Smart rg

Powering the Connected Home

SmartRG™ Residential Gateways

November 15th, 2012 Version 2.4

Table of Contents

List of Figures

Introduction

This document describes the features, functions and administration of SmartRG™ residential gateways.

Who Should Read This User’s Manual

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.

Additional Information

You may find the following documents to be helpful during your access network deployment:

- SmartRG Data Sheets
- SmartRG Product Release Notes
- Deployment and Provisioning Presentation

Contacting SmartRG Inc.

Contact SmartRG Inc. for further assistance.
Hours of operation: Monday – Friday, 5am-6pm Pacific Time (UTC-8:00)

Support

1-360-859-1780

1-877-486-6210 (Toll free from the US & Canada)
support@smartrg.com

Sales

1-360-859-1780

1-877-486-6210 (Toll free from the US & Canada)
sales@smartrg.com

SmartRG™ Residential Gateways

Advanced Features

Connect-and-Surf (Automatic Broadband Connection Configuration)

The *Connect-and-Surf* feature automatically establishes a WAN connection for default configured gateways obviating the need for manual or custom configurations. The active physical layer is detected (ADSL, VDSL or GigE) and layer 3 connectivity is established using PPP authentication or DHCP.

NOTE	If you prefer to configure your SmartRG's WAN interface manually, connect a laptop to any of the LAN ports and follow the instructions in the **"Logging in to Your SmartRG™ Gateway"** and **"Use Case: Creating WAN Connections for Internet Access and Remote Management"** sections. Do NOT connect the WAN interface cable until **after** the configuration is completed.

Activation (Automatic ACS Connection Configuration)

SmartRG gateways are designed to discover their service provider specific ACS management settings without the use of custom firmware. SmartRG Inc. maintains an *activation server* that associates a device's MAC address with its service provider's ACS settings. SmartRG gateways contact the activation server to have their ACS settings modified upon initial power up (or after being reset to factory default settings).

NOTE	Activation server support is provided for ALL SmartRG gateways at no additional cost. SmartRG Inc. enters gateway MAC addresses into the activation server prior to shipment.

TR-069 Remote Management – Automated Configuration Server Support

With a rich TR-069 heritage and a strong commitment to standards based, remote management, SmartRG gateways are designed for maximum interoperability with industry leading, TR-069 based remote management systems. SmartRG gateways provide maximum remote manageability and the highest level of visibility into the connected home yielding:

- shorter integration times
- lower system integration costs
- improved customer support –and-
- reduced operational expenses

SmartRG works closely with industry-leading, TR-069 automated configuration server (ACS) solutions providers to ensure "plug-n-play" interoperability.

Affinegy ACS

SmartRG gateways have been tested to confirm maximum interoperability with the Affinegy ACS solution.

Calix Compass/Consumer Connect ACS

In addition to being Calix physical layer certified (to ensure Calix access equipment compatibility), SmartRG gateways have been tested to confirm maximum interoperability with the Calix Compass/Consumer Connect ACS solution.

Calix
CERTIFIED
COMPATIBLE

Cisco Prime Home™ ACS

SmartRG gateways have a long history of Prime Home™ (formerly ClearVision) ACS interoperability.

SmartRG™ Product Family

SmartRG residential gateways combine WAN connectivity with a firewall protected router and industry leading TR-069 remote management support. Most variants provide 802.11n, Wi-Fi connectivity, as well. See the SmartRG feature details below:

	SR10	SR100	SR350N	SR350NE	SR500N	SR500NE	SR505N
Models							
Broadband Connection	ADSL2+	ADSL2+	ADSL2+	Ethernet	Tri-mode: ADSL2+, VDSL2, GigE	Tri-mode: ADSL2+, VDSL2, GigE	ADSL2+, VDSL2
10/100 Mbps LAN Ports	1	4	4	3	5	4	4
LAN Device Discovery	✓	✓	✓	✓	✓	✓	✓
Managed Firewall	✓	✓	✓	✓	✓	✓	✓
Managed WiFi			802.11n	802.11n	802.11n	802.11n	802.11n
WiFi Signal Monitor			✓	✓	✓	✓	✓
IPv6			✓	✓	✓	✓	✓
IPTV Ready			✓	✓	✓	✓	✓

Contact SmartRG Support for detailed descriptions and management of the features listed above.

Front Panel LEDs

The SmartRG's front panel LEDs can be useful for troubleshooting and diagnostic purposes:

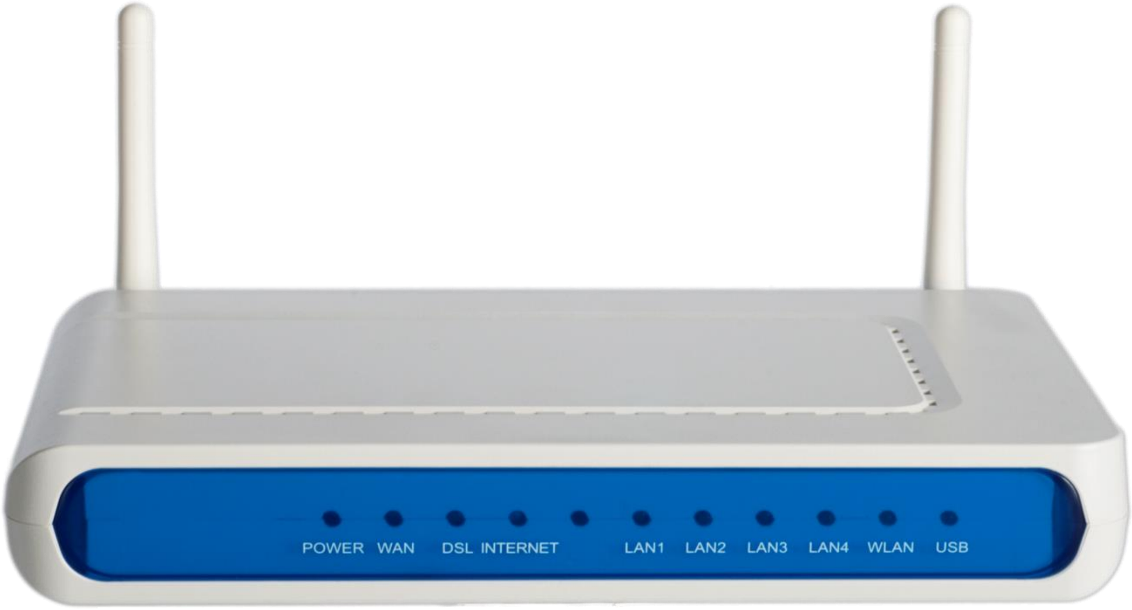


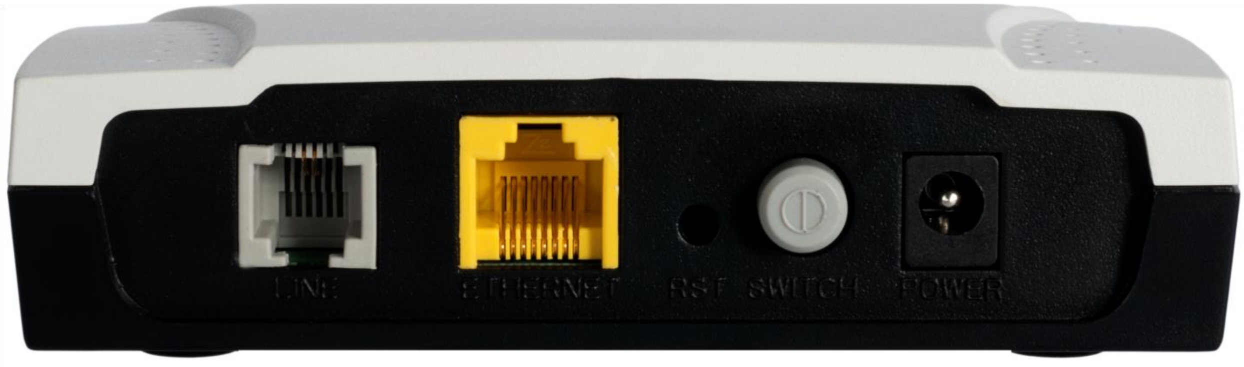
Figure 1 SmartRG Front Panel LEDs

The SmartRG front panel LEDs are defined as follows:

Power	**ON**: Power is on **OFF**: Power is off
WAN (SR500N/NE)	**ON:** Ethernet WAN Active **OFF:** No link
DSL	**ON**: Link established and active **OFF**: No link **Blinking**: Training mode
Internet	**ON**: Internet connection established **OFF**: No Internet connection **Blinking**: Data transfer on WAN Internet connection **RED**: PPP authentication failure
LAN 1-4	**ON**: LAN link established and active **OFF**: No LAN link **BLINKING**: Data transfer on LAN port
WLAN	**ON**: WLAN enabled **OFF**: WLAN disabled **Blinking**: data transfer currently occurring over the WiFi interface

Rear Panel Connectors

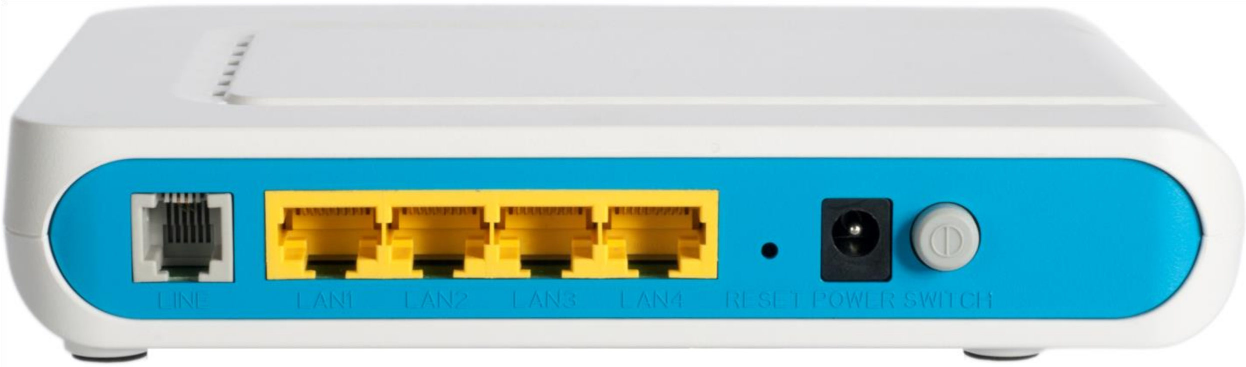
SR10



DSL(WAN) LAN Reset On/Off Power

Figure 2 SR10 Rear Panel Connectors

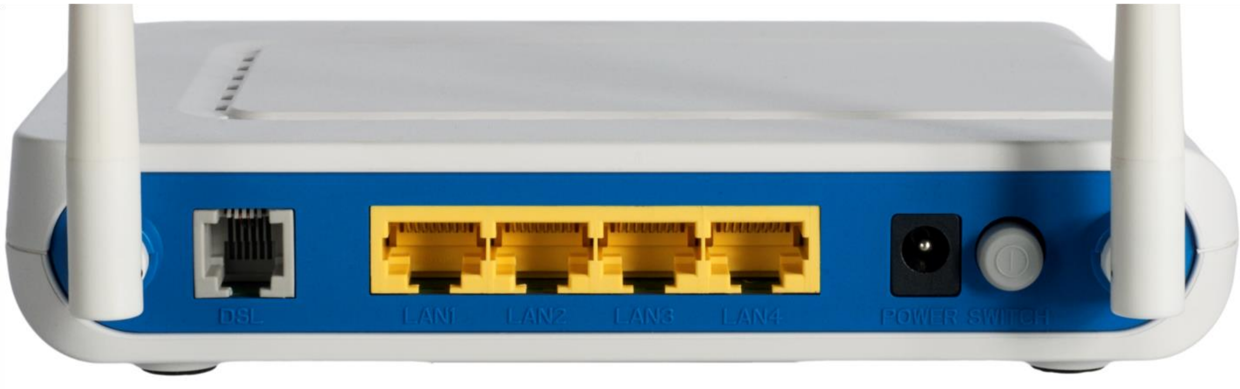
SR100



DSL(WAN) LAN1 - 4 Reset Power On/Off

Figure 3 SR100 Rear Panel Connectors

SR350N

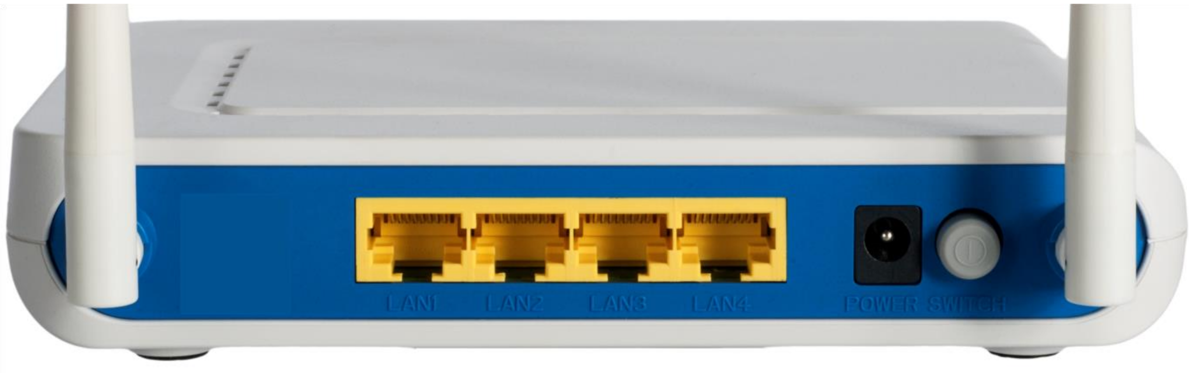


DSL(WAN) LAN1 - 4 Power On/Off

(Reset on bottom)

Figure 4 SR350N Rear Panel Connectors

SR350NE

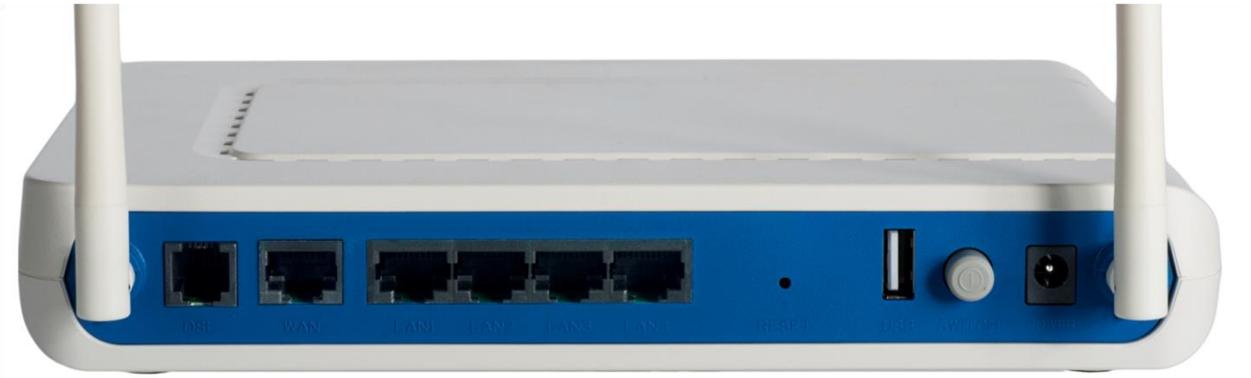


Ethernet(WAN) LAN1 - 3 Power On/Off

(Reset on bottom)

Figure 5 SR350NE Rear Panel Connectors

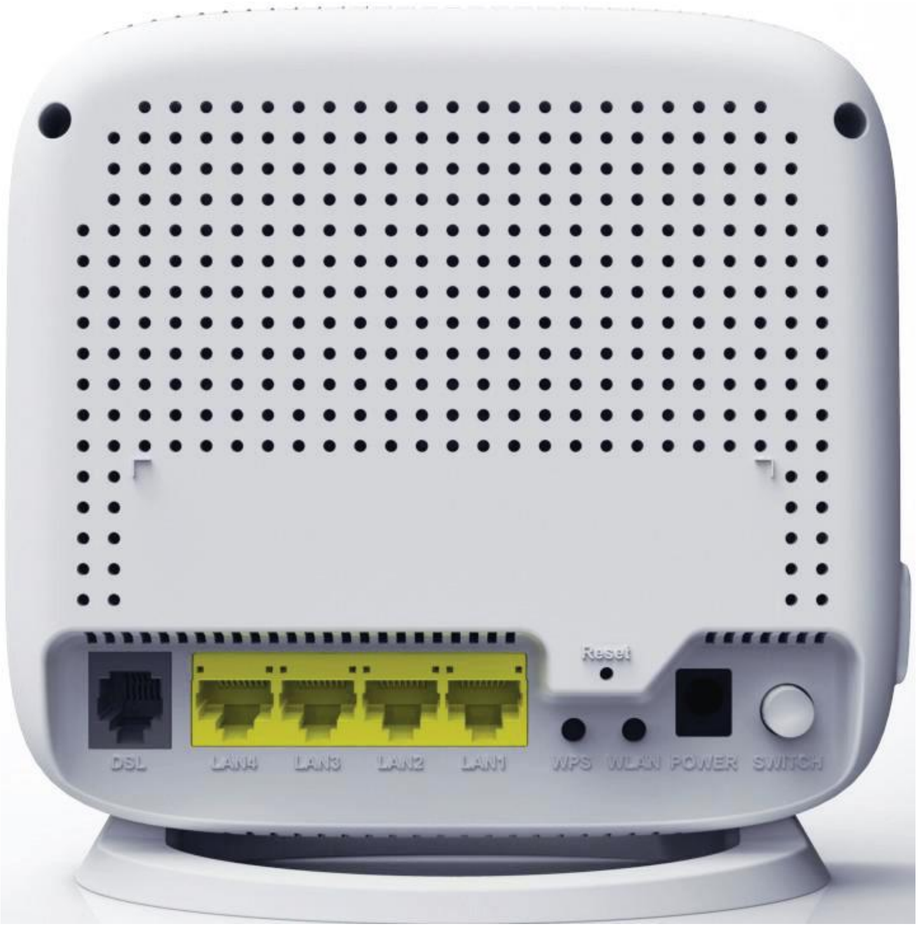
SR500N/SR500NE



DSL(WAN) GigE(WAN) LAN1 - 4 Reset USB On/Off Power

Figure 6 SR500N/NE Rear Panel Connectors

SR505N



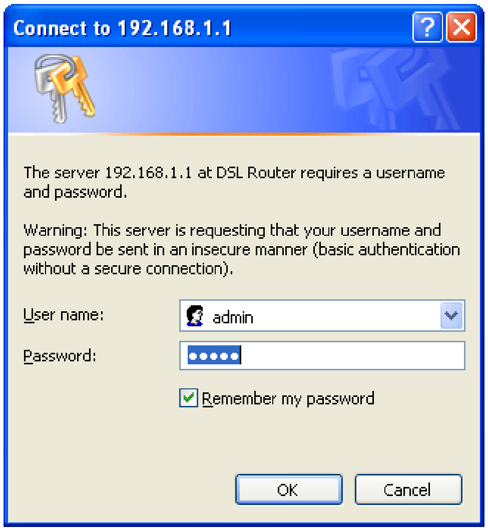
DSL(WAN) LAN1 - 4 WPS Reset Power On/Off USB(Side)

Figure 7 SR505N Rear Panel Connectors

Logging in to Your SmartRG™ Gateway's UI

To manually configure the SmartRG access the gateway's embedded web UI:

1. attach your computer's RJ45 connection to any of the SmartRG's LAN ports (1-4)
2. configure your computer's IP interface to acquire an IP address using DHCP (See the IMPORTANT note below for instructions on logging in to a SmartRG gateway configured for "bridge mode" operation.)
3. open a browser and enter the gateway's default address http://192.168.1.1/admin in the address bar



Connect to 192.168.1.1

The server 192.168.1.1 at DSL Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: •••••

☑ Remember my password

Figure 8 Login Username and Password

4. Enter the default username and password: **admin/admin** and click **OK** to display the Device Info page.

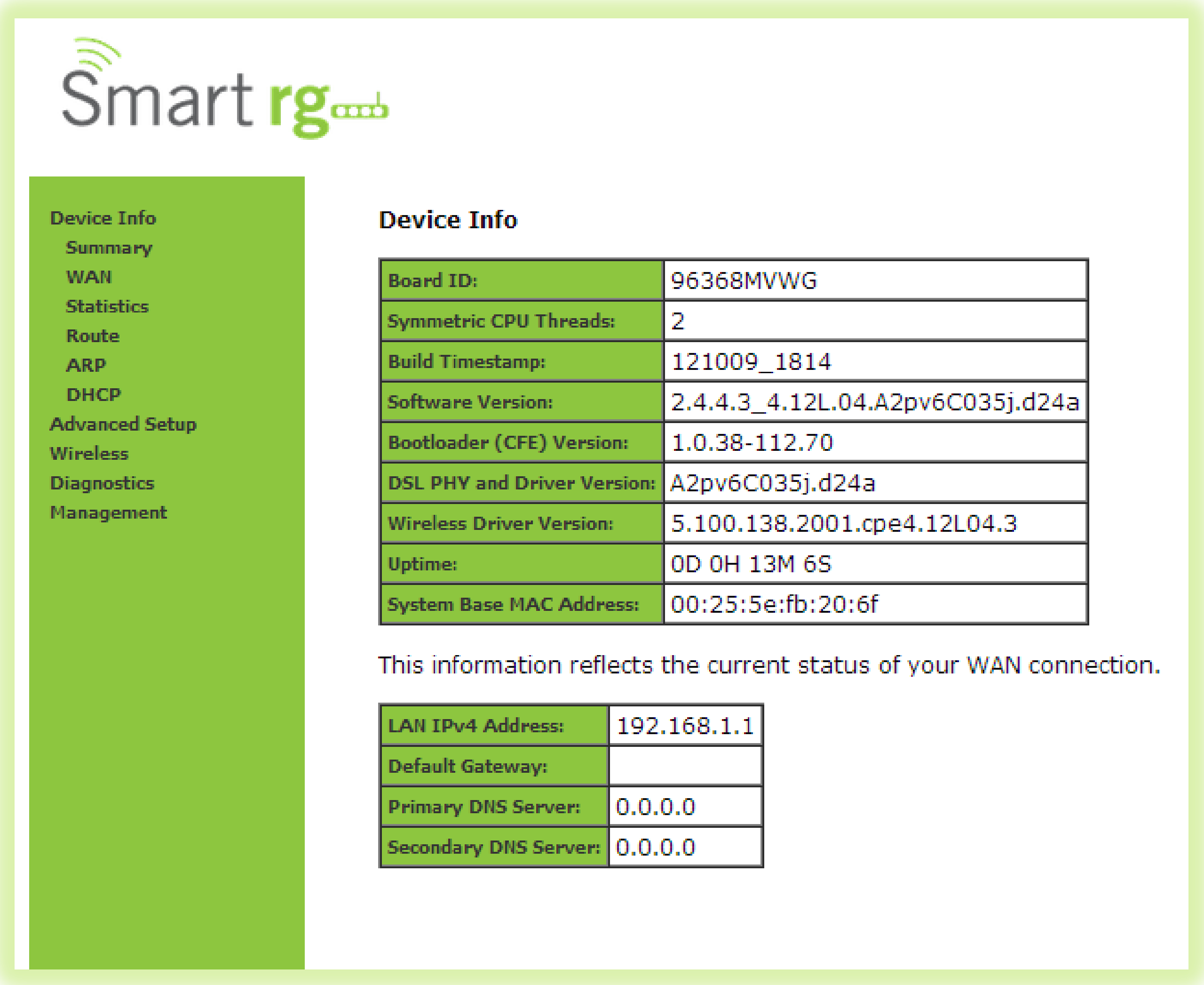
NOTE	The gateway's UI can be accessed via the WAN connection by entering the WAN IP address in your browser's address bar and entering the default username and password: support/support. WAN HTTP access MUST be enabled to access the gateway's UI via the WAN connection. See the "Configure Access Controls (HTTP, Telnet, SSH, etc.)" section for instructions on enabling WAN HTTP access.

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

Navigating Your SmartRG Gateway's Web UI

At login the Device Info page will appear. In addition to the basic identification info shown, the *Device Info* menu item can be expanded (by clicking the text) to reveal:

- WAN connection information
- WAN and LAN statistics
- Routing table entries
- ARP table entries –and-
- LAN host DHCP lease information



Device Info

Board ID:	96368MVWG
Symmetric CPU Threads:	2
Build Timestamp:	121009_1814
Software Version:	2.4.4.3_4.12L.04.A2pv6C035j.d24a
Bootloader (CFE) Version:	1.0.38-112.70
DSL PHY and Driver Version:	A2pv6C035j.d24a
Wireless Driver Version:	5.100.138.2001.cpe4.12L04.3
Uptime:	0D 0H 13M 6S
System Base MAC Address:	00:25:5e:fb:20:6f

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

Figure 9 Device Info Page

The remainder of the left menu bar items can be navigated in a similar fashion. Configure the following features and functions by expanding:

- **Advanced Setup** – WAN & LAN interfaces, routing, interface groupings, QoS, security, etc.
- **Wireless** – wireless access point and detailed radio settings
- **Diagnostics** – execute LAN & WAN interface diagnostics
- **Management** – backup/restore/default configurations, update device software, TR-069 ACS management settings, time zone & NTP settings and device reboot

Configuring Your SmartRG™ - Common Use Cases

To simplify your deployment of SmartRG gateways this document is structured around specific use cases designed to illustrate meaningful, service supporting configurations like:

- Creating WAN interfaces for Internet data access and remote gateway management
- Provisioning the SmartRG for remote management via TR-069
- Setting up the LAN
- Managing wireless
- Creating IPTV service configurations (bridged and routed)
- Classifying LAN traffic and applying QoS to support IPTV and VoIP applications
- Enabling secure communications (IPSec)

Given the breadth of a SmartRG residential gateway's features and the diversity of applications, only the most common use cases are detailed here. Please contact SmartRG Support to inquire about additional use cases.

Use Case: Creating WAN Connections for Internet Access and Remote Management

SmartRG residential gateways are commonly deployed to provide Internet access for LAN hosts such as workstations, gaming consoles, IP cameras and myriad other IP enabled devices increasingly found in the home or office. Packets routed between LAN hosts and the Internet pass through the gateway's routed WAN connection. Remote management (via TR-069) is also performed through this connection. The typical Internet access/remote management connection configuration is diagramed below.

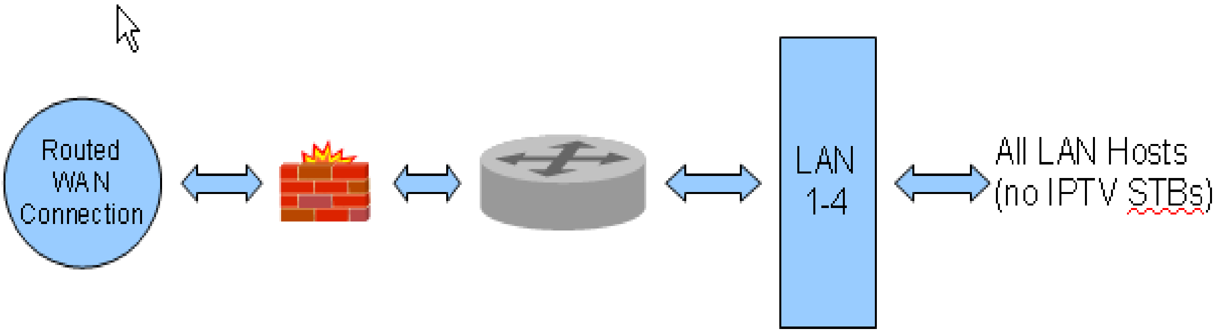


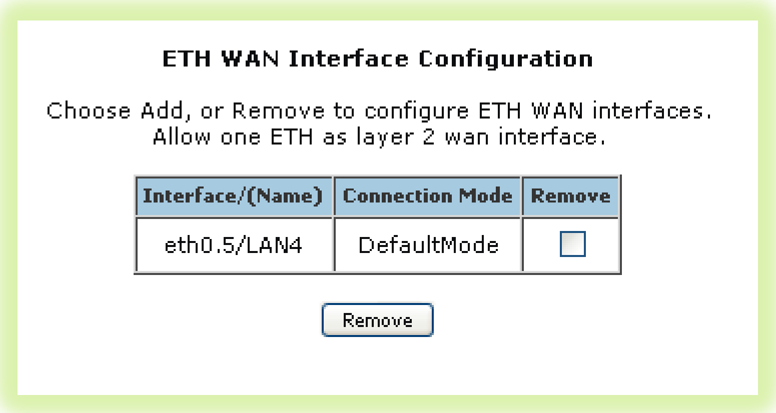
Figure 10 Internet / TR-069 Management WAN Connection

WAN connection creation is a two-step process beginning with the configuration of a layer 2 interface (Ethernet or DSL) followed by the creation of a layer 3, WAN service. Common WAN services include PPPoE, DHCP and Static IP.

Configuring the Layer 2 Interface (Ethernet)

To configure an Ethernet layer 2 interface:

1. Select *Advanced Setup -> Layer2 Interface.* The default Ethernet WAN interface (eth0.5/LAN4) will be displayed.



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
eth0.5/LAN4	DefaultMode	□

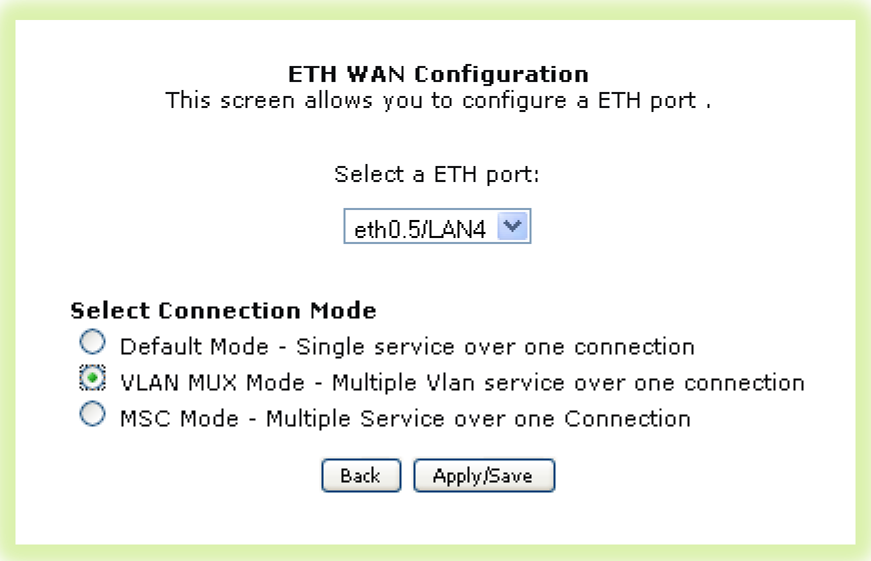
Figure 11 Ethernet Layer 2 Interface Configuration (Default)

No further configuration is necessary.

Configuring the Layer 2 Interface (Ethernet with VLAN Tags)

In some applications it may be necessary to segment the Ethernet WAN interface into separate VLANs. A common application for a VLAN segmented WAN interface is bridged IPTV as detailed in the "Bridged IPTV Configuration" section. To configure the layer 2 Ethernet interface to support VLAN tagged traffic:

1. Select *Advanced Setup -> Layer2 Interface.* The default Ethernet WAN interface (eth0.5/LAN4) will be displayed.
2. Check the "Remove" box and click **Remove.**
3. Click **Add.**
4. Select "VLAN MUX Mode."



ETH WAN Configuration
This screen allows you to configure a ETH port .

Select a ETH port:

eth0.5/LAN4

Select Connection Mode
○ Default Mode - Single service over one connection
● VLAN MUX Mode - Multiple Vlan service over one connection
○ MSC Mode - Multiple Service over one Connection

Figure 12 Ethernet Layer 2 Interface Configuration (VLAN Tagged)

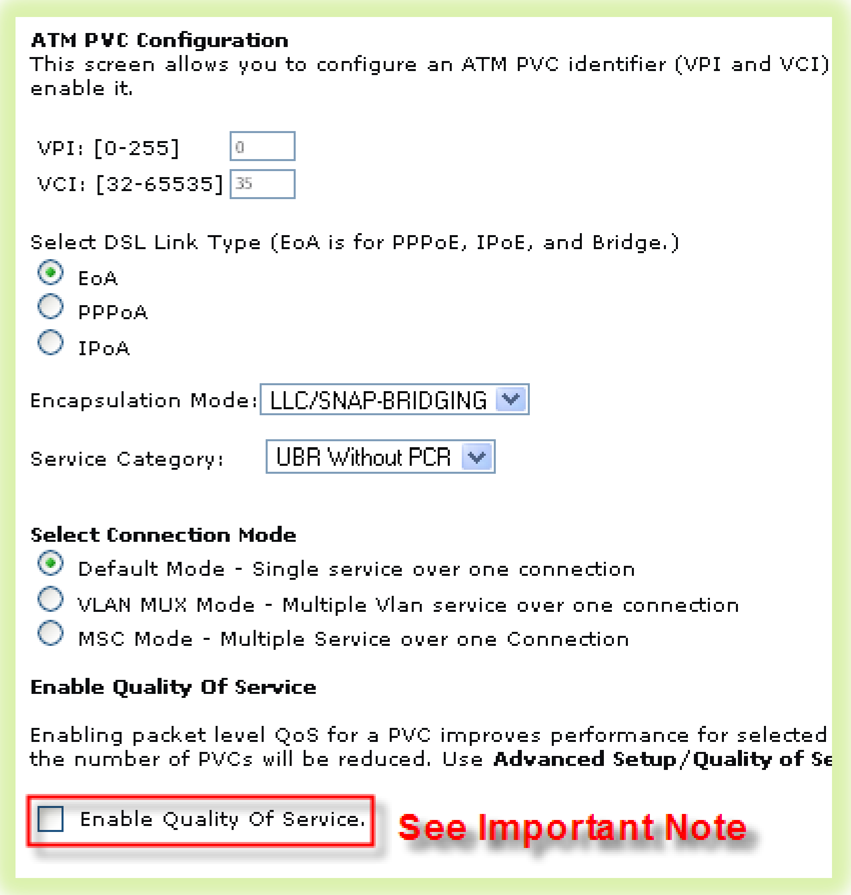
5. Click **Apply/Save.**

NOTE	802.1P (priority) and 802.1Q (VLAN tag) values will be set at the time of WAN Service creation as detailed in, "Creating the WAN Service."

Configuring the Layer 2 Interface (ADSL)

To configure an ADSL layer 2 interface:

1. Select *Advanced Setup -> Layer2 Interface* and click **Add.**



ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI)
enable it.

VPI: [0-255] 0
VCI: [32-65535] 35

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
● EoA
○ PPPoA
○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select Connection Mode
● Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection
○ MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected
the number of PVCs will be reduced. Use **Advanced Setup/Quality of Se**

□ Enable Quality Of Service.

See Important Note

Figure 13 ADSL Layer 2 Interface Configuration

2. Enter the PVC's identifier (VPI/VCI).
3. Select the "DSL Link Type" – Ethernet over ATM (RFC 2684) is typical.
4. Select the "Encapsulation Mode" – LLC/SNAP-BRIDGING is typical.
5. Select the "Service Category" (upstream ATM shaping) – "UBR Without PCR" (Unspecified Bit Rate Without Peak Cell Rate) is typical.
6. Select the "Connection Mode" – Choose Default Mode for non-VLAN tagged traffic. Choose VLAN MUX Mode if you intend to segment LAN traffic into separate VLAN tagged WAN services.

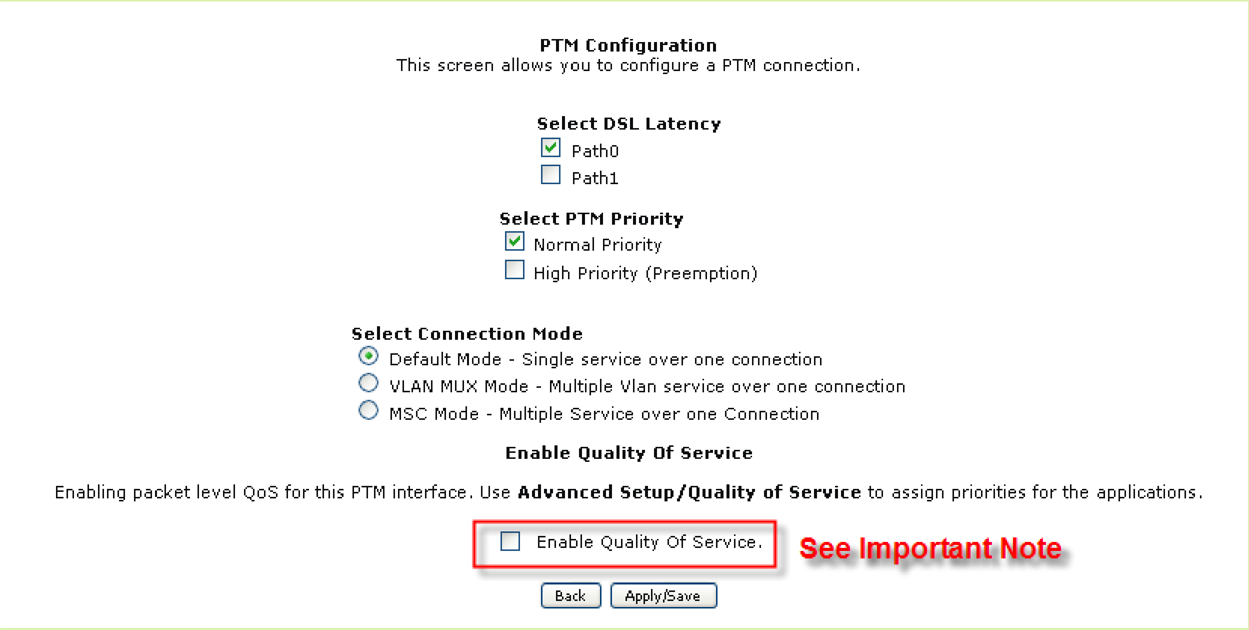
7. IMPORTANT - Check "Enable Quality of Service" if you intend to support QoS classified traffic through the WAN service.
8. Click **Apply/Save**.

NOTE	Enabling QoS for routed IPTV service configurations will improve channel change performance.

Configuring the Layer 2 Interface (PTM – Supported on ADSL and VDSL)

To configure a PTM layer 2 interface :

1. Select *Advanced Setup -> Layer2 Interface -> PTM Interface* and click **Add**.



PTM Configuration
This screen allows you to configure a PTM connection.

Select DSL Latency
☑ Path0
☐ Path1

Select PTM Priority
☑ Normal Priority
☐ High Priority (Preemption)

Select Connection Mode
● Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection
○ MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for this PTM interface. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

☐ Enable Quality Of Service.

See Important Note

Figure 14 VDSL Layer 2 Interface Configuration

2. Select the "DSL Latency" – Path0 is typical.
3. Select the "PTM Priority" – Normal Priority is typical.
4. Select the "Connection Mode" – Default Mode is typical (when VLAN segmentation is not required).

5. IMPORTANT - Check “Enable Quality of Service” if you intend to support QoS classified traffic through the WAN service.
6. Click **Apply/Save**.

NOTE	Enabling QoS for routed IPTV service configurations will improve channel change performance.

NOTE	802.1P (priority) and 802.1Q (VLAN tag) values will be set at the time of WAN Service creation as detailed in, “Creating the WAN Service.”

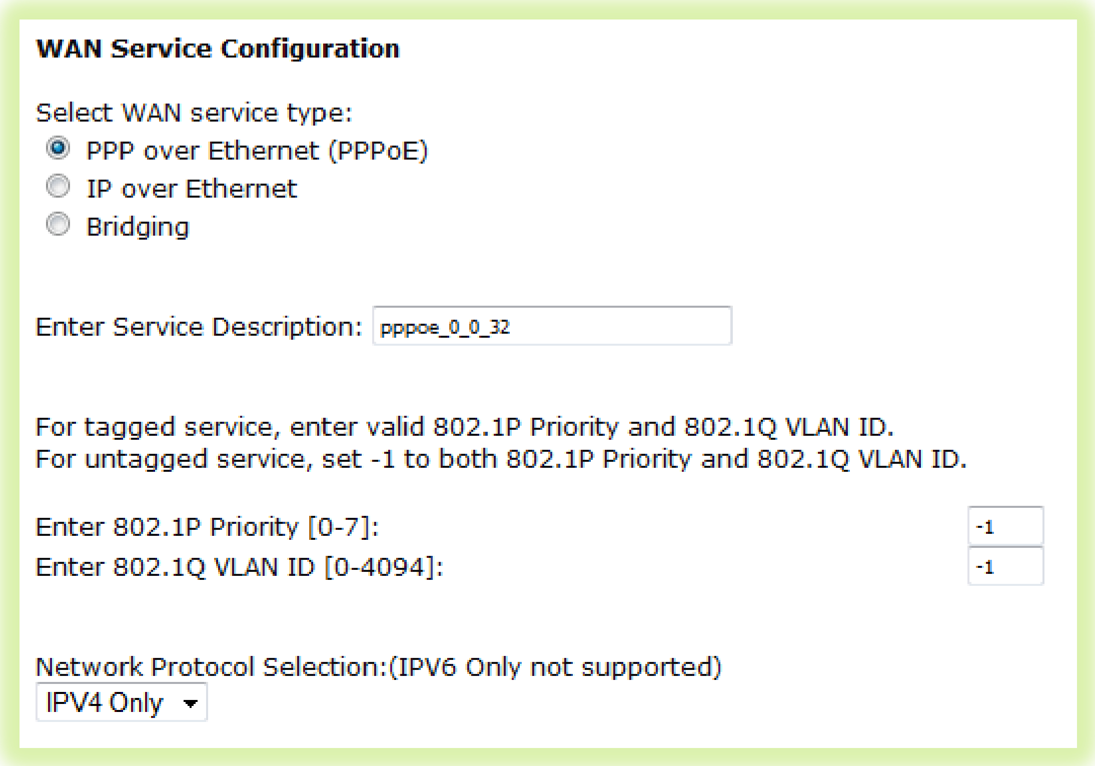
Configuring the Layer 2 Interface (VDSL/PTM with VLAN Tags)

In some applications it may be necessary to segment the PTM WAN interface into separate VLANs. A common application for a VLAN segmented WAN interface is bridged IPTV as detailed in the “Bridged IPTV Configuration” section. ***To configure the layer 2 PTM interface to support VLAN tagged traffic select “VLAN MUX Mode” for “Connection Mode” in step 4 of the “Configuring the Layer 2 Interface (PTM –*** Supported on ADSL and VDSL)***” section.***

Creating the WAN Service

WAN Services are created on top of previously created Layer 2 interfaces. To create a WAN service:

1. Select *Advanced Setup -> WAN Service* and click **Add**.
2. Select a previously created layer 2 interface from the drop down list and click **Next**.
3. Select the "WAN Service type" – "PPP over Ethernet" or "IP over Ethernet" are appropriate choices for routed WAN services. Bridged WAN services will be covered later in the "Bridged IPTV Configuration" section.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_0_32

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

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

Network Protocol Selection:(IPV6 Only not supported)
IPV4 Only

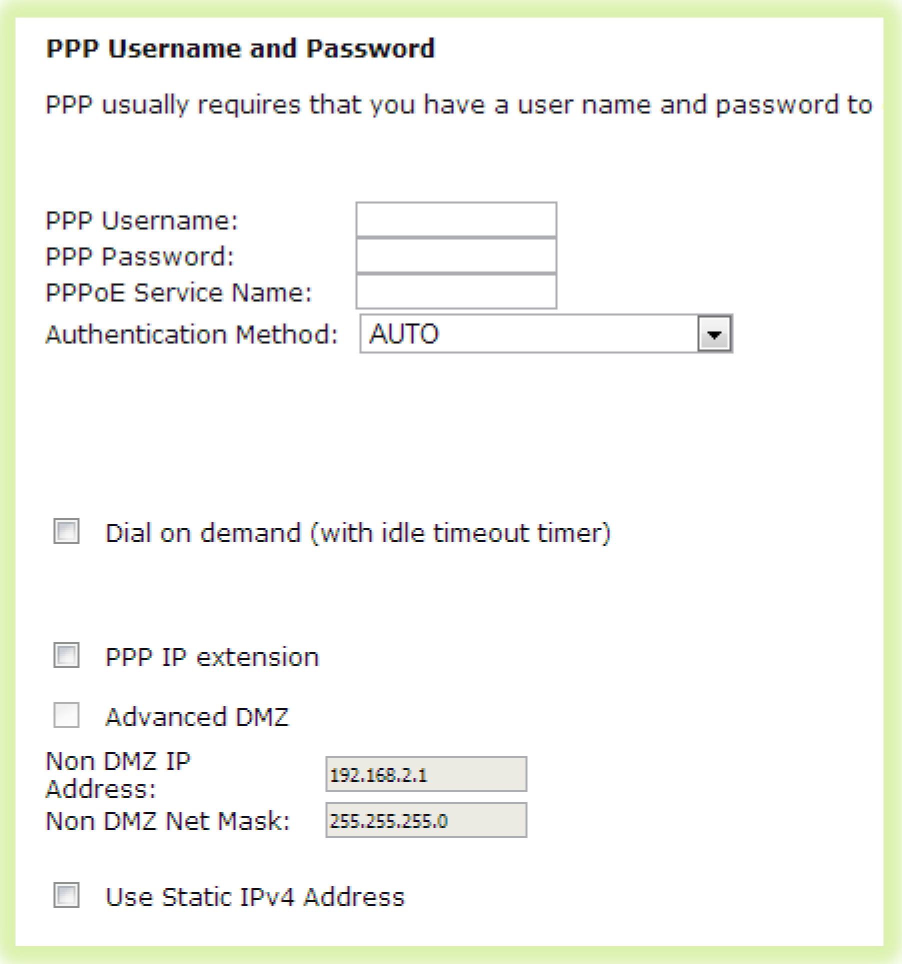
Figure 15 WAN Service Configuration (With or Without VLAN Tagging Support)

NOTE	If VLAN tagging support is desired, set the 802.1p and 802.1q values appropriately. 802.1P: 0 is lowest priority, 7 is highest priority, -1 is unused 802.1Q: -1 indicates no VLAN tagging

NOTE	The SR-350N/NE and SR-500N/NE gateways support mixed VLAN tagged/untagged traffic on the same WAN interface. Set the untagged WAN connection's VLAN ID to -1.

4. Click **Next**.

5. **For PPP WAN services** enter the "PPP Username" and "PPP Password". If desired, enable the firewall, NAT and IGMP Proxy. Click **Next.**



PPP Username and Password

PPP usually requires that you have a user name and password to

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Advanced DMZ

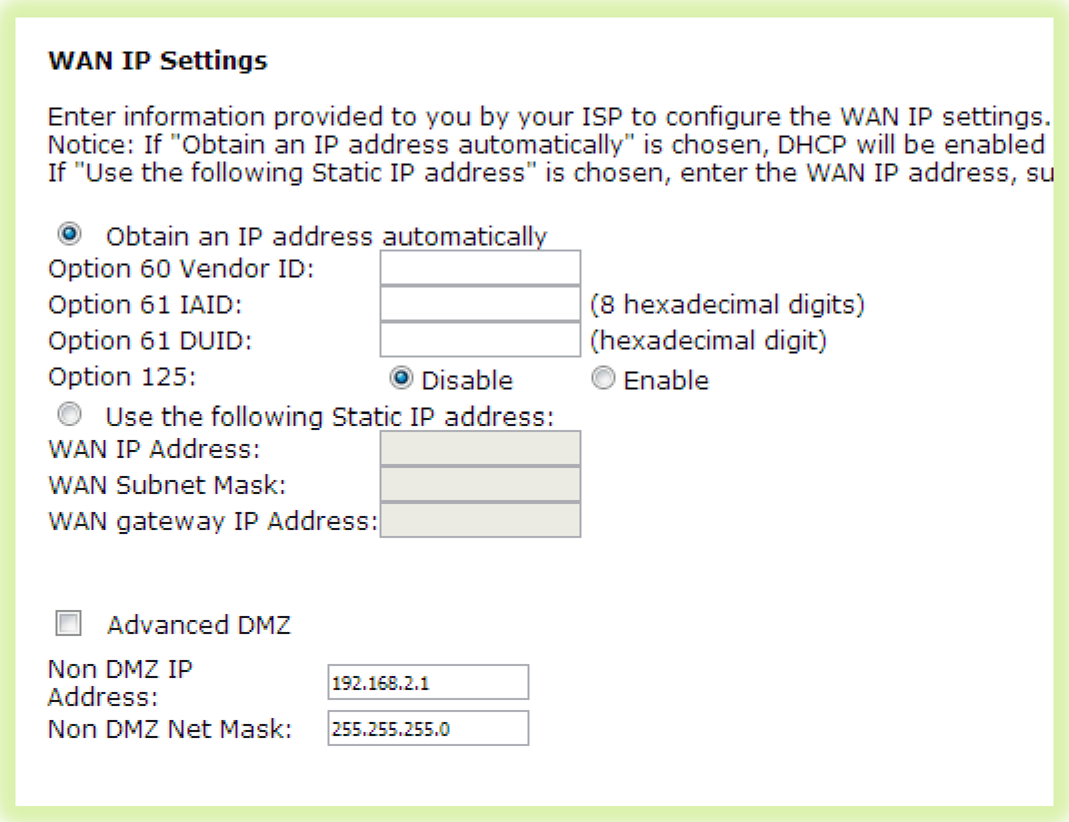
Non DMZ IP Address: 192.168.2.1
Non DMZ Net Mask: 255.255.255.0

□ Use Static IPv4 Address

Figure 16 PPP Username and Password

-OR-

6. **For IPoE WAN services** select “Obtain an IP address automatically” (DHCP) or select “Use the following Static IP address” and enter the “WAN IP Address”, “WAN Subnet Mask” and “WAN gateway IP.” Click **Next.**



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
If "Use the following Static IP address" is chosen, enter the WAN IP address, su

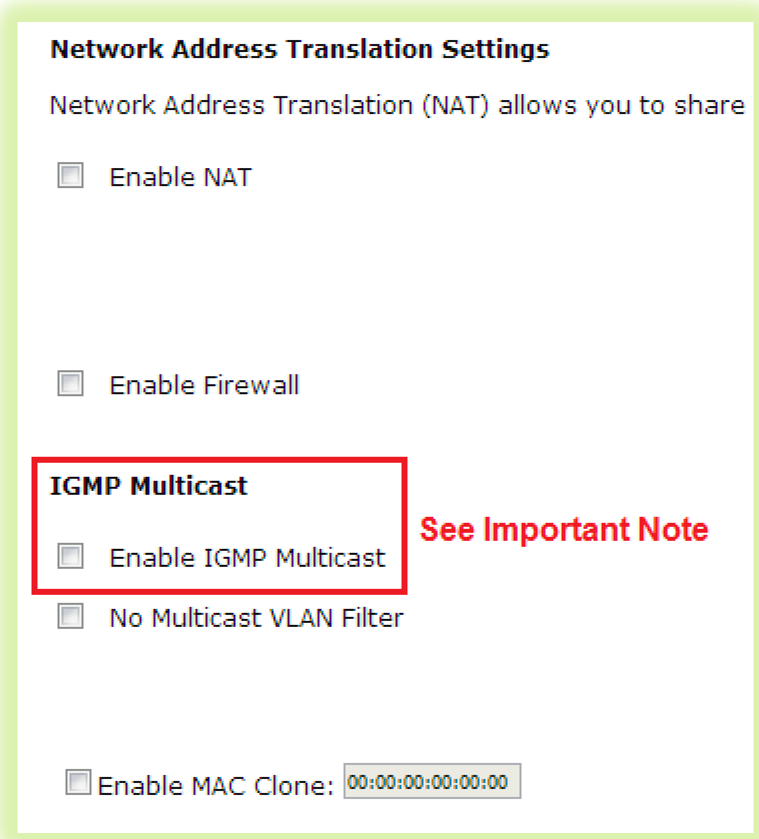
● Obtain an IP address automatically
Option 60 Vendor ID:
Option 61 IAID: (8 hexadecimal digits)
Option 61 DUID: (hexadecimal digit)
Option 125: ● Disable ○ Enable
○ Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

□ Advanced DMZ

Non DMZ IP Address: 192.168.2.1
Non DMZ Net Mask: 255.255.255.0

Figure 17 WAN IP Settings

7. If desired enable the firewall, NAT and IGMP Multicast.



Network Address Translation Settings

Network Address Translation (NAT) allows you to share

□ Enable NAT

□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

See Important Note

□ No Multicast VLAN Filter

□ Enable MAC Clone: 00:00:00:00:00:00

Figure 18 WAN NAT, Firewall and IGMP Settings

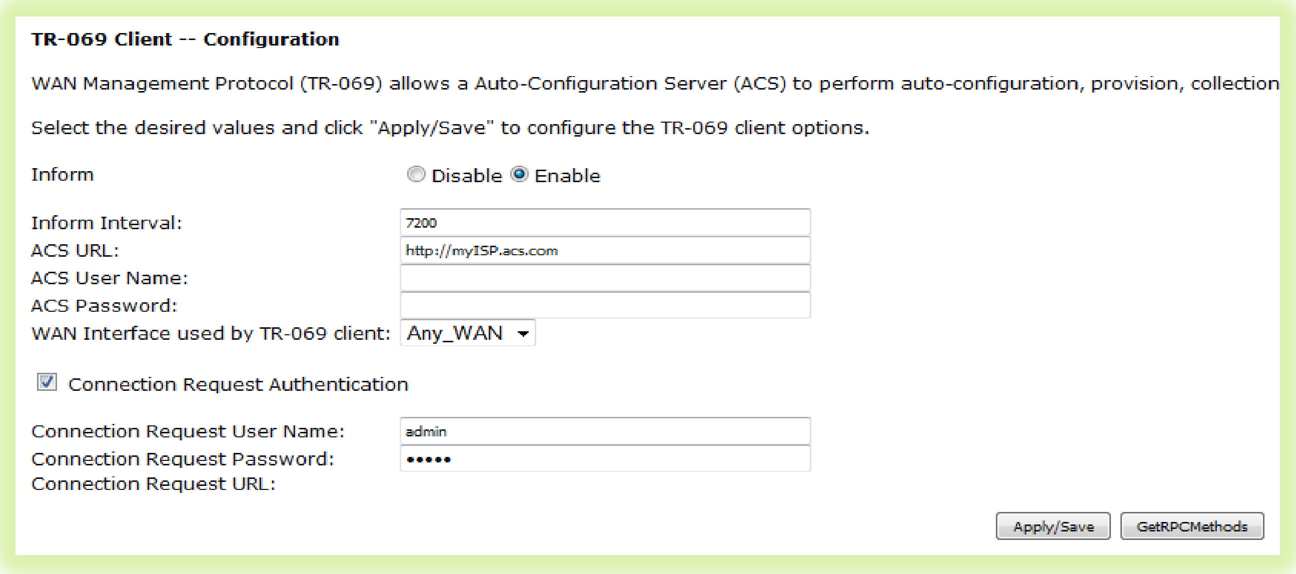
8. Select the WAN interface to be used by this WAN service. Click **Next.**
9. Select "Obtain DNS info from a WAN interface" and select the desired WAN interface from the drop down list (a single WAN interface is common *unless* you are creating bridged IPTV configurations) –or- select "Use the following Static DNS IP address" and enter the IP addresses of your network's primary and secondary DNS servers. Click **Next.**
10. Review the WAN service summary. If you are satisfied click **Apply/Save.**

Use Case: Provisioning Your SmartRG for Remote ACS Management

NOTE	This step is not required for production SmartRG gateways. SmartRG maintains an “Activation Server” that associates MAC addresses with service providers’ ACS management URLs. After the SmartRG has established its WAN connection (using the Connect-and-Surf algorithm) it connects to the SmartRG Activation Server and reports its MAC. The Activation Server changes the ACS management URL to point to the service provider’s ACS.

To manually provision your SmartRG for management by a TR-069 enabled Automated Configuration Server:

1. Select *Management -> Management Server -> TR-069 Client.*



TR-069 Client -- Configuration

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

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

Inform ○ Disable ● Enable

Inform Interval: 7200
ACS URL: http://myISP.acs.com
ACS User Name:
ACS Password:
WAN Interface used by TR-069 client: Any_WAN

☑ Connection Request Authentication

Connection Request User Name: admin
Connection Request Password: •••••
Connection Request URL:

Figure 19 TR-069 Management Settings

2. Enter the following parameter values:
   - Enable “Informs”
   - Set the “Inform Interval” to 7200 seconds
   - Set the “ACS URL” (e.g. http://myISP.acs.com/)
   - Leave the “ACS User Name” and “ACS Password” blank
   - Enable “Connection Request Authentication”
   - Set the “Connection Request User Name and Password” to admin/admin
3. Click **Apply/Save.**

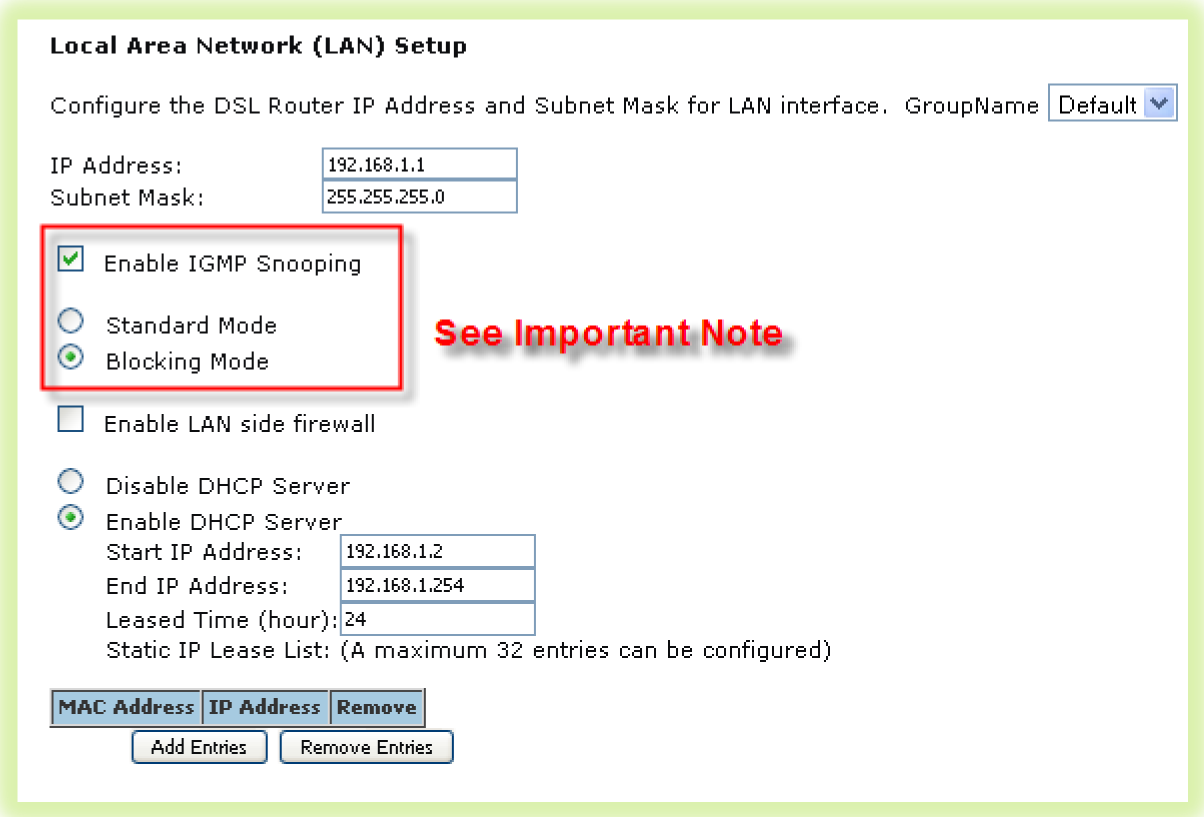
NOTE	Configure less and deploy more. Manage subscriber services and your entire gateway fleet with the ClearVision® management system. Contact SmartRG to start your trial

	today. See us at www.smartrg.com.

Use Case: Setting Up the LAN

To configure the SmartRG's LAN interface:

1. Select *Advanced Setup -> LAN*



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode
● Blocking Mode

See Important Note

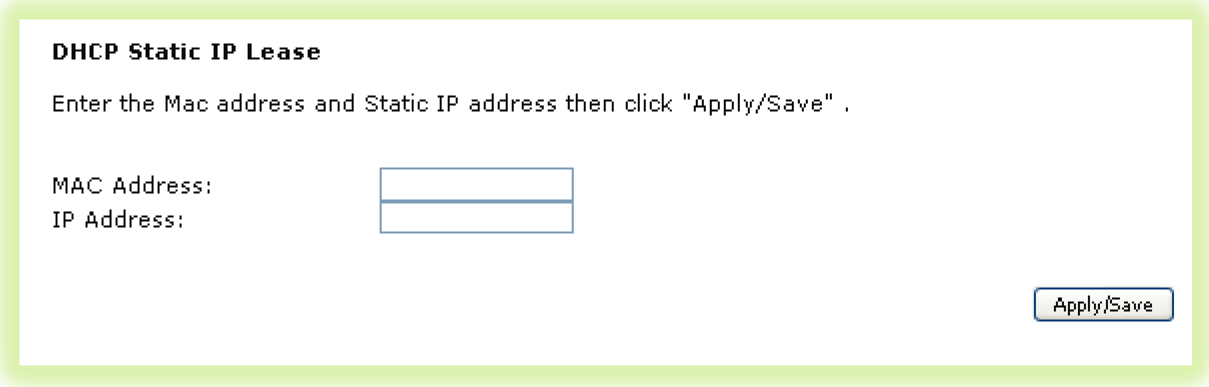
□ Enable LAN side firewall

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

Figure 20 LAN Settings

2. Leave the "GroupName" as Default.
3. Set the LAN interface's "IP Address" and "Subnet Mask" – Default values are: 192.168.1.1/255.255.255.0.
4. IMPORTANT – If you intend to support IPTV (either bridged or routed), you MUST select "Enable IGMP Snooping." Select "Blocking Mode."
5. Select "Enable DHCP Server" and set the DHCP address pool's start and end IP addresses.
6. Set the DHCP "Leased Time" in hours.
7. *If you would like to create static DHCP leases for specific LAN hosts,* click **Add Entries**.



DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

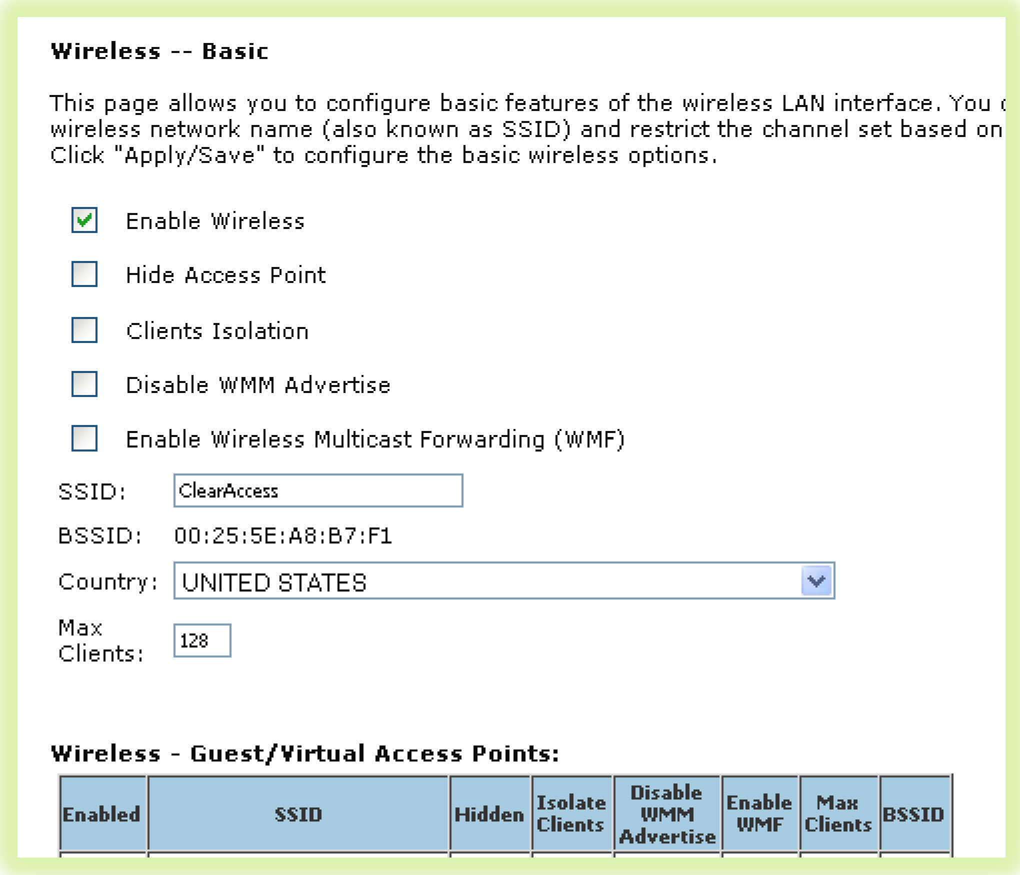
Figure 21 Adding DHCP Static IP Leases

8. Enter the LAN host's "MAC Address" and the desired "IP Address."
9. Click **Apply/Save** and repeat steps 7 and 8 for all static IP LAN hosts.

Use Case: Setting Up Wireless

To configure the SmartRG's Wireless interface:

1. Select *Wireless -> Basic*



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You c wireless network name (also known as SSID) and restrict the channel set based on Click "Apply/Save" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID: ClearAccess

BSSID: 00:25:5E:A8:B7:F1

Country: UNITED STATES

Max Clients: 128

Wireless - Guest/Virtual Access Points:

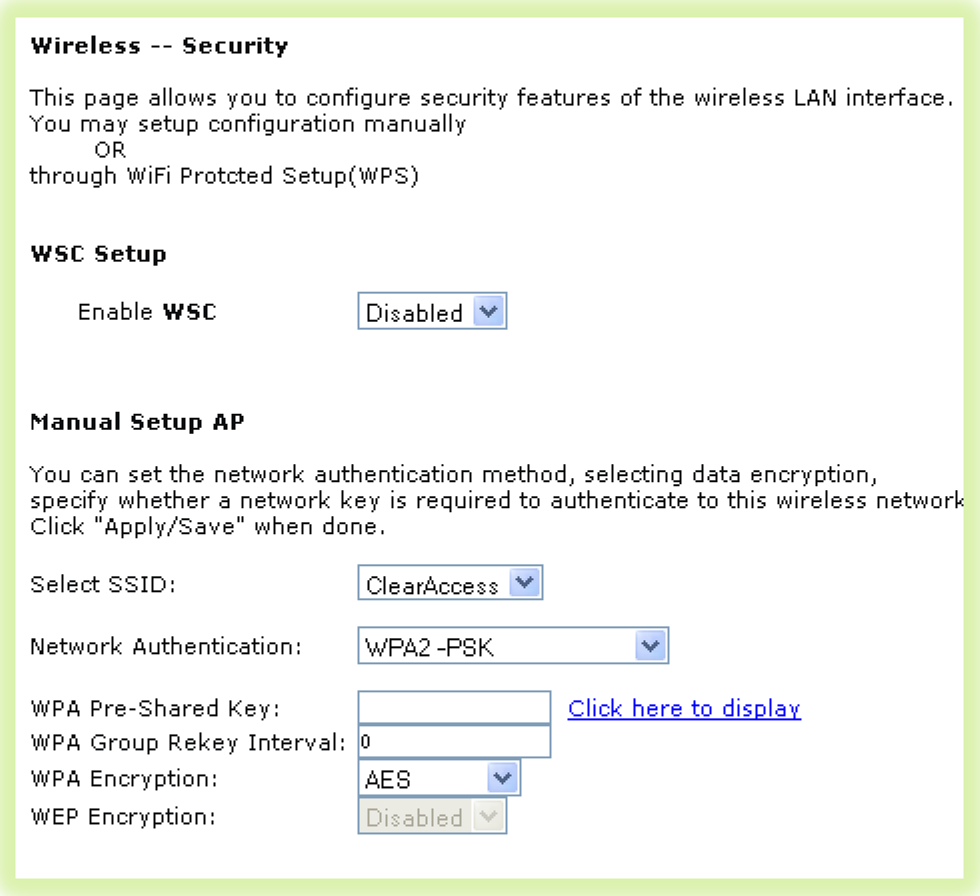
Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID

Figure 22 Wireless - Basic Settings

2. Select "Enable Wireless."
3. Set the wireless access point's "SSID."
4. Select the "Country" from the dropdown list.
5. Click **Apply/Save.**

NOTE	The SmartRG provides support for 3 additional guest/virtual wireless access points.

6. If you would like to select a specific Wi-Fi channel (1-11), select *Wireless -> Advanced* and change the Channel setting. The default value is “Auto.”
7. Select *Wireless -> Security*



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)

WSC Setup

Enable **WSC** Disabled

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
Click "Apply/Save" when done.

Select SSID: ClearAccess

Network Authentication: WPA2 -PSK

WPA Pre-Shared Key: Click here to display
WPA Group Rekey Interval: 0
WPA Encryption: AES
WEP Encryption: Disabled

Figure 23 Wireless - Security Settings

8. Select the “SSID” configured in step 3 above.
9. Select the “Network Authentication” – WPA2 with a Pre-Shared Key is common
10. Enter the “WPA Pre-Shared Key.” Click the link to display the private key value.
11. Click **Apply/Save.**

Use Case: Setting Up Wireless Distribution System (WDS)

When deployed in a larger home or office, a single wireless access point may not be able to provide adequate Wi-Fi coverage. Wireless Distribution Systems (WDS) provides a solution for this problem. WDS combines multiple gateways to act as a single larger wireless access point allowing Wi-Fi clients to seamlessly roam all access points plus it provides wired access to the entire network.

Two or more SmartRG gateways can be configured for WDS operation. The example below depicts a WDS deployment with three SmartRG gateways in a large home or office – one primary gateway in the center of the building and one remote gateway at either end of the building.

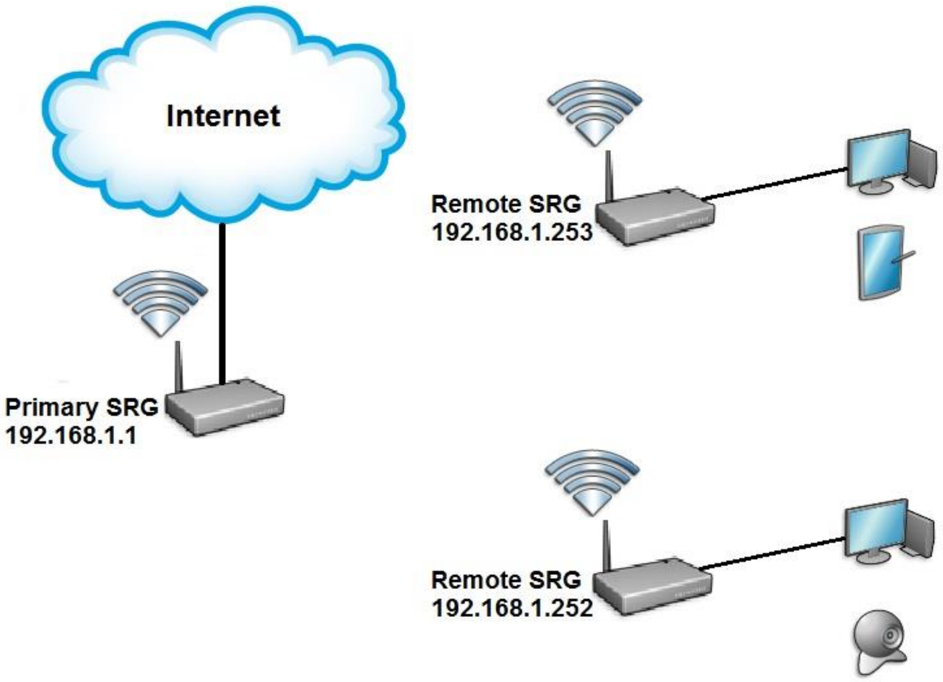


Figure 24 Wireless Distribution System

Configuring the SmartRG gateways for WDS operation requires the setting of **WAN**, **LAN** and **WIRELESS** parameters on all gateways included in the WDS system.

To configure the WAN connections…

1. On the primary SmartRG gateway: configure the routed WAN connection following the instructions in the “Use Case: Creating WAN Connections for Internet Access and Remote Management” section.
2. On the remote SmartRG gateway(s): no WAN configuration is required as the WAN connection is unused.

To configure the LAN interfaces…

3. On the primary SmartRG gateway:
   a) configure the LAN interface following the instructions in the “Use Case: Setting Up the LAN” section.
   b) ensure the DHCP Server is ENABLED and set the End IP Address such that enough LAN IP addresses are left for static allocation to the remote gateway(s) included in the WDS system.
4. On the remote SmartRG gateway(s):
   a) configure the LAN interface following the instructions in the “Use Case: Setting Up the LAN” section. **It is IMPORTANT to disable the DHCP server.**
   b) ensure the LAN IPaddress(es) are assigned from the remaining IP addresses not included in the DHCP server pool on the primary SmartRG gateway.

IMPORTANT	At this point your web browser session will terminate as the LAN IP address has changed from 192.168.1.1 to 192.168.1.x. Reconnect your web browser to the remote SmartRG referencing the new LAN IP address.

To configure the WIRELESS interfaces…

5. On the primary SmartRG gateway: configure the WIRELESS interface following the instructions in the “Use Case: Setting Up Wireless” section. **Do NOT select “Auto” for the Channel value.**
6. On the remote SmartRG gateway(s): configure the WIRELESS interface following the instructions in the “Use Case: Setting Up Wireless” section. **Select the same SSID, Security settings and Channel configured on the primary gateway.**
7. On the primary *and* remote SmartRG gateways:
   1. select Wireless -> Wireless Bridge and set “AP Mode” to Access Point
   2. set “Bridge Restrict” to Enabled(SCAN)
   3. click Apply/Save and wait for the page to refresh
   4. select the partner gateway (which has the same SSID as the primary gateway) by checking the box next to the SSID.
   5. Click Apply/Save

IMPORTANT	When configuring more than two gateways for WDS operation, the remote gateways MUST NOT be partnered together to avoid creating an Ethernet loop.

Use Case: Creating IPTV Service Configurations

The **SR350N, SR350NE, SR500N and SR500NE** SmartRG gateways are designed to meet the demands of IPTV service deployments.

Typically IPTV services have been deployed using bridged architectures with public IP addresses assigned to the IPTV Set-top-boxes (STBs) connected to the gateway's LAN ports. A typical bridged IPTV service configuration is shown below.

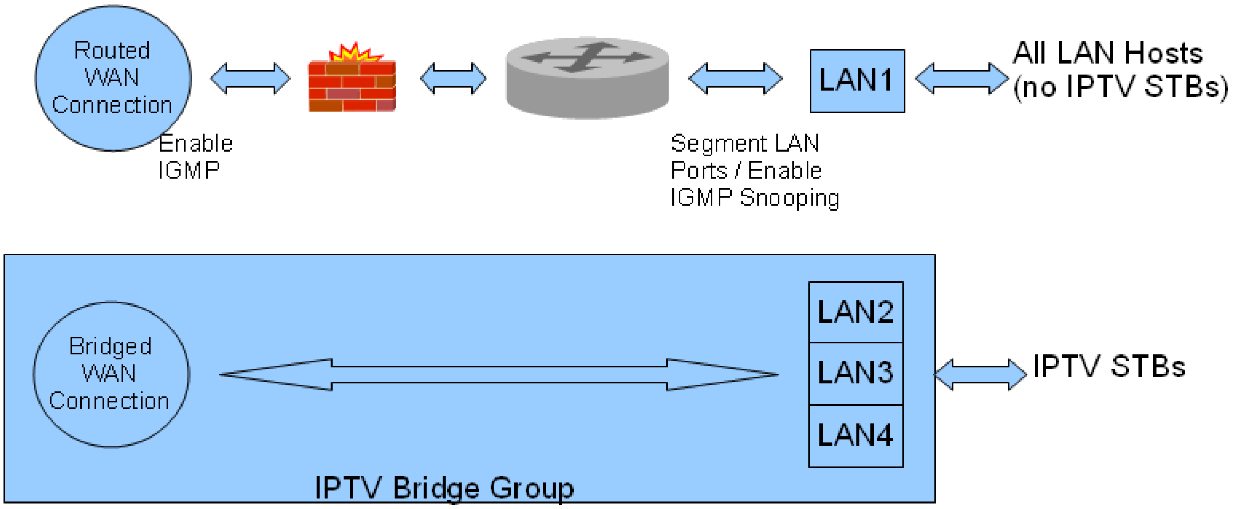


Figure 25 Bridged IPTV Configuration

Recently service providers have begun deploying routed IPTV services with STBs being assigned private LAN IP addresses by the gateway. A typical routed IPTV service configuration is shown below.

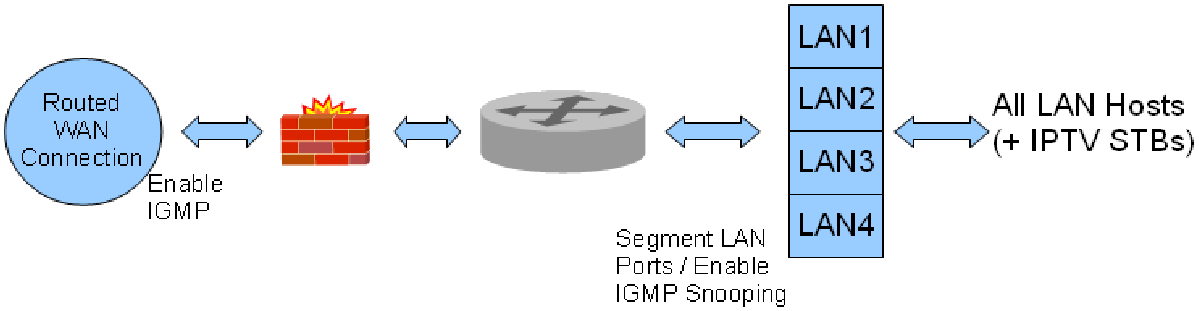

Routed WAN Connection
Enable IGMP
Segment LAN Ports / Enable IGMP Snooping
LAN1
LAN2
LAN3
LAN4
All LAN Hosts (+ IPTV STBs)

Figure 26 Routed IPTV Configuration

SmartRG gateways are designed to exceed the high bandwidth demands of either IPTV service architecture. Refer to the appropriate section below to configure the SmartRG gateway for your particular IPTV deployment architecture.

Bridged IPTV Configuration

A bridged IPTV configuration is comprised of:

- one (or more) WAN connections
- one (or more) LAN connections –and-
- an interface grouping structure to bind all of the connections together

The more generalized bridged IPTV service configuration with multiple WAN connections is shown below.

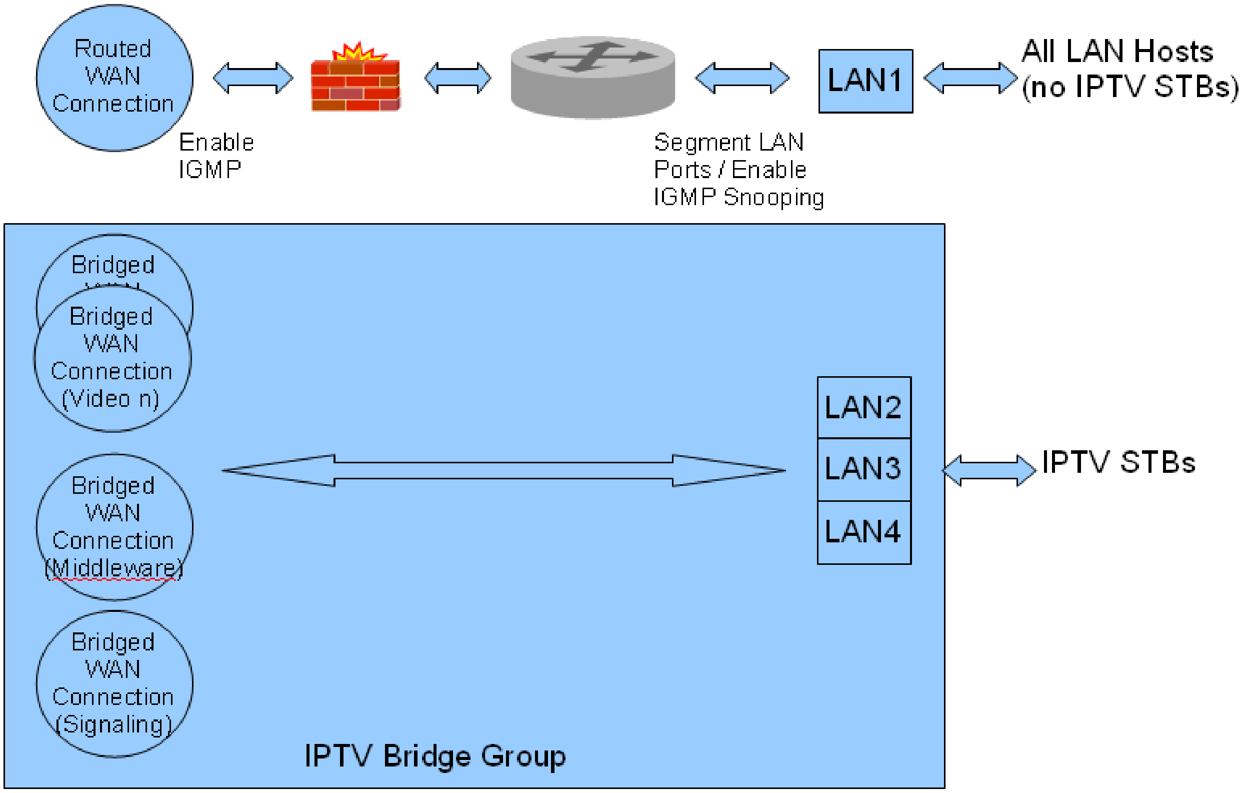

Routed WAN Connection
Enable IGMP
Segment LAN Ports / Enable IGMP Snooping
LAN1
All LAN Hosts (no IPTV STBs)
Bridged WAN
Bridged WAN Connection (Video n)
Bridged WAN Connection (Middleware)
Bridged WAN Connection (Signaling)
LAN2
LAN3
LAN4
IPTV STBs
IPTV Bridge Group

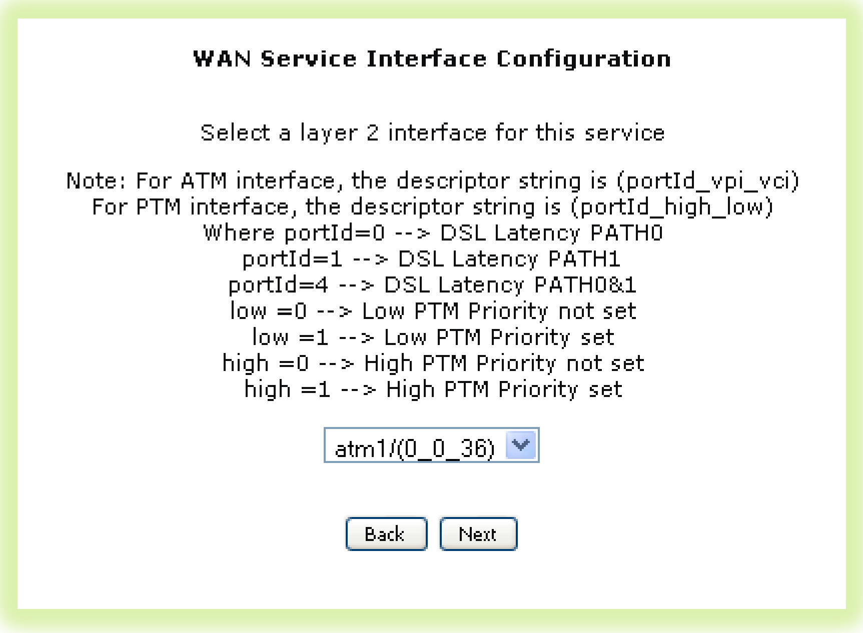
Figure 27 Multi-WAN Connection Bridged IPTV Configuration

Creating Bridged WAN Connections

To configure the SmartRG for bridged IPTV service deployments (with one or more WAN connections) start by creating the bridged WAN connections:

1. Create a Layer 2 interface following the instructions detailed in:
    a. “Configuring the Layer 2 Interface (Ethernet)”
    b. “Configuring the Layer 2 Interface (ADSL)” or
    c. “Configuring the Layer 2 Interface (PTM – Supported on ADSL and VDSL)”

   as appropriate for your particular SmartRG (Ethernet or DSL).
2. Select *Advanced Setup -> WAN Service.*



WAN Service Interface Configuration

Select a layer 2 interface for this service

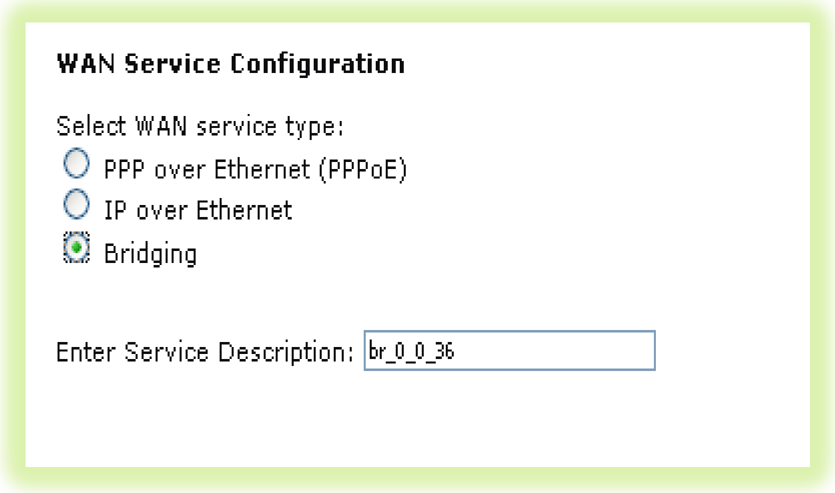
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high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

atm1/(0_0_36)

Figure 28 Selecting a Bridged WAN Service’s Layer 2 Interface

3. Select the Layer 2 Interface (created in step 1 above) from the drop down list and click **Next.**

4. Select “Bridging” and click **Next.**



WAN Service Configuration

Select WAN service type:

○ PPP over Ethernet (PPPoE)
○ IP over Ethernet
● Bridging

Enter Service Description: br_0_0_36

Figure 29 Creating a Bridged WAN Service

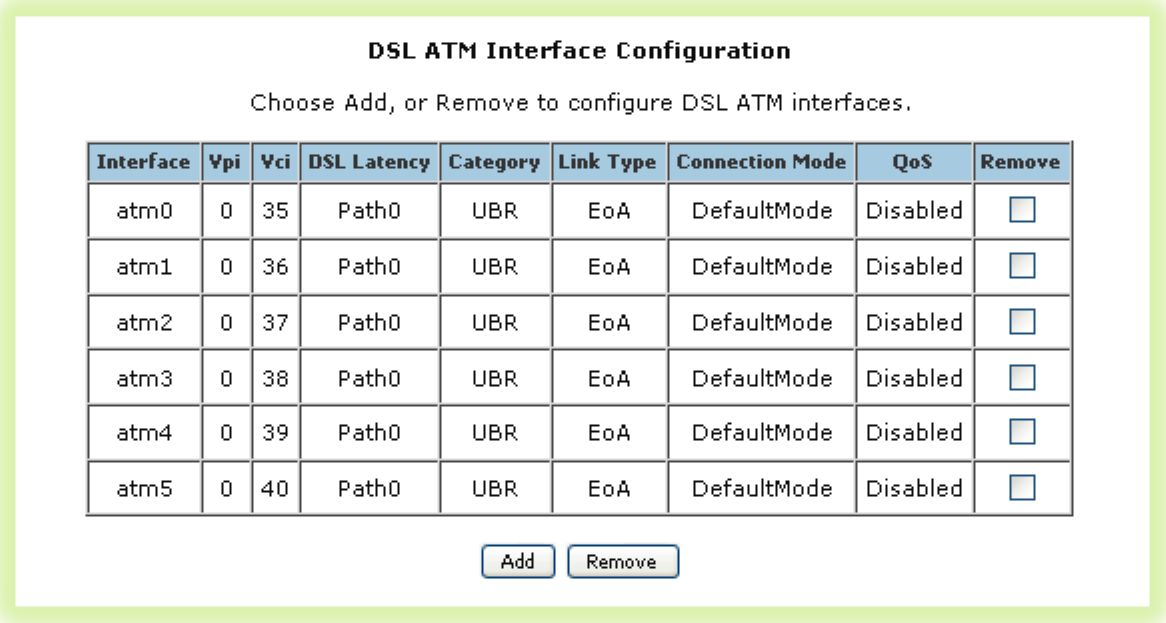
5. Review the bridged WAN service summary and click **Apply/Save** if you are satisfied.
6. Repeat steps 1-5 as necessary to support your particular IPTV configuration (i.e. single or multi-WAN connection).

NOTE	Some DSLAMs require multiple WAN connections to support IPTV services. Contact your DSLAM vendor for IPTV configuration details.

IMPORTANT NOTE	The IGMP bridged WAN connection MUST be the last bridged WAN connection created.

7. Ensure “IGMP Snooping” has been enabled on the LAN as detailed in the “Use Case: Setting Up the LAN” section.
8. Check “LAN(1-4)” – (This segments the four LAN ports into separate interfaces instead of a single switched block of ports).
9. Click **Apply/Save.**

At the conclusion of step 9 your Layer 2 Interface summary (*Advanced Setup -> Layer 2 Interface*) will look similar to:



DSL ATM Interface Configuration

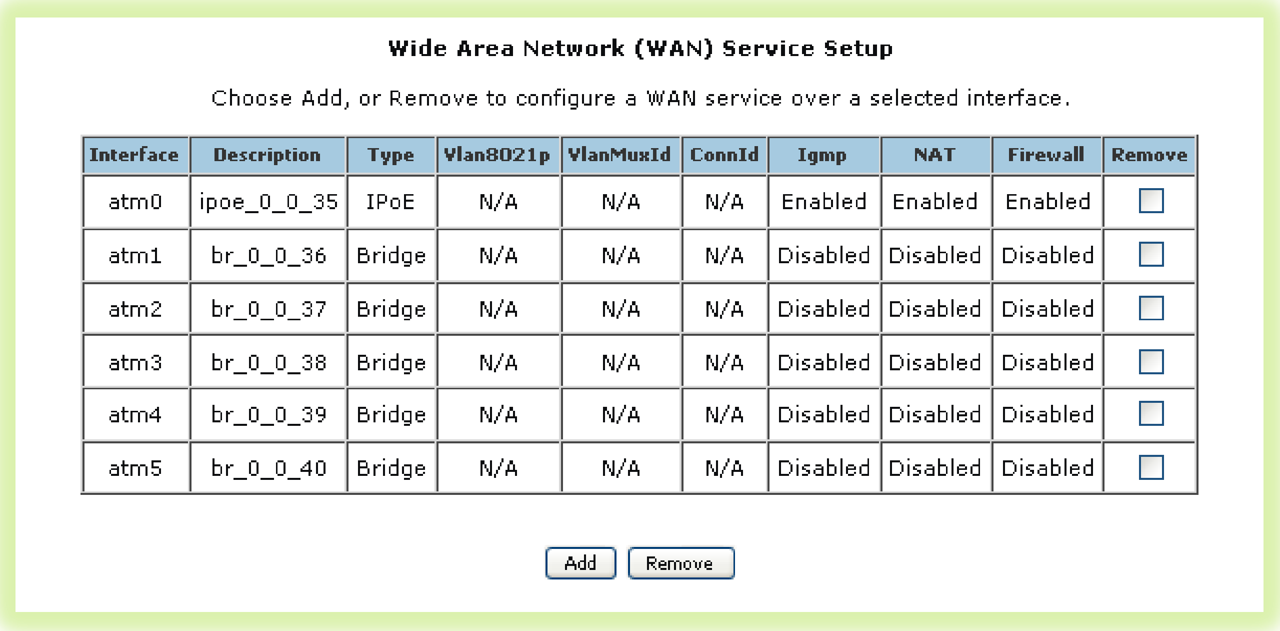
Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Disabled	□
atm1	0	36	Path0	UBR	EoA	DefaultMode	Disabled	□
atm2	0	37	Path0	UBR	EoA	DefaultMode	Disabled	□
atm3	0	38	Path0	UBR	EoA	DefaultMode	Disabled	□
atm4	0	39	Path0	UBR	EoA	DefaultMode	Disabled	□
atm5	0	40	Path0	UBR	EoA	DefaultMode	Disabled	□

Figure 30 IPTV Layer 2 Interface Summary (Multi-WAN Bridge Group)

NOTE	The generalized (more complex) IPTV bridge group is detailed here. The majority of DSLAMs require only a single WAN connection to support IPTV services. In that typical case: • The “atm0” interface would provide routed WAN access for Internet services and remote management –and- • The “atm1” interface would provide bridged WAN access for all IPTV related services (multi-cast streams, middleware server access and IGMP signaling)

Your WAN Service summary (*Advanced Setup* -> *WAN Service*) will look similar to:



Wide Area Network (WAN) Service Setup

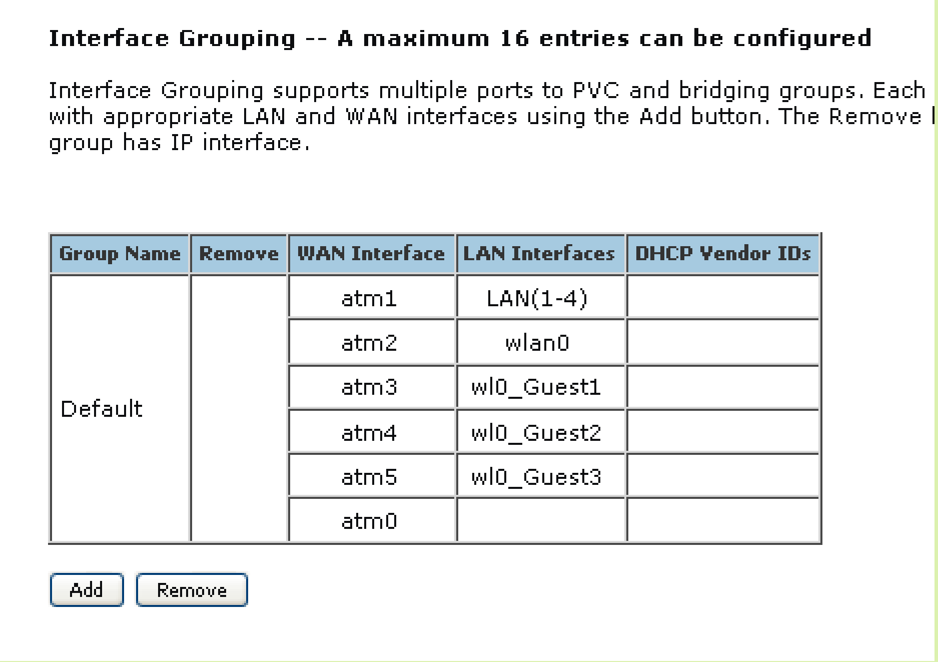
Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
atm0	ipoe_0_0_35	IPoE	N/A	N/A	N/A	Enabled	Enabled	Enabled	□
atm1	br_0_0_36	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	□
atm2	br_0_0_37	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	□
atm3	br_0_0_38	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	□
atm4	br_0_0_39	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	□
atm5	br_0_0_40	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	□

Figure 31 IPTV WAN Service Summary (Multi-WAN Bridge Group)

Creating Interface (Bridge) Groupings

10. Select *Advanced Setup -> Interface Grouping.*



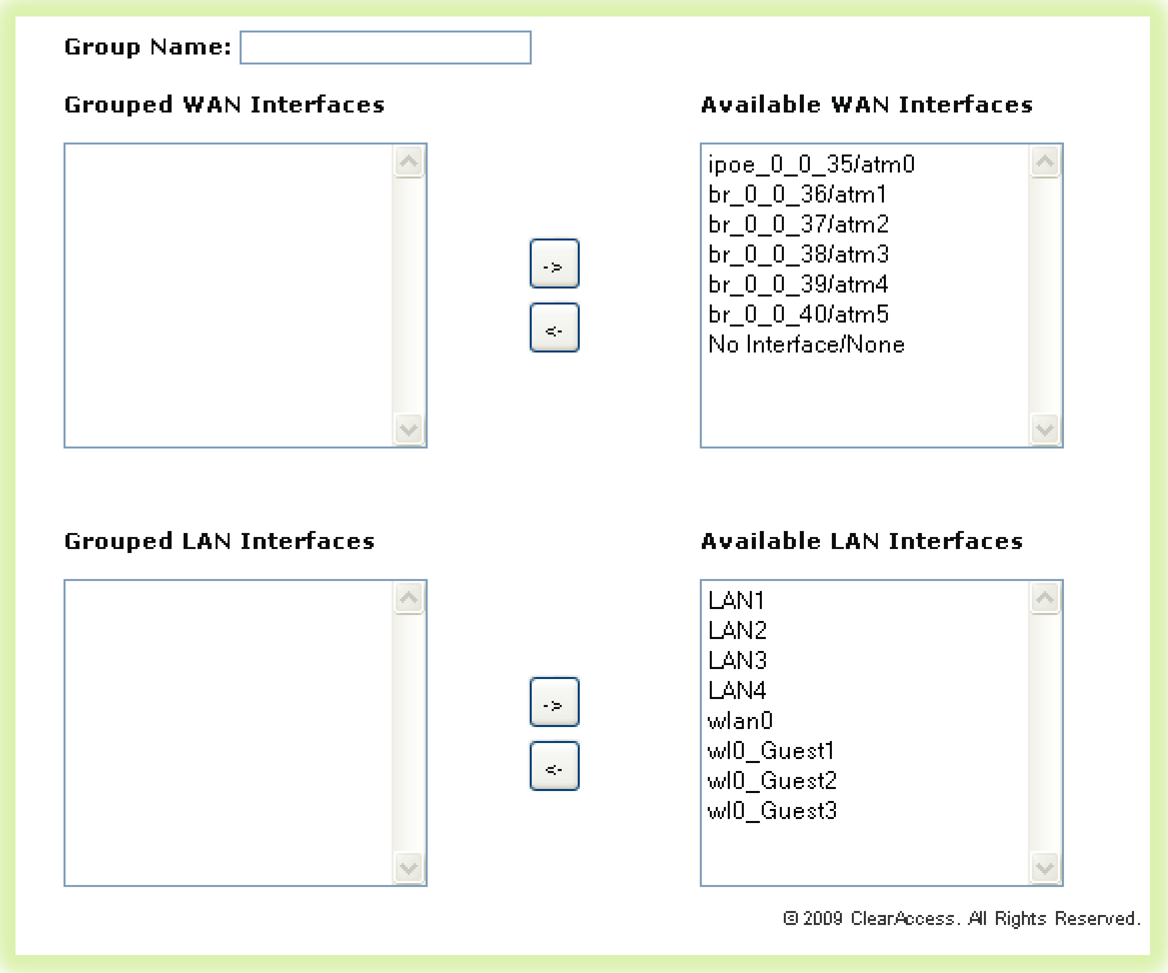
Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each with appropriate LAN and WAN interfaces using the Add button. The Remove group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		atm1	LAN(1-4)	
		atm2	wlan0	
		atm3	wl0_Guest1	
		atm4	wl0_Guest2	
		atm5	wl0_Guest3	
		atm0		

Figure 32 Creating an IPTV Bridge Interface Group

11. Click **Add.**



Group Name:

Grouped WAN Interfaces

Available WAN Interfaces

ipoe_0_0_35/atm0
br_0_0_36/atm1
br_0_0_37/atm2
br_0_0_38/atm3
br_0_0_39/atm4
br_0_0_40/atm5
No Interface/None

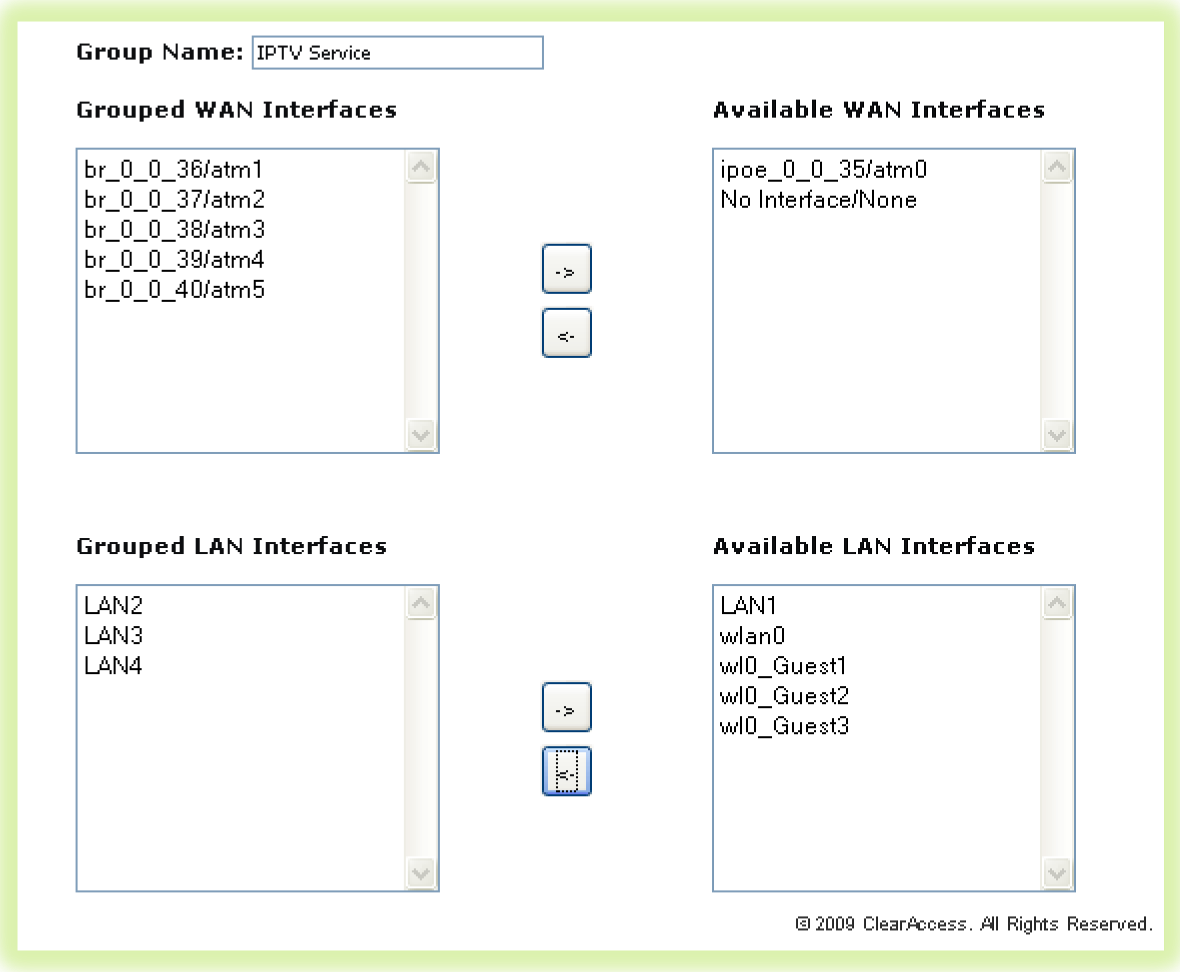
Grouped LAN Interfaces

Available LAN Interfaces

LAN1
LAN2
LAN3
LAN4
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

Figure 33 Defining an IPTV Bridge Interface Group

12. Enter the “Group Name.”
13. Highlight the bridged “WAN Interfaces” to be included in the bridge group and click **<-**.
14. Highlight the LAN Interfaces to be included in the bridge group and click **<-**.



Group Name: IPTV Service

Grouped WAN Interfaces

br_0_0_36/atm1
br_0_0_37/atm2
br_0_0_38/atm3
br_0_0_39/atm4
br_0_0_40/atm5

Available WAN Interfaces

ipoe_0_0_35/atm0
No Interface/None

Grouped LAN Interfaces

LAN2
LAN3
LAN4

Available LAN Interfaces

LAN1
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

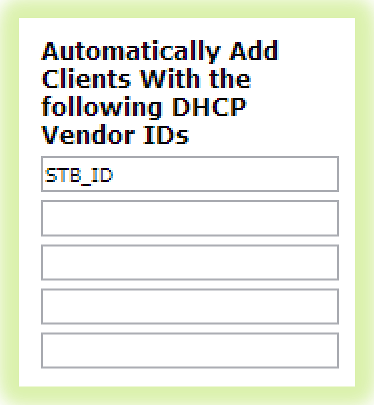
Figure 34 Typical IPTV Bridge Interface Group

15. Click **Apply/Save.**

Creating Vendor ID Based Interface (Bridge) Groupings

To provide greater flexibility when connecting set-top-boxes to LAN ports SmartRG gateways support “Vendor ID Based” bridge groupings. Instead of adding specific LAN ports to the bridge group, you can specify the Vendor ID of the set-top-box. Any traffic received on any LAN port containing the specified Vendor ID will be bridged to the designated bridged WAN connection.

To configure Vendor ID based interface groupings, add only the WAN interface(s) to the bridge group and then specify the required Vendor ID(s) in the following list:



Automatically Add Clients With the following DHCP Vendor IDs

STB_ID

Figure 35 Vendor ID Based Interface Groupings

Routed IPTV Configuration (Single WAN Connection)

The common routed IPTV configuration is virtually identical to the WAN connection configuration for Internet data services with one notable exception; the addition of quality of service (QoS).

While not an absolute requirement, applying QoS to LAN traffic (with higher priority given to STBs) ensures the timely and deterministic delivery of IPTV related uni-cast requests and IGMP signaling through the gateway. This provides repeatable, shortest time possible channel changes in the presence of other LAN traffic. A typical routed IPTV service configuration with only one WAN connection is shown below.

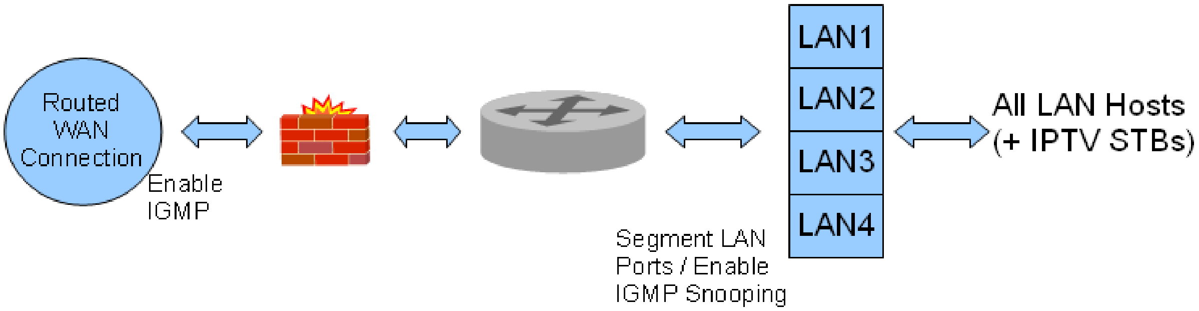

Routed WAN Connection
Enable IGMP
Segment LAN Ports / Enable IGMP Snooping
LAN1
LAN2
LAN3
LAN4
All LAN Hosts (+ IPTV STBs)

Figure 36 Routed IPTV Configuration (Single WAN Connection)

To configure the SmartRG for routed IPTV service deployments:

1. Ensure “IGMP Snooping” has been enabled on the LAN as detailed in, “Use Case: Setting Up the LAN.”
2. Create a routed WAN connection as detailed in, “Use Case: Creating WAN Connections for Internet Access and Remote Management.”
3. (Optional) Create traffic classifiers and priority queues for the various traffic categories on your LAN (e.g. Internet data, IPTV and VoIP) as detailed in, “Use Case: Applying Quality of S.”

NOTE	The SmartRG family of gateways employs “Differentiated Services” (RFC 2474) to provide IP traffic QoS. When configuring QoS for various traffic categories the following Differentiated Services Code Point (DSCP) values or suggested: • Internet data – Best Effort (DSCP 0) • IPTV – AF21 (DSCP 18) • VoIP – Expedited Forwarding (DSCP 46)

NOTE	Some STBs pre-mark their IP traffic making classification a relatively straightforward task for the gateway. If your STB pre-marks its traffic, passing the DSCP mark through

	unchanged is suggested.

Routed IPTV Configuration (Multiple WAN Connections)

It is also possible to create routed IPTV configurations with multiple WAN connections. The notable difference to typical routed IPTV configurations is the addition of one or more bridged WAN connections to support multiple multicast IPTV streams. Again QoS is suggested. A typical multi-WAN connection, routed IPTV service configuration is shown below.

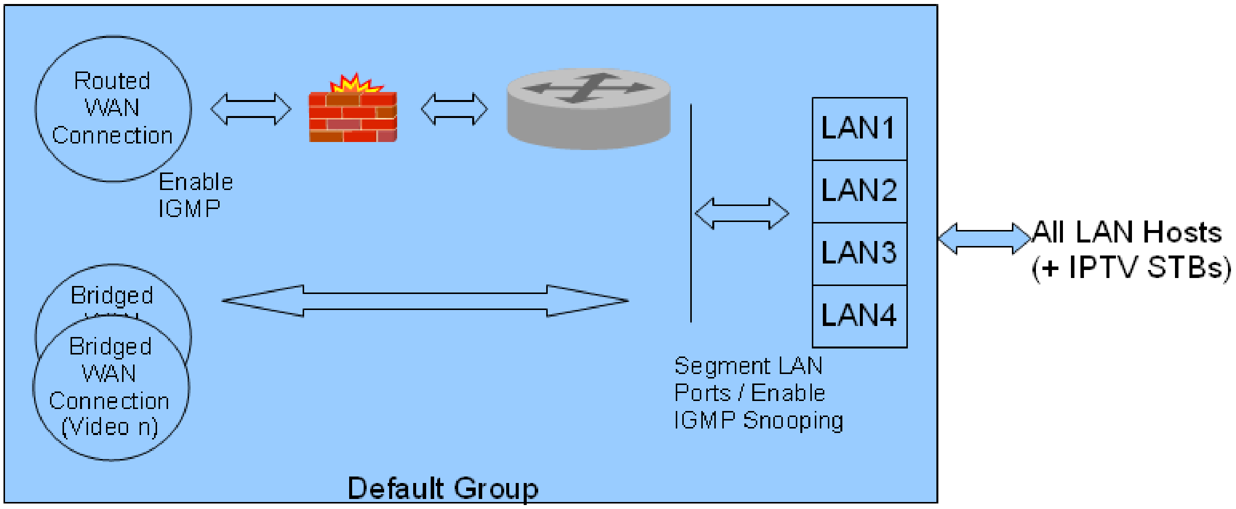

Routed WAN Connection
Enable IGMP
Bridged
Bridged WAN Connection (Video n)
LAN1
LAN2
LAN3
LAN4
All LAN Hosts (+ IPTV STBs)
Segment LAN Ports / Enable IGMP Snooping
Default Group

Figure 37 Routed IPTV Configuration (Multiple WAN Connection)

To configure the SmartRG for multi-WAN connection, routed IPTV service deployments, follow the single WAN connection, routed IPTV configuration instructions above –plus- add bridged WAN connections using the instructions detailed in, “Creating Bridged WAN Connections.”

Use Case: Applying Quality of Service (QoS) to VoIP and IPTV LAN Traffic

When deploying time critical services such as VoIP and IPTV comingled with common data services, it becomes necessary to prioritize the time critical, upstream LAN traffic over common data traffic (e.g Internet data and file transfers). Time critical traffic commonly includes SIP signaling (VoIP call setup/teardown) and IGMP signaling (IPTV channel change). The SmartRG line of gateways prioritizes time critical traffic using the "Differentiated Services Code Point" field in the IP header as defined by RFC 2474.

NOTE	The residential gateway plays no part in the prioritization of downstream traffic.

Traffic generated by LAN hosts such as VoIP phones, IPTV STBs and PCs is identified by "classifiers" and placed into prioritization "queues." Queues are emptied through the routed WAN connection based on queue priority. Classifiers can identify traffic based on a number of criteria including: source/destination MAC address, source/destination IP address, protocol, DSCP mark, etc. This section describes a *typical* QoS configuration to prioritized upstream VoIP and IPTV traffic.

A *typical* VoIP/IPTV/data QoS configuration is shown below:

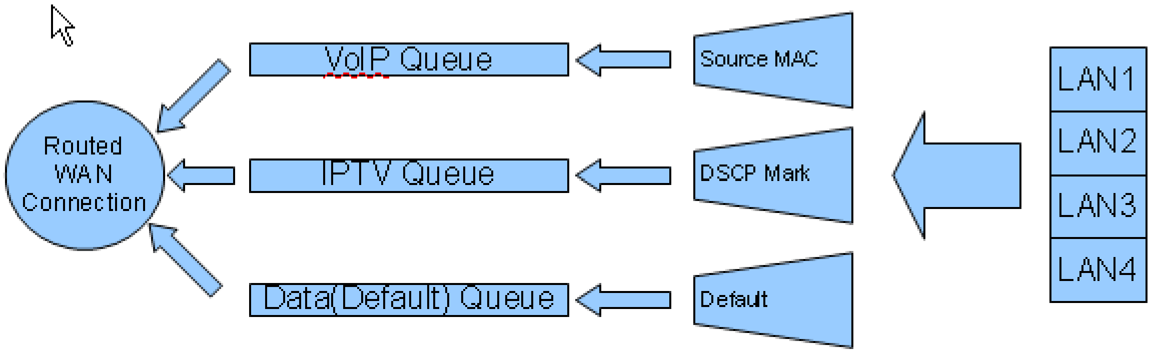


Figure 38 Typical QoS Configuration to Support VoIP and IPTV Services

VoIP traffic is identified by its source MAC/Mask (VoIP user agent OUI) and IPTV traffic is identified by the DSCP mark in its IP header. All remaining traffic is placed in the data (default) queue.

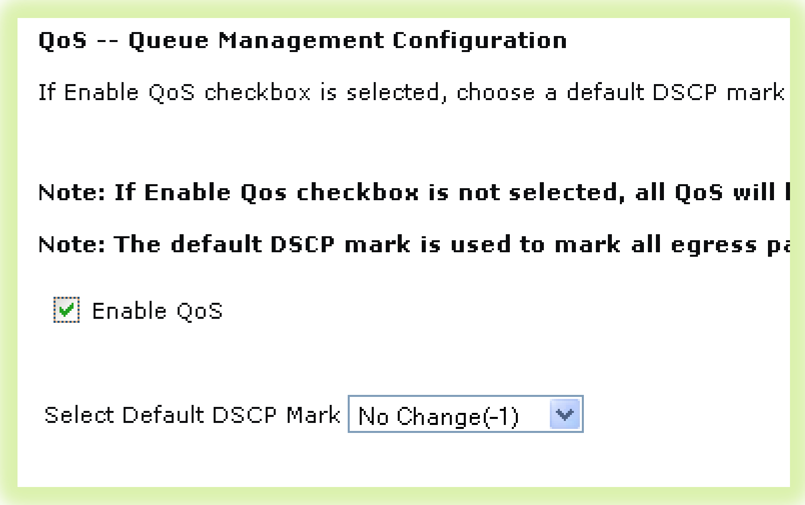
NOTE	Mediaroom based IPTV STBs place the **DSCP18** mark on all upstream traffic.

The QoS configuration process is comprised of three main steps:

- Enable QoS on the routed WAN connection and enable QoS processing
- Create traffic queues to prioritize the different types of traffic –and-
- Create traffic classifiers to identify the different types of traffic

To configure the SmartRG's QoS feature:

1. Ensure the layer 2 WAN interface "Enable Quality of Service" check box is checked as detailed in the Layer 2 Interface configuration sections.
2. Select *Advanced Setup -> Quality of Service -> QoS Config*



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark

Note: If Enable Qos checkbox is not selected, all QoS will l

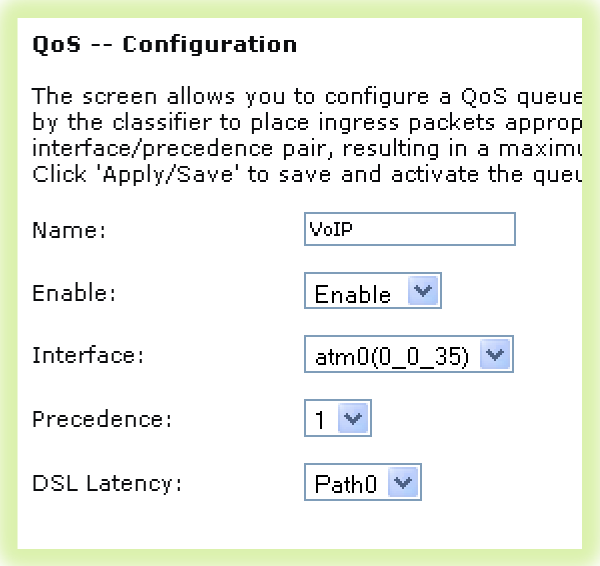
Note: The default DSCP mark is used to mark all egress pa

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

Figure 39 Enable SmartRG QoS Processing

3. Check "Enable QoS", set the "Default DSCP Mark" to "No Change(-1)" and click **Apply/Save.**
4. Create the VoIP queue by selecting *Advanced Setup -> Quality of Service -> QoS Queue Config* and click **Add.**



QoS -- Configuration

The screen allows you to configure a QoS queue
by the classifier to place ingress packets approp
interface/precedence pair, resulting in a maximu
Click 'Apply/Save' to save and activate the queu

Name: VoIP

Enable: Enable

Interface: atm0(0_0_35)

Precedence: 1

DSL Latency: Path0

Figure 40 QoS VoIP Queue Configuration

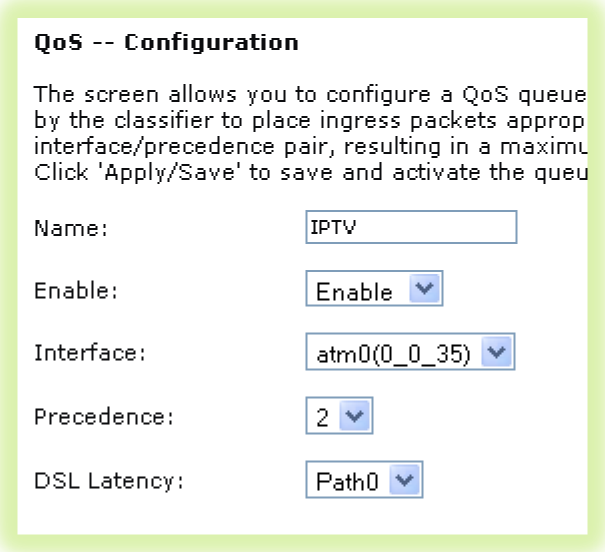
5. Name, enable and select the WAN interface to be fed by this queue.

IMPORTANT NOTE	Select the routed WAN interface created in the "Creating the WAN Service" section.

6. Select a "Precedence" of 1.

NOTE	Lower values of "Precedence" indicate HIGHER priority.

7. Leave the "DSL Latency" value set to Path0 and Click **Apply/Save**.
8. Create the IPTV queue by selecting *Advanced Setup -> Quality of Service -> QoS Queue Config* and click **Add**.



QoS -- Configuration

The screen allows you to configure a QoS queue
by the classifier to place ingress packets approp
interface/precedence pair, resulting in a maximu
Click 'Apply/Save' to save and activate the queu

Name: IPTV

Enable: Enable

Interface: atm0(0_0_35)

Precedence: 2

DSL Latency: Path0

Figure 41 QoS: IPTV Queue Configuration

9. Name, enable and select the WAN interface to be fed by this queue.

IMPORTANT NOTE	Again, select the routed WAN interface created in the "Creating the WAN Service" section.

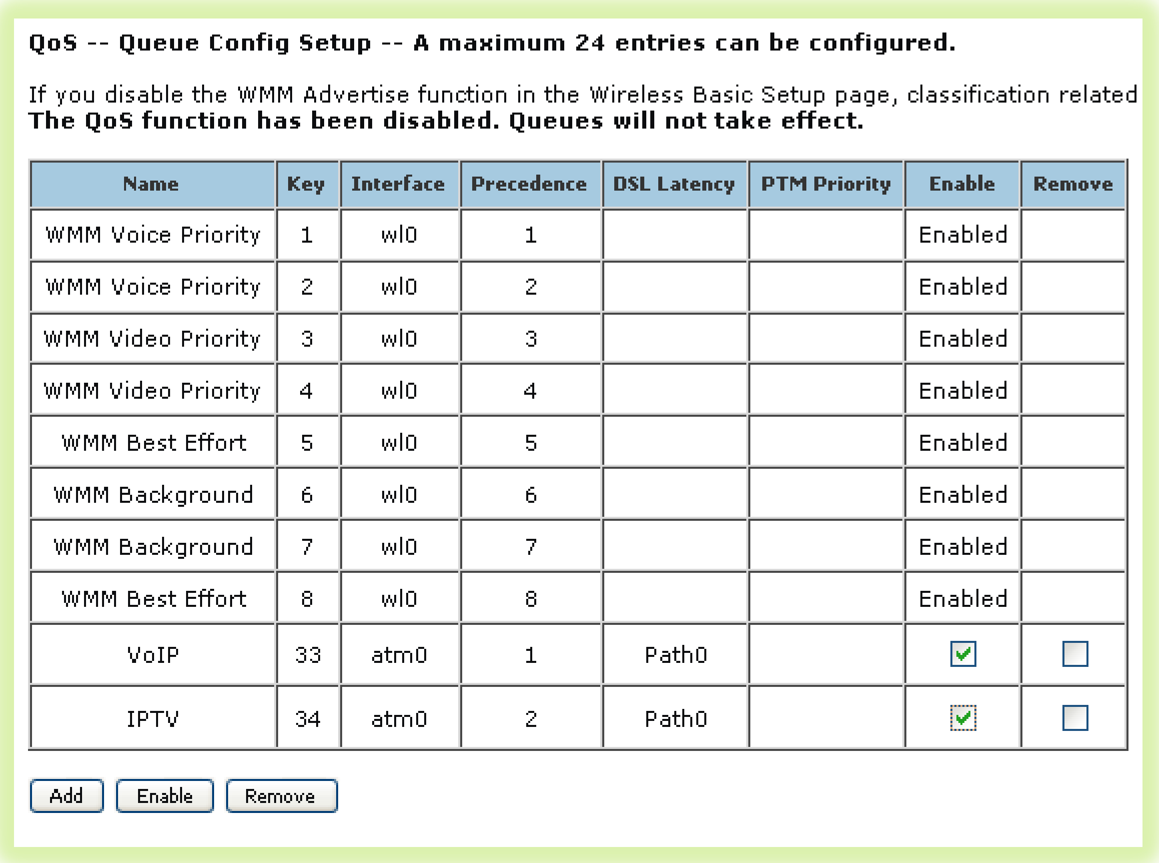
10. Select a "Precedence" of 2.

NOTE	IPTV traffic should be of LOWER priority (HIGHER Precedence value) than VoIP traffic.

11. Leave the "DSL Latency" value set to Path0 and Click **Apply/Save**.

NOTE	The default data queue depicted in the QoS architecture diagram above does not need to be specifically created.

12. Enable the newly created queues by selecting *Advanced Setup -> Quality of Service -> QoS Queue Config,* check the "Enable" boxes for the new queues and click **Enable**. The correct queue configuration for VoIP and IPTV services should look like:



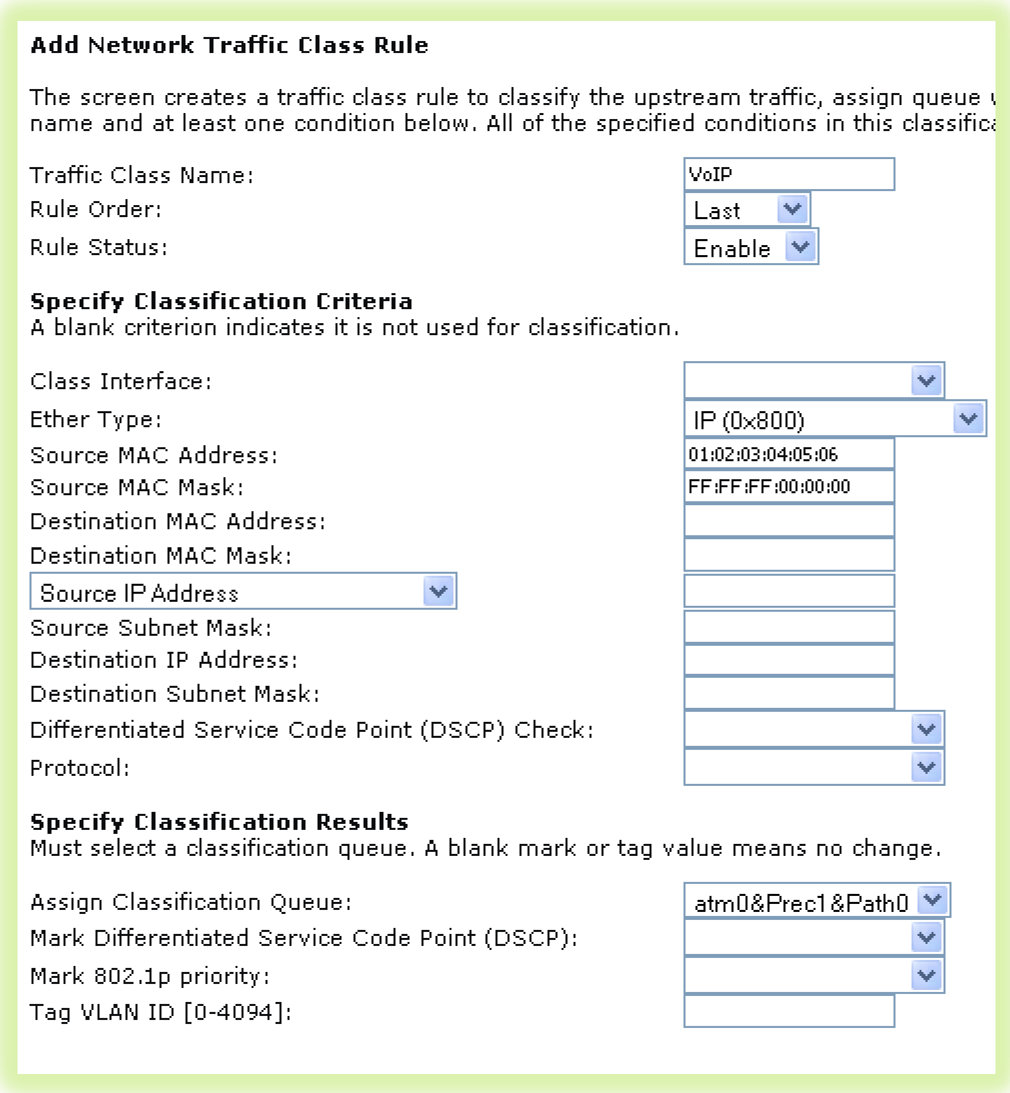
QoS -- Queue Config Setup -- A maximum 24 entries can be configured.

If you disable the WMM Advertise function in the Wireless Basic Setup page, classification related
The QoS function has been disabled. Queues will not take effect.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			Enabled	
WMM Voice Priority	2	wl0	2			Enabled	
WMM Video Priority	3	wl0	3			Enabled	
WMM Video Priority	4	wl0	4			Enabled	
WMM Best Effort	5	wl0	5			Enabled	
WMM Background	6	wl0	6			Enabled	
WMM Background	7	wl0	7			Enabled	
WMM Best Effort	8	wl0	8			Enabled	
VoIP	33	atm0	1	Path0		☑	☐
IPTV	34	atm0	2	Path0		☑	☐

Figure 42 QoS Queue Enable

13. Create the VoIP traffic classifier by selecting *Advanced Setup -> Quality of Service -> QoS Classification* and click **Add**.



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue
name and at least one condition below. All of the specified conditions in this classifica

Traffic Class Name:	VoIP
Rule Order:	Last
Rule Status:	Enable

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

Class Interface:	
Ether Type:	IP (0x800)
Source MAC Address:	01:02:03:04:05:06
Source MAC Mask:	FF:FF:FF:00:00:00
Destination MAC Address:	
Destination MAC Mask:	
Source IP Address	
Source Subnet Mask:	
Destination IP Address:	
Destination Subnet Mask:	
Differentiated Service Code Point (DSCP) Check:	
Protocol:	

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	atm0&Prec1&Path0
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID [0-4094]:	

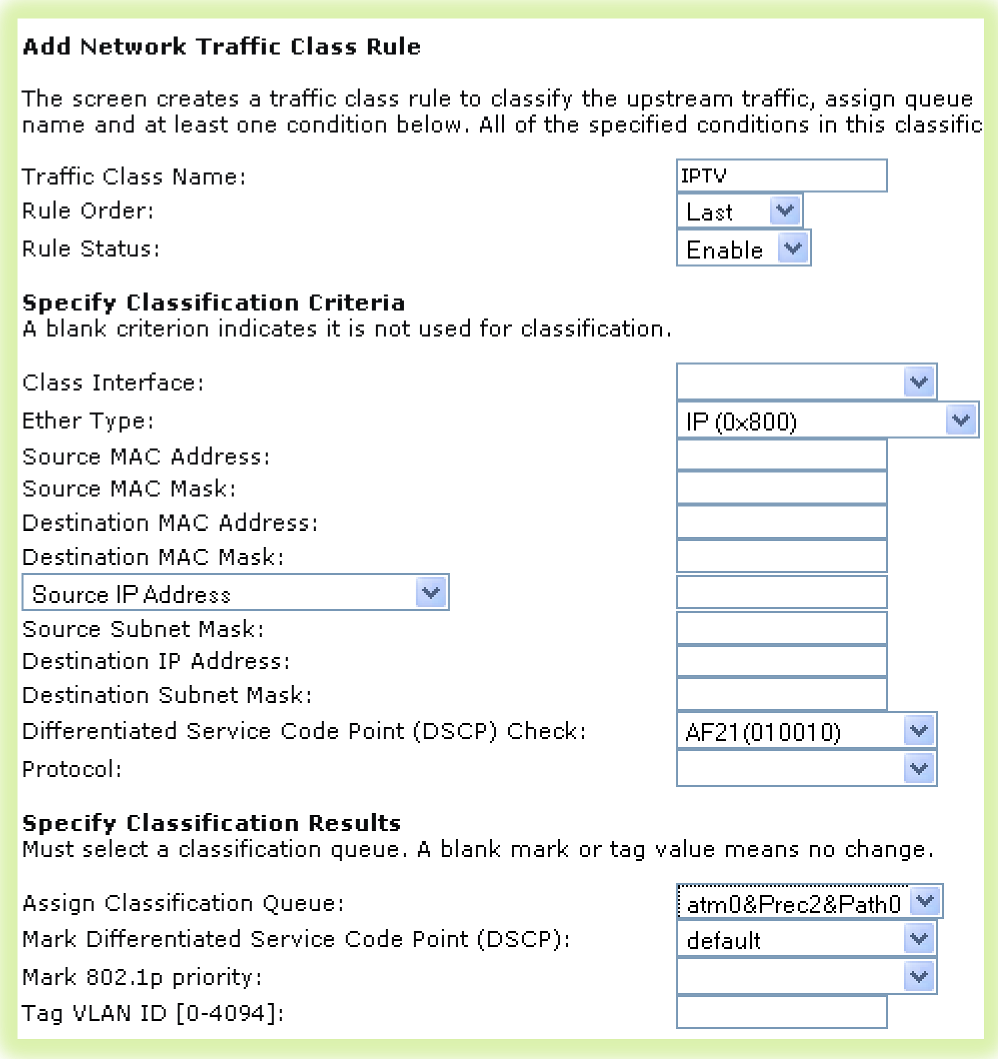
Figure 43 QoS VoIP Classifier Configuration

14. Set the Name, Rule Order, and enable the classifier rule.

IMPORTANT NOTE	**If you create the classifier rules in priority order (VoIP then IPTV), you may leave the "Rule Order" set to "Last." Each successive classifier rule created will become the last one checked in the traffic identification process.**

15. Select an "Ether Type" of IP (0x800).
16. Enter the source MAC and Mask values in 01:02:03:04:05:06/FF:FF:FF:00:00:00 format.
17. Assign the Classification Queue (identified by WAN interface&Precedence&Path).
18. Click **Apply/Save.**

19. Create the IPTV traffic classifier by selecting *Advanced Setup -> Quality of Service -> QoS Classification* and click **Add.**



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue name and at least one condition below. All of the specified conditions in this classific

Traffic Class Name:	IPTV
Rule Order:	Last
Rule Status:	Enable

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

Class Interface:	
Ether Type:	IP (0x800)
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Source IP Address	
Source Subnet Mask:	
Destination IP Address:	
Destination Subnet Mask:	
Differentiated Service Code Point (DSCP) Check:	AF21(010010)
Protocol:	

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	atm0&Prec2&Path0
Mark Differentiated Service Code Point (DSCP):	default
Mark 802.1p priority:	
Tag VLAN ID [0-4094]:	

Figure 44 QoS IPTV Classifier Configuration

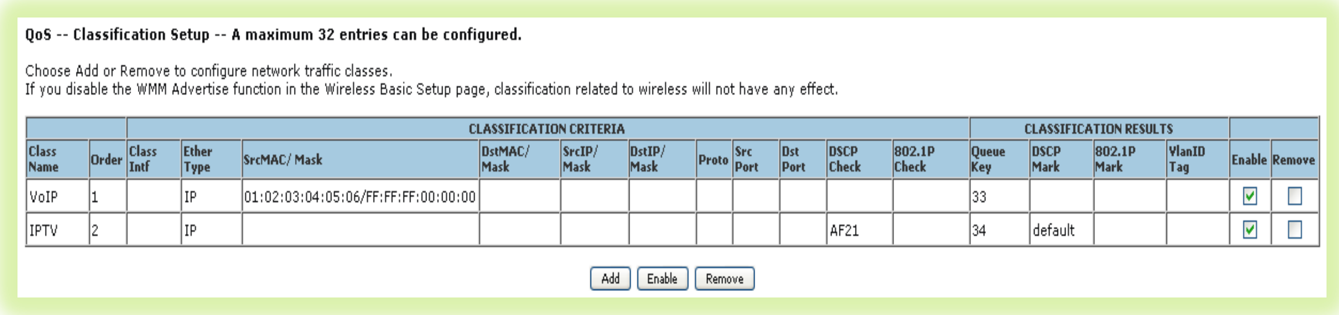
20. Set the Name, Rule Order, and enable the classifier rule.

IMPORTANT NOTE	If you create the classifier rules in priority order (VoIP then IPTV), you may leave the "Rule Order" set to "Last." Each successive classifier rule created will become the last one checked in the traffic identification process.

21. Select an “Ether Type” of IP (0x800).
22. Enter the “Differentiated Service Code Point (DSCP) Check” value.

NOTE	AF21 (DSCP18) is common for Mediaroom STBs.

23. Assign the Classification Queue (identified by WAN interface&Precedence&Path).
24. Click **Apply/Save.** The correct classifier configuration for VoIP and IPTV services should look like:



QoS -- Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable the WMM Advertise function in the Wireless Basic Setup page, classification related to wireless will not have any effect.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove
VoIP	1		IP	01:02:03:04:05:06/FF:FF:FF:00:00:00									33				☑	□
IPTV	2		IP								AF21		34	default			☑	□

Figure 45 QoS VoIP and IPTV Classifier Configurations

The QoS configuration is now complete.

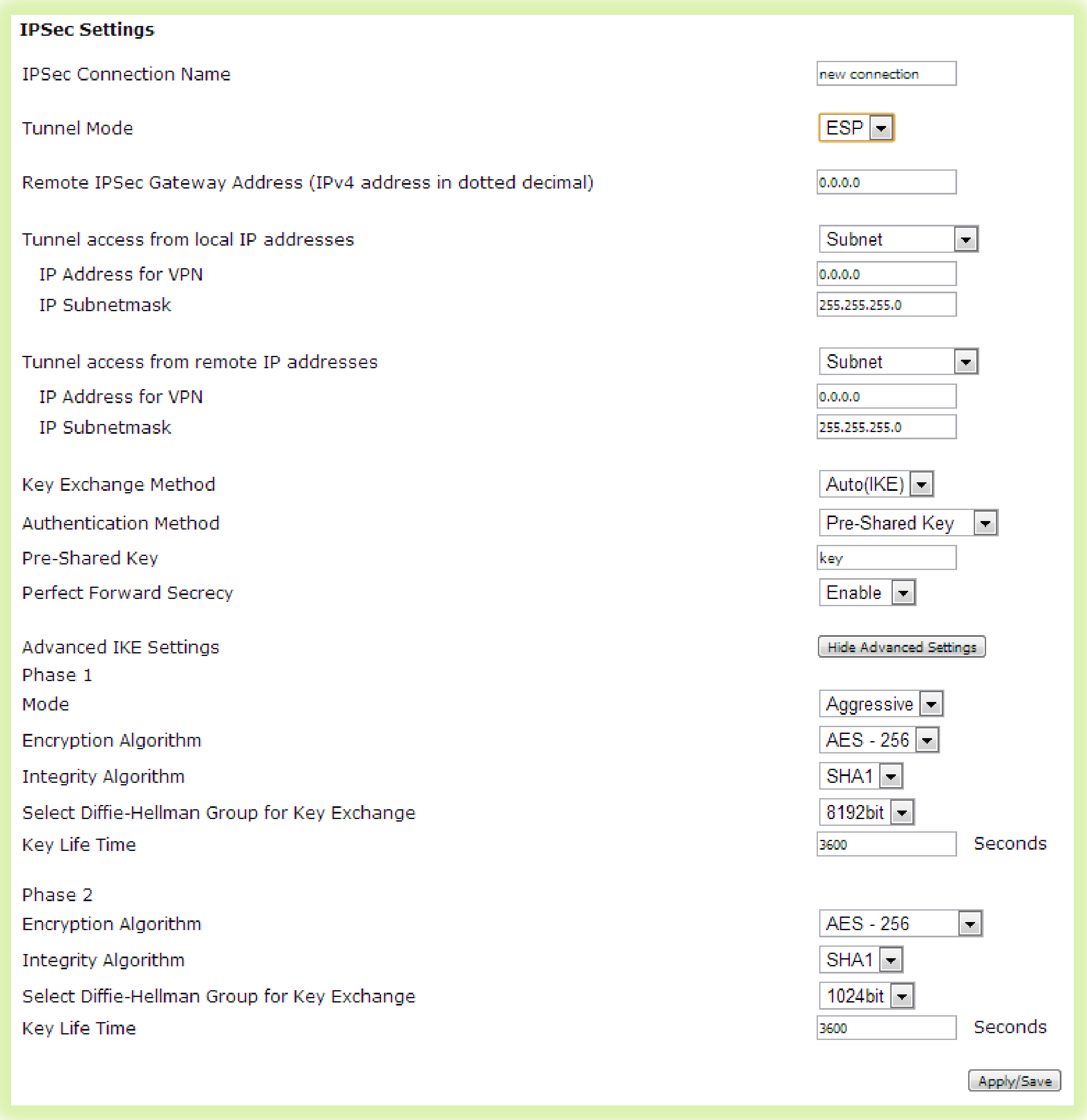
Use Case: Configuring IP Security (IPSec) in Support of VPNs

IP Security (IPSec) is a suite of IETF standards developed to provide data integrity and privacy, key management and data authentication at the IP layer. Typically IPSec is deployed to create Virtual Private Networks (VPNs) between communicating peers.

NOTE	When configuring an IPSec tunnel both ends of the tunnel must be configured with identical encryption and authentication methods.

To configure IPSec in the SmartRG gateway:

1. Select *Advanced Setup -> IPSec*
2. Click *Add New Connection* and then click *Show Advanced Settings* to bring up the following screen:



IPSec Settings

IPSec Connection Name	new connection	
Tunnel Mode	ESP	
Remote IPSec Gateway Address (IPv4 address in dotted decimal)	0.0.0.0	
Tunnel access from local IP addresses	Subnet	
IP Address for VPN	0.0.0.0	
IP Subnetmask	255.255.255.0	
Tunnel access from remote IP addresses	Subnet	
IP Address for VPN	0.0.0.0	
IP Subnetmask	255.255.255.0	
Key Exchange Method	Auto(IKE)	
Authentication Method	Pre-Shared Key	
Pre-Shared Key	key	
Perfect Forward Secrecy	Enable	
Advanced IKE Settings	Hide Advanced Settings	
Phase 1		
Mode	Aggressive	
Encryption Algorithm	AES - 256	
Integrity Algorithm	SHA1	
Select Diffie-Hellman Group for Key Exchange	8192bit	
Key Life Time	3600	Seconds
Phase 2		
Encryption Algorithm	AES - 256	
Integrity Algorithm	SHA1	
Select Diffie-Hellman Group for Key Exchange	1024bit	
Key Life Time	3600	Seconds

3. Enter a name for the IPSec connection.
4. Select the Tunnel Mode. "Authentication Header" (AH) protects both the IP payload and the IP header. "Encapsulating Security Protocol" (ESP) protects the original IP payload and

header by encapsulating it in an additional IP header. The outer IP header remains unprotected.

5. Enter the IP address of the tunnel's remote IPSec gateway.
6. Select either a single IP address or a subnet of IP addresses for the local end of the IPSec tunnel.
7. Enter either the single local IP address or the local subnet definition.
8. Select either a single IP address or a subnet of IP addresses for the remote end of the IPSec tunnel.
9. Enter either the single remote IP address or the remote subnet definition.
10. Select the Key Exchange Method. Keys can be exchanged manually (set identically on both ends) or automatically using "Internet Key Exchange" (IKE). This example assumes the selection of IKE.
11. Select the Authentication Method. Authentication can be performed either with a "Pre-Shared Key" or a certificate. This example assumes the selection of a Pre-Shared Key.
12. Enter the Pre-Shared Key value. Both character and hexadecimal values are acceptable (e.g. 0x123abc456def789 or VPN@tunnel_123)
13. Enable/Disable Perfect Forward Secrecy. PFS ensures the same key will not be generated again forcing a new Diffie-Hellman key exchange. This prohibits hackers from snooping a present transmission to decipher a key and then use that key to observe future data transmissions.
14. Set the Phase 1 Advanced IKE Settings (establish a secure, authenticated channel):
    a. Select the Mode: "Main" mode is more secure but adds delay. "Aggressive" mode is faster but less secure.
    b. Select the Encryption Algorithm: AES-256 is the most secure.
    c. Select the Integrity Algorithm: MD5 is a one way hash with a 128 bit digest. SHA1 is a one way hash with a 160 bit digest.
    d. Select the Diffie-Hellman Group for Key Exchange. Diffie-Hellman is a cryptography protocol enabling two devices to establish a shared secret via unsecured channels. More bits provide greater security but come with increased time for key computation.
    e. Specify the Key Life Time. Keys will be renewed after this interval.
15. Set the Phase 2 Advanced IKE Settings (generate keys and negotiate the IPSec Security Association):
    a. Repeat steps 14b-14e.
16. Click *Apply/Save.*

Managing Your SmartRG™ Gateway

Save, Restore or Default Configurations

To save the existing gateway configuration to your hard drive:

1. Select *Management -> Settings -> Backup.*
2. Click **Backup xxx Settings.**

NOTE	Two types of settings are available for backup: - Running Settings: settings governing the gateway's operation at the present time - Default Settings: settings restored at the time of a factory default You have the ability to create your own custom default settings.

To restore a previously saved gateway configuration as the gateway's *running* settings:

1. Select *Management -> Settings -> Update.*
2. Click the **Choose File** button (under the "Update working settings" section) and browse to find the saved config file on your hard drive (e.g. mySmartRGRunningConfig.conf)
3. Click **Update Working Settings.**

To restore a previously saved gateway configuration as the gateway's *default* settings:

1. Select *Management -> Settings -> Update.*
2. Click the **Choose File** button (under the "Update Default Broadband Router settings" section) and browse to find the saved config file on your hard drive (e.g. mySmartRGDefaultConfig.conf)
3. Click **Update Settings.**

To restore the gateway to default settings:

1. Select *Management -> Settings -> Restore Defaults.*
2. Click **Restore Default Settings.**

Update Software

To update the gateway's software:

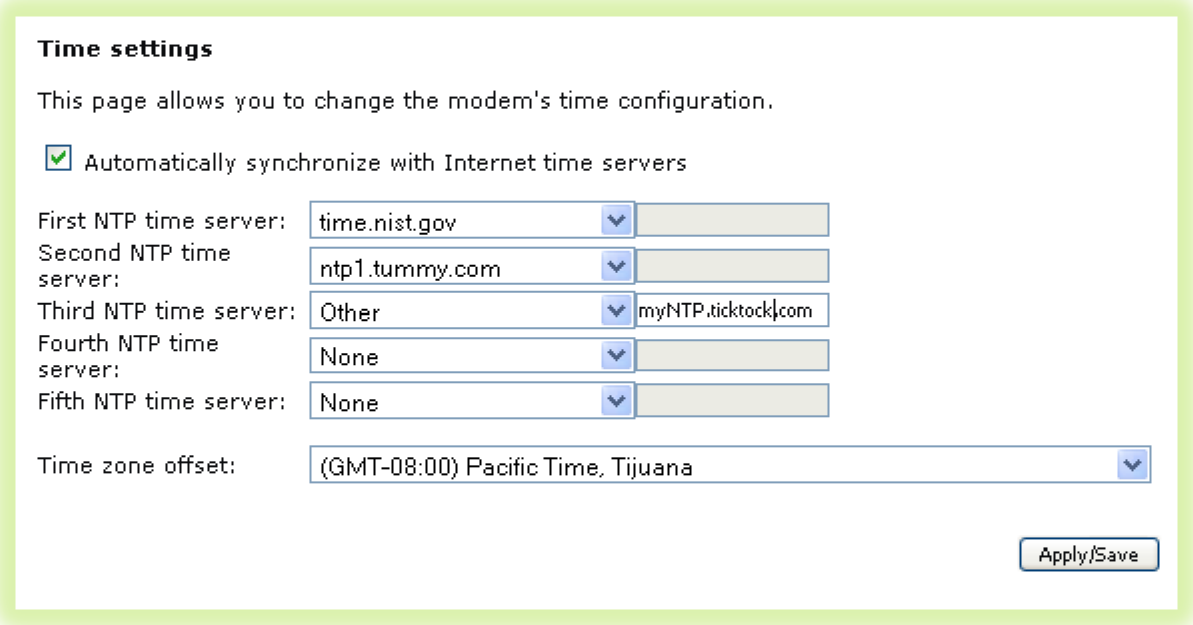
1. Select *Management -> Update Software.*
2. Browse to find the new gateway software on your hard drive (ex: *CA_2.4.3.7_24282_SR500N_fs_kernel*)
3. Click **Update Software.**

NOTE	The software update process takes approximately 2 minutes to complete. Do NOT power cycle the gateway until the software update process has completed.

Configure Time Settings

To set the gateway's time zone and NTP server settings:

1. Select *Management -> Internet Time.*
2. Select your time zone from the drop down list.
3. (Optional) Select the first, second … NTP servers from the drop down lists. (A custom NTP server can be configured by selecting "Other" from the drop down list and entering the custom URL.)



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:	Other	myNTP.ticktock.com
Fourth NTP time server:	None	
Fifth NTP time server:	None	
Time zone offset:	(GMT-08:00) Pacific Time, Tijuana	

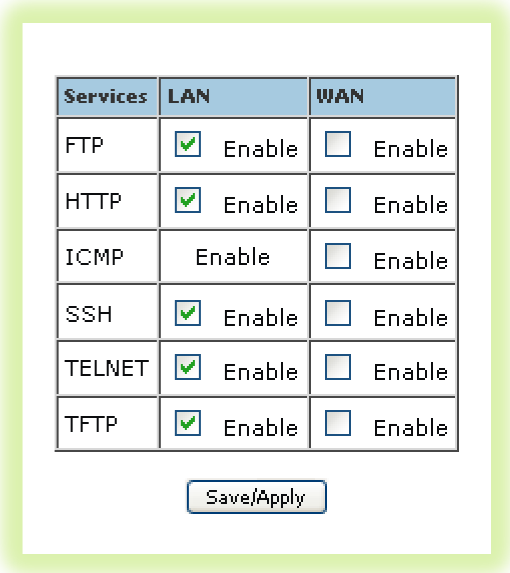
Figure 46 Time Zone and NTP Server Settings

4. Click **Apply/Save.**

Configure Access Controls (HTTP, Telnet, SSH, etc.)

To enable/disable gateway management services such as HTTP, Telnet and SSH:

1. Select *Management -> Access Control -> Services.*



Services	LAN	WAN
FTP	☑ Enable	□ Enable
HTTP	☑ Enable	□ Enable
ICMP	Enable	□ Enable
SSH	☑ Enable	□ Enable
TELNET	☑ Enable	□ Enable
TFTP	☑ Enable	□ Enable

Figure 47 Enabling/Disabling HTTP, Telnet, SSH... Access

2. Enable/disable LAN and/or WAN access to the various management services as desired .
3. Click **Save/Apply.**

NOTE	For security reasons it is strongly recommended that WAN access to all services be disabled accept during deployment or when troubleshooting.

Configure User Logins

SmartRG gateways support the following user roles:

- admin – unrestricted access by a PC connected to a LAN port
- support – unrestricted access by an ISP technician connected through the managed WAN interface

To change user passwords:

1. Select *Management -> Access Control -> Passwords.*
2. Enter the username (admin –or- support).
3. Enter the old password and the new password.
4. Click **Apply/Save.**

NOTE	Default username/password values are: - admin/admin (when accessed from the LAN) –and- - support/support (when accessed from the WAN)

Reset the Gateway

Hardware Reset

Reset the gateway by inserting a paper clip or similar tool into the reset switch hole located on either the rear or the bottom of the gateway (depending upon model). Press the switch briefly to reset the device.

Hardware Reset (to Factory Default Settings)

To reset the gateway to its factory default settings press the reset switch for 6 to 8 seconds. After releasing the reset switch the gateway will continue booting with a factory default configuration.

IMPORTANT	Pressing the reset switch for more than 10 seconds causes the SmartRG gateway to reset into its *boot image* rendering the gateway non-functional. This condition can be detected by: • the inability to access the SmartRG gateway's user interface using your web browser –and- • the inability to properly establish a WAN connection To correct this condition simply cycle power on the gateway.

Software Reset

To reset the gateway using the SmartRG gateway's web UI:

1. Select *Management -> Reboot.*
2. Click **Reboot.**

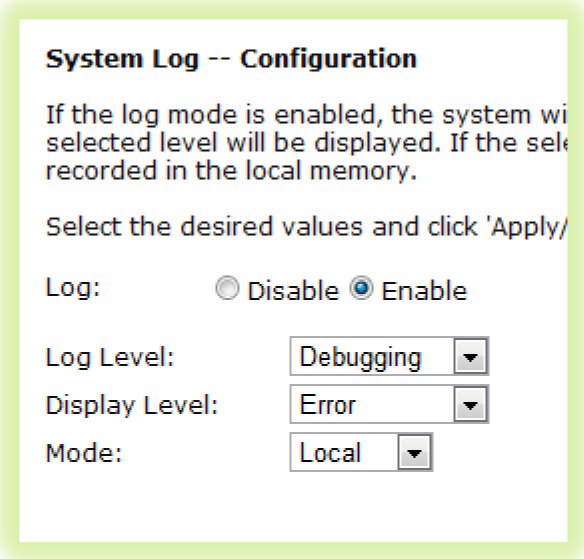
NOTE	Software resets, hardware resets and power cycles behave identically.

Troubleshooting

Accessing System Logs

To configure the System Log for use during troubleshooting efforts:

1. Select *Management -> System Log.*
2. Click **Configure System Log.**



System Log -- Configuration

If the log mode is enabled, the system wi
selected level will be displayed. If the sele
recorded in the local memory.

Select the desired values and click 'Apply/

Log: ○ Disable ● Enable

Log Level: Debugging

Display Level: Error

Mode: Local

Figure 48 Configuring the System Log for Use In Troubleshooting

3. Select the “Log Level” from the drop down list. “Debugging” provides the greatest level of log detail.
4. Select the “Display Level” from the drop down list. “Debugging” provides the greatest level of display detail.
5. Click **Apply/Save.**

NOTE	Gateway logs can be sent to a remote server for storage. To configure the remote “Mode” select “Remote” from the drop down list and configure the remote server’s IP address and UDP port number.

Executing Diagnostics

To execute the SmartRG's interface diagnostics:

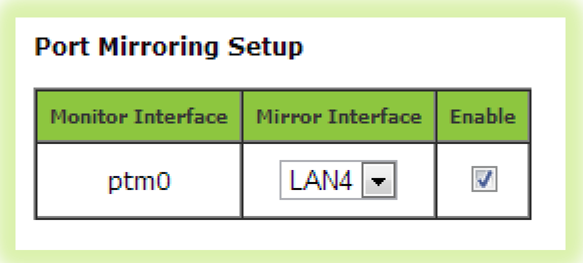
1. Select *Diagnostics.*

Monitoring Traffic on the WAN Interface (Port Mirroring)

Monitoring traffic on the WAN interface can be difficult as intervening equipment between the access gear and the gateway is necessary to provide a monitoring point for your work station. To simplify WAN traffic monitoring SmartRG gateways provide the capability of "mirroring" WAN traffic to any of the gateway's Ethernet LAN ports.

To configure the SmartRG gateway for port mirroring:

1. Enter the URL for the "Port Mirroring" hidden page into your browser: <LAN IP Address>/admin/engdebug.cmd.
2. Click the Enable check box.
3. Select the target LAN port from the Mirror Interface dropdown box.
4. Click Apply/Save.



Port Mirroring Setup

Monitor Interface	Mirror Interface	Enable
ptm0	LAN4 ▾	☑

Figure 49 Configuring Port Mirroring to Monitor WAN Interface Traffic

Contacting SmartRG Technical Support

For technical support contact:

Support

Monday – Friday, 5am-6pm Pacific Time (UTC-8:00)

1-360-859-1780

1-877-486-6210 (Toll free from the US & Canada)
support@smartrg.com