

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

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

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

Device info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT	QoS Wlan Queue Setup Usage Note: Wireless queues and classifications have no effect if WMM Advertise is disabled. The WMM Advertise function is located on the Wireless Basic Setup page.					
Security Parental Control	Name	Кеу	Interface	Qid	Prec/Alg/Wght	Enable
Quality of Service	WMM Voice Priority	1	wito	8	1/SP	Enabled
QoS Config QoS Queue Config	WMM Voice Priority	2	wło	7	2/SP	Enabled
Queue Configuration	WMM Video Priority	3	wło	6	3/SP	Enabled
Wlan Queue	WMM Video Priority	4	wło	5	4/SP	Enabled
QoS Classification QoS Port Shaping	WMM Best Effort	5	wło	4	5/SP	Enabled
Routing	WMM Background	6	wło	3	6/SP	Enabled
DSL	WMM Background	7	wło	2	7/SP	Enabled
DSL Bonding	WMM Best Effort	8	wio	1	8/SP	Enabled

QoS Classification

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

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

SMART/RO		SR552
Device Info	Add Network Traffic Class Rule	
Advanced Setup Layer2 Interface WAN Service	This screen creates a traffic class rule to classify queue and optionally mark the DSCP or Ethernet p Click 'Apply/Save' to save and activate the rule.	
LAN	Traffic Class Name:	
Ethernet Config	Rule Order:	Last v
NAT	Rule Status:	Enable V
Security		
Parental Control Quality of Service	Specify Classification Criteria (A blank criterion classification.)	indicates it is not used for
QoS Config	Ingress Interface:	LAN
QoS Queue Config	Ether Type:	
QoS Classification	Source MAC Address:	· · · · · · · · · · · · · · · · · · ·
QoS Port Shaping	Source MAC Mask:	
Routing	Destination MAC Address:	
DNS	Destination MAC Mask:	
DSL	Descination mask.	
DSL Bonding	Specify Classification Results (A blank value indi	cates no operation.)
UPnP	Secult Secure Interferenden der	
DNS Proxy	Specify Egress Interface (Required):	~
Storage Service	Specify Egress Queue (Required):	× ×
Interface Grouping	 Packets classified into a queue that exit through is not specified to exist, will instead egress to the 	
IPSec	Mark Differentiated Service Code Point (DSCP):	
Certificate		· · · · · · · · · · · · · · · · · · ·
Multicast	Mark 802.1p priority:	~
Wireless	- Class non-vlan packets egress to a non-vlan inte	rface will be tagged with VID 0
	and the class rule p-bits.	
Diagnostics	- Class vlan packets egress to a non-vlan interface	
Management	marked by the class rule p-bits. No additional vlan - Class non-vlan packets egress to a vlan interface	
Logout	VID and the class rule p-bits.	e will be tagged with the interface
	 Class vian packets egress to a vian interface will packet VID, and the class rule p-bits. 	be additionally tagged with the
	20.127.5.3272.5	
	Set Rate Limit:	[Kbits/s]
		1990 A. 1992 A. 2012 A. 2012
	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
Traffic Class Name	Enter a descriptive name for this rule. This is a free-form text field.
Rule Order	This option is set to Last and cannot be changed. Every rule is set as the very last classification rule to be processed.
Rule Status	Select whether this rule is active or inactive. Options are: Enable and Disable . The default is Enable .

Field Name	Description
Specify Classification Crite	eria section
Ingress Interface	Select an interface. Options are LAN, WAN and any interface already con- figured 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.
Source MAC Address Source MAC Mask	(Available for LAN, ATM, ETH, PPP-Routed and wireless interfaces only) Enter the source MAC address and source MAC mask for this classification.
Destination MAC Address Destination MAC Mask	(<i>Available for LAN, ETH and wireless interfaces only</i>) Enter the destination MAC address and destination MAC mask for this classification.
or Vendor Class ID or	(Available for WAN, ATM and PPP-Routed interfaces only) Select the source for this classification. Options are:
User Class ID	 Source IP Address[/Mask]: Enter the source IP address and source IP mask.
	• Vendor Class ID (DHCP Option 60): Enter the vendor class ID.
	• User Class ID (DHCP Option 77): Enter the user class ID.
Destination IP Address [/ Mask]	(Available for WAN and ATM interfaces only) Enter the destination IP address and source IP mask for this classification.
IP Length Check (Min/Max)	(<i>Available for Local, ATM interfaces only</i>) Enter the minimum and maximum number of digits required for IP addresses.
Differentiated Service Code Point (DSCP) Check	(<i>Available for WAN, Local, ATM, and PPP-Routed interfaces only</i>) Select the DSCP check protocol. Options include default and a range of protocol IDs.
Protocol	(Available for WAN, Local, and ATM interfaces only)Select the protocol spe- cified for this classification. Options are TCP , UDP , ICMP , and IGMP .
UDP/TCP Source Port	(<i>Appears when TCP or UDP is selected in the Protocol field</i>) Enter the source port to be used for this classification. You can enter a range (port:port) or a single port.
UDP/TCP Destination Port	(<i>Appears when TCP or UDP is selected in the Protocol field</i>) Enter the des- tination port to be used for this classification. You can enter a range (port:- port) or a single port.
Specify Classification Res	ults section
Egress Interface	Select the egress interface for this rule. Options are the interfaces already configured.
Egress Queue	Select the egress queue for this rule. Options are the queues already con- figured.

Field Name	Description		
	Note: Make sure to select a queue that is defined for the interface that you selected. If you select a queue that is not defined for the selected interface, any packets classified into that queue are processed by the default queue for the interface.		
Mark Applied Dif- ferentiated Service Code Point	Select the desired DSCP code.		
Mark 802.1P priority	(<i>Available for LAN, bridged and wireless interfaces only</i>) This value is inserted into the Ethernet frame and used to differentiate traffic. Lower values assign higher priorities. Options are: 0 - 7 .		
Set Rate Limit	Enter the data traffic rate limit applied for this classification.		





QoS Port Shaping

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

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

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

vice Info ivanced Setup Layer2 Interface WAN Service LAN	QoS Port Shaping Setup QoS Port Shaping supports traffic rate limiting on the Ethernet interfaces. If "Egress Shaping Rate" is set to "-1", shaping will be disabled and "Egress Burst Size" will be ignored. If "Ingress Policing Rate" is set to "-1", policing wil be disabled.			
Ethernet Config NAT	Interface	Egress Shaping Rate (Kbps)	Egress Burst Size (bytes)	Ingress Policing Rate (Kbps)
Security Parental Control	eth4/WAN	4	0	4
Quality of Service	eth3/LAN1	a	0	.1
QoS Config QoS Queue Config	eth2/LAN2	in .	0	[-t
QoS Classification	eth1/LAN3	a	0	[4
QoS Port Shaping	eth0/LAN4	.π	0	a

- 2. (Optional) For each interface in the table, enter an Egress Shaping Rate (in Kbps), an Egress Burst Size (in bytes), and an Ingress Policing Rate (in Kbps). The default settings work for most scenarios.
- 3. Click Apply/Save to commit your changes.

Routing

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

Default Gateway

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

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

SMART/R	G°	SR552n
Device Info Advanced Setup Layer2 Interface		t can have multiple WAN interfaces served as system
WAN Service LAN Ethernet Config NAT Security	being the highest and the las	e will be used according to the priority with the first it one the lowest priority if the WAN interface is be changed by removing all and adding them back in
Parental Control Quality of Service	Selected Default Gateway Interfaces	Available Routed WAN Interfaces
Routing Default Gateway Static Route Policy Routing RIP	ppp0	atm0.4 A ppp1.1 ppp2.2
DNS DSL DSL Bonding UPnP	~	~
DNS Proxy Storage Service Interface Grouping IP Tunnel	Select a preferred wan interf	ace as the system default IPv6 gateway.
IP Junnet IPSec Certificate Multicast	Selected WAN Interface ppp	oe_0_0_35/ppp1.1 v
Wireless 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. You must configure the IPv6 interface before it appears in this field.
- 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	6	SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN	Routing Static Route Add Enter the destination network address, subnet mask, gateway A WAN interface then click "Apply/Save" to add the entry to the ro	
LAN Ethernet Config NAT Security Parental Control Quality of Service Routing Default Gateway Static Route Policy Routing RIP DNS	IP Version: Destination IP address/prefix length: Interface: Gateway IP Address: (optional: metric number should be greater than or equal to zero Metric: 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
	Select the IP version associated with the static route you wish to create. Options are: IPv4 and IPv6. The default is IPv4.
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.
	Enter the destination IP address for this route. If needed, include the /prefix length.
	(<i>Optional</i>) Establishes traffic priority/weighting. Must be equal to or greater than zero (≥ 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/R	G SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN	Policy Routing Settup Enter the policy name, policies, and WAN interface then click "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.
Ethernet Config	Policy Name:
NAT Security Parental Control Quality of Service	Physical LAN Port: ~
Routing Default Gateway	Source IP:
Static Route Policy Routing RIP	Use Interface poe_0_0_35/atm0.4 ~ Default Gateway IP:
DNS	
DSL. DSL Bonding UPnP	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
Policy Name	Enter a descriptive name for this entry to the policy routing table. This is a free-form text field.
Physical LAN Port	Select a physical LAN interface for the policy route. Options include LAN1-4 and Wireless.
Source IP	Enter the IP address for the source of this policy route.
Use Interface	Select the WAN Interface for this policy route
Default Gateway IP	Enter the IP address of the default gateway.

RIP (Routing Information Protocol)

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

On this page, you can configure the RIP settings.

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

SMART/R	G [°] SR552n
Device Info	Routing RIP Configuration
Advanced Setup Layer2 Interface WAN Service	NOTE: If selected interface has NAT enabled, only Passive mode is allowed.
LAN Ethernet Config NAT Security	To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.
Parental Control Quality of Service Routing Default Gateway Static Route	Interface Version Operation Enabled atm0.4 2 V Passive V
Policy Routing RIP	Apply/Save

- 2. For the interface that you want to modify, select values using the information in the table below.
- 3. To enable a configuration, click the **Enabled** checkbox next to the interface.
- 4. 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. Options are: 1, 2, and Both. The default is 2.
	For detailed information on RIP versions, refer to RFC 1058 and RFC 1453.
Operation	This option is set to Passive and cannot be changed. This mode listens only. It does not advert- ise routes.

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.

SMART/RO	u	SR55
Device Info	DNS Server Configuration	
Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control	server IP addresses for the or static IPOE protocol is co entered. DNS Server Interfaces can servers but only one will be higest and the last one the	e from available WAN interfaces OR enter static DNS system. In ATM mode, if only a single PVC with IPoA infigured, Static DNS server IP addresses must be have multiple WAN interfaces served as system dns used according to the priority with the first being t lowest priority if the WAN interface is connected. ed by removing all and adding them back in again.
Quality of Service Routing	Select DNS Server In	terface from available WAN interfaces:
DNS DNS Server	Selected DNS Server Interfaces	Available WAN Interfaces
Dynamic DNS Static DNS DSL DSL Bonding UPnP	ppp0	
DNS Proxy Storage Service Interface Grouping IP Tunnel		
IPSec	O Use the following Sta	tic DNS IP address:
Certificate Multicast	Primary DNS server:	
Wireless	Secondary DNS server:	
Diagnostics		
Management Logout	enter the static IPv6 DNS s	interface for the IPv6 DNS server will enable the
	Obtain IPv6 DNS info	from a WAN interface:
	WAN Interface selected:	pppoe_0_0_35/ppp1.1 ~
	O Use the following Stat	the IDue ONE address
	Primary IPv6 DNS server:	IN ITTO UND BUBIESS.
	Secondary IPv6 DNS server	3
	20210000000000000000000000000000000000	

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

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

Field Name	Description
Selected DNS Server Interfaces	WAN service(s) selected to be your primary DNS server.
Available WAN Interfaces	WAN services available to be selected for the DNS server.

Field Name	Description
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	Enter the IP address of the secondary DNS server.
WAN Interface Selected	Select the WAN interface for the IPv6 server. field. If no WAN inter- face is configured for your gateway, this field is disabled.
Primary IPv6 DNS Server	Enter the IP address of the primary IPv6 primary DNS.
Secondary IPv6 DNS Server	Enter the IP address of the primary IPv6 primary DNS.

Dynamic DNS

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

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

SMART/R	G	SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN	Add Dynamic DNS This page allows you no-ip.com.	to add a Dynamic DNS address from DynDNS.org, TZO, or
LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DNS Server Dynamic DNS Static DNS	D-DNS provider Hostname Interface DynDNS Settings Username Password	DynDNS.org ~
DSL DSL Bonding UPnP DNS Proxy Storage Service Interface Grouping		Apply/fave

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

Field Name	Description
D-DNS provider	Select a dynamic Domain Name Server provider. The default is DynDNS.org .

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

Static DNS

The Static DNS service allows you to resolve DNS queries on the Broadband Router by adding a static host name to the IP Address mappings.

On this page, you can configure up to 10 static DNS entries.

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

SMART/R	G°	SR552n
Device Info	Static DNS Entry	
Advanced Setup Layer2 Interface WAN Service	Enter the Host Name and IP addre	ess then click "Apply/Save" .
LAN Ethernet Config NAT	Host Name: IP Address:	
Security Parental Control Quality of Service	Apply/5	ave
Routing	مندستم _ محمد م	

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

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



DSL

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

Warning: 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/R	G°	SR552n
Device Info	DSL Settings	
Advanced Setup Layer2 Interface WAN Service	Select the modulation below.	Select the profile below.
LAN	G.Dmt Enabled	🗹 8a Enabled
Ethernet Config	G,lite Enabled	8b Enabled
NAT Security	T1.413 Enabled	8c Enabled
Parental Control	ADSL2 Enabled	☑ 8d Enabled
Quality of Service	Annexi, Enabled	12a Enabled
Routing DNS		
DSL	ADSL2+ Enabled	12b Enabled
DSL Bonding	AnnexM Enabled	🗹 17a Enabled
UPnP	VDSL2 Enabled	
DNS Proxy		
Storage Service Interface Grouping		USO
IP Tunnel		Enabled
IPSec	Colored the observations and bolis	
Certificate	Select the phone line pair below Inner pair	×-
Multicast Wireless		
Diagnostics	O Outer pair	
Management	Capability	
Logout	Bitswap Enable	
	SRA Enable	
	PhyR Enable	
	ADSL PTM Mode Enabl	
	Stinger® Mode Enable	
	Inventory Management	
	Use board serial for E	OC Serial Number
	Apply/Save	Advanced Settings

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

- 3. To configure advanced settings, see "Advanced settings".
- 4. Click Apply/Save to commit your changes.

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

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

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

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

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

Other Settings	Dther Settings			
Field Name	Description			
Inner Pair/Outer Pair	The RJ11 connector has four contacts. The center pair of pins is DSL1. The outer pair pins are the contacts for DSL2. Select which pair should be used.			
Capability	 Bitswap Enable: Enables adaptive handshaking functionality. SRA Enable: Enables Seamless Rate Adaptation. PhyR Enable: Enables Physical Layer Retransmission. ADSL PTM Mode Enable: Enables Asymmetric Digital Subscriber Line in Packet Transfer Mode. Stinger® Mode Enable: (Available for SR515ac models only) Enables communication with Stinger type equipment. 			
Inventory Man- agement	Select whether to use the gateway serial number as the EOC serial number in your inventory management data- base.			

Advanced settings

Note: This option is not available for the SR515ac model.

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

SMART/R	RG°		
Device Info	DSL Advanced Settings		
Advanced Setup Layer2 Interface	Select the test mode below.		
WAN Service	Normal		
4G LTE Settings Ethernet Config	OReverb		
LAN	OMedley		
NAT	O No retrain		
Security Parental Control Quality of Service	ОЦ		
Routing		Apply	Tane Selection
DNS DSL	5 20 5 5 10		

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

	19911		-			U	pstrea	m Ton	95			an sec	-	1965	
0	1	⊠2	⊠3	₫4	125	126	☑7	⊠8	129	10	11	12	☑13	14	15
16	17	18	19	20	21	22	1 23	24	25	26	27	28	29	☑ 30	☑ 31
1.00		100000	1.418.14	-		Do	wnstre	am To	nes			10.000		and the state	
32	☑ 33	☑ 34	35	☑ 36	☑ 37	☑ 38	239	☑ 40	Ø41	₫ 42	☑ 43	44	☑ 45	☑ 46	247
48	249	1 50	₫51	1 52	☑ 53	₫ 54	₫ 55	₫ 56	₫ 57	₫ 58	☑ 59	160	1 61	162	☑ 63
64	1 65	1 66	67	1 68	269	70	1 1	172	₫73	1 74	₽75	76	177	78	79
80	281	82	83	284	85	88	87	88	289	Ø 90	291	192	193	294	295
296	297	298	299	100	101	102	103	104	105	106	107	108	109	110	11
112	113	114	1115	116	117	118	119	120	121	122	123	124	M 125	126	12
	00000000		131					100		1.			200 A CV	6 C C C C C	1000
			147												
			163					1000							
			179												
	1.1.1.1.1.1.4.6	0.000	195												
			211						1000						
			227												
														1000	
₩ 240	241	244	243	₩ 244	₩ 243	246	24/	M 248	249	250	251	₩ 252	₩253	2254	1222

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.

DSL Bonding

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

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

SMART/R	G° SR552n
Device Info	xDSL Bonding Capability Configuration
Advanced Setup Layer2 Interface	Any Changes will require a reboot.
WAN Service	Bonding/Non-bonding modes - Auto controlled from within the system.
LAN Ethernet Config	For any kind of xDSL bonding capability in the modern now or in the future,
NAT	Please keep this configuration enabled.
Parental Control Quality of Service	☑ xDSL Bonding Capability
Routing DNS DSL	Current WAN XDSL Mode: Von Bildided
DSL Bonding	an version second.
DNS Proxy	

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



UPnP

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

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

SMART/R	SR552n
Device Info	UPnP Configuration
Advanced Setup Layer2 Interface WAN Service LAN	NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.
Ethernet Config	Enable UPnP
Security Parental Control Quality of Service	Apply/Save
Routing	

- 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/R	G°	SR552r
Device Info	DNS Proxy Configuration	
Advanced Setup		
Layer2 Interface WAN Service	Enable DNS Proxy	
LAN	Host name of the Broadband Router:	ClearView
Ethernet Config NAT	Domain name of the LAN network:	Kome
Security		
Parental Control	Apply/Save	
Quality of Service		
Routing		and the second s

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

Storage Service

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

Storage Device Info

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

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

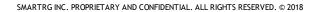


User Accounts

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

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





2. To add a new account:

a. Click Add. the following page appears.

SMART/F	RG°	SR552n
Device info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS	Storage User Account Setup In the boxes below, enter the user name, name on which the home directory is to t Username: Password: Confirm Password: volumeName:	
DSL DSL Bonding UPnP DNS Proxy Storage Service	Apply/Save	

- b. Enter a user name and enter the password twice. The password cannot contain spaces.
- c. (Optional) In the Volume Name field, enter a volume name where the home directory should be created.
- d. Click Apply/Save to save your settings. You are returned to the User Accounts page.
- 3. To remove a user account, click the **Remove** checkbox next to the account entry and then click the **Remove** button. The list refreshes to show your changes were applied.



Interface Grouping

On this page, you can create an interface group to map local interfaces to WAN interfaces. A typical application for this feature is assigning IPTV set-top boxes to a WAN interface.

1. In the left navigation bar, click Advanced Setup > Interface Grouping and then click Add. The following page appears. (The instructions that display at the top of this page are not shown below.)



MART/RO	0	SR552r
evice Info	Interface grouping Configuration	
Ivanced Setup Layer2 Interface WAN Service	To create a new interface group: 1. Enter the Group name and the group name m (dynamic) or 3. (static) below:	ust be unique and select either 2.
LAN Ethernet Config NAT Security	 If you like to automatically add LAN clients to DHCP vendor ID string. By configuring a DHCP wi the specified vendor ID (DHCP option 60) will be server. 	endor ID string any DHCP client request with
Varental Control Quality of Service Jouting INS	 Select interfaces from the available interface using the arrow buttons to create the required n clients may obtain public IP addresses 	
ISL ISL Bonding	 If this interface is to share the WAN interface otherwise the WAN interface you select will be re- 	
IPnP INS Proxy	5. Click Apply/Save button to make the changes	effective immediately
torage Service nterface Grouping	IMPORTANT If a vendor ID is configured for a client device attached to the modem to allow	
P Tunnel PSec	Group Name:	
ertificate witicast	Shared WAN Interface:	
eless gnostics	Grouped WAN Interfaces	Available WAN Interfaces
nagement jourt	•	br_0_0_35/atm0.3 poe_0_0_35/atm0.4 pppoe_0_0_35/ppp1.1 pppoe_0_0_35/ppp2.2 pppoe_0_0_1/pp0 No Interface/None
	-	
	Grouped LAN Interfaces	Available LAN Interfaces
	*	LAN4 LAN3 LAN2 LAN1 Wireless Guest[wi0.1 Wireless Guest]wi0.2 Wireless Guest]wi0.3
	Automatically Add Clients With the following DHCP Vendor IDs	9
ne	per pe	and her
	Marian Ann	
and the second		

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.
 - b. Add it to the **Grouped Interface** list by clicking the arrow to create the required mapping of the ports. Hold down the Shift key to select multiple interfaces.
 - Note: Depending on the WAN interface configuration, these clients may obtain public IP addresses.
- To automatically add LAN clients (such as set-top boxes) to a WAN Interface in the new group, enter the DHCP vendor ID string. You can add up to 16 vendor IDs.
 When you configure a DHCP vendor ID string, any DHCP client request that includes this vendor ID is denied an IP address from the local DHCP server (DHCP option 60).
- 6. Click Apply/Save. Your changes take effect immediately.
- 7. To remove a grouping, select the grouping and click **Remove**. You can only remove groupings that you create.

IP Tunnel

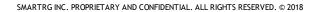
IP Tunneling is typically used as a means to establish a path between two independent networks. Your SmartRG gateway supports connecting islands of IPv6 networks across the IPv4 internet or IPv4 in IPv6 as well.

In this section, you can configure IP tunnel settings.

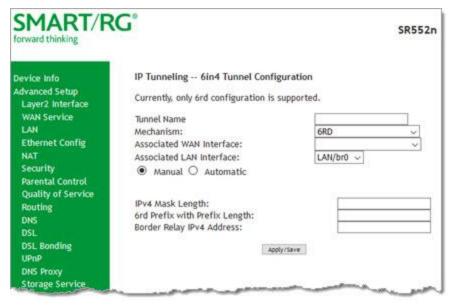
Note: For IPv6inIPv4, only 6rd configuration is supported. For IPv4inIPv6, only DS-Lite configuration is supported.

IPv6inIPv4

On this page, you can configure the IPv6inIP4 settings.



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



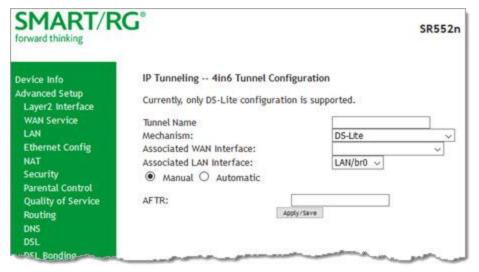
- 2. Enter a Tunnel Name.
- 3. Select the WAN and LAN interfaces associated with the tunnel you wish to establish.
- 4. The Manual button is selected by default. Enter appropriate values in the IPv4 Mask Length, 6rd Prefix with Prefix Length and Border Relay IPv4 Address fields. To configure these settings automatically, select Automatic under Associated LAN Interface.
- 5. Click Apply/Save to commit your changes.

IPv4inIPv6

On this page, you can configure the IPv4inIP6 settings.



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



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

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



IPSec

Internet Protocol Security is a protocol for securing communications by packet level encryption and authentication. On this page, you can create, enable, edit and remove connections. A maximum of 40 IPSec connections is allowed.

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

SMART/RG	6				SR552n	
Device Info	IPSec Settings					
Advanced Setup Layer2 Interface	IPSec Connection Name		new connection	NAT Traversal		
WAN Service LAN	IP Version:		IPv4 ~			
Ethernet Config NAT	Tunnel Mode		ESP ~			
Security Parental Control	WAN Interface:		Select inter	face 🗸		
Quality of Service Routing	Remote Security Gatewa	iy.	0.0.0.0	Anonymous		
DNS DSL DSL Bonding UPnP	LAN-side VPN IP Address Mask or Prefix Length		Subnet 0.0.0.0 255.255.255.0	~		
DNS Proxy Storage Service Interface Grouping	Local ID Type		Default ~	ID Content		
IP Tunnel IPv6in IPv4	Remote-side VPN	0.0.0.0	Subnet	~		
IPv4inIPv6	Mask or Prefix Length	255.255	255.0			
IPSec Certificate	Remote ID Type	haveragen	Default 🗸	ID Content		
Multicast Wireless	Key Exchange Method		Auto (IKE)	~		
Diagnostics	Authentication Method		Pre-Shared	Key 🗸		
Management Logout	Pre-Shared Key		key			
	Perfect Forward Secrecy		Disable ~			
	Advanced IKE Settings		Show Advance	ed Settings		
			Apply/Sav	•		

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

Field Name	Description	
IPSec Connection Name	A free form text field. Enter a descriptive name for this connection	
NAT Traversal	Click to enable the NAT traversal protocol.	
IP Version	Select the IP version environment associated with your infrastructure. Options are IPv4 and IPv6 . The default is IPv4 .	
Tunnel Mode	Select the encapsulation method to be used. Options are:	
	• AH: Use this mode to encapsulate a packet with AH and IP headers. For authen- tication, the entire packet is signed.	
	• ESP: Use this mode to encapsulate a packet with ESP and IP headers. An ESP trailer is added to the packet for authentication and integrity. This is the default.	
WAN Interface	Select the WAN connection for this tunnel.	
Remote Security Gateway	Enter the WAN IP for this tunnel.	
Anonymous	Click to enable anonymity protection on this connection.	
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. Enter the IP address and mask or prefix length for the VPN. This is the default.	
	• Single Address: Allows access to a single host. Enter the IP address for the host.	
IP Address	Enter the IP address for local access.	
Mask or Prefix Length	Enter the subnet mask or prefix length for IP address entered for local access, e.g., 255.255.255.0.	
Local ID Type	Select the type of ID for the local VPN. Options are Default , Domain , and E-Mail . The default is Default . When you select Domain or E-Mail , the ID Content field becomes available. Enter the ID.	
Remote-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. Enter up to three IP addresses and masks or prefix lengths for the VPN. This is the default.	
	• Single Address: Allows access to a single host. Enter the IP address for the host.	
IP Address	Enter the IP address for remote access.	
Mask or Prefix Length	Enter the subnet mask or prefix length for IP address entered for remote access, e.g., 255.255.255.0.	
Remote ID Type	Select the type of ID for the remote VPN. Options are Default , Domain , and E-Mail . The default is Default . When you select Domain or E-Mail , the ID Content field becomes	

Field Name	Description
	available. Enter the ID.
Key Exchange Method	 The key-exchange method to be used for IPSec. Options are: Auto(IKE): This method uses the negotiated key-exchange method for IPSec. This is the default and recommended for best results. Manual: This method requires that you configure the details.
Authentication Method	 Select the method by which the remote end will authenticate. Pre-Shared Key: A key is distributed to authorized users for logging into the system. Enter the key in the Pre-shared Key field. Certificate (x.509): A certificate is used for authentication. Select the certificate file in the Certificate field that appears.
Perfect forwarding Secrecy	 This setting determines whether a session key derived from a set of long-term keys is compromised if one of the long-term keys in the set is compromised. Enable: Prevents long-term key from being compromised.
	 Disable: Permits long-term keys to be compromised. Note: For SR515ac models, this field is named Perfect Forward Secrecy.

Advanced IKE Settings

You can configure advanced IKE settings if desired.



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

Field Name	Description
Mode	(<i>Appears in the Phase 1 section only</i>) Select whether to protect information about your network. Options are:
	• Main: Protect the identity of the peers. This is the default.
	• Aggressive: Do not protect the identity of the peers.
Encryption Algorithm	Select the encryption algorithm. Options are 3DES , AES -128 , AES-192 , and AES-256 . The default is 3DES .
Integrity Algorithm	Select the integrity algorithm. Options are MD5 and SHA1 . The default is MD5 .
Select Diffie-Hellman Group for Key Exchange	Select the D-H group. Options are 768bit - 8192bit . The default is 1024bit .
Key Life Time	Enter the number of seconds that a key is valid. The default is 3600 seconds.

3. Click Apply/Save to commit your changes.

Certificate

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

Local

Local certificates are used to identify the gateway to other users.

On this page, you can create a new certificate request locally and have it signed by a certificate authority, or you can import an existing certificate.

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

SMART/RC	Ĵ		SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT		e signing request you need	I to include Common Name, e 2-letter Country Code for
Security Parental Control Quality of Service Routing	State/Province Name: Country/Region Name:	US (United States)	×
DNS DSL DSL Bonding UPnP		400Vy	

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

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



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

SMART/F	RG°		SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service	Import certificate Enter certificate na Certificate Name:	ame, paste certificate content and private key.	
Routing DNS DSL DSL Ronding UPnP DNS Proxy Storage Service Interface Grouping IP Tunnel IPSec Certificate	Certificate:	BEGIN RSA FRIVATE KEY <insert here="" key="" private=""> EN RSA FRIVATE KEY</insert>	A
Local Trusted CA Multicast Wireless Diagnostics Management Logout	Private Key:		
		400ly	

- 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/RG		SR552r
Device Info Advanced Setup Layer2 Interface WAN Service LAN Ethernet Config NAT Security Parental Control Quality of Service Routing DNS DSL DSL Bonding UPNP DNS Proxy Storage Service Interface Grouping	Import CA certificate Enter certificate name and paste certificate content. Certificate Name:BEGIN CERTIFICATE <insert certificate="" here="">END CERTIFICATE Certificate:</insert>	
IP Tunnel IPSec Certificate Local Trusted CA Multicast		2
Wireless	Appky	

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

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

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/RC	G*					SR552n
Device Info Advanced Setup Layer2 Interface WAN Service LAN			Deable \sim lower value, higher priority Deable \sim			
Ethernet Config	ICHD Configuration					
NAT	IGMP Configuration					
Security Parental Control	Enter IGMP protocol configu	ration fie	elds if you w	ant modif	y default values shown below.	
Quality of Service	Default Version:	6	3			
Routing	Query Interval:		25			
DNS	Query Response Interval:		10			
DSL	Last Member Query Interval		10			
DSL Bonding	Robustness Value:		1			
UPnP	Maximum Multicast Groups: Maximum Multicast Data So	errors -		- 97		
DNS Proxy	(for IGMPv3):	L. Carlo	10		1	
Storage Service	Maximum Multicast Group	6	:5		1	
Interface Grouping	Members: Fast Leave Enable:		2		A. C.	
IP Tunnel	Past Leave Enable:		2			
PSec	IGMP Group Exception List	8				
Certificate Multicast	Group Address	Mask/M	lask bits	Remove		
Vireless	224.0.0.0	255.25	5.255.0			
lagnostics	239.255.255.250	255.255	.255.255			
anagement						
ogout	224.0.255.135	255.255	255.255.255			
				ASE		
	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value: Maximum Multicast Groups: Maximum Multicast Data Sources (for mldv2): Maximum Multicast Group		t) configuration fields if y		you want modify default values shown	below.
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group	urces	1p		1	
	Maximum Multicast Data So (for mldv2):	urces	1p		1	
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group Members:	urces	10		1	
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group Members: Fast Leave Enable:	urces	10	5	Remove	
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group Members: Fast Leave Enable: MLD Group Exception List	Nurces	10 72	5	Remové	
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group Members: Fast Leave Enable: MLD Group Exception List Group Address	Nurces	io 10 21 esk/Mask bit	ts	Remové	
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group Members: Fast Leave Enable: MLD Group Exception List Group Address ff01::0000 ff02::0000	Ma	io D sk/Mask bit ffff::0000			
	Maximum Multicast Data So (for mldv2): Maximum Multicast Group Members: Fast Leave Enable: MLD Group Exception List Group Address ff01::0000 ff02::0000	Ma	to ISK / Mask bit ffff::0000 ffff::0000			

- 2. Modify the fields as needed, using the information in the table below. The same fields are provided for both IGMP and MLD configuration.
- 3. 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:			
	• Enable: IGMP packets are prioritized using the multicast precedence value. The lower the multicast precedence value, the higher that IGMP packets will be placed in the queue.			
	• Disable: IGMP packets are not prioritized. This is the default.			
Multicast Strict Grouping Enforcement IGMP Configuration sect	Select whether grouping is strictly enforced. Options are Disable and Enable . The default is Disable .			
MLD Configuration section				
Default Version	Enter the supported IGMP version. Options are: $1 - 3$. The default is 3 .			
Query Interval	The interval at which the multicast router sends a query messages to hosts, expressed in seconds. The default is 125 .			
	If you enter a number below 128, the value is used directly. If you enter a num- ber 128, it is interpreted as an exponent and mantissa.			
Query Response Interval	Upon receiving a query packet, a host begins counting down seconds, from a random number. When the timer expires, the host sends its report.			
	Enter the maximum number of seconds that a host can pick to count down from. The value must be greater than the Query Interval . If using IGMP v1, this value is fixed at 10 seconds.			
Last Member Query Inter- val	Enter the maximum response time within which the host must respond to the Out of Sequence query from the router. The default is 10 seconds.			
	IGMP uses this value when the router receives an IGMPv2 Leave report indic- ating 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 25 .			
Maximum Multicast Data Sources (for IGMP v3)	Enter the maximum number of data sources allowed. Options are: 1 - 24 . The default is 10 .			
Maximum Multicast	Enter the maximum number of multicast groups that can be joined on a port or			

Field Name	Description
Group Members	group of ports. The default is 25 .
Fast Leave Enable	Select whether the IGMP proxy removes group members immediately without sending a query. Options are:
	 Enabled: Group members are removed immediately. This is the default. Disabled: Group members are removed after a query is sent and a response received

Wireless

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

Note: The pages in this section explain the fields for both wireless bands. The fields are the same for both bands.

Basic

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

orward thinking								
Device Info	Wireless	Basic						
Advanced Setup Wireless Basic Security	disable t name (al	e allows you to configure bas he wireless LAN interface, hi so known as SSID) and restri- uply/Save" to configure the ba	de the network t the channel se	from act et based	tive scans.	set the	wireles	ss network
MAC Filter Wireless Bridge	Er Er	able WiFi Button						
Advanced	Er Er	able Wireless						
Station Info Wifi Insight	Пн	ide Access Point						
liagnostics		ients Isolation						
Management		sable WMM Advertise						
ogout		able Wireless Multicast Forw	adda a factory					
	55ID:	smartslowite	stand (www.)					
	932932							
	BSSID:	00:23:64:A0:9F:1D						
		UNITED STATES			4			
	Country RegRev	ø						
	Max Clients:	128						
	Wireless	- Guest/Virtual Access Poin	ts:					
	Enabled		Hidden	Isolate Clients		Enable WMF	Max Clients	BSSID
		Ouest					128	N/A
	in the second second	Ovest1					128	N/A

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

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

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

Field Name	Description
Enable WiFi Button	(<i>Not applicable to the SR350n model</i>) This option is enabled by default. To <i>disable</i> the gateway's Wi-Fi button, click the checkbox to clear it.
Enable Wireless	This option is enabled by default. To <i>disable</i> the gateway's Wi-Fi radio, click the checkbox to clear it.
Hide Access Point	Click to hide the access point SSID from end users.

Field Name	Description		
Clients Isolation	Click to prevent LAN client devices from communicating with one another on the wireless network.		
Disable WMM Advertise	Click to stop the wireless from advertising Wireless Multimedia (WMM) functionality. WMM provides basic Quality of Service (QOS) for applications.		
Enable Wireless Multicast Forwarding	Click to enable Wireless Multicast Forwarding (WMF). Multicast traffic is for- warded across wireless clients.		
SSID	Enter the Wi-Fi SSID. If your gateway is connected to an ACS, it is recommended that SSID names be 1 - 32 characters long. Special characters are accepted.		
BSSID	Enter the Basic Service Set Identifier (BSSID) to provide the MAC address assigned to the wireless router.		
Country	Select the country in which the gateway is deployed.		
Country RegRev	Enter the revision number of the regulations being followed for the selected country. The default is ${\bf 0}.$		
Max Clients	Enter the maximum number of clients that can access the route wirelessly. Options are 1 through the value set in the Global Max Clients field on the Wire- less > Advanced page. The default is 128 .		
Wireless - Guest/Virtual A	Access Points table		
Enabled	Click to enable a virtual wireless access point for guest access.		
SSID	Enter your wireless SSID.		
Hidden	Click to hide the SSID from being broadcast publicly.		
Isolate Clients	Click to prevent client PCs from communicating with one another.		
Disable WMM Advertise	Click to stop the wireless from advertising Wireless Multimedia (WMM) func- tionality.		
Enable WMF	Click to enable Wireless Multicast Forwarding (WMF).		
Max Clients	Enter the maximum number of clients allowed for this wireless channel.		
BSSID	Displays the Basic Service Set Identifier or N/A.		

Security

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

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

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

SMART/F	RG*	SR552
evice Info	Wireless Security	
dvanced Setup Vireless Basic	You may setup configurat	onfigure security features of the wireless LAN interface.
Security MAC Filter Wireless Bridge		up(WPS) and Authorized MAC are empty, PBC is used. If Hide Access r list is empty with "allow" chosen, WPS2 will be disabled
Advanced Station Info	WPS Setup	
Wifi Insight lagnostics	Enable WPS	Enabled ~
anagement igout	Add Client (This feat mode is configured)	ure is available only when WPA-P5K(WPS1), WPA2 P5K or OPEN
		Enter STA PIN OUse AP PIN Add Enrollee Help
	Set Authorized Statio	DIN MAC Help
	Set WPS AP Mode	Configured ~
	Setup AP (Configure a	all security settings with an external registar)
	Device PIN	43045723 Help
	Manual Setup AP	
	You can set the network a	
	Select SSID:	SmartRG9f1b ~
	Network Authentication:	Mixed WPA2/WPA -PSK ~
	Protected Management Frames:	Disabled 🗸
	WPA passphrase: WPA Group Rekey Interval WPA Encryption:	t: c Click here to display
	WEP Encryption:	Deabled ~
		Apply/Save

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

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

Field Name	Description
Enable WPS	This option is enabled by default. To <i>disable</i> Wi-Fi Protected Setup, select Disabled .
Add Client	Select the method for generating the WPS PIN. Options are: Enter STA PIN and Use AP PIN.
	To add an enrollee station, click Add Enrollee.
	Note: If the PIN and Set Authorized Station MAC fields are left blank, the PBC (push- button) mode is automatically made active.
Set Authorized Sta- tion MAC	When manually pairing via WPS, enter the MAC address of the client device you are try- ing to connect.
Set WPS AP Mode	Select how security is assigned to clients. Options are:
	• Configured : The gateway assigns security settings to clients.
	• Unconfigured : An external client assigns security settings to the gateway.
Device PIN	This value is generated by the access point.
Manual Setup AP se	ction
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
Network Authentic- ation	Select the desired network security authentication type. Options are: Open , Shared , 802.1X , WPA , WPA-PSK , WPA2 , WPA2-PSK , Mixed WPA2/WPA , and Mixed WPA2/WPA-PSK . The default is WPA2-PSK .

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

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

Open & Shared Authentication

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

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

cuck Apply/Save when d	
Select SSID:	SmartRG9f1b ~
Network Authentication:	Open ~
WEP Encryption:	Enabled ~
Encryption Strength:	128-bt ~
Current Network Key:	1 ~
Network Key 1:	SmartRGWireless
Network Key 2:	
Network Key 3: Network Key 4:	
NEWOIK KEY 4:	Enter 13 ASCII characters or 26 hexadecimal digits for 128- bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
	Apply/Save

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

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

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

802.1X Authentication

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

Manual Setup AP	
Select SSID:	SmartRG9f1b 🗸
Network Authentication:	802.1X v
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled ~
Encryption Strength:	128-bit \sim
Current Network Key:	2 ~
Network Key 1:	SmartROWireless
Network Key 2:	
Network Key 3:	
Network Key 4:	Enter 13 ASCII characters or 26 hexadecimal digits for 128- bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
	Apply/Save

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

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

Field Name	Description
RADIUS Server IP address	Enter the IP address of the RADIUS (Remote Authentication Dial In User Service) server associated with your network.
RADIUS Port	Enter the port number for the RADIUS server. Port 1812 is the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port 1645 . Options are 1 - 65535 . The default is 1812 .
RADIUS Key	(<i>Optional</i>) Enter the encryption key (if required) needed to authenticate to the specified RADIUS Server.
WEP Encryption	Select to enable Wired Equivalent Privacy (WEP) mode. Options are Enabled and Dis-

Field Name	Description
	abled. The default is Enabled .
Encryption Strength	(<i>Appears when WEP Encryption is set to Enabled</i>) Select the length of the encryption method. Options are 128-bit and 64-bit . 128-bit is the more robust option for security.
Current Network Key	(<i>Appears when WEP Encryption is set to Enabled</i>) Select which of the four keys is presently in effect.
Network Key 1-4	(<i>Appears when WEP Encryption is set to Enabled</i>) Enter up to four encryption keys using the on-screen instructions to achieve the desired security strength (128-bit or 64-bit).

WPA2 & Mixed WPA2/WPA Authentication

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

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

thentication method, selecting data encryption, key is required to authenticate to this wireless network an ngth. one.
SmartRG9f1b ~
WPA2 ~
Disabled ~
Disabled ~
36000
0
0.0.0.0
1812
AES 🗸
Disabled ~
Apply/Save

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

Field Name	Description
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
Protected Management Frames	Select whether to enable this option. Options are Enabled and Disabled . The default is Disabled .
WPA2 Preauthentication	Select whether clients can pre-authenticate with the gateway while still con- nected to another AP. Options are Enabled and Disabled . The default is Dis- abled .
Network Re-Auth Interval	Enter the interval at which the client must re-authenticate with the gateway. Options are: 0-2,147,483 , and 647 seconds. The default is 36000 seconds (10 hours).
WPA Group Rekey Inter- val	The frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are: 1 - 65535 seconds.
RADIUS Server IP address	Enter the IP address of the RADIUS (Remote Authentication Dial In User Ser- vice) server associated with your network.
RADIUS Port	Enter the port number for the RADIUS server. Port 1812 is the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port 1645 . Options are 1 - 65535 .
RADIUS Key	(<i>Optional</i>) Enter the encryption key (if required) needed to authenticate to the specified RADIUS Server.
WPA Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are:
	 AES: Advanced Encryption Standard. TKIP+AES: AES combined with TKIP (Temporary Key Integrity Protocol).
WEP Encryption	This option is set to Disabled and cannot be changed.

WPA2-PSK & Mixed WPA2/WPA-PSK Authentication

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

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

key is required to ngth.	od, selecting data encryption, authenticate to this wireless network and
SmartRG9f1b $ \smallsetminus $	
WPA2 -PSK	~
Disabled 🗸	
	Click here to display
the second secon	
AES 🗸	
Disabled \lor	
Apply/Save	
	key is required to ngth. SmartRG9f1b ~ WPA2 -PSK Disabled ~ AES ~ Disabled ~

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

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

Field Name	Description
Select SSID	Select the SSID of the wireless network to which this security configuration will apply.
Protected Management Frames	Select whether to enable this option. Options are Enabled and Disabled . The default is Disabled .
WPA/WAPI passphrase	Enter the security password to be used by this security configuration.
Use base MAC address as WAP/WAPI Passphrase	Select whether to allow the base MAC address to be substituted for the password (in lieu of manually entering a password). When this box is checked, the WPA/WAPI passphrase field is ignored.
	The frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are: 1 - 65535 seconds.
WPA Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are:
	AES: Advanced Encryption Standard.
	• TKIP+AES : AES combined with TKIP (Temporary Key Integrity Protocol).
WEP Encryption	This option is set to Disabled and cannot be changed.

MAC Filter

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

On this page, you can configure the filter settings.

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

SMART/F	SR552n
Device Info Advanced Setup Wireless	Wireless MAC Filter Select SSID: SmartRG9f1b V
Basic Security MAC Filter Wireless Bridge Advanced	MAC Restrict MAC Restrict MAC Restrict Mac Allow Oeny filter is empty, WPS will be disabled Mac Allow Deny filter
Station Info Wifi Insight	MAC Address Remove
Diagnostics Management Logout	Add Remove

- 2. Select the SSID to which this MAC filter rule should apply.
- 3. In the MAC Restrict Mode field, select whether to apply MAC filtering. Options are:
 - Disabled: MAC filtering is off.
 - Allow: Access for the specified MAC address is permitted.
 - Deny: Access for the specified MAC address is rejected.
- 4. To add a MAC address to the filter list:
 - a. Click Add. The following page appears.

SMART/F	SR552n
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info	Wireless MAC Filter Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters. MAC Address: Apply/Save

- b. Enter the MAC Address that you want to add.
- c. Click Apply/Save.

You are returned to the Wireless -- MAC Filter page.



5. Click Apply/Save to commit your changes.

Wireless Bridge

On this page, you can configure the wireless bridge features (also called wireless distribution system) of the wireless LAN interface.

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

SMART/R	G°		SR552n
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Wifi Insight	Wireless Bridge This page allows you to configu LAN interface. Select 'Disabled restriction, and any wireless bri 'Enabled(Scan)' enables the wire specified by 'Remote Bridges M Click 'Refresh'' to update the re update to complete. Click ''Apply/Save'' to configure AP Mode:	for 'Bridge Restrict' to dis idge will be granted acces eless bridge restriction, a AC Address' will be grante mote bridges. Wait for a	able wireless bridge s. Selecting Enabled or nd only those bridges ed access. few seconds for the
Diagnostics	Bridge Restrict: Enabled	~	
Management Logout	Remote Bridges MAC Address:		
	1	Refresh Apply/Save	

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

Field Name	Description
AP Mode	Select whether to enable or disable access point (AP) functionality. Options are:
	Wireless Bridge: Disables AP functionality.
	 Access Point: Enables AP functionality. Wireless bridge functionality is still available and wireless stations can associate to the AP. This is the default.
Bridge Restrict	(Optional) Select to enable or disable wireless bridge restriction. Options are:
	 Enabled or Enabled(Scan): Enables wireless bridge restriction. Only bridges specified in the Remote Bridge MAC Address field are granted access. Click Refresh to update the station list. The list takes a few seconds to update. This is the default. Disabled: Disables wireless bridge restriction. Any wireless bridge is granted access.
Remote Bridges MAC Address	Enter up to four MAC addresses of remote bridges to be allowed access.

Advanced

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

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

Wireless particular cha Basic fragmentatio Security mode, set th MAC Filter preambles ar	we you to configure advanced f nonei on which to operate, force n threshold, set the RTS thresho beacon interval for the access e used. ave" to configure the advanced : : : : : : : : : : : : : : : : : : :	features of the wireless LAN interface. You can select a the transmission rate to a particular speed, set the old, set the wakeup interval for clients in power-save point, set XPress mode and set whether short or long d wireless options. Current: 11 (interference: acceptable)
Ireless particular cha Basic fragmentatio Security mode, set th MAC Filter preambles ar Wireless Bridge Advanced 802.11n Band Station Info Channel: Wiff Insight Auto Channel: MIMO-OFDM: anagement Bandwidth: agout Control Sideb MIMO Data R RTS / CTS Prol Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow RX Chain Pow S4g ** Rate: Fragmentatio RTS market Basic Rate: Fragmentatio RTS minterval Beacon Interv Global Max C XPress ** Tech Transmit Pow WMM (Wi-Fit	nnel on which to operate, force In threshold, set the RTS threshold beacon interval for the access aves to configure the advanced CAGE AND AND AND AND AND AND AND CAGE AND	 the transmission rate to a particular speed, set the old, set the wakeup interval for clients in power-save point, set XPress mode and set whether short or long d wireless options.
Advanced 802.11n Band Station Info Channel: Wifi Insight Auto Channel: anagement Bandwidth: gout Control Sideb MIMO Data R RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow RX Chain Pow RX Chain Pow S4g ** Rate: Multicast Rat Basic Rate: Fragmentable RTS Threshol DTM Interval Beacon Intral Beacon Intral Beacon Intral Clobal Max C XPress ** Tech Transmit Pow WMM (Wi Fi A	Timer(min)	Current: 11 (interference: acceptable)
Station Info Wifi Insight agnostics Imagement gout Channel: Auto Channel Auto Channel Bandwidth: Bandwidth: Gostrol Sideb MIMO Data R RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow RX Chain Pow Time: RX Chain Pow S4g [™] Rate: Fragmentatio RTS Threshol DTIM interval Beacon Interv Global Max C XPress [™] Tech Transmit Poir WMM (Wi-Fit	Timer(min)	Current: 11 (interference: acceptable)
vifi Insight Auto Channel gnostics MIMO-OFDM: nagement Bandwidth: Sout Control Sideb MIMO Data R RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow RX Chain Pow RX Chain Pow S4g [®] Rate: Fragmentatio RTS Threshol DTIM interval Beacon interv Global Max C XPress [®] Tech Transmit Pow WMM No Acknowledge	Timer(min) 15 Auto ~ 20MHz ~	Current: 11 (interference: acceptable)
gnostics MIMO-OFDM: hagement Bandwidth: out Control Sideb MIMO Data R. RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow RX Chain Pow Time: RX Chain Pow S4g* Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon interv Global Max C XPress* Tech Transmit Pow WMM (Wi-Fi A WMN No Acknowledger	Auto v 20MHz v	
agement Bandwidth: sut Control Sideb MMO Data R RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow Time: RX Chain Pow Time: RX Chain Pow S4g* Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTIM interval Beacon interv Global Max C XPress* Tech Transmit Pow WMM (Wi-Fi Acknowledgen	20MHz 🗸	
out Control Sideb MIMO Data R. RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow Time: RX Chain Pow Time: RX Chain Pow Time: RX Chain Pow S4g* Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTIM interval Beacon Interv Global Max C XPress* Tech Transmit Pow WMM(Wi-F1 A WMM No Acknowledger	The second	Current: 20MHz
MINO Data R. RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow Time: RX Chain Pow 54g** Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTIM Interval Beacon Interv Global Max C XPress** Tech Transmit Pow WMM (Wi-FI		Current: N/A
RTS/CTS Prot Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow Time: RX Chain Pow 54g** Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTIM Interval Beacon Interv Global Max C XPress** Tech Transmit Pow WMM (Wi-FI	VD C-1	
Support MIMO RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow Time: RX Chain Pow S4g ** Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon interv Global Max C XPress ** Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledger		~
RIFS Advertis OBSS Coexist RX Chain Pow RX Chain Pow Time: RX Chain Pow S4g ^{on} Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon interva Global Max C XPress ^{on} Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledger	annen anna anna anna anna anna anna ann	
OBSS Coexist RX Chain Pow RX Chain Pow Time: RX Chain Pow 54g** Rate: Multicast Rate Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon interv Global Max C XPress** Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledger	and the second se	
RX Chain Pow RX Chain Pow Time: RX Chain Pow 54g** Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTIM interval Beacon interv Global Max C XPress** Tech Transmit Pow WMM(Wi-Fi A WMM No Acknowledgen	property and and and	
RX Chain Pow Time: RX Chain Pow 54g** Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTIM Interval Beacon Interv Global Max Cl XPress** Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledger		Power Save status: Full Power
RX Chain Pow S49 "Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon Inter Global Max C XPress " Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledge	er Save Oulet	Power Save Status: Put Power
54g ** Rate: Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon Interv Global Max C XPress ** Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledge	In state Quiet 10	
Multicast Rat Basic Rate: Fragmentatio RTS Threshol DTM Interval Beacon Inter Global Max C XPress* Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledge	er Save PPS: 10	
Basic Rate: Fragmentatio RTS Threshol DTIM Interval Beacon Interv Global Max Cl XPress* Tech Transmit Pow WMM (Wi-Fi A WMM No Acknowledger	1 Mbps 🤍	
Fragmentatio RTS Threshol DTM Interval Beacon Interv Global Max C XPress ** Tech Transmit Pow WMM (Wi-Fi W MM No Acknowledger	e: Auto ~	
RTS Threshol DTM Interval Beacon interv Global Max C XPress ** Tech Transmit Pow WMM (Wi-F1 WMM No Acknowledger	Default	~
D TIM Interval Beacon Interv Global Max C XPress Tech Transmit Pow WMM (Wi-Fi WMM (Wi-Fi WMM No Acknowledge		
Beacon Interv Global Max C XPress* Tech Transmit Pow WMM (Wi-Fi WMM No Acknowledge		
Global Max C XPress* Tech Transmit Pow WMM (Wi-Fit WMM No Acknowledge	The second se	
XPress* Tech Transmit Pow WMM(Wi-Fi WMM No Acknowledge	and the second se	
Transmit Pow WMM(Wi-Fi A WMM No Acknowledge	and the second se	
WMM(Wi-Fi A WMM No Acknowledger	07	
WMM No Acknowledger	the second se	
Acknowledge	and an	
WMM APSD:	nent: Disabled ~	
2002/2012/2010/2012	Enabled 🗸	
Band Steerin Enable Traffi	Scheduler: Disable 🗸	
Airtime Fairn		
	ess: Enable v	Apply/Save

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

Field Name	Description
802.11n Band	This option is set to 2.4 GHz for compatibility with IEEE 802.11x standards and cannot be changed.
Channel	Select the Wi-Fi channel you want to use. Options are Auto and 1 - 11 .
Auto Channel Timer (min)	This options is set to 15 minutes and cannot be changed.
MIMO-OFDM	Select whether to enable Multiple-Input, Multiple-Output - Orthogonal Frequency- Division Multiplexing (MIMO-OFDM) interface. Options are: Auto and Disabled . The default is Auto .
Bandwidth	Select the operating bandwidth. Options are:
	• 20MHz : Only one 20MHz band is utilized.
	• 40MHz: Better throughput is provided by using two adjacent 20MHz bands.
Control Sideband	(<i>Applies only to 40 MHz, 802.11n operation</i>) The control sideband is the 20 MHz channel on which the network is advertised, where client devices will find beacons. Options are:
	• Lower: The additional 20 MHz of bandwidth for data will be positioned <i>above</i> the control channel.
	• Upper : The additional 20 MHz of bandwidth for data will be positioned <i>below</i> the control channel. Also, selecting this option changes the channel choices displayed.
MIMO Data Rate	Select the desired physical transmission rate. Options are Auto , Use 54G Rate , 1-11 , and 32 . The default is Auto .
	The Auto setting enables the Auto-Fallback feature which allows the gateway to automatically use the fastest possible data rate. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client.
RTS/CTS protection	Select whether to enable RTS/CTS and legacy clients to both work effectively on the network. Options are:
	• Auto: Provides maximum security but there is a noticeable impact on throughput. With this option, RTS/CTS behavior permits legacy clients to become aware of 802.11n transmit times, but decreases overall throughput of the system.
	• Off : Provides better throughput. This is the default.
Support MIMO Clients Only	Select whether to restrict non-MIMO clients from accessing the gateway. Options are On and Off . The default is On .

Field Name	Description
RIFS Advertisement	Reduced Inter-Frame Space (RIFS). Improves performance by reducing dead time required between OFDM transmissions. Options are Auto and Off . The default is Auto .
OBSS Coexistence	Coexistence of Overlapping Basic Service Sets (OBSS) prevents overlapping in the 20 MHz and 40 MHz frequencies. Options are:
	 Enable: The gateway automatically reverts to 20 MHz channel bandwidth when another WiFi network within 2 channels of its own channel is detected or when a client device with its 40 MHz Intolerant bit set is detected. Disable: The gateway advertises and operates in 40 MHz mode regardless of what other networks are configured nearby. This is the default.
RX Power Chain Save	Select whether to turn on power-save mode. Options are Enable and Disable . The default is Disable .
RX Power Chain Save Quiet Time	(<i>Available when RX Power Chain Save is set to Enable</i>) Sets the delay time (in seconds) between when system activity ceases and power-save mode engages. Options are: 0 - 2147483647 seconds. The default is 10 seconds.
RX Power Chain Save PPS	Available when RX Power Chain Save is set to Enable) Sets a throughput threshold (in seconds) for when the router engages power-save mode after the quiet time seconds have elapsed. Options are: 0 - 2147483647 packets per second. The default is 10 seconds.
54g™ rate	This option is set to 1Mbps and cannot be changed.
Multicast rate	Select the desired packet transmit rate for multicast. Options are $Auto$ and 1 - 54 Mbps. The default is $Auto$.
Basic Rate	Select the basic rate. Options are Default , 1 & 2 Mbps , and 1 & 2 & 5.5 & 6 & 11 & 12 & 24 Mbps . The default is Default .
Fragmentation Threshold	Enter the size at which packets will be fragmented into smaller units. The primary consideration for this setting is the size/capability of the circuit. Options are 256 - 2346 bytes. The default is 2346 bytes.
	A high packet error rate is an indication that a slightly increased fragmentation threshold is needed. When possible, the default value of 2346 bytes should be maintained. Poor throughput is a likely result of setting this threshold too low.
RTS Threshold	Enter the RTS (Request to Send) packet size beyond which the WLAN client hard- ware invokes its RTS/CTS mechanism. Smaller packets will otherwise be sent not using RTS/CTS. Options are 256 - 2347 bytes. The default is 2347 (disabled).

Field Name	Description
DTIM Interval	Enter the Delivery Traffic Indication Message (DTIM or Beacon rate) countdown vari- able used to indicate when the next window is available to client devices for listen- ing to buffered broadcast and multicast messages. Options are 1 and 65535 . The default is 1 .
Beacon Interval	Enter the time interval (in milliseconds) between beacon transmissions. Beacon transmissions make known the presence of an access point and convey to wireless NICs when to awake from power save mode to check for buffered frames at the access point. Options are 1 and 65535 ms. The default is 100 ms.
Global Max Clients	Enter the maximum number of client devices that can connect to the router. Options are 1 - 255 . The default is 128 .
Xpress™ Technology	Select whether to enable Xpress Technology. This technology is compliant with draft specifications of two planned wireless industry standards. Options are Enabled and Disabled . The default is Enabled .
Transmit Power	Enter the desired output power (by percentage). The default is 100% .
WMM (Wi-Fi Mul- timedia)	Select whether to enable this technology. It allows multimedia services (audio, video and voice packets) to get higher priority for transmission. Options are Auto , Enabled , and Disabled . The default is Enabled .
WMM No Acknow- ledgement	Select whether acknowledgements are sent (applied at the MAC level). Enabling this option allows better throughput but, in a noisy RF environment, higher error rates may result. Options are Enabled and Disabled . The default is Disabled .
WMM APSD	Select whether to enable Automatic Power Save Delivery, a power consumption saving feature. Options are Enabled and Disabled . The default is Enabled .
Band Steering	Select whether to detect if the client has the ability to use two bands. When enabled, the less-congested 5GHz network is selected (by blocking the client's 2.4GHz network). Options are Disabled and Enabled . The default is Disabled .
Enable Traffic Sched- uler	Select whether to enable scheduling of traffic to improve efficiency and increase usable bandwidth for some types of packets by delaying other types. Options are Disable and Enable . The default is Disable .
Airtime Fairness	Select how the gateway will manage the receiving signal with other devices. Options are Disable and Enable . The default is Enable .

Station Info

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

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

Click **Refresh** to update the information.

SMART/R	U.				SR
Device Info Advanced Setup Wireless	Wireless Authentio This page shows auth		88	ns and their sta	itus.
Basic Security	MAC	Associated	Authorized	SSID	Interface
MAC Filter	00:EE:BD:A0:C8:A5	Yes		SmartRG9f1b	wło
Wireless Bridge Advanced Station Info Wifi Insight			Refresh		

Wifi Insight

On this page, you can configure the WiFi Insight system.

1. In the left navigation menu, click Wireless > Wifi Insight. The following page appears. You can also reach this page by clicking Wireless > Wifi Insight > Configure.

ice Info	nfigure		
	his page you will be able to configure th	e WiFi Insight system	
eless			
isic curity	Sample Interval		
AC Filter	● 5 Second ○ 10 Second	0 15 Serred 0 20 S	acond
ireless Bridge	C Steam C To second	- 13 Second - 20 S	econo
vanced	Start/Stop Data Collection		
ition Info ifi Insight			
Configure	Start Data Collection performance	Caution - Enabling wifi	insight could result in reduced wij
ite Survey	performance		
Channel Statistics Metrics	Start collecting data every		
nostics	Sunday C Monday	Tiesday D ww	dnesday 🗌 Thursday 🗌
igement	Friday Saturday	idesday in ine	incisuay
ut			
	From 12:00 AM	To 12:00 AM	4
	Database Size		
	Database Size 2 (Please note that, for example, 2 hour will occupy approximately 1.30	MB of database)	
	(Please note that, for example, 2	STA's connected using a 5 si MB of database)	econds sample interval run for 1 te Older Data O Stop
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim	STA's connected using a 5 si MB of database)	
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxin Datacollection	STA's connected using a 5 si MB of database) num limit Overwrit	te Older Data 🔿 Stop
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics	STA's connected using a 5 si MB of database) num limit Overwrit	te Older Data O Stop Packet Retried
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxin Datacollection Counters Channel Statistics Chanim Statistics	STA's connected using a 5 s MB of database) num limit Overwrit	e Older Data O Stop Packet Retried Queue Utilization
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches	STA's connected using a 5 s MB of database) num limit Overwrit	e Older Data O Stop Packet Retried Queue Utilization Queue Length Per Precedence
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP	STA's connected using a 5 s MB of database) num limit Overwrit	e Older Data O Stop Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP Bad FCS	STA's connected using a 5 st MB of database) num limit Overwrit	e Older Data O Stop Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP	STA's connected using a 5 s MB of database) num limit Overwrit	Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput Physical Rate RTS Fall
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP Bad FCS Packet Requested	STA's connected using a 5 s MB of database) num limit Overwrit	Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput Physical Rate
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP Bad FCS Packet Requested Packet Stored	STA's connected using a 5 s MB of database) num limit Overwrit	Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput Physical Rate RTS Fall Retry Drop
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP Bad FCS Packet Requested Packet Stored	STA's connected using a 5 s MB of database) num limit Overwrit	Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput Physical Rate RTS Fall Retry Drop PS Retry
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP Bad FCS Packet Requested Packet Stored	STA's connected using a 5 s MB of database) num limit Overwrit	Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput Physical Rate RTS Fall Retry Drop PS Retry
	(Please note that, for example, 2 hour will occupy approximately 1.30 Once Database size reaches maxim Datacollection Counters Channel Statistics Chanim Statistics Rx CRS Glitches Bad PLCP Bad FCS Packet Requested Packet Stored	STA's connected using a 5 s MB of database) num limit Overwrit	Packet Retried Queue Utilization Queue Length Per Precedence Data Throughput Physical Rate RTS Fall Retry Drop PS Retry Acked

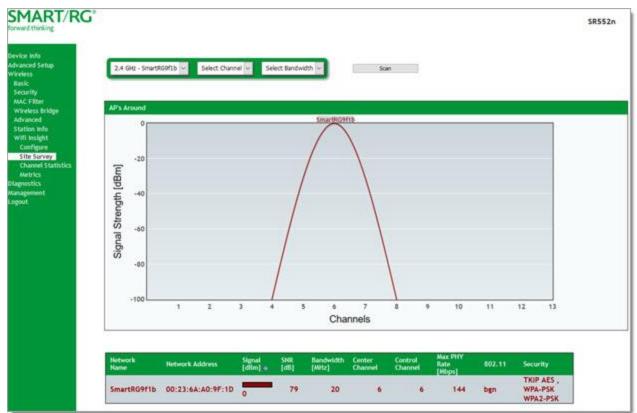
- 2. In the Sample Interval section, select the number of seconds for sampling to occur. Options are 5, 10, 15, and 20 seconds. The default is 5 seconds.
- 3. In the Start/Stop Data Collection section, configure the data sample:
 - a. Click Start collecting data every.
 - b. Select the days of the week when the data should be collected.
 - c. In the From and To fields, enter the start and end times for collection.

- 4. In the Database Size section, configure the database size limits:
 - a. In the **Database Size** field, enter the maximum size for the database file where the collected data will be stored. The default is **2** MB.
 - b. (*Optional*) Select whether to stop data collection when the maximum size is reached. Options are **Overwrite Older Data** and **Stop Data collection**. The default is **Overwrite Older Data**.
- 5. (Optional) In the Counters section, clear any counter options that you do not need. The default is to collect all counters.
- 6. Click **Submit** to save the configuration.
- 7. To export a database, in the Export Database section:
 - 1. Click Save Database to File. The open/save dialog box appears.
 - 2. Click OK to save or click Open and OK to view.

Site Survey

On this page, you can view signal strength and other details for your wireless networks.

1. In the left navigation menu, click Wireless > Wifi Insight > Site Survey. The following page appears.



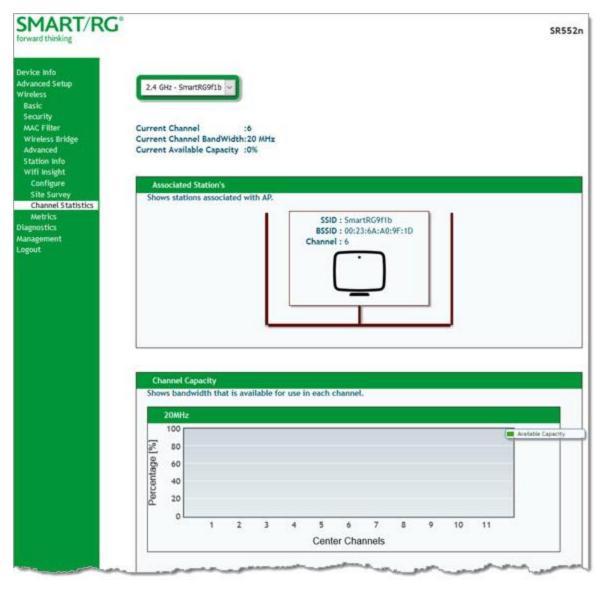
- 2. In the first field above the chart, select the wireless network that you want to review.
- 3. In the Select Channel field, select the channel that you want to review.
- 4. In the Select Bandwidth field, select the bandwidth.
- 5. Click Scan. The page refreshes to show the requested information.



Channel Statistics

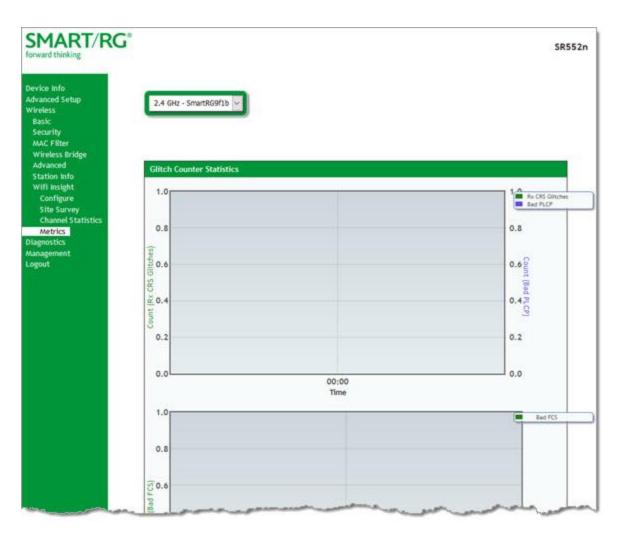
On this page, you can view signal strength, channel capacity, interference, and other details for specific channels.

In the left navigation menu, click Wireless > Wifi Insight > Channel Statistics. The following page appears.



Metrics

On this page, you can view glitch counter, chanim, associated stations, and packet queue statistics for your wireless networks. In the left navigation menu, click **Wireless** > **Wifi Insight** > **Metrics**. The following page appears.



Diagnostics

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

You can also ping a host or trace a connection.

Diagnostics

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

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

SMART/R	u .				SR552n
Device Info	br_0_0_35 Diagnostics				
Advanced Setup Wireless Diagnostics Diagnostics	Your modem is capable of testin below. If a test displays a fail st this page to make sure the fail s "Help" and follow the troublesho	atus, e	click "Rerun is consiste	Diagnostic Tests" nt. If the test cont	at the bottom of
Ethernet OAM	Test the connection to your loo	al net	twork		
Ping Host Trace Route to Host	Test your LAN1 connection:	FAIL	Help		
lanagement	Test your LAN2 connection:	PASS	Help		
ogout	Test your LAN3 connection:	FAIL.	Help		
	Test your LAN4 connection:	FAIL	Help		
	Test your Wireless Connection:	ON	Help		
	Test the connection to your DS	L serv	rice provid	ler	
	Test xDSL Synchronization:		PASS	Help	
	Test ATM OAM F5 segment ping	8	DISABLE	D Help	
	Test ATM OAM F5 end-to-end p	ing:	DISABLE	0 Help	
		Test	Next Connection	10.00	

To refresh the data, click Test at the bottom of the page. The normal test method is initiated, utilizing OAM F5 loopback cells.

To test the other defined connections, click the Next Connection and Previous Connection buttons.

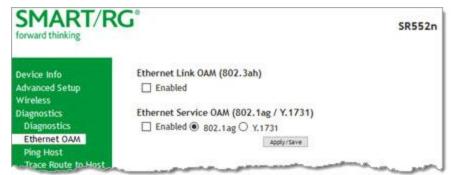
The table is updated with fresh diagnostic information about connection integrity. To learn more about what is being tested and what actions to take in the event that a particular test should fail, click the **Help** link at the far right of each line item.

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

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.

SMART/R	0	SR552n
Device Info Advanced Setup Wireless Diagnostics Diagnostics Ethernet OAM Ping Host Trace Route to Host Management Logout	Ethernet Link OAM (802.3ah) Enabled WAN Interface: atm0 OAM ID: OAM ID:	

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.

SMART/RC					SR552n
Device Info Advanced Setup	Ethernet Link OAM (802.3ah)			
Wireless	WAN Interface:	atm0 v			
Diagnostics Diagnostics	OAM ID:	1	(positive intege	r)	
Ethernet OAM	Auto Event	1			
Ping Host Trace Route to Host	Variable Retrieva	ā.			
Aanagement	Link Events				
ogout	Remote Loopbac	k			
	Active Mode				
	Ethernet Service OA				
	WAN Interface:	atm0 v			
	MD Level:	0 ~ [0-	7]		
	MD Name:	Broadcom	[e.g. Broadcom	1	
	MA ID:	BRCM	[e.g. BRCM]		
	Local MEP ID:	1	[1-8191]		
	Local MEP VLAN ID:	-1	[1-4094] (-1 me	eans no VLAN tag)	
	CCM Transmissio	n			
	Remote MEP ID:	-1	[1-8191] (-1 me	eans no Remote MEP)	
	Loopback and Linktr	ace Test			
	Target MAC:		[e.g. 02:10:18:	aa:bb:cc]	
	Linktrace TTL:	4	[1-255] (-1 mea	ans no max hop limit)	
	Loopback Result: N	/A			
	Linktrace Result: N	/Α			
		3	end Loopback Send Li	SRS7 BOB	

- 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 (802.3	ah) section

Field Name	Description
Ethernet Link OAM (802.3ah)	Click the Enabled checkbox to set options for this protocol. Additional fields appear.
WAN Interface	Select the WAN interface that you want tested.
OAM ID	Enter the ID of this OAM configuration. Only positive numbers are allowed.
Auto Event	Select whether to create event log entries automatically.
Variable Retrieval	Select to enable on-demand link diagnostics, including bit-error-rate approx- imation.
Link Events	Select to enable reporting of critical conditions that may cause link failure.
Remote Loopback	Select to enable on-demand link diagnostics, including bit-error-rate approx- imation.
Active Mode	Click to enable this feature.
Ethernet Service OAM (8	02.1ag/Y.1731) section
Ethernet Service OAM (802.1ag/Y.1731)	Click the Enabled checkbox and then click 802.1ag or Y.1731 to set options for this protocol. Additional fields appear.
WAN Interface	Select the WAN interface that you want tested.
MD Level	(<i>Appears for the 802.1ag option only</i>) Select the domain level for this main- tenance domain. Options are 0 - 7 . The larger the domain, the higher the value you should select.
MD Name	(<i>Appears for the 802.1ag option only</i>) Enter the name of the maintenance domain, e.g., Broadcom.
MAID	(Appears for the 802.1ag option only) Enter the MA ID, e.g., BRCM.
MEG Level	(Appears for the Y.1731 option only) Enter the MEG level for this service.
MEG ID	(Appears for the Y.1731 option only) Enter the MEG ID for this service.
Local MEP ID	Enter the ID of the local MEP. Options are 1 - 8191.
Local MEP VLAN ID	Enter the ID of the VLAN for the local MEP. Options are 1 - 4094 . The default is - 1 (no VLAN tag).
CCM Transmission	Select to enable CCM transmission.
Remote MEP ID	Enter the ID of the remote MEP. Options are 1 - 8191 . The default is -1 (no remote MEP).
Loopback and Linktrace	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. Options are 1 - 233 . The default is -1 (no hop limit).
Loopback Result	The results of the loopback test.
Linktrace Result	The results of the linktrace test.

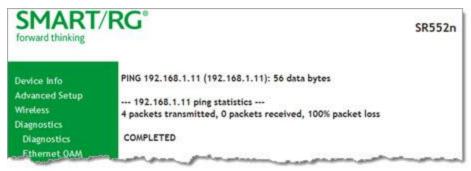
Ping

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

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

SMART/RG®	
Device Info	Ping Host
Advanced Setup Wireless 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.
Diagnostics Ethernet OAM	Target Host Address: Ping Most
Ping Host Trace Route to Host	a second s

- 2. Enter the host name or IP address.
- 3. Click Ping Host. 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/R	G°		SR552n
Device Info Advanced Setup Wireless Diagnostics Diagnostics Fault Management Ping Host Trace Route to Host Management Logout	Trace Route to Host Enter the IP address of the devic seconds) to appear. Target Host Address:	e that you wish to trace. The results will take a Trace Route to Host	few moments (up to 15

- 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.

Management

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

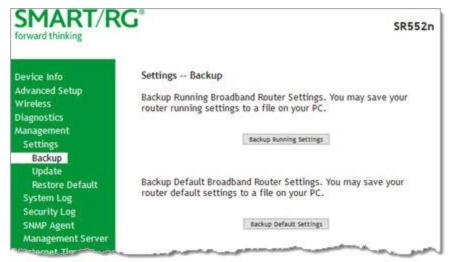
Settings

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

Backup

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

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



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

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

Update

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

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



- 2. Click the Browse button for the type of setting you wish to restore.
- 3. Locate the desired .conf file on your local system and click Open.
- 4. Click the appropriate **Update** button.

The gateway reboots when the update has completed.

Restore Default

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

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

SMART/RG®		
Device Info Advanced Setup Wireless Diagnostics Management	Settings Restore Default Restore Broadband Router setting to the defaults.	
Settings Backup	Restore Default Settings	

2. Click Restore Default Settings. The gateway is rebooted.

System Log

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

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



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	kernei: eth3 (switch port: 4) Link UP 1000 mbps full duplex	
Jan 1 00:00:59	daemon	err	syslog: CDM:caCdmPolForMessages: unrecognized msg 0x10000250	
Jan 1 00:10:44	daemon	err	syslog: httpd:644.295:cgiValidateSessionKey:2356:failed session key check. Got 2135380610, expected 658209780, age=0 max=600000	
Jan 1 00:13:10	daemon	err	syslog: httpd:790.530:cgiValidateSessionKey:2356:failed session key check. Got 685698293, expected 1511422544, age=0 max=600000	
Jan 1 00:15:59	daemon	crit	kernel: Line 1: xDSL G.994 training	
Jan 1 00:16:02	daemon	crit	kernel: Line 1: ADSL link down	
Jan 1 00:26:14	daemon	crit	kernel: Line 0: 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/RO	G [°] sr	552n
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log Security Log SNMP Agent 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 displayed. If the selected mode is 'Remote' of Both,' events will be sent to the specified IP address and UDP port of remote syslog server. If the selected mode is 'Local' or 'Both,' events will be call memory. Select the desired values and click 'Apply/Save' to configure the system log options. Log: Disable O Enable Log Level: Debugging v Display Level: Error v Mode: Local v	evel l to or the will

- b. To enable logging, click **Enable** next to the **Log** label.
- c. Modify the settings as needed.

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

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

Action	Description
	Both.

d. Click Apply/Save to save your changes.

Security Log

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

- Password change success/failure
- Authorized login success/failure
- Authorized user logged out
- Security lockout added/removed
- Authorized/Unauthorized resource access
- Software update
- 1. In the left navigation bar, click Management > Security Log. The following page appears.

SMART/Re	G° SR552n
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log Security Log	Security Log The Security Log dialog allows you to view the Security Log. Click "View" to view the Security Log. Click "Reset" to clear and reset the Security Log. Right-click <u>here</u> to save Security Log to a file.
SNMP Agent Management Server Internet Time Access Control	View Reset

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

SNMP Agent

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

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

SMART/R	G°	SR552n
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log Security Log SNMP Agent	application to retri in this device.	nagement Protocol (SNMP) allows a management eve statistics and status from the SNMP agent values and click "Apply" to configure the SNMP
Management Server Internet Time Access Control Update Software Reboot Logout	Read Community: Set Community: System Name: System Location: System Contact: Trap Manager IP:	public private SmartRG unknown unknown 0.0.0.0 Save/Apply

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

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

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

Management Server

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

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

TR-069 Client

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

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

SmartRG products can accommodate several ACS products, including:

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

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

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

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

SMART/RC	G		SR552n
Device info Advanced Setup Wireless Diagnostics Management Settings	configuration, provision, collection	 allows a Auto-Configuration Server (ACS) to perform auto- n, and diagnostics to this device. "Apply/Save" to configure the TR-069 client options. 	
Sectings System Log Security Log SNWP Agent Management Server TR-069 Client	OUI-Serial TR-069 Client ACS URL from DHCP:	MAC O Serial Number O Disable Enable Enabled	
STUN Config Internet Time Access Control 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://aci.smarting.com (huli) •••••• 20005 Anty_WAN - IPv4 - ↓	
	Connection Request Authentic Connection Request User Name: Connection Request Password: Connection Request URL:	ation admin admin terret terre	

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

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

Field Name	Description
OUI-Serial	Select whether to use the base MAC address or the serial number of your gateway when connecting to the ACS. This value may display in an ACS user interface when looking at the device details of a particular gateway. The default (and the most typical scenario) is MAC .
TR-069 Client	Enable or disable the TR-069 client on the CPE. You can disable the TR-069 WAN Management Client if no ACS is employed. The default is Enable .
	Note: If you may want to add an ACS to your infrastructure in the future, it is recommended that you leave this option enabled. When this feature is disabled, every gateway deployed with this setting must be manually re-configured to enable this client if needed later.

Field Name	Description
ACS URL from DHCP	Click the Enabled checkbox to enable your gateway to obtain the ACS URL via DHCP.
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.
ACS URL	Enter the URL for the CPE to connect to the ACS using the CPE WAN Man- agement Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
	You can include a port specification suffix if your ACS platform requires it, e.g., http://customer.acs.wanmanagmentservices.com:30005 where 30005 is the port number. The default is 30005 .
	A minimum firmware level of v2.5.0.x is required.
ACS User Name	Enter the user name by which this gateway logs in to the ACS. The default username is typically admin.
ACS Password	Enter the password to authenticate the above user name. The default pass- word is typically admin.
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 connect to the ACS.
Connection Request Authentication	This option is enabled by default. To <i>disable</i> authenticated connection requests, click the checkbox to clear it.
Connection Request Username	Enter the user name by which this gateway authenticates the ACS.
Connection Request Password	Enter the password by which this gateway will authenticate to the ACS.
Connection Request URL	There is typically no need to set the Connection Request URL as it is nor- mally established automatically based on the effective WAN IP. In some cases, the port can be configured as needed. An example value for this field might be "http://xxx.xxx.xxx.30005/" where the xxx values are specific WAN IP octet numbers.

Field Name	Description
	Note: The default port value is 30005.
	This URL may need to be configured for interoperability with your ACS vendor. If so, consult with SmartRG.

- 4. To force the gateway to attempt to sync with the ACS, click the GetRPCMethods button. This will assist you in verifying the TR-069 parameters entered above.
- 5. Click Apply/Save to save your changes.

STUN Config

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

STUN is most commonly used with older modems under ACS management connected via a NAT gateway. NAT accommodates a 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 following page appears.

SMART/R	G [®] SR552n
Device Info	TR-069 Client STUN Configuration
Advanced Setup Wireless	Select the desired values and click "Apply" to configure the TR-069 Client STUN options.
Diagnostics Management	
Settings System Log	STUN Server support
Security Log SNMP Agent	Save/Apply
Management Server	

2. To view the required STUN settings, click STUN Server Support. Additional fields appear.

SMART/RG	0	SR552n
Device Info Advanced Setup Wireless Diagnostics Management	TR-069 Client STUN C Select the desired values options.	onfiguration and click "Apply" to configure the TR-069 Client STUN
Settings System Log Security Log SNMP Agent Management Server TR-069 Client STUN Config Internet Time Access Control Update Software Reboot Logout	STUN Server support STUN Server Address: STUN Server Port: STUN Server User Name: STUN Server Maximum Keep Alive Period: STUN Server Minimum Keep Alive Period:	3478 -1 0 Save/Apply

- 3. Complete each field in accordance with the implementation specifics of your server.
- 4. Click Save/Apply to commit your changes.

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

Field Name	Description
STUN Server Address	The physical STUN server's assigned network address. An invalid address will pro- duce an immediate on-page error message from the gateway. You can enter a max- imum of 256 characters
	An ACS server may also have STUN functionality running on the same physical box. Consult your ACS vendor for implementation options and also TR-069 protocol 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. The value will be hidden.
STUN Server Pass- word	The password by which the modem authenticates the above username to the STUN infrastructure. Maximum length is 256 characters. Special characters are valid. The value will be hidden.
STUN Server Max- imum Keep Alive	Enter the maximum time(in seconds) that the keepalive function should be active. Options are -1 - Unlimited . The default is - 1 (no maximum limit).

Field Name	Description
Period *	
STUN Server Min- imum Keep Alive Period *	Enter the minimum time(in seconds) that the keepalive function should be active. Options are 0 - Unlimited . The default is 0 seconds.

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

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

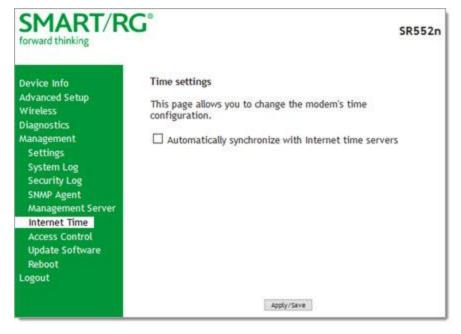
Selecting appropriate values for these two fields are influenced by a variety of environmental factors including devices types deployed, services employed and NAT configuration options enabled within the topology.



Internet Time

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

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



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

SMART/RC	i i		SR552n
Device Info Advanced Setup Wireless Diagnostics Management	and the second second	o change the modem's time configuration. hronize with Internet time servers	
Settings System Log Security Log	First NTP time server: Second NTP time server:	time.nist.gov v	
SNMP Agent Management Server	Third NTP time server: Fourth NTP time	None v	
Internet Time Access Control Update Software	server: Fifth NTP time server:	None v	
Reboot Logout	Time zone offset:	(GMT-08:00) Pacific Time, Tjuana	~

3. Select servers from the list or enter your own NTP servers.



- 4. Select the desired time zone for the gateway.
- 5. Click Apply/Save to commit your settings.

Access Control

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

Accounts

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

Add an Account

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

SMART/RG		SR552n
Device Info Advanced Setup	User Access Control Settings	
Wireless		
Diagnostics	Choos	e an option:
Management		
Settings	Create	Delete/Modify
Concerning in such	Account	Account
System Log		
System Log Security Log		
Security Log		
Security Log SNMP Agent	User Ac	count Status
Security Log SNMP Agent Management Server		
Security Log SNMP Agent Management Server Internet Time	User Ac	count Status
Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services		
Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services Passwords	Username	Status
Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services Passwords Access List	Username support user	Status Enabled Enabled
Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services Passwords Access List Logout Timer	Username support	Status Enabled
Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services Passwords Access List	Username support user	Status Enabled Enabled

Sector Contractor			
Device Info	c	reate Account	
Advanced Setup	Username:		
Wireless			
Diagnostics	Password:	Show Password	
Management			
Settings			
System Log	Assign Privileges		
Security Log	Device Info		
SNMP Agent		□ Wireless	
Management Server	Summary	Basic	
Internet Time	WAN	Security	
Access Control	Statistics	MAC Filter	
Accounts	Route	Wireless Bridge	
Services	ARP	Advanced	
Passwords	DHCP	Station Info	
Access List	Dec.		
Logout Timer	Advanced Setup		
Update Software	Layer 2 Interface	Diagnostics	
Reboot	WAN Service	Diagnostics	
Logout	4G LTE Settings	Ethernet OAM	
	Ethernet Config	Ping Host	
	LAN	Trace Route to Host	
	NAT		
	Security	Management	
	Parential Control	Settings	
	Quality of Service	System Log	
	Routing	Security Log	
	DNS	SNMP Agent	
	DSL	Management Server	
	DSL Bonding	Internet Time	
	UPnP	Access Control	
	DNS Proxy	Update Software	
	Interface Grouping	Beboot	
	IP Tunnel		
	[] IPSec	Support Tools	
	Certificate	Port Mirroring	
	Multicast	Factory reset	
	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 subcategory, the subordinate boxes are also selected.
- 5. Click Save Account to commit your changes. The new account is created. To test the account credentials, log out of the interface and then log back in using the new account.



Modify or Delete an Account

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

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

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

SMART/RG	SR552n
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log Security Log Security Log Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services Passwords Access List Logout Timer Update Software Reboot Logout	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.
	Back Update Account Delete Account

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

Advanced Setup Wireless	services on the ga	List ("SCL") is iteway.		ble or disable network • modify LAN SCLs.
System Log Security Log	Services	LAN	WAN	WAN Port Number
SNMP Agent	HTTP(S)	Enable	Enable	80
Management Server		lse encrypte	d HTTP(S) (init will restart.
Internet Time Access Control	FTP	Enable	Enable	(default)
Accounts	ICMP	Enable	Enable	(default)
Services	SNMP	Enable	Enable	(default)
Passwords Access List	SSH	Enable	Enable	22
Logout Timer	TELNET	Enable	Enable	(default)
				101009-012

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

s column identifies the SCL services that can be enabled or disabled. Options are: P, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP.
rk this checkbox to implement secured HTTP. rning: When you click this option, the gateway reboots.
ect the service enabled on LAN side firewall. Depending on configuration settings de elsewhere in the GUI, this column may be read-only. e: ICMP is an always-enabled service by default and has no checkbox in the LAN
- k

Field Name	Description
WAN	Select the service enabled on the WAN side firewall.
WAN Port Number	The port the access control applies to on the WAN side for the given service. See port information below.
Service port options	
FTP	FTP Service access (For WAN, this is the default port).
нттр	HTTP Service access (For WAN, this is in association with specified port (default is port 80).
ICMP	ICMP Service access (For WAN, this is the default port).
SNMP	SNMP Service access (For WAN, this is the default port).
SSH	SSH Service access (For WAN, this is in association with specified port (default is port 22).
TELNET	TELNET Service access (For WAN, this is the default port).
TFTP	TFTP Service Access (as with default port).

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/Re	G° SR552n
Device info Advanced Setup Wireless Diagnostics Management Settings System Log Security Log SNMP Agent Management Server Internet Time Access Control Accounts Services Passwords Access List Logout Timer Update Software Reboot Logout	Access Control Passwords Access to your Router is controlled through three user accounts: admin, support, and user. The user name "admin" has unrestricted access to change and view configuration of your Router. The user name "support" is used to allow an ISP technician to access your Router for maintenance and to run diagnostics. The user name "user" can access the Router, view configuration settings and statistics, as well as update the router's software. 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. User Name: Old Password: Confirm Password: Confirm Password:

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

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

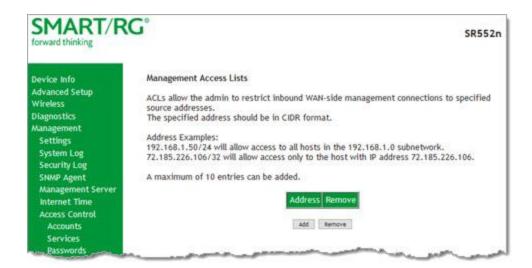
Field Name	Description
User Name	Specifies name of account to be configured. Options are admin, support, user.
Old Password	Enter the current password for the entered User Name.
New Password	Enter the new password for the entered User Name. A maximum of 16 characters is allowed.
Confirm Password Re-enter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

Access List

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

Note: This feature is available only for SR515ac models.

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



2. To add an address:

a. Click Add. The following page appears.

SMART/R	G°	SR552n
Device Info Advanced Setup Wireless Diagnostics	Management Access List Restrict inbound management connection	ns to specified source address
Management Settings System Log Security Log SNMP Agent	Source Address:	

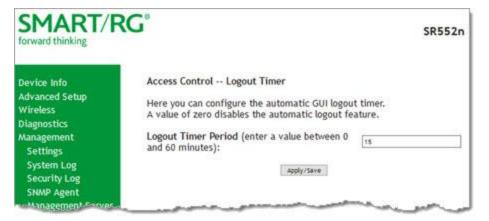
- b. Enter the address for which you want to restrict access.
- c. Click Apply/Save. You are returned to the Management Access Lists page.
- d. To add up to 9 more addresses, repeat steps 2a 2c.
- 3. To remove an address, click the **Remove** checkbox next to it and then click **Remove**. The list is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

Logout Timer

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

Note: This feature is available only for SR515ac models.

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



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

Update Software

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

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

SMART/R	G SR552n
Device Info	Update Software
Advanced Setup Wireless	Step 1: Obtain an updated software image file from your ISP.
Diagnostics Management	Step 2: Enter the path to the image file location in the box below or dick the "Browse" button to locate the image file.
Settings System Log	Step 3: Click the "Update Software" button once to upload the new image file.
Security Log SNMP Agent	NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Management Server Internet Time	Software File Name: Browse. Ho file selected.
Access Control	Update Software
Update Software	and

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.

Logout

1. To log out of your gateway, click Logout in the left navigation menu. The Logout page appears.

SMART/RG®		SR552n
Device Info Advanced Setup Wireless Diagnostics Management Logout	Click the button below to log out of the GUI.	2

2. Click the Logout button. A success message appears.

FCC Statements

FCC Interference Statement

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

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

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

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

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

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

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

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

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.

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: VW7DL01BSR555A.

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.

Ringer Equivalency Number Statement

Notice: The Ringer Equivalency 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 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, 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 device does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

IC CS-03 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.

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 (identify the device by certification number, or model number if Category II) 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.

5GHz

5150-5250 MHz band is restricted to indoor operations only.

Revision History

REV	DATE	CHANGES
4.1	6/29/2018	Updated to match SmartRG Firmware Release 2.6.1.6,
4.0	3/27/2018	Updated to match SmartRG Firmware Release 2.6.1.5.
3.7	3/27/2018	Updated with minor enhancements to content.
3.6	12/09/2016	Update SR515ac information to match new firmware release.
3.5	6/28/2016	Update FCC information; no substantive changes to content.
3.5	4/26/2016	 Added information about SR512nm gateway (MoCA feature) and the SR515ac gateway. Updated screen captures and related descriptions. Further standardized wording & formatting.
3.4	6/20/2015	 Updated behavior description for the reset button for FW v2.5.0.7 Clarified WLAN button operation with press and hold durations Expanded the field definitions for xDSL Statistics page
		 Expanded the definition for the MTU Size field added to the PPP Username and Password page Added section for Access Control (new feature in FW v2.5.0.7) Corrected the table content for the fields seen on the NAT page found in the IPoE WAN interface workflow Miscellaneous formatting and content corrections Implemented image compression to reduce .pdf file size
3.3	1/28/2015	 Cosmetic enhancements. Replaced page shots with new UI color scheme and logos. Expanded coverage of Advanced Setup > WAN Service General edit
3.2	10/20/2014	 Visual overhaul. New colors, logo and layout Added missing sections for Ethernet Config and LAN Expanded chapters for Management Server and STUN
3.0	6/26/2014	 Complete re-write with new layout Authored complete field-by-field descriptions for each page Complete compendium of page-shots for each feature Migrated use cases to on-line knowledge base. (See the SmartRG Customer Portal.)