

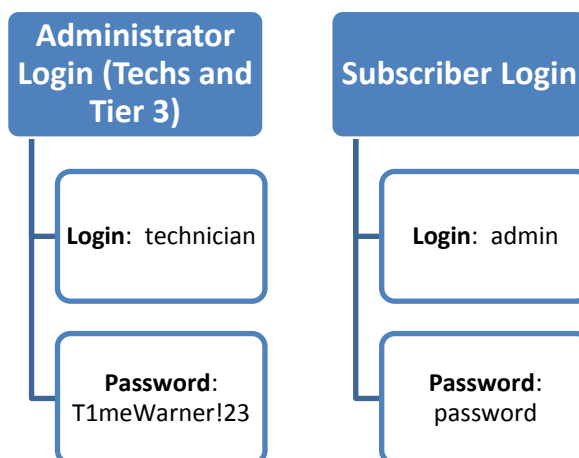
Purpose:



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

Basic Modem Information (Example: RF Cable MAC = 001DCF5451B2, Model = TC8717T)

- **Default Wireless SSID =**
Model + last 2 of RF MAC (all caps)
 - Example – TC8717TB2
- **Default Wireless Key =**
Model + last 6 of RF MAC (all caps)
 - Example – TC8717T5451B2
- **Default Wireless Encryption =**
WPA2-PSK
- **Compatibility:** DOCSIS 3/2/1.x,
Wireless 802.11 a/b/g/n/ac
- **Admin Access IP:** 192.168.0.1
 - Client will enter in browser address bar while using a wired connection



Modem Details:

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

Light	Power	US/DS	Online	2.4 Ghz	5 Ghz	Tel 1/2	WiFi
Status	Solid	Flash	Solid	Solid	Solid	Solid or Flash	Solid or Flash

In addition, there may be lights for the ports (Ethernet, Tel 1, Tel 2). These lights will only be on in the event the port specified is being used. For example, Ethernet, when present, will be solid when a device is hardline connected to that specific type of port on the AWG.

Technicolor DOCSIS 3.0 AWG eMTAs will have a Battery light indicating the charge status of the backup battery. Solid indicates the battery is charged and ready for use in the event of a power outage.

Optimizing the Technicolor AWG Wireless Connectivity

Basic Wireless Settings:

- Step 1:** Select **Gateway** from the side menu
- Step 2:** Select **Connection** from the side menu
- Step 3:** Select **Wi-Fi** from the side menu
- Step 4:** Click the **Edit** button next to the network you want to modify.

Private WiFi Network				
Name	Frequency Band	MAC Address	Security Mode	
TC8717T05	2.4 GHz	E0:88:5D:0D:FC:0B	WPA2-PSK (AES)	Edit
TC8717T05-5G	5 GHz	E0:88:5D:0D:FC:0C	WPA2-PSK (AES)	Edit

Wireless Network: Leave enabled unless bridging the AWG.

Network Name for 2.4Ghz (SSID): Change to client specification.

Security Mode: Select the level of Security based on client needs.

Network Password: Change to client specification. Must be at least 8 digits long.

Broadcast Network Name (SSID): Disable to stop broadcast of SSID.

Enable WMM: Leave checked.

Private WiFi Network Configuration (2.4 GHz)

Wireless Network: Enabled Disabled

Network Name for 2.4 GHz(SSID):

Security Mode: WPA2-PSK (AES)

Network Password:

WPA2 requires a 8-63 ASCII character.

Broadcast Network Name (SSID): ☒ Enabled

Enable WMM: ☒

[Save Settings](#) [Restore Default Settings](#)

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.

Changing the wireless channel:

- Step 1:** Select **Gateway** from the side menu
- Step 2:** Select **Connection** from the side menu
- Step 3:** Select **Wi-Fi** from the side menu
- Step 4:** Scroll downward until you reach the WiFi Basic Setting for 2.4Ghz or 5Ghz, and select Manual Channel Selection
- Step 5:** Select the desired Channel

5GHz WiFi Basic Setting

Mode: 802.11 n/ac

Transmit Power: 100%

Channel Selection: ☐ Automatic ☒ Manual

Channel: 36

Channel E h: ☐ 20 ☐ 20/40 ☒ 20/40/80(auto)

[Save Basic Settings](#)

Advanced Wireless Settings:

Step 1: Select **Gateway** from the side menu

Step 2: Select **Connection** from the side menu

Step 3: Select **Local IP Network** from the side menu

Lease Time: Change to 1 Week to avoid IP conflicts with devices that go into sleep mode (laptops)

DHCP Lease Time:

Save Settings

Restore Default Settings

Advanced Gateway Settings:

Step 1: Select **Advanced** from the side menu

Step 2: Select **Advanced Options** from the side menu

Enable Ipsec Pass Through: ☒ Enabled ☐ Disabled

Enable the following options as needed:

- Ipsec PassThrough – optimizes for traditional VPN with full access to systems

Step 1: Select **Advanced** from the side menu

Step 2: Select **Device Discovery** from the side menu

Enable UPnP: ☒ Enabled ☐ Disabled

Enable the following option as needed:

- UPnP Enable – optimizes for online gaming

Optimizing the Technicolor 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

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. Devices outside the optimal range may experience slow speeds and dropped connections.

Bridging the Gateway:

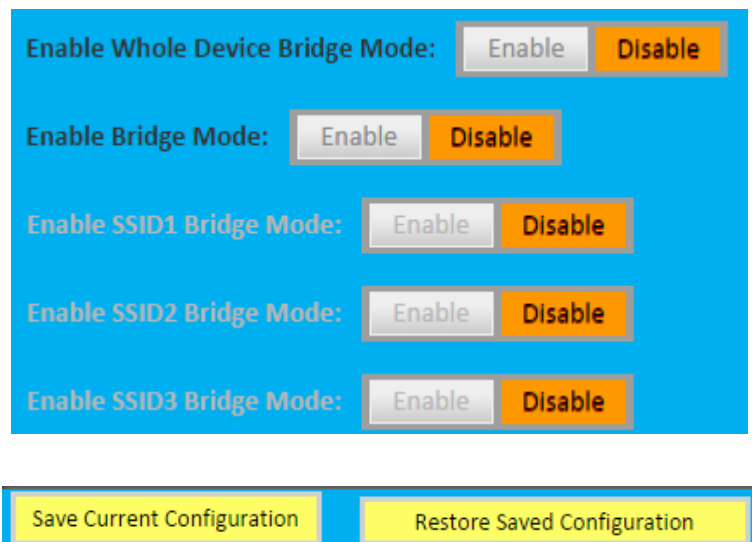
Some clients choose to bridge their AWG so they can use their own router. Before bridging the AWG, inform your client that bridging the gateway will result in TWC's inability to effectively troubleshoot the wireless connectivity within their home network. Once bridged, TWC can only troubleshoot the connection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

Step 1: Select **Gateway** from the side menu

Step 2: Select **At a Glance** from the side menu

Step 3: Enable the option to: **Enable Whole Device Bridge Mode**

Step 4: Click Save Current Configuration



The screenshot shows a configuration page with a blue background. At the top, there are two buttons: 'Enable' (grey) and 'Disable' (orange). Below this, there are five rows, each with a label and two buttons ('Enable' and 'Disable'). The labels are: 'Enable Whole Device Bridge Mode:', 'Enable Bridge Mode:', 'Enable SSID1 Bridge Mode:', 'Enable SSID2 Bridge Mode:', and 'Enable SSID3 Bridge Mode:'. At the bottom, there are two large yellow buttons: 'Save Current Configuration' and 'Restore Saved Configuration'.

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, Xbox360) and wireless printers.

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

Step 1: Select **Connected Devices** from the side menu

Step 2: Click the **Edit** button next to the device you wish to set the static IP address for.

Step 3: Under configuration select Reserved IP, and chose an IP address to static in. Comment optional.

Step 4: Select **Save**

Step 5: Select **Advanced** from the side menu.

Step 6: Select **DMZ** from the side menu

Step 7: Enable DMZ

Step 8: Enter the last section of the assigned IP address and select the Apply button

Online Devices-Private Network			
Host Name	DHCP/Reserved IP	RSSI Level	Connection
Unknown			
IPV4 Address 192.168.0.5	Reserved IP	-87 dBm	Wi-Fi
IPV6 Address			
MAC Address 10.30.47.B0.F5.2C			

Edit Device

Host Name:
Connection: **Wireless**
Configuration: ☐ DHCP ☒ **Reserved IP**
MAC Address: 10.30.47.B0.F5.2C
Reserved IP Address: 192.168.0.5
Comments:

Save
Cancel

DMZ (Demilitarized Zone)

Enable DMZ: ☒ **Enabled** ☐ Disabled
DMZ IPv4 Host: 192 . 168 . 0 . 0
DMZ IPv6 Host: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Save

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.

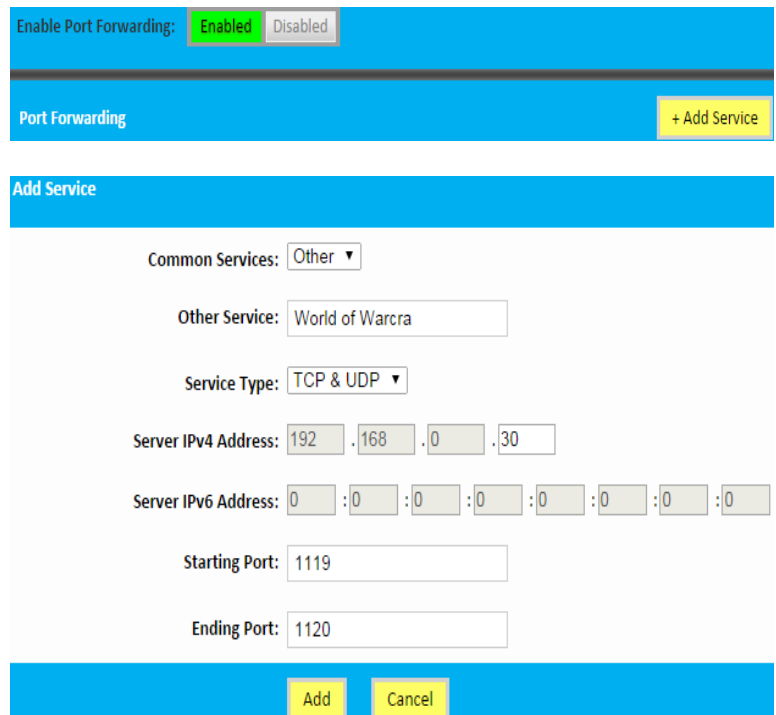
Port Forwarding opens designated ports for specific devices on the home network. Prior to setting up port forwarding, a static IP address should be assigned to the device in question. To set up a static IP address for a specific device, follow steps 1 through 5 on page 5. Once a static IP has been reserved,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

Step 1: Select **Advanced** from the side menu.

Step 2: Select **Port Forwarding** from the side menu

Step 3: Select Enable, and click +Add Service

Step 4: Use the Description field to name the port definition



Step 5: Enter the low range port under the first Inbound Port field, the high range port under the second Inbound Port field, select the Protocol (TCP/UDP/Both), enter the reserved IP in the Private IP Address field, enter the low range port under the first Local Port field and the high range port under the second Local Port field. Select the Add Virtual Server button

Repeat steps 3 through 5 for each port range being forwarded

Optimizing the Technicolor AWG Wireless Connectivity

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.

Enable Port Triggering: Enabled Disabled

Port Triggering + Add Port Trigger

Step 1: Select **Advanced** from the top menu

Step 2: Select **Port Triggering** from the side menu

Step 3: Select Enable, and click +Add Port Trigger

Step 4: Use the Service Name field to name the port definition

Add Port Trigger

Service Name:

Service Type:

Trigger Port From:

Trigger Port To:

Target Port From:

Target Port To:

Add Cancel

Step 5: Enter the low range port under the first Inbound Port field, the high range port under the second Inbound Port field, select the Protocol (TCP/UDP/Both), enter the low range port under the first Local Port field and the high range port under the second Local Port field. Select the Add Port Trigger button

Repeat steps 3 through 5 for each port range being triggered

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 Client List [Wireless Setup > Wireless Client List] – 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 Setup > Basic] – Proceed to Step 4
4. Confirm SSID/Password [Wireless Setup > Basic] – 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. [LAN Setup > LAN Settings]
 - a. Enable DHCP Server checked, Start IP Address set to “192.168.0.2” and End IP Address set to “192.168.0.254” – Proceed to Step 7
7. Confirm AWG is not bridged. [LAN Setup > LAN Settings] – NAT Mode = Routed with NAT
 - 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.
 2. Reset via CMTS in NYROC. If this does not fix the problem, 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.

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 7/a/i/1/b under No Connectivity
 - c. Wireless devices only
 - i. Check to ensure Output Power is at High [Wireless Setup > Basic]
 - ii. Check for signal interference [baby monitors, cordless phones, other home networks]
 1. If other devices are present, change the control channel [Wireless Setup > Basic]
 - iii. If possible, have the client try connecting the Wireless device via hardline to the AWG to test connection speed
 - iv. If none of the above items resolve the problem, proceed to Step 2.
2. Check DHCP Lease Time is set to 86400 [LAN Setup > LAN Settings] – Proceed to Step 3
3. Check the Client List to see the number of devices currently sharing the connection [Wireless Setup > Wireless Client List] – if there are multiple devices splitting the connection, educate customer. If not, proceed to Step 4.
4. Determine the type of activity the client is attempting to perform.
 - a. PC Online Gaming – Ensure UPnP is enabled [LAN Setup > LAN Settings] and discuss Port Forwarding/Triggering as an option
 - b. Console Online Gaming – Ensure UPnP is enabled [LAN Setup > LAN Settings] and discuss setting up a DMZ for the console
 - c. VPN – Ensure IPsec and PPTP Passthrough are enabled [Firewall > Firewall Settings]
5. 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.