Setting up a Ubiquiti Network
for use with PTZOptics Products

Created on 2018-5-17 by Matthew Davis

Goal

In this document, we will cover how to properly configure your Ubiquiti network for use with mDNS and multicast devices.

While the instructions provided below are specific to Ubiquiti products at this current date, the general concepts should apply to most managed networks.

We will cover enabling IGMP and mDNS, then how to setup routing to allow mDNS and multicast traffic to flow properly.

Assumptions & Warnings

We will assume that you are using an entirely managed network, and specifically for this document a Ubiquiti network *(Router, Switches and possibly Wireless Access Points)* that is already operational with static IPs assigned for all Ubiquiti hardware.

If any part of the network is NOT managed, or manually configured to work in unison with the rest of the network, failure will result because of incompatibilities in communication between the networking equipment.

Thus, it is highly recommended to use the same managed networking equipment from "top to bottom" to prevent frustrations caused by incompatibilities.

Once all changes have been made to make your network fully operational for multicast and mDNS, you must be aware that the mDNS routing is not a "persistent" change and thus will be overwritten with any power cycle or "provisioning" of the network switches, meaning these steps will need to be taken again.

We take no responsibility for any issues or losses that may arise from following the instructions presented in this document and implementation of the instructions is at your own risk.

Symptoms of a misconfigured network…

- mDNS
  - When you utilize a discovery or configuration tool, it is unable to locate your device connected to the same network
  - When you utilize a discovery or configuration tool, it randomly finds devices which also disappear randomly
- Multicast
  - When connecting to a multicast source, your video appears to "smear" or "bleed"
  - When connecting to a multicast source and have a successful connection, but receive no content
  - When connecting to a multicast source, your network crashes
  - When connecting to a multicast source, your network slows to an unusable speed

Overview of issue(s) and steps

When you have more than one (1) network switch being utilized in a situation with equipment and applications that utilize mDNS for discovery, the switches need to be told which switch will be the "holder" of mDNS discovery tables.

When the IGMP snooping querier is enabled, it periodically sends queries that trigger IGMP response messages from hosts that are requesting to receive IP multicast traffic.

These tables are what your network will reference when it tries to route traffic to your device. If the tables are not being held properly in one location the discovery will be intermittent at best.

The next step is enabling IGMP and possibly, depending on your exact requirements, enabling or disabling multicast traffic via wireless access points.

Multicast traffic via your WiFi network is a decision that should not be taken lightly as it is very easy to overload a wireless access point with multicast traffic. Also of note is that not all wireless access points are capable of handling multicast traffic; please refer to manufacturer documentation.

Ubiquiti Equipment used for this documentation

- (1) UC-CK "Unifi Cloud Key" or "Controller"
  - Firmware version 5.7.23-10670
- (1) USG "Unified Security Gateway"
  - Firmware version 4.4.18.5052172
- (1) US-48-750 "48 Port 750W PoE+ Managed Switch"
  - Firmware version 3.9.27.8537
- (1) US-24-500 "24 Port 500W PoE+ Managed Switch"
  - Firmware version 3.9.27.8537
- (1) US-8-150 "8 Port 150W PoE+ Managed Switch"
  - Firmware version 3.9.27.8537
- (1) US-8-60 "8 Port 60W PoE+ Managed Switch"
  - Firmware version 3.9.27.8537
- (1) UAP-AC-PRO-US "802.11ac Dual Radio Pro Access Point"
  - Firmware version 3.9.27.8537

Let's start configuring!

Enabling IGMP Snooping

Login to the web interface of your Ubiquiti network using the "Unifi Web Login" or by directly logging in to the IP of your controller / cloud key.

Once logged in you, should see a "Dashboard" displayed with current network statistics and graphs similar to what is shown below.
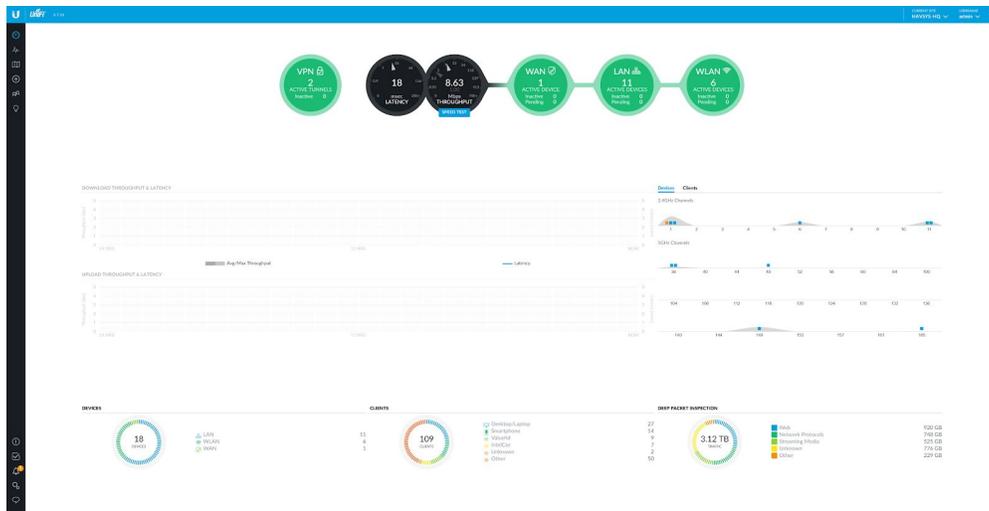

Click on the "settings" button that looks like a gear in the lower left of the "Dashboard" to navigate to your main network settings page.

From the navigation pane on the left side select the "Networks" option.

Locate your network in the list. If it is a basic network, you may only see one listed. Select the "EDIT" option to the far right of the network "NAME".

Make sure the "Enable IGMP snooping" checkbox has been checked.
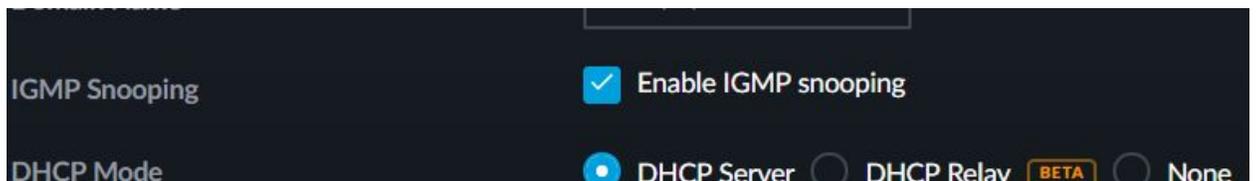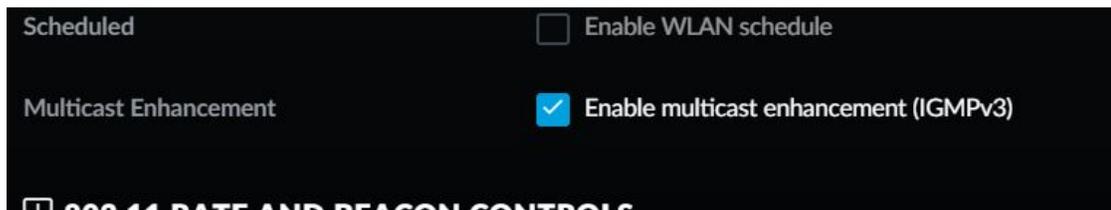

Click the "SAVE" button at the bottom of the page.

Enabling WiFi IGMPv3

Now that we have enabled IGMP Snooping for the network, we are going to continue where we left off and enable the wireless network configurations for IGMPv3.

Using the navigation pane on the left side, select "Wireless Networks"

You will now be presented with a list of all configured wireless networks. Please click the "EDIT" option on the one you intend to use with mDNS & multicast equipment.

> Near the bottom of the Wireless Network page is an option titled "Multicast Enhancement" with a checkbox for "Enable multicast enhancement (IGMPv3)" simply check that box.

> Now click the "SAVE" button at the bottom of the page

Blocking LAN to WiFi Multicast Traffic and Options

On the same page we just enabled IGMPv3, we now have some options in regards to multicast traffic and how it is handled between the LAN and the wireless network.

By default, the wireless network is setup to allow multicast traffic to move from the LAN to the wireless network.

This is fine if it is restricted to limited users who are aware of the limitations.

If we want to block multicast traffic from LAN to wireless, we simply need to check the box titled "Block LAN to WLAN Multicast and Broadcast Data"
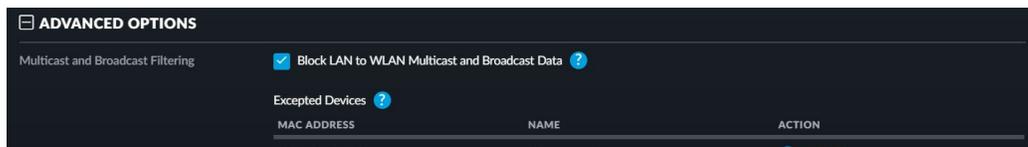
You may notice that when checked; by default the system adds the USG as an exception to the rule.

These exceptions allow you to define specific hardware that IS allowed to send multicast traffic from the LAN to the wireless.

If you are going to use multicast over wireless, this is a highly recommended method for implementation.

Add any additional hardware you may be trying to access multicast feeds from over the wireless network to this exception(s) list.

Note that you do not need to define any additional devices here if you plan to access all multicast feeds from your LAN.

Click the "SAVE" button at the bottom.

Enabling mDNS

Now that we have setup IGMP and Multicast Filtering, we are going to continue where we left off and enable mDNS.

Using the navigation pane on the left side select "Services"

> You will now see a top bar displayed with one of the options being "MDNS" please select that option.
>
> Click the toggle button to set "Enable Multicast DNS" to the "ON" state
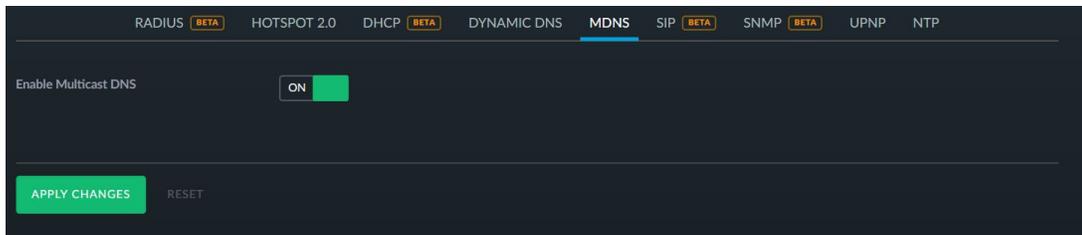
> Click "APPLY CHANGES"

Some good news…

You've setup EVERYTHING Ubiquiti allows for configuration via the WebUI for multicast traffic and mDNS discovery.

And some bad news…

If you have a network with more than one (1) switch these settings aren't enough.

And some more good news…

With the steps provided below we will log into each switch on the network and manually configure the switches to communicate properly.

So let's get configuring!

Configuring "Logical Querier" and "Query Interval" for each switch

Before beginning, there is an important decision that must be made…
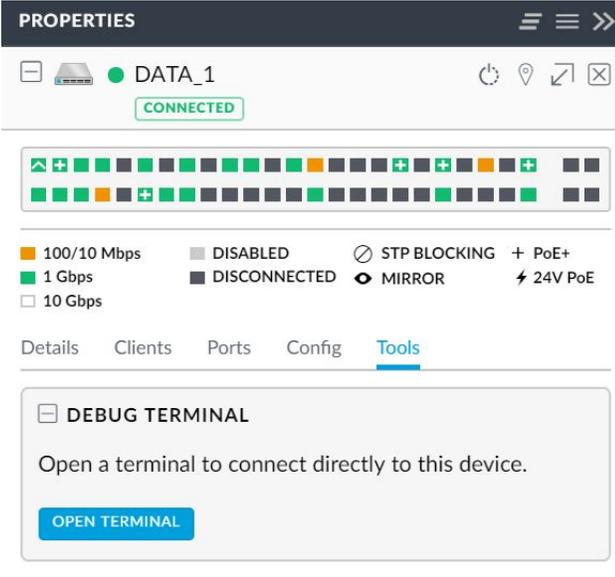
Which network switch is going to host the mDNS entries?

The simplest solution is to select the network switch that will result in the least "hops" between multicast equipment communicating.

Basically, we want to select the network switch that is the MOST central to all other switches and the multicast equipment being utilized on them.

Once we have identified that switch, please note its assigned static IP address as we will be using this IP address to manually configure every switch on the network.

To begin, please navigate to the "DEVICES" page represented by the symbol of a circle within a circle on the far right.

Highlight the first switch listed, regardless of which one, and the properties pane should open. Click on the "Tools" option.

Click on the "OPEN TERMINAL" button and a new window will open initializing the connection to the switches command line interface "CLI"
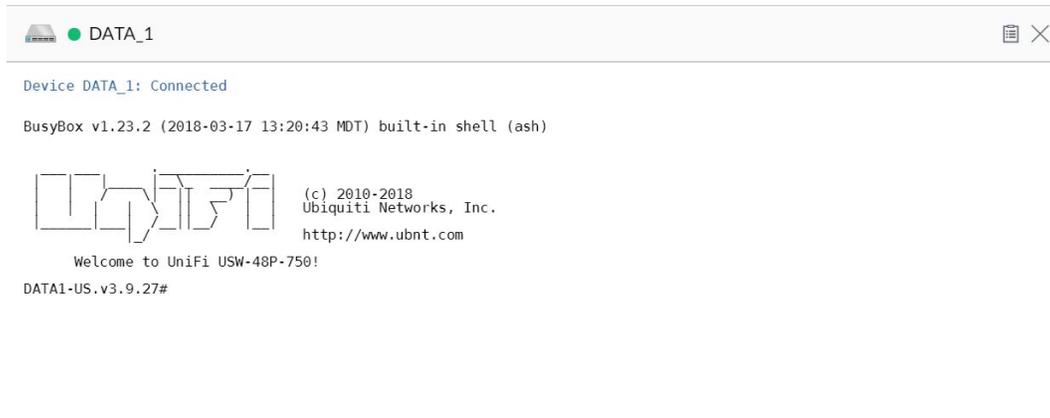
We are now going to enter the following commands followed by a return when [ENTER] is shown

> **telnet localhost**
> [ENTER]
> [ENTER]
> **en**
> [ENTER]
> **configure**
> [ENTER]
> **set igmp querier address** *<static IP of switch to host mDNS table>*
> [ENTER]
> **set igmp querier query-interval 10**
> [ENTER]
> **exit**
> [ENTER]
> **exit**
> [ENTER]

These commands are also shown below as an example from my own implementation.

```
        Welcome to UniFi USW-48P-750!
DATA1-US.v3.9.27# telnet localhost

Entering character mode
Escape character is '^]'.

Warning!
The changes may break controller settings and only be effective until reboot.

(UBNT) >en

(UBNT) #configure

(UBNT) (Config)#set igmp querier address 192.168.111.51

(UBNT) (Config)#set igmp querier query-interval 10

(UBNT) (Config)#exit

(UBNT) #exit

(UBNT) >
```

Now you must repeat these EXACT same steps, using the same static IP address of the switch with the least hops, for each of the switches within your network (including the switch with the least hops). Do this on EVERY switch on your network or the changes may not be successful in solving your problems.

Please also remember that these changes are not *currently* persistent. This means that, if your switches reboot or you make further configuration changes to the switches causing a provisioning, that these Logical Querier and Query-Interval settings will be wiped out and will need to be manually applied again.

Congratulations!

You have now properly configured your Ubiquiti network for use with mDNS and multicast in a multi-switch network deployment!

Please note we do not provide any support in relation to this document and take no responsibility for any impact or losses that may result from following this guide.

Final Notes:
If any errors are found in this documentation or updates that negate the necessity for this document come to light please feel free to let us know tryatyourownrisk@ptzoptics.com and we will be happy to update the documentation accordingly.