

501 SE Columbia Shores Boulevard, Suite 500

Vancouver, Washington 98661 USA

+1 360 859 1780 / smartrg.com

/ Gateway User Manual

Model: SR516ac

Release 1.6

July 2021

Table of Contents

| | |
|---|----|
| Welcome! | 4 |
| Purpose & Scope | 4 |
| Intended Audience | 4 |
| Getting Assistance | 4 |
| Copyright and Trademarks | 4 |
| Disclaimer | 5 |
| Getting Familiar with your Gateway | 6 |
| LED Status Indicators | 6 |
| Connections | 6 |
| External Buttons | 7 |
| 2.4GHz and 5GHz Buttons | 7 |
| Reset Button | 7 |
| Installing your SR516ac Gateway | 8 |
| Logging in to your Gateway's UI | 9 |
| Device Info | 10 |
| Summary | 10 |
| WAN | 10 |
| Statistics | 12 |
| LAN | 12 |
| WAN Service | 12 |
| xTM | 13 |
| xDSL | 14 |
| References | 17 |
| Running xDSL (BER) tests | 18 |
| Route | 19 |
| ARP | 20 |
| DHCP | 20 |
| DHCPv6 | 21 |
| VPN | 22 |
| CPU & Memory | 22 |
| Advanced Setup | 24 |
| Layer2 Interface | 24 |
| ATM Interface | 24 |
| PTM Interface | 27 |
| ETH Interface | 28 |
| WAN Service | 29 |
| PPP over Ethernet WAN Service | 30 |
| IP over Ethernet WAN Service | 38 |
| Bridging | 47 |
| LAN | 50 |
| IPv6 Autoconfig | 53 |
| Ethernet Config | 55 |
| NAT | 56 |
| Virtual Servers | 56 |
| Port Triggering | 59 |
| DMZ Host | 61 |
| Security | 61 |
| IP Filtering - Outgoing | 61 |
| IP Filtering - Incoming | 63 |
| MAC Filtering | 64 |
| Adding a MAC Filter | 65 |
| Parental Control | 66 |
| Time Restriction | 66 |
| Url Filter | 68 |
| Quality of Service | 68 |
| Quality of Service | 69 |
| QoS Queue | 70 |
| WLAN Queue | 72 |

| | |
|---|-----|
| QoS Classification | 73 |
| QoS Port Shaping | 75 |
| Routing | 75 |
| Default Gateway | 75 |
| Static Route | 76 |
| Policy Routing | 77 |
| RIP | 78 |
| DNS | 79 |
| DNS Server | 79 |
| Dynamic DNS | 81 |
| Static DNS | 82 |
| DSL | 82 |
| UPnP | 84 |
| DNS Proxy | 85 |
| Storage Service | 85 |
| Storage Device Info | 85 |
| User Accounts | 86 |
| Interface Grouping | 87 |
| IP Tunnel | 89 |
| IPv6inIPv4 | 90 |
| IPv4inIPv6 | 90 |
| IPSec | 91 |
| Certificate | 95 |
| Local | 95 |
| Creating certificate requests | 96 |
| Importing a local certificate and private key | 97 |
| Trusted CA | 98 |
| Power Management | 99 |
| Multicast | 99 |
| Managing group exception lists | 101 |
| Wireless | 102 |
| Basic | 102 |
| Security | 104 |
| Open and Shared Authentication | 106 |
| 802.1X Authentication | 107 |
| WPA2 and Mixed WPA2/WPA Authentication | 108 |
| WPA2-PSK and Mixed WPA2/WPA-PSK Authentic- ation | 110 |
| MAC Filter | 110 |
| Wireless Bridge | 111 |
| Advanced | 112 |
| Station Info | 116 |
| Wifi Insight | 117 |
| Site Survey | 119 |
| Channel Statistics | 120 |
| Metrics | 121 |
| Diagnostics | 123 |
| Diagnostics | 123 |
| Ethernet OAM | 124 |
| Ping Host | 126 |
| Trace Route to Host | 127 |
| Management | 129 |
| Settings | 129 |
| Backup | 129 |
| Update | 130 |
| Restore Default | 130 |
| System Log | 131 |
| Security Log | 133 |

Table of Contents

| | |
|---|------------|
| SNMP Agent | 134 |
| Management Server | 135 |
| TR-069 | 135 |
| STUN Config | 137 |
| Internet Time | 139 |
| Access Control | 141 |
| Accounts | 141 |
| Add an Account | 141 |
| Modify or Delete an Account | 142 |
| Default Passwords | 143 |
| Services | 143 |
| Passwords | 144 |
| Access List | 145 |
| Logout Timer | 146 |
| Update Software | 147 |
| Reboot | 148 |
| Logout | 149 |
| Appendix: FCC Statements | 150 |
| FCC Interference Statement | 150 |
| FCC Radiation Exposure Statement | 150 |
| FCC - PART 68 | 151 |
| Ringer Equivalency Number Statement | 151 |
| IC CS-03 statement | 151 |
| Canada Statement | 152 |
| 5GHz | 152 |
| Revision History | 153 |

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 SR516ac gateway.

Intended Audience

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

Getting Assistance

Frequently asked questions are provided on the [SmartRG Web site](#).

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

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

Copyright and Trademarks

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

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

Disclaimer

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

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

Getting Familiar with your Gateway

This section contains a quick description of the gateway's lights, ports, and buttons to help you get familiar with the SR516ac model.

LED Status Indicators

The indicator lights (LEDs) on the front of the SR516ac gateway can help you understand the state of your gateway.



Legend: ● Green ● Green Blinking ● Red

| LED | Action | Explanation |
|---|--------|---|
| All LEDs <i>except</i> those listed below | ● | Feature enabled &/or working correctly |
| | ● | Data being transferred |
| POWER | ● | Unit is booting up & preparing for use. When the unit is ready, the light changes to green. |
| | ● | Device powered on and ready for use |
| DSL | ● | DSL connected |
| INTERNET | ● | DSL sync acquired and gateway on line |
| | ● | Data being transferred |
| | ● | Internet authentication / connection has failed |

Connections

The ports located on the back of the gateway 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. |
| 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 Config section of this manual. |

| Feature | Description |
|-----------|---|
| 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 | |
| On/Off | Power switch. |
| 5GHz | Enables or disables the 5GHZ wireless function. |
| 2.4GHz | Enables or disables the 2.4GHZ 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 SR516ac 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 SR516ac Gateway

1. Connect one end of the included phone cable to the **DSL** port on the gateway and connect the other end to the wall jack.
2. Connect one end of an Ethernet cable to a **LAN** port of the gateway and connect the other end to your PC.
3. Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** port of the gateway.
4. Turn on the unit by pressing the On/Off button on the left side of the gateway.

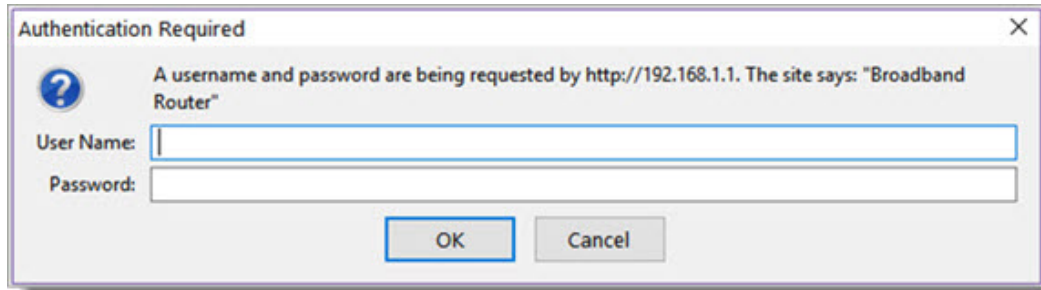
Your gateway is now automatically being set up to connect to the Internet. This process may take a few minutes to complete before you can begin using your Internet applications (browser, email, etc.).

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 SR516ac 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 gateway). The authentication dialog box appears.



3. Enter the user name and password. The default user name and password are admin and admin. It is recommended that you change these default values after logging in for the first time.
4. Click **OK**. The Network 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, 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 information such as the board ID, software 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 menu.

SMART/RG
forward thinking

SR516ac

[Device Info](#)
[Advanced Setup](#)
[Wireless](#)
[Diagnostics](#)
[Management](#)
[Logout](#)

Device Info

| | |
|-----------------------------|------------------------------|
| Board ID: | 963167GWV_004R |
| Symmetric CPU Threads: | 2 |
| Build Timestamp: | 200626_1254 |
| Software Version: | 2.6.2.5 |
| Configuration File Origin: | SmartRG |
| Bootloader (CFE) Version: | 1.0.38-118.8 |
| DSL PHY and Driver Version: | A2pv6F039x5.d26u |
| Wireless Driver Version: | 7.14.164.23.cpe4.16L05.0-kdb |
| Uptime: | 0D 0H 1M 14S |
| System Base MAC Address: | e8:2c:6d:23:9b:b2 |
| Serial Number: | SR516AA069-5005329 |

This information reflects the current status of your WAN connection.

| | |
|-----------------------|--------------|
| LAN IPv4 Address: | 192.168.1.22 |
| Default Gateway: | |
| WAN IPv4 Address: | 0.0.0.0 |
| Primary DNS Server: | 0.0.0.0 |
| Secondary DNS Server: | 0.0.0.0 |
| LAN IPv6 ULA Address: | |
| Default IPv6 Gateway: | ppp0.1 |

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.

| SMART/RG® forward thinking | | | | | | | | | | | | | | SR516ac | |
|-------------------------------|--------------|--------|-----------|----------|----------|---------------|----------|--------------|----------|----------|--|--------------|--------------|---------|--|
| Device Info | | | | | | | | | | | | | | | |
| Summary | | | | | | | | | | | | | | | |
| WAN | | | | | | | | | | | | | | | |
| Statistics | | | | | | | | | | | | | | | |
| Route | | | | | | | | | | | | | | | |
| ARP | | | | | | | | | | | | | | | |
| DHCP | | | | | | | | | | | | | | | |
| DHCPv6 | | | | | | | | | | | | | | | |
| VPN | | | | | | | | | | | | | | | |
| CPU & Memory | | | | | | | | | | | | | | | |
| WAN Info | | | | | | | | | | | | | | | |
| Interface | Description | Type | VlanMuxId | IPv6 | Igmp Pxy | Igmp Src Enbl | MLD Pxy | MLD Src Enbl | NAT | Firewall | Status | IPv4 Address | IPv6 Address | | |
| atm0.2 | ipoe_0_0_35 | IPoE | Disabled | Enabled | Disabled | Disabled | Disabled | Disabled | Enabled | Enabled | IPv4: Unconfigured IPv6: Unconfigured | 0.0.0.0 | (null) | | |
| atm0.3 | br_0_0_35 | Bridge | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Unconfigured | 0.0.0.0 | (null) | | |
| ppp0.1 | pppoe_0_0_35 | PPPoE | Disabled | Enabled | Disabled | Disabled | Disabled | Disabled | Enabled | Enabled | IPv4: Unconfigured IPv6: Unconfigured | 0.0.0.0 | (null) | | |

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 Enbl | 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.

| 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 | | |
| LAN1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| LAN2 | 5930399 | 28328 | 0 | 37 | 0 | 6619 | 18582 | 3127 | 20169822 | 162159 | 0 | 0 | 0 | 8381 | 19609 | 134169 | | |
| LAN3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| LAN4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| 5 GHz | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 8863927 | 150938 | 0 | 109 | 0 | 0 | 150938 | 0 | | |
| 2.4 GHz | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |

The fields on this page are defined below.

| Field Name | Description |
|---|---|
| Interface | Available LAN interfaces. Options are LAN1 - LAN4, 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 menu, 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

SR516ac

Device Info
Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP

Statistics -- WAN

| Service Description | Received | | | | | | | | Transmitted | | | | | | | |
|---------------------|----------|------|------|-------|-----------|---------|-----------|------|-------------|-------|------|-------|-------|-----------|---------|-----------|
| | Total | | | | Multicast | Unicast | Broadcast | | | Total | | | | Multicast | Unicast | Broadcast |
| | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts |
| ipoe_0_0_35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| br_0_0_35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| pppoe_0_0_35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Reset Statistics

The fields on this page are defined below.

| Field Name | Description |
|---|---|
| Service 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.

The screenshot shows the SMART/RG SR516ac web interface. On the left is a navigation menu with options: Device Info, Summary, WAN, Statistics, LAN, WAN Service, xTM (highlighted), and xDSL. The main content area is titled 'Interface Statistics' and contains a table with the following columns: 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, and In Cell Errors. Below the table is a 'Reset' button.

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. |
| 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

SR516ac

Statistics -- xDSL

| | | |
|--------------------------|------------|----------|
| Last Synchronized: | | |
| Retrain Count: | 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: | | |

xDSL BER Test Reset Statistics

2. To run an xDSL (BER) test, follow the instructions in "[Running xDSL \(BER\) tests](#)".
3. To reset the counters, click **Reset Statistics** near the bottom of the page.

The fields on this page are defined below.

| Field Name | Description |
|-------------------|--|
| Last Synchronized | Time when the last synchronization was performed. |
| Retrain Count | 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 . |

| Field Name | Description |
|---|--|
| 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 Ratio (SNR) margin 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) | Typically obtainable sync rate, i.e., the attainable net data rate that the receive PMS-TC and PMD functions are designed to support under the following conditions: <ul style="list-style-type: none"> • Single frame bearer and single latency operation. • Signal-to-Noise Ratio (SNR) Margin 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] |
| 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) | The nominal number of bytes from frame bearer #n per Mux Data Frame at Reference Point A in the current latency path. |
| M (# of Mux Data Frames in FEC Data Frame) | The number of Mux Data Frames per FEC Data Frame in the current latency path. |
| T (Mux Data Frames over sync bytes) | The ratio of the number of Mux Data Frames to the number of sync bytes in the current latency path. |
| R (# of check bytes in FEC Data Frame) | The number of Reed Solomon redundancy bytes per codeword in the current latency path. This is also the number of redundancy bytes per FEC Data Frame in the current latency path. |
| S (ratio of FEC over PMD Data Frame length) | The ratio of FEC over PMD Data Frame length. |
| L (# of bits in PMD Data Frame) | The number of bits from the latency path included per PMD. |
| D (interleaver depth) | The interleaving depth in the current latency path, used to manager error correction. |
| I (interleaver block size in bytes) | The block size used for interleaving data transmissions. |
| N (RS codeword size) | The size of the Reed-Solomon (RS) codeword used for managing error correction. |
| Delay (msec) | The PMS-TC delay in milliseconds of the current latency path (or the lowest latency path when running dual-latency paths). |
| INP (DMT symbol) | The input level for DMT-managed DSL environments. |
| (End of DSL-specific field group) | |
| Super Frames | Number of xDSL Super Frames transmitted/received. |

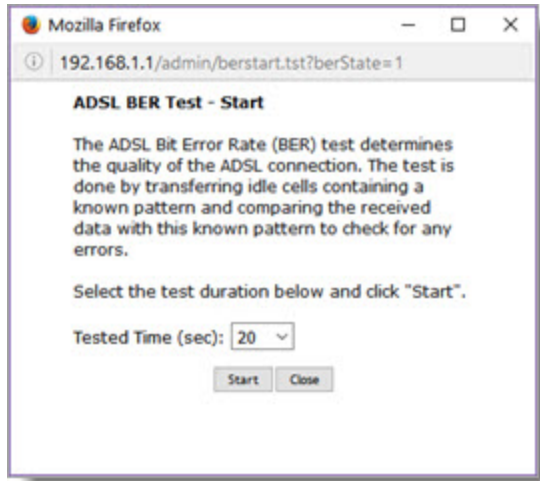
| Field Name | Description |
|-------------------------|--|
| Super Frame Errors | Number of xDSL SuperFrames transmitted/received with errors. |
| RS Words | Number of Reed-Solomon-based Forward Error Correction (FEC) codewords transmitted/received. |
| RS Correctable Errors | Number of Reed-Solomon-based 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. |
| HEC Errors | Count of ATM HEC errors detected. As per ITU-T G.992.1 and G.992.3, a 1-byte HEC is generated for each ATM cell header. Error detection is implemented as defined in ITU-T I.432.1 with the exception that any HEC error shall be considered as a multiple bit error, and therefore, HEC Error Correction is not performed. [1],[2] |
| OCD Errors | Total number of Out-of-Cell Delineation errors. ATM Cell delineation is the process which allows identification of the cell boundaries. The HEC field is used to achieve cell delineation. [4] An OCD Error is counted when the cell delineation process transitions from the SYNC state to the HUNT state. [2] |
| LCD Errors | Total number of Loss of Cell Delineation errors. An LCD Error is counted when at least one OCD error is present in each of four consecutive overhead channel periods and SEF (Severely Errored Frame) defect is present. [2] |
| Total Cells | 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] |
| Total UAS | Total number of Unavailable Seconds. 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). Once unavailable, the xDSL line becomes available at the onset of 10 contiguous seconds with no SESs (excluded from unavailable time). [4] |

References

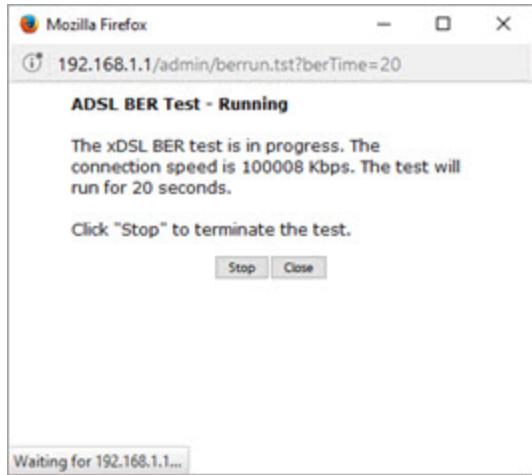
- [1] [ITU-T Recommendation G.992.1 \(1999\), Asymmetric digital subscriber line \(ADSL\) transceivers](#)
- [2] [ITU-T Recommendation G.992.3 \(2005\), Asymmetric digital subscriber line transceivers 2 \(ADSL2\)](#)
- [3] [ITU-T Recommendation G.997.1 \(2006\), Physical layer management for digital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

Running xDSL (BER) tests

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

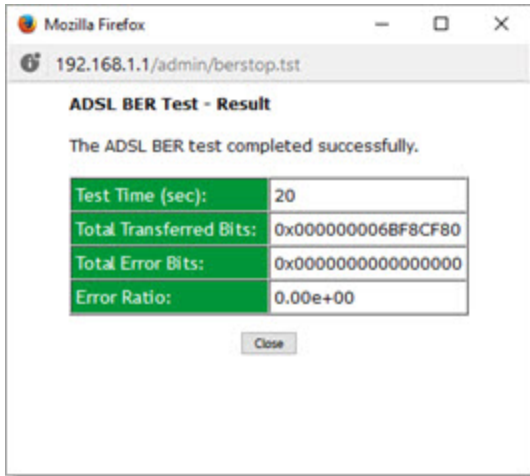


2. In the **Tested Time** field, select the duration in seconds and click **Start**. Options range from **1 second** to **360 seconds**. The test transfers idle cells containing a known pattern and compares the received data with this known pattern. Comparison errors are tabulated and displayed. To stop the test, click **Stop**.



3. When the test completes, a success dialog box appears.


Note: If the Error Ratio 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.


SR516ac

- Device Info
- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- DHCPv6
- VPN
- CPU & Memory
- Advanced Setup
- Wireless
- Diagnostics
- Management
- Logout

Device Info -- Route

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

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

IPv6 Route

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

| Destination | Next Hop | Flag | Metric | Service | Interface |
|-------------|----------|------|--------|---------|-----------|
| fe80::/64 | :: | U | 256 | | br0 |
| fe80::/64 | :: | U | 256 | | eth1 |
| fe80::/64 | :: | U | 256 | | eth4 |

The fields on this page are defined below.

| Field Name | Description |
|-------------|--|
| Destination | Destination IP addresses. |
| Gateway | (For IPv4 only) Gateway IP address. |
| Subnet Mask | (For IPv4 only) Subnet Mask. |
| Next Hop | (For IPv6 only) Identifies the next server in the IPv6 path, if any. |
| 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.

SMART/RG® forward thinking SR516ac

Device Info -- ARP

| IP address | Flags | HW Address | Device |
|-------------|----------|-------------------|--------|
| 192.168.1.2 | Complete | c8:f7:50:b4:61:c1 | br0 |

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 . |
| HW Address | Hardware 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.

SMART/RG® forward thinking SR516ac

Device Info -- DHCP Leases

| Hostname | MAC Address | IP Address | Expires In |
|----------------|-------------------|--------------|----------------------------------|
| kdadamo7390w10 | c8:f7:50:b4:61:c1 | 192.168.1.23 | 23 hours, 39 minutes, 17 seconds |

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. |
| Expires In | Time until the DHCP lease expires for each LAN device. |

DHCPv6

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

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

SMART/RG® forward thinking SR516ac

IPv6 LAN Host Info

| Hostname | MAC Address | IP Address |
|----------|-------------|------------|
|----------|-------------|------------|

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. |

VPN

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

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

The fields on this page are defined below.

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

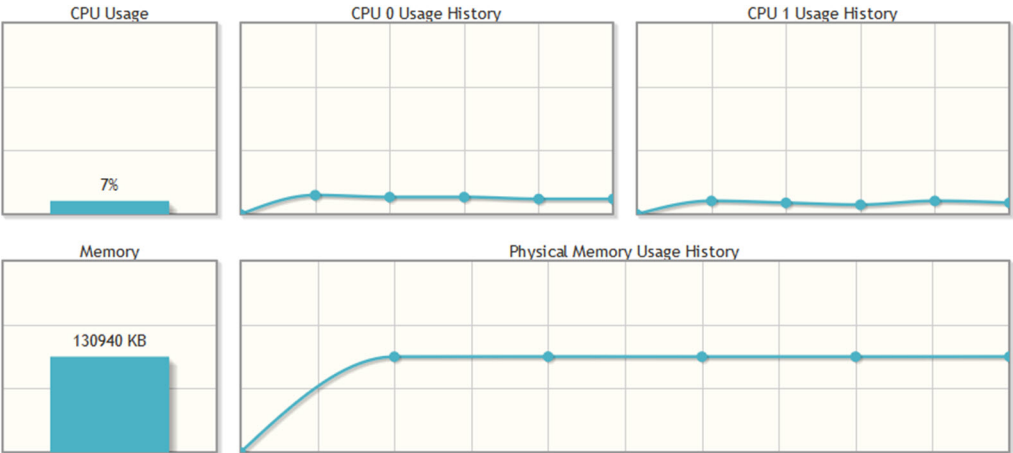
CPU & Memory

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

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

- Device Info
- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- DHCPv6
- VPN
- CPU & Memory**
- Advanced Setup
- Wireless
- Diagnostics
- Management
- Logout

System Performance



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 Circuit (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.

SMART/RG®
forward thinking

SR516ac

Device Info

- Advanced Setup
 - Layer2 Interface
 - ATM Interface
 - PTM Interface
 - ETH Interface
 - WAN Service
 - LAN
 - Ethernet Config
 - NAT
- Security
 - Parental Control
 - Quality of Service
 - Routing
 - DNS
 - DSL
 - UPnP
 - DNS Proxy
 - Storage Service
 - Interface Grouping
 - IP Tunnel
 - IPSec
 - Certificate
 - Power Management
 - Multicast
- Wireless
- Diagnostics
- Management
- Logout

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

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

Select DSL Latency

Path0 (Fast)
 Path1 (Interleaved)

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

EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

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

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin
 Weighted Fair Queuing

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

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

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

2. Modify the settings as 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) . |
| VCI | Enter a Virtual Channel Identifier. A VCI is a 16-bit identifier for a unique channel. Options are 32-65535 . The default is 35 . Note: 1-31 are reserved for known protocols. |

| Field Name | Description |
|---|---|
| Select DSL Latency | Select the level of DSL latency. Options are: <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 | Select the linking protocol. Options are: <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 | Select whether multiple protocols or only one protocol is carried per PVC (Permanent Virtual Circuit). Options are: <ul style="list-style-type: none"> • LLC/ENCAPSULATION: (Available for PPPoA only) Logical Link Control (LLC) encapsulation protocols used with multiple PVCs • LLC/SNAP-BRIDGING: (Available for EoA only) LLC used to carry multiple protocols in a single PVC. • LLC/SNAP-ROUTING: (Available for IPoA only) LLC used to carry one protocol per PVC. • VC/MUX: Virtual Circuit/Multiplexer creates a virtual connection used to carry one protocol per PVC. |
| Service Category | Select the bit rate protocol. Options are: <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. This is the default. • 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. |
| Select Scheduler for Queues of Equal Precedence | Select the algorithm used to schedule queue behavior. VC scheduling is different than scheduling done for default queues. Options are: <ul style="list-style-type: none"> • Weighted Round Robin: Packets are accessed in a round robin style. 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 . |

| Field Name | Description |
|---------------|---|
| 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.

The screenshot shows the PTM Configuration page for device SR516ac. The left navigation bar includes: Device Info, Advanced Setup, Layer2 Interface (selected), ATM Interface, PTM Interface, ETH Interface, WAN Service, LAN, Ethernet Config, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, and Storage Service. The main content area is titled "PTM Configuration" and includes the following settings:

- Select DSL Latency:
 - Path0 (Fast)
 - Path1 (Interleaved)
- Select Scheduler for Queues of Equal Precedence as the Default Queue:
 - Weighted Round Robin
 - Weighted Fair Queuing
- Default Queue Weight: [1-63]
- Default Queue Precedence: [1-8] (lower value, higher priority)
- Default Queue Minimum Rate: [1-0 Kbps] (-1 indicates no shaping)
- Default Queue Shaping Rate: [1-0 Kbps] (-1 indicates no shaping)
- Default Queue Shaping Burst Size: [bytes] (shall be >=1600)

Buttons for "Back" and "Apply/Save" are located at the bottom of the configuration area.

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.

| Field Name | Description |
|---|---|
| Select DSL Latency | Select the level of DSL latency. Options are: <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 | Select the algorithm used to schedule queue behavior. VC scheduling is different than scheduling done for default queues. Options are: |

| Field Name | Description |
|----------------------------------|---|
| | <ul style="list-style-type: none"> • Round Robin (weight=1): 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 . |
| Default Queue Minimum Rate | The default minimum rate at which traffic can pass through the queue. Options are: 1-1255 Kbps. |
| Default Queue Shaping Rate | The shaping rate for the specified queue. Options are: 1-1255 Kbps. |
| Default Queue Shaping Burst Size | 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.

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.
1. In the left navigation bar, click **Advanced Setup > Layer2 Interface > ETH Interface**. The following page appears.

SMART/RG
forward thinking

SR516ac

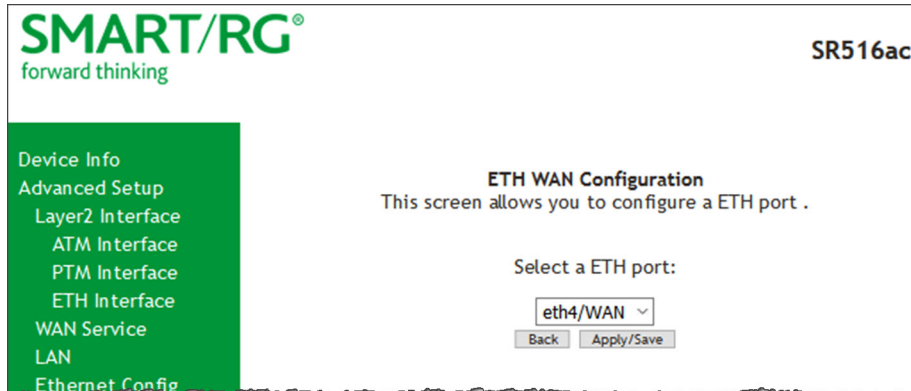
ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 WAN interface.

| Interface/(Name) | Connection Mode | Remove |
|------------------|-----------------|--------------------------|
| eth4/WAN | VlanMuxMode | <input type="checkbox"/> |

Remove

- To remove an entry, click the **Remove** checkbox next to the entry and then click the **Remove** button.
- To add an entry, click **Add**. The following page appears.

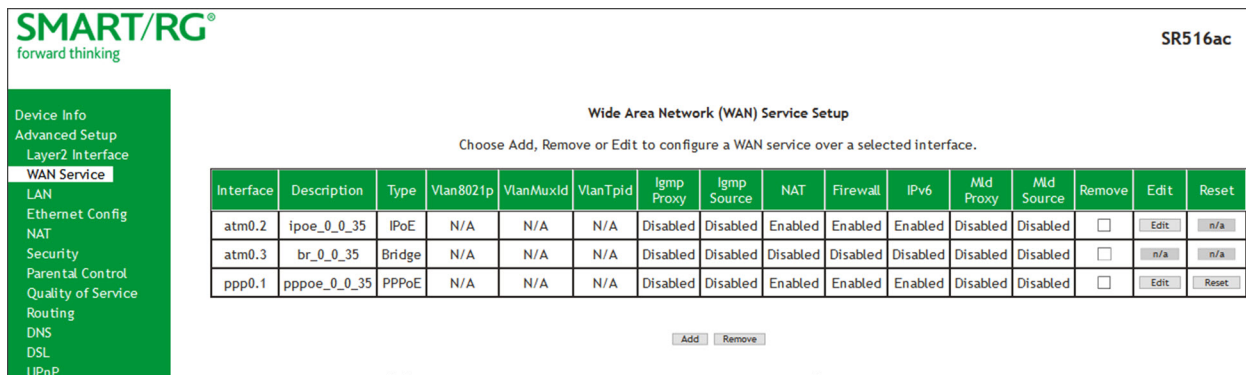


- Select the LAN port you want to use as a WAN port.
- Click **Apply/Save** to commit your changes. The interface is added to the ETH WAN Interface Configuration page.

WAN Service

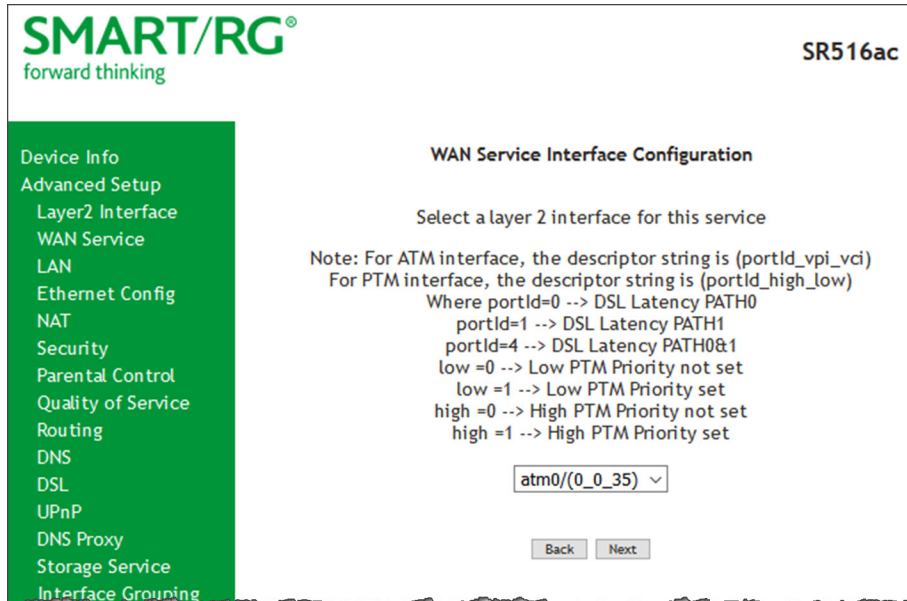
On this page, you can add, remove, or edit a WAN service. You must configure the related interface (ATM, ETH or PTM) first. You can configure services for PPPoE, IPoE, and Bridging. A sample configuration scenario is provided for each variation.

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



- To reset a service, click the **Reset** button at the far right. This takes about 15 seconds to complete.
- To edit an interface:
 - Click the **Edit** button in the **Edit** column.
 - Modify the settings as needed and then click through to click **Apply/Save**.
- To remove an interface, click the **Remove** checkbox next to it and then click the **Remove** button.

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



6. Modify the settings as desired, using the information in the topics listed below:

- ["PPP over Ethernet WAN Service"](#)
- ["IP over Ethernet WAN Service"](#)
- ["Bridging"](#)

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

SR516ac

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

atm0/(0_0_35) v

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

SR516ac

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
Select VLAN TPID: Select a TPID v

Internet Protocol Selection:
IPv4 Only v

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

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

SMART/RG
forward thinking
SR516ac

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

PPP Username and Password

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

Use base MAC address as username

 Authentication Method:

Link Control Protocol

LCP Keepalive Period (s):
 LCP Retry Threshold:

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

Use Static IPv4 Address
 Use Static IPv6 Address
 Enable IPv6 Unnumbered Model
 Launch Dhcp6c for Address Assignment (IANA)
 Launch Dhcp6c for Prefix Delegation (IAPD)
 Retry PPP password on authentication error
 Max PPP authentication retries (1-65536): (use 65536 to retry forever)

Enable PPP Debug Mode
 Bridge PPPoE Frames Between WAN and Local Ports
 Enable Firewall
 Enable SYN Flood rules
Enabling the SYN Flood rules can degrade TCP performance.

Network Address Translation Settings

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

Enable NAT
 Enable Fullcone NAT
 Enable SIP ALG
 Port Control Protocol Mode:

PCP Server:

IGMP Multicast

Enable IGMP Multicast Proxy
 Enable IGMP Multicast Source

MLD Multicast

Enable MLD Multicast Proxy
 Enable MLD Multicast Source

MTU size [1370-1492]:

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

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

| Field Name | Description |
|---|---|
| PPP Username | Enter the username required for authentication to the PPP server. To use the gateway's MAC address as the user name, click the Use base MAC address as user-name checkbox. |
| PPP Password | Enter the password required for authentication to the PPP server. |
| PPPoE Service Name | <i>(Optional)</i> Enter a description for this service. |
| Authentication Method | Select a means for authentication. Options are: <ul style="list-style-type: none"> • 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). |
| Link Control Protocol | This option is enabled by default. To disable keepalive packets, clear the checkbox. Enter values in the following fields: <ul style="list-style-type: none"> • LCP Keepalive Period(s): Enter the interval for sending echos in seconds. The default is 30 seconds. • LCP Retry Threshold: Enter the number of times that echos should be sent before reporting echo failure. The default is 5 times. |
| 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. |
| Advanced DMZ | Non DMZ IP Address: The default is the address of the gateway. Non DMZ Net Mask: The default is 255.255.255.0. |
| Use Static IPv4 Address | Click to use the IPv4 Address associated with this WAN service. The IPv4 Address field appears. Enter the static IPv4 address for this WAN service. |
| Use Static IPv6 Address | Click to use the IPv6 Address associated with this WAN service. The IPv6 Address field appears. Enter the static IPv4 address for this WAN service. |
| 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. |
| Retry PPP password on authentication error | 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). |

| Field Name | Description |
|---|--|
| | To <i>prevent</i> retrying the PPP password after authentication errors, 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 Firewall | This option is enabled by default. To disable the firewall, clear the checkbox. |
| Enable SYN Flood rules | Select to enable rules for preventing SYN flood distributed denial of service attacks. |
| Enable NAT | This option is enabled by default. To disable NAT (Network Address Translation), clear the checkbox. |
| 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 SIP ALG | Click to enable Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications. |
| Port Control Protocol Mode | PCP is a computer networking protocol that allows hosts on IPv4 or IPv6 networks to control how the incoming IPv4 or IPv6 packets are translated and forwarded by an upstream router that performs network address translation (NAT) or packet filtering. Options are Disable , DS-Lite , and NAT444 . The default is Disable . |
| PCP Server | Enter the server name to be used with PCP. |
| 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. |
| MTU size | Enter the maximum transmission unit size. Options are 1370 - 1492. The default is 1492. |
| Use Base MAC Address on this WAN interface | Select this option to use the MAC address for a single WAN interface. |
| MTU [1370 -1492] | Enter the MTU (Maximum Transmission Unit) size. Options are 1370 - 1492 bytes . The default is 1492 bytes . |
| Use Base MAC Address on this WAN interface | Use the SmartRG device's Base (Primary) MAC address. When this field is unchecked, a unique MAC is assigned for each service. |

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

SMART/RG®
forward thinking

SR516ac

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

Routing -- Default Gateway

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

Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

ppp1.4
atm0.2

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

Selected WAN Interface: pppoe_0_0_35/ppp0.1

Back Next

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.

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

SMART/RG
forward thinking

SR516ac

DNS Server Configuration

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

Select DNS Server Interface from available WAN interfaces:

| | | |
|--|---------------------------|---|
| <p>Selected DNS Server Interfaces</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">ppp0.1</div> | <p>-></p> <p><-</p> | <p>Available WAN Interfaces</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">ppp1.4 atm0.2</div> |
|--|---------------------------|---|

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

12. Do any 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

SR516ac

WAN Setup - Summary

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

| | |
|--------------------------------|------------------------|
| PORT / VPI / VCI: | 0 / 0 / 35 |
| Connection Type: | PPPoE |
| Service Name: | pppoe_0_0_35 |
| Service Category: | UBR |
| IP Address: | Automatically Assigned |
| Service State: | Enabled |
| 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: | Disabled |

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

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

SR516ac

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

atm0/(0_0_35) v

Back Next

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


- Select **IP over Ethernet**.
- 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. |
| Internet Protocol Selection | Different scheduling priorities can be applied to statistically multiplexed data flows. Since each data flow has its own queue, an ill-behaved flow (which has sent larger packets or more packets per second than the others) will only punish itself and not other sessions. Options are IPv4 Only , IPv4&IPv6 (Dual Stack), and IPv6 Only . The default is IPv4 Only . |

| Field Name | Description |
|------------|-------------|
|------------|-------------|

Note: When you select **IPV4&IPV6** or **IPV6**, the options presented on later pages change accordingly.

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


SR516ac

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

WAN IP Settings

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

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 77 User ID:

Option 125: Disable Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Advanced DMZ

Non DMZ IP Address:

Non DMZ Net Mask:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.
Notice:
If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.
Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

6. Enter the relevant WAN IP Settings, using the information provided in the table 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 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 . |
| 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. |
| 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. |
| Advanced DMZ | Non DMZ IP Address: The default is the address of the gateway. Non DMZ Net Mask: The default is 255.255.255.0. |

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 <i>disable</i> 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 <i>disable</i> this option, clear the checkbox. |
| Use the following Static IPv6 address | Select this option to enter the v6 Static IP information provided by your ISP. |

| Field Name | Description |
|--------------------------------|--|
| 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. |
| 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. |

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

The screenshot shows the SMART/RG SR516ac web interface. On the left is a green sidebar with navigation options: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Ethernet Config, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, Storage Service, Interface Grouping, IP Tunnel, IPSec, Certificate, Power Management, Multicast, Wireless, Diagnostics, Management, and Logout. The main content area is titled "Network Address Translation Settings". It includes a descriptive paragraph about NAT, several checkboxes for enabling NAT, Fullcone NAT, Firewall, SYN Flood rules, SIP ALG, IGMP Multicast Proxy, IGMP Multicast Source, MLD Multicast Proxy, and MLD Multicast Source. A dropdown menu for "Port Control Protocol Mode" is set to "Disable", and there is a text input field for "PCP Server". A red warning message states "Enabling the SYN Flood rules can degrade TCP performance." At the bottom, there are "Back" and "Next" buttons.

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 <i>disable</i> 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 <i>disable</i> network acceleration and some security settings. |
| Enable Firewall | This option is selected by default. Click to <i>disable</i> functions in the Security sub-menu. |
| Enable SYN Flood rules | Select to enable rules for preventing SYN flood distributed denial of service attacks. |
| Enable SIP ALG | Click to enable Session Initiation Protocol (SIP) pass-through NAT. Used for Voice over IP (VOIP) applications. |
| Port Control Protocol Mode | PCP is a computer networking protocol that allows hosts on IPv4 or IPv6 networks to control how the incoming IPv4 or IPv6 packets are translated and forwarded by an upstream router that performs network address translation (NAT) or packet filtering. Options are Disable , DS-Lite , and NAT444 . The default is Disable . |
| PCP Server | Enter the server name to be used with PCP. |
| 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 | <i>(Available only for IPv6 environments)</i> Click to enable multicast filtering. 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> Select to enable this service to act as a multicast source. |
| Use Base MAC Address on this WAN interface | Select this option to use the MAC address for a single WAN interface. |

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

SMART/RG
forward thinking

SR516ac

Routing -- Default Gateway

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

Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

atm0.2


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

Selected WAN Interface

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.

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


SR516ac

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

DNS Server Configuration

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

Select DNS Server Interface from available WAN interfaces:

| Selected DNS Server Interfaces | | Available WAN Interfaces |
|--------------------------------|--|--------------------------|
| ppp0.1 | <input type="button" value="→"/> <input type="button" value="←"/> | atm0.2 |

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

13. Modify the settings as needed.

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

SMART/RG
forward thinking

SR516ac

WAN Setup - Summary

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

| | |
|--------------------------------|------------------------|
| PORT / VPI / VCI: | 0 / 0 / 35 |
| Connection Type: | IPoE |
| Service Name: | ipoe_0_0_35 |
| Service Category: | UBR |
| IP Address: | Automatically Assigned |
| Service State: | Enabled |
| 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: | Disabled |

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

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 Layer2 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

SR516ac

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

atm0/(0_0_35) ▾

Back Next

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

SMART/RG
forward thinking

SR516ac

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
Select VLAN TPID: Select a TPID ▾

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 | <i>(Optional)</i> 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. |
| Select VLAN TP ID | <i>(Optional)</i> Select the TPID for this VLAN. Options are 0x8100 , 0x88A8 , and 0x9100 . |

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

SMART/RG®
forward thinking

SR516ac

WAN Setup - Summary

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

| | |
|--------------------------------|----------------|
| PORT / VPI / VCI: | 0 / 0 / 35 |
| Connection Type: | Bridge |
| Service Name: | br_0_0_35 |
| Service Category: | UBR |
| IP Address: | Not Applicable |
| Service State: | Enabled |
| 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: | Disabled |

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

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

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

LAN

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.

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

SMART/RG
forward thinking

SR516ac

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName

IP Address:
Subnet Mask:

Enable IGMP Snooping

Standard Mode
 Blocking Mode

Enable IGMP LAN to LAN Multicast: (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

Enable LAN side firewall

Disable DHCP Server
 Enable DHCP Server

Start IP Address:
End IP Address:
Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

| MAC Address | IP Address | Remove |
|-------------|------------|--|
| | | <input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/> |

Automatically create static IP leases for the following OUIs:

| OUI | Remove |
|-----|--|
| | <input type="button" value="Add OUI"/> <input type="button" value="Remove OUI"/> |

Static DNS Servers (optional)

If specified, the DHCP server will pass these addresses to LAN hosts regardless of the DNS Proxy or the WAN Service settings.

Primary:
Secondary:

Configure DHCP Options:

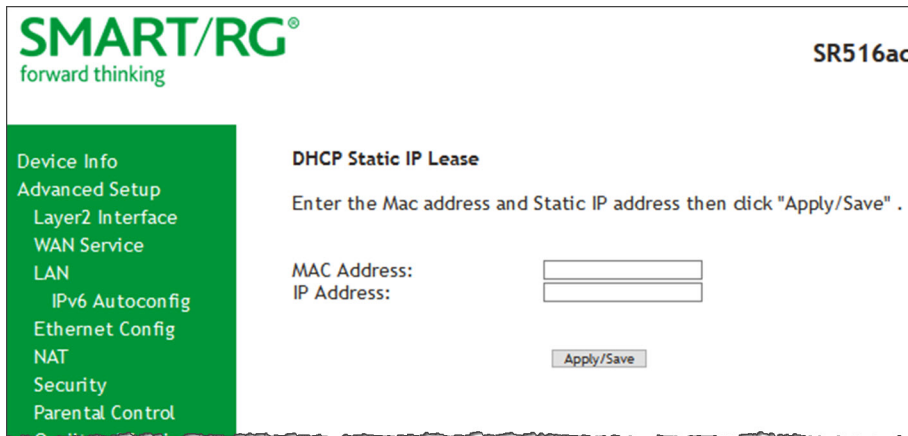
Option 66: (TFTP Server Name)
Option 150: (Comma-separated list of TFTP Server IPv4 Address(es) (maximum 2 entries))
Option 43: (ASCII format) (Hex format)

Configure the second IP Address and Subnet Mask for LAN interface

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 | (Optional) 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. |
| Enable IGMP Snooping | This option is enabled by default. Options are Standard Mode and Blocking Mode . The default is Blocking Mode . To <i>disable</i> this option, clear the check box. |
| Enable IGMP LAN to LAN Multicast | This option is disabled by default. To <i>enable</i> 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 <i>disable</i> the DHCP server, click Disable DHCP Server . Then, if needed, enter different server information for the LAN. |
| Enable DHCP Server Relay | (Appears when the NAT option is not enabled) This option enables a relay agent to forward packets between the DHCP client and server. The DHCP Server IP Address field appears. Enter the IP address for the DHCP server in this field. |

4. 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.
5. To remove entries from the **Static IP Lease List**, click the **Remove** check box next to the entry and then click **Remove Entries**.

6. To add OUIs:
 - a. Click **Add OUI**. The DHCP OUI page appears.

The screenshot shows the SMART/RG web interface for device SR516ac. On the left is a green navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN (highlighted), IPv6 Autoconfig, Ethernet Config, NAT, and Security. The main content area is titled 'Auto add static IP lease' and contains the text 'Enter the OUI then click "Apply/Save".' Below this is a text input field labeled 'OUI:' with a placeholder '(format as xx:xx:xx)' and an 'Apply/Save' button.

- b. Enter the OUI for the DHCP and click **Apply/Save**.
7. To remove entries from the **OUI** list, click the **Remove** check box next to the entry and then click **Remove OUI**.
8. (*Optional*) To define static DNS servers, enter IP addresses in the **Primary** and **Secondary** DNS server fields.
9. To define a second IP address and 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. To configure DHCP options, do any of the following:
 - **Option 66**: Enter the TFTP server name.
 - **Option 150**: Enter 1 or 2 TFTP server addresses, separated by commas.
 - **Option 43**: Enter the Cisco Aironet Wireless Controller address to your access point and then select **ASCII** or **Hex** format.
11. 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
forward thinking

SR516ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
IPv6 Autoconfig
Ethernet Config
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate
Power Management
Multicast
Wireless
Diagnostics
Management
Logout

IPv6 LAN Auto Configuration
Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration
Interface Address (prefix length is required):

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless
 Stateful
Start interface ID:
End interface ID:
Leased Time (hour):

Enable RADVD
 Enable ULA Prefix Advertisement
 Randomly Generate
 Statically Configure
Prefix:
Preferred Life Time (hour):
Valid Life Time (hour):

Enable MLD Snooping
 Standard Mode
 Blocking Mode

Enable MLD LAN to LAN Multicast: (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

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

| Field Name | Description |
|--------------------------------------|--|
| Interface Address | (Optional) Enter a static IP address for your LAN. The prefix length is required. |
| IPv6 LAN Applications section | |
| Enable DHCPv6 Server | This option is selected by default. To <i>disable</i> the DHCP v6 feature on the LAN, click this checkbox to clear it. Options are: <ul style="list-style-type: none"> • Stateless: (Available only when Enable DHCPv6 Server is selected) This option is selected by default. Click to stop inheriting IPV6 address assignments from the WAN IPV6 interface. • Stateful: (Available only when Enable DHCPv6 Server is selected) Identifies the DHCPv6 server given by the LAN IPV6 network as configured with additional options. |

| Field Name | Description |
|---------------------------------|---|
| | <p>Note: Zero compression is not supported. Make sure to enter zeros between the colons; that is, do not use shorthand notation (enter "0:0:0:2", not ":::2").</p> <p>Enter values in the following fields:</p> <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): Enter the length of time before a new IPv6 lease is requested by the LAN client. |
| Enable RADVD | 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 <i>disable</i> RADVD. |
| 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 become available. 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). 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). |
| 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 <i>disable</i> 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 | (<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 . |

Ethernet Config

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

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

SMART/RG
forward thinking

SR516ac

Ethernet Port Configuration

| Port | Configure | Current Bit Rate | Duplex Mode | Status |
|-----------|-----------|------------------|-------------|--------|
| eth0/LAN1 | Auto | Auto | Auto | Down |
| eth1/LAN2 | Auto | 1000 | Full | Up |
| eth2/LAN3 | Auto | Auto | Auto | Down |
| eth3/LAN4 | Auto | Auto | Auto | Down |
| eth4/WAN | Auto | 1000 | Full | Up |

** Always configure 1000BaseT connections with Auto.*

Save/Apply

2. To set a specific speed, select it in the **Configure** 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.

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**. The following page appears.


SR516ac

- Device Info
- Advanced Setup
- Layer2 Interface
- WAN Service
- LAN
- Ethernet Config
- NAT
- Virtual Servers
- Port Triggering
- DMZ Host
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnP
- DNS Proxy
- Storage Service
- Interface Grouping

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 96 entries can be configured.

Add
Remove

| Server Name | External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End | Server IP Address | WAN Interface | Remove |
|---------------|---------------------|-------------------|----------|---------------------|-------------------|-------------------|---------------|--------------------------|
| Active Worlds | 3000 | 3000 | TCP | 3000 | 3000 | 192.168.1.33 | atm0.2 | <input type="checkbox"/> |
| Active Worlds | 5670 | 5670 | TCP | 5670 | 5670 | 192.168.1.33 | atm0.2 | <input type="checkbox"/> |
| Active Worlds | 7777 | 7777 | TCP | 7777 | 7777 | 192.168.1.33 | atm0.2 | <input type="checkbox"/> |
| Active Worlds | 7000 | 7000 | TCP | 7000 | 7000 | 192.168.1.33 | atm0.2 | <input type="checkbox"/> |

2. To add a virtual server:
 - a. Click **Add**. The following page appears.

- 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. |
| Service Name | Select or enter the service for which you want to forward IP packets. Options are: <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. |

| Field | Description |
|--|---|
| Server IP Address | Enter the final octet of the IP address for this virtual server. |
| 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 | (Optional) 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. Click **Apply/Save** to save the settings. The server or servers for the selected service appear on the NAT - Virtual Servers Setup page.
4. To remove a server from the list, click the **Remove** check box next to the entry, click the **Remove** button, and 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 SR516ac

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 96 entries can be configured.

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

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

- Modify the fields as needed, using the information in the following table.
- To remove a trigger, click the **Remove** check box next to it and then click the **Remove** button. The list is refreshed.
- Click **Apply /Save** to implement the settings.

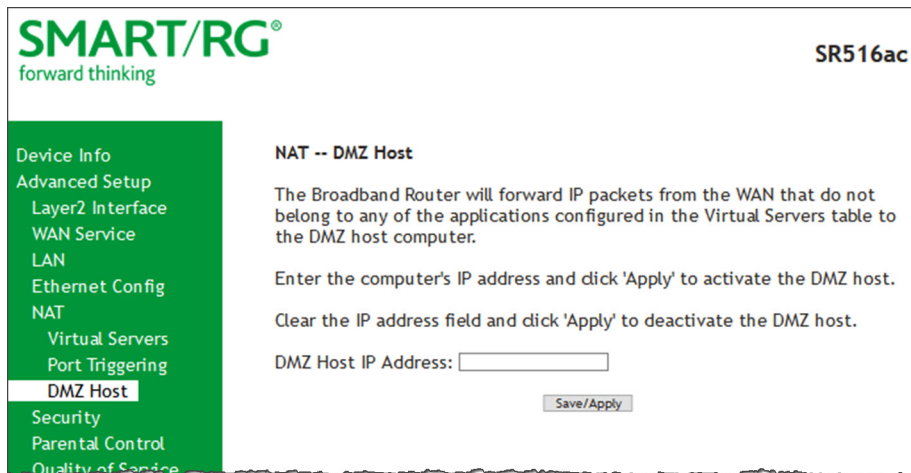
| Field Name | Description |
|--|---|
| Use Interface | Select the interface for which the port triggering rule will apply. |
| Application Name | Select or enter the application that requires a port trigger. Options are: <ul style="list-style-type: none"> Select an Application: Select an available application. 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. You must enter the ports and select a protocol in the table at the bottom of the page. |
| Trigger Port Start Trigger Port End | Enter the starting and ending numbers of the range of available outgoing trigger ports. Options are 1 - 65535. 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. The default is TCP. |

| Field Name | Description |
|----------------------------------|--|
| 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.

Security

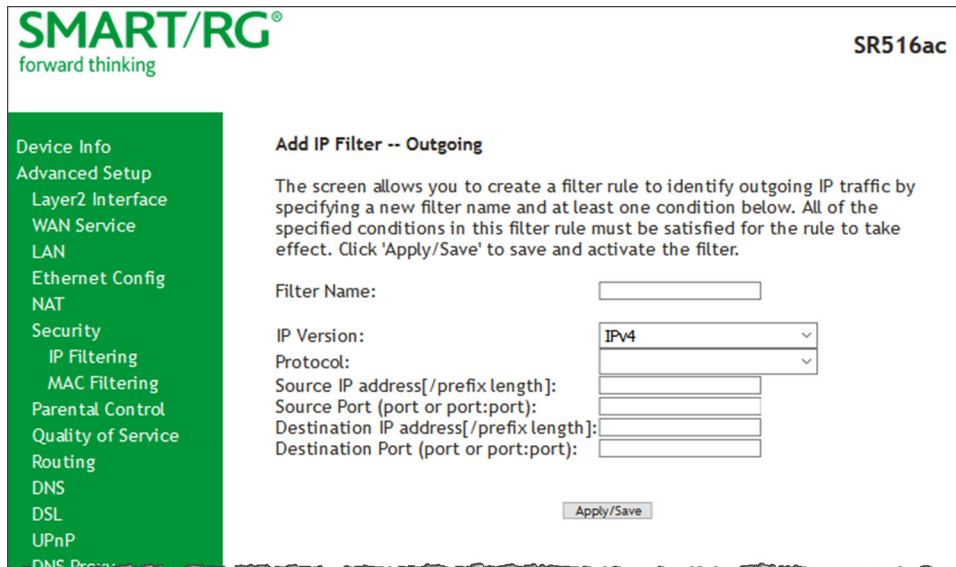
In this section, you can configure the incoming and outgoing IP filtering and MAC filtering.

IP Filtering - Outgoing

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

You can define up to 32 outgoing IP filters.

1. In the left navigation bar, click **Advanced Setup** > **Security** and then click **Add**. The following page appears. 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). |
| Destination IP address [/prefix length] | 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 (pre- |

| Field Name | Description |
|--------------------------------------|---|
| | ceded 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.

SMART/RG®
forward thinking

SR516ac

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

Default behavior for Incoming filter rules is to **ACCEPT** packets meeting the specified conditions. However, the DROP checkbox will create a filter that will **DROP** packets. Dropping packets is useful for such purposes as restricting access to Virtual Servers, as the default condition for Virtual Servers will allow access from any source.

Incoming filters will *not* restrict access to the Service Ports of the Broadband Router itself (HTTP, FTP, Telnet, etc). Use the 'Management Access List' at **Management-> Access Control-> Access List** instead.

Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

DROP:

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All ipoe_0_0_35/atm0.2 pppoe_0_0_35/ppp0.1 br0/br0

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. |
| 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 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). |
| DROP | Select this option to drop packets that meet this filter's requirements. The packets are deleted. |
| WAN Interfaces | Click to apply this rule to all WAN interfaces or only certain types. Options are 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.

SMART/RG
forward thinking

SR516ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Ethernet Config
NAT
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate

MAC Filtering Setup

MAC Filtering is only effective on WANs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

| Interface | Policy | Change |
|-----------|----------------|--------------------------|
| atm0.3 | FORWARD | <input type="checkbox"/> |

Change Policy

Choose Add or Remove to configure MAC filtering rules.

| Interface | Protocol | Destination MAC | Source MAC | Frame Direction | Remove |
|--|----------|-----------------|------------|-----------------|--------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> | | | | | |

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.

| 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 SR516ac

Access Time Restriction

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

User Name

Browser's MAC Address

Other MAC Address

(xx:xx:xx:xx:xx:xx)

| 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 the user name for which this rule applies.
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 **Exclude**.
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. Click **Apply/Save** to save your changes. You are returned to the Parental Control > URL Filter page.

Quality of Service

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

SMART/RG
forward thinking

SR516ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Ethernet Config
NAT
Security
Parental Control
Quality of Service
QoS Config
QoS Queue Config
QoS Classification
QoS Port Shaping
Routing
DNS
DSL
UPnP
DNS Proxy
Storage Service
Interface Grouping
IP Tunnel
IPSec

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Usage Notes:
If the Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

The default DSCP mark is used to mark all egress packets that do not match any classification rules.

QoS and a non-default queue are highly recommended for PPP WAN services. Each time a PPP WAN service starts or resets, if a non-default queue does not exist, one will be created and QoS automatically enabled.

Enable QoS


Select Default DSCP Mark

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 Config**. The following page appears.


SR516ac

Device Info

Advanced Setup

Layer2 Interface

WAN Service

LAN

Ethernet Config

NAT

Security

Parental Control

Quality of Service

QoS Config

QoS Queue Config

Queue Configuration

Wan Queue

QoS Classification

QoS Port Shaping

Routing

DNS

DSL

UPnP

DNS Proxy

Storage Service

Interface Grouping

IP Tunnel

IPSec

Certificate

Power Management

Multicast

QoS -- Queue Config Setup

In ATM mode, the maximum queues that can be configured is 16.
In PTM mode, the maximum queues that can be configured is 8.
For each Ethernet interface, the maximum queues that can be configured is 4; for a WAN-eth, 8.

Usage Notes:
TCP ACK packets unconditionally egress via Qid 2 of their WAN interface, if that Qid exists.

Queues created for VoIP, or similar low-latency media streaming purposes, should have a higher priority (lower numerical precedence) than that of Qid 2. Conversely, queues created for bulk-data upload purposes, if such are required, should have a lower priority (higher numerical precedence) than that of Qid 2.

Network management packets, such as PPP connection keep-alive messages, unconditionally egress via the highest priority queue (lowest numerical precedence) of their WAN interface.

In most cases, general purpose Cloud Services should *not* require dedicated queues. If you deem a queue for a Cloud Service is necessary, it should probably not have a higher priority than the queue used for your interactive web browsing, which is typically the Default Queue. Finally, be aware these are *egress* queues. Generally speaking, they will not speed-up *incoming* traffic, and will not optimize *inbound* media streaming.

| Name | Key | Interface | Qid | Prec/Alg/Wght | DSL Latency | PTM Priority | Shaping Rate(bps) | Min Bit Rate(bps) | Burst Size(bytes) | Enable | Remove |
|---------------|-----|-----------|-----|---------------|-------------|--------------|-------------------|-------------------|-------------------|--------|--------|
| Default Queue | 65 | ptm0 | 1 | 8/WRR/1 | Path0 | Low | | | | | |
| Default Queue | 66 | atm0 | 1 | 8/WRR/1 | Path0 | | | | | | |

Add
Enable
Remove

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



- 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 Config 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. |
| Precedence | <i>(Appears when atm, eth or ptm interfaces are selected in the Interface field)</i> Select the priority value to be associated with the defined QoS queue. Options vary by interface and can include 1(SP), 1(WRR WFQ), 2(SP), 3(WRR), 4(SP WRR WFQ), and so on. 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. |

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 . |

| Field Name | Description |
|---------------------|---|
| Queue Weight | Enter the weighting value to associate with this queue. Options are 1 - 63. The default is 1. 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. |
| Scheduler Algorithm | Select an algorithm for data priority in queues. Options are: <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.

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

SMART/RG®
forward thinking

SR516ac

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Ethernet Config
NAT
Security
Parental Control
Quality of Service
QoS Config
QoS Queue Config
Queue Configuration
Wlan Queue
QoS Classification
QoS Port Shaping
Routing
DNS
DSL
UPnP

QoS -- Wlan Queue Setup

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

| Name | Key | Interface | Qid | Prec/Alg/Wght | Enable |
|--------------------|-----|-----------|-----|---------------|---------|
| WMM Voice Priority | 1 | wt0 | 8 | 1/SP | Enabled |
| WMM Voice Priority | 2 | wt0 | 7 | 2/SP | Enabled |
| WMM Video Priority | 3 | wt0 | 6 | 3/SP | Enabled |
| WMM Video Priority | 4 | wt0 | 5 | 4/SP | Enabled |
| WMM Best Effort | 5 | wt0 | 4 | 5/SP | Enabled |
| WMM Background | 6 | wt0 | 3 | 6/SP | Enabled |
| WMM Background | 7 | wt0 | 2 | 7/SP | Enabled |
| WMM Best Effort | 8 | wt0 | 1 | 8/SP | 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.

SMART/RG®
forward thinking

SR516ac

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Ingress Interface: ▼

Ether Type: ▼

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Egress Interface (Required): ▼

Specify Egress Queue (Required): ▼

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

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

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. | |
| Ingress Interface | Select an interface for incoming traffic. Options are LAN , WAN , Local , 2.4GHz , 5GHz , and any interface defined for your network. The default is LAN . |
| 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 | <i>(Available for LAN, ATM, ETH, PPP-Routed and wireless interfaces only)</i> Enter the source MAC address and source MAC mask for this classification. |
| Destination MAC Address / Mask | <i>(Available for LAN, ETH and wireless interfaces only)</i> Enter the destination MAC address and destination MAC mask for this classification. |
| Source IP Address [/ Mask] or Vendor Class ID or User Class ID | <i>(Available for WAN, ATM and PPP-Routed interfaces only)</i> Select the source for this classification. Options are: <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] | <i>(Available for WAN and ATM interfaces only)</i> Enter the destination IP address and source IP mask for this classification. |
| Differentiated Service Code Point (DSCP) Check | <i>(Available for WAN, Local, ATM interfaces only)</i> Select the DSCP code that should be associated with this rule.imum and maximum number of digits required for IP addresses. |
| Protocol | <i>(Available for WAN, Local, and ATM interfaces only)</i> Select the protocol specified for this classification. Options are TCP , UDP , ICMP , and IGMP . |
| UDP/TCP Source Port | <i>(Appears when TCP or UDP is selected in the Protocol field)</i> Enter the source port to be used for this classification. You can enter a range (port:port) or a single port. |
| UDP/TCP Destination Port | <i>(Appears when TCP or UDP is selected in the Protocol field)</i> Enter the 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 Differentiated Service Code Point (CP) | Select the desired DSCP code. |

| Field Name | Description |
|----------------------|---|
| Mark 802.1p priority | (Available for LAN, bridged and wireless interfaces only) This value is inserted into the Ethernet frame and used to differentiate traffic. Lower values assign higher priorities. Options are 0 - 7. |
| Set Rate Limit | Enter the data traffic rate limit (in Kbits/second) for this classification. |

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

SR516ac

QoS -- Port Shaping Setup

QoS Port Shaping supports traffic rate limiting on the Ethernet interfaces.
If "Egress Shaping Rate" is set to "-1", shaping will be disabled and "Egress Burst Size" will be ignored.
If "Ingress Policing Rate" is set to "-1", policing will be disabled.

| Interface | Egress Shaping Rate (Kbps) | Egress Burst Size (bytes) | Ingress Policing Rate (Kbps) |
|-----------|----------------------------|---------------------------|------------------------------|
| eth4/WAN | -1 | 0 | -1 |
| eth0/LAN1 | -1 | 0 | -1 |
| eth1/LAN2 | -1 | 0 | -1 |
| eth2/LAN3 | -1 | 0 | -1 |
| eth3/LAN4 | -1 | 0 | -1 |

Apply/Save

2. (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.
3. 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.

SMART/RG
forward thinking

SR516ac

Routing -- Default Gateway

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

Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

atm0.2

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

Selected WAN Interface

Apply/Save

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.

SMART/RG
forward thinking

SR516ac

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

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 | <i>(Not available for PTM interfaces)</i> Enter the next-hop IP address. If needed, include the /prefix length. |
| Metric | <i>(Optional)</i> 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.

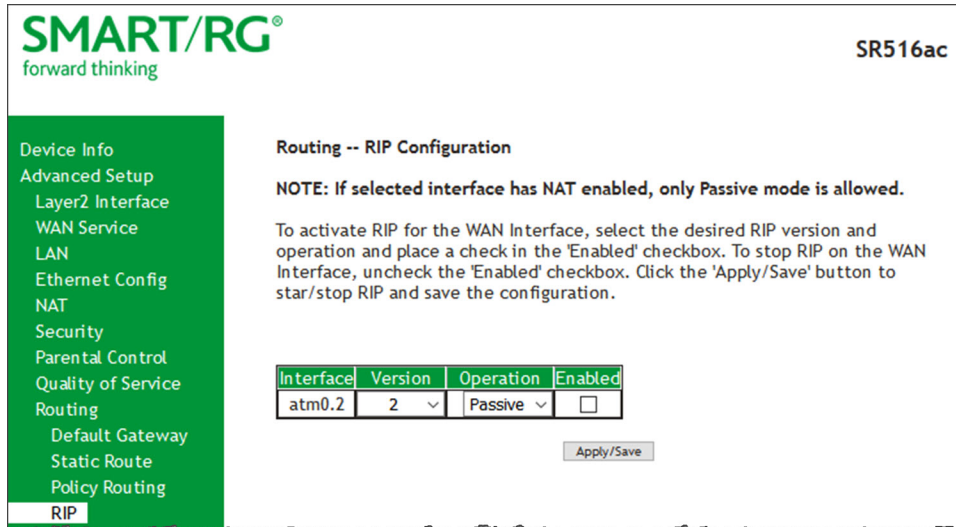
The fields on this page are defined below.

| 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 . |
| Default Gateway IP | 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.



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 . The default is 2 . |
| 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**. The following page appears.

SMART/RG® forward thinking SR516ac

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

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

Select DNS Server Interface from available WAN interfaces:

| | | |
|--------------------------------|--|--------------------------|
| Selected DNS Server Interfaces | <input type="button" value="→"/> <input type="button" value="←"/> | Available WAN Interfaces |
| ppp0.1 | | atm0.2 |

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

2. 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 for your gateway, 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.

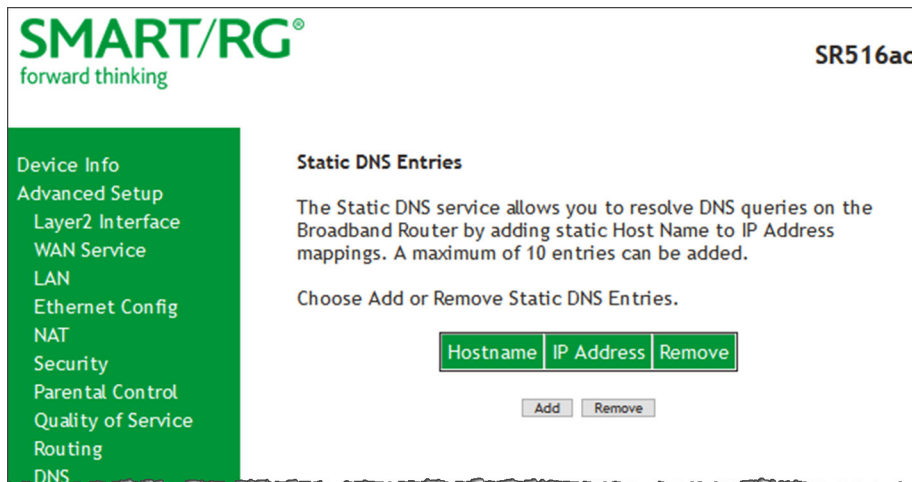
2. Modify the fields as needed, using the information in the table below.
3. Click [Apply/Save](#) to commit your changes.

| 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. |

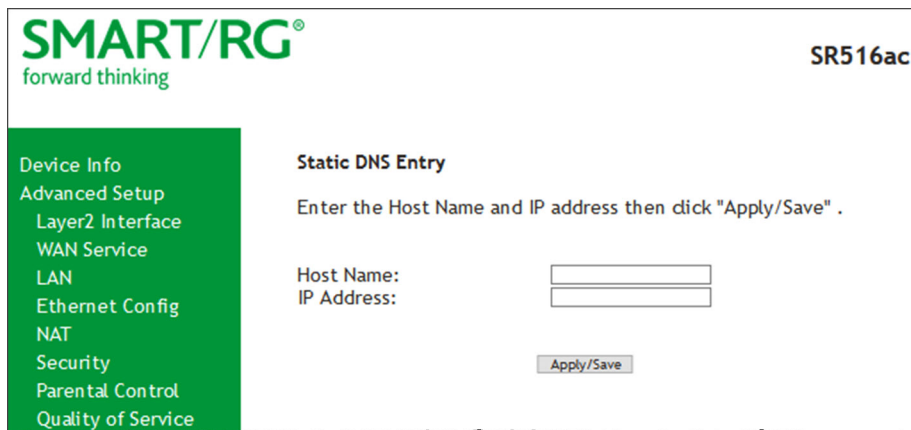
Static DNS

On this page, you can configure static DNS domains.

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



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



3. Enter a host 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

SR516ac

Device Info

Advanced Setup

Layer2 Interface

WAN Service

LAN

Ethernet Config

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DSL

UPnP

DNS Proxy

Storage Service

Interface Grouping

IP Tunnel

IPSec

Certificate

Power Management

Multicast

Wireless

Diagnostics

Management

Logout

DSL Settings

Select the modulation below. Select the profile below.

| | |
|--|---|
| <input checked="" type="checkbox"/> G.Dmt Enabled | <input checked="" type="checkbox"/> 8a Enabled |
| <input checked="" type="checkbox"/> G.lite Enabled | <input checked="" type="checkbox"/> 8b Enabled |
| <input checked="" type="checkbox"/> T1.413 Enabled | <input checked="" type="checkbox"/> 8c Enabled |
| <input checked="" type="checkbox"/> ADSL2 Enabled | <input checked="" type="checkbox"/> 8d Enabled |
| <input checked="" type="checkbox"/> AnnexL Enabled | <input checked="" type="checkbox"/> 12a Enabled |
| <input checked="" type="checkbox"/> ADSL2+ Enabled | <input checked="" type="checkbox"/> 12b Enabled |
| <input type="checkbox"/> AnnexM Enabled | <input checked="" type="checkbox"/> 17a Enabled |
| <input checked="" type="checkbox"/> VDSL2 Enabled | |

US0

Enabled

Select the phone line pair below.

Inner pair

Outer pair

Capability

Bitswap Enable

SRA Enable

PhyR Enable

ADSL PTM Mode Enable

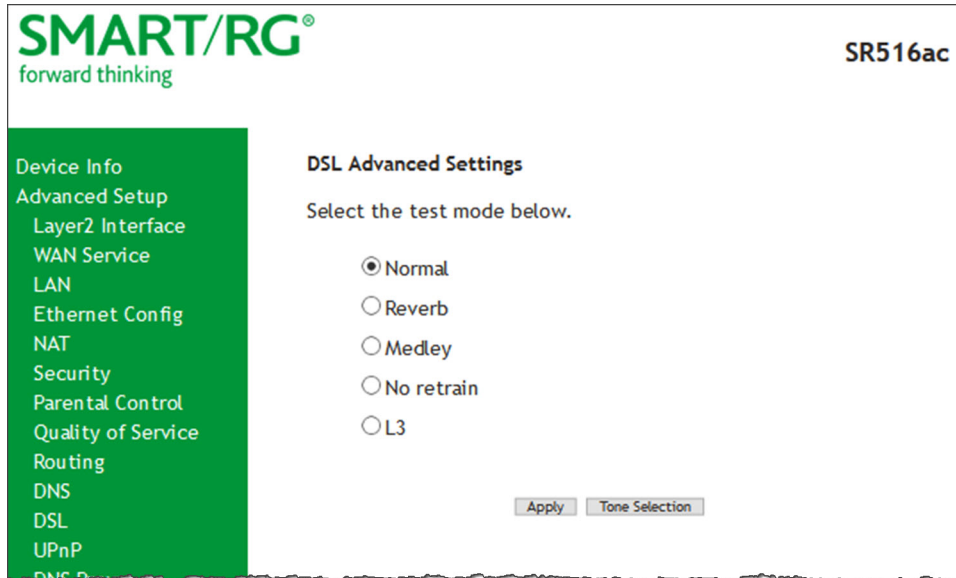
Stinger® Mode Enable

Inventory Management

Use board serial for EOC Serial Number

2. Modify the settings as needed.

- (Optional) To modify additional parameters, click **Advanced Settings**. The following page appears.

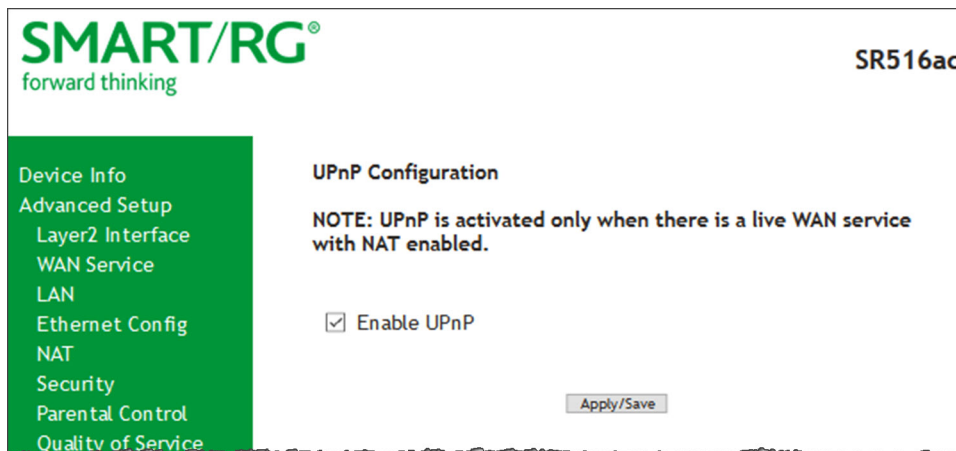


- Select the test mode that you want to run.
- To view the tone selection table, click **Tone Selection**. Changing these settings arbitrarily is *not recommended*. Close the window to return to the DSL Advanced Settings page.
- Click **Apply** and then click **DSL** in the left menu to return to the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

UPnP

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

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

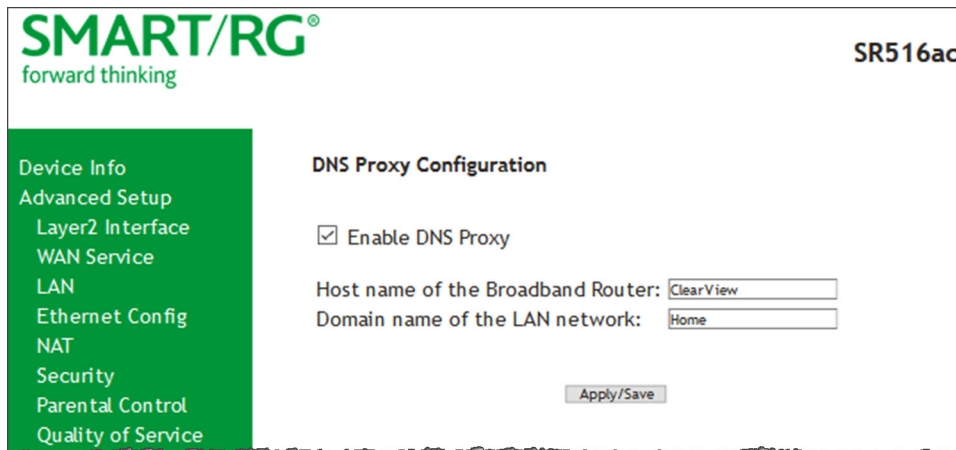


2. To *disable* UPnP, click the **Enable UPnP** check box to clear it.
3. Click **Apply/Save** to save and apply the settings.

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.



The screenshot shows the SMART/RG SR516ac web interface. On the left is a green navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Ethernet Config, NAT, Security, Parental Control, and Quality of Service. The 'Advanced Setup' menu item is highlighted, and 'DNS Proxy' is selected. The main content area is titled 'DNS Proxy Configuration'. It features a checked checkbox for 'Enable DNS Proxy'. Below this are two text input fields: 'Host name of the Broadband Router' with the value 'ClearView' and 'Domain name of the LAN network' with the value 'Home'. At the bottom of the configuration area is an 'Apply/Save' button.

2. To *disable* the DNS Proxy, click the **Enable DNS Proxy** checkbox 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.

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.

The screenshot shows the SMART/RG SR516ac web interface. The top left features the SMART/RG logo with the tagline "forward thinking". The top right displays the device model "SR516ac". On the left, a green navigation menu lists: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Ethernet Config, NAT, and Security. The main content area is titled "Storage Service" and includes the text: "The Storage service allows you to use Storage devices with modem to be more easily accessed". Below this text is a table with four columns: "Volumename", "FileSystem", "Total Space", and "Used Space".

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.

The screenshot shows the SMART/RG SR516ac web interface for "Storage UserAccount Configuration". The top left features the SMART/RG logo with the tagline "forward thinking". The top right displays the device model "SR516ac". On the left, a green navigation menu lists: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Ethernet Config, NAT, and Security. The main content area is titled "Storage UserAccount Configuration" and includes the text: "Choose Add, or Remove to configure User Accounts." Below this text is a table with three columns: "UserName", "HomeDir", and "Remove". At the bottom of the table are two buttons: "Add" and "Remove".

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


The screenshot shows the SMART/RG web interface for device SR516ac. The left sidebar contains a menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, Ethernet Config, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, and DNS Proxy. The main content area is titled 'Storage User Account Setup' and contains the following text: 'In the boxes below, enter the user name, password and volume name on which the home directory is to be created.' Below this text are four input fields: 'Username:', 'Password:', 'Confirm Password:', and 'volumeName:'. An 'Apply/Save' button is located at the bottom right of the form area.

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

Interface Grouping

On this page, you can 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.



SR516ac

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

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 | | ppp0.1 | LAN1 | |
| | | atm0.2 | LAN2 | |
| | | atm0.3 | LAN3 | |
| | | | LAN4 | |
| | | | 5 GHz - wlan0 | |
| | | | 5 GHz - Guest wl0.1 | |
| | | | 5 GHz - Guest wl0.2 | |
| | | | 5 GHz - Guest wl0.3 | |
| | | | 2.4 GHz - wlan1 | |
| | | | 2.4 GHz - Guest wl1.1 | |
| | | | 2.4 GHz - Guest wl1.2 | |
| | | | 2.4 GHz - Guest wl1.3 | |

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

SMART/RG®
forward thinking

SR516ac

Interface grouping Configuration

To create a new interface group:

- Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
- 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.
- 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**
- If this interface is to share the WAN interface, click the "shared WAN interface" box, otherwise the WAN interface you select will be removed from any other interface groups.
- 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:

Shared WAN Interface:

Grouped WAN Interfaces

Available WAN Interfaces

ipoe_0_0_35/atm0.2
br_0_0_35/atm0.3
pppoe_0_0_35/ppp0.1
No Interface/None

Grouped LAN Interfaces

Available LAN Interfaces

LAN1
LAN2
LAN3
LAN4
5 GHz - wlan0
5 GHz - Guest|wl0.1
5 GHz - Guest|wl0.2
5 GHz - Guest|wl0.3
2.4 GHz - wlan1
2.4 GHz - Guest|wl1.1

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

- Follow the on-screen instructions and then click **Apply/Save**.
- 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.

SMART/RG
forward thinking

SR516ac

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

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.

The screenshot shows the SMART/RG web interface for device SR516ac. The left navigation bar is highlighted in green, with 'Advanced Setup' selected. The main content area is titled 'IP Tunneling -- 4in6 Tunnel Configuration'. Below the title, it states 'Currently, only DS-Lite configuration is supported.' The configuration fields are as follows:

- Tunnel Name: [Text input field]
- Mechanism: [Dropdown menu showing 'DS-Lite']
- Associated WAN Interface: [Dropdown menu]
- Associated LAN Interface: [Dropdown menu showing 'LAN/br0']
- Radio buttons: Manual, Automatic
- AFTR: [Text input field]


An 'Apply/Save' button is located at the bottom right of the configuration area.

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.



forward thinking

SR516ac

- Device Info
- Advanced Setup
- Layer2 Interface
- WAN Service
- LAN
- Ethernet Config
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnP
- DNS Proxy
- Storage Service
- Interface Grouping

IPSec Tunnel Mode Connections

Manage the IPSec tunnel connections from this page.

Usage Notes:
IPSec accepts connections from Remote Gateways according to the order in which they are defined. If key exchange fails, IPSec aborts the connection attempt. IPSec will not retry the connection on a different tunnel definition. As such, Anonymous tunnels should be defined last, as they necessarily match to *any* incoming Remote Gateway.

If you wish to Add a new tunnel that is similar to, or based upon, an existing tunnel, you can pre-load all the parameters by first clicking 'Edit' on the existing tunnel, then using your browser's back button to return to this page, followed by clicking the 'Add' button.

| Connection Name | Remote Gateway | Local Addresses | Remote Addresses | Enable | Remove | Edit |
|--|----------------|-----------------|------------------|--------|--------|------|
| Add Enable Remove | | | | | | |

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

3. 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. |
| NAT Transversal | Click this checkbox to enable the Network Address Translation protocol. |
| 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. <ul style="list-style-type: none"> AH: Use this mode to encapsulate a packet with AH and IP headers. For authentication, the entire packet is signed. ESP: Use this mode to encapsulate a packet with ESP and IP headers. An ESP trailer is added to the packet for authentication and integrity. This is the default. |

| Field Name | Description |
|-------------------------|---|
| WAN Interface | Select the interface for the local gateway. |
| Remote Security Gateway | Enter the WAN IP for the tunnel. To allow anonymous connections, click the Anonymous checkbox. |
| LAN-side VPN | Select whether to allow access to the entire LAN or a single host for local IP addresses. <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. • Single Address: Allows access to a single host. Enter the IP address for the host. |
| IP Address | Enter the IP address for local access. |
| Mask or Prefix Length | Enter the subnet mask or prefix length for the IP address entered for local access, e.g., 255.255.255.0. |
| Local ID Type | Select the type of ID for the local VPN. Options are Default , Domain , and E-Mail . The default is Default . When you select Domain or E-Mail , the ID Content field becomes available. Enter the ID. |
| Remote-side VPN | Select whether to allow access to the entire LAN or a single host for remote IP addresses. <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. • Single Address: Allows access to a single host. Enter the IP address for the host. |
| IP Address | Enter the IP address for remote access. |
| Mask or Prefix Length | Enter the subnet mask or prefix length for the IP address entered for remote access, e.g., 255.255.255.0. |
| Remote ID Type | Select the type of ID for the remote VPN. Options are Default , Domain , and E-Mail . The default is Default . When you select Domain or E-Mail , the ID Content field becomes available. Enter the ID. |
| Key Exchange Method | Select the key-exchange method to be used for IPsec. <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 | Select the method by which the remote end will authenticate. <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. If you have not yet uploaded a certificate file, follow the instructions in the "Certificate" section of this manual. |
| Perfect Forward Secrecy | 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. <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:
 - a. Click **Show Advanced Settings**. Additional fields appear.

The screenshot shows the 'Advanced IKE Settings' configuration interface. It features a 'Hide Advanced Settings' button at the top right. The settings are organized into two sections: 'Phase 1' and 'Phase 2'. Each section includes dropdown menus for 'Mode', 'Encryption Algorithm', 'Integrity Algorithm', and 'Select Diffie-Hellman Group for Key Exchange', and a text input field for 'Key Life Time' with 'Seconds' as a unit. The 'Apply/Save' button is located at the bottom center of the form.

- b. Fill in the fields, using the information provided in the table below. 16

| Field Name | Description |
|--|--|
| Mode | (Appears in the <i>Phase 1</i> section only) Select whether to protect information about your network. Options are: <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. |
| 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). |

5. 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

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

SMART/RG
forward thinking

SR516ac

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

| Name | In Use | Subject | Type | Action |
|------|--------|---------|------|--------|
|------|--------|---------|------|--------|

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

SMART/RG
forward thinking

SR516ac

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

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.

| Field Name | Description |
|---------------------|--|
| Certificate Name | Enter a certificate name that describes 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 of 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.

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 SR516ac

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:
 Query Response Interval:
 Last Member Query Interval:
 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:

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.

| Field Name | Description |
|---|---|
| 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. |
| Multicast Strict Grouping Enforcement | Select whether to enforce strict key management rules. Options are Enable and Disable . The default is Disable . |
| IGMP Configuration and MLD Configuration sections | |
| 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. |
| 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. The default is 25 for IGMP and 10 for MLD. |
| 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 few 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 5 GHz band.

SMART/RG
forward thinking

SR516ac

Wireless -- Basic

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

- Enable WiFi Button
- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Country RegRev:

Max Clients:

Wireless - Guest/Virtual Access Points:

| Enabled | SSID | Hidden | Isolate Clients | Disable WMM Advertise | Enable WMM | Max Clients | BSSID |
|--------------------------|--|--------------------------|--------------------------|-------------------------------------|-------------------------------------|---------------------------------|-------|
| <input type="checkbox"/> | <input type="text" value="Guest-5G"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="32"/> | N/A |
| <input type="checkbox"/> | <input type="text" value="Guest1-5G"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="32"/> | N/A |
| <input type="checkbox"/> | <input type="text" value="Guest2-5G"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="32"/> | N/A |

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.

| Field Name | Description |
|--------------------|--|
| Enable WiFi Button | This option is selected by default. To <i>disable</i> the gateway's 2.4GHz button, clear the checkbox. |
| 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. |

| Field Name | Description |
|--------------------------------------|---|
| 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. If your gateway is connected to an ACS, it is recommended that SSID names be 1 - 32 characters long. Special characters are accepted. |
| 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 871 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. The default is 20 . Note: Before you can change this setting, you must change the Global Max Clients setting. |

Wireless - Guest/Virtual Access Points section

| | |
|-----------------------|---|
| Enabled | Click to <i>enable</i> a virtual wireless access point for guest access. |
| SSID | Enter the wireless SSID for guests to use. |
| Hidden | Click to <i>prevent</i> the SSID from being broadcast publicly. |
| Isolate Clients | Click to <i>prevent</i> client PCs from communicating with one another. |
| Disable WMM Advertise | Click to <i>stop</i> the wireless from advertising Wireless Multimedia (WMM) functionality. |
| Enable WMF | Click to <i>disable</i> Wireless Multicast Forwarding (WMF). |
| 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.

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 <i>enabled</i> by default. To <i>disable</i> WiFi Protected Setup, select Disabled . |
| Add Client | (Available for WPA-PSK , WPA2-PSK and Open Network Authentication methods) Select the method for generating the WPS PIN. Options are: <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. |

| Field Name | Description |
|----------------------------|--|
| | <ul style="list-style-type: none"> • 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 | Select how security is assigned to clients. <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 5 GHz 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 and **WEP Encryption** is enabled.

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:

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 and then click [Apply/Save](#).

| Field Name | Description |
|---------------------|--|
| 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 defined keys is presently in effect. |
| Network Key 1-4 | 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 defined keys is presently in effect. The default is 2 . |
| Network Key 1-4 | Enter up to three encryption keys using the on-screen instructions to achieve the desired security strength. Network Key 1 is 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 | <i>(Optional)</i> Enter the encryption key needed to authenticate to the specified RADIUS Server. |
| WPA Encryption | Select the encryption standard. This field displays the option most compatible with the selected network authentication method. Options are: <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:

Network Authentication:

Protected Management Frames:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

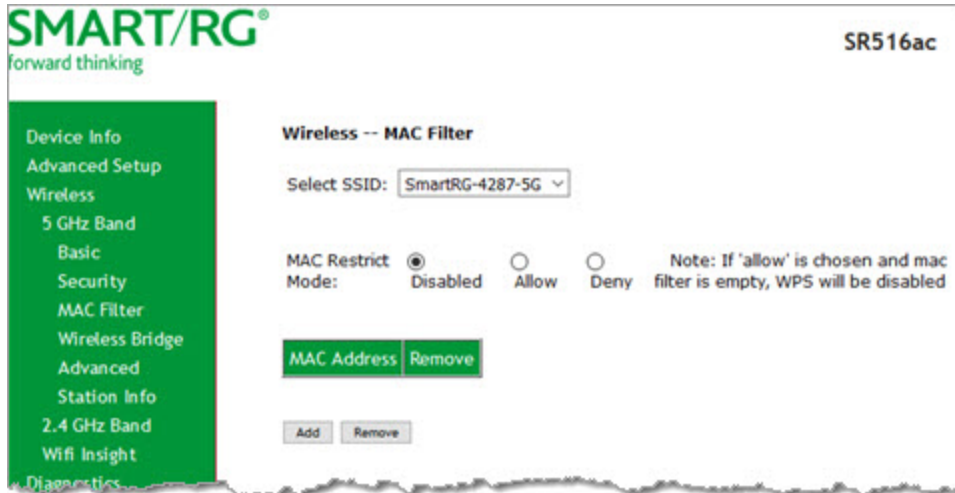
Modify the fields as needed, using the information provided in the table below, and then click **Apply/Save**.

| Field Name | Description |
|-----------------------------|---|
| Protected Management Frames | Select whether management frames are protected. Options are Disabled , Capable , and Required . The default is Disabled . |
| 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. The default is 0 . |
| 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. 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. |

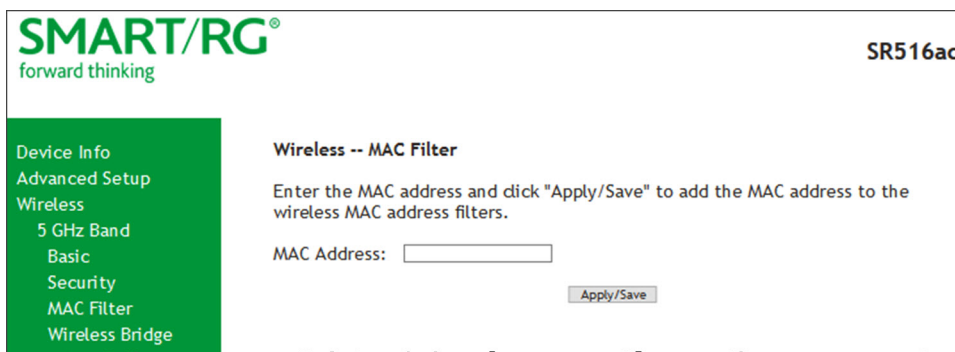
MAC Filter

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.

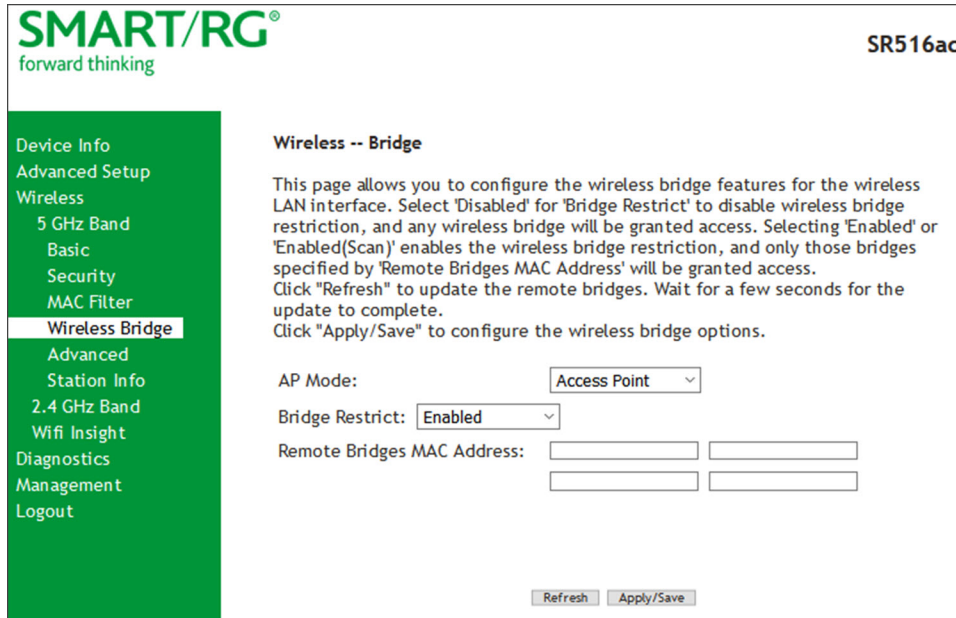


- b. Enter the **MAC address** of the wireless client.
 - c. Click **Apply/Save** to save the address to the list. You are returned to the Wireless - MAC Filter page.
5. To remove a MAC address from the list, click the **Remove** check box next to it and then click the **Remove** button. The list refreshes.

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 |
|----------------------------|---|
| AP Mode | Select whether to use this gateway as an access point or a wireless bridge. The default is Access Point . |
| Bridge Restrict | Enable or disable the bridge restrict function for MAC addresses in the Remote Bridges MAC Address field. Options are: <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 SR516ac

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.

| | | |
|---------------------------------|----------|-------------------------------|
| 802.11ac Band: | 5GHz | |
| Channel: | Auto | Current: 100 |
| Auto Channel Timer(min) | 15 | |
| MIMO-OFDM: | On | |
| Bandwidth: | 80MHz | Current: 80MHz |
| Control Sideband: | Lower | Current: N/A |
| MIMO Data Rate: | Auto | |
| RTS/CTS Protection: | Auto | |
| Support MIMO Clients Only: | Off | |
| RIFS Advertisement: | Auto | |
| OBSS Coexistence: | Disable | |
| RX Chain Power Save: | Disable | Power Save status: Full Power |
| RX Chain Power Save Quiet Time: | 10 | |
| RX Chain Power Save PPS: | 10 | |
| 54g™ 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: | Enabled | |
| Regulatory Mode: | 802.11h | |
| Pre-Network Radar Check: | -1 | |
| In-Network Radar Check: | -1 | |
| TPC Mitigation(db): | 0(off) | |
| Transmit Power: | 100% | |
| WMM(Wi-Fi Multimedia): | Enabled | |
| WMM No Acknowledgement: | Disabled | |
| WMM APSD: | Enabled | |
| Beamforming Transmission (BFR): | Disabled | |
| Beamforming Reception (BFE): | Disabled | |
| Band Steering: | Disabled | |
| Enable Traffic Scheduler: | Disable | |
| Airtime Fairness: | Enable | |

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

| Field Name | Description |
|---------------|---|
| 802.11ac Band | The only option for this field is the band selected in the left menu. |

| Field Name | Description |
|--------------------------------|--|
| 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. |
| Auto Channel Timer (min) | Enter the frequency (in minutes) at which the gateway scans channels for interference. If a threshold of inference is detected, a new channel will be selected automatically. Options are 0 - 65535 minutes. The default is 15 minutes. |
| MIMO-OFDM | Select whether to enable Multiple-Input, Multiple-Output - Orthogonal Frequency-Division Multiplexing (MIMO-OFDM) interface. Options are: Auto and Disabled . The default is Auto . |
| Bandwidth | Select the operating bandwidth. Options are 20 MHz and 40 MHz . The default is 40MHz for the 2.4 GHz band and 80 MHz for the 5 GHz band. The current bandwidth setting displays to the right of the field. |
| Control Sideband | This option is not available. The value is set by the system and cannot be changed. |
| MIMO Data Rate | Select the desired physical transmission rate. Options are Auto , Use 54G Rate , 1-11 , and 32 . The default is Auto . The Auto setting enables the Auto-Fallback feature which allows the gateway to automatically use the fastest possible data rate. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client. |
| RTS/CTS Protection | Select whether to enable RTS/CTS and legacy clients to both work effectively on the network. Options are: <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 MIMO clients only | Select whether to restrict MIMO clients from accessing the gateway. Options are On and Off . The default is Off . |
| RIFS Advertisement | RIFS (Reduced InterFrame Speed) is the time in micro seconds by which the multiple transmissions from a single station is separated. This option Improves performance by reducing dead time required between OFDM transmission. Options are 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. • Disable: The gateway advertises and operates in 40 MHz mode regardless of how other nearby networks are configured. This is the default. |
| RX Chain Power Save | Select whether power-save mode is enabled. Options are Disable and Enable . The default is Enable . |
| 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 period has elapsed. The default is 10 seconds. |
| 54g Rate | This option is set to 1 Mbps for the 2.4GHz radio and to 6 Mbps for the 5GHz radio and cannot be |

| Field Name | Description |
|-------------------------|---|
| | changed. |
| Multicast rate | Select the multicast transmission rate for the network according to the speed of your wireless network. Select from a range of transmission speeds or select Auto to have the gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the gateway and a wireless client. Options are Auto and 6 - 54 Mbps . The default value is Auto . |
| Basic Rate | Select the basic transmission rate ability for the AP. Options are Default, All, 6 & 12 Mbps, and 6 & 12 & 24 Mbps . The default is Default . |
| Fragmentation Threshold | Enter the size at which packets will be fragmented into smaller units. The primary consideration for this setting is the size/capability of the circuit. Options are 256 - 2346 bytes . The default is 2346 bytes . Note: A high packet error rate is an indication that a slightly increased fragmentation threshold is needed. When possible, the default value of 2346 bytes should be maintained. Poor throughput is a likely result of setting this threshold too low. |
| RTS Threshold | The gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. If a packet is smaller than this setting, the WLAN client hardware does not invoke its RTS/CTS mechanism. Options are 256 - 2347 bytes . The default value 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. |
| DTIM Interval | Enter the Delivery Traffic Indication Message (DTIM or Beacon rate) countdown variable used to indicate when the next window is available to client devices for listening to buffered broadcast and multicast messages. Options are 1 - 255 . The default is 1 . |
| Beacon Interval | 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. Enter the time interval (in milliseconds) between beacon transmissions. Options are 1 - 65535 ms . The default is 100 ms , which is recommended. |
| Global Max Clients | Enter the maximum number of clients that can access this wireless network at one time. The maximum for 5 GHz is 80 ; the maximum for 2.4 GHz is 128 . The default is the maximum for each band. Note: You must change this field before you can change the Max Clients on the Wireless > Basic. page. |
| Xpress™ Technology | Select whether to enable Xpress Technology, a special accelerating technology for IEEE802.11g. Options are Enabled and Disabled . The default is Enabled . |
| Regulatory Mode | Select the regulation to be used for this network. Options are Disabled, 802.11h, and 802.11d . |
| Pre-Network Radar Check | The radar check parameter setting for traffic trying to access your gateway from outside the network. |
| In-Network Radar Check | The radar check setting for traffic trying to access your gateway from inside your network. |
| TPC Mitigation | Select the TPC (transmitter power control) mitigation value in db. Options are 0 and 2 - 4 db . The default is 0 (Off) . |
| Transmit Power | Enter the desired output power (by percentage). Options are 20%, 40%, 60%, and 100% . The default is |

| Field Name | Description |
|--------------------------------|--|
| | 100%. |
| WMM (WiFi Multimedia) | This technology allows multimedia services (audio, video and voice packets) to get higher priority for transmission. Options are Auto , Enabled , and Disabled . The default is Enabled . Warning: If you disable this option, all QoS queues and classifications defined for the wireless network are also disabled. |
| WMM No Acknowledgment | The acknowledge policy used at the MAC level. Enabling this option allows better throughput but, in a noisy RF environment, higher -96.3 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 , SU BFR , and MU BFR . The default is Disabled . |
| Beamforming Reception (BFE) | Select to concentrate the transmission signal at the gateway location. Options are Disabled , SU BFE , and MU BFE . 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.

SMART/RG
forward thinking

SR516ac

Device Info
Advanced Setup
Wireless
5 GHz Band
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
2.4 GHz Band

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

| MAC | Associated | Authorized | SSID | Interface |
|-------------------|------------|------------|-----------------|-----------|
| 00:EE:BD:A0:C8:A5 | Yes | Yes | SmartRG-9bb2-5G | wl0 |

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
SR516ac

Device Info
Advanced Setup
Wireless
5 GHz Band
2.4 GHz Band
Wifi Insight
Configure
Site Survey
Channel Statistics
Metrics
Diagnostics
Management
Logout

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

Caution - Enabling wifi insight could result in reduced wifi performance

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

Export Database

- 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**. Skip the **Start Data Collection** button for now.
 - b. Select the days of the week when the data should be collected.
 - c. In the **From** and **To** fields, enter the start and end times for collection.
4. In the **Database Size** section, configure the database size limits:
 - a. In the **Database Size** field, enter the maximum size for the database file where the collected data will be stored. The default is 2 MB.
 - b. *(Optional)* Select whether to stop data collection when the maximum size is reached. Options are **Overwrite Older Data** and **Stop Datacollection**. The default is **Overwrite Older Data**.
5. *(Optional)* In the **Counters** section, clear any counter options that you do not need. The default is to collect all counters.
6. If you're ready to start collecting data now, click **Start Data Collection**.
7. Click **Submit** to save the configuration.
8. 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** 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.

SMART/RG[®]
forward thinking

SR516ac

Device Info
Advanced Setup
Wireless
5 GHz Band
2.4 GHz Band
Wifi Insight
Configure
Site Survey
Channel Statistics
Metrics
Diagnostics
Management
Logout

2.4 GHz - SmartRG-9bb2 Select Channel Select Bandwidth Scan

AP's Around

Signal Strength [dBm]

SmartRG-9bb2

Channels

| Network Name | Network Address | Signal [dBm] | SNR [dB] | Bandwidth [MHz] | Center Channel | Control Channel | Max PHY Rate [Mbps] | 802.11 | Security |
|--------------|-------------------|--------------|----------|-----------------|----------------|-----------------|---------------------|--------|------------------------|
| SmartRG-9bb2 | E8:2C:6D:23:9B:B5 | 0 | 84 | 20 | 1 | 1 | 144 | bgn | AES , WPA-PSK WPA2-PSK |

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

Channel Statistics

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

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

SMART/RG
forward thinking

SR516ac

Device Info
Advanced Setup
Wireless
5 GHz Band
2.4 GHz Band
Wifi Insight
Configure
Site Survey
Channel Statistics
Metrics
Diagnostics
Management
Logout

2.4 GHz - SmartRG-9bb2

Current Channel : 1
Current Channel BandWidth: 20 MHz
Current Available Capacity : 0%

Associated Station's
Shows stations associated with AP.

SSID : SmartRG-9bb2
BSSID : E8:2C:6D:23:9B:B5
Channel : 1

Channel Capacity
Shows bandwidth that is available for use in each channel.

20MHz

Percentage [%]

100
80
60
40
20
0

1 2 3 4 5 6 7 8 9 10 11

Center Channels

Available Capacity

40MHz

Percentage [%]

100
80
60
40
20
0

3 4 5 6 7 8 9

Center Channels

Available Capacity

Interference
Shows interference level in each channel.

20MHz

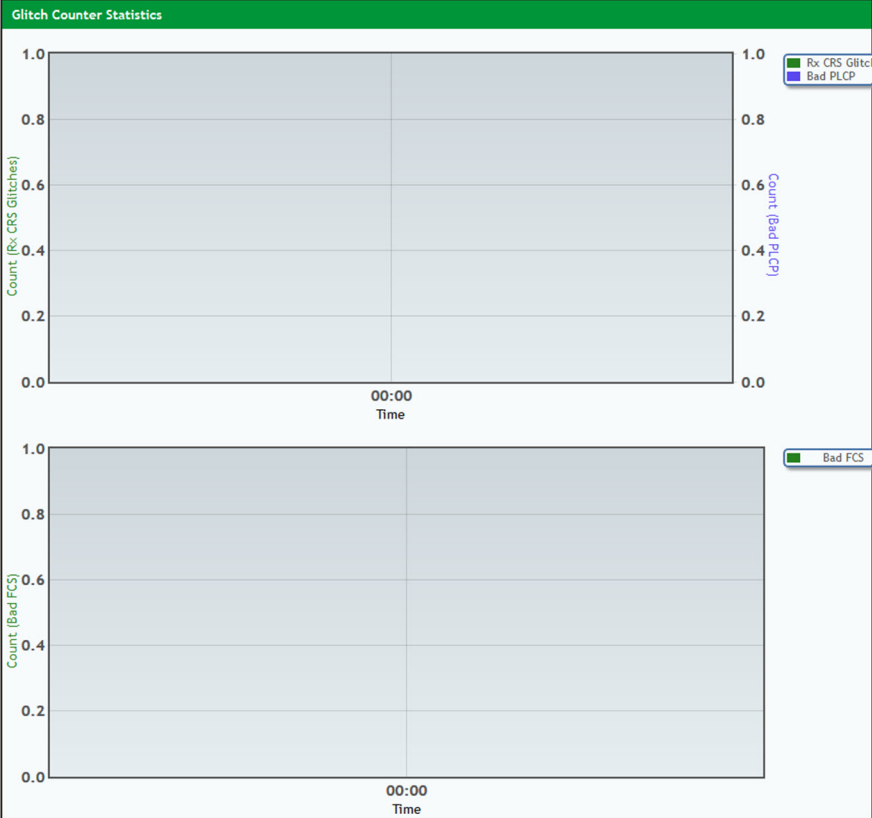
Metrics

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.

- Device Info
- Advanced Setup
- Wireless
 - 5 GHz Band
 - 2.4 GHz Band
 - Wifi Insight
 - Configure
 - Site Survey
 - Channel Statistics

2.4 GHz - SmartRG-9bb2

- Metrics**
- Diagnostics
- Management
- Logout



Chaninm Statistics

| | | | | | | | | | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| tx | inbss | obss | nocat | nopkt | doze | txop | goodtx | badtx | glitch | badplcp | knoise | idle | |

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

SR516ac

Device Info
Advanced Setup
Wireless
Diagnostics
Diagnostics
Ethernet OAM
Ping Host
Trace Route to Host
Management
Logout

ipoe_0_0_35 Diagnostics

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 LAN1 connection: | FAIL | Help |
| Test your LAN2 connection: | PASS | Help |
| Test your LAN3 connection: | FAIL | Help |
| Test your LAN4 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: | FAIL | Help |
| Ping primary Domain Name Server: | FAIL | 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.

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

SMART/RG®
forward thinking

SR516ac

Device Info

Advanced Setup

Wireless

Diagnostics

Diagnostics

Ethernet OAM

Ping Host

Trace Route to Host

Management

Logout

Ethernet Link OAM (802.3ah)

Enabled

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.

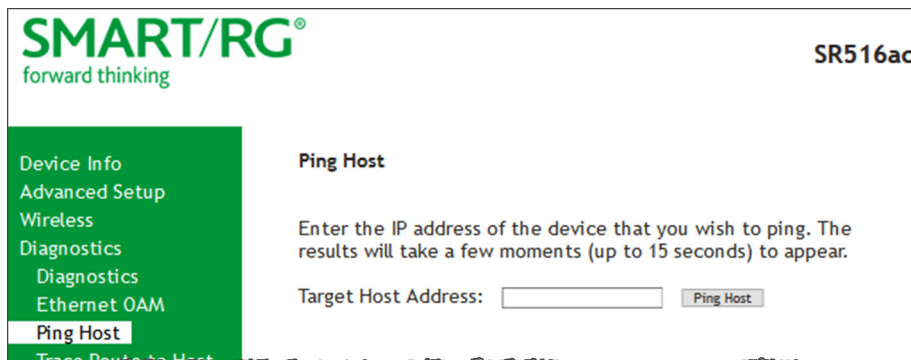
| Field Name | Description |
|--|--|
| Ethernet Link OAM (802.3ah) section | |
| WAN Interface | Select the WAN interface that you want to test. |
| OAM ID | Enter the ID of this OAM configuration. Only positive numbers are allowed. |
| Auto Event | Click to <i>enable</i> automatic reporting of events.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

| Field Name | Description |
|--|---|
| Remote Loopback | Click to <i>enable</i> on-demand link diagnostics, including bit-error-rate approximation. |
| Active Mode | Click to <i>enable</i> 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 <i>enable</i> 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. |

Ping Host

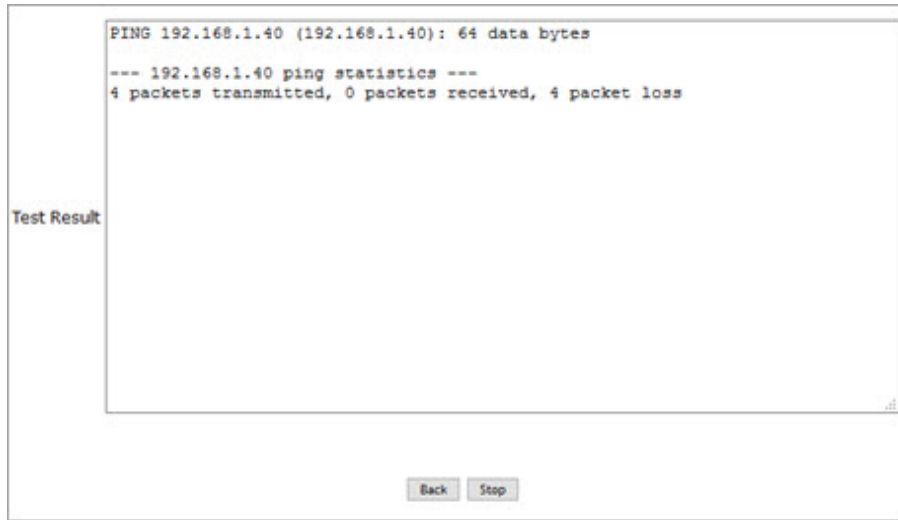
On this page you can ping a server by host name or IP address.

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



2. Enter the host name or IP address.

3. Click **Submit**. The details of the ping appear on the page.

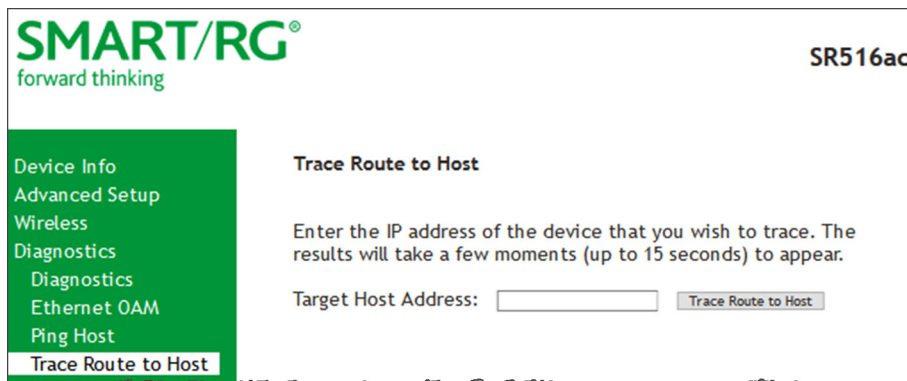


4. To return to the Ping Host page, click **Back**.
5. To stop a test, click **Stop**.

Trace Route to Host

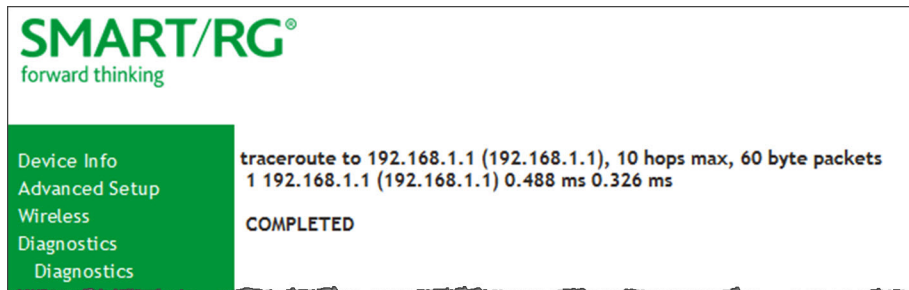
On this page, you can use the traceroute utility to trace a connection.

1. In the left navigation menu, click **Diagnostics > Trace Route to Host**. 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 Trace Route to Host page, click **Back**.
5. To stop a test, click **Stop**.

Management

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

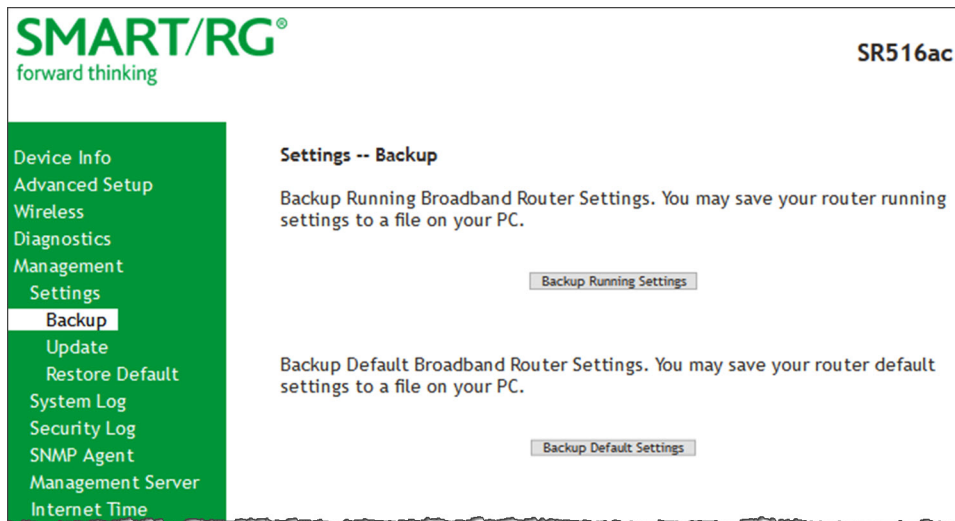
Settings

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.

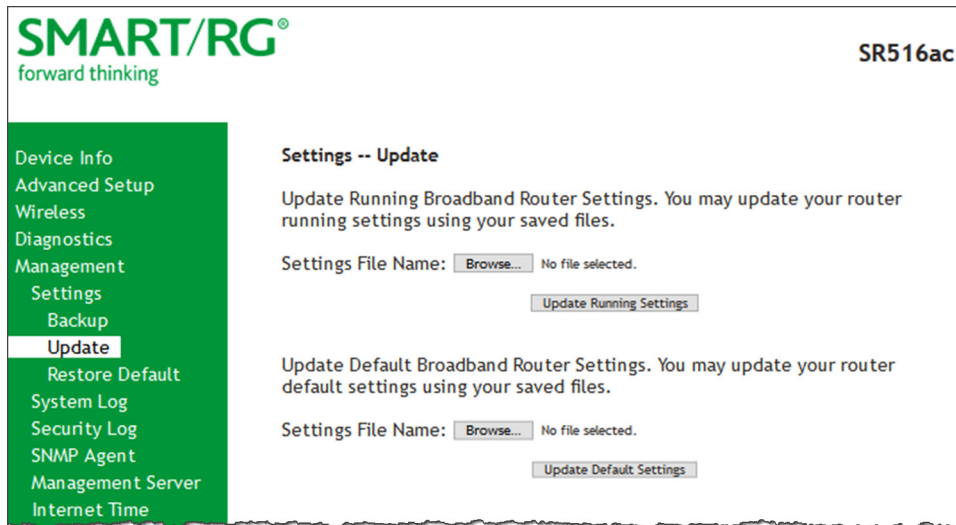


2. To back up the current *running* settings:
 - a. Click **Backup Running Settings**. The Opening file dialog box appears.
 - b. Click **OK**. The file is saved to your default download location and is named "backupsettings.conf".
3. To back up the current *default* settings:
 - a. Click **Backup Default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

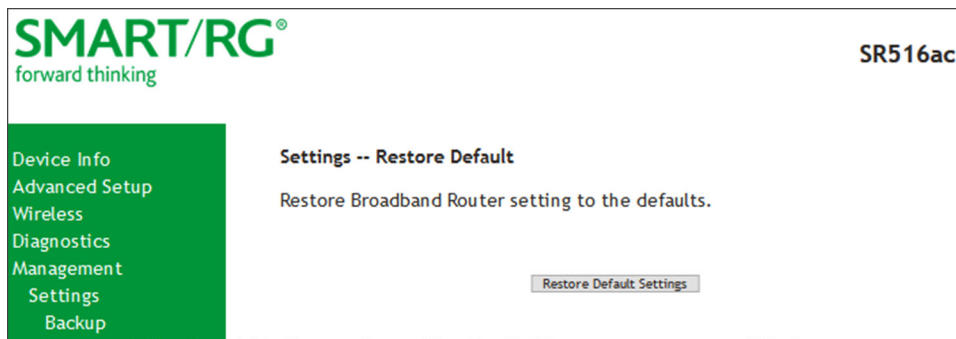


2. To update settings from a file that you saved previously:
 - a. Click the **Browse** button to locate either a customized setting file or the default setting file (.conf file) on your local system and click **Open**.
 - b. Click **Update Settings**. The gateway reboots when the update has completed.

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.

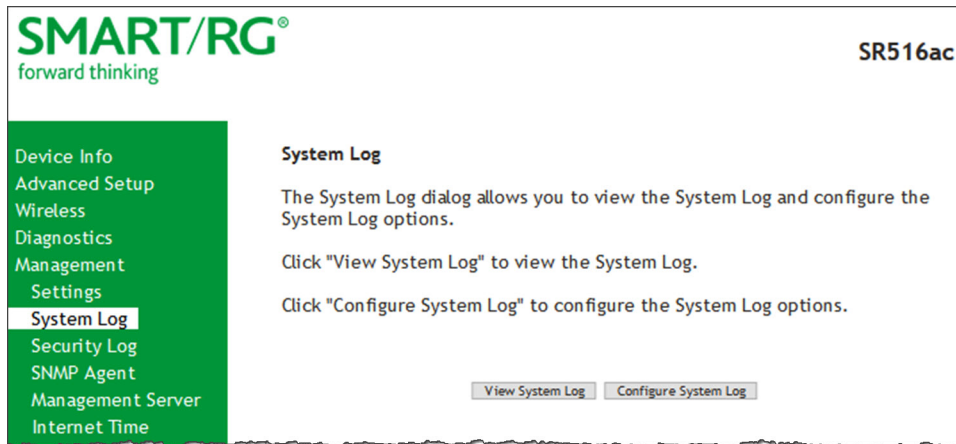


2. Click **Restore Default Settings**. The system returns to the default settings and reboots.

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.

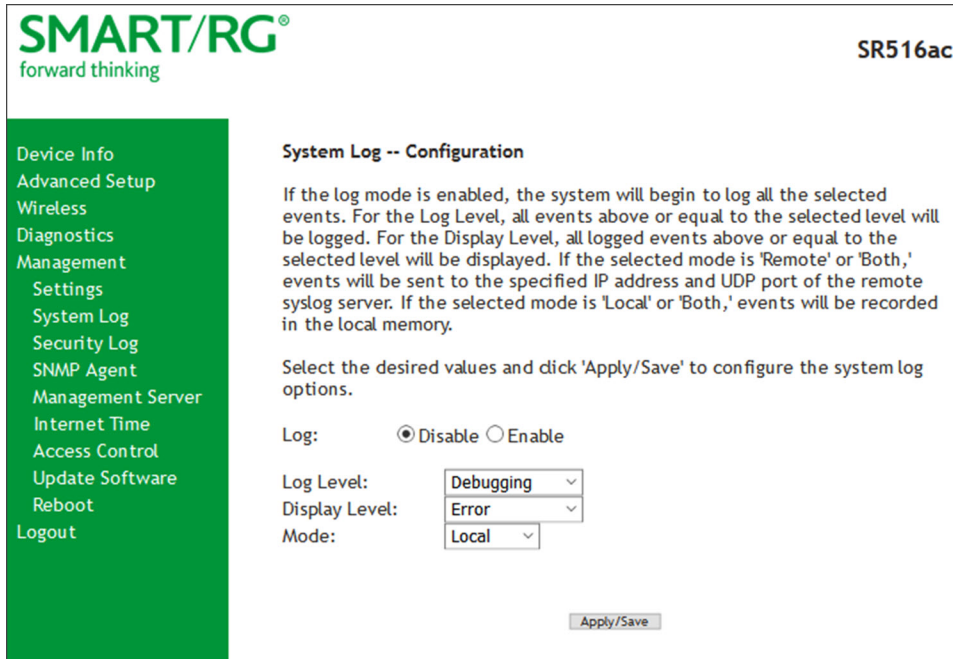


2. To view the system log details:
 - a. Click **View System Log**. The log appears in a separate window.

| Date/Time | Facility | Severity | Message |
|-----------------|----------|----------|---|
| Feb 13 14:57:23 | kern | err | kernel: PPP_KERN: num0=0, num1=1, num2=2, index=524290 register device ppp0.2 |
| Feb 13 14:57:23 | daemon | crit | syslog: PPP LCP UP. |
| Feb 13 14:57:24 | daemon | err | syslog: User name and password authentication failed. |
| Feb 13 14:57:33 | daemon | crit | syslog: PPP server detected. |
| Feb 13 14:57:33 | daemon | crit | syslog: PPP session established. |
| Feb 13 14:57:33 | kern | err | kernel: PPP_KERN: ppp_create_interface: unit=524290 |
| Feb 13 14:57:33 | kern | err | kernel: PPP_KERN: num0=0, num1=1, num2=2, index=524290 register device ppp0.2 |
| Feb 13 14:57:33 | daemon | crit | syslog: PPP LCP UP. |
| Feb 13 14:57:34 | daemon | err | syslog: User name and password authentication failed. |
| Feb 13 14:57:43 | daemon | crit | syslog: PPP server detected. |
| Feb 13 14:57:43 | daemon | crit | syslog: PPP session established. |
| Feb 13 14:57:43 | kern | err | kernel: PPP_KERN: ppp_create_interface: unit=524290 |
| Feb 13 14:57:43 | kern | err | kernel: PPP_KERN: num0=0, num1=1, num2=2, index=524290 register device ppp0.2 |
| Feb 13 14:57:43 | daemon | crit | syslog: PPP LCP UP. |
| Feb 13 14:57:44 | daemon | err | syslog: User name and password authentication failed. |
| Feb 13 14:57:47 | daemon | crit | syslog: PPP server detected. |
| Feb 13 14:57:47 | daemon | crit | syslog: PPP session established. |
| Feb 13 14:57:47 | kern | err | kernel: PPP_KERN: ppp_create_interface: unit=524290 |
| Feb 13 14:57:47 | kern | err | kernel: PPP_KERN: num0=0, num1=1, num2=2, index=524290 register device ppp0.2 |
| Feb 13 14:57:47 | daemon | crit | syslog: PPP LCP UP. |
| Feb 13 14:57:48 | daemon | err | syslog: User name and password authentication failed. |
| Feb 13 14:57:57 | daemon | crit | syslog: PPP server detected. |
| Feb 13 14:57:57 | daemon | crit | syslog: PPP session established. |

- 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.

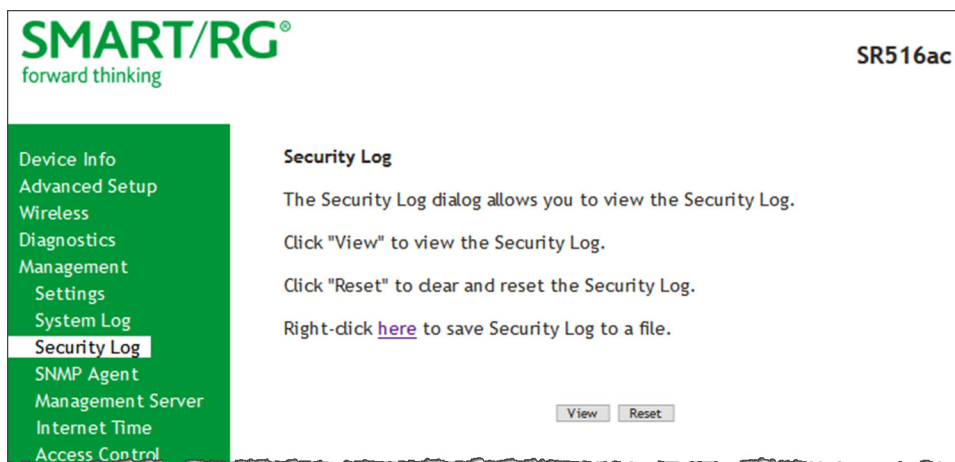
| Action | Description |
|---------------|--|
| Log Level | Select the type of information that you want logged. Options are Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debugging . The options are listed in order from least detailed to most detailed. The default is Debugging . |
| Display Level | Select the level of information that should be displayed. Options are Emergency, Alert, Critical, Error, Warning, Notice, 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. Options are Local, Remote, and Both . 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:

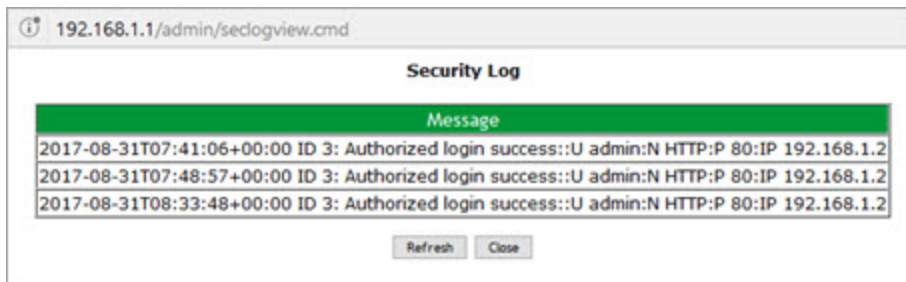
- Password change success / failure
- Authorized login success / failure
- Security lockout added / removed
- Authorized / unauthorized resource access
- Software update

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 confirming 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.

SMART/RG
forward thinking

SR516ac

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

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 | <i>(Optional)</i> Enter the location of the system. |
| System Contact | <i>(Optional)</i> Enter the contact for the system. |
| Trap Manager IP | <i>(Optional)</i> 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

SR516ac

Device Info

Advanced Setup

Wireless

Diagnostics

Management

Settings

System Log

Security Log

SNMP Agent

Management Server

TR-069 Client

STUN Config

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.

OUI-Serial MAC Serial Number

TR-069 Client Disable Enable

ACS URL from DHCP: Disabled Enabled

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

TR-069 Client Port:

WAN Interface used by TR-069 client:

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

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

| Field Name | Description |
|-------------------|--|
| OUI-Serial | Select whether to use the MAC address or the device serial number as the identifier. The default is MAC . |
| TR-069 Client | This option is enabled by default. To <i>disable</i> this feature, click Disable . |
| ACS URL from DHCP | Click to enable the gateway to obtain the ACS URL from the DHCP server. |
| 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. The default is 3600 seconds (1 hour). |
| ACS URL | <p>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.</p> <p>You can include a port specification suffix if your ACS platform requires it, e.g., http://customer1.acs.smartrg.com:30005 where 30005 is the port number. The default port is 30005.</p> |

| Field Name | Description |
|-------------------------------------|--|
| ACS User Name | Enter the user name by which this gateway logs in to the ACS. |
| ACS Password | Enter the password to authenticate the above user name. |
| TR-069 Client Port | If your ACS platform requires it, enter a port specification suffix here, e.g., http://-customer1.acs.smartrg.com:30005 where 30005 is the port number. The default port is 30005 . |
| 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. |

- (Optional) Configure the modem client Connection Request mechanism used by your ACS to communicate with subscriber gateways, using the information in the table below.
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 URL | This URL is set automatically and cannot be changed. It includes the request port number, e.g., http://10.101.40.115:30005/. |

- 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.
- 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 |

| Field Name | Description |
|---|---|
| | 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.

Internet Time

On this page, you can configure the gateway to synchronize its time with the Internet time servers.

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

SMART/RG
forward thinking

SR516ac

- Device Info
- Advanced Setup
- Wireless
- Diagnostics
- Management
- Settings
- System Log
- Security Log
- SNMP Agent
- Management Server
- Internet Time**
- Access Control
- Update Software
- Reboot
- Logout

Time settings

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

Automatically synchronize with Internet time servers

Apply/Save

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

SMART/RG
forward thinking

SR516ac

- Device Info
- Advanced Setup
- Wireless
- Diagnostics
- Management
- Settings
- System Log
- Security Log
- SNMP Agent
- Management Server
- Internet Time**
- Access Control
- Update Software
- Reboot
- Logout

Time settings

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

Automatically synchronize with Internet time servers

First NTP time server: time.nist.gov

Second NTP time server: ntp1.tummy.com

Third NTP time server: None

Fourth NTP time server: None

Fifth NTP time server: None

Time zone offset: (GMT-08:00) Pacific Time, Tijuana

Apply/Save

3. Select the desired time servers.
4. Select the **Time zone offset**.
5. (Optional) Click **Enable Daylight Savings Time**.
6. Click **Apply/Save** to save and apply the settings.
7. 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.

Accounts

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

Add an Account

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

SMART/RG®
forward thinking

SR516ac

User Access Control Settings

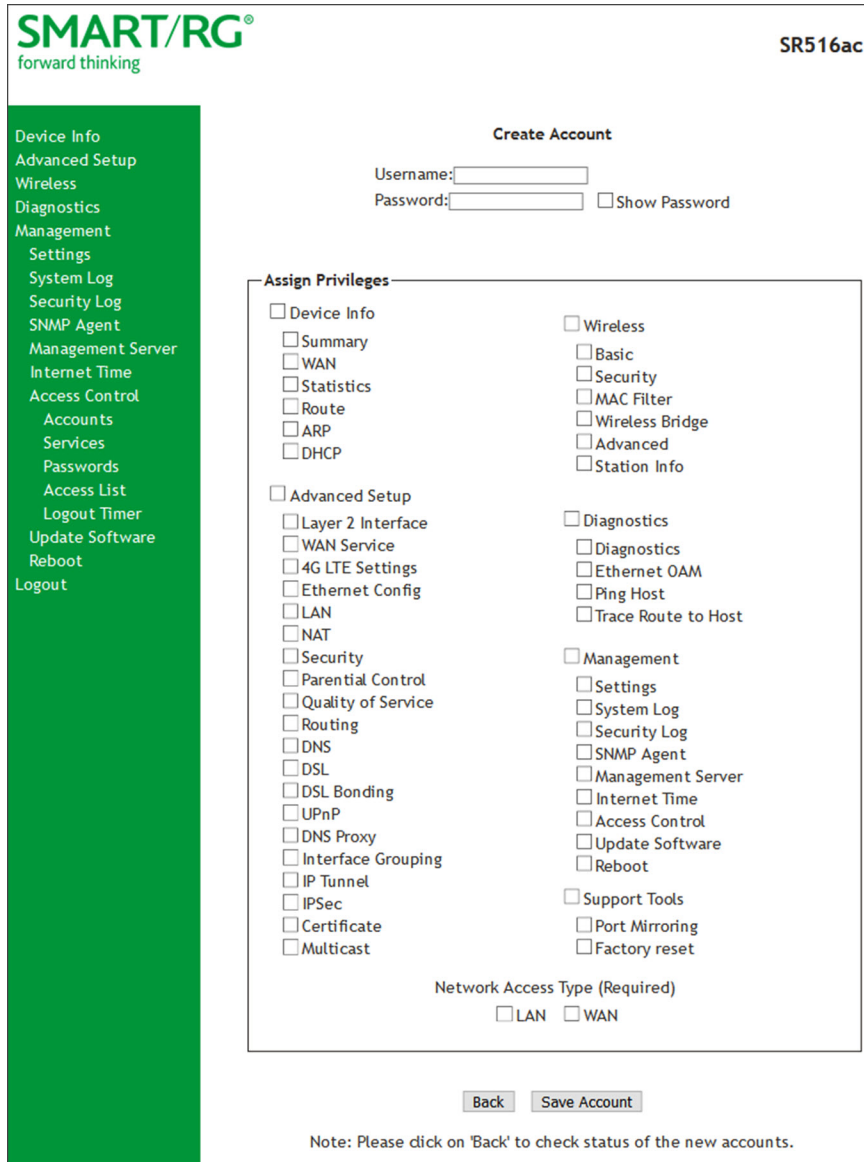
Choose an option:

Create Account Delete/Modify Account

User Account Status

| Username | Status |
|----------|---------|
| support | Enabled |
| user | Enabled |
| mfg | Enabled |

- To set up a new user, click **Create Account**. The following page appears.



SMART/RG
forward thinking

SR516ac

Create Account

Username:

Password: Show Password

Assign Privileges

| | |
|---|--|
| <input type="checkbox"/> Device Info | <input type="checkbox"/> Wireless |
| <input type="checkbox"/> Summary | <input type="checkbox"/> Basic |
| <input type="checkbox"/> WAN | <input type="checkbox"/> Security |
| <input type="checkbox"/> Statistics | <input type="checkbox"/> MAC Filter |
| <input type="checkbox"/> Route | <input type="checkbox"/> Wireless Bridge |
| <input type="checkbox"/> ARP | <input type="checkbox"/> Advanced |
| <input type="checkbox"/> DHCP | <input type="checkbox"/> Station Info |
| <input type="checkbox"/> Advanced Setup | <input type="checkbox"/> Diagnostics |
| <input type="checkbox"/> Layer 2 Interface | <input type="checkbox"/> Diagnostics |
| <input type="checkbox"/> WAN Service | <input type="checkbox"/> Ethernet OAM |
| <input type="checkbox"/> 4G LTE Settings | <input type="checkbox"/> Ping Host |
| <input type="checkbox"/> Ethernet Config | <input type="checkbox"/> Trace Route to Host |
| <input type="checkbox"/> LAN | |
| <input type="checkbox"/> NAT | <input type="checkbox"/> Management |
| <input type="checkbox"/> Security | <input type="checkbox"/> Settings |
| <input type="checkbox"/> Parental Control | <input type="checkbox"/> System Log |
| <input type="checkbox"/> Quality of Service | <input type="checkbox"/> Security Log |
| <input type="checkbox"/> Routing | <input type="checkbox"/> SNMP Agent |
| <input type="checkbox"/> DNS | <input type="checkbox"/> Management Server |
| <input type="checkbox"/> DSL | <input type="checkbox"/> Internet Time |
| <input type="checkbox"/> DSL Bonding | <input type="checkbox"/> Access Control |
| <input type="checkbox"/> UPnP | <input type="checkbox"/> Update Software |
| <input type="checkbox"/> DNS Proxy | <input type="checkbox"/> Reboot |
| <input type="checkbox"/> Interface Grouping | <input type="checkbox"/> Support Tools |
| <input type="checkbox"/> IP Tunnel | <input type="checkbox"/> Port Mirroring |
| <input type="checkbox"/> IPSec | <input type="checkbox"/> Factory reset |
| <input type="checkbox"/> Certificate | |
| <input type="checkbox"/> Multicast | |

Network Access Type (Required)

LAN WAN

Note: Please click on 'Back' to check status of the new accounts.

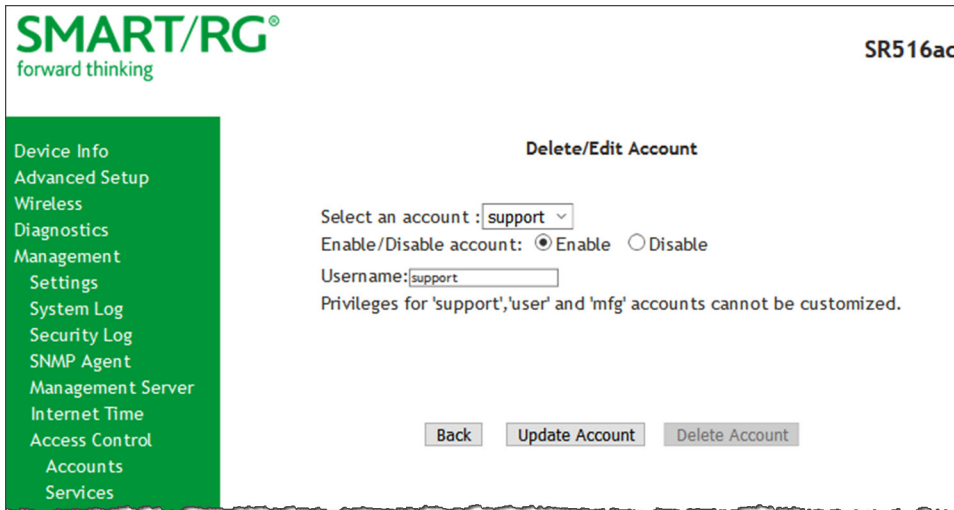
- Enter a **Username** and **Password** for the new account.
- Select the features that you want this user to access. If you select a subcategory, the subordinate boxes are also selected.
- Click **Save Account** to commit your changes. The new account is created. To test the account credentials, log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

Modify or Delete an Account

Notes:

- While you can NOT modify or delete the default user accounts (Admin, Support, MFG, or User), you can disable the **Support**, **MFG**, or **User** accounts.
- You must be logged into the gateway as the Admin or Support user to modify or delete any accounts.

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



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

Your changes are implemented immediately.

Default Passwords

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

Services

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

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

SMART/RG
forward thinking

SR516ac

Access Control -- Services

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

| Services | LAN | WAN | WAN Port Number |
|--|--|---------------------------------|---------------------------------|
| HTTP(S) | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="text" value="80"/> |
| <input type="checkbox"/> Use encrypted HTTP(S) -- unit will restart. | | | |
| FTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | (default) |
| ICMP | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | (default) |
| SNMP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | (default) |
| SSH | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="text" value="22"/> |
| TELNET | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | (default) |
| TFTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | (default) |

Save/Apply

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) If a WAN interface is defined, 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.

Passwords

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

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

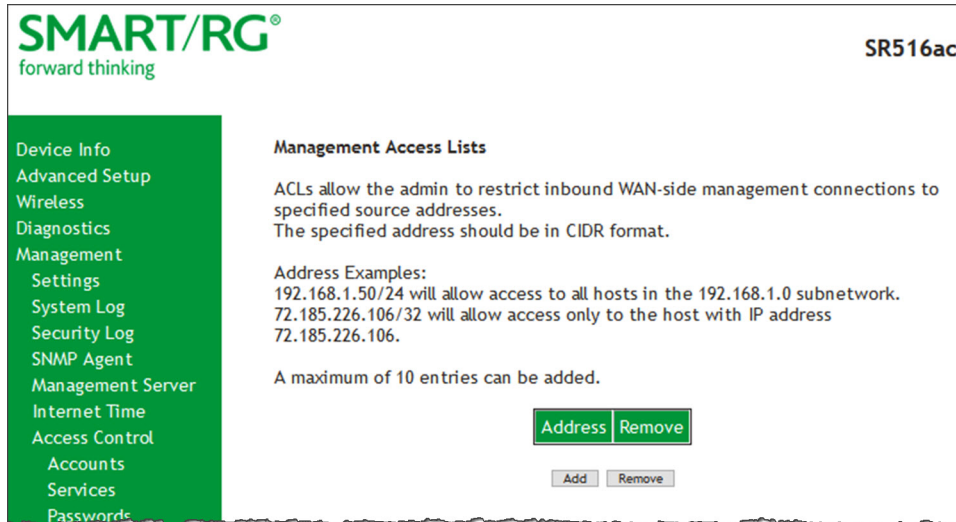
The screenshot shows the SMART/RG SR516ac web interface. On the left is a green navigation menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, Security Log, SNMP Agent, Management Server, Internet Time, Access Control, Accounts, Services, Passwords (highlighted), Access List, Logout Timer, Update Software, Reboot, and Logout. The main content area has a title 'Access Control -- Passwords' and the following text: 'Access to your Router is controlled through three user accounts: admin, support, and user. The user name "admin" has unrestricted access to change and view configuration of your Router. The user name "support" is used to allow an ISP technician to access your Router for maintenance and to run diagnostics. The user name "user" can access the Router, view configuration settings and statistics, as well as update the router's software. Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.' Below the text are four input fields: 'User Name:', 'Old Password:', 'New Password:', and 'Confirm Password:'. An 'Apply/Save' button is located at the bottom right of the form.

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.

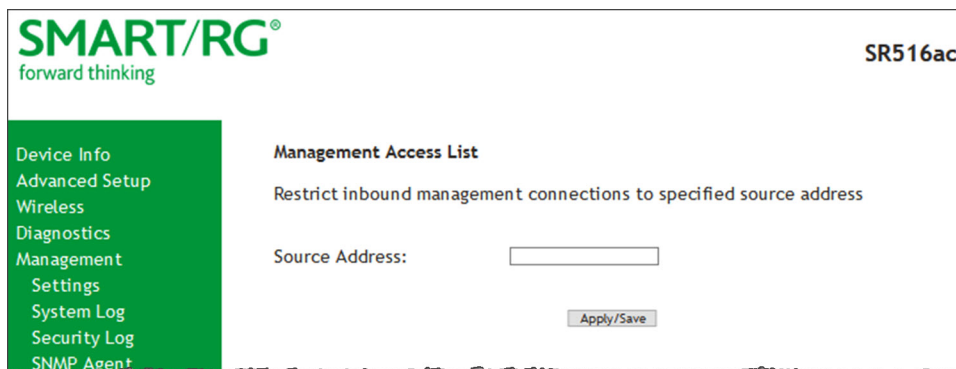
Access List

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.

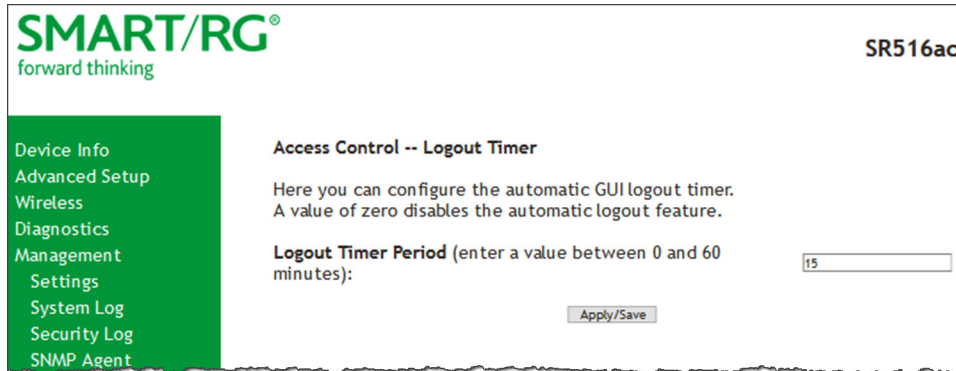


3. Enter the IP address and mask of the station allowed to access local management services.
4. To remove a connection, click the **Remove** checkbox to the right of the entry and then click the **Remove** button.
5. Click **Apply/Save** to save and apply the settings.

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.



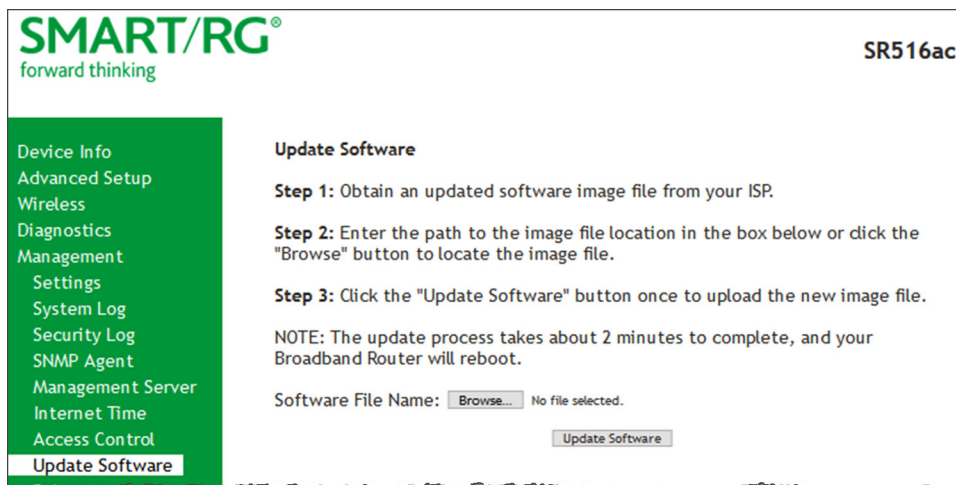
2. In the **Logout Timer Period** field, type the number of minutes after which a session will be ended. Options are 0 - 60 minutes. The default is 15 minutes. To disable this feature, enter a zero (0) in the field.

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: VW7DL01BSR516A.

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

REN=0.1

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 |
|----------|----------------|---|
| 1.6 | July 2021 | Added information for the DHCP Relay field on the LAN configuration page. |
| 1.5 | July 2020 | Updated to match SmartRG Firmware Release 2.6.2.5 |
| 1.4 | March 2020 | Updated to match SmartRG Firmware Release 2.6.2.4. |
| 1.3 | September 2019 | Updated to match SmartRG Firmware Release 2.6.2.3. |
| 1.2 | July 2019 | Updated to match SmartRG Firmware Release 2.6.2.2. |
| 1.1 | Feb 2018 | Updated to match release 1.0.0.112.. |
| 1.0 | Sept 2017 | Initial release of this user manual. |