SMART/RG®
forward thinking

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

/ Gateway User Manual

Model: SR808ac

Release 1.1

April 2018

Table of Contents

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 their SR808ac gateway.

Intended Audience

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

Getting Assistance

Frequently asked questions are provided at the bottom of the Support page of the SmartRG Web site.

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

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

Copyright and Trademarks

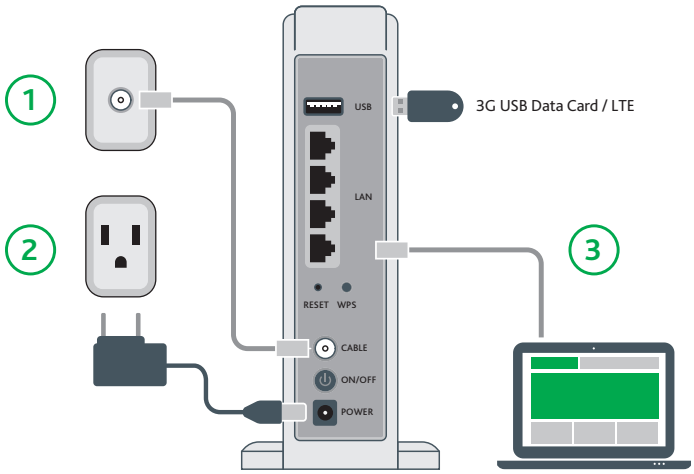
Disclaimer

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.

Installing your Gateway

The connectors located on the back of the SR808ac gateway are described below (from top to bottom).



1. Connect one end of the supplied cable to the port labeled **Cable** on the gateway.
2. Plug the power cord into the wall outlet and into the power jack on the back of the gateway. Turn on the unit by pressing the **On/Off** button on the back of the gateway.
3. Connect one end of an Ethernet cable to a **LAN** port on the gateway. Connect the other end to your laptop.

Your gateway is now automatically being set up to connect to the Internet. Various LEDs on the front of the gateway will flash as setup proceeds. When the **DS** and **US** LEDs glow steady blue and the **Online** LED glows steady white, the gateway is ready for use. This process may take a few minutes to complete.

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

Getting Familiar with Your Gateway

This section describes the gateway's lights, ports, and buttons to help you get familiar with the SR808ac model.

LED Status Indicators

Your SmartRG gateway has several indicator lights (LEDs) on its front. The following table describes those LEDs.

Note: The **POWER**, **DS**, **US** and **ONLINE** LEDs may flash briefly when the gateway boots up.

Legend: White | White blinking | Blue | Blue blinking

INDICATOR	COLOR	STATE	DESCRIPTION
POWER	White		Gateway is powered on and operating normally.
DS US	White		Gateway is ready to connect.
			Connection is being set up.
DS US	Blue		Connection is established and synchronization is accomplished.
			Data is being transferred and synchronization is in progress.
ONLINE	White		Gateway is online and the gateway is ready for use.
			Gateway is connecting to the network or is unable to connect.
2.4 GHz 5 GHz WPS	White		Device is powered on and the device operates normally.
			Software is upgrading or data is being transferred.

Connections

The connectors located on the back of the SR808ac gateway are described below (from top to bottom).

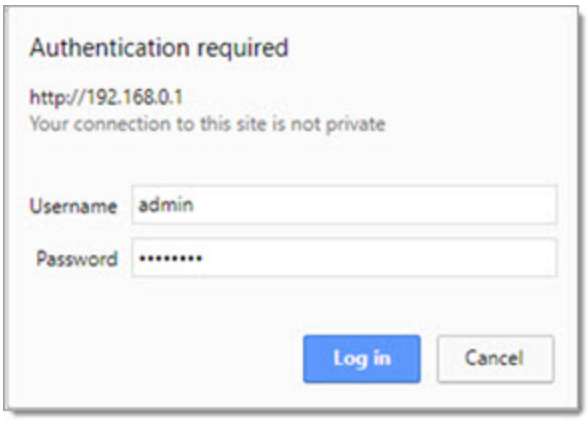
Interface	Description
USB	USB port for connecting other USB storage devices.
LAN 4 - 1	RJ45 ports for connecting the gateway to a PC or another network device.
Reset	The **Reset** button is in a small circular hole on the rear panel. Press the button for at least 1 second and then release it. The system reboots and returns to the factory defaults. **Warning:** Do not press the **Reset** button unless you want to clear the current settings.

Interface	Description
WPS	Button for activating WPS.
Cable	RF cable port, for connecting HFC cable.
On/Off	On/Off button.
Power	Power interface, for connecting the power adapter.

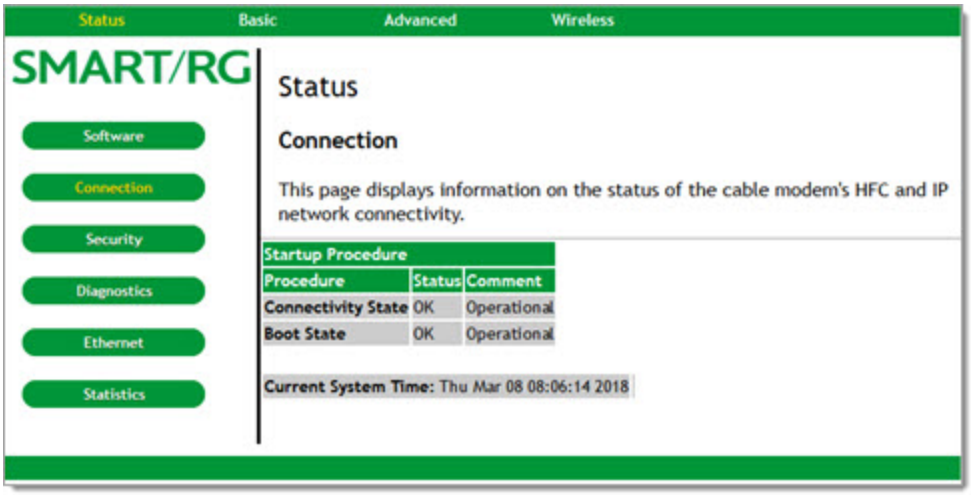
Logging in to Your Gateway's Interface

To manually configure the SmartRG SR808ac gateway, you must log in to the gateway's embedded UI.

1. Open a Web browser on your computer.
2. Enter http://192.168.0.1 (the default IP address of the cable modem gateway) in the address bar. The login dialog box appears.



3. Enter the user name and password. The default user name is admin. The default password is unique for each device (last 4 of MAC address + last 4 of serial number) and is located on the bottom of the gateway. It is recommended that you change these default values after logging in to the gateway for the first time.
4. Click **Log In**. The Status > Connection page appears.



Status

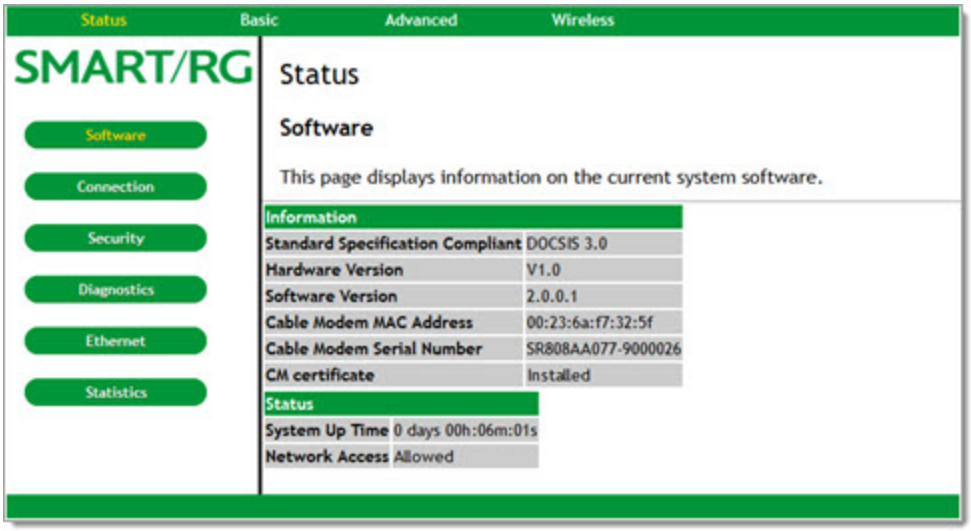
In this section, you can review status data for software, connections, security, diagnostics, Ethernet speed, and gateway statistics.

Software

On this page you can view information about the hardware and software versions, MAC address, serial number, system “up” time, and network registration status.

In the top navigation bar, click **Status** and then click **Software** in the left menu. The Status > Software page appears, where you can view detailed information about the software installed on your gateway.

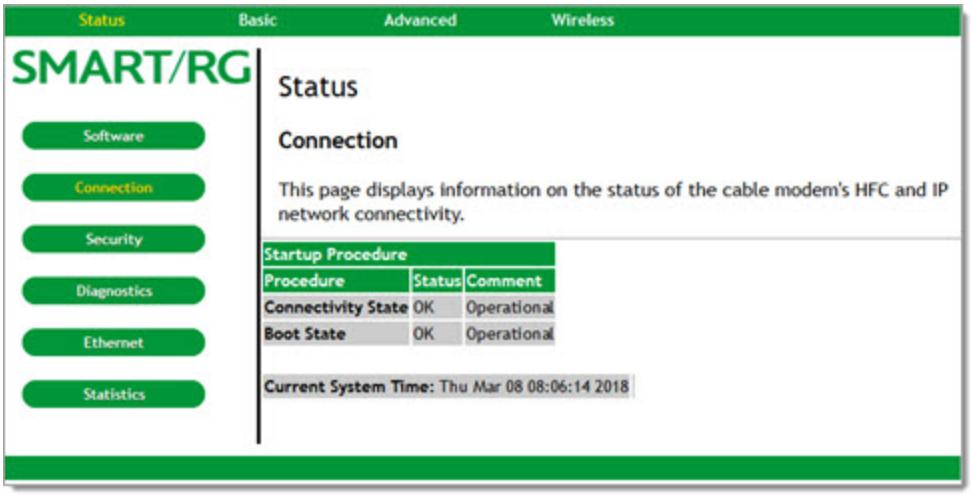
If you need to upgrade the firmware on your gateway, instructions are provided in the Customer Portal in Upgrading or Downgrading a DOCSIS Gateway.



Connection

On this page, you can view the status of the gateway's connectivity, boot state, and the current system time.

In the top navigation bar, click **Status**. The Status > Connection page appears. To refresh the information on this page, click your web browser’s **Refresh** button.



Security

On this page, you can change a user's password and restore the factory default settings.

1. In the top navigation bar, click **Status** and then click **Security** in the left menu. The Status > Security page appears.

2. To change the security password:
   a. In the **Password Change User ID** field, enter the ID for which you want to change the password. The user ID must be 15 characters or less.
   b. In the **Current Password** field, enter the current password.
   c. In the **New Password** and **Re-Enter New Password** fields, enter the new password. Passwords must be 8 char-

acters or less.

d. Click **Apply** to save your changes. You do NOT have to restore factory defaults to change the password.

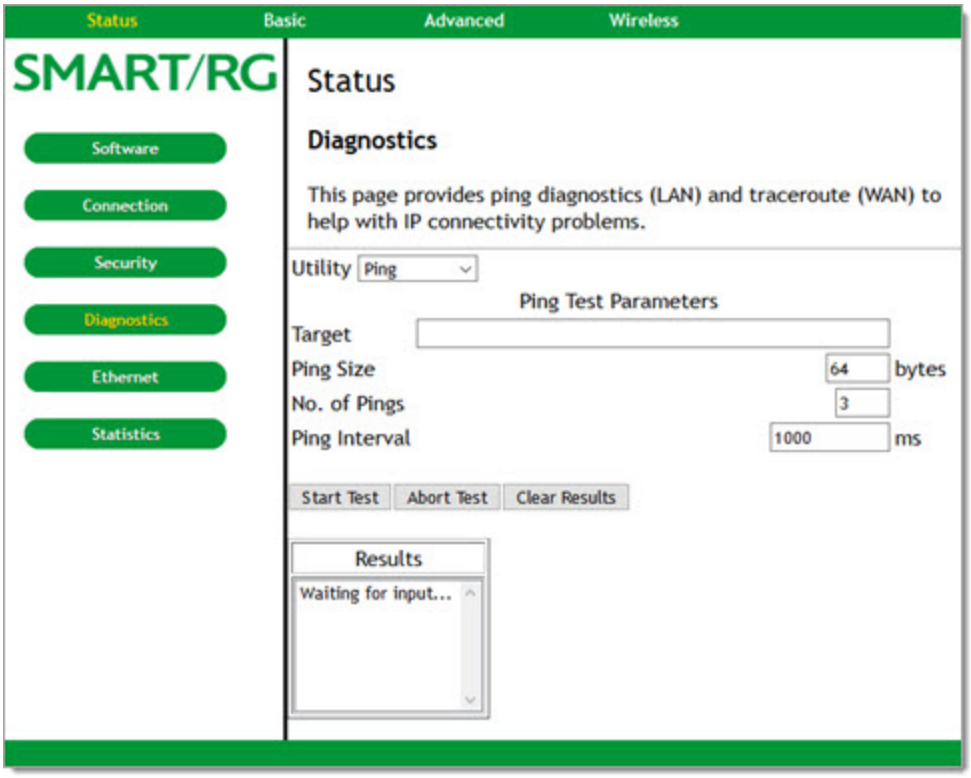
3. To restore factory defaults, click **Yes** and then click **Apply**. The gateway reboots.
4. To log back into the gateway after the factory defaults are restored, you must enter the factory default user name (admin) and the password found on the **Password** label on the bottom of the unit.

Diagnostics

On this page, you can run the Ping and Traceroute utilities to trouble shoot network connectivity:

- Ping allows you to check connectivity between the gateway and devices on the LAN.
- Traceroute allows you to map the network path from the gateway to a public host. When you select **Traceroute** from the **Utility** list, the applicable fields appear.

1. In the top navigation bar, click **Status** and then click **Diagnostics** in the left menu. The Status > Diagnostics page appears.



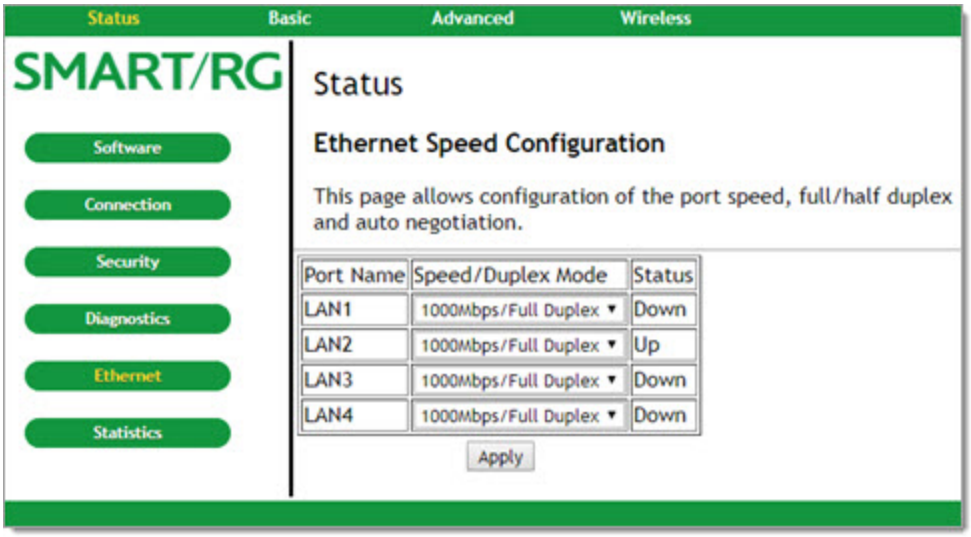
2. To run either utility:
   a. In the **Utility** field, select the utility that you want to run. Options are **Ping** and **Traceroute**. The default is **Ping**.
   b. In the **Target** field, enter the IP address or name.
   c. (*Optional*) Modify the parameters:
      - For a ping test, you can modify **Ping Size**, **No. of Pings** and **Ping Interval**.
      - For a Traceroute test, you can modify **Max Hops**, **Data Size**, **Base Port** and **Resolve Host**.

d. Click **Start Test**. The **Results** field is refreshed automatically as the test is performed. The minimum, maximum and average time statistics display in the **Results** field.
Note: You can abort a ping test by clicking **Abort Test** but you cannot abort a trace test.
e. To clear the test results, click **Clear Results**.

Ethernet

On this page, you can view the current speed and duplex mode settings for each of the four LAN ports and you can adjust the settings for individual LAN ports.

1. In the top navigation bar, click **Status** and then click **Ethernet** in the left menu. The Status > Ethernet Speed Configuration page appears.



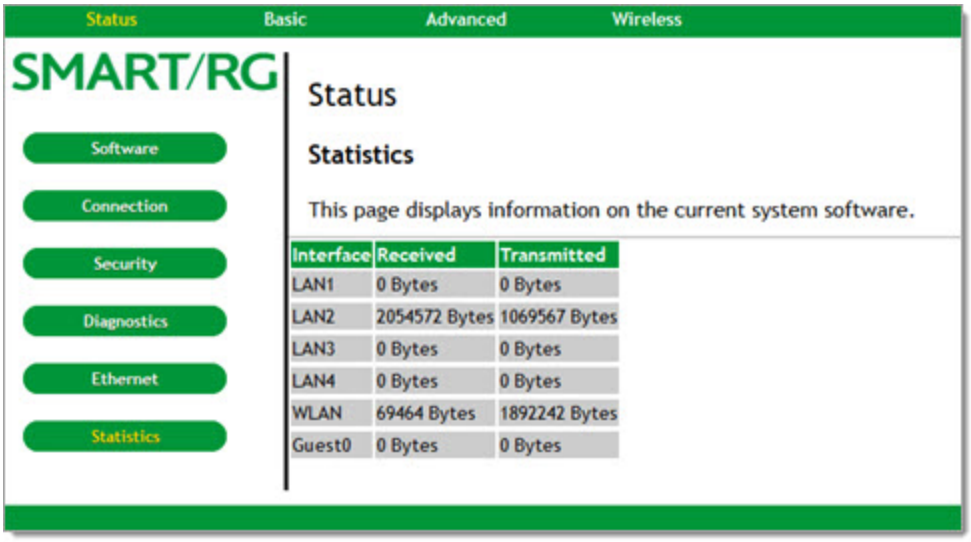
2. For each LAN port that you want to configure, in the **Speed/Duplex Mode** cell, select the appropriate setting. Options are: **10Mbps/Half Duplex**, **10Mbps/Full Duplex**, **100Mbps/HalfDuplex**, **100Mbps/Full Duplex**, **1000Mbps/Full Duplex**, and **Auto Negotiation**. The default is **1000Mbps/Full Duplex**.
3. Click **Apply** to commit your changes.

Statistics

This page displays the bytes transmitted and received for each interface defined for this gateway, such as:

- **LAN1-4**: Bytes transmitted and received for each of the Local Area Network ports.
- **WLAN**: Bytes transmitted and received by the WiFi interface.
- **Guest*n***: Bytes transmitted and received by each of the guest networks in use.

In the top navigation bar, click **Status** and then click **Statistics** in the left menu. The Status > Statistics page appears.



Basic

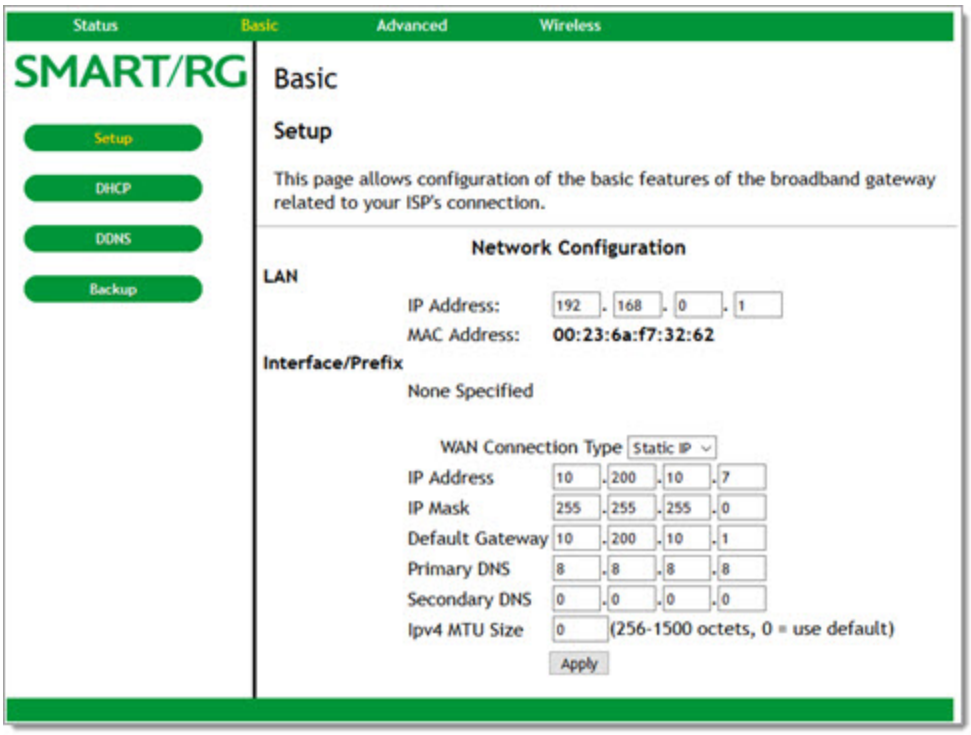
In this section, you can configure the basic features for your gateway such as WAN connection type, DHCP, DDNS, and backup settings.

Setup

On this page, you can configure the basic connection features for your gateway.

Note: If you change the **WAN Connection Type**, the gateway will reboot when you click **Apply**.

1. In the top navigation bar, click **Basic**. The Basic > Setup page appears, showing the settings for a static WAN connection.

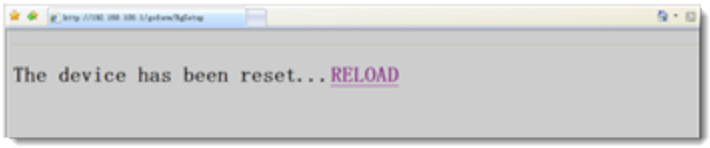


2. (*Optional*) In the **IP Address** field, enter the IP address for your LAN.
3. Enter the applicable IP addresses in the first 5 fields. This information is determined by your ISP.
4. If desired, enter a value in the **IPv4 MTU Size** field. Options are **0** and **256**-**1500** octets. The default is **0** (use default).
5. To configure a dynamic WAN connection, in the **WAN Connection Type** field, select **DHCP**. All other fields except the **Ipv4 MTU Size** field are hidden.
6. Click **Apply** to reset the gateway. The gateway is configured for basic use. It will attempt to obtain an Internet-routable IP address whenever it is connected. For DHCP connections, the **Release WAN Lease** and **Renew WAN Lease** buttons appear when you log back in.
7. To *release* the current lease, click **Release WAN Lease**.
8. To *renew* the current lease, click **Renew WAN Lease**.

Communication with the LAN will work whether the WAN connection provided by the cable gateway is up or down. However, you will not be able to access the Internet until the WAN connection is enabled and has an IP address.

Most configuration items can be changed without rebooting the gateway, but some settings (such as the static WAN IP address parameters) are retrieved only when the gateway first powers up. If you change these settings, the gateway resets so that the new configuration can be retrieved.

When this mandatory reset occurs, the following message appears.



Wait for the gateway to reboot and then click the **RELOAD** link to return to the page where you made your last change.

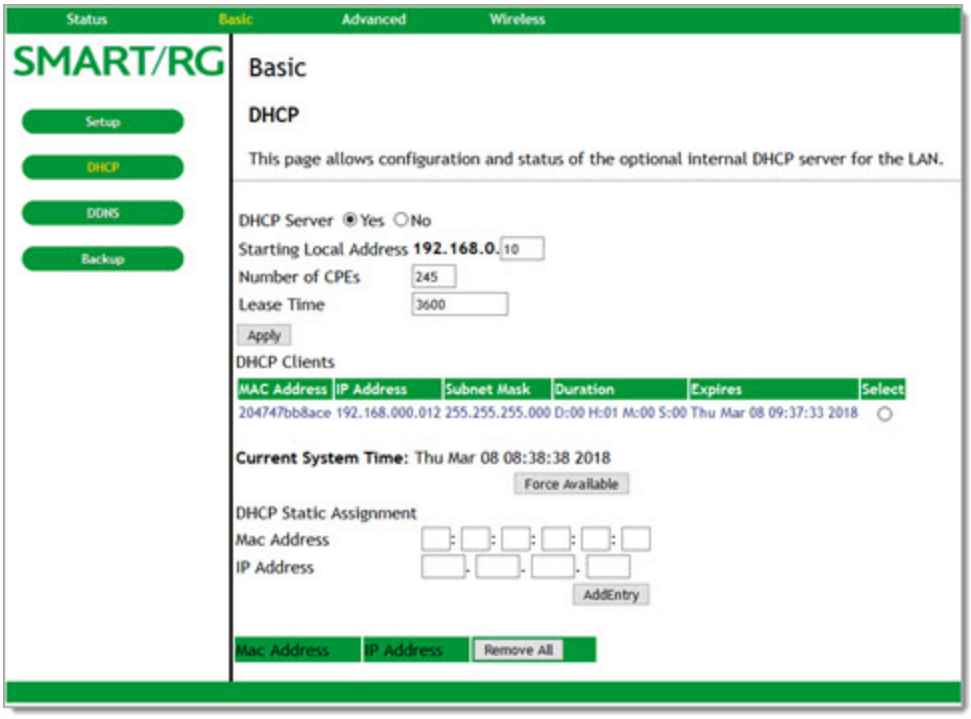
DHCP

On this page, you can view status and configure the optional internal DHCP server for the LAN.

If you have your own DHCP server servicing the LAN side (or choose to "hardcode" all of your PC's IP addresses), you can disable the internal DHCP server, following the instructions below.

You can also set the starting IP address for IP leases available to the LAN, and change the number of PCs supported on the LAN. In this case, you can use addresses 192.168.0.2 through 192.168.0.9 as hard-coded IP addresses without concerns about IP address conflict with the DHCP pool. Configured WINS server addresses can also be passed to CPEs behind the gateway via DHCP.

1. In the top navigation bar, click **Basic** and then click **DHCP** in the left menu. The Basic > DHCP page appears. The **DHCP Server** feature is enabled by default.



2. (*Optional*) Modify the entries in the **Starting Local Address**, **Number of CPEs**, and **Lease Time** fields. Then click **Apply**.
3. To use a specific DHCP client, click **Select** to the right of the entry.
4. To add static DHCP clients that will be allowed to connect to the LAN, in the **DHCP Static Assignment** section:
    a. Enter either the **MAC Address** or **IP Address**. Make sure that the static IP address you enter is on the same subnet as the LAN IP address of the gateway or you won't be able to access the gateway from the LAN. You can find the IP address of the gateway on the Basic > Setup page.
    a. Click **AddEntry**. The address is added to the table at the bottom of the page.
5. To remove an entry, select it and click **Remove**. To clear the list, click **Remove All**.
6. To disable the internal DHCP server:
    a. Make sure the IP address assigned to the gateway is on the same subnet as the external DHCP server (the subnet mask is always 255.255.255.0), or you won't be able to access the gateway from the LAN. You can find the IP address of the gateway on the Basic > Setup page.
    b. Select **No** next to **DHCP Server**.
7. Click **Apply** (located beneath the **Lease Time** field).

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

Field	Description
DHCP Server	Select whether to enable the internal DHCP server. Options are **Yes** and **No**. The default is **Yes**.
Starting Local Address	Enter the last three digits of the local IP address.
Number of CPEs	Enter the maximum number of CPEs permitted on this server. The default is **245**.
Lease Time	Enter the maximum number of minutes for a leased session. The default is **3600** or 6 hours.

Field	Description
DHCP Clients	The list of connected DHCP clients.
Current System Time	The current system date and time.
Force Available	To force the current IP address to always be assigned to the select DHCP client, click this option.

DDNS

On this page, you can to configure Dynamic DNS (DDNS). DDNS allows you to alias a dynamic IP address to a static, pre-defined host name so that the host can be easily contacted by other hosts on the Internet even if its IP address changes. The DDNS client notifies the DDNS service whenever the WAN IP address changes so that the chosen host name can be resolved properly by inquiring hosts.

The SR808ac gateway supports a dynamic DNS client compatible with the Dynamic DNS service.

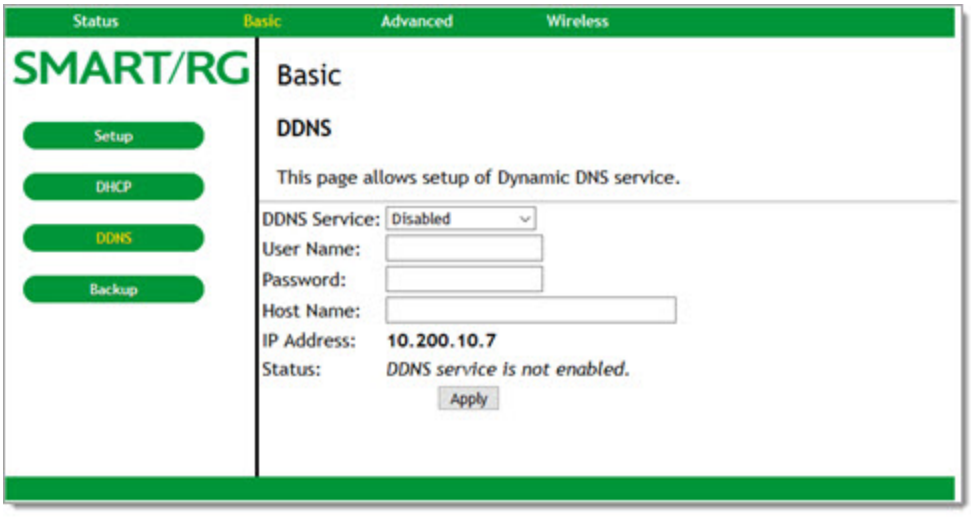
Prerequisite

If you do not already have an account for your DDNS, go to www.DynDNS.org and create an account. You will asked to:

- Create a username and password.
- Select a host name for your server.
- Enter the dynamic DNS domain to which your host will be assigned.
- Enter your host's current IP address. This is the WAN IP address that was assigned to your SR808ac gateway during provisioning and is displayed on the Basic > Setup page.)

To configure DDNS for your gateway, proceed as described below.

1. In the top navigation bar, click **Basic** and then click **DDNS** in the left menu. The Basic > DDNS page appears. The current status of the service is shown at the bottom of the DDNS page.



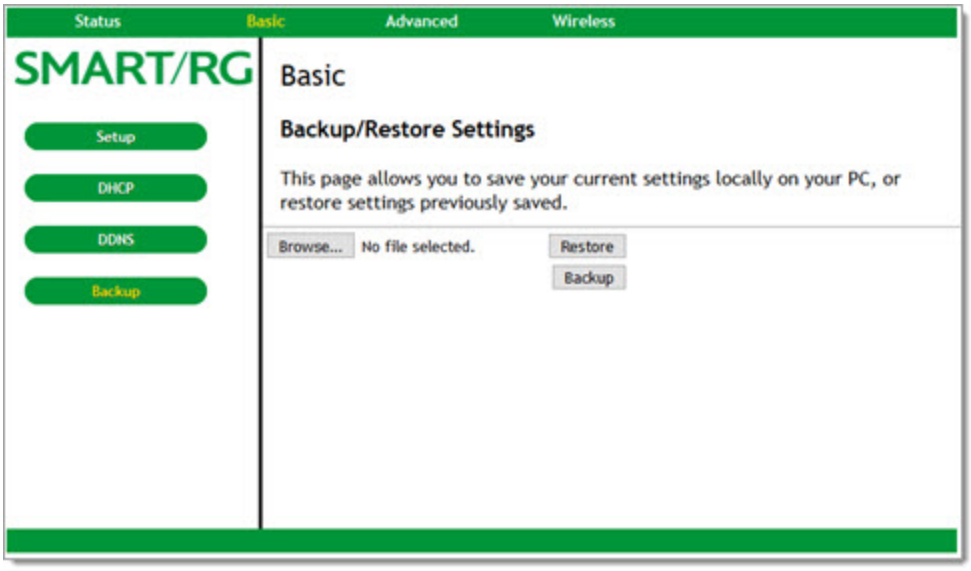
2. In the **DDNS Service** field, select **www.DynDNS.org**.

3. Enter your DynDNS account information.
4. Click **Apply** to save your changes. The **Status** statement is updated.

Backup

On this page, you can save the current configuration settings to a local PC. You can later restore these settings if you need to return to a particular configuration or to recover from changes you made that had an undesirable effect.

1. In the top navigation bar, click **Basic** and then click **Backup** in the left menu. The Basic > Backup/Restore Settings page appears.



2. To restore a previous configuration:
   a. Click **Browse** to select the file that you want to restore. By default, this is GatewaySettings.bin, but you can select any saved configuration file.
   b. Click **Restore** to restore the settings. Once the settings are restored, the device reboots. When reboot is completed, the Status > Connection page appears.
3. To back up the current configuration, click **Backup** and follow the prompts.

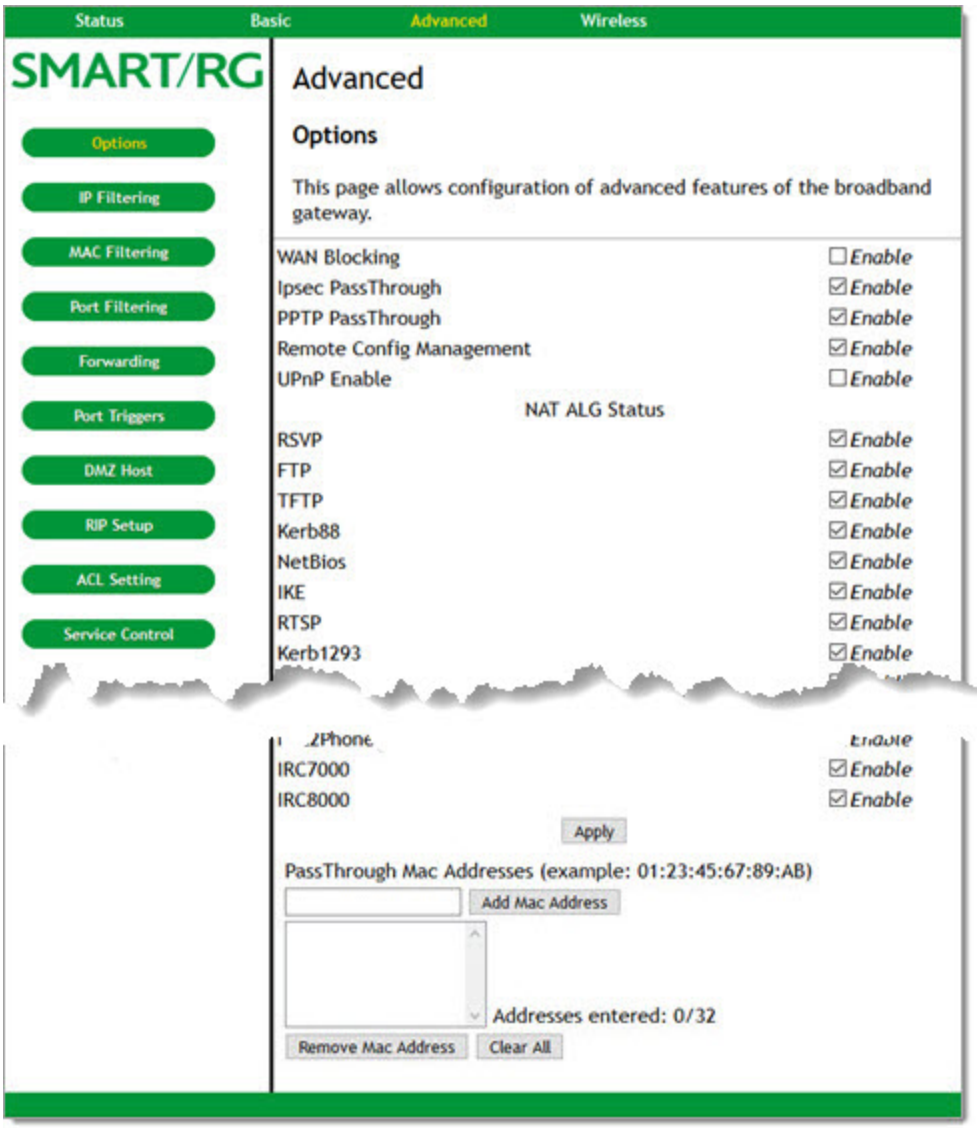
Advanced

In this section, you can configure IP and MAC filtering, port filtering and triggers, forwarding, and RIP settings.

Options

On this page, you can configure features are accessible to end users. A system reset is not needed.

1. In the top navigation bar, click **Advanced**. The Advanced > Options page appears.



2. To *enable* a feature, click the **Enable** check box next to it.
3. To *disable* a feature, clear the **Enable** check box next to it. For detailed descriptions of some of the available features, see the table provided below.
4. To add pass-through MAC addresses:
    a. In the **PassThrough Mac Addresses** field, enter the first MAC address.
    b. Click **Add Mac Address**. The list below the field is refreshed.
    c. Repeat these steps to enter additional MAC addresses. You can enter up to 32 addresses.
5. To remove a pass-through MAC address:
    a. In the **PassThrough Mac Addresses** list, select the MAC address that you want to remove.
    b. Click **Remove Mac Address**. The list refreshes.
6. To remove all addresses in the list, click **Clear All**. All entries are removed.
7. When you are satisfied with your selections, click **Apply** (located above the **PassThrough Mac Addresses** field).

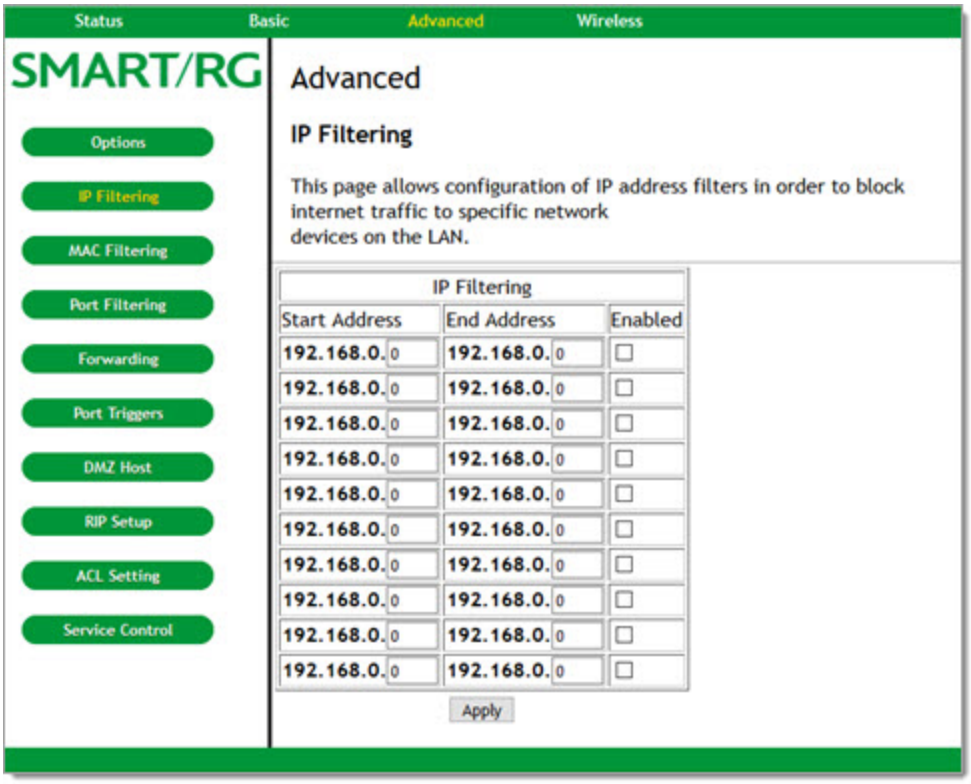
The following table describes some of the options on this page.

Field	Description
WAN Blocking	Prevents the gateway or the PCs behind it from being visible to the WAN. For instance, pings to the gateway's WAN IP address or the PCs behind it are not returned. This feature makes it more difficult for hackers to discover your WAN IP address and begin an attack on your private LAN.
IPSec and PPTP PassThrough	Enables the IPSec and PPTP (Point-to-Point) protocols to be used through the gateway allowing a VPN device (or software) to communicate properly with the WAN.
Remote Configuration Management	Allows the gateway to be administered (configured) from the WAN via surfing to the WAN IP address on port 8080 of the gateway from anywhere on the Internet (e.g.,in the browser URL window, enter http://<*WanIPAddress*>:8080/ to access the gateway remotely).
UPnP Enable	Enables the UPnP agent in the gateway. If you are running a CPE application that requires UPnP, click this box.

IP Filtering

On this page, you can configure the gateway to prevent local PCs from getting access to the WAN.

1. In the top navigation bar, click **Advanced** and then click **IP Filtering** in the left menu. The Advanced > IP Filtering page appears.



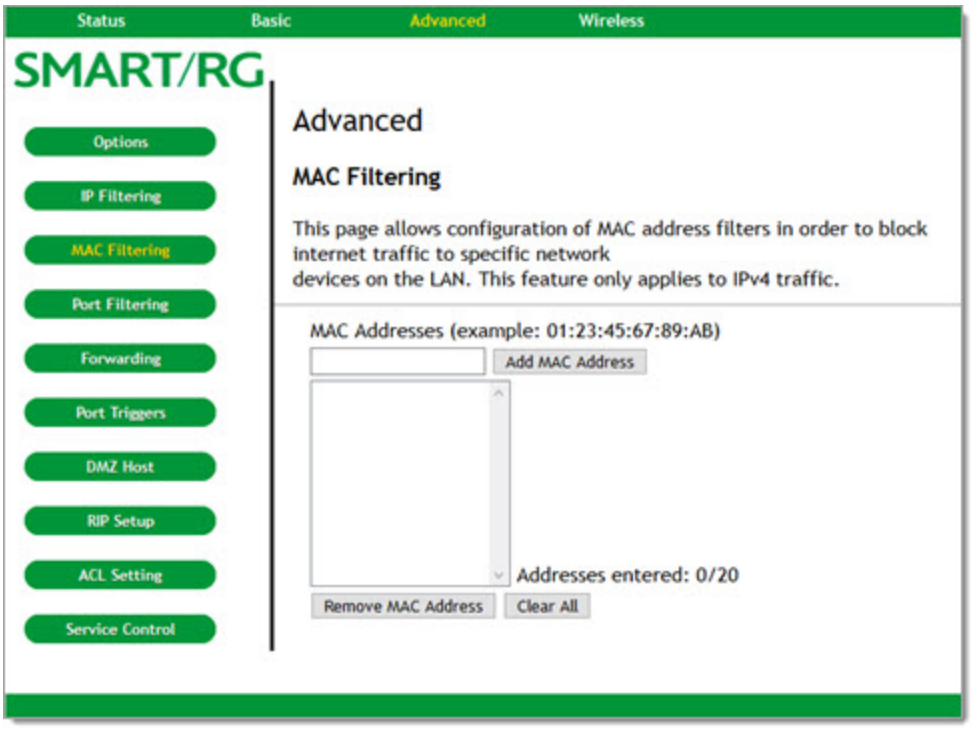
2. Enter starting and ending IP address ranges to specify which local PCs are denied access to the WAN.

   You need only enter the last 3 digits of the IP address; the other bytes of the IP address are set automatically from the gateway's IP address. Your selections are stored when you click **Apply**. This allows you to define commonly used ranges but not have them active until needed.
3. Next to each address range that you want blocked, click the **Enabled** check box.
4. Click **Apply** to save your changes.

MAC Filtering

On this page, you can prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC address. This is useful because the MAC address of a specific NIC never changes, unlike its IP address which can be assigned via DHCP server or hard-coded to various addresses over time.

1. In the top navigation bar, click **Advanced** and then click **MAC Filtering** in the left menu. The Advanced > MAC Filtering page appears.

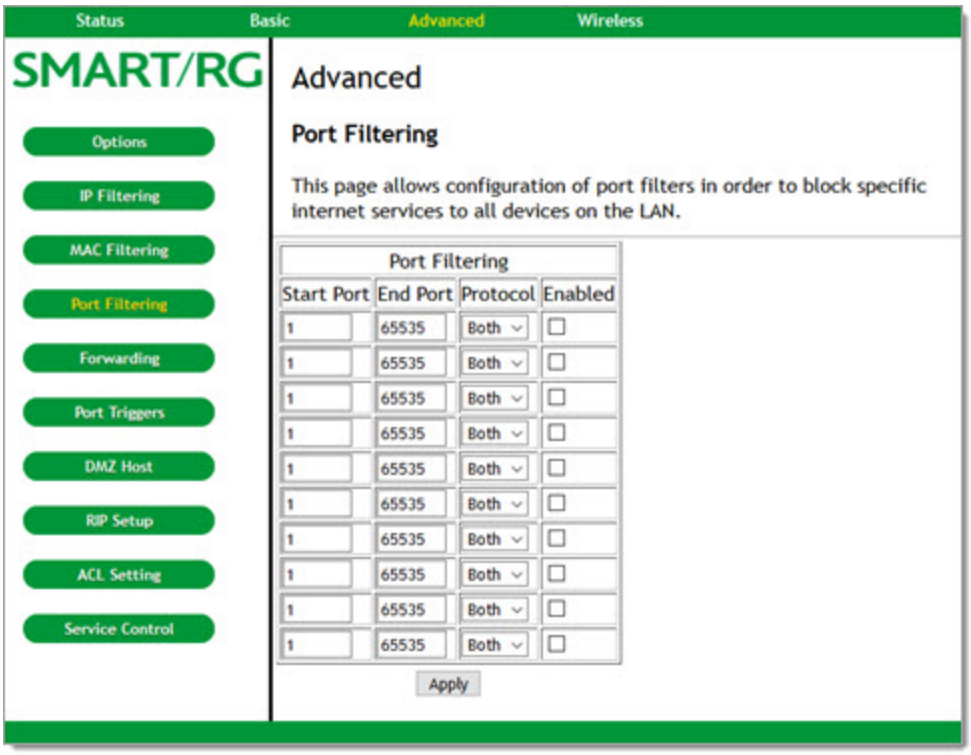


2. To add a MAC address:
   a. Enter the MAC address in the text field.
   b. Click **Add MAC Address**. The list refreshes.
   c. To add more MAC addresses, repeat these steps. You can enter up to 20 MAC addresses.
3. To remove a MAC address:
   a. Select the address in the list
   b. Click **Remove MAC Address**. The list refreshes.
4. To clear all addresses in the list, click **Clear All**. The list is cleared.

Port Filtering

On this page, you can prevent PCs from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. For instance, if you want to block all PCs on the private LAN from accessing HTTP sites (or "web surfing"), set the **Start Port** to **80**, the **End Port** to **80**, the **Protocol** to **TCP**.

1. In the top navigation bar, click **Advanced** and then click **Port Filtering** in the left menu. The Advanced > Port Filtering page appears.



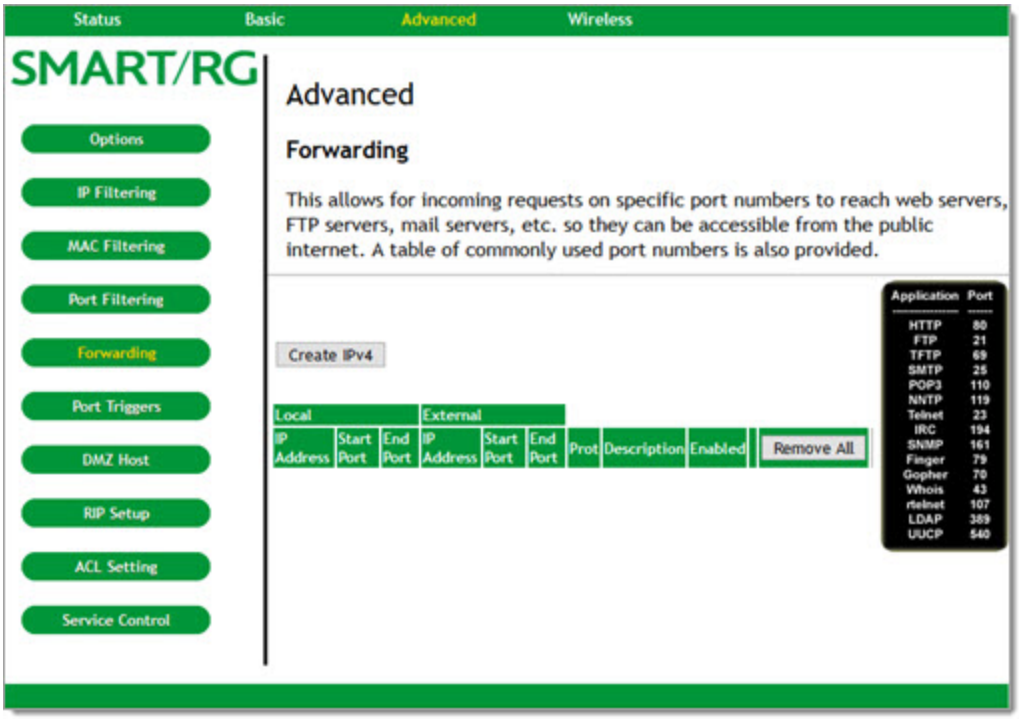
2. Enter a starting and ending port range for the services that you want to filter. The specified port ranges are blocked for all PCs; this setting is not IP address or MAC address specific.
3. In the **Protocol** field, select the type of traffic. Options are **TCP**, **UDP**, and **Both**. The default is **Both**.
4. To enable a filter, click the **Enabled** check box to next to it.
5. Click **Apply** to save your changes.

Forwarding

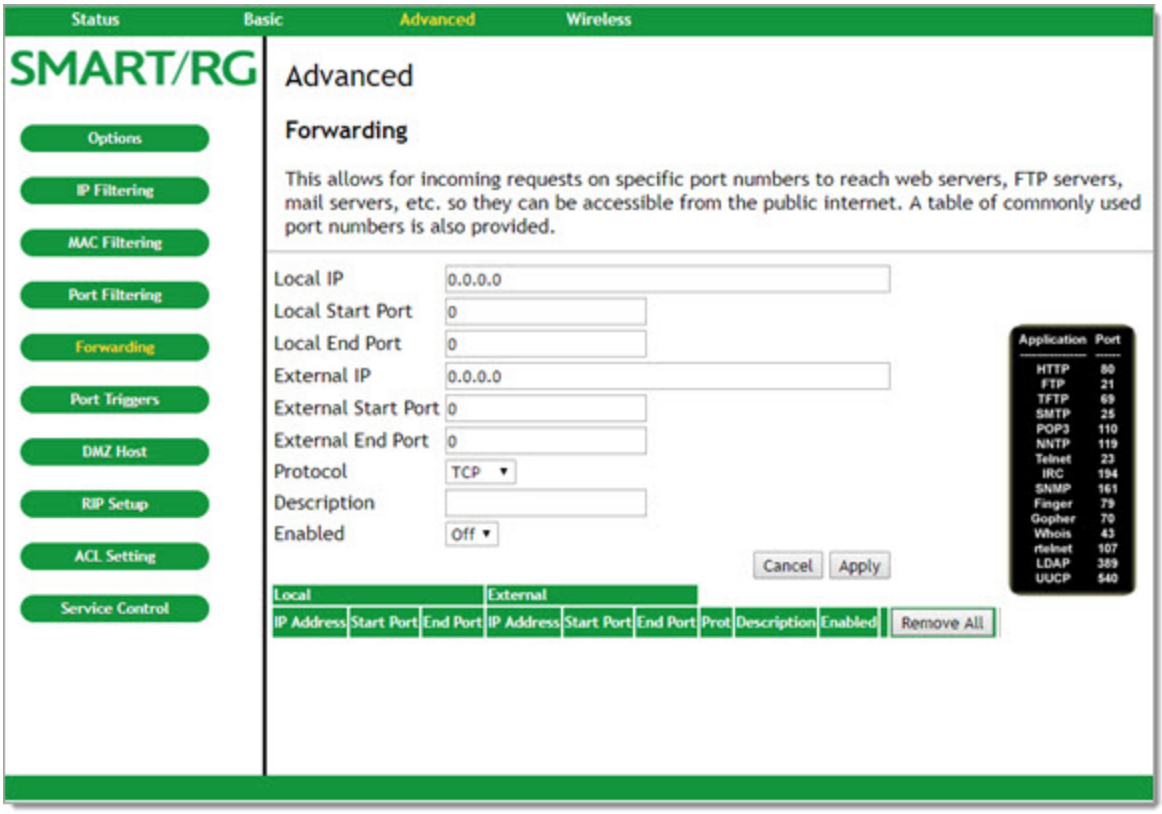
On this page, you can configure forwarding settings to allow incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc., so they are accessible from the public Internet. Forwarding allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC.

A table of commonly used port numbers displays on the page.

1. In the top navigation bar, click **Advanced** and then click **Forwarding** in the left menu. The Advanced > Forwarding page appears.



2. To specify a mapping, click **Create IPv4**. Additional fields appear.



3. Complete the fields, using the information provided in the table below. A table of commonly used Port numbers is supplied on the page for convenience.
4. Click **Apply**. The table refreshes.
5. To edit a forwarding configuration:
   a. Click the **Edit** button next to it.
   b. Change the entries.
   c. Click **Apply**.
6. To remove a forwarding configuration, click the **Remove** button next to it. The table refreshes.
7. To remove all forwarding configurations, click **Remove All**. All addresses are removed.
8. Click **Apply** to save your changes.

Field	Description
Local IP	Enter the local IP address to which you want certain ports to be forwarded.
Local Start Port Local End Port	Enter the range of port numbers that should be forwarded locally. If you want to forward a single port, enter the same port number in the **Start** and **End Port** fields. If you enter external port numbers, both fields are required.

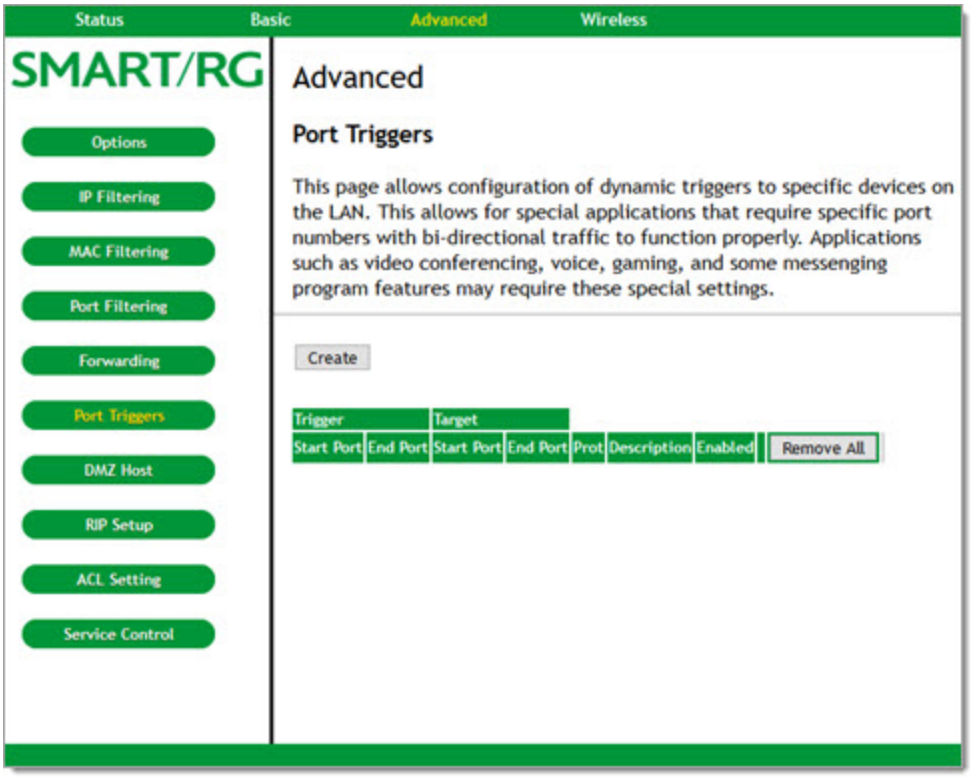
Field	Description
External IP	Enter the external IP address to which you want certain ports to be forwarded.
External Start Port External End Port	Enter the range of external port numbers that should be forwarded. If you want to forward a single port, enter the same port number in the **Start** and **End Port** fields. **Note**: If you enter both external and local/internal port numbers, the local port fields are required and the external port fields are optional. When external port numbers are entered, the gateway translates the external port number to the internal port number.
Protocol	Select the protocol for this configuration. Options are **TCP**, **UDP**, and **Both**. The default is **TCP**.
Description	(*Optional*) Enter a brief description of this forwarding configuration.
Enabled	To *enable* the service, select **On**. To save your settings without enabling forwarding, leave the setting as **Off** and click **Apply**.

Port Triggers

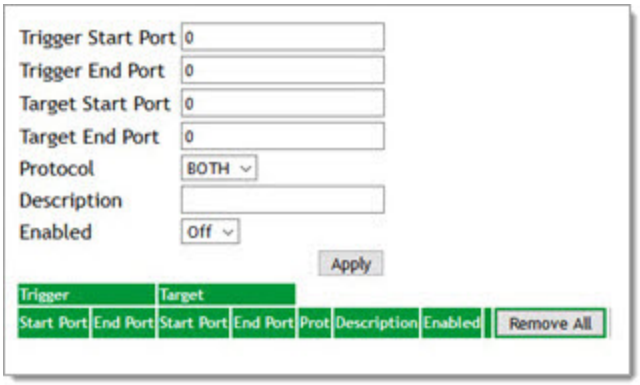
On this page, you can configure port triggers. Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. When the gateway detects outgoing data on an IP port number included in the trigger range, the ports included in the target range are opened for incoming (or bi-directional) data. If no outgoing traffic is detected on the trigger range ports for 10 minutes, the target range ports will close.

This is a safer method for opening specific ports for special applications (e.g., video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the gateway administrator and exposed for potential hackers to discover.

1. In the top navigation bar, click **Advanced** and then click **Port Triggers** in the left menu. The Advanced > Port Triggers page appears.



2. To create a port trigger:
    a. Click **Create**. Additional fields appear.



    b. Complete the fields, using the information provided in the table below.
    c. Click **Apply**. The table refreshes.
3. To edit a trigger:
    a. Click the **Edit** button next to it.
    b. Change the entries.
    c. Click **Apply**.

4. To remove a trigger, click the **Remove** button next to it. The table refreshes.
5. To remove all listed triggers, click **Remove All**. The list is cleared.
6. Click **Apply** to save your changes.

The options on this page are described in the following table.

Field	Description
Trigger Start Port Trigger End Port	Enter the range of port numbers that are available as outgoing trigger ports. Options are **1** - **65535**. If you want to use a single port, enter the same port number in the **Start** and **End Port** fields. If external port numbers are entered, both fields are required.
Target Start Port Target End Port	Enter the range of external port numbers that you want to configure. If you want to use a single port, enter the same port number in the **Start** and **End Port** fields.
Protocol	Select the protocol for this configuration. Options are **TCP**, **UDP**, and **BOTH**. The default is **BOTH**.
Description	(*Optional*) Enter a brief description of this trigger configuration.
Enabled	To enable the service, select **On**. To save your settings without enabling forwarding, you can skip this setting and just click **Apply**.

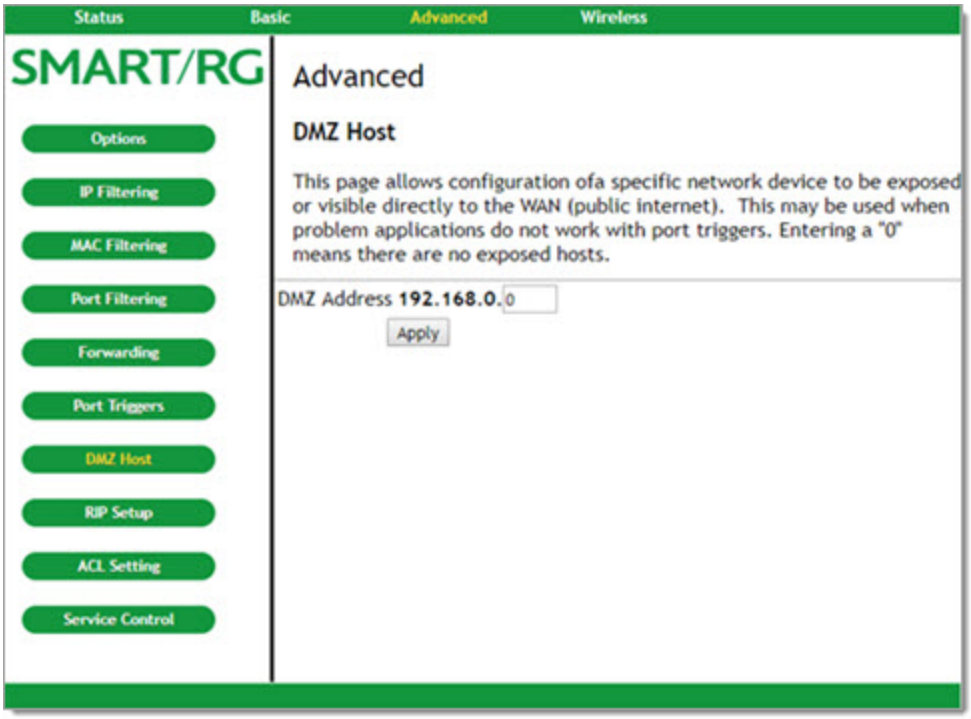
DMZ Host

DMZ (De-Militarized Zone) hosting (also known as "Exposed Host") allows you to specify the "default" recipient of WAN traffic that NAT is unable to translate to a known local PC. This can also be described as a computer or small sub-network that sits between the trusted internal private LAN, and the untrusted public Internet.

You may configure one PC to be the DMZ host. This setting is generally used for PC's running "problem" applications that use random port numbers and do not function correctly with specific port triggers or the port forwarding setups mentioned earlier.

Warning: If you set a specific PC as a DMZ Host, remember to set this back to "0" when finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

1. In the top navigation bar, click **Advanced** and then click **DMZ Host** in the left menu. The Advanced > DMZ Host page appears.



2. In the text field, enter the last three digits of the DMZ address that you want to expose.
3. Click **Apply**.

RIP Setup

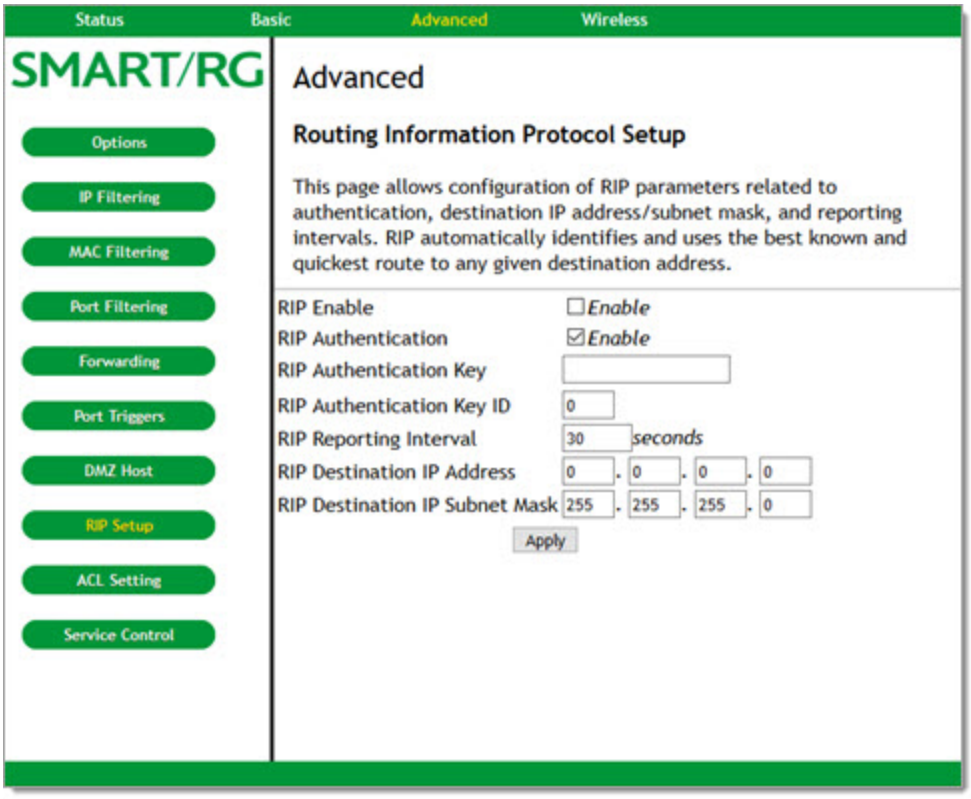
Warning: Your ISP must configure this information for proper operation. Do *not* alter these settings without first contacting your ISP.

RIP (Router Information Protocol) is a protocol that requires negotiation from both sides of the network (i.e., the gateway and the CMTS). The ISP would normally set this up because they understand how to configure these settings on the gateway.

RIP is used in WAN networks to identify and use the best known and quickest route to given destination addresses to help reduce network congestion and delays.

Note: RIP messaging will only be sent upstream when running in Static IP Addressing mode on the Basic – Setup page. You must enable Static IP Addressing and then set the Wan IP network information. Normally, RIP is tightly controlled via the ISP, that is, RIP Authentication Keys and IDs are kept secret to prevent unauthorized RIP settings.

1. In the top navigation bar, click **Advanced** and then click **RIP Setup** in the left menu. The Advanced > Routing Information Protocol Setup page appears.



2. To activate RIP MD5 Authentication, click the **RIP Enable** check box.
3. Modify the other fields as needed, using the information provided in the table below.
4. To enable the CMTS for RIPv2 with MD-5 authentication, follow the instructions in the Cisco ubr example provided in the Configuring RIPv2 for Cisco CMTS section.
5. Click **Apply** to save your changes.

Field	Description
RIP Authentication Key	Enter the RIP authentication key name. This key name must match the CMTS key name value. For this example, type “BRCMV2”.
RIP Authentication Key ID	Enter the key number that matches the CMTS key number value such as “1”.
RIP Reporting Interval	Type the number of seconds for the desired interval. By default, this interval is set to **30 seconds**.
RIP Destination IP Address RIP Destination IP Subnet Mask	To specify a RIP unicast destination IP address, enter the IP address and subnet mask.

Configuring RIPv2 for Cisco CMTS

The following steps explain how to configure RIPv2 for a Cisco CMTS. The network number used in this configuration will vary from network to network, so use the network number that matches your set-up. In this example, the gateway is set up to send

RIPv2 messages to the CMTS and the CMTS is set up to receive these messages. The configuration file looks similar to the following:

```
7223#configure terminal
7223(config)#key chain ubr
7223(config-keychain)#key 1
7223(config-keychain-key)#key-str BRCMV2
7223(config-keychain-key)#exit
7223(config-keychain)#exit
7223(config)#router rip
7223(config-router)#ver 2
7223(config-router)#no validate-update
7223(config-router)#passive-interface cable 2/0
7223(config-router)#network 10.0.0.0
7223(config-router)#exit
7223(config)#inter cable 2/0
7223(config-if)#ip rip receive ver 2
7223(config-if)#ip rip authentication mode md5
7223(config-if)#ip rip authentication key-chain ubr
7223(config-if)#exit
7223(config)#exit
```

In this example, the key chain is named "ubr. You can use any name you like as long as you specify the correct name when specifying which key chain to use for RIPv2 authentication.

The next step is enable RIP debugging to ensure that the CMTS is receiving and authenticating messages from the residential gateway.

```
7223#debug ip rip
RIP protocol debugging is on.
7223#term mon
```

The CMTS is now configured to accept RIPv2 messages. If the gateway is registered on the CMTS, you should see messages similar to the following:

```
00:28:41: RIP: received packet with MD5 authentication
00:28:41: RIP: received v2 update from 10.24.81.148 on Cable2/0
00:28:41: 10.24.81.0/24 via 10.24.81.148 in 1 hops
```

Based on these messages, the gateway has broadcast that it is connected to the network 10.24.81.0/24 through the interface 10.24.81.148. This information is not very useful to the CMTS because it already knows that the network 10.24.81.0/24 is connected directly to one of its interfaces (Cable2/0). It ignores this message and does not add any information to the IP routing table. Below is the IP routing table after the CMTS has received RIPv2 messages:

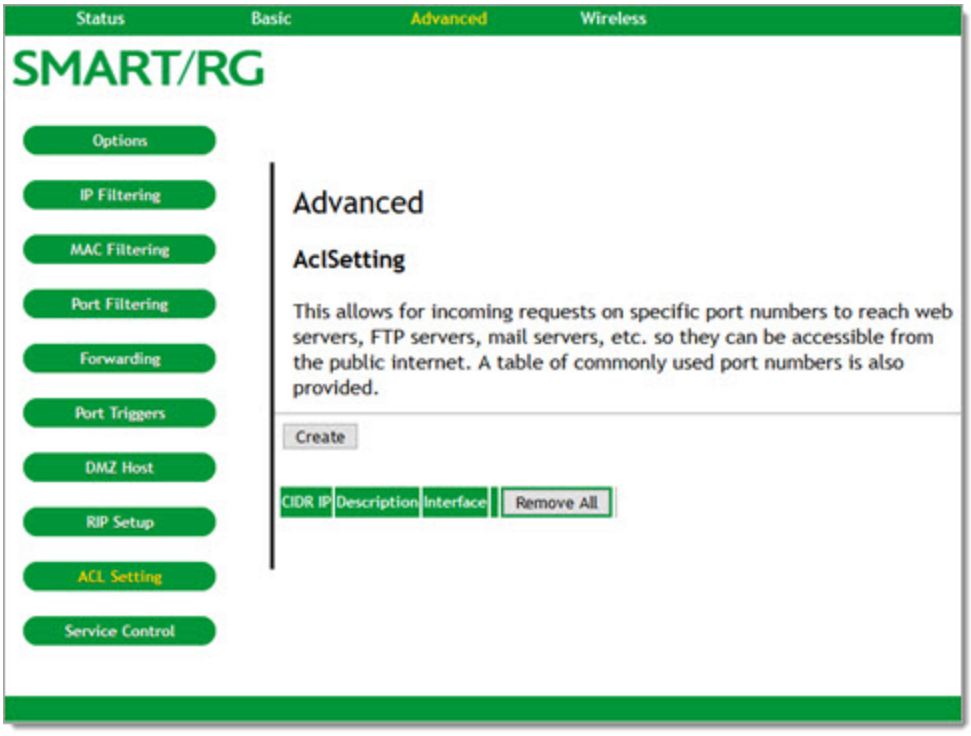
```
7223#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 10.24.95.17 to network 0.0.0.0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.24.80.0/24 is directly connected, Cable2/0
C 10.24.81.0/24 is directly connected, Cable2/0
C 10.24.95.16/28 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 10.24.95.17
```

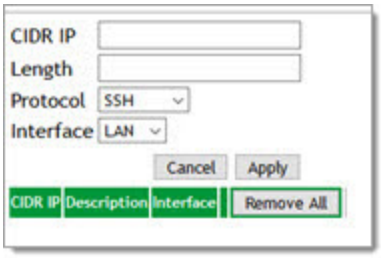
ACL Setting

Classless Inter-Domain Routing (CIDR) is a method used with incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public Internet.

1. In the top navigation bar, click **Advanced** and then click **ACL Setting** in the left menu. The Advanced > AclSetting page appears.



2. To create an access configuration:
    a. Click **Create**. Additional fields appear.

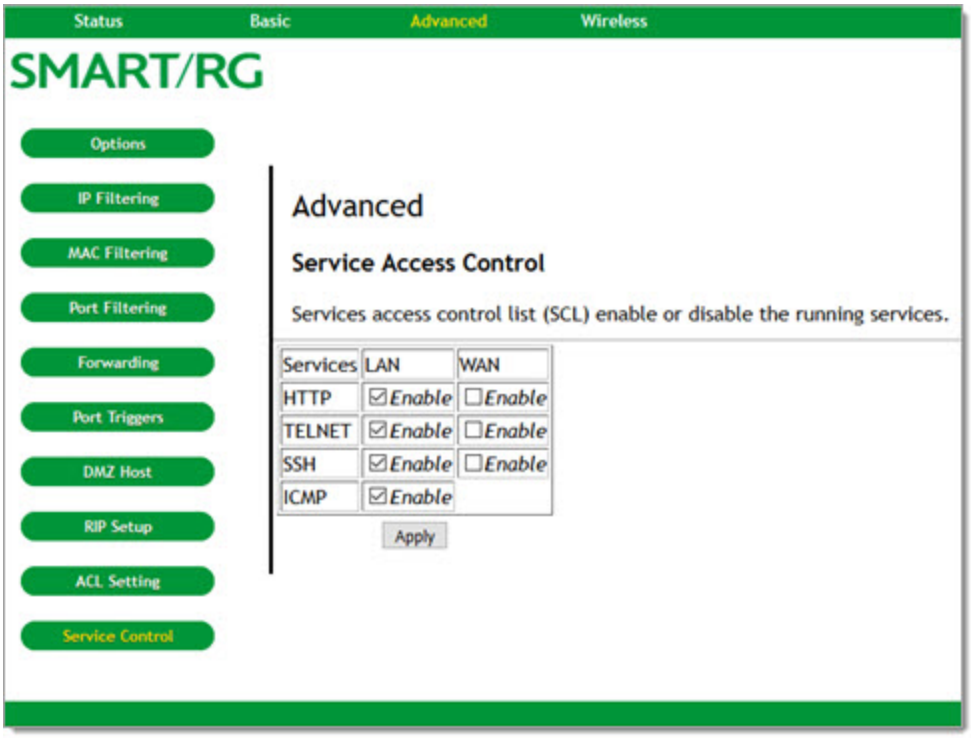


    b. In the **CIDR IP** field, enter the IP address that you want to be accessible.
    c. (*Optional*) In the **Length** field, enter the length of the subnet, e.g., "/24".
    d. In the **Protocol** field, select the protocol. Options are **SSH**, **HTTP**, and **TELNET**. The default is **SSH**.
    e. In the **Interface** field, select **LAN** or **WAN**. The default is **LAN**.
    f. Click **Apply**. The table refreshes.
3. To edit a setting:
    a. Click the **Edit** button next to it.
    b. Change the entries.
    c. Click **Apply**.
4. To remove a setting, click the **Remove** button next to it. The table refreshes.
5. To remove all listed settings, click **Remove All**. The table refreshes.
6. Click **Apply** to save your changes.

Service Control

On this page, you can enable or disable services for your gateway.

1. In the top navigation bar, click **Advanced** and then click **Service Control** in the left menu. The Advanced > Service Access Control page appears.



2. To *enable* a service, click the **Enable** check box in the same row for **LAN**, **WAN**, or both.
3. To *disable* a service, clear the **Enable** check box in the same row for **LAN**, **WAN**, or both.
4. Click **Apply** to save your changes.

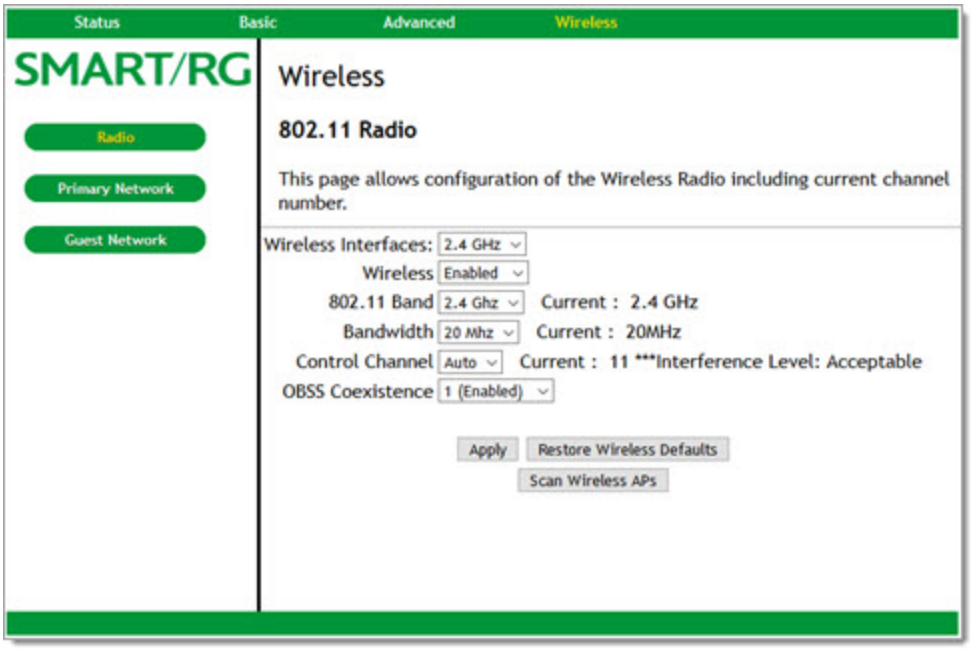
Wireless

In this section. you can configure wireless settings for the primary and guest networks, WMM, access control, bridging, and so on.

Radio

On this page, you can configure the physical parameters of your wireless network. The MAC address for your network displays in the **Wireless Interfaces** field at the top of the page.

1. In the top navigation bar, click **Wireless**. The Wireless > 802.11 Radio page appears.



2. To force the gateway to scan for available wireless access points within range, click **Scan Wireless APs**. A pop-up window appears, showing a list of available networks. Identify the network you want to access and close the window.
3. Modify the settings, using the information provided in the table below.
4. Click **Apply** to save your changes.
5. To back out your changes, click **Restore Wireless Defaults**.

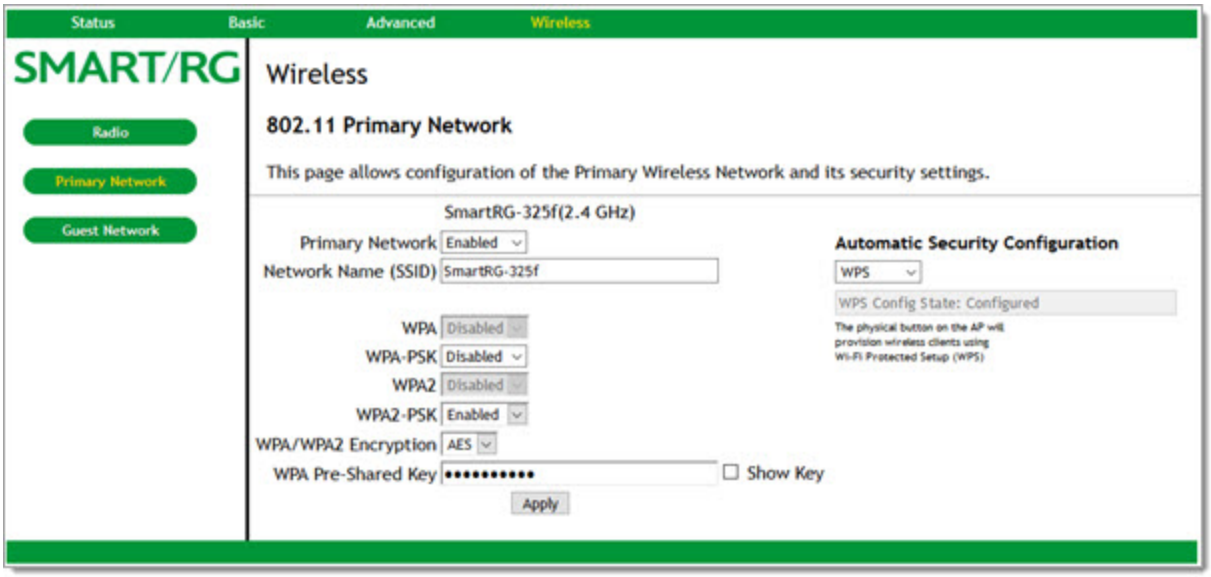
Field	Description
Wireless Interfaces	Select the wireless interface that you want to configure. Options are **2.4 GHz** and **5 GHz**. The 2.4 GHZ interface is shown by default.
Wireless	Select whether to disable the wireless interface. Options are **Enabled** and **Disabled**. The default is **Enabled**.
802.11 Band	This option is set to the band associated with the wireless interface selected above and cannot be changed.

Field	Description
Bandwidth	Select the bandwidth for your wireless network. Options are **20 MHz** and **40 MHz** for the 2.4 GHZ band plus **80 MHz** for the 5.0 GHz band. The default is **20 MHz**. for the 2.4 GHz band and **80 MHz** for the 5 GHz band. 802.11b/g channels are only 20 MHz wide, but 802.11n channels may be 40 MHz wide. There are some backward compatibility issues with 40 MHz channels. These issues are more likely to be encountered in the 2.4 GHz band where legacy (802.11b/g) devices may be operating using 20 MHz channels.
Control Channel / Channel Specification	Select the channel for AP operation. The active channel and interference level are shown to the right of this field. For the 2.4 GHz band, this field is labeled **Control Channel**, options are **Auto** and **1** - **11** and the default is **Auto**. For the 5 GHz band, this field is labeled **Channel Specification**, is set to **N/A** and cannot be changed.
OBSS Coexistence	Select whether to disable Overlapping BSS Coexistence. Options are **0 (Disabled)** and **1 (Enabled)**. The default is **1 (Enabled)**. OBSS coexistence refers to the ability of the AP to support 20 MHz devices within 40 MHz channels. It also allows the AP to better deal with nearby 20 MHz devices that are interfering with part of its 40 MHz channel.

Primary Network

On this page, you can configure the primary wireless network.

1. In the top navigation bar, click **Wireless** and then click **Primary Network** in the left menu. The Wireless > 802.11 Primary Network page appears.



2. Fill in the fields using the information provided in the table below. The network selected on the Wireless > Radio page is shown above the **Primary Network** field.
3. Click **Apply** to save your changes.

Field	Description
Primary Network	Select whether to *disable* the primary network. Guest networks may still be operational when the primary network is disabled. Options are **Enabled** and **Disabled**. The default is **Enabled**.
Network Name (SSID)	(*Optional*) Enter the network name (also known as SSID) of the primary network. This can be 1-32 characters. The current network name is shown by default.
WPA	This option is **Disabled** by default and cannot be changed.
WPA-PSK	Select whether to enable WPA-PSK authentication. This is also known as WPA Personal. Options are **Disabled** and **Enabled**. The default is **Disabled**.
WPA2	This option is **Disabled** by default and cannot be changed.
WPA2-PSK	Select whether to *disable* WPA2-PSK (or WPA2 Personal) authentication. Options are **Disabled** and **Enabled**. The default is **Enabled**. **Note:** You can use WPA2-PSK and WPA-PSK at the same time to provide backward compatibility with devices that do not support WPA2.
WPA/WPA2 Encryption	Select the type of encryption. If you enable **WPA-PSK** authentication, the **TKIP + AES** option becomes available. Otherwise, only the **AES** option is available. The **TKIP + AES** mode allows both TKIP and AES-capable clients to connect.
WPA Pre-Shared Key	(*Available when **WPA-PSK** or **WPA2-PSK** is enabled*) Enter the WPA Pre-Shared Key (PSK). This is an 8-63 ASCII character string, or a 64-digit hex number. To display the characters entered in the field, click **Show Key** to the right of the field.

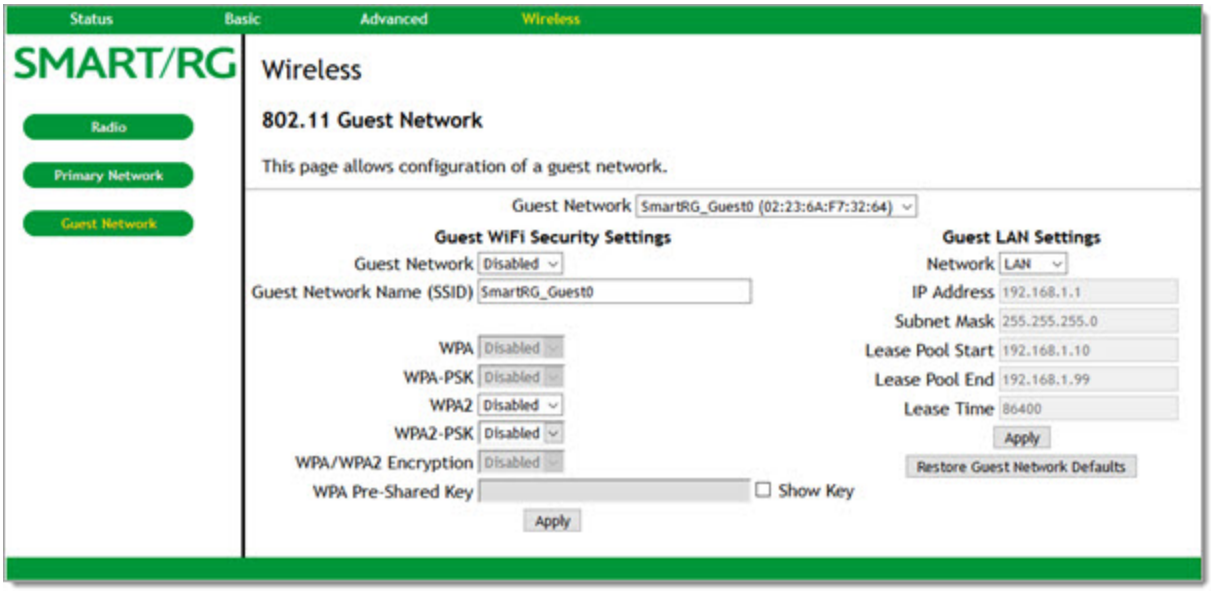
Field	Description
Automatic Security Configuration	Select whether to use Wi-Fi Protected Setup (WPS) for the primary network. Options are **WPS** (enabled) and **Disabled**. The default is **WPS**.

Guest Network

On this page, you can configure a secondary guest network on the wireless interface. This network is isolated from the LAN. Any clients that associate with the guest network SSID will be isolated from the private LAN and can only communicate with WAN hosts.

Note: Most of the parameters on the Guest Network page are identical to those on the Primary Network page (described above). Parameters that are unique to the Guest Network page are explained below. There is no Automatic Security Configuration section on the 802.11 Guest Network page.

1. In the top navigation bar, click **Wireless** and then click **Guest Network** in the left menu. The Wireless > 802.11 Guest Network page appears.



2. Select options using the information provided in the table below.
3. To restore the defaults, click **Restore Guest Network Defaults**.
4. Click **Apply** to save your changes.

Field	Description
Guest Network	Select the guest network that you want to configure from a list of guest networks already defined for this system.

Field	Description
Guest WiFi Security Settings section	
Guest Network	Select whether to enable the selected guest network. Options are **Disabled** and **Enabled**. The default is **Disabled**.
Guest Network Name	(*Optional*) Enter a name for the guest network.
WPA	This option is **Disabled** by default and cannot be changed.
WPA-PSK	This option is **Disabled** by default and cannot be changed.
WPA2	Select whether to *enable* WPA2 encryption. Options are **Disabled** and **Enabled**. The default is **Disabled**. **Note**: When **WPA2** is enabled, WPA becomes active, **WPA2-PSK** is disabled, and the **WPA/WPA2 Encryption** field becomes active.
WPA2-PSK	Select whether to *enable* WPA2-PSK (i.e., WPA2 Personal) authentication. Options are **Disabled** and **Enabled**. The default is **Disabled**. **Note:** You can use WPA2-PSK and WPA-PSK at the same time to provide backward compatibility with devices that do not support WPA2.
WPA/WPA2 Encryption	(*Available when **WPA2** is enabled*) This option is **Disabled** by default. When WPA2 is enabled, this field is set to **AES** and cannot be changed.
WPA Pre-Shared Key	(*Available when **WPA-PSK** or **WPA2-PSK** is enabled*) Enter the WPA Pre-Shared Key (PSK). This is an 8 - 63 ASCII character string, or a 64-digit hex number. To display the characters entered in the field, click **Show Key** to the right of the field.
Guest LAN Settings section	
Network	Select the network type. Options are **LAN** and **Guest**. The default is **LAN**.
IP Address	The gateway IP relayed to guest clients in DHCP lease offers.
Subnet Mask	The subnet mask for the guest network.
Lease Pool Start	The starting IP address for the guest network lease pool.
Lease Pool End	The ending IP address for the guess network lease pool.
Lease Time	The lease time for the guest network lease pool, once the gateway completes WAN.

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 numrique de la classe B est conforme Ã la norme NMB-003 du Canada.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

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

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

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

FCC - PART 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom case of this equipment is a label that contains, among other information, a product identifier in the format US: VW7DL01BSR555A.

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

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

Ringer Equivalency Number Statement

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

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

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

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

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

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

IC CS-03 statement

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

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

Canada Statement

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

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

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

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

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

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

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

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

Revision History

Revision	Date	Description
1.1	April 2018	Clarified LED Indicator descriptions.
1.0	March 2018	Initial release of this document.