Optimizing the Ubee AWG Wireless Connectivity

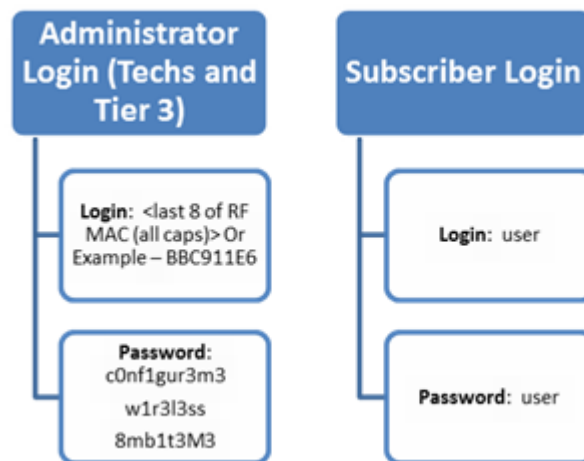**Learning Development & Inclusion**
educate   inspire   lead

Purpose:

This job aid details the proper settings and troubleshooting for Ubee 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 = 906EBBC911E6, Model = DDW3611)

- **Default Wireless SSID** = Model + last 2 of RF MAC (all caps)
    - o   Example – DDW3611E6
- **Default Wireless Key** = Model + last 6 of RF MAC (all caps)
    - o   Example – DDW3611C911E6
- **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 or 192.168.100.1
    - o   Client will enter in browser address bar while using a wired connection

Administrator Login (Techs and Tier 3)

Login: <last 8 of RF MAC (all caps)> Or Example – BBC911E6

Password: c0nf1gur3m3 w1r3l3ss 8mb1t3M3

Subscriber Login

Login: user

Password: user

Modem Details:

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

Light	Power	DS/US	Online	WiFi
Status	Solid	Solid	Solid	Solid

In addition, there may be lights for each port (Eth-1, Eth-2, Eth-3, Eth-4, USB Host, Tel 1, Tel 2). These lights will only be on in the event the port specified is being used. For example, Eth-1, when present, will be solid when a device is hardline connected to that specific port on the AWG.

Some Ubee 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).

Ubee 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 Ubee AWG Wireless Connectivity

Learning Development & Inclusion
educate   inspire   lead

Basic Wireless Settings:

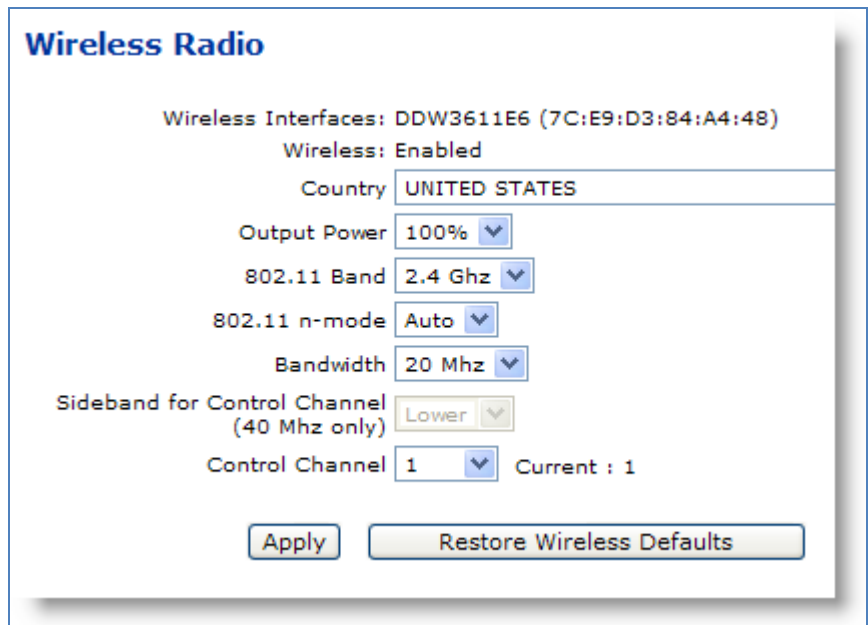**Step 1**: Select [WIRELESS] from the top menu

Step 2: Select •Radio from the side menu

Restore Wireless Defaults: Selecting this will revert all settings, including SSID and Password, to factory default

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

802.11 Band: Leave at 2.4 Ghz.

Wireless Radio

Wireless Interfaces: DDW3611E6 (7C:E9:D3:84:A4:48)
Wireless: Enabled

Country	UNITED STATES
Output Power	100%
802.11 Band	2.4 Ghz
802.11 n-mode	Auto
Bandwidth	20 Mhz
Sideband for Control Channel (40 Mhz only)	Lower
Control Channel	1 Current : 1

[Apply]   [Restore Wireless Defaults]

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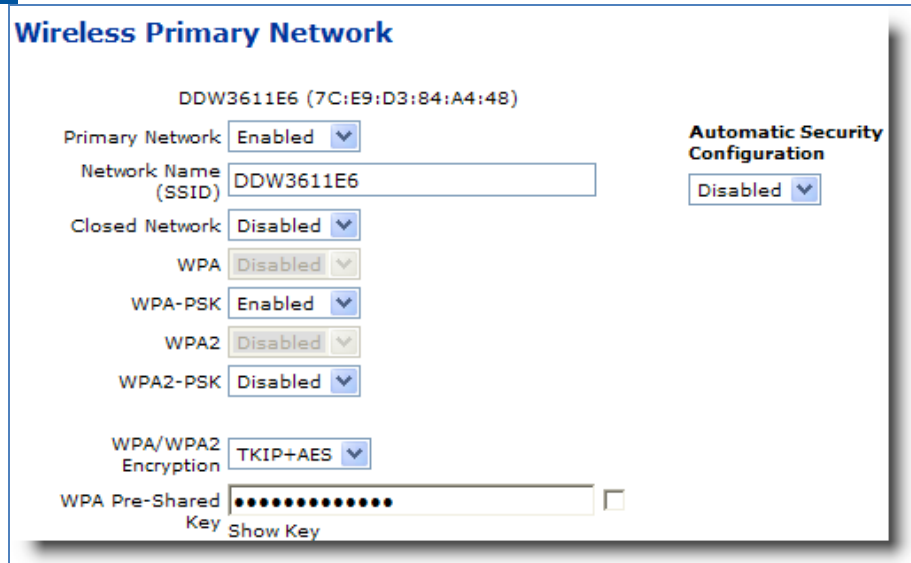
Primary Wireless Settings:

Step 1: Select [WIRELESS] from the top menu

Step 2: Select •Primary Network from the side menu

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

Wireless Primary Network

DDW3611E6 (7C:E9:D3:84:A4:48)

		Automatic Security Configuration
Primary Network	Enabled	Disabled
Network Name (SSID)	DDW3611E6	
Closed Network	Disabled	
WPA	Disabled	
WPA-PSK	Enabled	
WPA2	Disabled	
WPA2-PSK	Disabled	
WPA/WPA2 Encryption	TKIP+AES	
WPA Pre-Shared Key	•••••••••••• Show Key	

> **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 Ubee AWG Wireless Connectivity

Advanced Wireless Settings:

Step 1: Select | GATEWAY | from the top menu

Step 2: Select •DHCP from the side menu

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

Gateway - DHCP

DHCP Server ◉ Yes ◯ No

Starting Address Set

Private Starting Address 192.168.0. 3 (1~253) Number of CPEs 252

Public Starting Address 0.0.0. 0 (1~254) Number of CPEs 0

Lease Time 86400

Apply

Advanced Gateway Settings:

Step 1: Select | GATEWAY | from the top menu

Step 2: Select •Options from the side menu

Advanced Gateway - Options

WAN Blocking ☐ Enable
Ipsec PassThrough ☑ Enable
PPTP PassThrough ☑ Enable
Multicast Enable ☑ Enable
UPnP Enable ☑ Enable
DNS Relay ☐ Enable

Apply

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
- DNS Relay – forwards DNS requests to a specified DNS server as opposed to the default

Firewall Content Filter:

Step 1: Select | FIREWALL | from the top menu

Step 2: Select •Content Filter from the side menu

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

Firewall Settings

Block Fragmented IP Packets ☐ Enable
Port Scan Detection ☑ Enable
IP Flood Detection ☐ Enable
Firewall Protection ☑ Enable
Protection against incoming connection requests on routed subnet ☐ Enable

Apply

Optimizing the Ubee 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 **Basic** from the top menu

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

Step 3: View the Connected Clients chart

Connected Clients	MAC Address	Age(s)	RSSI(dBm)
	7C:61:93:82:8A:EB	0	-60
	F4:0B:93:AB:18:4B	4896	0

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** from the side menu

Step 3: Select Disabled from Primary Network dropdown

Step 4: Click Apply

Step 5: Select **Wireless** from the top menu

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

Step 7: Set Wireless Bridging to Enable and select Apply

Step 8: Go to **Advanced** from the top menu

Step 9: Select **Options** from the side menu

Step 10: Click the checkbox labled Primary Network Bridged

¦ Primary Network

DDW365C9 (3C:77:E6:55:0A:A2)

Primary Network Disabled

¦ Bridging

Wireless Bridging Enabled
Remote Bridges

Apply

¦ Options

WAN Blocking	☐ Enable
Ipsec PassThrough	☑ Enable
PPTP PassThrough	☑ Enable
Multicast Enable	☐ Enable
UPnP Enable	☐ Enable
Primary Network Bridged	☑ Enable
DNS Relay	☐ Enable

Learning Development & Inclusion
educate   inspire   lead

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: Create a **Static IP** for the device. Select **Basic** from the top menu

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

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
No DHCP Clients					

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

Step 4: Select **Static Lease** from the side menu

Step 5: Enter the MAC Address and current IP Address of the device into the appropriate fields and check the Enable box

Step 6: Select the Apply button

Step 7: Select **Advanced** from the top menu

Gateway - DHCP Static Lease

Note: If some IP addresses turn to red color,you should check the DHCP pools!
Current DHCP Server IP Ranges' information
Private IP Range:192.168.0.3 -- 192.168.0.253
Public IP Range:0.0.0.0 -- 0.0.0.0

Index	MAC Address	IP Address	Enabled	Clear
1.	7c : 61 : 93 : 82 : 8a : eb	192.168.0.6	☑	☐
2.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
3.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
4.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
5.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
6.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
7.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
8.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐

Apply

Step 8: Select **DMZ Host** from the side menu

DMZ Host

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

DMZ Address **192.168.0.** 0

Apply

Optimizing the Ubee 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 7 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 top menu

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

Step 3: Click **Create IPv4**

Step 4: Enter the static IP into the row/rows needed for the ports being forwarded

Step 5: Enter the low range port under Start Port, the high range port under End Port and select the Protocol (TCP/UDP/Both)

Step 6: Select the Enabled drop down for the definition entered and select the Apply button

Forwarding

Local IP	0.0.0.0
Local Start Port	0
Local End Port	0
External Start Port	0
External End Port	0
Protocol	TCP
Description	
Enabled	Off

Cancel   Apply

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**.

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)

Step 5: Select the Enabled drop down for the definition entered and select the Apply button

Port Triggers

Trigger Start Port	0
Trigger End Port	0
Target Start Port	0
Target End Port	0
Protocol	BOTH
Description	
Enabled	Off

Apply

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 [Tools > 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 > 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. Change setting to AES [Wireless > Primary Network]
      ii. 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. [Gateway > DHCP]
   a. DHCP Server set to "Yes" and number of CPEs set to "252" – Proceed to Step 7
7. Confirm AWG is not bridged. [Tools > Operation Mode] – Enable NAT 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.

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 100% [Wireless > Radio]
        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 > Radio]
        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 > Content Filter] – Proceed to Step 3
3. Check DHCP Lease Time is set to 86400 [Gateway > DHCP] – Proceed to Step 4
4. Check the Client List to see the number of devices currently sharing the connection [Tools > Client List] – 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 [Gateway > Options] and discuss Port Forwarding/Triggering as an option
    b. Console Online Gaming – Ensure UPnP is enabled [Gateway > Options] and discuss setting up a DMZ for the console
    c. Streaming Video – Ensure Multicast is enabled [Gateway > Options]
    d. VPN – Ensure IPSec and PPTP Passthrough are enabled [Gateway > 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.