

/ Gateway User Manual

Model: SR655ac

Release 1.3

July 2017

Firmware Version: 1.0.0.76

Table of Contents

Welcome!	4
Purpose & Scope	4
Intended Audience	4
Getting Assistance	4
Copyright and Trademarks	4
Disclaimer	4
Getting Familiar with your Gateway	5
LED Status Indicators	5
Connections	6
External Buttons	7
2.4GHz and 5GHz Buttons	7
Reset Button	7
Installing your SR655ac Gateway	8
Logging in to your Gateway's UI	9
Device Info	10
Summary	10
WAN	11
Statistics	12
LAN	12
WAN Service	12
xTM	13
xDSL	14
Route	19
ARP	20
DHCP	21
CPU & Memory	22
Advanced Setup	23
Layer2 Interface	23
ATM Interface	23
PTM Interface	26
ETH Interface	28
WAN Service	28
PPP over Ethernet WAN Service	30
IP over Ethernet WAN Service	38
Bridging	47
USB Mobile Service	50
VPN	54
L2TP Client Configuration	54
PPTP Client	57
Ethernet Mode	60
LAN	61
IPv4 Autoconfig	61
IPv6 Autoconfig	64
Local VLAN Setting	67
NAT	68
Virtual Servers	68
Port Triggering	70
DMZ Host	72

ALG	73
Multi NAT	73
Security	74
IP Filtering - Outgoing	74
IP Filtering - Incoming	76
MAC Filtering	77
Parental Control	79
Time Restriction	79
Url Filter	81
Quality of Service	82
Quality of Service	82
QoS Queue	83
QoS Classification	85
QoS Port Shaping	87
Routing	88
Default Gateway	88
Static Route	89
Policy Routing	90
RIP	91
DNS	92
DNS Server	92
Dynamic DNS	93
DNS Config	94
DSL	94
DSL Bonding	96
UPnP	97
DNS Proxy	97
Print Server	98
DLNA	99
Storage Service	99
Storage Device Info	99
User Accounts	100
Interface Grouping	101
IP Tunnel	103
IPv6inIPv4	104
IPv4inIPv6	104
IPSec	105
Certificate	108
Local	108
Trusted CA	111
Power Management	111
Multicast	111
Managing group exception lists	114
Wireless	115
Basic	115
Security	117
Open and Shared Authentication	118
802.1X Authentication	119
WPA2 and Mixed WPA2/WPA Authentication	120

Table of Contents

WPA2-PSK and Mixed WPA2/WPA-PSK		
Authentication	121	
MAC Filter	122	
Wireless Bridge	124	
Advanced	124	
Station Info	128	
Wifi Insight	128	
Site Survey	130	
Channel Statistics	131	
Metrics	132	
Voice	134	
VoIP Status	134	
SIP Basic Setting	134	
SIP Advanced Setting	137	
SIP Star Code Setting	142	
SIP Extra Setting	142	
SIP Debug Setting	144	
Diagnostics	146	
Diagnostics	146	
Ethernet OAM	147	
Diagnostic Tools	150	
Ping	150	
Traceroute	151	
Start / Stop DSL	151	
Management	153	
Settings	153	
Backup	153	
Update	154	
Auto Update	154	
Restore Default	155	
System Log	155	
Security Log	157	
SNMP Agent	158	
Management Server	159	
TR-069	159	
STUN Config	161	
XMPP Connection	163	
Internet Time	165	
Access Control	165	
Passwords	166	
Access List	166	
Services Control	167	
Logout Timer	168	
Update Software	169	
Reboot	169	
Logout	171	
Appendix: FCC Statements	172	
FCC Interference Statement	172	
FCC Radiation Exposure Statement	172	
FCC - PART 68	173	
Ringer Equivalency Number Statement	173	
IC CS-03 statement	173	
Canada Statement	173	
5GHz	174	
Revision History	175	

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 Gateway User Manual provides SmartRG customers with installation, configuration and monitoring information for the SR655ac 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 [Subscribers](#) 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

Copyright © 2017 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 to help you get familiar with the SR655ac model.

LED Status Indicators

The indicator lights (LEDs) on the front of the SR655ac gateway can help you understand the state of your gateway.

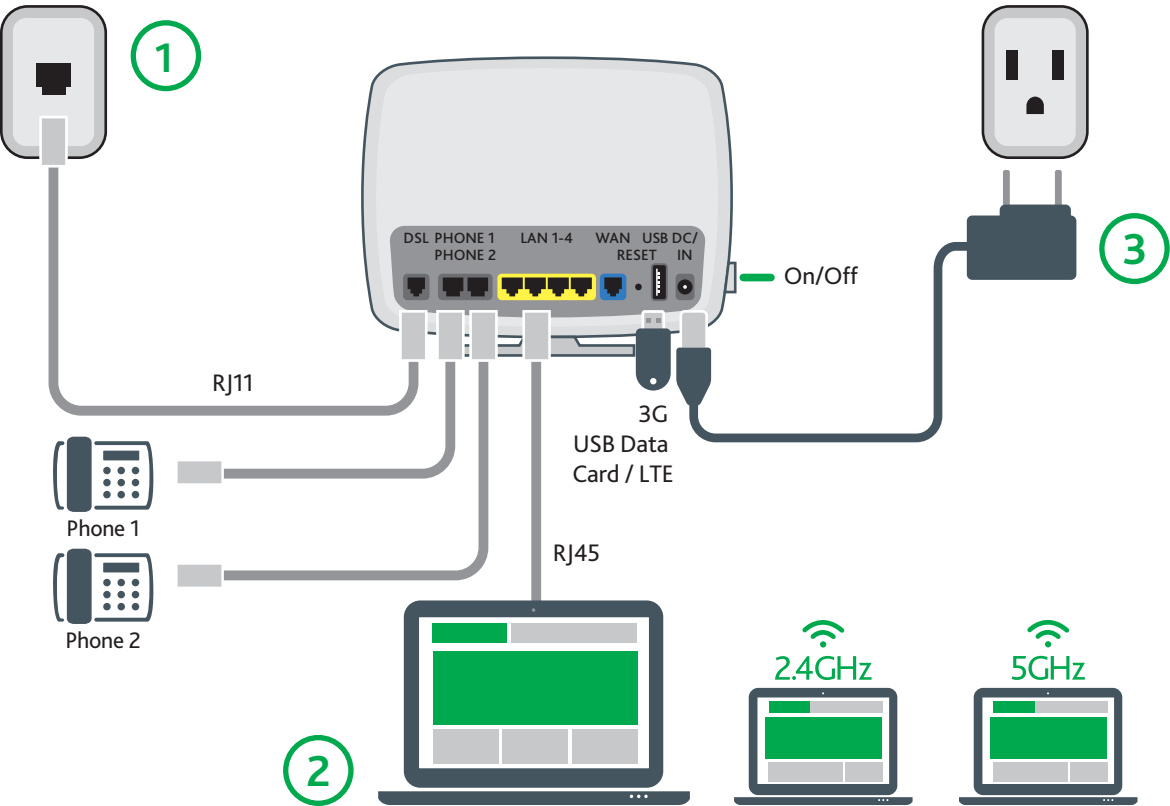


Legend: ● Green ⚙️ Green Blinking ● Red ● Lt. Blue ⚙️ Lt. Blue Blinking ● Dk Blue ⚙️ Dk. Blue Blinking

LED	Action	Explanation
All LEDs <i>except</i> those listed below	⚙️	Feature enabled &/or working correctly Data being transferred
POWER	●	Device in CFE mode Device powered on and ready for use
DSL		For VDSL only / WAN service (<i>Single Line - Inner or Outer Pair</i>)
	⚙️ / ⚙️	DSL line 0 acquiring sync
	●	DSL line 0 (inner pair) connected
	⚙️ / ⚙️	DSL line 1 (outer pair) acquiring sync and connected
	●	DSL connected
	⚙️	DSL down
	Not lit	No lines connected
Note: This LED may flash green briefly on startup.		
INTERNET	⚙️	DSL sync acquired and gateway on line Data being transferred
	●	Internet authentication / connection has failed

Connections

Below is an illustration of the connectors located on the back of the SR655ac gateway.



The ports depicted above, and the buttons and ports located on the left side of the gateway, are described below.

Feature	Description
Rear panel	
DSL	This grey RJ11 port is used to connect your gateway to an Internet provider via a DSL service.
Phone 1 - 2	These grey RJ11 ports can be used to connect your gateway to an Internet provider via a telephone line.
LAN 1 - 4	The yellow RJ45 ports can be used to connect client devices such as computers and printers to your gateway.
WAN	The blue RJ45 port is used to hard-wire your gateway to another network device. For models with both WAN and DSL ports, when your Internet connection is via DSL, you can configure the WAN port to function as an additional LAN port. For detailed instructions, see the Ethernet Configuration section of this manual.
USB 1	Can transfer data, act as a printer interface, and handle a 3G accessory.
Power	Use only the power supply included with your gateway. Intended for indoor use only.
Left side	

Feature	Description
On/Off	Power switch.
USB2	Can transfer data, act as a printer interface, and handle a 3G accessory.
5GHz	Enables or disables the 5GHZ wireless function.
2.4GHz	Enables or disables the 5GHZ wireless function.

External Buttons

Smart RG gateways provide push-button controls on the exterior for critical features. These buttons provide a convenient way to toggle the Wi-Fi radio on and off or reset the gateway. These controls are described below.

2.4GHz and 5GHz Buttons

Note: On early production units of the SR655ac gateway, these buttons are labeled WiFi (instead of 2.4 GHz) and WPS (instead of 5 GHz).

These buttons are located on the left side of the gateway and control the Wi-Fi radio functions.

To turn a wireless radio on or off, press the related button briefly (1-2 seconds). For example, to turn the 2.4 GHz radio on or off, press the **2.4GHz** button for 1-2 seconds.

To enable WPS, press the related button and hold it for 4-6 seconds.

Reset Button

The **Reset** button is a small hole in the back of the gateway with the actual button mounted beneath the surface. This style of push-button prevents the gateway from being inadvertently reset during handling.

Warning: Do not press the **Reset** button unless you are sure that you want to clear the current settings.

To reset your gateway, use a fine wire (such as a paper clip) to press the button for 7-10 seconds and release. The factory default settings are restored.

Installing your SR655ac Gateway

1. Locate the splitter cable that is included with your SmartRG gateway. It has three parts.
2. Connect the splitter as follows:
 - a. Connect the DSL port of the gateway and the Modem port of the splitter with a telephone cable
 - b. Connect the phone to the phone port of the splitter with a telephone cable
 - c. Connect the incoming line to the Line port of the splitter.
3. Connect the LAN port of the gateway to the network card of the PC using an Ethernet cable.
4. Plug the power adapter to the wall outlet and then connect the other end of it to the Power port of the gateway.
5. Turn on the unit by pressing the On/Off button on the side of the gateway.

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

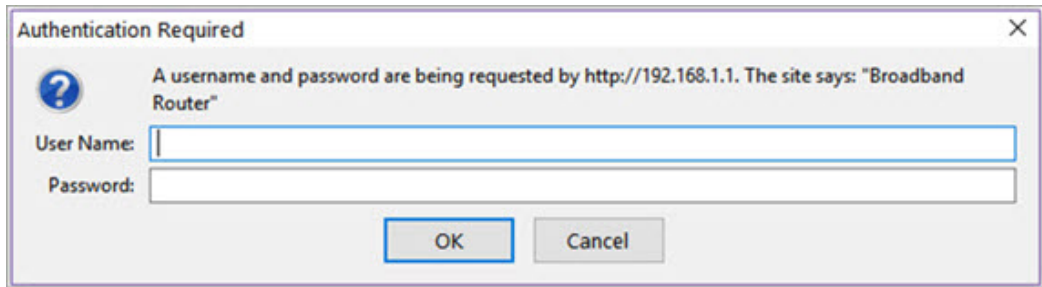
Your gateway is now automatically being set up to connect to the Internet. This process may take a few minutes to complete before you can begin using your Internet applications (browser, email, etc.).

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

Logging in to your Gateway's UI

To configure the SmartRG SR655ac gateway's settings, access the gateway's embedded UI.

1. Open a Web browser on your computer.
2. In the address field, enter `http://192.168.1.1` (the default IP address of the DSL gateway). The login page appears.



3. Enter the user name and password. The default user name and password of the super user are admin and admin. The username and password of the common user are user and user. It is recommended that you change these default values after logging in to the DSL gateway for the first time.
4. Click **OK**. The gateway status page appears.
5. To view the log for this gateway, click **View log** at the bottom of the page. The log appears in a separate window.
6. To log into the GUI, at the bottom of the page, click **Manage gateway (advanced)**. The gateway interface appears, showing the Device Info summary page.

Device Info


In this section, you can view data about your gateway and network, and configure DHCP, ARP, and WAN interfaces.

Summary

On this page, you can view device such as the board ID, software and voice service version, and information about your WAN connection such as the upstream rate and the LAN address.

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

You can also reach this page by clicking [Device Info](#) > [Summary](#) in the left navigation menu.



SR655ac

Device Info

Advanced Setup

Wireless

Voice

Diagnostics

Diagnostics Tools

Management

Logout

Device Info

Board ID:	SR655ac
Symmetric CPU Threads:	2
Manufacturer:	SmartRG
System Base MAC Address:	3c90662ca9a2
Configuration File Origin:	SmartRG
Serial Number:	SR655AA076-S000053
Build Timestamp:	170325_1014
Software Version:	1.0.0.65
Bootloader (CFE) Version:	1.0.38-118.3
DSL PHY and Driver Version:	A2pvbH042rd26q_rc1a
Wireless Driver Version:	7.35.260.64013
Voice Service Version:	Voice
Uptime:	0D 0H 4M 15S

This information reflects the current status of your WAN connection.

Traffic Type:	Inactive
Aggregate Line Rate - Upstream (Kbps):	0
Aggregate Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	eth0.1
Primary DNS Server:	8.8.8.8
Secondary DNS Server:	8.8.4.4
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	
Date/Time:	Mon Mar 27 09:38:15 2017

WAN

The WAN status screen provides a high level overview of the connection between your Internet Service Provider and your gateway device. The WAN interface can physically be DSL or Ethernet and supports a number of Layer 2 and later configuration options covered later in this document.

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

WAN Info													
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enable	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ptm0.1	ipoe_0_1_1	IPoE	N/A	Disabled	Disabled	Disabled	N/A	N/A	Enabled	Enabled	Unconfigured	0.0.0.0	
eth0.1	ipoe_eth0	IPoE	N/A	Disabled	Disabled	Disabled	N/A	N/A	Enabled	Enabled	Connected	192.168.1.2	

The fields on this page are defined below.

Field Name	Description
Interface	The connection interface (Layer 2 interface) through which the gateway handles the traffic.
Description	The service identifier such as pppoe_0_1_1.35 .
Type	The service type. Options are PPPoE , IPoE , and Bridge .
VlanMuxId	The VLAN ID. Options are Disabled or 0 - 4094 .
IPv6	The state of IPv6. Options are Enabled , Disabled , and N/A .
Igmp Pxy	The state of the IGMP proxy. Options are Enabled , Disabled , and N/A .
Igmp Src Enbl	The state of the IGMP source. Options are Enabled and Disabled .
MLD Pxy	The state of the MLD proxy. Options are Enabled , Disabled , and N/A .
MLD Src Enable	The state of the MLD source. Options are Enabled , Disabled , and N/A .
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 DSL. Data is updated at 15-minute intervals.

LAN

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

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

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

SMART/RG[®]

forward thinking

SR655ac

Device Info

Summary

WAN

Statistics

LAN

WAN Service

xTM

xDSL

Route

ARP

DHCP

CPU & Memory

Advanced Setup

Wireless

Voice

Statistics -- LAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
ETH1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH2	216783	1710	0	8	0	562	1039	109	1082095	1552	0	2	0	138	1091	323
ETH3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5 GHz Band	0	0	0	3	0	0	0	0	37414	470	0	0	0	0	0	0
2.4 GHz Band	0	0	0	15	0	0	0	0	0	0	0	0	0	0	0	1

Reset Statistics

The fields on this page are defined below.

Field Name	Description
Interface	Available LAN interfaces. Options are ETH1 - ETH4, ETHWAN, 5GHz Band, and 2.4 GHz Band.
Received & Transmitted columns	
Bytes	The total number of packets in bytes.
Pkts	The total quantity of packets.
Errs	The total quantity of error packets.
Drops	The total quantity 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 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/RG®

forward thinking

SR655ac

Device Info

Summary

WAN

Statistics

LAN

WAN Service

xTM

xDSL

Route

Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
ptm0.1	ipoe_0_1_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth0.1	ipoe_eth0	329218	1610	0	0	200075	782	3	825	1468	17	0	0	0	0	17	0

Reset Statistics

The fields on this page are defined below.

Field Name	Description
Interface	Available WAN interfaces.
Description	The service description. Options are pppoe , ipoe , and b , followed by the identifier for each service.
Received & Transmitted columns	
Bytes	The total number of packets in bytes.
Pkts	The total quantity of packets.
Errs	The total quantity of error packets.
Drops	The total quantity of dropped packets.

xTM

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

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

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

SMART/RG® forward thinking SR655ac

Device Info
Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route

Interface Statistics

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

Reset

The fields on this page are defined below.

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.

Field Name	Description
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 gateway are included. The terms and their explanations are derived from the relevant ITU-T standards and referenced accordingly.

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

SMART/RG®
forward thinking

SR655ac

Statistics -- xDSL

Bonding Line Selection

Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

2. In the **Bonding Line Selection** field, select the line for which you want to view statistics or to run an xDSL Bit Error Rate (BER) test that determines the quality of the xDSL connection. Options are **line 0** and **line 1**.
3. To run an xDSL (BER) test, follow the instructions in "Running xDSL (BER) tests".
4. To reset the counters, click **Reset Statistics** near the bottom of the page.

The fields on this page are defined below.

Field Name	Description
Synchronized Time	Time when the last synchronization was performed.
Number of Synchronizations	Number of synchronizations performed.
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 Upstream columns	
Line Coding (Trellis)	State of the Trellis Coded Modulation. Options are On and Off .
SNR Margin (0.1 db)	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)	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)	Typical obtainable sync rate, i.e., the attainable net data rate that the receive PMS-TC and PMD functions are designed to support under the following conditions: <ul style="list-style-type: none"> • Single frame bearer and single latency operation. • Signal-to-Noise Ratio Margin (SNRM) to be equal or above the SNR Target Margin. • BER not to exceed the highest BER configured for one (or more) latency paths. • Latency not to exceed the highest latency configured for one (or more) latency paths. • Accounting for all coding gains available (e.g., trellis coding, RS FEC) with latency bound. • 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 feature status. Options are Inactive and Active .
G. inp Status	<i>(Visible only for gateways connected via DSL)</i> Status of video data retrieval from the buffer. Options are Inactive and Active .
Rate (Kbps)	Current net data rate of the xDSL link. Net data rate is defined as the sum of all frame bearer data rates over all latency paths. [2]
Downstream and Upstream columns for DSL-specific fields only	
B (# of bytes in Mux Data Frame)	Nominal number of bytes from frame bearer #n per Mux Data Frame at Reference Point A in the current latency path.
M (# of Mux Data Frames in FEC Data Frame)	Number of Mux Data Frames per FEC Data Frame in the current latency path.
T (Mux Data Frames over sync bytes)	Ratio of the number of Mux Data Frames to the number of sync bytes in the current latency path.
R (# of check bytes in FEC Data Frame)	Number of Reed Solomon redundancy bytes per codeword in the current latency path. This is also the number of redundancy bytes per FEC Data Frame in the current latency path.

Field Name	Description
S (ratio of FEC over PMD Data Frame length)	Ratio of FEC over PMD Data Frame length.
L (# of bits in PMD Data Frame)	Number of bits from the latency path included per PMD.
D (interleaver depth)	Interleaving depth in the current latency path.
Delay (msec)	PMS-TC delay in milliseconds of the current latency path (or the lowest latency path when running dual-latency paths).
INP (DMT symbol)	Input level for DMT-managed DSL environments.
OH Frames	Number of xDSL OH Frames transmitted/received.
OH Frame Errors	Number of xDSL OH Frames transmitted/received with errors.
<i>(End of DSL-specific field group)</i>	
Super Frames	Number of xDSL Super Frames transmitted/received.
Super Frame Errors	Number of xDSL Super Frames transmitted/received with errors.
RS Words	Number of Reed-Solomon-based Forward Error Correction (FEC) codewords transmitted/received.
RS Correctable Errors	Number of Reed-Solomon-based FEC codewords received with errors that have been corrected.
RS Uncorrectable Errors	Number of Reed-Solomon-based FEC codewords received with errors that were not correctable.
RS Codewords Received	<i>(Visible only for gateways connected via DSL)</i> Total number of Reed-Solomon Codewords received.
RS Codewords Corrected	<i>(Visible only for gateways connected via DSL)</i> Total number of Reed-Solomon Codewords corrected.
RS Codewords Uncorrected	<i>(Visible only for gateways connected via DSL)</i> Total number of Reed-Solomon Codewords Uncorrected
HEC Errors	Count of ATM HEC errors detected. As per ITU-T G.992.1 and G.992.3, a1-byte HEC is generated for each ATM cell header. Error detection is implemented as defined in ITU-T I.432.1 with the exception that any HEC error shall be considered as a multiple bit error, and therefore, HEC Error Correction is not performed. [1],[2]
OCD Errors	Total number of Out-of-Cell Delineation errors. ATM Cell delineation is the process which allows identification of the cell boundaries. The HEC field is used to achieve cell delineation. [4] An OCD Error is counted when the cell delineation process transitions from the SYNC state to the HUNT state. [2]
LCD Errors	Total number of Loss of Cell Delineation errors. An LCD Error is counted when at least one OCD error is present in each of four consecutive overhead channel periods and SEF (Severely Errored Frame) defect is present. [2]
Total Cells	Total number of cells (OAM and Data cells) transmitted/received.
Data Cells	Total number of data cells transmitted/received.
Bit Errors	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, LOS (Loss of Signal) defects, SEF (Severely Errored Frame) defects, or LPR (Loss of Power) defects. [4]

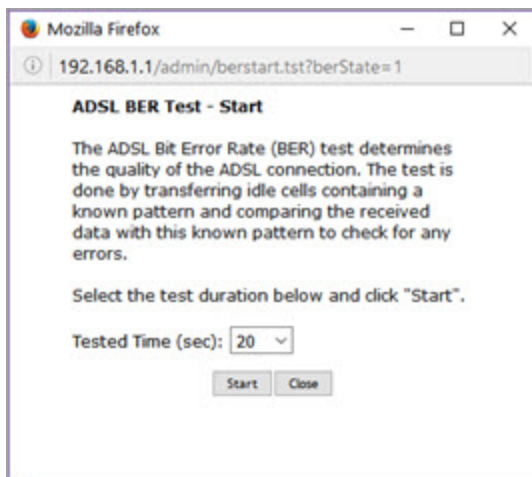
Field Name	Description
Total UAS	<p>Total number of Un-Aavailable Seconds.</p> <p>This is a count of 1-second intervals for which the xDSL line is unavailable. The xDSL line becomes unavailable at the onset of 10 contiguous SESs (included in the unavailable time).</p> <p>Once unavailable, the xDSL line becomes available at the onset of 10 contiguous seconds with no SESs (excluded from unavailable time). [4]</p>

References

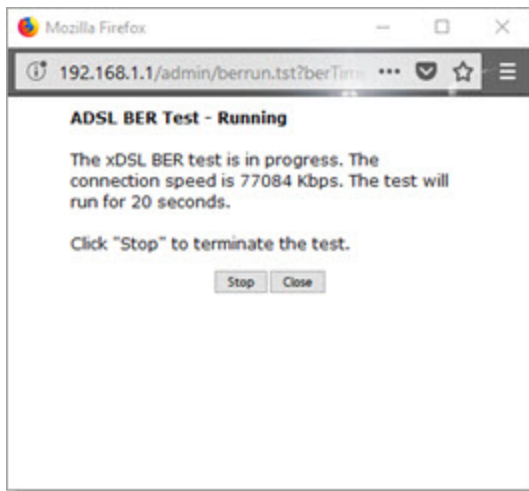
- [1] [ITU-T Recommendation G.992.1 \(1999\), Asymmetric digital subscriber line \(ADSL\) transceivers](#)
- [2] [ITU-T Recommendation G.992.3 \(2005\), Asymmetric digital subscriber line transceivers 2 \(ADSL2\)](#)
- [3] [ITU-T Recommendation G.997.1 \(2006\), Physical layer management for digital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

Running xDSL (BER) tests

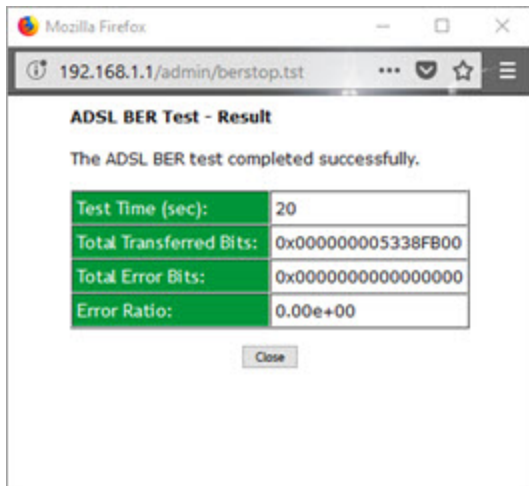
1. Scroll to the bottom of the page and click **xDSL BER Test**. The ADSL BER Test dialog box appears.



2. 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**.



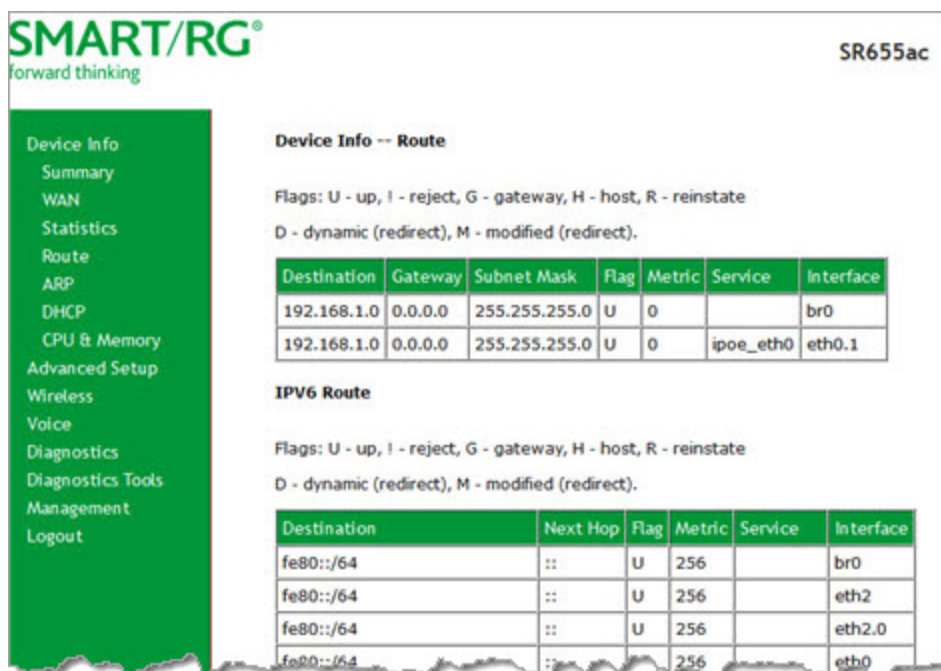
- When the test completes, a success dialog box appears.
Note: If the BER reaches e-5, you cannot access the Internet.



Route

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

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



The fields on this page are defined below.

Field Name	Description
Destination	Destination IP addresses.
Next Hop	(For IPv6 only) Identifies the next server in the IPv6 path, if any.
Gateway	Gateway IP address.
Subnet Mask	Subnet Masks.
Flag	Status of the flags.
Metric	Number of hops to reach the default gateway.
Service	Service type.
Interface	WAN/LAN interface.

ARP

On this page, you can view the MAC address and IP address information for the devices connected to the gateway.

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



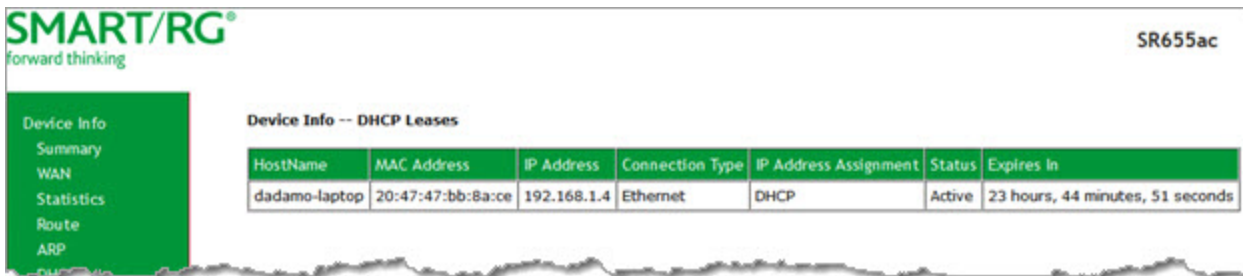
The fields on this page are defined below.

Field Name	Description
IP address	IP address of the host.
Flags	Each entry in the ARP cache is marked with a status flag. Options are Complete , Permanent , and Published .
MAC Address	MAC address of the host.
Device	System level interface by which the host is connected. Options are: br(#) , atm(#) , eth(#) , and ptm(#) .

DHCP

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

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



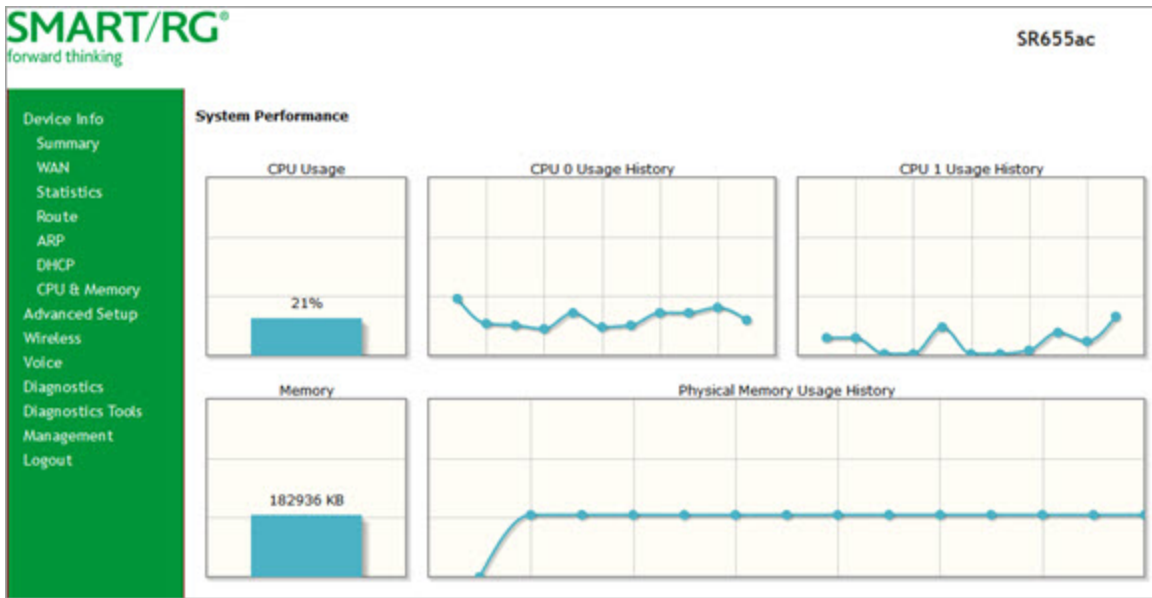
The fields on this page are defined below.

Field Name	Description
Hostname	Host name of each connected LAN device.
MAC Address	MAC address for each connected LAN device.
IP Address	IP address for each connected LAN device.
Connection Type	Type of connection for each LAN devices, such as Ethernet .
IP Address Assignment	Type of IP address assignment, such as DHCP .
Status	Status of the connection. Options are Active and Inactive .
Expires In	Time until the DHCP lease expires for each LAN device.

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, UPnP, quality of service, and other features.

Layer2 Interface

In this section, you can configure the network interfaces for your gateway.

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 (gateways) on both ends of the connection must support ATM / PVC.

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

2. Modify the settings as needed, using the information in the table below.
3. Click **Apply/Save** to commit your changes. The new interface appears on the DSL ATM Interface Configuration page.
4. To remove an interface, click the **Remove** checkbox next to it and then click the **Remove** button.

The fields on this page are defined below.

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 zero (0) .

Field Name	Description
VCI	<p>Enter a Virtual Channel Identifier. A VCI is a 16-bit identifier for a unique channel. Options are 32-65535. The default is 35.</p> <p>Note: 1-31 are reserved for known protocols.</p>
Select DSL Latency	<p>Select the level of DSL latency. Options are:</p> <ul style="list-style-type: none"> • Path0 (Fast): No error correction and can provide lower latency on error-free lines. This is the default. • Path1 (Interleaved): Error checking that provides error-free data which increases latency.
Select DSL Link Type	<p>Select the linking protocol. Options are:</p> <ul style="list-style-type: none"> • EoA: Ethernet over ATM, used for PPPoE, IPoE, and Bridge. This is the default. • PPPoA: Point-to-Point Protocol over ATM. • IPoA: Internet Protocol over ATM.
Encapsulation Mode	<p>Select whether multiple protocols or only one protocol is carried per PVC (Permanent Virtual Circuit). Options are:</p> <ul style="list-style-type: none"> • LLC/ENCAPSULATION: <i>(Available for PPPoA only)</i> Logical Link Control (LLC) encapsulation protocols used with multiple PVCs • LLC/SNAP-BRIDGING: <i>(Available for EoA only)</i> Logical Link Control used to carry multiple protocols in a single PVC. • LLC/SNAP-ROUTING: <i>(Available for IPoA only)</i> 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	<p>Select the bit rate protocol. Options are:</p> <ul style="list-style-type: none"> • UBR without PCR: Unspecified Bit Rate with no Peak Cell Rate, flow control or time synchronization between the traffic source and destination. Commonly used with applications that can tolerate data / packet loss. • UBR with PCR: Same as above but with a Peak Cell Rate. • CBR: Constant Bit Rate relies on timing synchronization to make the network traffic predictable. Used commonly in Video and Audio traffic network applications. • Non Realtime VBR: Non Realtime Variable Bit Rate used for connections that transport traffic at a variable rate. This category requires a guaranteed bandwidth and latency. It does not rely on timing synchronization between the destination and source. • Realtime VBR: Realtime Variable Bit Rate. Same as the above option but relies on timing and synchronization between the destination and source. This category is commonly used in networks with compressed video traffic.
Minimum Cell Rate	<p>Enter the number of cells per second for applying shaping. Options are 1 - 0. The default is -1 (no shaping).</p>

Field Name	Description
Select Scheduler for Queues of Equal Precedence as the Default Queue	<p>Select the algorithm used to schedule queue behavior. VC scheduling is different than scheduling done for default queues. Options are:</p> <ul style="list-style-type: none"> • Weighted Round Robin: Packets are accessed in a round robin style and classes can be assigned. Time slices are assigned to each process in equal portions and in circular order, handling all processes without priority (also known as cyclic executive). This is the default. • Weighted Fair Queuing: Packets are assigned in a specific queue. This data packet scheduling technique allows different scheduling priorities to be assigned to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (that sent larger packets or more packets per second than the others since it became active) will only affect itself and not other sessions.
Default Queue Weight	Enter the default weight of the specified queue. Options are 1-63 . The default is 1 .
Default Queue Precedence	Enter the precedence of the specified group. The lower the value, the higher the priority. 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

SmartRG gateway follow VDSL2 standards to 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).

On this page, you can configure PTM WAN interfaces.

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

2. Modify the settings as desired, using the information in the table below.
3. Click **Apply/Save** to commit your changes. The new interface appears on the PTM Configuration page.
4. To remove an interface, click the **Remove** checkbox next to it and then click the **Remove** button.

The fields on this page are defined below.

Field Name	Description
Select DSL Latency	<p>Select the level of DSL latency. Options are:</p> <ul style="list-style-type: none"> • Path0 (Fast): No error correction and can provide lower latency on error-free lines. This is the default. • Path1 (Interleaved): Error checking that provides error-free data which increases latency.
Select Scheduler for Queues of Equal Precedence as the Default Queue	<p>Select the algorithm used to schedule queue behavior. VC scheduling is different than scheduling done for default queues. Options are:</p> <ul style="list-style-type: none"> • Weighted Round Robin: Packets are accessed in a round robin style and classes can be assigned. Time slices are assigned to each process in equal portions and in circular order, handling all processes without priority (also known as cyclic executive). This is the default. • Weighted Fair Queuing: Packets are assigned in a specific queue. This data packet scheduling technique allows different scheduling priorities to be assigned to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (that sent larger packets or more packets per second than the others since it became active) will only affect itself and not other sessions.

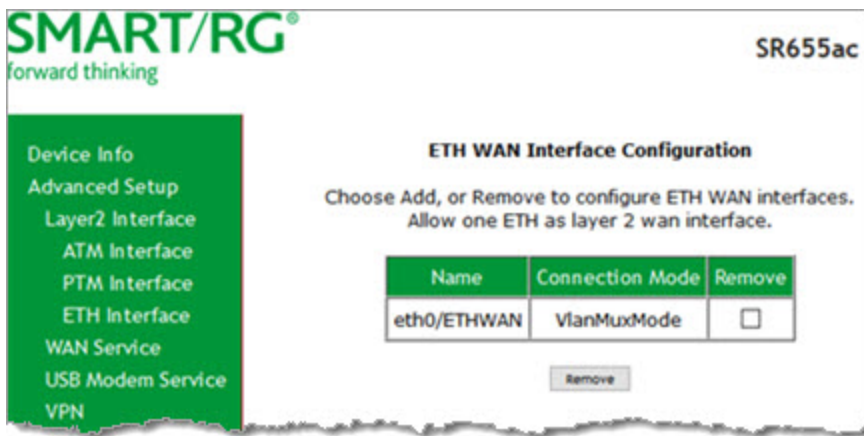
Field Name	Description
Default Queue Weight	Enter the default weight of the specified queue. Options are 1-63. The default is 1.
Default Queue Precedence	Enter the precedence of the specified group. The lower the value, the higher the priority. Options are 1-8. The default is 8.
Default Queue Minimum Rate	Enter the default minimum rate at which traffic can pass through the queue. Options are 1-0 Kbps. The default is -1 (no shaping).
Default Queue Shaping Rate	Enter the shaping rate for the specified queue. Options are 1-0 Kbps. The default is -1 (no shaping).
Default Queue Shaping Burst Rate	Enter the maximum rate at which traffic can pass through the queue. Options are 1600 bytes or greater. The default is 3000 bytes.

ETH Interface

On this page, you can configure ETH WAN interfaces. One of the four LAN ports on your gateway can be re-purposed to become an RJ45 WAN port when needed. !!! ASKSME: Can one of the LAN ports be repurposed on the 555 & 655?

Notes:

- Only one Ethernet WAN interface is allowed. If a WAN port it is already configured, you must remove it before you can define a new one. Click the **Remove** checkbox and then click the **Remove** button. The **Add** button appears when the existing port is removed.
 - If a WAN port is already configured and associated with a WAN service, you must remove the WAN service configuration before you can remove the port on this page.
- In the left navigation bar, click **Advanced Setup > Layer2 Interface > ETH Interface**. The following page appears.

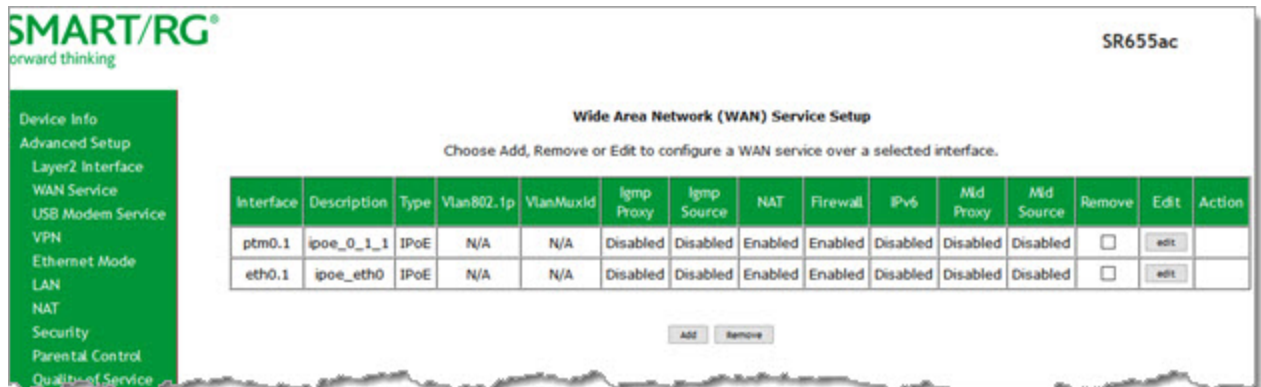


- Select the LAN port you want to use as a WAN port.
- Click **Apply/Save** to commit your changes. The interface is added to the ETH WAN Interface Configuration page.
- To remove an entry, click the **Remove** checkbox next to the entry and then click the **Remove** button.

WAN Service

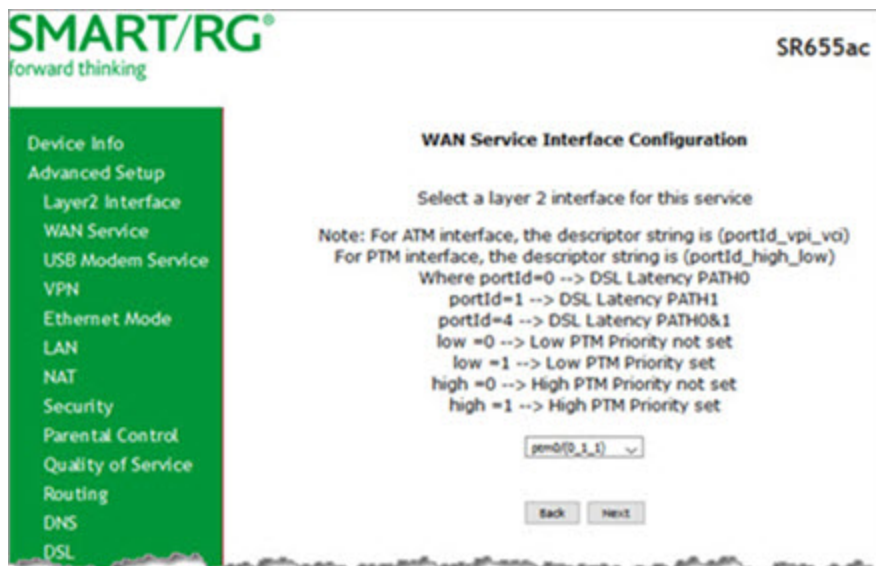
On this page, you can add, remove, or edit a WAN service. You must configure the related interface (ATM, ETH or PTM) first. You can configure services for PPPoE, IPoE, and Bridging. A sample configuration scenario is provided for each variation.

1. In the left navigation, click **Advanced Setup > WAN Service**. The following page appears, showing the services already configured.



!!!

2. To add a service, click **Add**. The following page appears.



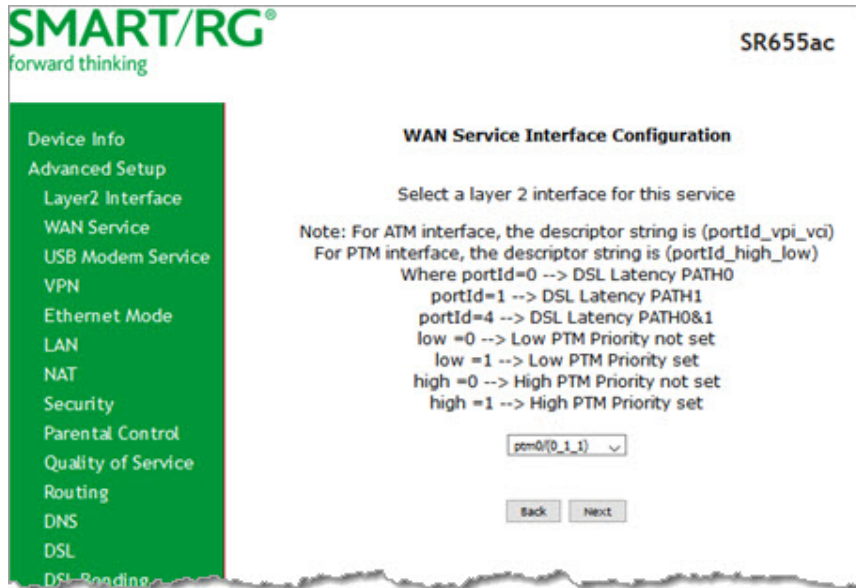
3. Modify the settings as desired, using the information in the topics listed below:
 - "PPP over Ethernet WAN Service"
 - "IP over Ethernet WAN Service"
 - "Bridging"
4. To edit an interface:
 - a. Click the **Edit** button at the far right.
 - b. Modify the settings as needed and then click through to click **Apply/Save**.
5. To remove an interface, click the **Remove** checkbox next to it and then click the **Remove** button.

PPP over Ethernet WAN Service

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

Note: You can configure 7 services. If 7 services are configured, you must remove 1 of the services before configuring a new one.

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



SMART/RG®
forward thinking

SR655ac

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

pcm0/(0_1_1) ▾

Back Next

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

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

SMART/RG® forward thinking SR655ac

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
ETH Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP

WAN Service Configuration

Select WAN service type:
☒ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☐ Bridging

Enter Service Description:

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.

Enter 802.1P Priority [0-7]:
Enter 802.1Q VLAN ID [0-4094]:
Network Protocol Selection:


Back Next

4. In the **WAN Service Type** field, accept the default of **PPP over Ethernet (PPPoE)**.
5. (Optional) Modify the other fields, using the information in the following table.

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

Field Name	Description
Network Protocol Selection	<p>Different scheduling priorities can be applied to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (which has sent larger packets or more packets per second than the others) will only punish itself and not other sessions. Options are IPv4 Only, IPv4&IPv6 (Dual Stack), and IPv6 Only.</p> <p>Note: When you select IPv4&IPv6 or IPv6, the options presented on later pages change accordingly.</p>

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


forward thinking

SR655ac

Device Info

Advanced Setup

Layer2 Interface

WAN Service

USB Modem Service

VPN

Ethernet Mode

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DSL

DSL Bonding

UPnP

DNS Proxy

Print Server

DLNA

Storage Service

Interface Grouping

IP Tunnel

IPSec

Certificate

Power Management

Multicast

Wireless

VoIP

Diagnostics

Diagnostics Tools

Management

Logout

PPP Username and Password

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

PPP Username:
 PPP Password:
 PPPoE Service Name:
 Authentication Method: AUTO ▼
 MTU[576-1492]:

☒ Enable KeepAlive
 LCP Echo Interval[1-60]: seconds
 LCP Echo Failure[1-100]: times

☒ Enable NAT
☐ Enable Fullcone NAT
☐ Enable MAC Clone
☒ Enable Firewall

☐ Dial on demand (with idle timeout timer)
☐ PPP IP extension
☐ Use Static IPv4 Address
☒ Retry PPP password on authentication error

Max PPP authentication retries(1-65536): (use 65536 to retry forever)

☐ Enable IPv6 Unnumbered Model
☐ Launch Dhcp6c for Address Assignment (IANA)
☒ Launch Dhcp6c for Prefix Delegation (IAPD)
☐ Enable PPP Debug Mode
☐ Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

☐ Enable IGMP Multicast Proxy
☐ Enable IGMP Multicast Source

MLD Multicast

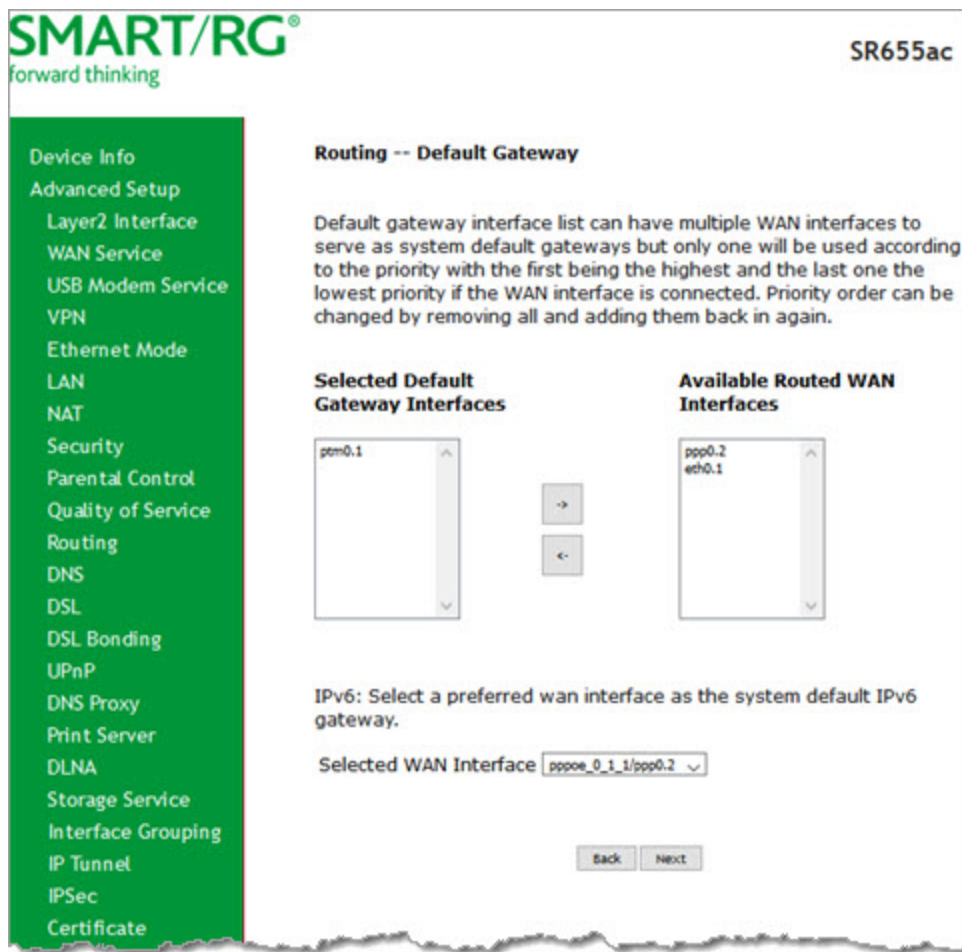
☐ Enable MLD Multicast Proxy
☐ Enable MLD Multicast Source

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

Field Name	Description
PPP Username	Enter the username required for authentication to the PPP server.
PPP Password	Enter the password required for authentication to the PPP server.
PPPoE Service Name	(Optional) Enter a description for this service.
Authentication Method	<p>Select a means for authentication. Options are:</p> <ul style="list-style-type: none"> • AUTO: Attempt to automatically detect the handshake protocol (listed below). • 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).
MTU [576-1492]	Enter the MTU (Maximum Transmission Unit) size. Options are 576 - 1492 bytes . The default is 1492 bytes .
Enable KeepAlive	<p>This option is enabled by default. To disable keepalive packets, clear the checkbox. Enter values in the following fields:</p> <ul style="list-style-type: none"> • LCP Echo Interval [1-60]: Enter the interval for sending echos in seconds. The default is 30 seconds. • LCP Echo Failure [1-100]: Enter the number of times that echos should be sent before reporting echo failure. The default is 5 times.
Enable NAT	This option is enabled by default. To disable NAT (Network Address Translation), clear the checkbox.
Enable Fullcone NAT	<p>Click to enable "one-to-one" NAT. All requests from the same internal IP address and port are mapped to the same external IP address and port. In addition, any external host can send a packet to the internal host by sending a packet to the mapped external address.</p> <p>Warning: Enabling this option will disable network acceleration and some security settings.</p>
Enable MAC Clone	<p>Click to enable MAC cloning. Additional fields appear. Options are:</p> <ul style="list-style-type: none"> • Enter the MAC address that you want to clone. • To use the MAC address of the connected PC, click Clone the PC MAC Address.
Enable Firewall	This option is enabled by default. To disable the firewall, clear the checkbox.

Field Name	Description
Dial on Demand	<p>Click to enable dialing on-demand. The Inactivity Timeout (minutes) field appears. Enter the of minutes before a session is timed out. Options are 1 - 4320. The default is zero (0).</p> <p>When this option is enabled, connection automatically starts when there is outbound traffic to the Internet. It automatically terminates if the connection is idle, based on the value in the Idle Timeout setting.</p>
PPP IP Extension	Click to forward all traffic to the specified DMZ IP. When you select this option, the NAT and Firewall fields are hidden.
Use Static IPv4 Address	Click to use the IPv4 Address associated with this WAN service. The IPv4Address field appears. Enter the static IPv4 address for this WAN service.
Retry PPP password on authentication error	<p>This option is enabled by default. In the Max PPP authentication retries (1-65536) field, enter the number of tries allowed. The default is 65536 (unlimited tries).</p> <p>To prevent retrying the PPP password after authentication errors, clear the checkbox.</p>
Enable IPv6 Unnumbered Model	Click to enable IP processing on a serial interface without assigning it an explicit IP address. The IP address of another interface can be can "borrow" the IP address of another interface already configured on the router, which conserves network and address space.
Launch Dhcp6c for Address Assignment (IANA)	<i>(Available only for IPv6 environments)</i> Click to enable the gateway to receive the WAN IP from the ISP.
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 disable this options, clear the checkbox.
Enable PPP Debug Mode	Click to have the system put more PPP connection information into the system log of the device. This is for debugging errors and not for normal usage.
Bridge PPPoE Frames Between WAN and Local Ports	Select to enable PPPoE passthrough to relay PPPoE connections from behind the modem. Also known as Half-Bridged mode.
Enable IGMP Multicast Proxy	Click to enable Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable IGMP Multicast Source	Click to enable this service to act as an IGMP multicast source.
Enable MLD Multicast Proxy	<i>(Available only for IPv6 environments)</i> Click to enable MLD multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable MLD Multicast Source	<i>(Available only for IPv6 environments)</i> Click to enable this service to act as an MLD multicast source.

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



9. Click the **arrows** to move your selections from left to right or from right to left.
10. (Optional) For IPv6 environments, in the **Selected WAN Interface** field, select the preferred WAN interface for the default IPv6 gateway.

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

SMART/RG®
forward thinking

SR655ac

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 to serve as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces	Available WAN Interfaces
ppp0.1	ppp0.2 eth0.1

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information. 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:

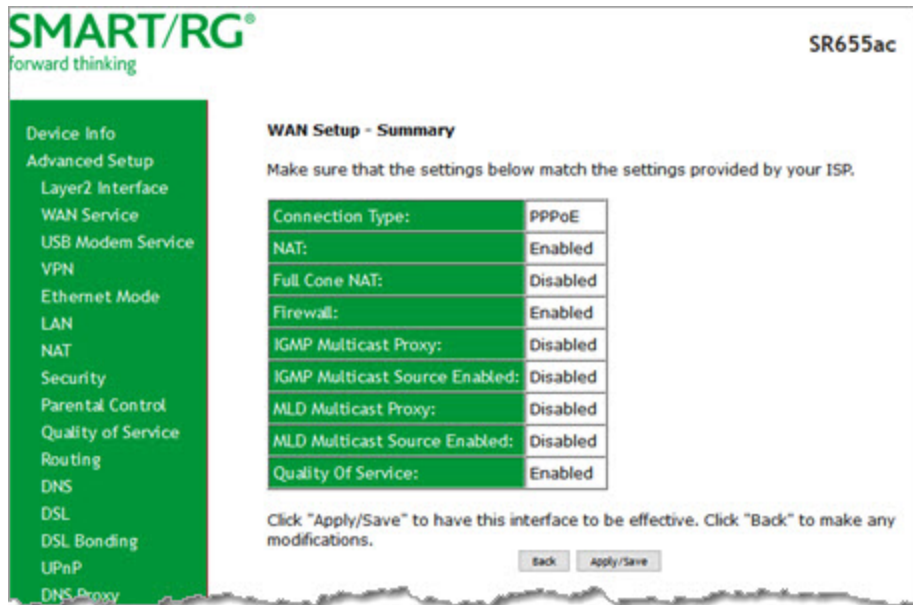
☐ **Use the following Static IPv6 DNS address:**

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

- 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.
13. Click [Next](#). The summary page appears indicating that your PPPoE WAN setup is complete.



SMART/RG®
forward thinking

SR655ac

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy

14. 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 WAN Service

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

Before you can configure a WAN service, make sure that the related Layer2 Interface has been configured.

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

SMART/RG®
forward thinking

SR655ac

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0(0_1_1) v

Back Next

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

SMART/RG®
forward thinking

SR655ac

WAN Service Configuration

Select WAN service type:

☒ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☐ Bridging

Enter Service Description: pppoe_0_0_35

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocol Selection:
IPv4 Only v

Back Next

3. Select **IP over Ethernet**.

4. Modify the other fields as needed, using the information in the following table.

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

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

SMART/RG® SR655ac
forward thinking

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix Length and interface gateway.

☒ Obtain an IP address automatically

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Option 55 Request List : (e.g:1,3,6,12)

Option 58 Renewal Time: (hour)

Option 59 Rebinding Time: (hour)

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 77 User ID:

Option 125: ☒ Disable ☐ Enable

☐ Use the following Static IP address

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Primary DNS server:

Secondary DNS server:

☐ Enable MAC Clone

- Enter the relevant WAN IP Settings, using the information provided in the table below.

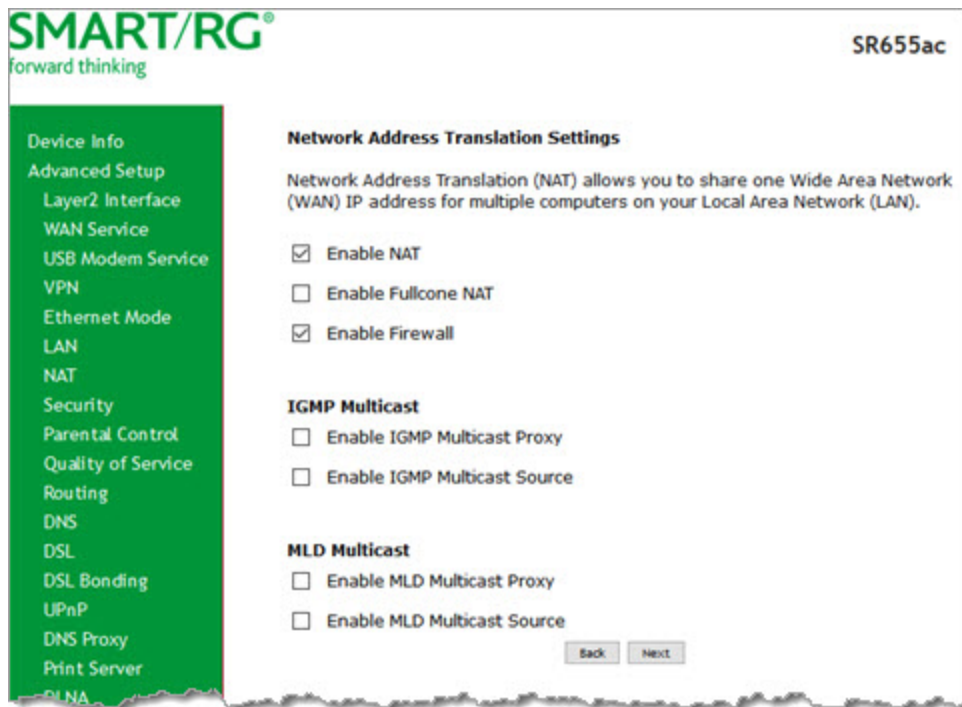
The fields on this page are defined below.

Field Name	Description
Obtain an IP address automatically	This option is selected by default. DHCP is enabled in MER mode. Click to prevent the ISP automatically assigning the WAN IP to the gateway.
Option 50 Request IP Address	Enter the IP address to be used when sending messages. If the specified address is not available, the DHCP server assigns the next allowed IP address.
Option 51 Request Leased Time	Enter the maximum lease time defined for the client. The default is zero (0) .
Option 54 Request Server Address	Enter the IP address of the source server.
Option 55 Request List	Enter the configuration parameter numbers, separated by commas.

Field Name	Description
Option 58 Renewal Time	Enter the number of hours before the DHCP client begins to renew its address lease with the DHCP server.
Option 59 Rebinding Time	Enter the number of hours before the DHCP client enters the rebinding state if it has not renewed its current address lease with the DHCP server.
Option 60 Vendor ID	(Optional) Enter the vendor ID to broadcast so the DHCP server can accept the device.
Option 61 IAID	(Optional) Enter the Interface Association Identifier (IAID). This is a unique identifier for an IA, chosen by the client.
Option 61 DUID	(Optional) Enter the DHCP Unique Identifier (DUID) is used by the client to get an IP address from the DHCP server.
Option 77 User ID	(Optional) Enter the user class ID that should be used to filter traffic.
Option 125	(Optional) Select whether local devices can automatically receive DHCP options from the server. The default is Disable .
Use the following Static IP address	Click to manually declare the static IP information provided by your ISP. When you select this option, you must enter the WAN IP address, subnet mask and gateway IP address.
WAN IP Address	(Available only when Static IP address is selected) Enter the static WAN IPV4 Address.
WAN Subnet Mask	(Available only when Static IP address is selected) Enter the static Subnet Mask.
WAN gateway IP Address	(Available only when Static IP address is selected) Enter the static Gateway IP address.
Primary DNS Server	(Available only when Static IP address is selected) (Optional) Enter the IP address of the primary DNS server.
Secondary DNS Server	(Available only when Static IP address is selected) (Optional) Enter the IP address of the secondary DNS server.
IPv6 settings section	
The following fields appear when either IPv6 Only or IPv4&IPv6 (Dual Stack) is selected in the Network Protocol Selection field on the WAN Service Configuration page.	
Obtain an IPv6 address automatically	This option is set to enabled by default and allows the ISP to automatically assign the WAN IP address to the gateway. To disable the DHCPv6 Client on this WAN interface, click the radio button.
Dhcpv6 Address Assignment (IANA)	Select this option for the CPE to receive the WAN IP from the ISP.
Dhcpv6 Prefix Delegation (IAPD)	This option is selected by default. The CPE generates the WAN IP's prefix from the server's REST by MAC address. To disable this option, clear the checkbox.

Field Name	Description
Use the following Static IPv6 address	Select this option to manually declare the v6 Static IP information provided by your ISP.
WAN IPv6 Address/Prefix Length	(Available only when Static IPv6 address is selected) 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.
Prefix Delegation/Prefix Length	(Available only when Static IPv6 address is selected) (Optional) Enter the prefix delegation ID and prefix length for WAN.
WAN Next-Hop IPv6 address	(Available only when Static IPv6 address is selected) 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.
Enable MAC Clone	(Available for IPv4-only or IPv4-IPv6 Dual Stack environments) Select to enable MAC cloning; then enter the MAC address that you want to clone. To use the MAC address of the connected PC, click Clone the PC MAC Address . To use a dynamic MAC address, leave this field as-is.

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



8. Modify the settings as needed for your environment.
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple

computers on your Local Area Network (LAN). If you do not want to enable NAT (atypical) and wish the user of this gateway to access the Internet normally, you need to add a route on the uplink equipment. Failure to do so will cause access to the Internet to fail.

The fields on this page are defined below.

FIELD NAME	DESCRIPTION
Enable NAT	This option is selected by default. Click to disable sharing the WAN interface across multiple devices on the LAN. This setting also enables the functions in the NAT sub-menu and addition PPPoE NAT features to select.
Enable Fullcone NAT	Click to enable one-to-one NAT. All requests from the same internal IP address and port are mapped to the same external IP address and port. In addition, any external host can send a packet to the internal host by sending a packet to the mapped external address. Warning: Enabling this option will disable network acceleration and some security settings.
Enable Firewall	This option is selected by default. Click to disable functions in the Security sub-menu.
Enable IGMP Multicast Proxy	Select to enable Internet Group Membership Protocol (IGMP) multicast. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable IGMP Multicast Source	Select to enable this service to act as an IGMP multicast source.
Enable MLD Multicast Proxy	Click to enable multicast filtering. Used by IPv4 hosts to report multicast group memberships to any neighboring multicast routers.
Enable MLD Multicast Source	Select to enable this service to act as a multicast source.

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

SMART/RG®
forward thinking

SR655ac

Routing -- Default Gateway

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

Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

atm0.1
eth0.1
ppp0.2

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: ipoe_0_35/atm0.1

Back Next

- Select a WAN interface to act as the system default gateway or accept the default interface.
- (Optional) For IPv6 environments, in the **Selected WAN Interface** field, select the preferred WAN interface for the default IPv6 gateway.

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

SMART/RG®
forward thinking

SR655ac

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 to serve as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces	Available WAN Interfaces
<p>ptm0.1</p>	<p>atm0.1 eth0.1 ppp0.2</p>

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information. 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:

☐ **Use the following Static IPv6 DNS address:**

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

- Modify the settings as needed.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Print Server

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

15. Review the IPoE settings. You can modify the settings by clicking the **Back** button.
16. Click **Apply/Save** to save and apply the settings.

Bridging

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

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

SMART/RG®
forward thinking

SR655ac

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

ptm0(0_1_1) v

Back Next

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

SMART/RG®
forward thinking

SR655ac

WAN Service Configuration

Select WAN service type:

☐ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☒ Bridging

☐ Allow as IGMP Multicast Source
☐ Allow as MLD Multicast Source

Enter Service Description: br_0_0_35

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1

Back Next

3. Select **Bridging**. Multicast source fields appear.

4. Modify the other fields as needed, using the information in the following table.

Field Name	Description
Allow as IGMP Multicast Source	Select to enable this service to act as an IGMP multicast source.
Allow as MLD Multicast Source	Select to enable this service to act as an MLD multicast source.
Enter Service Description	(Optional) Enter a different 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 (disabled) in this field and in 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, accept the default of -1 (disabled) in this field and in the 802.1P Priority field.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Print Service

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

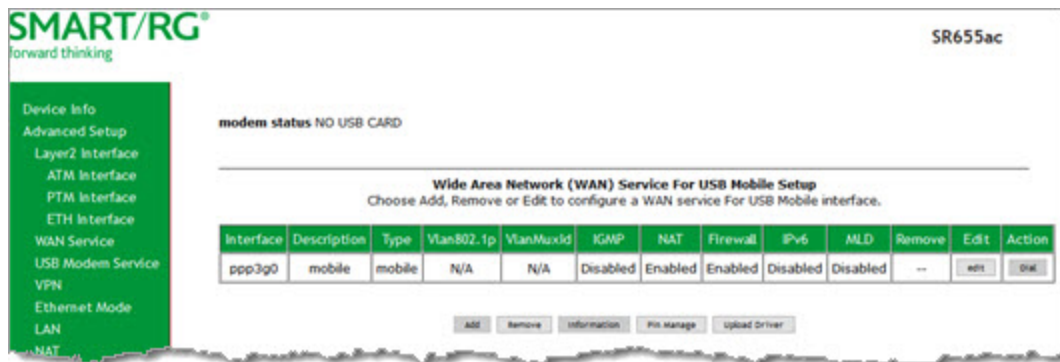
- Review the summary and either click **Apply/Save** to commit your changes or click **Back** to step through the pages in reverse order to make any necessary alterations.

USB Mobile Service

On this page, you can configure a USB Mobile interface for your gateway. A WWAN (Wireless WAN) card must be connected to a USB port on your gateway and you can only configure one connection at a time.

Note: When there is no DSL WAN connection, you can insert the WWAN network card, and the system will perform dial-up automatically. If the DSL WAN connection and the WWAN connection both exist, the DSL WAN connection takes priority over the 3G connection. When the DSL WAN connection starts to perform dial-up, the WWAN connection will be disconnected. If the DSL WAN connection has established, you can manually perform dial-up. The DSL WAN connection will be disconnected.

- Connect the WWAN network card to a USB port on the gateway.
- In the left navigation menu, click **Advanced Setup** > **USB WAN Service**. The following page appears.



- To add a connection:
 - If a connection is already defined, you must remove it before you can a new one. Click the **Remove** button. The page refreshes.

- b. Click **Add**. The following page appears.

- c. Fill in the fields, using the information provided in the table below. You can also click the **Auto Setting** button to automatically configure the 3G connection.

Field Name	Description
Support NDIS	This option is enabled by default. It enables the USB modem for accessing the Internet via the 3G network card.
DHCP	(Appears when you select Support NDIS) Click to enable DHCP connection. When you click this check box, the Dial on Demand check box is hidden.
User Name	Enter the user name provided by your 3G ISP.
Password	Enter the password provided by your 3G ISP.
Authentication Method	Select the appropriate authentication method. Options are AUTO , PAP , CHAP , and MSCHAP . The default is AUTO .
APN	Enter the APN (Access Point Name) provided by your 3G ISP.

Field Name	Description
Dial Number	Enter the dial number provided by your 3G ISP.
Net Select	Select an available 3G network. Options are EVDO , WCDMA , CDMA2000 , TD-SCDMA , GSM , LTE , and AUTO . The default is AUTO .
Dial on demand	Select to enable dial on demand feature. If the gateway does not detect data flow continuously within the designated time limit, the gateway automatically stops the 3G connection. Once data flow is detected again, the 3G dialup is restarted. Note: This field is not available when the DHCP option is selected.
Idle time (in sec)	<i>(Appears when Dial on demand is selected)</i> Enter the number of seconds that the gateway should wait before disconnecting. The default is 360 seconds (6 minutes).
Dial Delay (in sec)	The number of seconds that the 3G connection waits to dial after the DSL is disconnected. The default is 10 seconds .
Default WAN Connection Select	Select the default WAN connection. Options are 3G and DSL OR ETHERNET . The default is DSL OR ETHERNET .
WAN backup mechanism	Click to define how this connection is used as backup for the DSL connection. Options are: <ul style="list-style-type: none"> • DSL: If the DSL is disconnected, the 3G starts to dial. This is the default. • IP connectivity: If the system fails to ping the specified IP address, the 3G starts to dial.
Checking IP address	<i>(Appears when IP connectivity is selected in WAN backup mechanism)</i> Enter the IP address to be used as the WAN backup.
Period time (in sec)	<i>(Appears when IP connectivity is selected in WAN backup mechanism)</i> Enter the length (in seconds) of downtime before WAN backup is activated. The default is 10 seconds .
Timeout (in sec.)	<i>(Appears when IP connectivity is selected in WAN backup mechanism)</i> Enter the length of time (in seconds) before the login attempt times out. The default is 5 seconds .
Fail Tolerance	<i>(Appears when IP connectivity is selected in WAN backup mechanism)</i> Enter the maximum number of failed access attempts allowed. The default is 3 attempts .

- d. Click **Apply/Save** to implement your changes. You are returned to the USB Modem Service setup page.
4. To view information about the 3G network card, click **Information**. The information appears on the page.
5. To dial or disconnect a connection, click the button in the **Action** column.

6. To edit a connection:
 - a. Click the button in the **Edit** column. The setup page for the connection appears.
 - b. Modify the fields as necessary, using the information in the table below. You can also click **Auto Setting** to use the default configuration.
 - c. Click **Apply/Save**. You are returned to the 3G Wan Service page.
7. To remove the existing connection, click **Remove**. The connection is removed and you can add a new one.
8. To manage the PIN configuration:
 - a. Click **PIN Manage**. The following page appears.

- b. Complete the fields as necessary, using the information in the field description table below.

Field Name	Description
Enable PIN protect	If you enable this option, you must enter the PIN code when rebooting or inserting the USB network card.
Unlock with PIN code	If you disable this option, you must to enter the PIN code when using 3G.
Unlock with PUK & PIN	If you disable this option, you must enter the PUK code after failing to enter the PIN code correctly 3 times.
Change PIN code	Click to change the PIN code.

- c. Click **Submit** to save your changes.
9. To upload a driver file, click **Upload Driver**. The Tools page appears. Click **Browse** to select a driver file and then click **Update Settings**.
10. When your changes are completed, click **Submit** to implement them.

VPN

In this section, you can configure tunneling protocols (L2TP or PPTP clients) for your network. The settings are usually specific to a customer's ISP.

L2TP Client Configuration

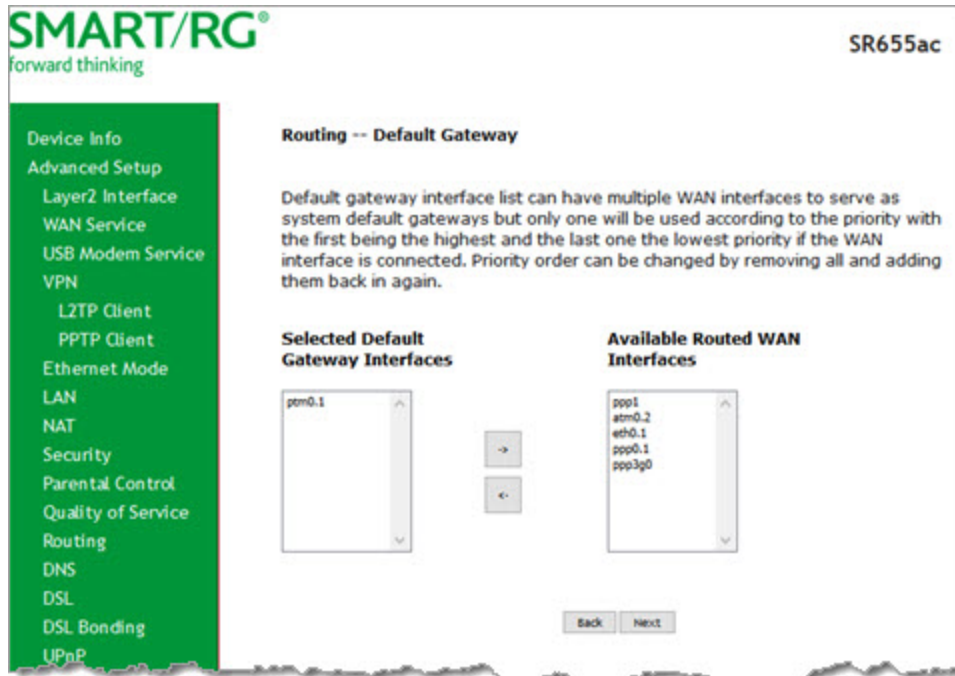
On this page, you can configure the L2TP (Layer 2 Tunneling Protocol) client.

1. In the left navigation menu, click **Advanced Setup** > **VPN** and then click **Add**. The following page appears.

2. Fill in the fields, using the information in the table below.

Field Name	Description
Description	Enter a useful description of this configuration.
WAN Interface	Select the WAN interface for this client.
L2TP Server IP/Domain	Enter the IP address of the L2TP server.
L2TP Username	Enter the user name for the server.
L2TP Password	Enter the password for the server.
Authentication	Select the authentication method. Options are NOAUTH, AUTO, PAP, CHAP, MS-CHAP_V1, and MS-CHAP_V2. The default is AUTO.
Enable MPPE	(Optional) Click to enable Microsoft Point-to-Point Encryption.
MTU	(Optional) Enter the maximum number of transmission units allowed for this client. Options are 1 - 1454. The default is 1454.
Enable NAT	(Optional) Click to enable Network Address Translation features.
Enable Firewall (SPI)	(Optional) Click to enable the firewall.
Enable	Click to enable this L2TP client configuration.

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



4. Select the default gateway by selecting interface entries and clicking the **arrows** to move the entries right or left.

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

SMART/RG® SR655ac
forward thinking

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 to serve as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces	Available WAN Interfaces
ppm0.1	ppp1 atm0.2 eth0.1 ppp0.1 ppp3g0

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Back Next

- Do one of the following to configure the DNS server:
 - Select the DNS server interface by selecting interface entries and clicking the **arrows** to move the entries right or left.
 - Click **Use the following Static DNS IP address** and enter the DNS server IP addresses.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
L2TP Client
PPTP Client
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL

L2TP Client Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPN Type:	L2TP
Server IP/Domain:	192.168.1.24
Authentication:	AUTO_AUTH
MPPE:	Disabled
MTU:	1454
NAT:	Disabled
Firewall:	Disabled
Enable:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

- Click **Apply / Save** to implement your settings.

PPTP Client

On this page, you can configure the PPTP (Point-to-Point Tunneling Protocol) client.

- In the left navigation menu, click **Advanced Setup > VPN > PPTP Client** and then click **Add**. The following page appears.

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
L2TP Client
PPTP Client
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service

PPTP Client Configuration (Point-to-Point Tunneling Protocol)

Description:

WAN Interface:

PPTP Server IP/Domain:

PPTP Username:

PPTP Password:

Authentication:

☐ Enable MPPE (Microsoft Point-to-Point Encryption)

MTU [576-1454]: Maximum Transmission Unit

☐ Enable NAT

☐ Enable Firewall (SPI)

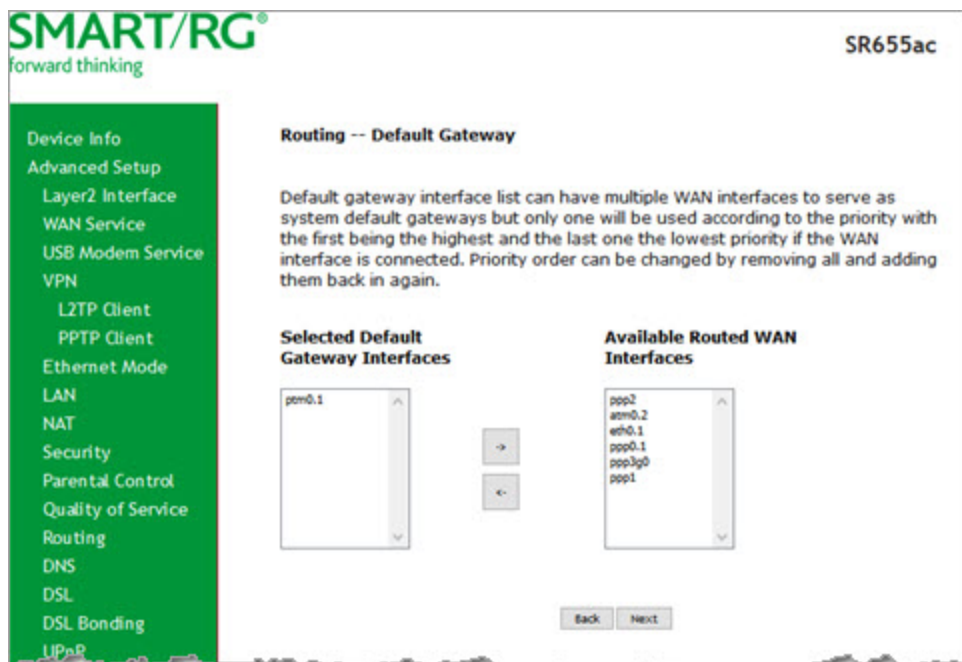
☐ Enable

Back Next

- Fill in the fields, using the information in the table below. The **Description**, **WAN Interface**, and **PPTP Server IP/Domain** fields are required.

Field Name	Description
Description	Enter a useful description of this configuration.
WAN Interface	Select the WAN interface for this client.
PPTP Server IP/Domain	Enter the IP address of the PPTP server.
PPTP Username	If not using the default of "admin", enter the user name for the server.
PPTP Password	If not using the default of "admin", enter the password for the server.
Authentication	Select the authentication method. Options are NOAUTH, AUTO, PAP, CHAP, MS-CHAP_V1, and MS-CHAP_V2.
Enable MPPE	(Optional) Select to enable Microsoft Point-to-Point Encryption.
MTU	(Optional) Enter the maximum number of transmission units allowed for this client. Options are 1-1454. The default is 1454.
Enable NAT	(Optional) Select to enable Network Address Translation features.
Enable Firewall (SPI)	(Optional) Select to enable the firewall.
Enable	Click to enable this PPTP client configuration.

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



- Select the default gateway by selecting interface entries and clicking the **arrows** to move the entries right or left.

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

SMART/RG®
forward thinking

SR655ac

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 to serve as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

☒ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces	Available WAN Interfaces
ppm0.1	ppp2 atm0.2 eth0.1 ppp0.1 ppp3g0 ppp1

☐ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

- Do one of the following to configure the DNS server:
 - Select the DNS server interface by selecting interface entries and clicking the **arrows** to move the entries right or left.
 - Click **Use the following Static DNS IP address** and enter the DNS server IP addresses.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
L2TP Client
PPTP Client
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS

Make sure that the settings below match the settings provided by your ISP.

VPN Type:	PPTP
Server IP:	192.168.1.25
Authentication:	AUTO_AUTH
MPPE:	Disabled
MTU:	1454
NAT:	Disabled
Firewall:	Disabled
Enable:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

- Click **Apply / Save** to implement your settings.

Ethernet Mode

On this page, you can configure the Ethernet speed for your gateway.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS

Ethernet Speed Configuration

Port	Configure	Current Bit Rate	Duplex Mode	Status
eth0/ETHWAN	Auto	100	Full	Up
eth1/ETH1	Auto	Auto	Auto	Disabled
eth2/ETH2	Auto	1000	Full	Up
eth3/ETH3	Auto	Auto	Auto	Disabled
eth4/ETH4	Auto	Auto	Auto	Disabled

Apply/Save

- To set a specific speed, select it in the **Speed** field.

Options are **Auto**, **100 Full**, **100 Half**, **10 Full**, and **10 Half**. The default is **Auto**.

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

LAN

In this section, you can configure an IP address for the DSL gateway, enable IGMP snooping, enable or disable the DHCP server, edit the DHCP options, configure the DHCP advanced setup, and set the binding between a MAC address and an IP address.

IGMP snooping enables the gateway to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the gateway listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

If you enable the DHCP server, the clients will automatically acquire the IP address from the DHCP server. If the DHCP server is disabled, you need to manually set the start IP address, end IP address and the lease time for the clients in the LAN.

IPv4 Autoconfig

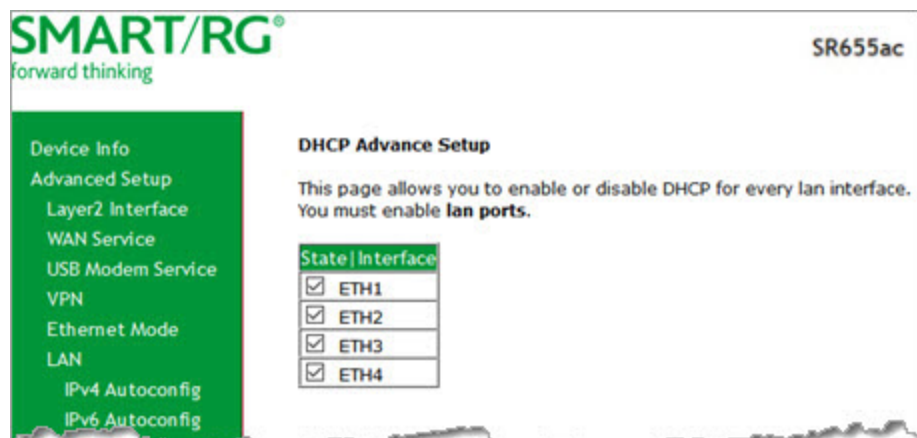
1. In the left navigation menu, click **Advanced Setup > LAN**. The following page appears. You can also reach this page by clicking **Advanced Setup > LAN > IPv4 Autoconfig** in the left menu.

2. (Optional) In the **GroupName** field, select the interface group for this configuration. If there are no groupings defined, the only option is **Default**.
3. Modify the other fields using the information in the following table. The default configuration settings work for most scenarios.

Field	Description
IP Address / Subnet Mask	Modify the IP address and subnet mask of the device. The default IP address is that of the gateway and the subnet mask is 255.255.255.0.

Field	Description
Enable IGMP Snooping	This option is enabled by default. Options are Standard Mode and Blocking Mode . The default is Blocking Mode . To disable this option, clear the check box.
Enable LGMP LAN to LAN Multicast	This option is disabled by default. To enable this option, select Enable .
Enable LAN side firewall	Click to enable the LAN-side firewall.
Disable DHCP Server / Enable DHCP Server	This option is enabled by default. You can modify the address, server and leased time fields as needed. To disable the DHCP server, click Disable DHCP Server . Then, if needed, enter different server information for the LAN.
Edit DHCP Option 60	To modify the vendor class information, click Edit DHCP Option 60 , modify the entries, and then click the appropriate action button. Then click Return .
Edit DHCP Option	To add information about other DHCP options, click Edit DHCP Option , enter the information for the desired options, and then click the appropriate action button. Then click Return .

4. To enable or disable DHCP for individual LAN interfaces:
 - a. Click **DHCP Advanced setup**. The DHCP Advance Setup page appears.



- b. Click the **State** checkboxes as needed to manage DHCP for each LAN interface in the table, and then click **Advanced Setup > LAN > IPv4 Autoconfig**.

5. To add addresses to the **Static IP Lease List**:
 - a. Click **Add Entries** below the **MAC Address** field. The DHCP Static IP Lease page appears.

- b. Enter the MAC address of the LAN host.
 - c. Enter the static IP address that is reserved for the host.
 - d. Click **Apply/Save** to apply the settings. You are returned to the LAN Setup page.
6. To remove entries from the **Static IP Lease List**, click the **Remove** check box next to the entry and then click **Remove Entries**.
7. To add OUIs:

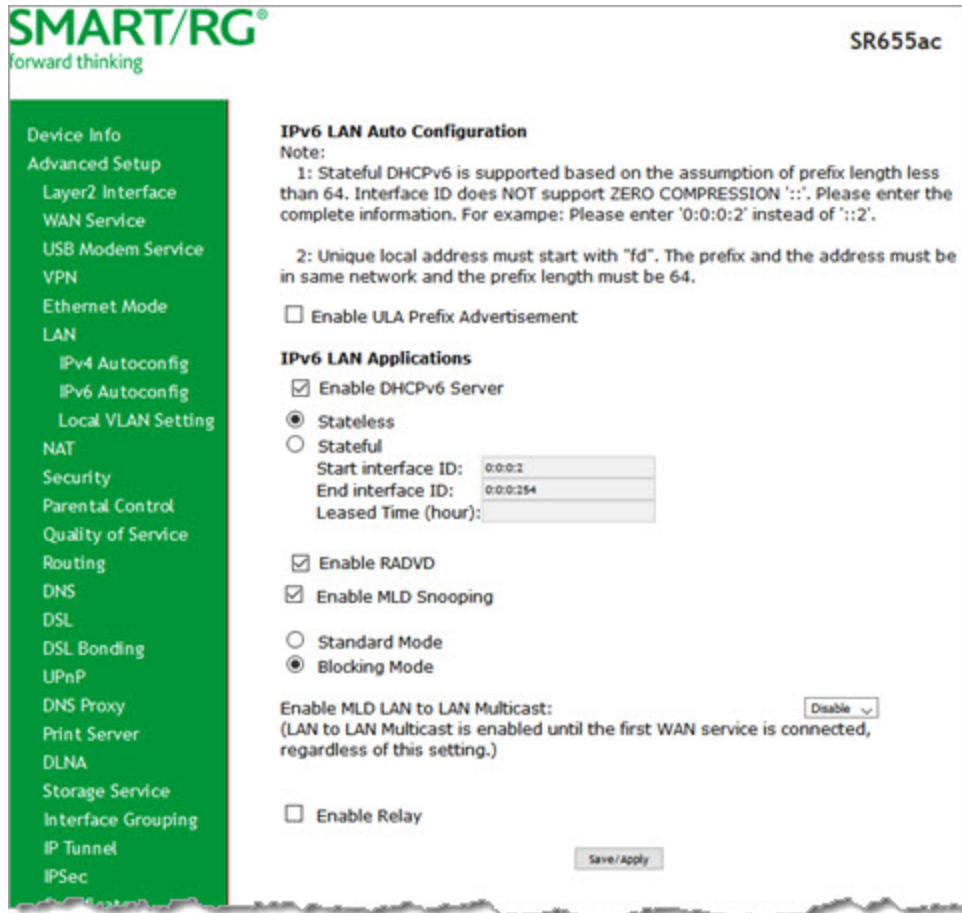
- a. Click **Add OUI**. The DHCP OUI page appears.

- b. Enter the OUI for the DHCP and click **Apply/Save**.
8. To remove entries from the **OUI** list, click the **Remove** check box next to the entry and then click **Remove OUI**.
9. To set the second IP address and the subnet mask for a LAN interface:
 - a. Click **Configure the second IP Address and Subnet Mask for LAN interface**. Additional fields appear.
 - b. Enter an IP address and a subnet mask for the LAN interface.
10. Click **Apply/Save** to apply your settings.

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/RG® SR655ac
forward thinking

Device Info
Advanced Setup
 Layer2 Interface
 WAN Service
 USB Modem Service
 VPN
 Ethernet Mode
LAN
 IPv4 Autoconfig
 IPv6 Autoconfig
 Local VLAN Setting
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DNS
 DSL
 DSL Bonding
 UPnP
 DNS Proxy
 Print Server
 DLNA
 Storage Service
 Interface Grouping
 IP Tunnel
 IPSec

IPv6 LAN Auto Configuration
 Note:
 1: 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 example: Please enter '0:0:0:2' instead of '::2'.
 2: Unique local address must start with "fd". The prefix and the address must be in same network and the prefix length must be 64.

☐ Enable ULA Prefix Advertisement

IPv6 LAN Applications
☒ Enable DHCPv6 Server
☒ Stateless
☐ Stateful
 Start interface ID: 0:0:0:2
 End interface ID: 0:0:0:254
 Leased Time (hour):
☒ Enable RADVD
☒ Enable MLD Snooping
☐ Standard Mode
☒ Blocking Mode
 Enable MLD LAN to LAN Multicast: Disable
 (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)
☐ Enable Relay
 Save/Apply

2. To enable advertisement of the ULA prefix, click **Enable ULA Prefix Advertisement**. Additional fields appear.
3. Modify these and the other fields as needed, using the information in the table below.
4. Click **Save/Apply** to commit your changes.

Field Name	Description
Enable ULA Prefix Advertisement	<p>Check this option to enable unique local address (ULA) advertisement on the LAN. Options are Randomly Generate and Statically Configure. The default is Randomly Generate which enables the gateway to generate a random IPv6 prefix.</p> <p>If you select Statically Configure, additional fields appear. Modify these fields as needed:</p> <ul style="list-style-type: none"> • Interface Address: Enter the interface address in IPv6 format (including the prefix length, e.g., fd80::1/64. This address must begin with "fd". The prefix length must be "64". The address and prefix must reside on the same network. • Prefix: Enter the prefix, e.g., fd80::/64. • Preferred Life Time: The default is -1 (no limit). The value in this field must be less than or equal to the value in the Valid Life Time field. • Valid Life Time: The value in this field must be greater than or equal to the value in the Preferred Life Time field. The default is -1 (no limit).
IPv6 LAN Applications section	
Enable DHCPv6 Server	<p>This option is selected by default. Click this checkbox to disable the DHCP v6 feature on the LAN.</p> <ul style="list-style-type: none"> • Stateless: (<i>Appears when Enable DHCPv6 Server is selected</i>) Click to stop inheriting IPV6 address assignments from the WAN IPV6 interface. • Stateful: (<i>Appears when Enable DHCPv6 Server is selected</i>) This option is selected by default. Identifies the DHCPv6 server given by the LAN IPV6 network as configured with additional options. Zero compression is not supported. Make sure to enter zeros between the colons, that is, do not use shorthand notation (::2). Enter values in the following fields: <ul style="list-style-type: none"> • 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	<p>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.</p>
Enable MLD Snooping	<p>This option is enabled by default. It enables Multicast Listener Discovery (MLD) snooping to manage IPV6 multicast traffic. If you clear the check box to disable this feature, the MLD-related fields are hidden. Options are:</p> <ul style="list-style-type: none"> • 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	<p>(<i>Optional</i>) This option enables LAN-to-LAN Multicast until the first WAN service is connected. Options are Disable and Enable. The default is Disable.</p>

Field Name	Description
Enable Relay	Click to enable the relay function. Additional fields appear. Do the following: <ol style="list-style-type: none"> 1. Enter the DHCPv6 Server IP Address. 2. Select a WAN interface. The default is Default. 3. Enter a Hop limit. The default is zero (0).

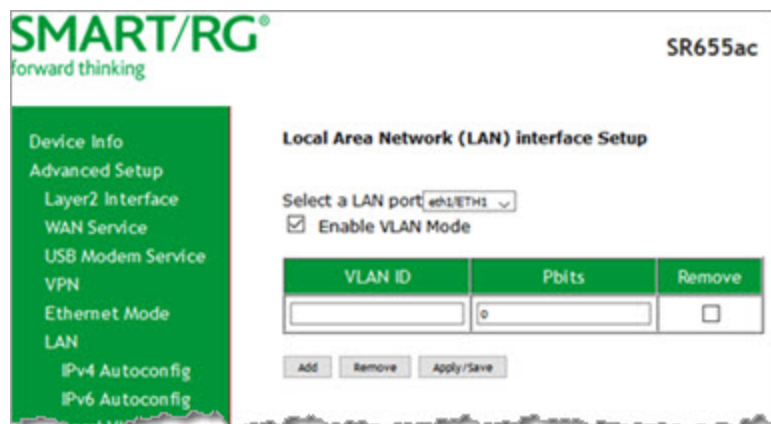
Local VLAN Setting

On this page, you can select a LAN port and enable VLAN mode on it.

1. In the left navigation menu, click **Advanced Setup** > **LAN** > **Local VLAN Setting**. The following page appears.



2. Select the LAN port on which you want to enable VLAN mode.
3. Click **Enable VLAN Mode**.
4. To add a VLAN:
 - a. Click **Add**. A table appears where you can enter the details.



- b. Enter the **VLAN ID**. Options are **1 - 4094**.
 - c. In the **Pbits** field, enter the number of bits being passed. Options are **1 - 7**.
5. Click **Apply/Save** to apply your settings.
 6. To remove a VLAN entry, click the **Remove** checkbox next to it and then click the **Remove** button.

NAT

In this section, you can configure the NAT (Network Address Translation) settings.

Virtual Servers

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

On this page, you can add or remove virtual server entries.

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

SMART/RG®
forward thinking

SR655ac

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	LAN Loopback	Enable/Disable	Remove
<div> Add Save/Apply Remove </div>										

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

Field	Description
Use interface	Select the interface that you want to configure.

Field	Description
Service Name	<p>Select or enter the service for which you want to forward IP packets. Options are:</p> <ul style="list-style-type: none"> • 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.
Enable LAN Loopback	Click to enable on-demand link diagnostics for this server.
Server IP Address	Assign an IP address to this virtual server. The default shown in the field (192.168.1) is not a complete address; you must enter the final octet.
External Port Start External Port End	When you select a service, the external port start and end numbers display automatically. Modify them if necessary.
Protocol	Select the protocol for this service. Options are TCP/UDP , TCP , and UDP . The default is TCP .
Internal Port Start Internal Port End	When you select a service, the internal port start and end numbers display automatically. Modify them if necessary.

3. In the **Status** field, select **Enable** to enable this server or select **Disable** when you want to save the settings but not enable the server.
4. Click **Apply/Save** to save the settings. The server or servers for the selected service appear on the NAT -- Virtual Servers Setup page.
5. To disable a server, click the **Enable/Disable** check box next to it to clear it and then click **Apply/Save**.
6. To remove a server from the list, click the **Remove** check box next to the entry and then click the **Remove** button. Then click **Save/Apply**.

Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
Multi Nat
Security
Parental Control
Quality of Service

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger 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 Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum **32** entries can be configured.

Due to limited resources, port triggering feature has some limitation:
 sum of the out-ports of all configuration entries <= 1000
 sum of the in-ports of one configuration entry <= 1000

Application Name	Trigger		Open			WAN Interface	Remove
	Protocol	Port Range	Protocol	Port Range			
		Start End		Start End			

Add Remove

2. To add a port trigger, click **Add**. The following page appears.

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
Multi Nat
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:

Use Interface: ipoe_0_0_35/asm0.2

Application Name:

☒ Select an application: Select One

☐ Custom application:

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply/Save

3. Modify the fields as needed, using the information in the following table.

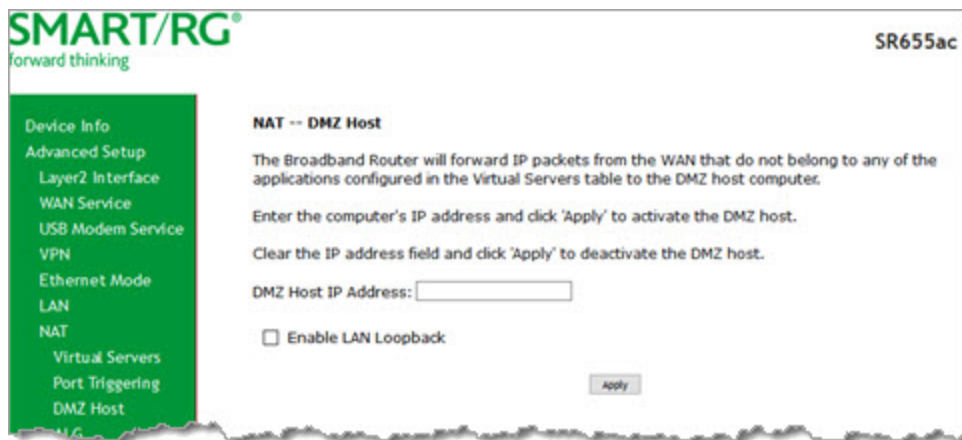
4. To remove a trigger, click the **Remove** check box next to it and then click the **Remove** button. The list is refreshed.
5. Click **Apply /Save** to implement the settings.

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: <ul style="list-style-type: none"> • 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.
Trigger Port Start Trigger Port End	Enter the starting and ending numbers of the range of available outgoing trigger ports. Options are 1 - 65535. 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 specified range. Options are TCP , UDP , and TCP/UDP .
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 .

DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. On this page, you can set the IP address of a PC to be the DMZ host, so that the DMZ host will not be blocked by your firewall.

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



2. Enter the **DMZ Host IP Address**.
3. (Optional) To enable on-demand link diagnostics, click **Enable LAN Loopback**.

4. To deactivate a DMZ host, delete the IP address from the **DMZ Host IP Address** field, and then click **Apply**.
5. Click **Apply** to commit the new or changed address.

ALG

On this page, you can enable Session Initiation Protocol (SIP) for your NAT. SIP is a communications protocol for signaling and controlling multimedia communication sessions.

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



2. To *disable* SIP for your NAT, clear the **SIP Enabled** checkbox.
3. Click **Save/Apply** to commit the new or changed address.

Multi NAT

On this page, you can define rules for managing access to your NAT. You can create multiple rules and apply them to as many as eight address ranges.

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

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

Field	Description
Rule Type	Select the type of rule. Options are One to One , One to Many , Many to One , and Many to Many .
Use Interface	Select the interface to which this rule will apply. Options include any interfaces defined for your gateway.
internalAddrStart	Enter the starting address for the internal server.
internalAddrEnd	Enter the ending address for the internal server.
externalAddrStart	Enter the starting address for the external server.
externalAddrEnd	Enter the ending address for the external server.

3. Click **Apply/Save** to save and apply the settings. The server or servers for the selected service appear on the MultiNat table page.

Security

In this section, you can configure the incoming and outgoing IP filtering and MAC filtering.

IP Filtering - Outgoing

On this page, you can add an outgoing filter and prevent certain data being transferred from the LAN to the WAN.

1. In the left navigation bar, click **Advanced Setup > Security** and then click **Add**. The following page appears. You can also reach this page by clicking **Advanced Setup > Security > IP Filtering > Outgoing**.

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

The fields on this page are defined below.

Field Name	Description
Filter Name	Enter a descriptive name for this filter. No special characters or spaces are allowed.
IP Version	For the filter to be configured and effective for IPV6, the gateway must be installed on a network that is either a pure IPV6 network (with that protocol enabled) or is both IPV4 and IPV6 dual protocol enabled/configured. Options are IPv4 and IPv6 . The default is IPv4 . If you select IPv6 , Source IP address and Destination IP address must be specified in IPV6 format, i.e., an IPV6-compliant, hexadecimal address such as: 2001:0DB8:AC10:FE01:0000:0000:0000:0001.
Protocol	Select the protocol profile for the filter you are defining. TCP/UDP is most commonly used. Options are TCP/UDP , TCP , UDP , and ICMP .
Source IP address [/prefix length]	Enter the source IP address of a LAN side host for which you wish to block outgoing traffic using the specified protocol(s). 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.
Source Port (port or port:port)	Set the source host port (or range of ports) for the above host (or range of hosts) to define the ports profile for which egress traffic will be blocked from reaching the specified destination(s).

Field Name	Description
Destination IP address	Enter the destination IP address of a LAN side host for which you wish to filter/block outgoing traffic using 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 associated routing "/prefix" length decimal value (preceded with the slash).
Destination Port (port or port:port)	Set the destination host port (or range of ports) for the above host (or range of hosts) to define the destination port profile for which egress traffic will be blocked, e.g., for a computer external to the local network.

IP Filtering - Incoming

On this page, you can add an incoming filter and prevent certain data being transferred from the WAN to the LAN.

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

2. Fill in the fields, using the information in the table below. The **Filter Name** and **Protocol** fields are required.
3. Click **Apply/Save** to commit your changes.

The fields on this page are defined below.

Field Name	Description
Filter Name	Enter a descriptive name for this filter. No special characters or spaces are allowed.

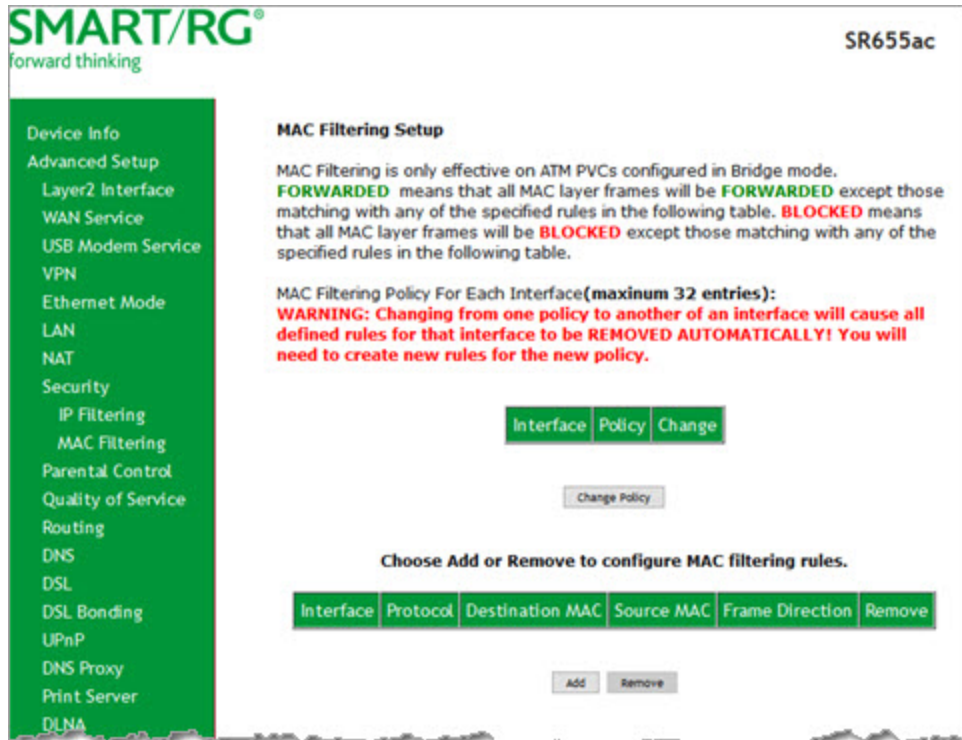
Field Name	Description
IP Version	<p>For the filter to be configured and effective for IPV6, the gateway must be installed on a network that is either a pure IPV6 network (with that protocol enabled) or is both IPV4 and IPV6 dual protocol enabled/configured. Options are IPv4 and IPv6. The default is IPv4.</p> <p>If you select IPv6, Source IP address and Destination IP address must be specified in IPV6 format, i.e., an IPV6-compliant, hexadecimal address such as: 2001:0DB8:AC10:FE01:0000:0000:0000:0001.</p>
Protocol	Select the protocol to be associated with this incoming filter. Options are TCP/UDP , TCP , UDP , or ICMP .
Source IP address [/prefix length]	Enter the source IP address for this filter. For IPV6, enter the prefix as well.
Source Port (port or port:port)	Enter a source port number or range (xxxxx:yyyyy).
Destination IP address [/prefix length]	Enter the destination IP address for this filter. 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 select any of the types defined for your network. the default is Select All .

MAC Filtering

On this page, you can manage MAC filtering for your gateway.

Your 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.

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



2. To modify settings for an existing policy, click the **Change** checkbox next to it, and then click **Change Policy**. Options are **BLOCKED** and **FORWARD**. The page refreshes, showing that the action has changed. The **Change Policy** button acts like a toggle switch, clicking it switches the policy from **BLOCKED** to **FORWARD** and back again.
3. To add a MAC filtering rule, click **Add** and follow the instructions in [Adding a MAC Filter](#).
4. To remove a rule, click the **Remove** checkbox next to the rule and click **Remove**.
5. When your changes are completed, click **Apply/Save** to commit your changes.

Adding a MAC Filter

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

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

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

The fields on this page are defined below.

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 device that you want to associate with this filter.
Source MAC Address	Enter the MAC address of the device that originates the requests intended for the device associated with the Destination MAC address.
Frame Direction	Select the incoming/outgoing packet interface. Options are LAN<=>WAN, WAN=>LAN, and LAN=>WAN. The default is LAN<=>WAN (both directions).
WAN Interfaces	Select the WAN interface(s) for which the filter should apply. Only interfaces configured for Bridge mode are available.

Parental Control

In this section, you can manage time restrictions and block or allow specific URLs.

Time Restriction

On this page, you can control time restriction settings for a LAN device that connects to the gateway.

Note: Before you can create a time restriction rule, the gateway's time must be set. You can do this on the Management > Internet Time page.

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

SMART/RG®
forward thinking

SR655ac

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN devices, click the 'Other MAC Address' button and enter the MAC address of the other LAN devices. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.

User Name

☒ Browser's MAC Address

☐ Other MAC Address

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

2. Enter a descriptive name for the rule.
3. (Optional) Enter an additional MAC address by clicking **Other MAC Address** and entering the address in the adjacent field.
4. Select the days of the week when this rule should apply.
5. Enter the starting and ending times for the periods that you want blocked. Use 24-hour format.
6. Click **Apply/Save** to implement the settings. You are returned to the Parental Control > Access Time Restriction page.

Url Filter

On this page, you can prevent the LAN users from accessing some Web sites in the WAN.

1. Click **Advanced Setup** > **Parental Control** > **Url Filter**, and 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. The default is **Include**.
3. To create the list of URLs, click **Add**. The following page appears.

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. Select the days of the week when this rule will apply.
6. Enter the starting and ending time periods when this rule should be active. Use 24-hour format.
7. Click **Apply/Save** to save the entry. 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, video, data) exceeds the capacity of the line.

In this section, you can disable/enable QoS and configure queues and classification rules.

Quality of Service

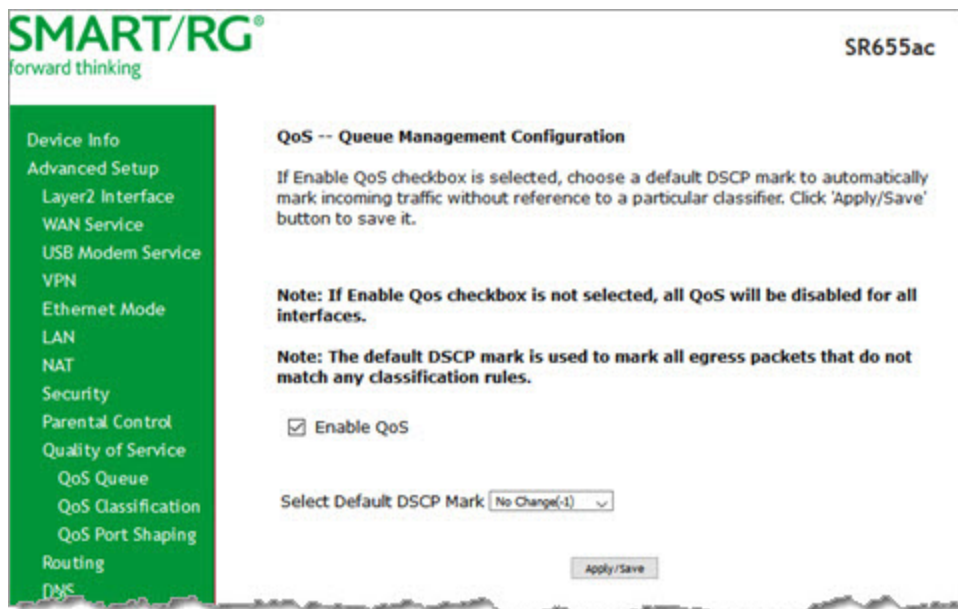
On this page, you can enable or disable QoS and set the DSCP Mark classification.

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

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

Note: Queues for wireless connections (e.g., WMM Voice Priority) are shown only when wireless is enabled. If the **WMM Advertise** option 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**. The following page appears. The Quality of Service feature is enabled by default.



2. To disable QoS for ALL interfaces, click the **Enable QoS** check box to clear it.

3. (Optional) Select the default DSCP Mark (Differentiated Services Code Point) classification value to be used. The default is **No Change(-1)**.
4. Click **Apply/Save** to save your settings.

QoS Queue

On this page, you can configure a queue and add it to a selected Layer2 interface. You can also edit and delete queues. A number of standard queues are already defined. You may have to remove queues that you don't need in order to create the desired queues.

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

SMART/RG® forward thinking SR655ac

QoS Queue Setup

In ATM mode, a maximum of 16 queues can be configured.
 In PTM mode, a maximum of 8 queues can be configured.
 For each Ethernet interface, a maximum of 8 queues can be configured.
 For each Ethernet WAN interface, a maximum of 8 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled.
 Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.

Note: Ethernet LAN queue configuration only takes effect when all the queues of the interface have been configured.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate(bps)	Min Bit Rate(bps)	Burst Size(bytes)	Enable	Remove
LAN Q8	1	ETH1	8	1/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q7	2	ETH1	7	2/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q6	3	ETH1	6	3/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q5	4	ETH1	5	4/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. To add a queue:
 - a. Click **Add** at the bottom of the table. The following page appears.

SMART/RG® forward thinking SR655ac

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Name:

Enable:

Interface:

- b. Fill in the fields, using the information in the following table. The visible fields vary by interface and queue precedence selections. In most cases, you can use the default values.
 - c. Click **Apply/Save**. You are returned to the QoS Queue Setup page.
3. To remove a queue, click the **Remove** checkbox to the right of the entry and then click the **Remove** button at the bottom of the page.
4. Click **Apply/Save** to save your settings.

The applicable fields are explained below.

Field Name	Description
Name	Enter a descriptive name for this configuration.
Enable	Select to enable or disable this QoS queue for the interface that you select. Options are Enable and Disable . The default is Enable .
Interface	Select the Layer 2 interface to be associated with the defined QoS queue, e.g., eth0 or ptm01.
Queue Precedence	<p>(Appears when atm, eth or ptm interfaces are selected in the Interface fields) Select the priority value to be associated with the defined QoS queue. Options vary by interface and can include 1(SP), 2(SP), 3(WRR), 4(SP WRR WFQ), and so on.</p> <p>Note: The lower the precedence value, the higher priority the queue is given. Traffic is given priority based on the combined values from this field and Queue Weight field.</p>

The following fields become visible based on your selections in the **Interface** and **Queue Precedence** fields. Which fields appear vary by your selections. The fields are listed below in alphabetical order.

DSL Latency	This option is set to Path0 by default and cannot be changed. No error correction is performed. This can reduce latency on error-free lines.
Minimum Rate	Enter the minimum shaping rate defined for packets in QoS queues. Options are 1 - 100000 Kbps . The default is -1 (no minimum shaping rate).
PTM Priority	Select the priority for this queue. Options are Low and High . The default is Low .
Queue Weight	<p>Enter the weighting value to associate with this queue. Options are 1 - 63. The default is 1.</p> <p>Note: The higher the weighting value, the more frames that are sent proportionately given the WRR algorithm employed. Traffic is given priority based on the combined values from this field and the Queue Precedence field.</p>
Scheduler Algorithm	<p>Select an algorithm for data priority in queues. Options are:</p> <ul style="list-style-type: none"> 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.
Shaping Burst Size	Enter the shaping burst size to be applied to packets in the defined queue. Options are 1600 bytes or greater.
Shaping Rate	Enter the shaping rate for packets in QoS queues. Options are 1 - 100000 Kbps . The default is -1 (no minimum shaping).

WLAN Queue

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

Note: Make sure that wireless connection is active by going to [Wireless](#) and clicking [Apply/Save](#).

In the left navigation bar, click [Advanced Setup](#) > [Quality Of Service](#) > [QoS Queue](#) > [Wlan Queue](#). The following page appears.

SMART/RG®
forward thinking

SR655ac

QoS Wlan Queue Setup

Note: If WMM function is disabled in Wireless Page, queues related to wireless will not take effect.

Name	Key	Interface	Qid	Prec/Alg/Wght	Enable
WMM Voice Priority	33	wlan0	8	1/SP	Enabled
WMM Voice Priority	34	wlan0	7	2/SP	Enabled
WMM Video Priority	35	wlan0	6	3/SP	Enabled
WMM Video Priority	36	wlan0	5	4/SP	Enabled
WMM Best Effort	37	wlan0	4	5/SP	Enabled
WMM Background	38	wlan0	3	6/SP	Enabled
WMM Background	39	wlan0	2	7/SP	Enabled
WMM Best Effort	40	wlan0	1	0/CP	Enabled

QoS Classification

On this page, you can create classifications (traffic class rules) for assigning ingress traffic to a priority queue.

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

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

The fields on this page are defined below.

Field Name	Description
Add Network Traffic Class Rule section	
Traffic Class Name	Enter a descriptive name for this rule.
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 .

Specify Classification Criteria section

All fields in this section are optional. A blank field identifies a criterion that is not used.

Field Name	Description
Ingress Interface	Select an interface for incoming traffic. Options are LAN , WAN , Local , and any interface defined for your network.
Ether Type	Select the Ethernet interface type for this classification. Options include IP , ARP , IPv6 , PPPoE , and any other Ethernet interface defined for your network.
Source MAC Address / 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 / Mask	(Available for LAN , ETH and wireless interfaces only) Enter the destination MAC address and destination MAC mask for this classification.
Source IP Address [/ Mask] or Vendor Class ID or User Class ID	(Available for WAN , ATM and PPP-Routed interfaces only) Select the source for this classification. Options are: !!! ASK SME: Only Source IP Address/Mask option displays now for all Ingress Interface values. Remove other values? <ul style="list-style-type: none"> • 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)	(Available for WAN , Local , ATM interfaces only) Enter the minimum and maximum number of digits required for IP addresses.
Protocol	(Available for WAN , Local , and ATM interfaces only) Select the protocol specified for this classification. Options are TCP , UDP , ICMP , and IGMP .
UDP/TCP Source Port	(Appears when TCP or UDP is selected in the Protocol field) 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	(Appears when TCP or UDP is selected in the Protocol field) Enter the destination port to be used for this classification. You can enter a range (port:port) or a single port.
Specify Classification Results section	
Specify Egress Interface	Select an interface for outgoing traffic. Options include any interface defined for your network.
Specify Egress Queue	Select from the available queues. 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 802.1p priority	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 (Kbps)	Enter the data traffic rate limit for this classification in kilobits per second.

QoS Port Shaping

On this page, you can configure a fixed rate (Kbps) for each of the Ethernet ports.

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

SMART/RG®
forward thinking

SR655ac

QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.
If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	Shaping Rate (Kbps)	Burst Size (bytes)
eth0	WAN	-1	0
ETH1	LAN	-1	0
ETH2	LAN	-1	0
ETH3	LAN	-1	0
ETH4	LAN	-1	0

Apply/Save

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

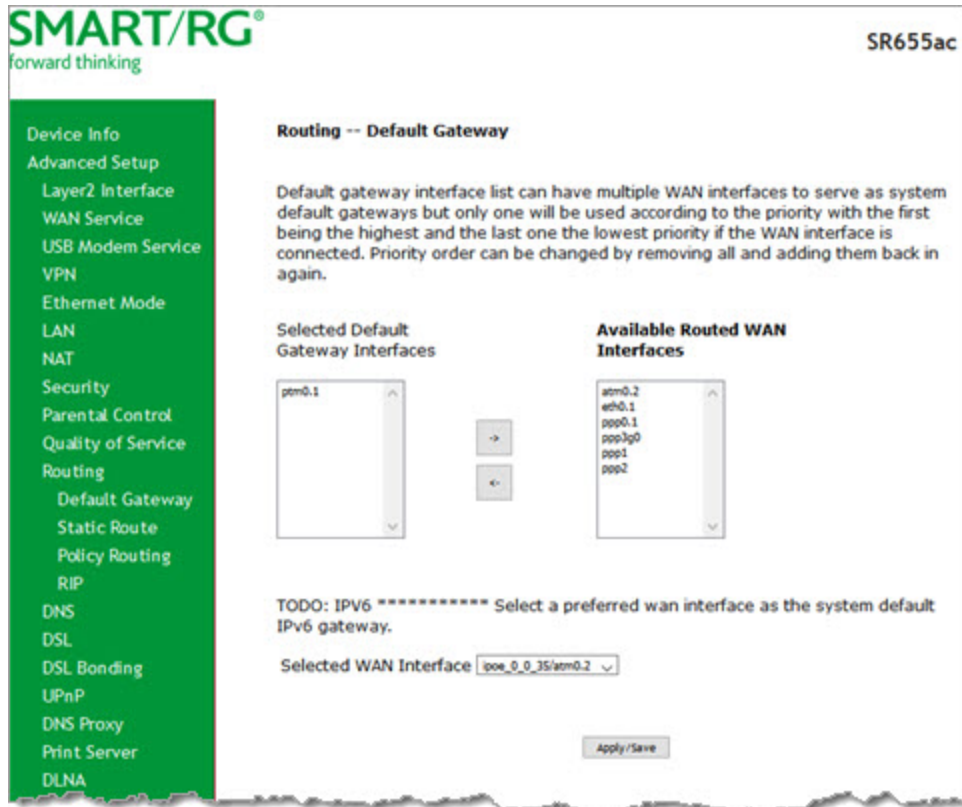
Routing

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

Default Gateway

On this page, you can select the WAN interface for the default gateway.

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



2. (Optional) Select entries in the lists and click the **arrows** to move your selections from left to right or right to left.
3. (Optional) In the **Selected WAN Interface** field, select the appropriate interface.
4. Click **Apply/Save** to implement the settings.

Static Route

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

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

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

The fields on this page are defined below.

Field Name	Description
IP Version	Select the IP version associated with the static route you wish to create. Options are IPv4 and IPv6 .
Destination IP address/prefix length	Enter the destination network address / subnet mask for this route.
Interface	Select the WAN Interface for this route. This list is filtered by the selected IP version.
Gateway IP Address	Enter the next-hop IP address. If needed, include the /prefix length.
Metric	(Optional) Enter a number that is zero or higher.

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. Use this feature to establish similar policies.

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

2. Fill in the fields, using the information in the table below.
3. Click **Apply/Save** to commit your changes. You are returned to the Policy Routing Setting page.
4. To remove a route, click the **Remove** check box next to it and then click the **Remove** button. The list is refreshed.

The fields on this page are defined below.

Field Name	Description
Policy Name	Enter a descriptive name for this entry to the policy routing table. The maximum is 8 characters. Special characters are not allowed.
Physical LAN Port	Select a physical LAN interface for the policy route. Options include Ethernet (LAN) ports 1-4 and both wireless bands.
Source IP	Enter the IP address for the source of the policy route.
Use Interface	Select the WAN Interface for this policy route. If you select an IPoE interface, you must enter the IP address for the Default Gateway .

RIP

RIP (Routing Information Protocol) 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.

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

SMART/RG
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

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 start/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm0.2	2	Passive	<input type="checkbox"/>
ptm0.1	2	Passive	<input type="checkbox"/>
eth0.1	2	Passive	<input type="checkbox"/>

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.

The fields on this page are defined below.

Field Name	Description
Interface	Displays a list of available WAN interfaces.
Version	Select the applicable version of the Routing Interface Protocol. For detailed information about versions, refer to RFC 1058 and RFC 1453. Options are 1, 2, and Both.
Operation	This option is set to Passive and cannot be changed. This mode listens only. It does not advertise routes.

DNS

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

DNS Server

On this page, you can select a DNS server interface from the available interfaces, manually enter the DNS server addresses, or obtain the DNS address from a WAN interface.

1. In the left navigation bar, click **Advanced Setup > DNS > DNS Server**. The following page appears.
2. Do one of the following to configure the DNS server:
 - **Select the DNS server interface from available WAN interfaces:** Select interface entries in the lists 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 information from a WAN interface:** Select the interface in the **WAN Interface Selected** field. If no WAN interface is configured, this field is disabled.
 - **Define a static IPv6 DNS IP address:** Click **Use the following Static IPv6 DNS address** and enter the DNS server IP addresses.
3. Click **Apply/Save** to apply your settings.

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. You can configure the settings for this feature on this page.

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

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

The fields on this page are defined below.

Field Name	Description
D-DNS provider	Select a dynamic Domain Name Server provider. Options are DynDNS.org , TZO or no-ip.com . The default is DynDNS.org .
Hostname	Enter the host name of the dynamic DNS server.
Interface	Select the WAN interface whose traffic will be pointed at the specified Dynamic DNS provider.
DynDNS Settings section	
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

DNS Config

On this page, you can configure DNS domains.

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

2. To add a DNS domain, click **Add**. The following page appears.

3. Enter a domain name and IP address for the domain. Only letters, numbers, dashes, and periods are allowed.
4. Click **Apply/Save** to apply your settings.

DSL

On this page, you can set the DSL settings. The modem negotiates the modulation mode with the DSLAM; you usually do not need to modify the factory default settings.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
 Layer2 Interface
 WAN Service
 USB Modem Service
 VPN
 Ethernet Mode
 LAN
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DNS
 DSL
 DSL Bonding
 UPnP
 DNS Proxy
 Print Server
 DLNA
 Storage Service
 Interface Grouping
 IP Tunnel
 IPSec
 Certificate
 Power Management
 Multicast
 Wireless
 Voice
 Diagnostics
 Diagnostics Tools
 Management
 Logout

DSL Settings

Select the modulation below.

☒ G.Dmt Enabled
☒ G.lite Enabled
☒ T1.413 Enabled
☒ ADSL2 Enabled
☒ AnnexL Enabled
☒ ADSL2+ Enabled
☐ AnnexM Enabled

Select the profile below.

☒ VDSL2 Enabled
☒ 8a Enabled
☒ 8b Enabled
☒ 8c Enabled
☒ 8d Enabled
☒ 12a Enabled
☒ 12b Enabled
☒ 17a Enabled
☒ 30a Enabled
☒ 35b Enabled

US0
☒ Enabled

Select the phone line pair below.

☒ Inner pair
☐ Outer pair

Capability

☒ Bitswap Enable
☐ SRA Enable
☐ PhyR Enable
☐ ADSL PTM MODE Enabled
☒ G.INP Upstream
☒ G.INP Downstream

Dsl Led set

☒ Enable led blinking when dsl is down

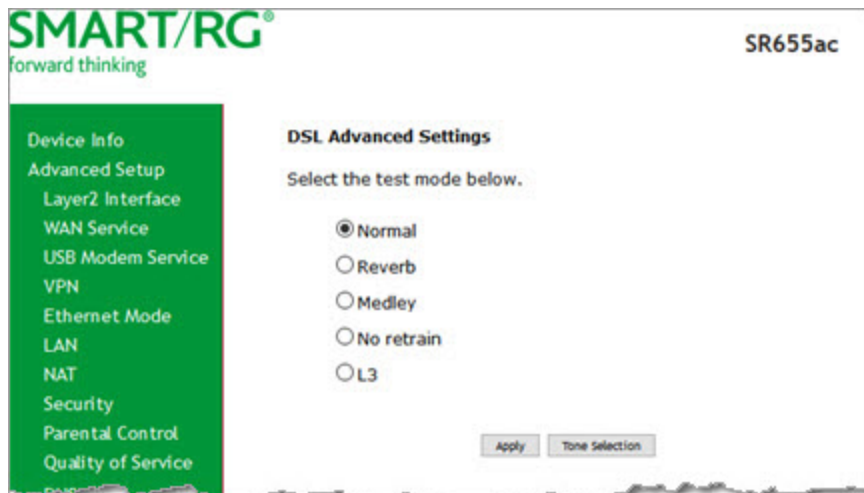
Inventory Management

☒ Use board serial for EOC Serial Number

Apply/Save Advanced Settings

2. Modify the settings as needed.

3. To modify additional parameters, click **Advanced Settings**. The following page appears.



4. Select the test mode that you want to run.
5. To view the tone selection table, click **Tone Selection**. Changing these settings arbitrarily is *not* recommended. Close the window to return to the DSL Advanced Settings page.
6. Click **Apply** and then click **DSL** in the left menu to return to the DSL page.
7. Click **Apply/Save** to save your changes.

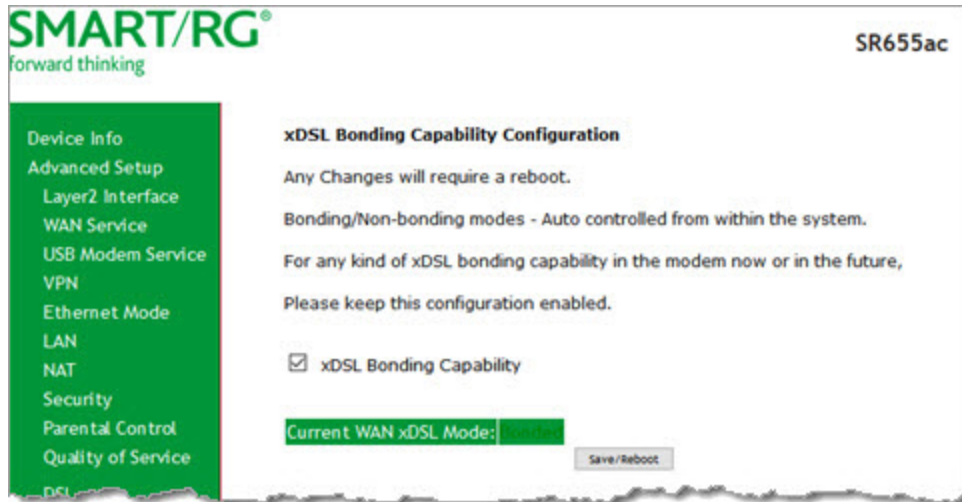
DSL Bonding

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.

On this page, you can enable xDSL bonding.

Note: Any changes you make on this page will reboot the gateway.

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



2. To *disable* bonding, click **xDSL Bonding Capability**. This action is not recommended.
3. Click **Save/Reboot** to commit your changes. Your gateway is rebooted.

UPnP

On this page, you can enable or disable the UPnP function.

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



2. To *disable* UPnP, click the **Enable UPnP** check box to clear it.
3. Click **Apply/Save** to save and apply the settings.

DNS Proxy

On this page, you can enable or disable the DNS proxy function. This function is enabled by default.

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

SMART/RG® forward thinking SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
Security

DNS Proxy Configuration

☒ Enable DNS Proxy

Host name of the Broadband Router:

Domain name of the LAN network:

Apply/Save

2. To *disable* the DNS Proxy, click the **Enable DNS Proxy** check box to clear it.
3. To modify the host and domain, enter the host name of the new broadband gateway and the domain name of the LAN network.
4. Click **Apply/Save** to implement the settings.

Print Server

On this page, you can enable or disable a printer server. You also need to set up your PC to use the connected printer.

1. Power up the printer that you want to configure.
2. Connect the printer to one of the USB ports on your gateway. When the USB LED glows solid, proceed to Step 3.
3. In the left navigation menu, click **Advanced Setup > Print Server**. The following page appears.

SMART/RG® forward thinking SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN

Print Server settings

This page allows you to enable / disable printer support.

☐ Enable on-board print server.

Apply/Save

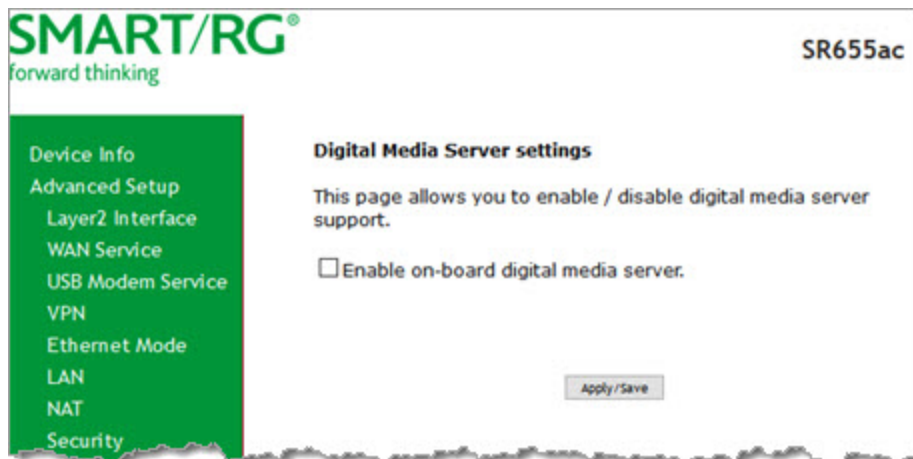
4. Click **Enable on-board print server**. Additional fields appear.
5. Enter the **Printer Name**.
6. Enter the **Make and model**.
7. Copy and save the HTTP address; you will need it later to connect to the printer.

- Click **Apply/Save** to save and apply the settings. For more information about configuring your PC to access this printer, see the related [How-To article](#) in the SmartRG Customer Portal.

DLNA

On this page, you can manage on-board digital media servers.

- In the left navigation menu, click **Advanced Setup > DLNA**. The following page appears.



- Click **Enable on-board digital media server**. Additional fields appear. The **Interface** field is set to **Default**.
- (Optional) In the **Media Library Path** field, enter the custom path for the server. The default folder is **/mnt/disk1_1**.
- (Optional) In the **Media Library Update Period** field, enter the number of seconds that should elapse between update checks. The default is **3600** (60 minutes).
- Click **Apply/Save** to save the settings.

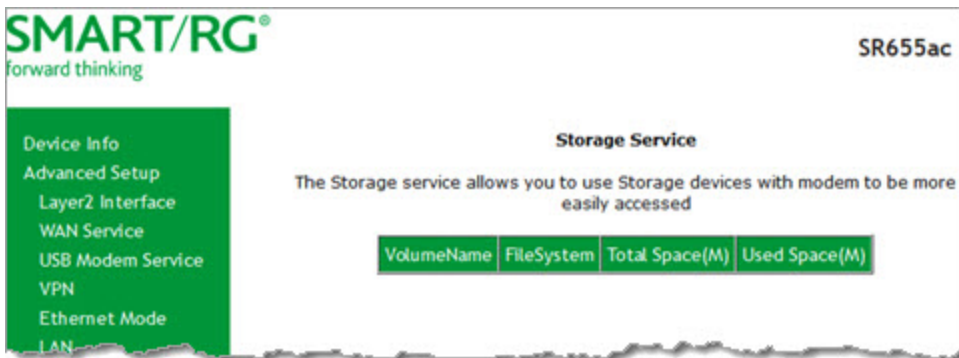
Storage Service

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.

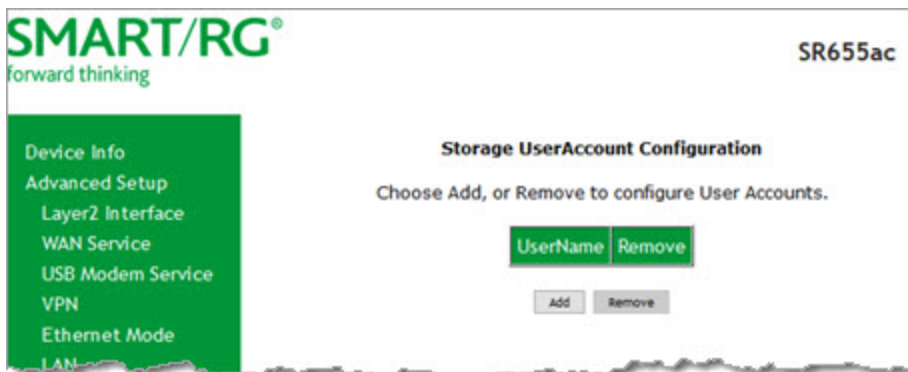
In the left navigation menu, click **Advanced Setup > Storage Service**. The following page appears, showing information about the connected storage device, if any.



User Accounts

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

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




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

- b. Enter a user name and enter the password twice. The password cannot contain spaces.
 - c. Click **Apply/Save** to save your settings. You are returned to the User Accounts page.
3. To remove a user account, click the **Remove** checkbox next to the account entry and then click the **Remove** button. The list refreshes to show your changes were applied.

Interface Grouping

On this page, you can configure interface groupings. Interface grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. Only the default group has an IP interface. To support this feature, you must create mapping groups with the appropriate LAN and WAN interfaces.

1. In the left navigation menu, click **Advanced Setup > Interface Grouping**. The following page appears.



SR655ac

Device Info

Advanced Setup

Layer2 Interface

WAN Service

USB Modem Service

VPN

Ethernet Mode

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DSL

DSL Bonding

UPnP

DNS Proxy

Print Server

DLNA

Storage Service

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ptm0.1 eth0.1 ppp0.1 atm0.2 ppp3g0 ppp1 ppp2	ETH1.0	
			ETH2.0	
			ETH3.0	
			ETH4.0	
			5 GHz Band	
			2.4 GHz Band	

Add Remove

SMARTRG INC. PROPRIETARY AND CONFIDENTIAL. ALL RIGHTS RESERVED. COPYRIGHT © 2017

102

2. To add a new grouping, click **Add**. The following page appears.

SMART/RG®
forward thinking

SR655ac

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately.

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

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces

Available LAN Interfaces

ETH1.0
ETH2.0
ETH3.0
ETH4.0
5 GHz Band
2.4 GHz Band

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

3. Follow the on-screen instructions and then click **Apply/Save**.
4. To remove a grouping from the list, click the **Remove** checkbox next to the group name and then click the **Remove** button. 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.

In this section, you can configure connections of IPv6 networks across the IPv4 internet or IPv4 in IPv6.

IPv6inIPv4

On this page, you can configure a tunnel for IPv6inIPv4.

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

2. Enter a **Tunnel Name**. In the **Mechanism** field, the only option is **6RD**.
3. Select the **WAN** and **LAN** interfaces associated with the tunnel you wish to establish.
4. Do one of the following:
 - To configure the LAN interface settings manually, enter values in the fields located below the **Manual** button:
 - **IPv4 Mask Length**: Options are 0 - 32.
 - **6rd Prefix with Prefix Length**: Prefix/length, such as: 2002::/64.
 - **Border Relay IPv4 Address**: IP address for the IPv4 relay server.
 - To configure these settings automatically, click **Automatic**.
5. Click **Apply/Save** to commit your changes.

IPv4inIPv6

On this page, you can configure a tunnel for IPv4inIPv6.

1. In the left navigation bar, click **Advanced Setup** > **IP Tunnel** > **IPv4inIPv6** and then click **Add**. The following page appears.

2. Enter a **Tunnel Name**. In the **Mechanism** field, the only option is DS-Lite.
3. Select the **LAN** and **WAN** interfaces associated with the tunnel you wish to establish.
4. In the **AFTR** (Address Family Transition Router) field, do either of the following:
 - To configure manually, enter the remote address in the **AFTR** field.
 - To configure automatically, select **Automatic** above the **AFTR** field.
5. Click **Apply/Save** to commit your changes.

IPSec

Internet Protocol Security is a protocol for securing communications by packet level encryption and authentication. On this page, you can enable and remove connections, or edit existing connections.

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

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
-----------------	----------------	-----------------	------------------	--------

- Click **Add New Connection**. The following page appears.

- Fill in the fields, using the information in the field description table below.

Field Name	Description
IPsec Connection Name	Enter a descriptive name for this connection.
IP Version	Select the IP version for this connection. Options are IPv4 and IPv6 . The default is IPv4 .
Tunnel Mode	Select the encapsulation method to be used. Options are: <ul style="list-style-type: none"> 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. AH: Use this mode to encapsulate a packet with AH and IP headers. For authentication, the entire packet is signed.
Local Gateway Interface	Select the interface for the local gateway.

Field Name	Description
Remote IPSec Gateway Address	Enter the WAN IP address for the tunnel.
Tunnel Access From Local IP Addresses	<p>Select whether to allow access to the entire LAN or a single host for local IP addresses. Options are:</p> <ul style="list-style-type: none"> • 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.
Tunnel Access From Remote IP Addresses	<p>Select whether to allow access to the entire LAN or a single host for remote IP addresses. Options are:</p> <ul style="list-style-type: none"> • 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.
Key Exchange Method	<p>Select the key-exchange method to be used for IPSec.</p> <ul style="list-style-type: none"> • 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	<p>Select the method by which the remote end will authenticate. Options are:</p> <ul style="list-style-type: none"> • Pre-Shared Key: A key is distributed to authorized users for logging into the system. This is the default. Enter the key in the Pre-Shared Key field. • Certificate (X.509): A certificate is used for authentication. Select a certificate file in the Certificates field.
Perfect Forward Secrecy	<p>Select 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. Options are:</p> <ul style="list-style-type: none"> • Enable: Prevents long-term keys from being compromised. • Disable: Permits long-term keys to be compromised. This is the default.

4. (Optional) To select Phase 1 and Phase 2 specific parameters:

- Click **Show Advanced Settings**. Additional fields appear.
- Fill in the fields, using the information provided in the table below.

Field Name	Description
Mode	<p>(Appears in the Phase 1 section only) Select whether to protect information about your network. Options are:</p> <ul style="list-style-type: none"> • Main: Protect the identity of the peers. This is the default. • Aggressive: Do not protect the identity of the peers.

Field Name	Description
Encryption Algorithm	Select the encryption algorithm. Options are 3DES , AES - 128 , AES - 192 , and AES - 256 . The default is A3DES .
Integrity Algorithm	Select the integrity algorithm. Options are MD5 and SHA1 .
Select Diffie-Hellman Group for Key Exchange	Select the encryption group for exchanging keys. Options range from 768 bit - 8192 bit . The default is 1024 bit .
Key Life Time	Enter how long the key is effective in seconds. The default is 3600 (60 minutes).

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

Certificate

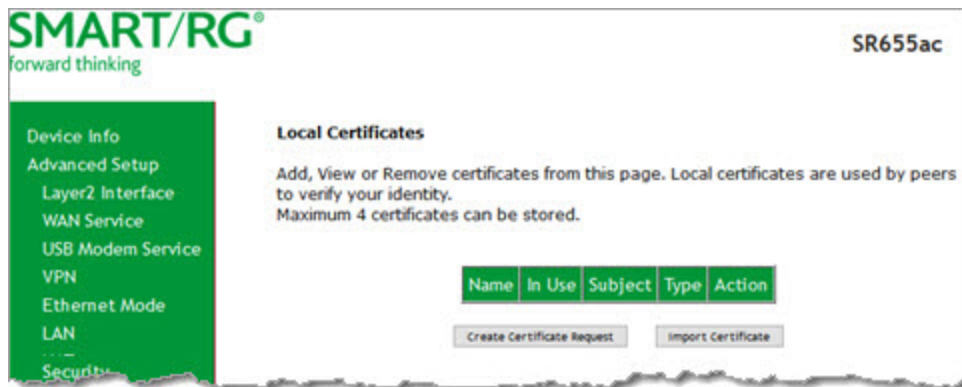
In this section, you can configure certificates (local and Trusted CA) for the gateway. For more information about certificates, refer to the ITU X.509 standard.

Local

On this page, you can manage local certificates used to identify the gateway to other users. You can create a new certificate request locally and have it signed by a certificate authority, or you can import an existing certificate. For additional info regarding Public Key Infrastructure (PKI), refer to ITU-T X.509.

Creating certificate requests

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



2. Click **Create Certificate Request**. The following page appears.

3. Enter your connection details, using the information provided in the table below.
4. Click **Apply** to complete the request.
5. Submit your certificate request to a certificate authority for signature.

The fields on this page are defined below.

Field Name	Description
Certificate Name	Enter a 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. Browsers use this information to verify your certificate is valid.
Organization Name	Enter the name or the company or organization creating the request.
State/Province Name	Enter the full name of the state or province where your organization's head office is located.
Country/Region	Select the country or region in which this certificate will be employed.

Importing a local certificate and private key

1. In the left navigation bar, click **Advanced Setup > Certificate > Local**. Then click **Import Certificate**. The following page appears.

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate
Local

Import certificate
Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

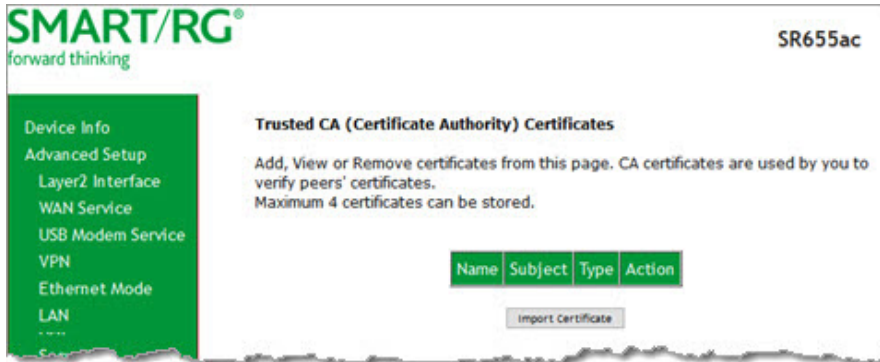
Apply

2. In the **Certificate Name** field, type "cpecert".
3. Paste the **Certificate** details between the **BEGIN** and **END** markers.
4. Paste the **Private Key** information between the **BEGIN** and **END** markers.
5. Click **Apply** to commit this certificate.

Trusted CA

On this page, you can import Trusted Certificates to identify other gateways to your gateway as a trusted source.

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



2. To import a certificate, click **Import Certificate**. The following page appears.
3. In the **Certificate Name** field, type a descriptive name for this certificate. If you are using this certificate with TR-069, the name must be "acscert".
4. Paste the certificate details between the **BEGIN** and **END** markers.
5. 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

On this page, you can configure the multicast parameters.

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
USB Modem Service
VPN
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
DSL Bonding
UPnP
DNS Proxy
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate
Power Management
Multicast
Wireless
Voice
Diagnostics
Diagnostics Tools
Management
Logout

Multicast Precedence: lower value, higher priority
Multicast Strict Grouping Enforcement:

IGMP Configuration
 Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:
 Query Interval (s):
 Query Response Interval (1/10s):
 Robustness Interval (1/10s):
 Robustness Value:
 Maximum Multicast Groups:
 Maximum Multicast Data Sources (for IGMPv3):
 Maximum Multicast Group Members:
 Fast Leave Enable: ☒

IGMP Group Exception List

Group Address	Mask/Mask bits	Remove
224.0.0.0	255.255.255.0	<input type="checkbox"/>
239.255.255.250	255.255.255.255	<input type="checkbox"/>
224.0.255.135	255.255.255.255	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

MLD Configuration
 Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:
 Query Interval (s):
 Query Response Interval (1/10s):
 Last Member Query Interval (1/10s):
 Robustness Value:
 Maximum Multicast Groups:
 Maximum Multicast Data Sources (for mldv2):
 Maximum Multicast Group Members:
 Fast Leave Enable: ☒

MLD Group Exception List

Group Address	Mask/Mask bits	Remove
:::0000	:::0000	<input type="checkbox"/>
:::0000	:::0000	<input type="checkbox"/>
:::0001:0003	:::0001:0003	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

2. Fill in the fields, using the information in the table below. The fields provided for the IGMP and MLD configurations are largely the same.
3. To create or remove exceptions in the **Group Exception List** table, follow the instructions in "Managing group exception lists".
4. Click **Apply/Save** to save and apply the settings.

The fields on this page are defined below.

Field Name	Description
Source Specific Multicast	Select whether a specific multicast source is used. Options are Disable and Enable . The default is Disable .
Multicast Precedence	Select whether IGMP packets are given priority handling and at what level. Options are: <ul style="list-style-type: none"> • 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.
IGMP Configuration and MLD Configuration sections	
Multicast Strict Grouping Enforcement	Select whether to enforce strict key management rules. Options are Enable and Disable . The default is Disable .
Default Version	Enter the supported IGMP version. Options are 1 - 3 .
Query Interval	Enter the interval at which the multicast router sends a query messages to hosts, expressed in seconds. If you enter a number below 128 , the value is used directly. If you enter a number above 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 .
Robustness Interval	<i>(Applies to IGMP configuration only)</i> 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.
Last Member Query Interval	<i>(Applies to MLD configuration only)</i> Enter the maximum response time within which the host must respond to the Out of Sequence query from the router. The default is 10s . IGMP uses this value when the router receives an IGMPv2 Leave report indicating at least one host wants to leave the group. Upon receiving the Leave report, the router verifies whether the interface is configured for IGMP Immediate Leave. If not, the router sends the out-of-sequence query.
Robustness Value	Enter the value representing the complexity of the query. The greater the value, the more robust the query. Options are 2 - 7 .
Maximum Multicast Groups	Enter the maximum number of groups allowed.
Maximum Multicast Data Sources (for IGMPv3)	Enter the maximum number of data sources allowed. Options are 1 - 24 .
Maximum Multicast Group Members	Enter the maximum number of multicast groups that can be joined on a port or group of ports.
Fast Leave Enable	Select whether the IGMP proxy removes group members immediately without sending a query. Options are: <ul style="list-style-type: none"> • Enabled: Group members are removed immediately. This is the default. • Disabled: Group members are removed after a query is sent and a response received.

Managing group exception lists

You can manage exceptions for multicast groups using the **IGMP Group Exception List** or **MLD Group Exception List** tables. The first two entries are created by default; you cannot change these entries.

To add an exception, type the IP address in the **Group Address** field, enter the mask information in the **Mask / Mask bits** field, and then click **Add**.

To remove an exception, click the **Remove** check box next to it and then click the **Remove Checked Entries** button. The list refreshes.

Click **Apply / Save** to implement your changes.

Wireless

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

Basic

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

- 1. In the left navigation bar, click **Wireless**. The following page appears, showing the information for the 5GHz band.

SMART/RG®
forward thinking

SR655ac

Device Info

Advanced Setup

Wireless

5 GHz Band

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Station Info

2.4 GHz Band

WiFi Insight

Voice

Diagnostics

Diagnostics Tools

Management

Logout

Wireless -- Basic

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

☒ Enable Wireless

☒ Enable WiFi Button

☐ Enable Wireless Hotspot2.0

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☒ Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 3C:90:66:2C:A9:A3

Country:

Country RegRev:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Enable WMM Advertise	Enable WMF	Enable HSPOT	Max Clients	BSSID
<input type="checkbox"/>	wifi_guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	20	N/A
<input type="checkbox"/>	wifi_guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	20	N/A
<input type="checkbox"/>	wifi_guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	20	N/A

Apply/Save

- 2. If you want to view or configure the 2.4GHz band settings, click **2.4 GHZ Band** in the left menu.
- 3. Modify the settings as desired, using the information provided in the table below.

4. (Optional) Define up to three virtual access points for guest access using the information from the **Wireless - Guest/Virtual Access Points** section of the table below.
5. Click **Apply/Save** to commit your settings.

The fields on this page are defined below.

Field Name	Description
Enable Wireless	This option is selected by default. To <i>disable</i> the wireless feature, clear the checkbox. All other fields on the page are hidden.
Enable WiFi Button	This option is selected by default. To disable the gateway's 2.4GHz button, clear the checkbox.
Enable Wireless Hotspot 2.0	This option is disabled.
Hide Access Point	Click to hide the access point SSID from end users and passive scanning.
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. Selecting this option can improve transmission performance for voice and video data.
Enable Wireless Multicast Forwarding	This option is selected by default allowing multicast traffic to be forwarded across wireless clients. This option can improve the quality of video services such as IPTV. To <i>disable</i> Wireless Multicast Forwarding (WMF), clear the checkbox.
SSID	(Optional) Enter the WiFi SSID. For security purposes, this identifier should be unique for your system.
BSSID	Displays the Basic Service Set Identifier (BSSID), the MAC address assigned to the wireless router.
Country	This option is set by default and cannot be changed. The wireless channel adjusts to the frequency provision for the selected country.
Country RegRev	This option is set to 910 and cannot be changed.
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 Wireless > Advanced page. Note: Before you can change this setting, you must change the Global Max Clients setting.
Wireless - Guest/Virtual Access Points section	
Enabled	Click to enable a virtual wireless access point for guest access.
SSID	Enter the wireless SSID for guests to use.
Hidden	Click to hide the SSID from being broadcast publicly.
Isolate Clients	Click to prevent client PCs from communicating with one another.
Enable WMM Advertise	Click to stop the wireless from advertising Wireless Multimedia (WMM) functionality.
Enable WMF	Click to enable Wireless Multicast Forwarding (WMF).
Enable HSPOT	Click to enable Hotspot 2.0 access.
Max Clients	Enter the maximum number of clients that can connect to this access point.
BSSID	Displays the Basic Service Set Identifier or N/A .

Security

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

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

Note: To use the PIN method, you need a Registrar (access point/wireless gateway) to initiate the registration between a new device and an active access point/wireless gateway. The PBC method may also need a Registrar when used in a special case where the PIN is all zeros.

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

1. In the left navigation bar, click **Wireless > 5 GHz Band** or **2.4 GHz Band > Security**. The following page appears.

SMART/RG®
forward thinking

SR655ac

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

☒ Enter STA PIN ☐ Use AP PIN

[Help](#)

Set Authorized Station MAC [Help](#)

Set WPS AP Mode

Setup AP (Configure all security settings with an external registrar)

Device PIN [Help](#)

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

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

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

Field Name	Description
Enable WPS	This option is enabled by default. To <i>disable</i> WiFi Protected Setup, select Disabled .
Add Client	<p>(Available for WPA-PSK, WPA2-PSK and Open Network Authentication methods) Select the method for generating the WPS PIN. Options are:</p> <ul style="list-style-type: none"> • Enter STA PIN: Type the input station PIN for the client in the field below the radio button. Click Add Enrollee. The PIN is verified. • Use AP PIN: The entry field and the Set Authorized Station MAC field disappear. <p>Note: If the PIN and Set Authorized Station MAC fields are left blank, the PBC (push-button) mode is automatically made active.</p>
Set Authorized Station MAC	(Available only when Enter STA PIN is selected) Enter the MAC address of the authorized (input) station in format: xx:xx:xx:xx:xx:xx.
Set WPS AP Mode	<p>Select how security is assigned to clients.</p> <ul style="list-style-type: none"> • Configured: The gateway assigns security settings to clients. This is the default. • Unconfigured: An external client assigns security settings to the gateway.
Device PIN	This value is generated by the access point.

3. In the **Manual Setup AP** section, select the SSID for the device that you want to configure. The default is the 5GHz wireless band defined for your gateway.
4. Select the **Network Authentication** method and then fill in the fields that appear. The default method is **Mixed WPA2 / WPA-PSK**. Detailed instructions are provided for each method in the following sections:
 - "Open and Shared Authentication"
 - "802.1X Authentication"
 - "WPA2 and Mixed WPA2/WPA Authentication"
 - "WPA2-PSK and Mixed WPA2/WPA-PSK Authentication"
5. Click **Apply/Save** to commit your changes.

Open and Shared Authentication

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

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

Manual Setup AP

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

Select SSID:

SmartRG

Network Authentication:

Open

WEP Encryption:

Disabled

Apply/Save

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

The fields on this page are defined below.

Field Name	Description
WEP Encryption	Select the Wired Equivalent Privacy (WEP) mode. Options are Enabled and Disabled . The default is Disabled for Open authentication and Enabled for Shared authentication.
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 default and 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>(Appear 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.

802.1X Authentication

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

Manual Setup AP

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

Select SSID:

Network Authentication:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

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

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

Field Name	Description
RADIUS Server IP address	Enter the IP address of the RADIUS (Remote Authentication Dial In User Service) server associated with your network. RADIUS server is used to authenticate the hosts on the wireless network.
RADIUS Port	Enter the port number for the RADIUS server. Port 1812 is the default and the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port 1645. Options are 1 - 65535.
RADIUS Key	(Optional) Enter the encryption key if needed to authenticate to the specified RADIUS server.
WEP Encryption	This option is set to Enabled and cannot be changed. It enables WEP (Wired Equivalent Privacy) mode.
Encryption Strength	Select the length of the encryption method. Options are 128-bit and 64-bit . 128-bit is the default and is the more robust option for security.
Current Network Key	Select which of the four keys is presently in effect. The default is 2.
Network Key 1-4	Enter up to two encryption keys using the on-screen instructions to achieve the desired security strength. Network Keys 1 & 4 are set automatically and cannot be changed.

WPA2 and Mixed WPA2/WPA Authentication

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

Manual Setup AP

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

Select SSID:

Network Authentication:

Protected Management Frames:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA/WAPI Encryption:

WEP Encryption:

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

Field Name	Description
Protected Management Frames	Select whether management frames are protected. Options are Disabled , Capable , and Required . The default is Disabled .
WPA2 Preauthentication	Select whether clients can pre-authenticate with the gateway while still connected to another AP. Options are Enabled and Disabled . The default is Disabled .
Network Re-Auth Interval	Enter the interval at which the client must re-authenticate with the gateway. The default is 36000 seconds (10 hours).
WPA Group Rekey Interval	Enter the frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are 0 - 65535 seconds. The default is 0 .
RADIUS Server IP address	Enter the IP address of the RADIUS (Remote Authentication Dial In User Service) server associated with your network.
RADIUS Port	Enter the port number for the RADIUS server. Options are 1 - 65535 . Port 1812 is the default and is the current standard for RADIUS authentication per the IETF RFC 2865. Older servers may use port 1645 .
RADIUS Key	(Optional) Enter the encryption key needed to authenticate to the specified RADIUS Server.
WPA/WAPI Encryption	Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are: <ul style="list-style-type: none"> AES: Advanced Encryption Standard. This is the default. TKIP+AES: AES combined with TKIP (Temporary Key Integrity Protocol) allows access by either standard.
WEP Encryption	This option is set to Disabled and cannot be changed.

WPA2-PSK and Mixed WPA2/WPA-PSK Authentication

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

Manual Setup AP

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

Select SSID:

SmartRG

Network Authentication:

WPA2 -PSK

Protected Management Frames:

Disabled

WPA/WAPI passphrase:

.....

[Click here to display](#)

WPA Group Rekey Interval:

0

WPA/WAPI Encryption:

AES

WEP Encryption:

Disabled

Apply/Save

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

Field Name	Description
Protected Management Frames	Select whether management frames are protected. Options are Disabled , Capable , and Required . The default is Disabled .
WPA/WAPI passphrase	Enter the security password to be used by this security configuration. When you click Click here to display , the passphrase appears in a separate window.
WPA Group Rekey Interval	Enter the frequency at which the gateway automatically updates the group key and sends it to connected LAN client devices. Options are 1 - 65535 seconds .
WPA/WAPI Encryption	Select the encryption standard. This field is displays the option most compatible with the selected network authentication method. Options are: <ul style="list-style-type: none">AES: Advanced Encryption Standard.TKIP+AES: AES combined with TKIP (Temporary Key Integrity Protocol).
WEP Encryption	This option is set to Disabled and cannot be changed. It disables WEP (Wired Equivalent Privacy) mode.

MAC Filter

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

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

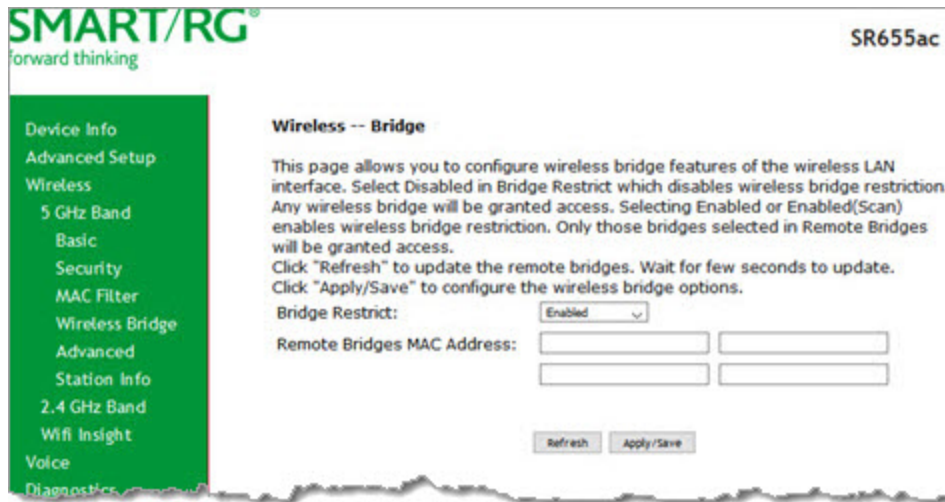
2. In the **Select SSID** field, select the access point that you want to configure.
3. Select the **MAC Restrict Mode**. Options are:
 - **Disabled:** Disable wireless MAC address filtering. This is the default.
 - **Allow:** Allow the wireless clients in the **MAC Address** list to access the wireless network.
Note: For this option to work, you must add at least one MAC address to this page.
 - **Deny:** Reject requests from the wireless clients in the **MAC Address** list to access the wireless network.
4. To add a **MAC Address** to the filter list:
 - a. Click **Add**. The following page appears.

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

Wireless Bridge

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

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



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

Field Name	Description
Bridge Restrict	<p>Enable or disable the bridge restrict function for MAC addresses in the Remote Bridges MAC Address field. Options are:</p> <ul style="list-style-type: none"> • Enabled: Allow only those bridges selected in the Remote Bridges MAC Address table to access the wireless LAN. This is the default. • Enabled (Scan): Allow only those bridges selected in the Remote Bridges MAC Address table to access the wireless LAN but the scanning feature is active. • Disabled: Disable the wireless MAC address filtering function. Any wireless bridge can access the wireless LAN.
Remote Bridges MAC Address	Enter up to four MAC addresses for the remote bridges that are allowed to access the wireless LAN.

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

Advanced

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

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

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

SMART/RG®
forward thinking

SR655ac

Wireless -- Advanced

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

Band: 5GHz
Channel: Auto
Auto Channel Timer(min): 15
802.11n/EWC: Auto
Bandwidth: 40 MHz
Control Sideband: Lower
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
RIFS Advertisement: Auto
OBSS Co-existence: Disable
RX Chain Power Save: Enable
RX Chain Power Save Quiet Time: 10
RX Chain Power Save PPS: 10
S4g Rate: 6 Mbps
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 80
XPress Technology: Enable
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enable
WMM No Acknowledgement: Disable
WMM APSD: Enable
Beamforming Transmission (BFR): Disabled
Beamforming Reception (BFE): Disabled
Band Steering: Disabled
Enable Traffic Scheduler: Disable
Airtime Fairness: Enable

Current: 44
Current: 20MHz
Current: N/A

Power Save status: Low Power

Apply/Save

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

Field Name	Description
Band	The band you are configuring: 2.4 GHz or 5 GHz.
Channel	Select the Wi-Fi channel you want to use. The current channel number displays to the right of the field. For the 5GHz band, options are Auto and 36 through 157. For the 2.4GHz band, options are Auto and 1 - 7. The default is Auto . All devices in your wireless network must use the same channel in order to work correctly.

Field Name	Description
Auto Channel Timer (min)	Enter the frequency (in minutes) at which the gateway scans channels for interference. If a threshold of inference is detected, a new channel will be selected automatically. Options are 0 - 65535 minutes. The default is 15 minutes.
802.11n/EWC	Select whether to enable this standard. Options are Auto and Disabled . The default is Auto . For detailed information about this standard, refer to IEEE 802.11n Draft 2.0.
Bandwidth	Select the operating bandwidth. Options are 20 MHz , 40 MHz , and, for the 5GHz band, 80 MHz . The default is 40MHz . The current bandwidth setting displays to the right of the field.
Control Sideband	This option is set to Lower and cannot be changed.
802.11n rate	Select the desired physical transmission rate. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds (1 - 15), select Use 54g Rate , or select Auto to have the gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client. The default is Auto .
802.11n protection	Select whether to enable 802.11n and legacy clients to both work effectively on the network. Options are: <ul style="list-style-type: none"> Auto: Provides maximum security but produces a noticeable impact on throughput. With this option, RTS/CTS behavior permits legacy clients to become aware of 802.11n transmit times, but decreases overall throughput. This is the default. Off: Provides better throughput.
Support 802.11n client only	Select whether to restrict 802.11b/g clients from accessing the gateway. Options are On and Off . The default is Off .
RIFS Advertisement	RIFS (Reduced InterFrame Speed) is the time in micro seconds by which the multiple transmissions from a single station is separated. This option Improves performance by reducing dead time required between OFDM transmission. Options are Auto and Off . The default is Auto .
OBSS Co-Existence	Coexistence of Overlapping Basic Service Sets (OBSS) prevents overlapping in the 20 MHz and 40 MHz frequencies. Options are: <ul style="list-style-type: none"> Enable: The gateway automatically reverts to 20 MHz channel bandwidth when another WiFi network within 2 channels of its own channel is detected or when a client device with its 40 MHz Intolerant bit set is detected. This is the default. Disable: The gateway advertises and operates in 40 MHz mode regardless of how other nearby networks are configured.
RX Chain Power Save	Select whether power-save mode is enabled. Options are Disable and Enable . The default is Enable . Note : Before setting this parameter, make sure that 802.11n/EWC is set to Auto .
RX Chain Power Save Quiet Time	Enter the number of minutes that will elapse before quiet time begins. The default is 10 minutes.
RX Chain Power Save PPS	Enter the throughput threshold(in seconds) for when the router engages power save mode after the quiet time seconds have elapsed. The default is 10 seconds.
54g Rate	This option is set to 1 Mbps and cannot be changed.

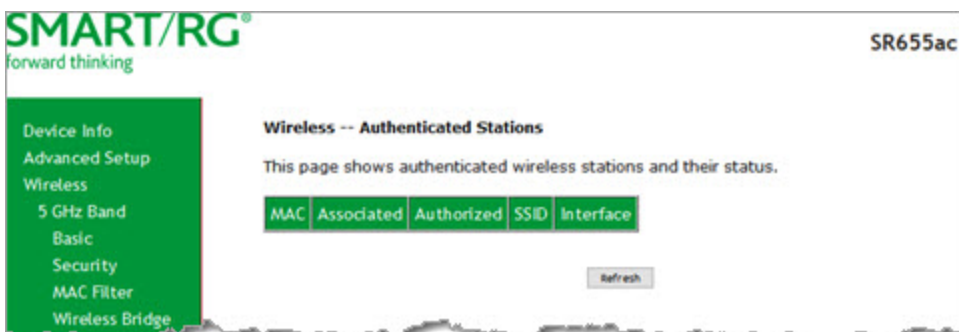
Field Name	Description
Multicast rate	<p>Select the multicast transmission rate for the network according to the speed of your wireless network. Select from a range of transmission speeds or select Auto to have the gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client.</p> <p>Options are Auto and 6 - 54 Mbps. The default value is Auto.</p>
Basic Rate	<p>Select the basic transmission rate ability for the AP. Options are Default, All, and 1 & 2 Mbps and 1 & 2 & 5.5 & 6 & 11 & 12 & 24 Mbps. The default is Default.</p>
Fragmentation Threshold	<p>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.</p> <p>Note: A high packet error rate is an indication that a slightly increased fragmentation threshold is needed. When possible, the default value of 2346 bytes should be maintained. Poor throughput is a likely result of setting this threshold too low.</p>
RTS Threshold	<p>The gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.</p> <p>If a packet is smaller than this setting, the WLAN client hardware does not invoke its RTS/CTS mechanism. Options are 256 - 2347 bytes.</p> <p>The default value of 2347 (disabled) should be left in place unless you encounter inconsistent data flow. In that case, make small reductions to this value until the issue is resolved.</p>
DTIM Interval	<p>Enter the Delivery Traffic Indication Message (DTIM or Beacon rate) countdown variable used to indicate when the next window is available to client devices for listening to buffered broadcast and multicast messages. Options are 1 - 255. The default is 1.</p>
Beacon Interval	<p>Beacon information packets are sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is the period of time (sent with the beacon) that the device waits before sending the beacon again.</p> <p>Enter the time interval (in milliseconds) between beacon transmissions. Options are 1 - 65535 ms. The default is 100 ms, which is recommended.</p>
Global Max Clients	<p>Enter the maximum number of clients that can access this wireless network at one time. The maximum for 5GHz is 80; the maximum for 2.4GHz is 128. The default is the maximum number for each band.</p> <p>Note: You must change this field before you can change the Max Clients on the Wireless > Basic. page.</p>
Xpress™ Technology	<p>Select whether to enable Xpress Technology, a special accelerating technology for IEEE802.11g. Options are Enable and Disable. The default is Enable.</p>
Transmit Power Level	<p>Select the level of power used for transmittals. Options are 4 dBm (2mw), 8 dBm (6 mw), 12 dBm (16 mw), 14 dBm (25 mw), 16 dBm (40 mw), and 18 dBm (60mw). The default is 18 dBm (60 mw).</p>
WMM (WiFi Multimedia)	<p>Select whether to disable 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.</p> <p>Warning: If you disable this option, all QoS queues and classifications defined for the wireless network are also disabled.</p>

Field Name	Description
WMM No Acknowledgment	The acknowledge policy used at the MAC level. Enabling this option allows better throughput but, in a noisy RF environment, higher -963 error rates may result. The default is Disabled , meaning that an acknowledgment packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. Disabling the acknowledgment can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree. Options are Enabled and Disabled . The default is Disabled .
WMM APSD	APSD (Automatic Power Save Delivery) is an automatic power saving feature. Enabling ensures very low power consumption. WMM Power Save is an improvement to the 802.11e amendment, adding advanced power management functionality to WMM. Options are Enabled and Disabled . The default is Enabled .
Beamforming Transmission (BFR)	Select to concentrate the transmission signal at the gateway location. This results in a better signal and potentially better throughput. Options are Disabled and Enabled . The default is Disabled .
Beamforming Reception (BFE)	Select to concentrate the transmission signal at the gateway location. Options are Disabled and Enabled . The default is Disabled .
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 Scheduler	Select whether to enable scheduling of traffic to improve efficiency and increase usable bandwidth for some types of packets by delaying other types. Options are Disable and Enable . The default is Disable .
Airtime Fairness	Select how the gateway will manage the receiving signal with other devices. Options are Disable and Enable . The default is Enable .

Station Info

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

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



To update the data, click **Refresh**.

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**.

SMART/RG®
forward thinking

SR655ac

Configure
In this page you will be able to configure the Wifi Insight system

Sample Interval

☒ 5 Second ☐ 10 Second ☐ 15 Second ☐ 20 Second

Start/Stop Data Collection

Start Data Collection

☐ Start collecting data every

☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

From To

Database Size

Database Size MB

(Please note that, for example, 2 STA's connected using a 5 seconds sample interval run for 1 hour will occupy approximately 1.30 MB of database)

☐ Once Database size reaches maximum limit ☒ Overwrite Older Data ☐ Stop Datacollection

Counters

<input checked="" type="checkbox"/> Channel Statistics	<input checked="" type="checkbox"/> Packet Retried
<input checked="" type="checkbox"/> Chanin Statistics	<input checked="" type="checkbox"/> Queue Utilization
<input checked="" type="checkbox"/> Rx CRS Glitches	<input checked="" type="checkbox"/> Queue Length Per
<input checked="" type="checkbox"/> Bad PLCP	Precedence
<input checked="" type="checkbox"/> Bad FCS	<input checked="" type="checkbox"/> Data Throughput
<input checked="" type="checkbox"/> Packet Requested	<input checked="" type="checkbox"/> Physical Rate
<input checked="" type="checkbox"/> Packet Stored	<input checked="" type="checkbox"/> RTS Fail
<input checked="" type="checkbox"/> Packet Dropped	<input checked="" type="checkbox"/> Retry Drop
	<input checked="" type="checkbox"/> PS Retry
	<input checked="" type="checkbox"/> Acked

Submit

Export Database

[Download Database File](#) **Save Database to File**

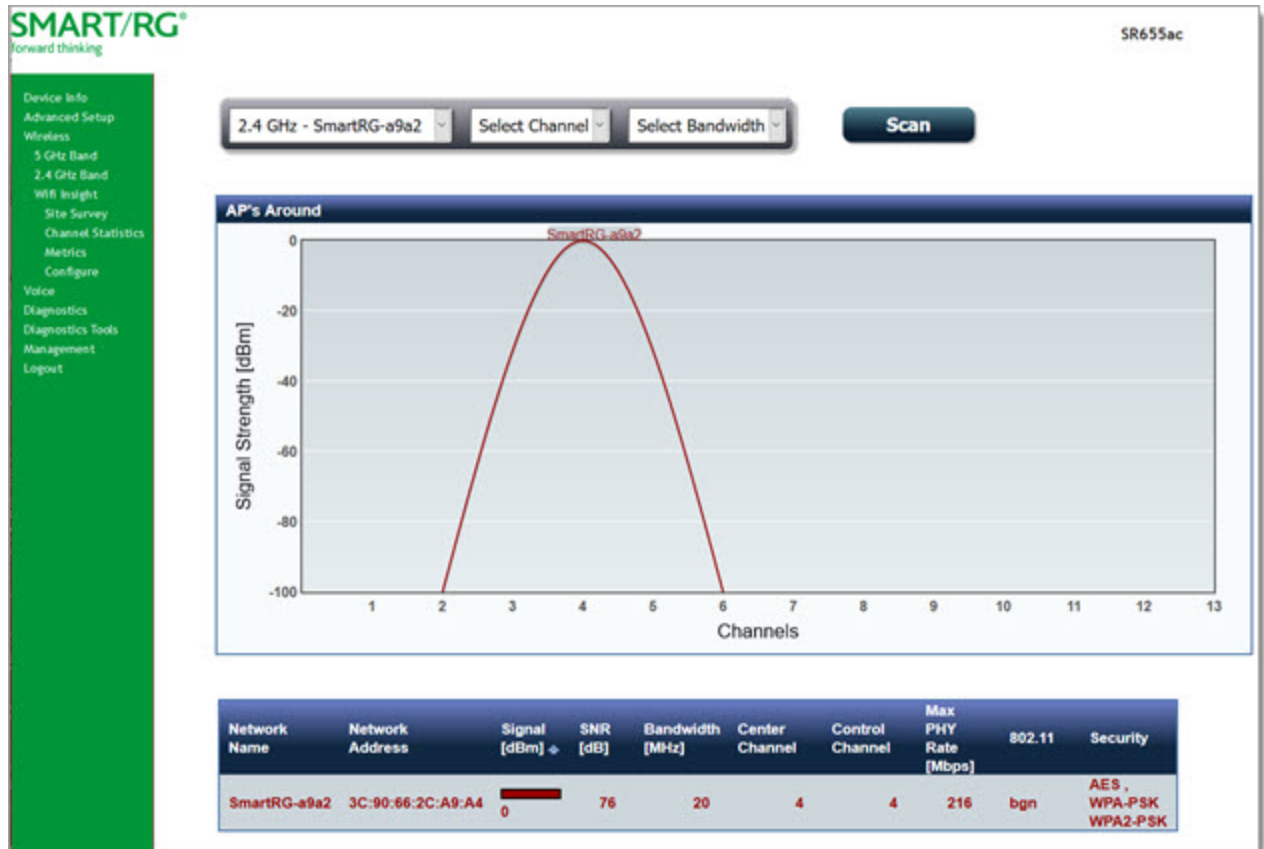
2. In the **Sample Interval** section, select the number of seconds for sampling to occur. Options are 5, 10, 15, and 20 seconds. The default is 5 seconds.

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.
 - a. *(Optional)* In the **Counters** list, clear any counter options that you do not need. The default is to collect all counters.
 - b. Click **Submit** to save the configuration.
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 Datacollection**. The default is **Overwrite Older Data**.
5. 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.

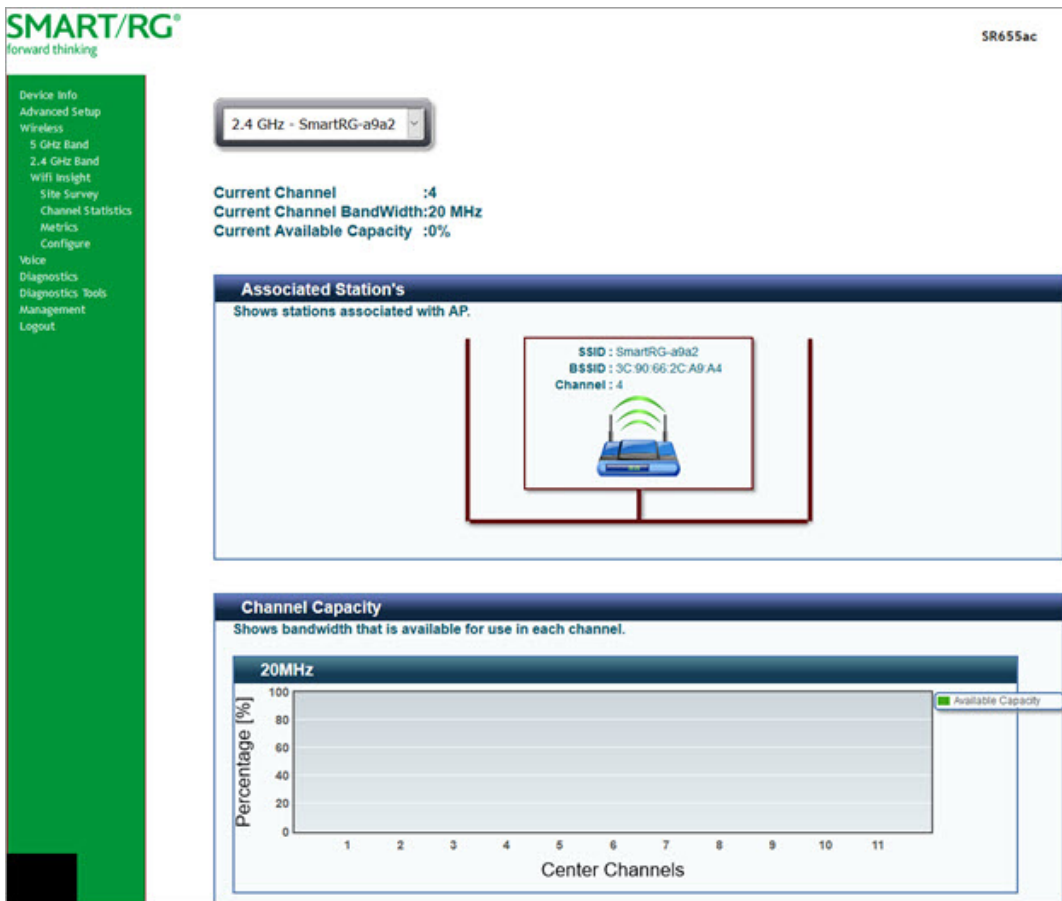


2. In the first field above the chart, select the wireless network that you want to review.
3. In the **Channel** field, select the channel that you want to review.
4. In the **Bandwidth** field, select the bandwidth.
5. Click **Scan**. The page refreshes to show the requested information.

Channel Statistics

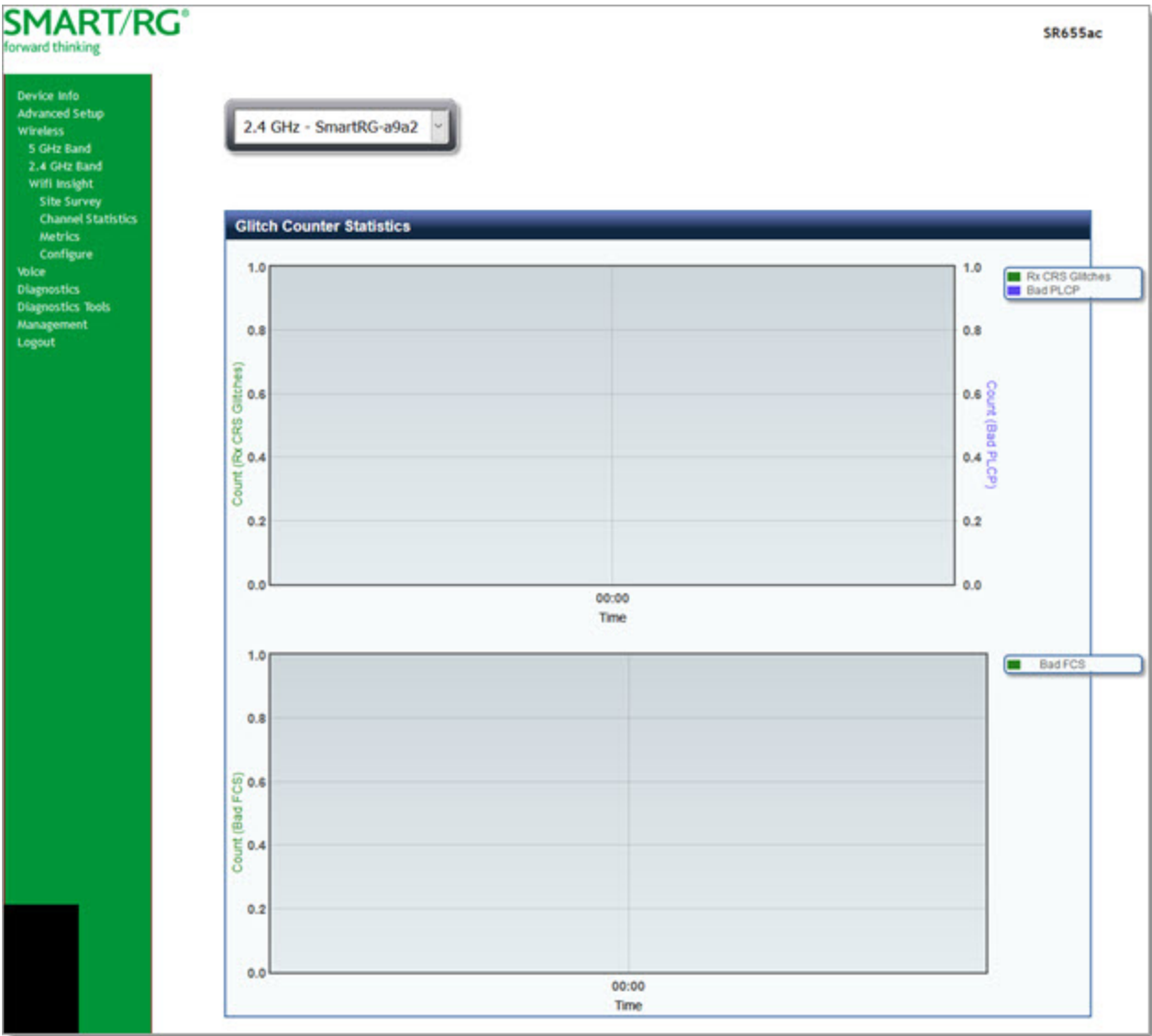
On this page, you can view signal strength, channel capacity, interference, and other details for specific channels.

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.



screen capture for 655.

!!! TW: Replace

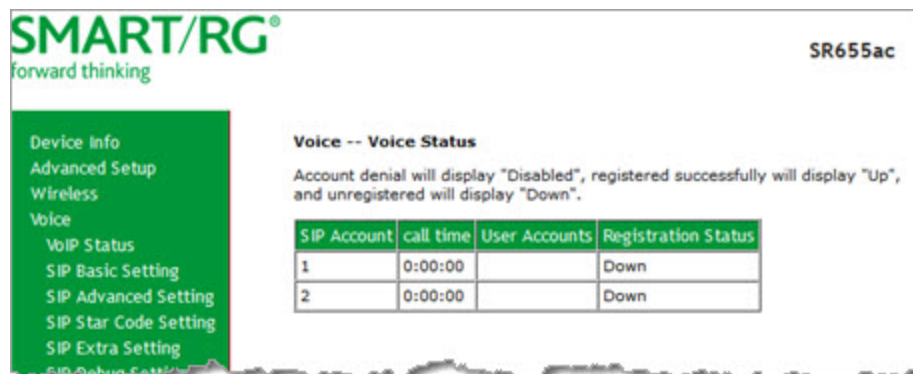
Voice

In this section, you can view status, enable features, and configure settings for VoIP.

VoIP Status

On this page, you can view status data for your SIP accounts.

In the left navigation menu, click **Voice**. The following page appears.



In the **Registration Status** field, **Up** means registered successfully, **Down** means unregistered, **Disabled** means the account is not enabled.

SIP Basic Setting

On this page, you can configure basic SIP settings including proxies and registrars.

1. In the left navigation menu, click **Voice > SIP Basic Setting**. The following page appears.

SMART/RG®
forward thinking

SR655ac

Voice -- SIP Basic Setting

Bound Interface Name: LAN

Country : USA - NORTHAMERICA

sip local port(1-65535): 5060

☐ Use SIP Proxy.

☐ Use SIP Outbound Proxy.

☐ Use SIP Registrar.

☐ Use SIP Proxy2.

☐ Use SIP Outbound Proxy2.

☐ Use SIP Registrar2.

SIP Account	1	2
Account Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Polarity Reverse Enable	<input type="checkbox"/>	<input type="checkbox"/>
Authentication name		
Password		
Cid Name		
Cid Number		

codec-line 1	ptime(ms)	priority	enable	codec-line 2	ptime(ms)	priority	enable
G711u	20	1 (1-100)	<input checked="" type="checkbox"/>	G711u	20	1 (1-100)	<input checked="" type="checkbox"/>
G711A	20	1 (1-100)	<input checked="" type="checkbox"/>	G711A	20	1 (1-100)	<input checked="" type="checkbox"/>
G729	20	2 (1-100)	<input checked="" type="checkbox"/>	G729	20	2 (1-100)	<input checked="" type="checkbox"/>
G723_8k	30	4 (1-100)	<input checked="" type="checkbox"/>	G723_8k	30	4 (1-100)	<input checked="" type="checkbox"/>
G728_24	20	5 (1-100)	<input checked="" type="checkbox"/>	G728_24	20	5 (1-100)	<input checked="" type="checkbox"/>
G728_32	20	6 (1-100)	<input checked="" type="checkbox"/>	G728_32	20	6 (1-100)	<input checked="" type="checkbox"/>
G728_16	20	7 (1-100)	<input checked="" type="checkbox"/>	G728_16	20	7 (1-100)	<input checked="" type="checkbox"/>
G728_40	20	8 (1-100)	<input checked="" type="checkbox"/>	G728_40	20	8 (1-100)	<input checked="" type="checkbox"/>
G722	20	9 (1-100)	<input checked="" type="checkbox"/>	G722	20	9 (1-100)	<input checked="" type="checkbox"/>

Apply

2. Modify the fields as needed, using the information in the following table.
3. Click **Apply** to implement your changes.

The fields on this page are defined below.

FIELD NAME	DESCRIPTION
Bound Interface Name	Select the bound interface name. Options are LAN , Any_WAN , and any other interfaces configured for your network.
Country	Select the country or region for this voice configuration.
SIP local port	Enter the local port of the gateway which is the SIP UA (user agent) port. Options are 1 - 65535 . The default value is 5060 .
Use SIP Proxy	Select this option if your DSL gateway uses a SIP proxy. SIP proxy allows other parties to call DSL gateway through it. When you select this option, the following fields appear: <ul style="list-style-type: none"> • SIP Proxy: The IP address of the proxy. • SIP Proxy port: The port that this proxy is listening on. The default port value is 5060.
Use SIP Outbound Proxy	Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and it is the only way to let SIP traffic pass from the internal network to the Internet. When you select this option, the following fields appear: <ul style="list-style-type: none"> • SIP Outbound Proxy: The IP address of the outbound proxy. • SIP Outbound Proxy port: The port that the outbound proxy is listening on. By default, the port value is 5060.
Use SIP Registrar	Select the checkbox of Use SIP Registrar to register your user ID on the SIP registrar of the proxy. SIP registrar works with SIP proxy, allowing other parties to call DSL gateway through it. When you select this option, the following fields appear: <ul style="list-style-type: none"> • SIP Registrar: The IP address of the SIP registrar. • SIP Registrar port: The port that SIP registrar is listening on. By default, the port value is 5060.
Use SIP Proxy2	Select this option if you need to define a second SIP Proxy. Fill in the fields that appear.
Use SIP Outbound Proxy2	Select this option if you need to define a second SIP outbound proxy. Fill in the fields that appear.
Use SIP Registrar2	Select this option if you need to define a second SIP registrar. Fill in the fields that appear.
SIP Account table	
Account Enabled	If this option is not selected, the corresponding account is disabled and you cannot use it to initiate or accept calls.
Polarity Reverse Enable	Enable or disable this function by selecting and clearing the check boxes.
Authentication name	Enter the user name.
Password	Enter the password.
Cid Name	Enter the user name that should display as the caller ID name.
Cid Number	Enter the number that should display as the caller ID number.
Codec line settings table	
Codec -line 1 / 2	The 1st and 5th columns identify the codec. The most common codec IDs display by default.

FIELD NAME	DESCRIPTION
ptime [ms]	The 2nd and 6th columns identify the packetization time (ptime) which is the length of the digital voice segment that each packet holds. Enter the ptime in milliseconds. The default is 20 millisecond packets. Note: Selecting 10 millisecond packets improves voice quality; less information is lost, but there is more load on the network traffic.
Priority	The 3rd and 7th columns identify the priority of each codec. The priority of the codec is defined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited. However, its voice quality is not as good as other codecs, such as the G711. If you do not select a codec (accepting the default value), the gateway chooses the codec automatically.
Enable	The 4th and 8th columns contain the Enable check boxes. Click to enable a particular codec.

SIP Advanced Setting

On this page, you can configure the advanced VoIP features.

1. In the left navigation menu, click **Voice > SIP Advanced Setting**. The following page appears. Detailed information about each VoIP line is shown in the top table.

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Wireless
Voice
VoIP Status
SIP Basic Setting
SIP Advanced Setting
SIP Star Code Setting
SIP Extra Setting
SIP Debug Setting
Diagnostics
Diagnostics Tools
Management
Logout

Voice -- SIP Advanced Setting

Line	1	2
Call waiting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unconditionally Call forwarding number		
Busy Call forwarding number		
No Answer Call forwarding number		
Options Time	0	0
Forward unconditionally	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Forward on "busy"	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Forward on "no answer"	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MWI	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous call blocking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anonymous calling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Anonymous calling mode	Display anonymous	Display anonymous
DND	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable Call Return	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call Transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Call conference	<input type="checkbox"/>	<input type="checkbox"/>
Warm Line	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warm Line URI		
Warm Line Delay Timer	10	10

===Fax Setting===
 Fax Negotiate Mode: AutoSwitch Bypass Codec: G711A
☐ Enable T38 redundancy support
☐ Enable vhd-red support

In the bottom section are settings for Fax, QoS, caller ID, service offer models and so on.

==Fax Setting==

Fax Negotiate Mode: Auto_switch Bypass Codec: G711_A

☐ Enable T38 redundancy support

☐ Enable vbd redundancy support

==Settings==

☒ Enable VAD support VAD mode in signal: None

☐ Enable RTCP Flow Ctrl

☒ Enable Echo Cancellation

☐ Enable # To ASCII

☐ Enable call waiting callid

==SIP Timer Setting==

Registration Expire: 172800

Timeout:

Session Expire: 86400

Timeout:

Min Session Expire: 90 (need >= 90s)

==Digitmap Setting==

Voip Dialplan Setting: [9]([0-9]*,[1]*[0-9]*[0-9]*[1]*)

==Qos Setting==

DSCP for SIP: DEFAULT (000000)

DSCP for RTP: DEFAULT (000000)

==Payload Setting==

RFC2198 Payload Value: 128 (range 97~127)

Dtmf Relay setting: Inband

==Call ID Setting==

Caller ID send Delay Time: 800 (range 500~1500ms)

Caller ID Message Type: FSK_MDMF

FSK modulation Mode: BellcoreGen

==Transport Setting==

SIP Transport protocol: UDP

==SIP Extends==

PRACK (100rel): SUPPORTED

Agent Header:

==Service Offer Setting==

Complementary business models: Local model

Apply

2. Modify the fields as needed, using the information provided in the table below.
3. Click **Apply** to implement the settings.

The fields on this page are defined below.

FIELD NAME	DESCRIPTION
Line	The VoIP line you want to configure.

FIELD NAME	DESCRIPTION
Call waiting	Select to enable call waiting notification. When users hear the call waiting tone during a call, they press FLASH to put the first call on hold and to answer the second call. Pressing FLASH again switches back to the previous call. Note: Call forward feature settings (Busy or All) take priority over the call waiting feature. The Call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.
Unconditionally Call forwarding number	Enter the number to which you want <i>all</i> incoming calls to be forwarded.
Busy Call forwarding number	Enter the number to which you want all incoming calls to be forwarded when the line is busy.
No Answer Call forwarding number	Enter the number to which you want all incoming calls to be forwarded when the calls are not answered.
Options Time	Enter the time interval for sending the Options message.
Forward unconditionally	Select to enable unconditional forwarding.
Forward on "busy"	Select to enable forwarding when the line is engaged.
Forward on "no answer"	Select to enable forwarding when a call is not answered.
MWI	When the message waiting indicator (MWI) is enabled, the gateway sends a SIP SUBSCRIBE message to the proxy, asking for a notification when its voicemail status changes. When its status does change, the proxy sends a NOTIFY message to the gateway which sounds a MWI tone on the user's receiver.
Anonymous call blocking	Select to block anonymous calls. Users can dial *77 to enable this feature and dial *87 to disable it.
Anonymous calling	Select to enable using an anonymous name as a call number when calling out. Users can dial *68 to enable this feature and dial *82 to disable it.
Anonymous calling mode	Select the anonymous calling mode. Options are Display anonymous or All anonymous .
DND	Select to reject all incoming calls. Users can dial *78 to enable this feature.
Enable Call Return	Select to enable this function.
Call Transfer	Select to enable transferring calls either manually or automatically.
Call conference	Select to enable multiple extensions to join a single call.
Warm Line	Warm lines are configured to dial a specific number after a short delay (entered in seconds). Select to enable the warm line feature.
Warm Line URI	If using the warm line feature, enter the URI to which the line should connect.
Warm Line Delay Timer	Enter the number of seconds before a incoming call to the warm line is transferred.
Fax Setting section	
Fax Negotiate Mode	Select the negotiation mode. Options are Auto_switch and Negotiate .
Bypass Codec	Select the bypass codec. Options are G711_A , G711_MU , and T.38 .
Enable T38 redundancy support	Select to enable this function.
Enable vbd redundancy support	Select to enable this function.
Settings section	

FIELD NAME	DESCRIPTION
Enable VAD support	Select to enable VAD support. Select the VAD mode in signal value. Options are None , Silencsupp , and annexa/annexb/vad .
Enable RTCP Flow Ctrl	Select to enable RTCP flow control for improved quality of service.
Enable Echo Cancellation	Select to enable echo cancellation for improved quality of service.
Enable # to ASCII	Select to enable conversion of numbers to their ASCII equivalents.
SIP Timer Setting section	
Registration Expire Timeout	Enter the registration expire timeout.
Session Expire Time	Enter the time interval for closing a conversation.
Min Session Expire Time	Enter the minimum interval for closing a conversation. This value must be 90 seconds or greater.
Digitmap Setting section	
VoIP DialPlan Setting	Enter the VoIP dial plan parameters. If a user-dialed number matches it, the number is processed by the gateway immediately.
QoS Setting section	
DSCP for SIP	Select the DSCP mark for SIP. The default is DEFAULT (000000) .
DSCP for RTP	Select the DSCP mark for RTP. The default is DEFAULT (000000) .
Payload Setting section	
RFC2198 Payload Value (range 96-127)	Enter the RFC2198 payload value. Options are 96 - 127 .
DTMF Relay Setting	Select the DTMF transmit method. Options are: <ul style="list-style-type: none"> InBand: DTMF events are mixed with user voice in RTP packet. RFC2833: Use RTP packet to encapsulate DTMF events, as specified in RFC 2833. SIP Info: Use SIP INFO message to transmit DTMF digits.
Call ID Setting section	
Caller ID send Delay time	Enter the number of milliseconds that the system will delay before sending the caller ID.
Caller ID Message Type	Select the message format for the caller ID. Options are FSK-MDMF , FSK-SDMF , and DTMF .
FSK modulation Mode	<i>(Appears when an FSK value is selected in the Caller ID Message Type field)</i> Select the modulation mode for FSK message types. Options are BellcoreGen , V23Gen , and V23UK .
Transport Setting section	
SIP Transport Protocol	Select the transport protocol to use for SIP signaling. Note that the SIP proxy and registrar need to support the protocol you select.
SIP Extends section	
PRACK (100rel)	Select to enable provisional responses. Options are DISABLE , SUPPORTED , and REQUIRED .
Agent Header	Enter the agent name that you want displayed to users in the response header.
Service Offer Setting section	

FIELD NAME	DESCRIPTION
Complementary business models	Options are Local model , Server model , IMS model , and Undefined . If you select IMS model , the ETSI Malicious call tracing field appears. To enable malicious call tracing option, click the checkbox.

SIP Star Code Setting

On this page, you can set the numbers that are used with the * key to enable and disable various features.

1. In the left navigation menu, click **Voice > SIP Star Code Setting**. The following page appears.

Feature	Activate	Deactivate
Call Return		
Do Not Disturb		
Anonymous Block		
Call Transfer		
Call Transfer Conditionally		
Call Waiting		
Anonymous Call		
Call Forward Unconditionally		
Call Forward Busy		
Call Forward No Answer		
Call Forward		

2. Enter the numbers that you want assigned to various features. Users press the star (*) key and then enter these numbers to enable or disable the various calling features.
3. Click **Apply** to implement your settings.

SIP Extra Setting

On this page, you can set the ring tones and their durations.

1. In the left navigation menu, click **Voice > SIP Extra Setting**. The following page appears.

Line	1	2	
Dial tone time	15	15	10 ~ 20
Busy tone time	40	40	30 ~ 180
Inter digit time	5	5	1 ~ 5
Offhook warning tone time	60	60	30 ~ 180
Ringback tone time	80	80	30 ~ 180
T digit timer	4		
Short digit timer	4		

Apply

2. Modify the fields as needed, using the information in the table below.
3. Click **Apply** to implement the settings.

The fields on this page are defined below.

Field	Description
Line	The VoIP line that you want to configure.
Dial tone time	Enter the number of seconds that the dial tone will persist. Options are 10 - 20 seconds. The default is 15 seconds.
Busy tone time	Enter the number of seconds that the busy tone will persist. Options are 30 - 180 seconds. The default is 40 seconds.
Inter digit time	Enter the number of seconds allowed between dialing individual digits. The valid range is 1 - 5 seconds. The default is 5 seconds.
Offhook warning tone time	Enter the number of seconds that the off-the-hook warning tone will persist. Options are 30 - 180 seconds. The default is 60 seconds.
Ringback tone time	Enter the number of seconds that the ringback tone will persist. Options are 30 - 180 seconds. The default is 80 seconds.
T digit timer	Enter the maximum number of seconds that the system waits to dial after the last digit has been entered. The default is 4 seconds.
Short digit timer	Enter the maximum number of seconds allowed between dialed digits. The default is 4 seconds.

SIP Debug Setting

On this page, you can configure the debugging settings.

1. In the left navigation menu, click **Voice > SIP Debug Setting**. The following page appears.

2. Modify the fields as needed, using the information in the table below.
3. Click **Apply** to implement the settings.

The fields on this page are defined below.

Field	Description
Vodsl Console Log Level	(Optional) Select the level of detail stored in the VODSL Console log. Options are Error , Notice , and Debug .
System Log Level	(Optional) Select the level of detail stored in the System log. Options are SPY_GEN_INFO , SPY_FNENTER , SPY_EVENT , SPY_MINOR_ERR , SPY_MAJOR_ERR , SPY_FATAL_ERR , and SPY_LEVEL_OFF . The default is SPY_EVENT .

Field	Description
Protocol Stack Log Level Call Control Log Level Register Log Level DSP Log Level Tele Log Level Dialplan Log Level Restart Log Level	(Optional) Select the level of detail stored in these logs. Options are SPY_GEN_INFO , SPY_FNENTER , SPY_EVENT , SPY_MINOR_ERR , SPY_MAJOR_ERR , SPY_FATAL_ERR , and SPY_LEVEL_OFF . The default is SPY_MAJOR_ERR .
Master Level Control settings section	
Master Level	(Optional) Select the lowest level of log entries for VoIP. When debugging, this level must be lower than the levels selected in the other fields in this section. Options are Emerg , Alert , Crit , Error , Warn , Notice , Info , and Debug . The default is Crit .
LOGIC PROVISION VOICE AGENT	(Optional) Select the level of logging for these modules. Options are Emerg , Alert , Crit , Error , Warn , Notice , Info , and Debug . The default is Error .
SIP log server IP address	Enter the IP address of the server where the SIP logs should be stored.
SIP log server port	Enter the port number for the same server.
Gain Settings table	(Optional) Select the gain levels for incoming and outgoing transmissions for each line. Options are -14 to 6 .

Diagnostics

Line performance diagnostic tools are supported by your SmartRG gateway. Three legs of the data path are included in the available tests: LAN connectivity, DSL connectivity, and Internet connectivity tests.

Diagnostics

On this page, you can test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.

1. In the left navigation bar, click **Diagnostics**. The following page appears, showing information about the connection encountered by the gateway.

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Wireless
Voice
Diagnostics
Diagnostics Tools
Ethernet OAM
Diagnostics Tools
Management
Logout

ipoe_0_0_35Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ETH1 Connection:	FAIL	Help
Test your ETH2 Connection:	PASS	Help
Test your ETH3 Connection:	FAIL	Help
Test your ETH4 Connection:	FAIL	Help
Test your Wireless Connection:	5 GHz:ON 2.4 GHz:ON	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

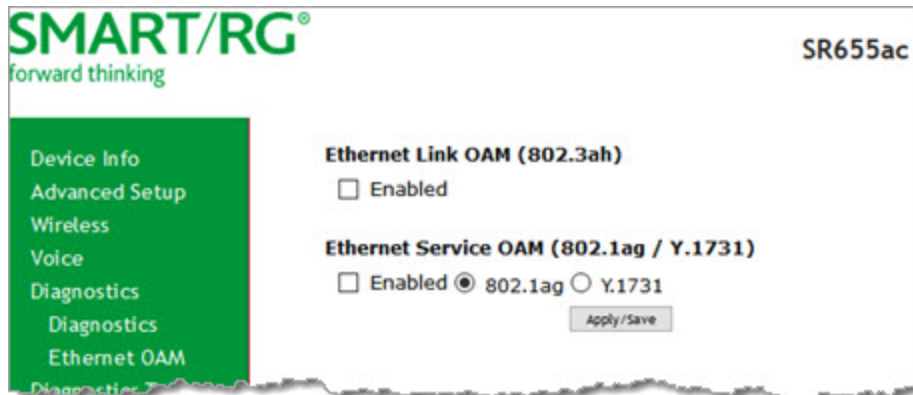
Next Connection
Test Test With OAM F4

2. To run a test (and refresh the data), click the appropriate **Test** button.
The table is updated with fresh diagnostic information regarding connection integrity.
3. To test another connection, click **Next Connection**. The data refreshes and the **Previous Connection** button appears.
4. If a test fails, click the **Help** link located in the last column to learn more about what is being tested and what actions you can take.

Ethernet OAM

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

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



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

Ethernet Link OAM (802.3ah)

☒ Enabled

WAN Interface:

OAM ID: (positive integer)

☐ Auto Event

☐ Variable Retrieval

☐ Link Events

☐ Remote Loopback

☐ Active Mode

- b. Modify the fields as needed, using the information in the **Ethernet Link OAM (802.3ah)** section of the table below.
3. To enable **Ethernet Service OAM (802.1ag/Y.1731)**:
 - a. Click the **Enabled** checkbox. Additional fields appear showing values for 802.1ag. To configure Y.1731, click the **Y.1731** radio button. The page refreshes.

Ethernet Service OAM (802.1ag / Y.1731)

☒ Enabled
 ☒ 802.1ag
 ☐ Y.1731

WAN Interface:

MD Level: [0-7]

MD Name: [e.g. Broadcom]

MA ID: [e.g. BRCM]

Local MEP ID: [1-8191]

Local MEP VLAN ID: [1-4094] (-1 means no VLAN tag)

☐ CCM Transmission

Remote MEP ID: [1-8191] (-1 means no Remote MEP)

Loopback and Linktrace Test

Target MAC: [e.g. 02:10:18:aa:bb:cc]

Linktrace TTL: [1-255] (-1 means no max hop limit)

Loopback Result:	N/A			
Linktrace Result:	N/A			

- 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.

The fields on this page are defined below.

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

Field Name	Description
Remote Loopback	Click to enable on-demand link diagnostics, including bit-error-rate approximation.
Active Mode	Click to enable this feature.
Ethernet Service OAM (802.1ag/Y.1731) section	
WAN Interface	Select the WAN interface that you want to test.
MD Level	<i>(Appears for the 802.1ag option only)</i> Select the domain level for this maintenance 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.
MA ID	<i>(Appears for the 802.1ag option only)</i> Enter the maintenance association ID, e.g., BRCM.
MEG Level	<i>(Appears for the Y.1731 option only)</i> Enter the level of the maintenance entity group.
MEG ID	<i>(Appears for the Y.1731 option only)</i> Enter the ID of the MEG.
Local MEP ID	Enter the ID of the local maintenance entity group end point.. Options are 1 - 8191. The default is 1.
Local MEP VLAN ID	Enter the VLAN ID of the local MEP. Options are 1 - 4094. The default is -1 (no VLAN tag).
CCM Transmission	Click to enable continuity check message transmission.
Remote MEP ID	Enter the ID of the remote MEP. Options are 1 - 8191. The default is -1 (no remote MEP).
Loopback and 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 limit).
Loopback Result	Displays the results of the loopback test.
Linktrace Result	Displays the results of the linktrace test.

Diagnostic Tools

In this section, you can ping or trace the communication route, and start or stop your DSL connection.

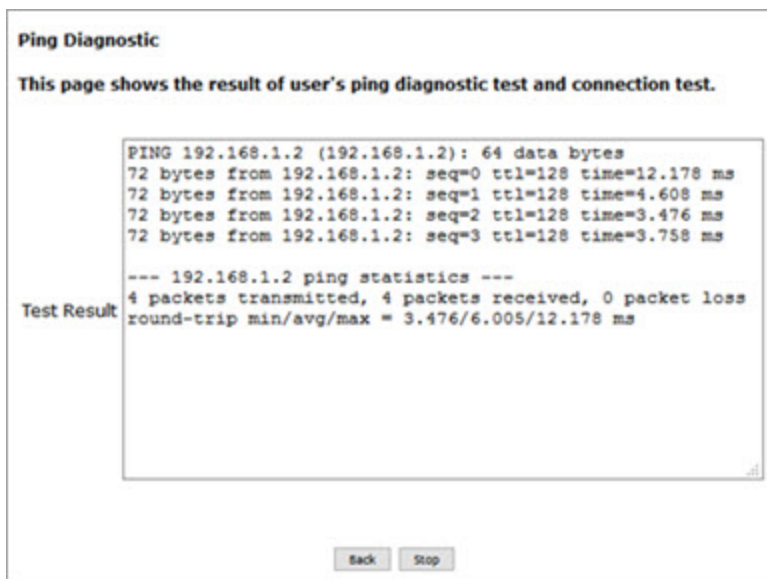
Ping

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

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



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



4. To return to the Ping Diagnostic page, click **Back**.
5. To stop a test, click **Stop**.

Traceroute

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

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

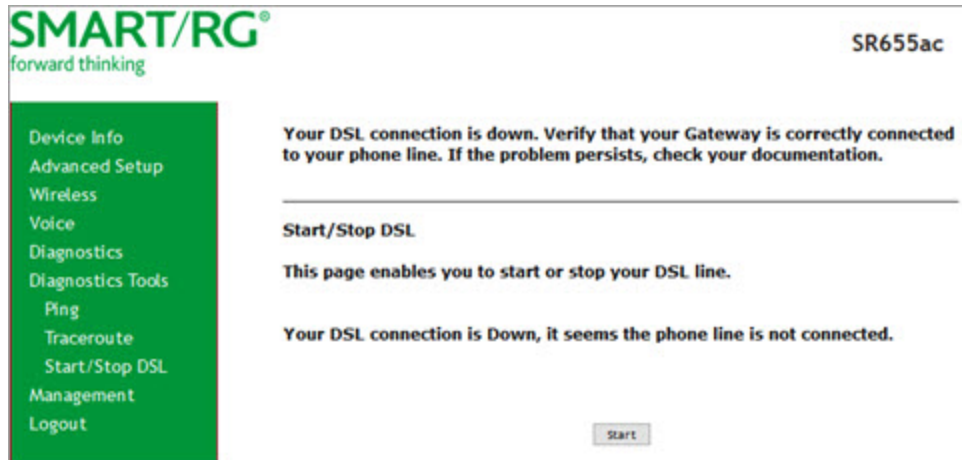
2. Enter the host name or IP address.
3. Click **Submit**. The details of the trace appear on the page.

4. To return to the Traceroute Diagnostic page, click **Back**.
5. To stop a test, click **Stop**.

Start / Stop DSL

On this page, you can start or stop your DSL connection.

1. In the left navigation menu, click **Diagnostics Tools > Start/Stop DSL**. The following page appears.



2. To connect to your DSL, click **Start**. A message appears, with instructions for refreshing the page. When the connection is ready, the "DSL connection is up" message appears.
3. To stop your connection, click **Stop**. A message appears, stating that your DSL connection is down.

Management

In this section, you can configure server and system log settings, control access, and configure clients.

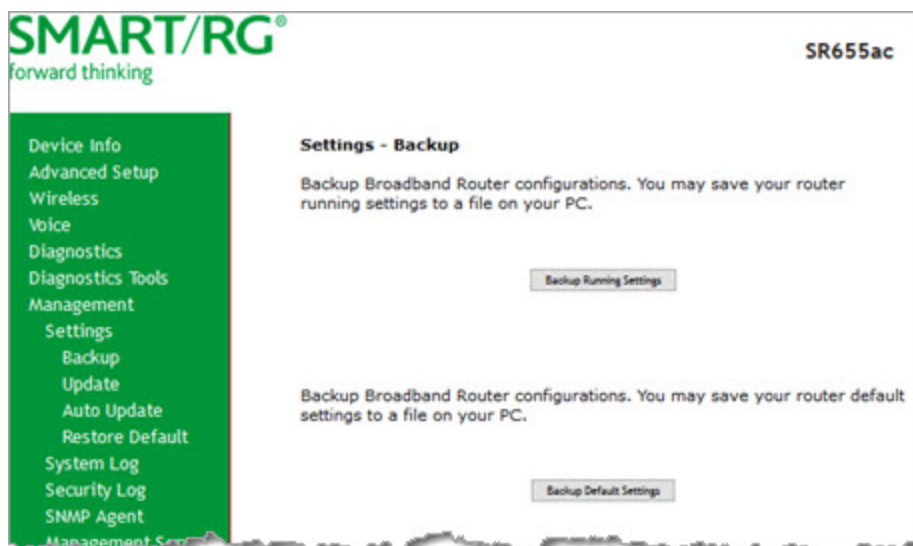
Settings

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

Backup

On this page, you can back up the current settings for your gateway in a file stored on your computer.

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

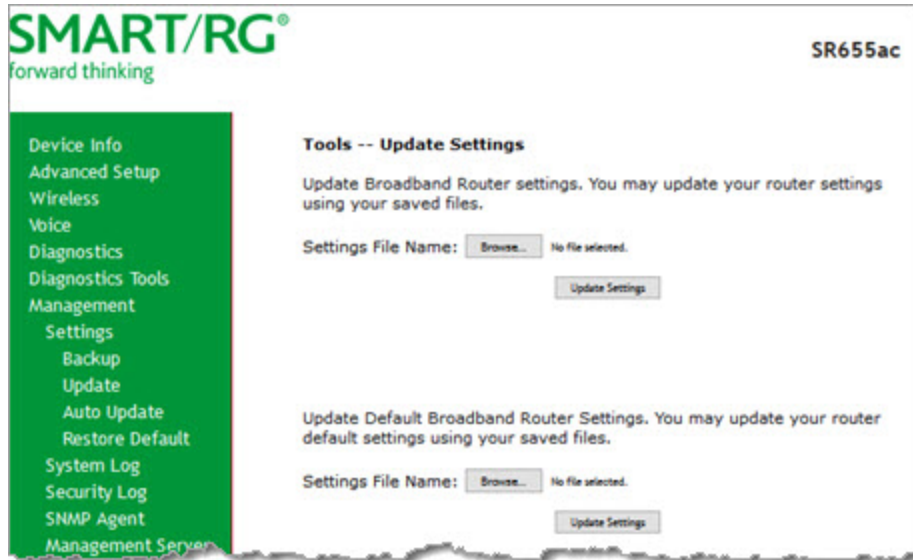


2. To back up the current *running* settings:
 - a. Click **Backup Running Settings**. The Opening file dialog box appears.
 - b. Click **OK**. The file is saved to your default download location and is named "backupsettings.conf".
3. To back up the current *default* settings:
 - a. Click **Backup Default Settings**. The Opening file dialog box appears.
 - b. Click **OK**. The file is saved to your default download location and is named "backupdefaultsettings.conf".

Update

On this page, you can restore previously backed-up gateway settings.

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

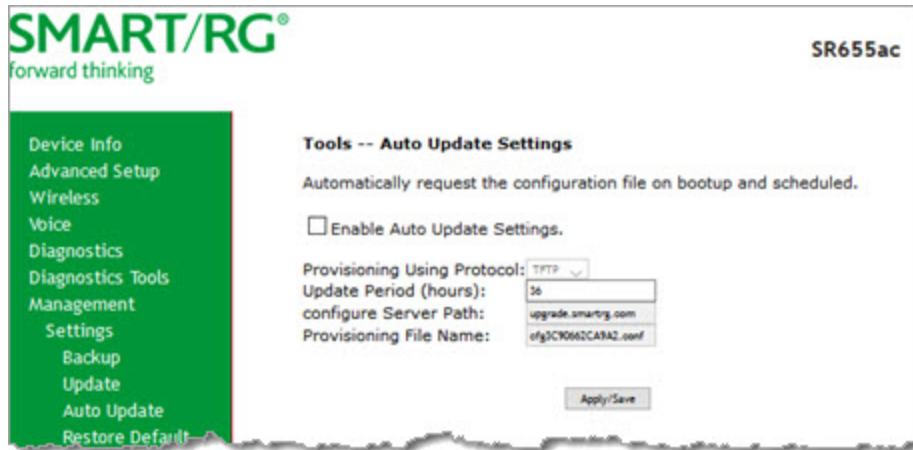


2. To update settings from a file that you saved previously:
 - a. Click the **Browse** button to locate either a customized setting file or the default setting file (.conf file) on your local system and click **Open**.
 - b. Click **Update Settings**. The gateway reboots when the update has completed.

Auto Update

On this page, you can configure the gateway to automatically request the latest configuration file on bootup and as scheduled. This feature is disabled by default.

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

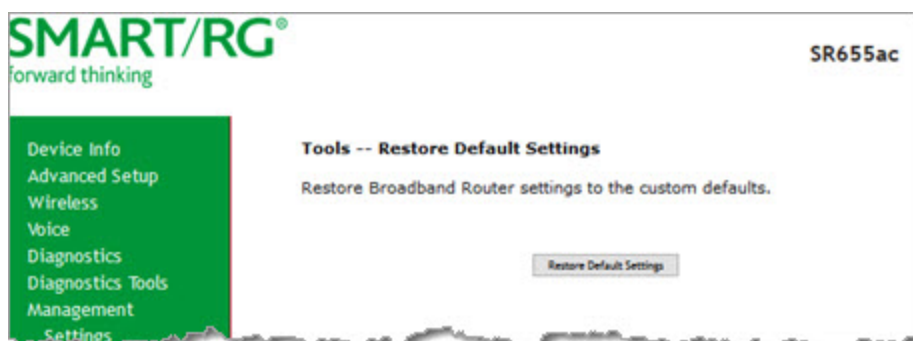


2. Click **Enable Auto Update Settings**.
3. In the **Update Period (hours)** field, enter the number of hours between automatic updates. The default is **36** hours. The **Provisioning Using Protocol**, **configure Server Path**, and **Provisioning File Name** fields cannot be changed.
4. Click **Apply/Save** to implement your changes.

Restore Default

On this page, you can restore the gateway to the factory default settings. If you think you might need to reload the current settings, create a backup (on the **Management > Settings > Backup** page) before proceeding.

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

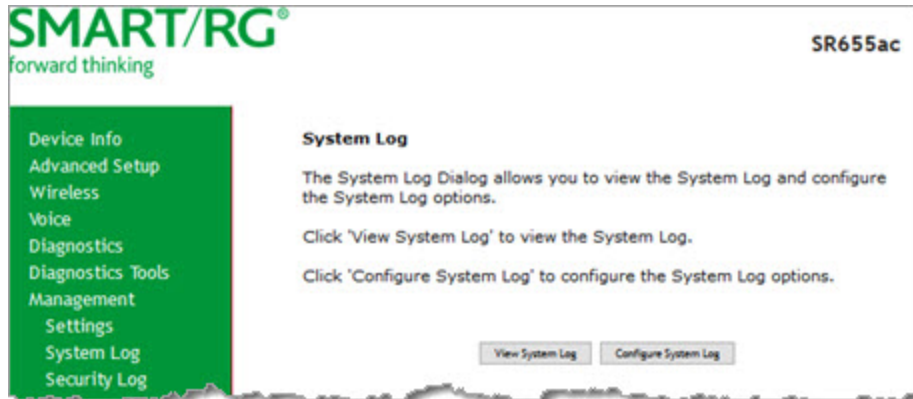


2. Click **Restore Default Settings**. The system returns to the default settings and reboots.

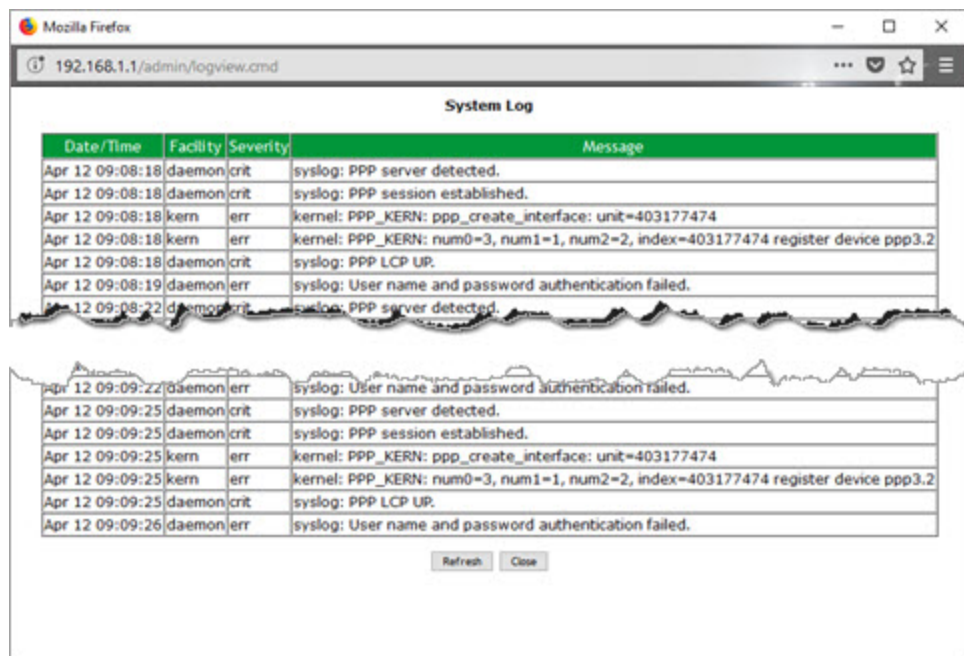
System Log

The System Log page displays a history of error conditions and other events encountered by your gateway. You can configure the system log and view the security log.

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



2. To view the system log details:
 - a. Click **View System Log**. The log appears in a separate window.



- b. To update the data, click **Refresh**.

3. To configure the log settings:

- a. Click **Configure System Log**. The following page appears.

- b. Modify the fields as needed, using the information in the table below.
- c. Click **Apply/Save** to save and apply your changes. You are returned to the System Log page.

The fields on this page are defined below.

Action	Description
Log Level	Select the type of information that you want logged. Options are Emergency , Alert , Critical , Error , Warning , Notice , Informational , and Debugging . The options are listed in order from least detailed to most detailed. The default is Debugging .
Display Level	Select the level of information that should be displayed. Options are Emergency , Alert , Critical , Error , Notice , Warning , Informational , and Debugging . The options are listed in order from least detailed to most detailed. The default is Error . This level is recommended (least verbose) unless you are actively troubleshooting a situation with a subscriber for which increased detail is required.
Mode	Select where log events will be sent. Select Remote or Both to send to the specified IP address and UDP port of a remote syslog server. Select Local or Both to record events in the local memory of your gateway. The default is Local . When you select Remote or Both , additional fields appear. Enter the IP address and port number for the remote syslog server.

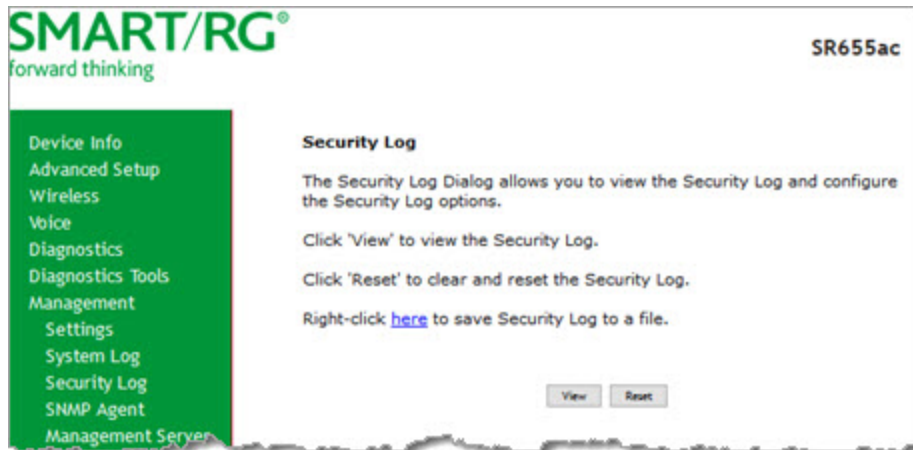
Security Log

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

- Password change success / failure
- Authorized login success / failure

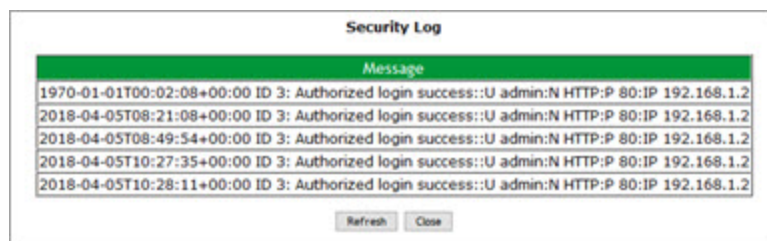
- Authorized user logged out
- Security lockout added / removed
- Authorized / unauthorized resource access
- Software update

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



2. Do any of the following:

- To view the log, click **View**. The log appears in a separate window.



- To purge the log entries and start fresh, click **Reset**. A confirmation message appears. Click **Close**.
- To export the log to a local drive, right-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 text file and save the file.

SNMP Agent

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

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

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

The fields on this page are defined below.

Field Name	Description
SNMP Agent	This option is disabled by default. Click Enable to enable the SNMP agent.
Read Community	Select whether access to the network community is restricted. Options are public and private . The default is public .
Set Community	Select whether access to the write (set) community is restricted. Options are public and private . The default is private .
System Name	Enter the name of the system.
System Location	(Optional) Enter the location of the system.
System Contact	(Optional) Enter the contact for the system.
Trap Manager IP	(Optional) Enter the IP address where the trap manager is installed.

Management Server

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

TR-069

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

the default settings, consult the materials provided by your ACS vendor to determine the appropriate parameters and server settings.

SmartRG products can accommodate several ACS products, including:

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

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

SMART/RG®
forward thinking

SR655ac

Device Info
Advanced Setup
Wireless
Voice
Diagnostics
Diagnostics Tools
Management
Settings
System Log
Security Log
SNMP Agent
Management Server
TR-069 Client
STUN Config
XMPP Connection
Internet Time
Access Control
Update Software
Reboot
Logout

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click 'Apply/Save' to configure the TR-069 client options.

TR-069 Client ☐ Disable ☒ Enable

ACS URL from DHCP: ☐ Enabled

OUI-Serial ☒ MAC ☐ Serial Number

Inform ☐ Disable ☒ Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console ☒ Disable ☐ Enable

☐ Connection Request Authentication

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

The fields on this page are defined below.

Field Name	Description
TR-069 Client	This option is enabled by default. To disable this feature, click the Disable button.
ACS URL from DHCP	Click to enable the gateway to obtain the ACS URL from the DHCP server.
OUI-Serial	Select whether to use the MAC address or the device serial number as the identifier. The default is MAC .
Inform	Select whether to disable this function.

Field Name	Description
Inform Interval	Enter the frequency (in seconds) at which the CPE (gateway) checks in with the ACS to sync and exchange data. A typical production environment has CPEs informing to the ACS once a day or every 86,400 seconds.
ACS URL	Enter the URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication. You can include a port specification suffix if your ACS platform requires it, e.g., <code>http://customer1.acs.smartrg.com:30005</code> where 30005 is the port number. The default port is 30005 .
ACS User Name	Enter the user name by which this gateway logs in to the ACS. This is usually "admin".
ACS Password	Enter the password to authenticate the above user name. This is usually "admin".
WAN Interface used by TR-069 client	Select any_WAN , LAN , Loopback or any configured connection to identify how this gateway will connect to the ACS.
Display SOAP messages on serial console	Select whether to enable the display of messages on consoles.

3. (Optional) To configure the modem client Connection Request mechanism used by your ACS for communication with subscriber gateways, click **Connection Request Authentication**. Additional fields appear.

Note: Consult with your ACS vendor for any specific connection request requirement impacted by the following settings.

Field Name	Description
Connection Request Username	Enter the user name by which this gateway authenticates the ACS. For example, many ACS platforms use "admin" or "tr069".
Connection Request Password	Enter the password by which this gateway will authenticate to the ACS.
Connection Request Port	(Optional) Enter the port number, e.g., "http://xxx.xxx.xxx.xxx:30005/" where the xxx values are specific WAN IP octet numbers. The default port value is 30005 .
Connection Request URL	This URL is set automatically and cannot be changed. It includes the request port number, e.g., <code>http://10.101.40.115:30005/</code> .

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

STUN Config

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

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

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

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

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

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

3. Modify the fields using the information provided in the following table.
4. Click **Save/Apply** to commit your changes.

The fields on this page are defined below.

Field Name	Description
STUN Server Address	Enter the physical STUN server's assigned network address. An invalid address will produce an immediate on-page error message from the gateway. You can enter a maximum of 256 characters An ACS server may also have STUN functionality running on the same physical box. Consult your ACS vendor for implementation options and also TR-069 protocol documentation, if necessary.
STUN Server Port	Enter the port number associated with your STUN server infrastructure. Options are 0 - 64435. The default is 3478.
STUN Server User Name	Enter the username by which the gateway accesses the STUN infrastructure. Maximum length is 256 characters. Special characters are accepted.
STUN Server Password	Enter the password by which the modem authenticates the above username to the STUN infrastructure. Maximum length is 256 characters. Special characters are accepted. The value will be hidden.
STUN Server Maximum Keep Alive Period *	Enter the maximum time(in seconds) that the keepalive function should be active. Options are 0-Unlimited. The default is -1 (no maximum limit).
STUN Server Minimum 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 for refreshing NAT bindings with using Restricted Cone NAT or Port Restricted Cone NAT. A device's internal address / port mappings (which the STUN protocol can use) can have keep alive values attributed. These minimum and maximum keep alive times define the minimum time to retain the mapping information that STUN has discovered, and the maximum time to retain that information, before refreshing it through forced re-discovery.

With these NAT schemes, the initial network address translation may not be used after a specified elapsed time. Internal mapping is dropped. The gateway then assigns a different address mapping. This mechanism allows for coordinated refresh on the bindings for mappings used by the STUN protocol. For further information, review STUN-related RFCs.

Selecting appropriate values for these two fields is influenced by a various environmental factors including device types deployed, services employed and NAT configuration options enabled within the topology.

XMPP Connection

On this page, you can configure a connection between the gateway and an XMPP server.

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

SMART/RG®
forward thinking

SR655ac

XMPP -- Connection Setup

XMPP connection allows CPE to connect with XMPP server to advertise IP addresses of devices on the LAN side. A maximum 32 entries can be configured.

User Name	Domain	Resource	Jabber ID	Use TLS	Established TLS	Server Address	Server Port	Last Change Date	Status	Remove
<div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>										

2. To add a connection, click **Add**. The following page appears.

SMART/RG®
forward thinking

SR655ac

XMPP -- Connection Add

The Connection represents a XMPP connection between the device and a server. The Username, Domain and Resource comprise the full identity (JabberID) of this Connection for this device.

To setup XMPP connection, username, and password are required, but domain, resource, and use TLS can be optional. After entering specific information, click "Apply/Save" to add XMPP connection.

XMPP Connection ☐ Use TLS ☐ Enable

Username:

Password:

Domain:

Resource:

XMPP Server Address:

XMPP Server Port:

3. In the **XMPP Connection** field, select whether to use TLS and then click **Enable**.
4. Modify the fields as needed, using the information provided in the table below.

Field	Description
Username	Enter the username for accessing the XMPP server.
Password	Enter the password for accessing the XMPP server.
Domain	(Optional) Enter the domain for this connection.
Resource	(Optional) Enter a descriptive name for this connection.

Field	Description
XMPP Server Address	Enter the IP address for the server.
XMPP Server Port	Enter the port for the IP address entered above.

- Click **Apply/Save** to save and apply the settings.
- To remove a connection, click the **Remove** checkbox to the right of the entry and then click the **Remove** button.

Internet Time

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

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

SMART/RG®
forward thinking

SR655ac

Time settings

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server: time.nist.gov
 Second NTP time server: ntp1.summy.com
 Third NTP time server: None
 Fourth NTP time server: None
 Fifth NTP time server: None

Current Router Time: Mon Mar 20 13:51:20 2017
 Time zone offset: (GMT-05:00) Eastern Time (US & Canada)

☐ Enable Daylight Savings Time

Apply/Save

- Select the desired time servers.
- Select the **Time zone offset**.
- (Optional) Click **Enable Daylight Savings Time**.
- Click **Apply/Save** to save and apply the settings.
- To disable this feature, click the **Automatically synchronize with Internet time servers** check box to clear it and then click **Apply/Save** to save your changes.

Access Control

In this section, you can manage user passwords and the services that are available for users.

The following user names are assigned specific rights:

- "admin" has unrestricted access
- "support" has general access rights plus additional rights to perform maintenance tasks and run diagnostics.
- "user" can view settings and statistics and update the firmware.

Passwords

On this page, you can modify the username and password of your users.

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

SMART/RG®
forward thinking

SR655ac

Access Control -- Passwords

Access to your broadband 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 Broadband Router.

The user name 'support' is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name 'user' can access the Broadband 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.

Username:

Old Password:

New Password:

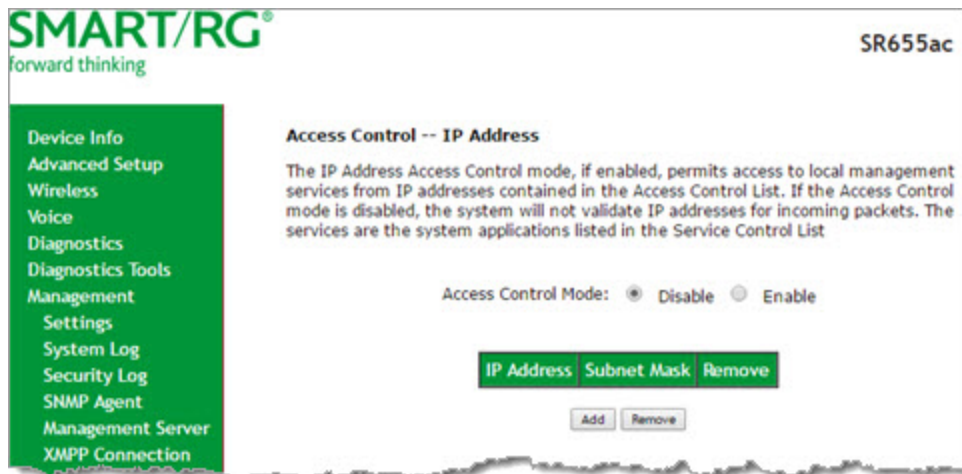
Confirm Password:

2. Enter the user name in the **Username** field.
3. Enter the current password in the **Old Password** field.
4. Enter the new password in the **New Password** and **Confirm Password** fields. Passwords cannot contain spaces.
5. Click **Apply/Save** to implement your changes.

Access List

On this page, you can create list of IP addresses that are allowed to access local management services (defined in the Services Control list). When Access Control mode is disabled, IP addresses for incoming packets are not validated.

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



2. Click **Add**. The following page appears.



3. Enter the IP address and mask of the station allowed to access local management services.
4. Click **Apply/Save**. You are returned to the Access Control - IP Address page.
5. To enable the listed IP addresses to access local management services, in the **Access Control Mode** field, click **Enable**.
6. Click **Apply/Save** to save and apply the settings.
7. To remove a connection, click the **Remove** checkbox to the right of the entry and then click the **Remove** button. If you remove the only entry, **Access Control Mode** is set to **Disable**.

Services Control

On this page, you can enable or disable the different types of services that your gateway can access.

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

SMART/RG®
forward thinking

SR655ac

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

Services	LAN	LAN Port	WAN	Port	WAN Interface
HTTP	<input checked="" type="checkbox"/> enable	80	<input type="checkbox"/> enable	80	ALL ▼
HTTPS	<input checked="" type="checkbox"/> enable	443	<input type="checkbox"/> enable	443	ALL ▼
TELNET	<input checked="" type="checkbox"/> enable	23	<input type="checkbox"/> enable	23	ALL ▼
SSH	<input checked="" type="checkbox"/> enable	22	<input type="checkbox"/> enable	22	ALL ▼
FTP	<input checked="" type="checkbox"/> enable	21	<input type="checkbox"/> enable	21	ALL ▼
TFTP	<input checked="" type="checkbox"/> enable	69	<input type="checkbox"/> enable	69	ALL ▼
ICMP	<input checked="" type="checkbox"/> enable	0	<input type="checkbox"/> enable	0	ALL ▼
SNMP	<input checked="" type="checkbox"/> enable	161	<input type="checkbox"/> enable	161	ALL ▼
SAMBA	<input checked="" type="checkbox"/> enable	445	<input type="checkbox"/> enable	445	ALL ▼

Apply/Save

2. Select or clear the **enable** checkbox next to each service and interface that you want to change.
3. (Optional) In the **LAN Port** and **Port** fields, modify the port numbers for the services.
4. (Optional) In the **WAN Interface** field, select an interface. The default is **ALL** and works best for most environments.
5. Click **Apply/Save** to save and apply the settings.

Logout Timer

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

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

SMART/RG®
forward thinking

SR655ac

Access Control -- Logout Timer

Here you can configure the automatic GUI logout timer.

A value of zero disables the automatic logout feature.

Logout Timer Period (enter a value between 0 and 60 minutes):

Apply/Save

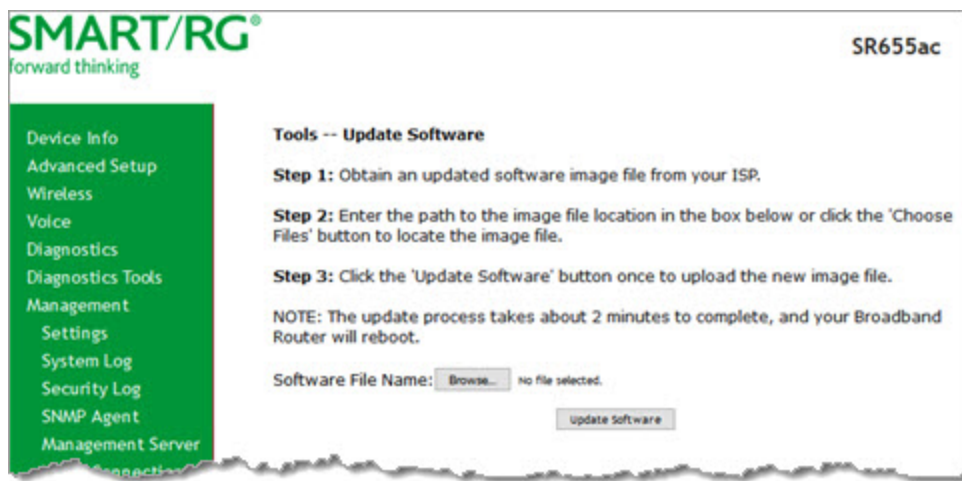
2. In the **Logout Timer Period** field, type the number of minutes after which a session will be ended. Options are **0 - 60** minutes. The default is **15** minutes. To disable this feature, enter a zero (**0**) in the field.

Update Software

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

Note: Make sure that you have downloaded the correct software file as instructed by your ISP.

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



2. Click **Browse** to locate and select the correct software file.
3. Click **Update Software**.

Note: When software update is in progress, do *not* shut down the gateway. After the software update completes, the gateway automatically reboots.

Reboot

On this page, you can reboot your gateway without needing physical access to the unit.

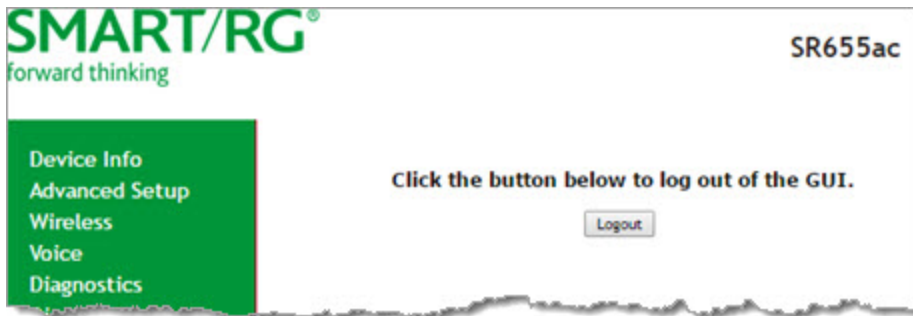
1. In the left navigation, click **Management** > **Reboot**. The following page appears.



2. Click **Reboot**. The gateway reboots and, after a few minutes, the Login dialog box appears.

Logout

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



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

Appendix: 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 numérique 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 and operated with a minimum distance of 20cm between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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 spécifications 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

Revision	Date	LAN ports
1.3	July 2017	Updated to match release 1.0.0.76.
1.2	May 2017	Corrected wireless radio button instructions.
1.1	March 2017	Multiple updates to match current environment.
1.0	AugustOctober 2016	Initial release of this user manual.