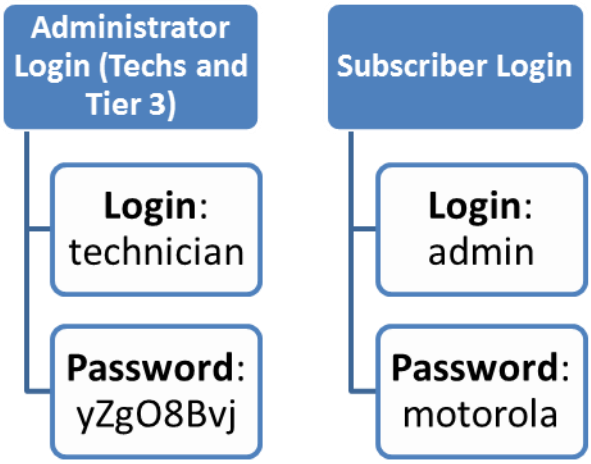
Optimizing the Motorola AWG Wireless Connectivity

Purpose:

This job aid details the proper settings and troubleshooting for Motorola DOCSIS 3.0 Advanced Wireless Gateways. These processes apply to all Tier 3 groups in the East Region.

Basic Modem Information (Example: RF Cable MAC = A47AA434B958, Model = SBG6580)

- **Default Wireless SSID** = Model + last 2 of RF MAC (all caps)
  - Example – SBG658058
- **Default Wireless Key** = Model + last 6 of RF MAC (all caps)
  - Example – SBG658034B958
- **Default Wireless Encryption** = WPA-PSK
- **Compatibility**: DOCSIS 3/2/1.x, Wireless 802.11 a/b/g/n
- **Admin Access IP**: 192.168.0.1
  - Client will enter in browser address bar while using a wired connection



Note: with firmware 3.1.0.0 password "8mb1t3M3" , firmware 3.2.1.0 "M0t0R01a"

Modem Details:

The lights on the Motorola DOCSIS 3.0 AWGs will vary from model to model, however several lights are on all models.

Light	POWER	RECEIVE	SEND	ONLINE	WIRELESS
Status	Solid	Solid	Solid	Solid	Solid or Flash

Some Motorola DOCSIS 3.0 AWGs have a WPS light, indicating whether or not advanced security encryption is enabled for the wireless home network. This option can be turned on and off using a button on the modem, as well as through an option in the interface. It is recommended that clients use advanced security encryption (WEP or WPA).

Optimizing the Motorola AWG Wireless Connectivity

Basic Wireless Settings:

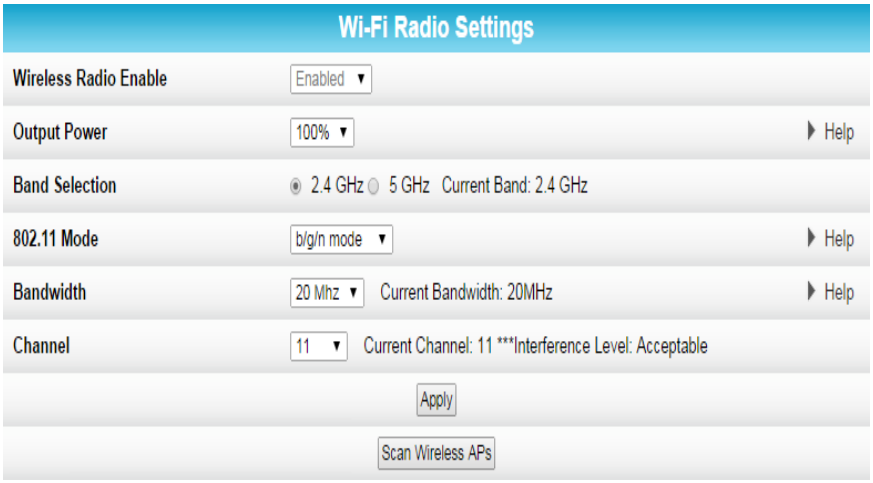
Step 1: Select WIRELESS from the top menu

Step 2: Select 802.11 Radio from the drop down menu

Wireless: Leave Enabled unless bridging the AWG.

Output Power: Leave at the 100% default for maximum signal strength/range.

802.11 Band: Leave at 2.4 Ghz.



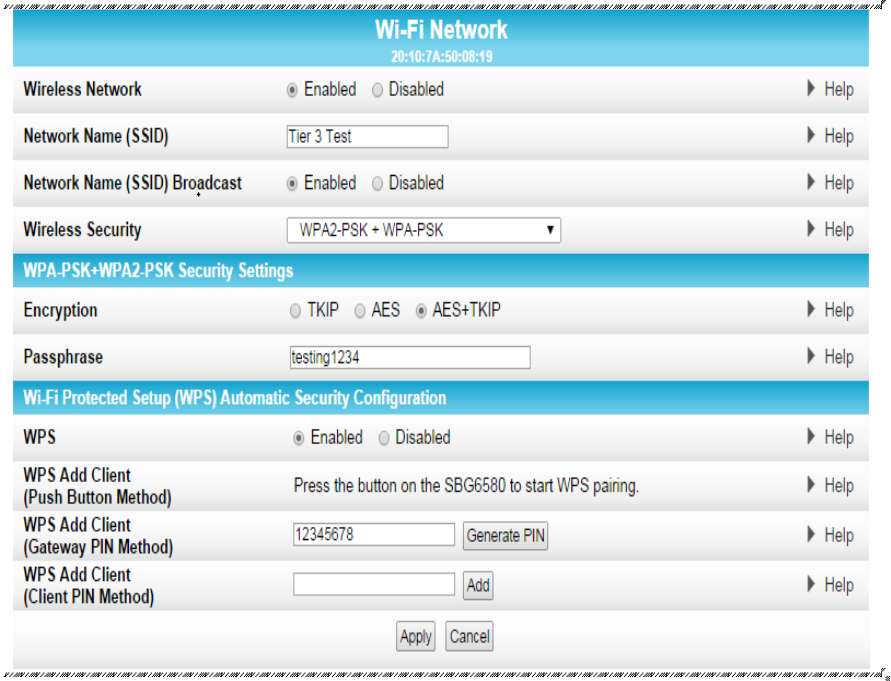
Control Channel: Change the channel to minimize interference from other wireless devices in or around the home (cordless phones, baby monitors, etc.).

Step 1: Select WIRELESS from the top menu

Step 2: Select Primary Network Settings from the drop down menu

Primary Network: Leave Enabled unless bridging the AWG.

Closed Network: Enable to stop broadcast of SSID. You must disable WPS for the Enable option to appear.



WPA vs. WPA2: It is preferred to enable both WPA and WPA2 as many devices a client owns may require the lower tier security (WPA). You must enable the PSK version of both when the client chooses to use a password on their network. TKIP is used for WPA and AES is used for WPA2.

WEP: Only use WEP as the security encryption method when the client owns a WEP-only device, such as a Nintendo DS.

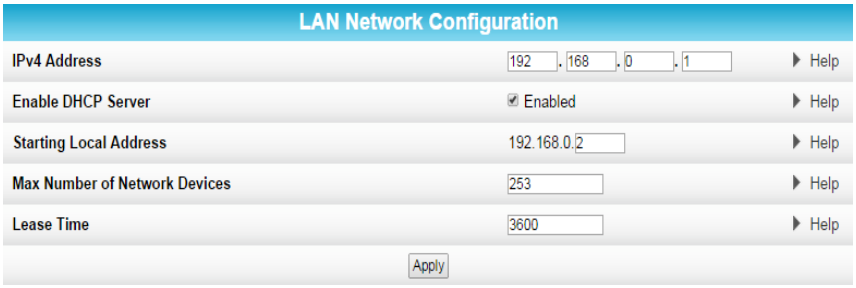
Optimizing the Motorola AWG Wireless Connectivity

Advanced Wireless Settings:

Step 1: Select BASIC from the top menu

Step 2: Select DHCP from the drop down menu

Lease Time: Change to 86400 to avoid IP conflicts with devices that go into sleep mode (laptops)



Advanced Gateway Settings:

Step 1: Select ADVANCED from the top menu

Step 2: Select Options from the drop down menu

Enable the following options as needed:

- Ipsec PassThrough – optimizes for traditional VPN with full access to systems
- PPTP PassThrough – optimizes for limited VPN setups with access to intranet sites and email
- Multicast Enable – optimizes for streaming video content
- UPnP Enable – optimizes for online gaming

Disable the following options:

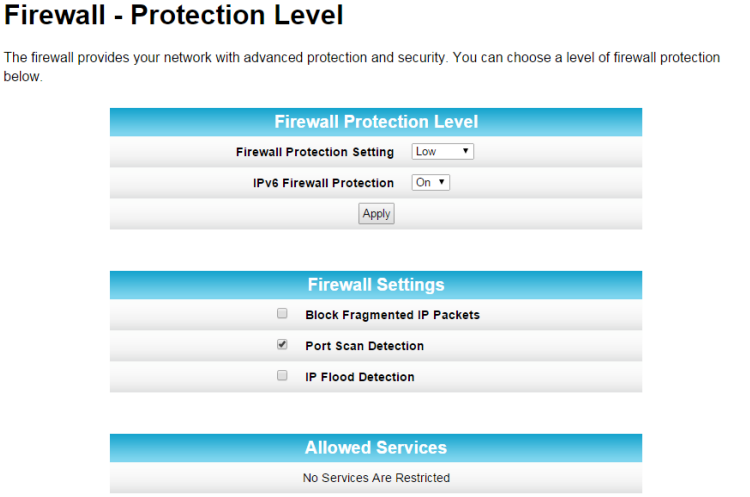
- WAN Blocking – blocks the ability of devices to request connections
- SIP ALG – disable when the client uses VoIP software and programs
- RG PassThrough – disables NAT operations, thus forcing a "bridge" status [NEVER ENABLE]

Firewall Content Filter:

Step 1: Select FIREWALL from the top menu

Step 2: Select Protection Level from the drop down menu

Step 3: Ensure the AWG settings match the screenshot to the right



Optimizing the Motorola AWG Wireless Connectivity

Signal Attenuation:

Signal Attenuation and performance drops can result when the wireless signal is absorbed by an object or material, or as the wireless client moves farther away from the Wireless Gateway. This table illustrates rule of thumb attenuation (dB loss) for different kinds of materials.

Material	Attenuation (dB)	
	2.4 Ghz	5.0 Ghz
Interior Drywall	3 – 4	3 – 5
Cubicle Wall	2 – 5	4 – 9
Wood Door	3 – 4	6 – 7
Brick/Concrete Wall	6 – 18	10 – 30
Glass/Window (non tinted)	2 – 3	6 – 8
Double-Pane Coated Glass	13	20

Follow the steps below to view the current signal strength for connected devices. Have the client move the device closer to the gateway to increase signal strength. Reducing barriers between the device and the gateway (walls, doors, etc.) can greatly improve connectivity performance. Optimal levels per device range from 0 to -65 dB. Devices outside this range may experience slow speeds and dropped connections.

Step 1: Select WIRELESS from the top menu

Step 2: Select Access Control from the drop down menu

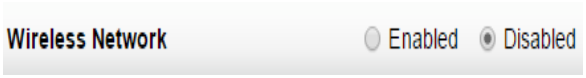
Step 3: View the Connected Clients chart

Bridging the Gateway:

Some clients choose to bridge their AWG so they can use their own router. Before bridging the AWG, inform your client that bridging the gateway will result in TWC's inability to effectively troubleshoot the wireless connectivity within their home network. Once bridged, TWC can only troubleshoot the connection to the router. Connectivity beyond the router will be the full responsibility of the client.

Step 1: Select WIRELESS from the top menu

Step 2: Select Primary Network Settings from the drop down menu



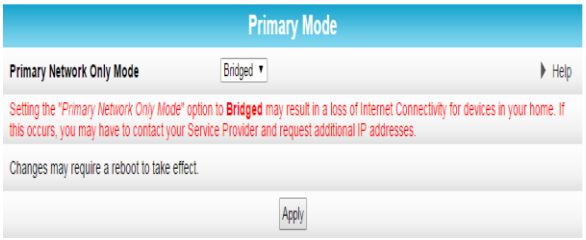
Step 3: Select Disabled from the Wireless Network section

Step 4: Click Apply

Step 5: Select BASIC from the top menu

Step 6: Select Setup from the drop down menu

Step 7: Set the Primary Network Only Mode to **Bridged**



Step 8: Click Apply

Optimizing the Motorola AWG Wireless Connectivity

Creating a DMZ:

A DMZ, or demilitarized zone, is often used for devices which only use an internet connection for a single purpose. The DMZ allows all communication to and from the device to bypass the firewall built into the gateway. The gateway allows for only one device to be set into a DMZ at a time. DMZs should only be used for devices such as gaming systems (PS3, PS4, Xbox360, XboxOne) and wireless printers.

Follow the steps below to create a DMZ for a device.

Step 1: Create a **Static IP** for the device. Select WIRELESS from the top menu

Step 2: Select Access Control from the drop down menu

Step 3: Note the IP Address currently assigned to the device you are creating the DMZ for

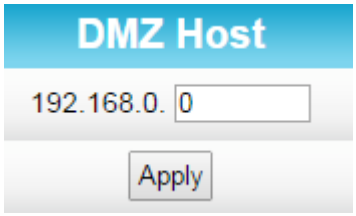
Step 4: Select BASIC from the top menu

Step 5: Select DHCP from the drop down menu

Step 6: Enter the MAC Address and desired IP Address for the device into the appropriate fields and select Apply

Step 7: Select ADVANCED from the top menu

Step 8: Select DMZ Host from the drop down menu



Step 9: Enter the last section of the assigned IP address and click the Apply button

Optimizing the Motorola AWG Wireless Connectivity

Setting Up Port Forwarding or Triggering:

Ports are the paths used for communication from the client device to the web servers they access (such as online gaming servers). For programs which require extensive downloads or which require a constant open-pathway such as VoIP tools, clients can set up Port Forwarding or Port Triggering.

Port Forwarding opens designated ports for specific devices on the home network. Prior to setting up port forwarding, a static IP address should be assigned to the device in question. To set up a static IP address for a specific device, follow steps 1 through 6 on page 5. Once a static IP has been reserved, follow the steps below. Most ports can be found at portforward.com.

Note: Remember to set a static IP address for port forwarding, instructions found in DMZ section.

Step 1: Select ADVANCED from the top menu

Step 2: Select Port Forwarding from the side menu

Step 3: Click Create IPv4 and start by putting in the Local IP address you set to static for the device.

Step 4: Enter the low range port under Start Port, the high range port under End Port, select the Protocol (TCP/UDP/Both), and the Description.

Step 5: Set the Enabled option to On and click the Apply button.

Port Triggering does not specify a device for the ports to be opened to. Therefore, setting up port triggering will open the designated ports for all devices on the home network. Follow the steps below to set up port triggering.

Step 1: Select ADVANCED from the top menu

Step 2: Select Port Triggers from the side menu

Step 3: Click Create Port Triggers

Step 4: Enter the low range port under Start Port, the high range port under End Port under both Trigger Range AND Target Range, then select the Protocol (TCP/UDP/Both), and enter a description.

Step 5: Set the Enabled option to On and click the Apply button.

Optimizing the Motorola AWG Wireless Connectivity

Troubleshooting Scenarios:

There are two basic scenarios clients will contact us for in reference to their AWGs. Both scenarios assume you have already checked the account using the BOB method (Billing > Outages > Balancing)

No Connectivity:

1. Ensure the modem is online and you are able to log in
    a. Modem offline – check physical connections > schedule a TC
    b. Modem online – check signal levels
        i. Poor signal levels
            1. Check physical connections
            2. Move AWG as far from the other equipment as possible [a few feet can have a dramatic affect on signal strength] – Proceed to Step 2
        ii. Proper signal levels – Proceed to Step 2
2. Confirm device appears in AWG Connected Client list [Wireless > Access Control] – Device present?
    a. Yes – Proceed to "Slow Connectivity" troubleshooting steps [Step 1b for a wired device or 1c for a wireless device]
    b. No – Proceed to Step 3
3. Confirm Wireless network is enabled [Wireless > Primary Network] – Proceed to Step 4
4. Confirm SSID/Password [Wireless > Primary Network] – Proceed to Step 5
5. If device still cannot get online, check the following items.
    a. Does the device have an active Wi-Fi adaptor/Network card? – Educate Client
    b. Is the device capable of understanding the encryption method (WEP vs. WPA/WPA2)?
        i. Disable encryption and check device. If this works, the device itself is the problem.
    c. Does the device itself have an old IP address saved?
        i. Have client powercycle their device. If this does not work, proceed to Step 6.
6. Confirm DHCP settings are correct. [Basic > DHCP]
    a. DHCP Server set to "Yes" and number of CPEs set to "252" – Proceed to Step 7
7. Confirm RG PassThrough is disabled [Advanced > Options] – Proceed to Step 8
8. Confirm AWG is not bridged. [Basic > Setup] – Enable NAPT Mode
    a. Can any devices get online?
        i. Yes – Wireless devices only
            1. Check the physical Ethernet/USB connection to the wired devices, including the "Link" lights around the port.
                a. Link lights on – A setting in the client's computer/device is blocking the connection. Follow standard demarcation guidelines.
                b. Link lights off – Have the client try to connect to another port on the AWG. If the other ports do not work, have the client try a hardline connection with another device using the same port on the AWG. If another device works, it is a problem with the client's device. They will need to contact the manufacturer of their device. If the second device does not work, schedule a TC.
        ii. No devices able to get online
            1. Check BIN file, Firmware version and IP assignment to the AWG.
            2. Reset via CMTS in NYROC. If this does not fix the problem, schedule a TC.

Optimizing the Motorola AWG Wireless Connectivity

Troubleshooting Scenarios Continued:

Slow Connectivity:

1. Is the client experiencing slow connectivity on all or only some devices?
    a. All devices – Check signal levels in NYROC
        i. Poor signal levels
            1. Check physical connections
            2. Move AWG as far from the other equipment as possible [a few feet can have a dramatic affect on signal strength]
        ii. Proper signal levels – Check BIN file and Firmware version to the AWG
            1. BIN File and Firmware correct?
                a. Yes – Proceed to Step 2
                b. No – Reset via CMTS in NYROC. If this does not fix the problem, schedule a TC.
    b. Wired devices only?
        i. Check the physical Ethernet/USB connection to the wired devices, including the "Link" lights around the port.
            1. Link lights on – Proceed to Step 2.
            2. Link lights off – Review Step 8/a/i/1/b under No Connectivity
    c. Wireless devices only
        i. Check to ensure Output Power is at 100% [Wireless > Basic]
        ii. Check the RSSI of the connected device(s) in question [Wireless > Access Control]
            1. RSSI for each device should be between 0 and -65 dB. If the device is outside of this range, have the client move the device closer to the AWG.
        iii. Check for signal interference [baby monitors, cordless phones, other home networks]
            1. If other devices are present, change the control channel [Wireless > Basic]
        iv. If possible, have the client try connecting the Wireless device via hardline to the AWG to test connection speed
        v. If none of the above items resolve the problem, proceed to Step 2.
2. Check to ensure IP Flood Detection is turned off [Firewall > Web Filter] – Proceed to Step 3
3. Check DHCP Lease Time is set to 86400 [Basic > DHCP] – Proceed to Step 4
4. Check the Connected Client list to see the number of devices currently sharing the connection [Wireless > Access Control] – if there are multiple devices splitting the connection, educate customer. If not, proceed to Step 5.
5. Determine the type of activity the client is attempting to perform.
    a. PC Online Gaming – Ensure UPnP is enabled [Advanced > Options] and discuss Port Forwarding/Triggering as an option
    b. Console Online Gaming – Ensure UPnP is enabled [Advanced > Options] and discuss setting up a DMZ for the console
    c. VoIP Software/Hardware – Disable SIP ALG [Advanced > Options]
    d. Streaming Video – Ensure Multicast is enabled [Advanced > Options]
    e. VPN – Ensure IPSec and PPTP Passthrough are enabled [Advanced > Options]
6. For any of the above scenarios, or if the customer is simply experiencing slow internet browsing, the problem is in the client's device. Follow standard demarcation support for slow browsing.