Home-Network Implementation

Using the Ubiquiti EdgeRouter ER-X and Ubiquiti AP-AC-LR Access Point

By Mike Potts

Check for updates at: https://github.com/mjp66/Ubiquiti or https://github.com/mjp66/Ubiquiti?files=1

Table of Contents

Table of Tables

1. Overview

This guide will attempt to show users how to set up two Ubiquiti pieces of equipment, to provide for a secure and flexible firewall / router and a Wi-Fi Access Point. The two pieces of equipment used in this guide are:

- Ubiquiti EdgeRouter ER-X (about $60 when this guide was written)
- Ubiquiti AP-AC-LR Wi-Fi Access Point (about $130 when this guide was written).

This equipment can provide (at least) 3 isolated or semi-isolated wired networks, and up to 4 isolated or semi-isolated Wi-Fi SSIDs. The networks provided by this equipment configuration of this guide are as follows:

- Wired/Wi-Fi Home Network For most of the household personal computers, tablets, and smartphones
- Wired Separate Network For an isolated and/or separate network and/or personal computer(s)
- Wired/Wi-Fi IOT Network For Internet-Of-Things devices (can be accessed via Home Network)
- Wi-Fi Guest Network For visiting friends' tablets and smartphones

Your network naming and use may / can be different. A fourth Wi-Fi Network is also available.
See Figure 1 - Overview Diagram.

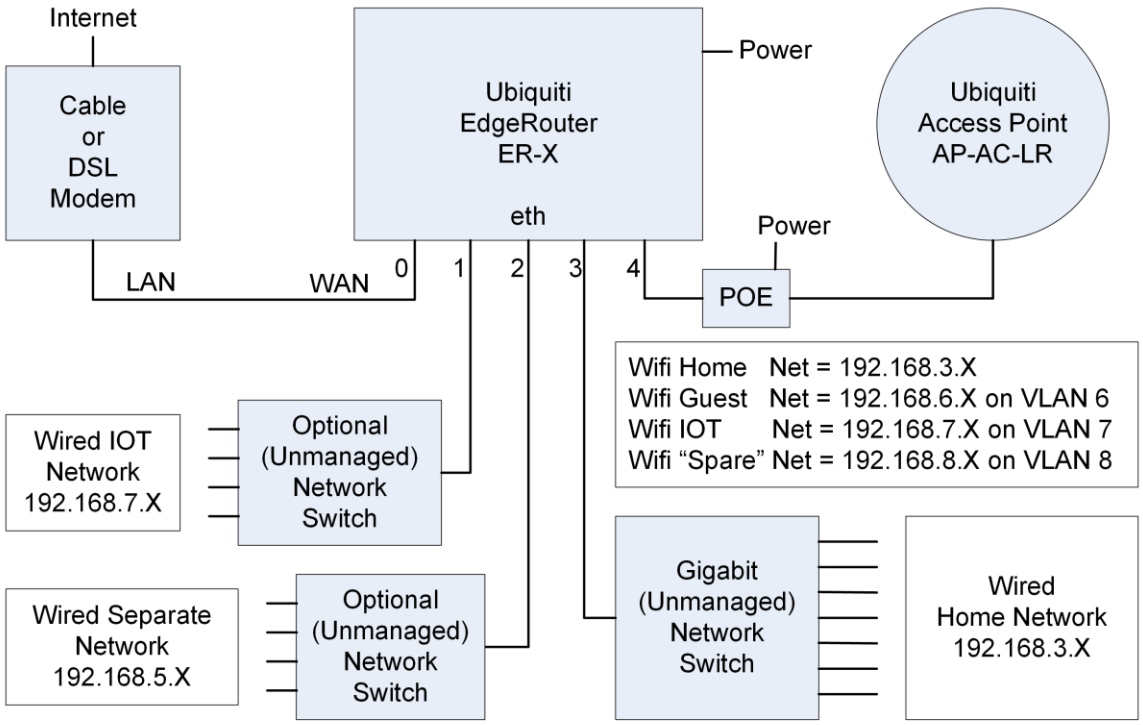


Figure 1 - Overview Diagram

With this setup, the Home Network (both Wired and Wi-Fi) is able to initiate connections / communicate with devices on the Wired/ Wi-Fi IOT Network. Devices on the IOT Networks are NOT able to initiate connections / independently communicate to the Home Network. None of these Networks can communicate with the Wired Separate Network, and the Wired Separate Network cannot communicate with any of them.

This guide assumes that you will be using both an Ubiquiti EdgeRouter ER-X and some model of Ubiquiti Access Point (UAP / AP). I tend to use the terms ER-X and EdgeRouter somewhat interchangeable within this guide.

Ubiquiti ER-X Product Links:
https://store.ui.com/collections/operator-edgemax-routers/products/edgerouter-x

For Ubiquiti Access Points (UAPs/ APs) see section 5 -Ubiquiti Access Points (UAPs or APs).

2. Disclaimer

This is a guide, your results may vary. I am not a network engineer. Enough said.

3. Purpose

One purpose of this guide is to provide a stable and usable router / firewall / Access Point configuration. This specific implementation is aimed at the Home / SOHO user.

Another purpose is to provide background on what these configuration settings accomplish, so that the reader can understand why these settings were chosen.

I wrote this guide because I REALLY like this router.

I was mostly motivated to switch routers by reading http://routersecurity.org/ and http://routersecurity.org/bugs.php. This website should scare just about anybody that is currently using consumer / commercial routers. I'm so glad to be finished with that buggy equipment.

The only trouble with this router is that it is meant for professionals to use. You have to scrounge around forums for postings on how to configure specific items. This doesn't mean that the forum people are not friendly, just that the needed answers are not all in one place. Sometimes the answers are a little bit terse for a new user. As stated, I am not a network engineer.

This guide is the documentation, for the configuration that I setup for myself. It took me a huge amount of time to put this document together. I've tried to write this guide in a teaching manner, and cite references where I could. Note that I specifically call this a 'guide'. When you go through this document you should: experiment, modify, learn, tinker and play, extend, and learn some more. Mix and match the sections as you see fit.

Most of my source information came from reading postings at (the now revamped) EdgeMax Ubiquiti Community:
(Formerly) https://community.ubnt.com/t5/EdgeMAX/bd-p/EdgeMAX
(Currently) https://community.ui.com/tags/edgemax/questions?

When this document was ready, I joined the Ubiquiti community and announced it at (formerly / currently):
https://community.ubnt.com/t5/EdgeMAX/New-ERX-AC-AP-LR-setup-guide-for-beginners/td-p/1906477

(https://community.ui.com/questions/New-ERX-AC-APLR-setup-guide-for-beginners-/700af0ae-35d5-41ac-af80-f50963c8dad3)

If you have specific questions about this configuration, your best bet is to research postings at the above EdgeMax link, then try and experiment for yourself. If you get stuck, then join the Ubiquiti community and ask. I've now purchased an additional ER-X router to continue experimenting and for use in refining this guide.

Note that the associated backup file(s) on github are not being actively maintained or updated with later changes being made in this guide. Those files are there as references.

When originally writing this guide, I was not able to figure out how to combine the Wired IOT Network (as 192.168.4.X) and the Wi-Fi IOT Network (as 192.168.7.X) as a single Network / Subnet. I now enable the internal ER-X switch chip to be VLAN aware, which solves this. Those steps are in section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks. You should just wait to do this until you get to that section, or you might not be able to follow-along in this guide. For me to have instead performed those steps earlier, now that I know what to do, I would have had to re-write most of this guide and re-take way-too-many screenshots. So that section is still much later in this guide.

---

4. Alternate / Similar EdgeRouters

There are now alternate "nicely priced" (more powerful) **EdgeRouters** available.
I have no experience with any of the following EdgeRouters.

https://www.ui.com/edgemax/comparison/

EdgeRouter -10X:

> https://store.ui.com/products/edgerouter-10x
>
> https://community.ubnt.com/t5/EdgeRouter/Anyone-want-to-share-their-experience-with-ER-10X/m-p/2765723#M250254

EdgeRouter-12:

> https://store.ui.com/collections/routing-switching/products/edgerouter-12
>
> https://community.ubnt.com/t5/EdgeRouter/New-ER-12-owner-ER-12-Questions/m-p/2768623#M250484

If you were to try to configure one of these alternate routers using this guide, you would have more ports available, and would need to adjust port number and port ranges as needed. You would need to follow the *concepts* of this guide, adjusting / modifying as you go for your specific equipment.

5. Ubiquiti Access Points (UAPs or APs)

There are many models of **Ubiquiti Access Points (UAPs or APs)** which can work well.

Until 2022, I had only purchased AP-AC-LRs, and had used (only) them for various setups / installations.
A single AP-AC-LR seemed to work for all my household needs, as my single-family-dwelling (home) is not that big, too wide, or that crammed full of IOT devices.

As of 2022, I've tried a U6-Lite, and am now using a U6-Pro-US, and a U6-LR-US in my house. The U6-Lite is now my cold (unplugged / boxed) spare. The U6-LR has, until recently, been unstable for me; there were (and still are) a lot of Ubiquiti-Community complaints about the U6-LR. If the U6-LR gets bad again, I'll shelve the U6-LR and deploy the U6-Lite.

Having two APs in my home, with the power levels each reduced, seems to provide better coverage at the far edges of my house.

I originally chose the AP-AC-LR (in 2016, when I started writing this guide) because it seemed to provide the widest coverage area, i.e. Longer range, at the almost lowest price. More expensive models can handle several hundred connections per AP. Please don't *fully* believe the marketing fluff about the supported numbers of client connections.

Access Point AC Long-Range = UAP-AC-LR-US ($110 USD with / including 24V passive Power Adapter)
https://store.ui.com/collections/unifi-network-wireless/products/unifi-ac-lr

5.1 Number of Ubiquiti Access Points to Install / Placement

For your home install, from what I have been reading:

> **It is better to deploy more (cheaper) Access Points, than deploy fewer (more expensive) Access Points,**
>
> **i.e. walls, floors, and distance seem to make the real difference.**
>
> **You will want every UAP to be Ethernet-wired back to your router.**

@gregorio
Most of the homes we've done in this size are at least 1 AP per 1000 [square feet], generally. The issue is getting excellent WIFI to the places that need it. One in that [great] room is good but what about the bedrooms, especially the master? One wall and about 20 feet are the limits we use when estimating another AP but we also start with them in the rooms where we know excellent signal is needed.
https://community.ui.com/questions/Recommendations-for-new-home-network-set-up/f2f65fe9-ca6f-4120-adbb-04542b135bc7#answer/3d92c9b4-50fa-4d6e-884c-b96cbc48759b

@ChessMck
Here is my rule of thumb - Assuming average size rooms - Great coverage in room with AP, good coverage one sheetrock wall away from AP and ok to poor coverage 2 walls between the AP and device.
https://community.ui.com/questions/Range-and-functionality-for-UniFi-AP-AC-LR-WAP/e5542247-bba9-45c7-b160-03b6d3611527#answer/b918a65e-651c-4d15-9bcc-e09af2f2c749

@gregorio
[New House: Suggestions on AP's]
… One way to look at this is to start with an AP in every room that needs excellent WIFI and then put another AP after the second wall. This means that there is at least one AP within one wall of every device.
I'd assume that the office, master bedroom, family room and kitchen are the top spots where you want APs.
… Oh, yeah. At least one U6-Mesh outside.
https://community.ui.com/questions/New-House-Suggestions-on-APs/59b6126a-9e54-44ee-8d5f-e9d379990649#answer/2fea182f-90b3-4518-ace9-56017cd2a720
[Editorial: Said another way: No device has more than one wall to some AP.]

@gregorio
[Outdoor Access Point for 180 deg X 50m radius]
Probably the UAP-AC-M-Pro is going to give you the best shot at this distance. U6-Mesh is second but 50m is about the max I would push it
https://community.ui.com/questions/Outdoor-Access-Point-for-180-deg-X-50m-radius/e08bfd16-582d-4efd-b532-b8bdfdac8aa7#answer/98dd3630-2276-4c79-91cb-cca8e260fba8

5.2 Ubiquiti Access Point Models

If you are buying new Access Points, there are Wi-Fi 6 (Dome type) Access Point models available:
Sorted by Price, LR = Long Range, EA = Early Access, Gains in dBi, Gen = Generation

U6 Model	2.4GHz	5GHz	6GHz	Throughput	2.4Gain	5Gain	6Gain	Gen	Price
U6-Lite-US	2x2 *	2x2		1.5 Gbps	2.8	3		5th	$100 USD
U6+ (EA)	2x2	2x2		3.0 Gbps	3	5.4		5th	$130 USD
U6+ LR (EA)	2x2	3x3		3.0 Gbps	4	5.5		5th	$150 USD
U6-Pro-US	2x2	4x4		5.3 Gbps	4	6		6th	$150 USD
U6-LR-US	4x4 *	4x4		3.0 Gbps	4	5.5		5th	$180 USD
U6-Enterprise-US	2x2	4x4	4x4	10.2 Gbps	3.2	5.3	6	6th	$299 USD

* U6-Lite and U6-LR have only Wi-Fi 4 on the 2.4GHz frequency band, i.e. No Wi-Fi 6 on 2.4 GHz.

All of the above U6 APs are sold without Power Adapters, use a (dependent upon model) POE / POE+ network switch OR one of the below adapters:

PoE Injector, 802.3at	= U-POE-AT	($12 USD, i.e. 30W Power Adapter)
PoE Injector, 802.3af	= U-POE-AF	($8 USD, i.e. 15W Power Adapter)

You can use an 802.3at adapter for units which only need 802.3af amount of power.

These WiFi-6 APs are somewhat new to brand new, somewhat un-available (because of supply-chain issues), and some models are still somewhat buggy. It will likely be years before your Wi-Fi devices are 6-capable to take advantage of (any) faster speeds. It is likely that these U6 APs will have a longer supported life span over the existing families / models of Access Points. Some of these models must be configured via the newest-version of Unifi controller.

If I were buying UAPs for a new installation, I would purchase either **U6-Lites** or **U6-Pros** (including using a mixture of these models).

Before purchasing any new APs, you might also want to read through all of section 5 and also all of section 77 - Setting UniFi / Access Point's SSIDs, Channels, and Power Levels. , I suggest also you read community postings, and postings associated with Access Point firmware releases.

As always, match your Power Adapter to your specific UAP. Older / non-U6 models are (typically) 24V passive, newer models are 48V 802.11af/at.

2022 Note: The AP-AC-LR model is now four generations old, i.e. in the oldest AP family currently supported by Ubiquiti. See https://help.ui.com/hc/en-us/articles/4409162471447-UniFi-Identify-your-Access-Point-Model

2022 Note: Newer firmware for AP-AC-LRs may be limiting power levels
https://community.ui.com/questions/AP-AC-LR-TX-Power-Neutered/bb383790-a09e-4f0e-87ed-d100cf9c82bd

@mrevanmccann
Since you can buy them individually, you may want a few different models. If you want maximum performance in one area, you can have a U6-Enterprise or AC-HD there, and then use a U6-Lite or a mesh AP to extend the network into less-used areas. If you want to expand coverage in the future, you don't need to match the models you currently have. You can add any of them at any time, wherever you need them.
https://evanmccann.net/blog/2021/1/unifi-ap-guide

@gregorio
[U6 Pro or U6 LR?]
What led you to these two APs? In a home, (more of) the U6-Lite is probably better.
Pro has 160MHz 4x4 support and WIFI6 on 2 GHz. Neither are of any consequence in a residence.
LR has 4x4 2GHz (SU-MIMO) support. Again, no real benefit there.
https://community.ui.com/questions/U6-Pro-or-U6-LR/00c690fd-2e7d-40e9-9706-d257b7d34993#answer/392b1a6c-8927-4b19-94b8-c31f7795025e
Editorial: Not said above, but implied: The U6-Lite has Wi-Fi 6 ONLY on 5 GHz.

@kanewolf
[Do we need 2 long range models or will one long range model be enough?]
Don't be fooled by the marketing. Long range is relative. You won't get twice the coverage, for example.
The best answer is to have multiple APs geographically distributed, but near the most client devices.
Those APs should have a wired connection back to the primary router.
All other implementations are compromises of some kind.
https://community.ui.com/questions/Different-Access-Points/94a94d40-b827-4904-9670-73d2210346f3#answer/bdb506a4-e94c-43e4-93a3-f5dba40c152f

@gregorio
[… Discussion about U6-LR-US …]
The U6-Pro is cheaper, more capable, and from what I can see, more reliable.
https://community.ui.com/questions/Rebuild-a-pretty-basic-wireless-setup/a0ba47ac-1806-4422-99b8-427b9edf111e#answer/ddab9fa2-4959-4ad9-b9df-3705fe65fa54
[Editorial: see my notes about U6-LR's instability, above]

@gregorio
[https://evanmccann.net/blog/2021/9/unifi-speed-tests]
[U6-LR is good for residential where they want minimum # of APs and not necessary shooting for The Best performance everywhere in the house i.e. if you can get by with 2 LRs its cheaper than 3 Pros.]
If you are making recommendations based on this, you are doing WIFI wrong. In 99.99% of all residential cases, four U6-Lite will beat two U6-LR. If two U6-LR are enough to provide better than -55dBm everywhere, then two U6-Lite will do the same thing at half the price.
https://community.ui.com/questions/U6-Pro-vs-U6-LR-Why-are-both-offered-when-theyre-so-similar/6b498fe3-36e2-4c1e-a324-1761ee87642f#answer/8b74093c-ff91-45e8-b65c-38908ccc21e0
@mrevanmccann
If you are making recommendations based on this, you are doing WIFI wrong.]
Author of that link here, and I agree. I've seen a lot of people misinterpret those results, and that article in general. Hopefully I'll do it better next time.
https://community.ui.com/questions/U6-Pro-vs-U6-LR-Why-are-both-offered-when-theyre-so-similar/6b498fe3-36e2-4c1e-a324-1761ee87642f#answer/12f5e9d8-b8b4-469e-b8fd-1a7c81749dcc

5.3 Mesh vs Roaming

Many newcomers posting on Ubiquiti forums ask for how to do Mesh. Most of these posters are actually asking for their mobile client's to do efficient Roaming. Roaming is where a mobile client will seamlessly re-connect to the closest AP, as the client moves around.

@s_squire
Mesh refers to how the APs are connected. When they are connected wirelessly, they are forming a mesh network. Marketing morons have really screwed people up by using it all over and implying that it is somehow good (it is not, just better than nothing).
Roaming is when a client moves between APs and [that] is something managed by the client.
You will need to tune the APs, but keep in mind that to mesh, they will need to share a channel and every hop will cut performance.
https://community.ui.com/questions/Is-this-a-Mesh-Network-Or-just-extenders/01781be7-9b5b-472d-9bdb-5de5cfb71e33#answer/c6088624-84a1-40fb-b355-e1fb91f5212b

@nuttersrest
In Unifi language, meshing means an AP wirelessly uplinks to a wired AP to extend WiFi coverage to areas you cannot get a cable. What you are talking about is roaming, where all APs present the same SSID and clients seamless move between them as devices move without breaking their connections. Unifi can do both but you will be using roaming, just make sure you tune your radio settings correctly and do not leave the Power and Channel settings on auto, set them manually.
https://community.ui.com/questions/Mesh-setup-wifi-network/ff77573f-943c-4b27-9258-9a909efd5129#answer/e36df89f-5218-4903-a23a-dd122b0d1805

Mesh is like using a Wi-Fi extender / Wi-Fi repeater device, where some of your AP-type-devices are not Ethernet connected. These non-Ethernet-connected (AP) devices use (some) of your available Wi-Fi channel's bandwidth to connect themselves back to the wired APs, and then use the same Wi-Fi channel's bandwidth to ALSO connect to client devices. Bandwidth is how much data can flow through a (Wi-Fi) link, in a given period of time. Note that every extender / repeater device you use will cut your client's bandwidth in half. This dual use of Wi-Fi is a very inefficient.

You can do limited "Mesh" networks using any of Ubiquiti's (currently supported) APs. Note that many of the UAP's have "Mesh" in their names, but that is only Ubiquiti's marketing department playing games. Ubiquiti's real term for "Meshing" is "Wireless Uplink".

You want to Ethernet wire ALL of your APs, if you can achieve this.

5.4 Ethernet Wiring your UAPs

You want to Ethernet wire ALL of your APs. All my APs are deployed via wired Ethernet. There are lots of YouTube videos and how-to articles on the internet which can help you with installing Ethernet cables in an already-constructed home. If you are running Ethernet cables via a house's cold air returns, I believe that plenum rated cable is required. Use at-least Cat-5E cable, as Cat-5E is rated at gigabit speeds. I've also seen postings that say CAT 7 cable is worthless because of the connectors.

5.5 UAP Comparison Data

The antenna radiation pattern URLs are probably the best of these links:
https://help.ui.com/hc/en-us/articles/360008036574-UniFi-Access-Point-Comparison-Charts
https://help.ui.com/hc/en-us/articles/115005212927-UniFi-UAP-Antenna-Radiation-Patterns
https://help.ui.com/hc/en-us/articles/115012664088-UniFi-Introduction-to-Antenna-Radiation-Patterns
https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf
https://ui.com/wi-fi

Here are some pages comparing Ubiquiti equipment, which seem to provide much better detail than Ubiquiti's own pages. Reference to where I found it, is below. If you are purchasing new APs, I suggest you explore (at least) the following pages:
https://evanmccann.net/blog/2020/5/unifi-wifi-6-lite?format=amp
https://evanmccann.net/blog/2021/1/unifi-ap-guide
https://evanmccann.net/blog/2021/9/unifi-speed-tests

U6-Pro ($149): My vote for the best value, and the best omnidirectional Wi-Fi 6 AP… if you can find it in stock.
Per https://evanmccann.net/blog/2021/1/unifi-ap-guide

Which is the Best AP for You? (Crosstalk Solutions)
https://www.youtube.com/watch?v=y5I_WhnviYY

6GHz Support
https://help.ui.com/hc/en-us/articles/8691786444567-UniFi-Network-6-GHz-Support-with-UniFi6-Access-Points

Here are some Ubiquiti product links:
https://store.ui.com/collections/unifi-network-wireless/products/unifi-6-long-range-access-point
https://store.ui.com/collections/unifi-network-wireless/products/unifi-ap-6-lite
https://store.ui.com/collections/unifi-network-wireless/products/unifi-ap6-professional
https://store.ui.com/collections/unifi-accessories-poe-injectors/products/u-poe-at
https://store.ui.com/collections/related/products/u-poe-af

5.6 UAP Wireless Uplinking

Meshing involves using Wi-Fi to connect APs together. At least one AP must be Ethernet wired. Note that this steals Wi-Fi bandwidth from your devices. The data connecting APs together is sometimes called “backhaul”. Note that if you do have at least one AP which is wirelessly uplinked, you will likely use a lot-of or all-of your 5GHz channel. I have not tried this, so good luck.

https://store.ui.com/blogs/news/moving-beyond-the-conventional-wireless-network-with-unifi-mesh

You can additionally chain a wireless uplinked AP to another wireless uplinked AP, but this is not recommended, as each “hop” will reduce stability, and will also result in (another) nearly 50% performance decrease.
From https://help.ui.com/hc/en-us/articles/115002262328

If you really need to wireless uplink, maybe the following will help:

> https://lazyadmin.nl/home-network/unifi-wireless-uplink/
>
> https://www.youtube.com/watch?v=s2tOOPwVjxw Ubiquiti Mesh Wireless
>
> https://community.ui.com/questions/Proper-settings-to-wirelessly-connect-UAP-AC-M-to-a-wired-AP-AC-PRO/f94e7bff-8a01-4b08-bfeb-46aec5abdc58#answer/02c1ffce-b98b-4020-9baa-5d9f094f50be
> (Please see entire thread)

I believe when using wireless uplinking, that the wired and uplinked AP’s will all need to be tuned to the same 5GHz channel. It is likely that you would want to set the 5GHz power to maximum on each of these linked APs to attempt to increase bandwidth. Maximum 5GHz power is typically not used when tuning APs for correct device (smartphone / tablet) roaming. If you are using uplinking, you should research these settings.

Per this @RobbieH posting, maybe selecting newer / 4x4 APs will help with wireless uplinking bandwidth.
https://community.ui.com/questions/Bridging-two-different-Unifi-Access-Points/b6fd2e18-8b0b-4619-b9a7-8be87a5c1e31#answer/bd5d3823-6ad2-41b3-804d-49fe83e626e0

@gregorio
Some more detail to optimize your config. Pick a clear 5GHz channel for the wired AP and leave the downlink on AUTO. Use non-overlapping fixed channels on 2GHz. Look at the signal level of the mesh. Make sure it is no lower than -70dBm. It would be better to be -65dBm. There are two ways to change the signal, move the APs or increase the power symmetrically. The former is preferred as the latter will change your cell overlap and negatively impact device roaming.
https://community.ui.com/questions/WIFI-extended-coverage/766cd85c-5e95-4187-9036-b0ac36e93f45#answer/9378c5bd-e9e8-40cd-9cca-008603996fc6

@gregorio
[Roaming / mesh / big problems]
The problem is usually traced back to poor tuning and mesh. Having APs with such wide differences in gain is not helping either. To support the needs of the mesh, it requires settings that are in conflict with good roaming. Generally for dual band devices, you will want to lower your 2G power so that it is 7dBm below 5G. This will help them prefer the often cleaner 5G band. Your power levels should not allow RF overlaps more than 10% or so. This means that when walking away from one AP, you do not hear the next one above -65dBm until the one you are on is about this level.
https://community.ui.com/questions/Roaming-mesh-big-problems/c91ade5e-2c5c-494d-b88d-f7b985460a1e#answer/8eb0f79c-b3ad-41fd-a691-107d5788bebc

@gregorio
[AC Mesh Pro vs UniFi6 Mesh for hotel]
1. Depends more on client mix and the distance to them. The output power of the AC-M-Pro is 1dBm less than the U6-mesh on 5G but 5dBm more on 2G. More importantly, the antenna gain of the former is 3-5dBi greater (5G/2GHz) than the latter. This makes the AC-M-Pro better at distance. However, it is 3x3 SU-MIMO vs. 4x4 MU-MIMO for the U6-Mesh meaning the latter can handle twice the simultaneous clients as the Pro. So, if your outdoor APs (you will likely need more than one) are well placed in relation to the clients and you have plans to serve more than 20 on an AP, the U6-Mesh is the way to go. If you have poor placement, the AC-M-Pro can help overcome that a little better.
2. Since it is WIFI, the only way to make it work is to increase power in BOTH directions. Truth be told, you want a balanced link and this can be a combination of power and gain. Since the mobile clients are so weak in radiated power (Tx power plus antenna gain), the APs that work best have higher receive gain. This is why the AC-M-Pro is the king in omni coverage. Regarding mixing AC and AX, don't worry about it. They work fine together even in a mesh but at all costs avoid mesh. Wire every AP or you will kill your performance and stability.
3. Yes, all current Unifi APs will mesh. If you absolutely cannot run wires and must use mesh, 4x4 APs are best for this. They suffer the least performance penalty.
https://community.ui.com/questions/AC-Mesh-Pro-vs-UniFi6-Mesh-for-hotel/a2d50d2e-2461-4220-8653-5e276bbac08e (Above posts within this thread)

@lcire1
Mesh with unifi is a backstop move. it is a two radio solution so the 5Ghz is shared space when mesh is enabled. If you want a mesh network, IMO Orbi is a better solution Where Unifi has 1 x 2.4 and 1 x 5ghz, Orbi has 1 x 2.4 and 2 x 5ghz. i.e. they have a dedicated uplink radio rather then sharing the single 5ghz.
https://community.ui.com/questions/Initial-Setup-for-Home-Networking-Makeover-Is-This-Correct/d6a58052-045a-438e-877f-6f05951186ab#answer/3276593a-25a6-4007-be40-f5ede780f6e9

5.7 UAP Expanded References

(Original posting data may be slightly edited and/or re-formatted for clarity)

@mikesg
This guy does a better job explaining UniFi gear detail and providing charts than Ubiquiti does.
https://evanmccann.net/blog/2020/5/unifi-wifi-6-lite?format=amp
From https://community.ui.com/questions/U6-Pro-or-U6-LR/00c690fd-2e7d-40e9-9706-d257b7d34993#answer/3bf831c4-5ac4-440b-8deb-c45438dfd1c4

@AlexWilsonsBlog
Consumer grade routers are usually running at full power and bristling with high gain antennas designed to flood the place with coverage from a single device. Of course, they rarely flood it well. Then you end up cobbling together a bunch of "extenders" which make it worse usually.
https://community.ui.com/questions/Very-limited-range-on-new-AC-Pro-setup/2f48b246-72e4-4bfe-a33a-ba31913332ba#answer/e7d8e952-6a38-4fec-9030-e38a5b7801f5

@gregorio
You will likely need more than one AP. For stable WiFi, your APs need to be close to your devices. Place APs in all areas where you want excellent coverage and tune them accordingly. Shape of your home and its construction are more important than its size. Walls and distance kill signal. This is even more important given your 5G requirement. The type of AP is unimportant.
https://community.ui.com/questions/Home-network-advice-100-20-11-Devices-550m2/a177a4bc-a54a-40b1-a03f-e22c2ee4a2b4#answer/d5e525a3-8cbd-4929-943e-7189e8c6b646

@gregorio
WiFi is very complicated. There is only so much bandwidth available for a given channel. Because only a single client device can transmit at a time, all other devices must wait for it to finish. If that client device is connected at a low/slow rate, the latency for all the devices goes up. The faster the connection rate, the sooner that client is done transmitting data which frees up the channel for other devices to start transmitting. By moving from one AP to two APs, you have just cut your latency in half and doubled your throughput. However, the effect is even greater than that because you are getting your devices closer to your APs. Having them close means they will have a faster connection which lowers latency and speeds throughput even more.
https://community.ui.com/questions/High-density-Gaming-Setting-AP/43672883-a05f-4c9c-acc1-524b0df0d24c#answer/27297dfa-1a92-4009-a1f7-eef0ffaa3517

@mackey
Hi there... 1x1, 2x2, 3x3 & 4x4 is referring to the number antennas inside the device, so the more internal antennas the higher speeds should be achievable in ideal conditions. So, based on your iPhone 11 Pro.....
here are part of the specs I copied from Apples website:

Gigabit-class LTE with 4x4 MIMO and LAA4
802.11ax Wi-Fi 6 with 2x2 MIMO

Looks like it has a 4x4 design for when using an actual phone carrier network for data..... and has a 2x2 design when using wifi..... therefore the maximum wifi rated speed is 866 Mpbs, but you need to take off about 40% of that figure just for wifi overheads, leaving you with actual maximum throughput of about 520 Mpbs in ideal conditions.
https://community.ui.com/questions/nanoHD-speed-issues/b617d157-5d56-4a73-bb71-ac0bddd0046a#answer/3d1ced35-407f-4cb9-8601-57e35cbcda2c

@gregorio
[… I have a home network with 3 access points… I am wondering if I should upgrade my APs and to what.]
Unless you are in the 0.05% of users that stream 4K to multiple devices simultaneously, there really is no need to upgrade unless you like spending time and money. Internet Speed Test bragging aside, the average home will not see any benefit from WIFI6 over WIFI5.
https://community.ui.com/questions/What-Wireless-Access-point-to-upgrade-to/d3793347-494a-4008-972e-420fb1b8a5ff#answer/432e375a-b3ce-48ff-9d73-5a7214ee790a

5.8 UAP End-Of-Life

Recently, many older models of Access Points are going End of Life (EOL). You probably don't want to purchase any of those. [Note that UAP-LR is discontinued, NOT the UAP-AC-LR.]

https://community.ui.com/questions/Announcement-EOL-for-some-UniFi-AP-models/65487283-ce9d-49f4-85b9-b6aa54659ef7

Access Point Generation Chart (ensure that the "UniFi Access Points" picture is clicked)
https://help.ui.com/hc/en-us/articles/360012192813-UniFi-Getting-Started
https://help.ui.com/hc/en-us/articles/4409162471447-UniFi-Identify-your-Access-Point-Model

…UAP-AC-Pros are notorious for failed POE negotiation chips. …
https://community.ui.com/questions/UAP-AC-Pro-works-with-POE-injector-but-not-POE-from-switch/8e94df2b-bc9b-4151-901d-bb8d280535cf#answer/66fc1fe6-bd19-4625-91a2-12cc946c3a62

UAP-AC-PRO dead before its time, with 203 "mine is dead also" responses and counting.
https://community.ui.com/questions/UAP-AC-PRO-dead-before-its-time/65e3f80e-0eef-487e-aa73-4e0f602d841a

Potential (self) Hardware fix for UAP-AC-PRO (if you are unlucky enough to already own them)
https://community.ui.com/questions/Hardware-fix-UAP-AC-PRO-does-not-power-with-a-switch-but-works-with-a-passive-injector-issue/2ba799ae-d2d3-4971-ae62-df3d7612dce6

6. EdgeRouter IP Address Use

For the purposes of this guide, I am assuming that you will put your Ubiquiti EdgeRouter in series-with / behind your existing firewall / router, after the EdgeRouter has been initially configured. This way, you can leave your existing network alone, while securely setting up and testing your EdgeRouter. You need to ensure that your existing network does not use any of the following network addresses: 192.168.3.X, 192.168.4.X, 192.168.5.X, 192.168.6.X, 192.168.7.X, 192.168.8.X or 192.168.9.X, as these address ranges will be used within the EdgeRouter. I suggest that you set up or re-configure your existing router to use IP addresses of 192.168.2.X on its LAN ports. Existing router addresses of 192.168.0.X or 192.168.1.X will also work. Your existing equipment may have the "Cable or DSL Modem" portion and "Your Existing Firewall / Router" portion combined into one single unit. See Figure 2 - EdgeRouter Configuration Setup. You will also need a computer to setup the EdgeRouter.

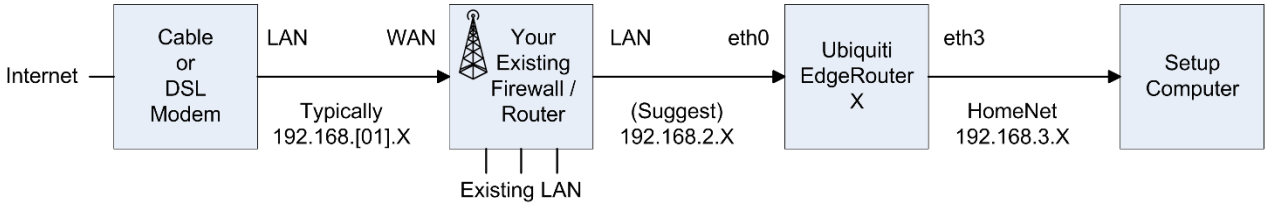


Figure 2 - EdgeRouter Configuration Setup

Most cable / DSL modems seem to be pre-configured for DHCP, and for using addresses of 192.168.0.X or 192.168.1.X on their LAN ports. Therefore, I configured the EdgeRouter Network addresses not to include those ranges. I deliberately left the address range of 192.168.2.X unused within the EdgeRouter, so those addresses could be used by an existing firewall / router's LAN ports.

If the EdgeRouter was using an address that was also used by your Cable / DSL modem, it would mask / hide that equipment's setup web page(s), and you would not be able to access those pages.

The EdgeRouter will NOT work if the address presented via DHCP to its eth0 port maps anywhere within one of the address ranges used internally by the EdgeRouter.

If your Internet Service Provider's (ISP) equipment does not provide an IP address via DHCP, then you will need to adjust your WAN (eth0) settings after running the setup wizard. If the internet is only partially working, or you need to use PPPoE, then you might want to read:

https://community.ui.com/questions/Mss-Clamping-MTU-Setting/2d8534d3-044a-4264-b472-ee8eef8fe2d0

https://community.ubnt.com/t5/EdgeRouter/Adjust-the-MSS-value-for-the-PPPOE/td-p/2617231

https://community.ui.com/questions/How-to-set-up-MTU-properly/dbb28fa7-0873-418b-bae5-0ed471b84a88#answer/c1f591d1-57ac-40a8-bef9-80061615eecf

https://community.ubnt.com/t5/EdgeMAX/Can-t-open-some-webpages/m-p/1950743/highlight/true#M163311

https://samuel.kadolph.com/2015/02/mtu-and-tcp-mss-when-using-pppoe-2/

https://community.ui.com/questions/Google-Fiber-Speed-Issues-with-EdgeRouter/bd3e9acb-fa4c-4711-9a7f-9f1d66d5578c

7. Acquire EdgeRouter Documentation

On the computer you use to setup the EdgeRouter X, download the newest documentation from:

https://www.ui.com/download/edgemax/edgerouter-x/er-x

There are both a User's Guide and a Quick Start Guide.

Note that Ubiquiti makes several models of EdgeRouter equipment. Each model uses different hardware, has different capabilities, supports a different number of ports, and may be configured (sometimes subtly) differently from each other. For instance, the EdgeRouter Lite typically uses eth1 as its WAN port, while the EdgeRouter X typically uses eth0 as its WAN port. Watch out for these types of differences when doing internet searches. EdgeMAX is the operating system for the EdgeRouter series.

8. Web Resources

EdgeMax	https://community.ui.com/tags/edgemax/questions?page=1
UniFi	https://community.ui.com/tags/unifi-wireless/questions?page=1
Unofficial	https://www.reddit.com/r/Ubiquiti/

Here are some more references:

https://help.ui.com/hc/en-us/articles/115002531728-EdgeRouter-Beginners-Guide-to-EdgeRouter

http://www.guruadvisor.net/en/networking/321-edgerouter-x-tiny-but-full-of-resources

These postings perform similar items as this guide does:

https://community.ui.com/questions/New-noob-owner-of-Edgerouter-x-a-simple-way-to-change-the-router-lan-network-ip-address-including-e/d3c27485-a93f-4f9c-8e92-4dc4f1b29a31#answer/073f4175-3df1-4cbf-86b2-38fbb05936da

https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-segmentation/td-p/1767545

https://help.ubnt.com/hc/en-us/articles/218889067-EdgeMAX-How-to-Protect-a-Guest-Network-on-EdgeRouter

Ben Pin (sometime Ubiquiti Employee) has a bunch of tutorial videos:
https://www.youtube.com/channel/UC9jUG4FPm9mPM555WOKSl6g
Including "QC Ubiquiti EdgeMAX - UAP with Guest WLAN & VLAN Trunks (VIF)":
https://www.youtube.com/watch?v=SKeFqFhBwJY

9. Initial EdgeRouter Hardware Setup

Configure the setup computer's Ethernet jack as having a fixed IP address of 192.168.1.X (where X is 2 to 254), and a netmask of 255.255.255.0. There are many tutorials available on the internet that shows how to configure a computer's Ethernet port to use a fixed IP address

One way to configure a Windows 10 computer is:

Control Panel -> Network & Internet -> Ethernet -> Change Adapter Settings -> Internet Protocol Version 4 -> Properties -> Use the following IP address, IP Address: 192.168.1.100.

@BuckeyeNet has made the following two observations.

1. The IP address is not actually changed until you press BOTH the #1 and #2 OKs.
2. Also if you are using a browser to connect to the GUI, close the old tab and open a new one. I don't know for sure why this makes a difference, but it does. Perhaps a shift reload would work, but I didn't try that. Normally the IP address is changing anyway, so I just open a new tab out of habit.

See Figure 3 – Windows 10 Ethernet Address Setup.

If you are still having trouble reconnecting, reference the following post he made:
https://community.ui.com/questions/Help-ER-X-cannot-connect-after-re-set-and-cannot-get-serial-USB-ttl-cable-to-work/ae154217-492f-49e1-a8c9-e82961dd6c4c#answer/2d8c606f-eb79-4237-ad6c-6942bcdfbd87

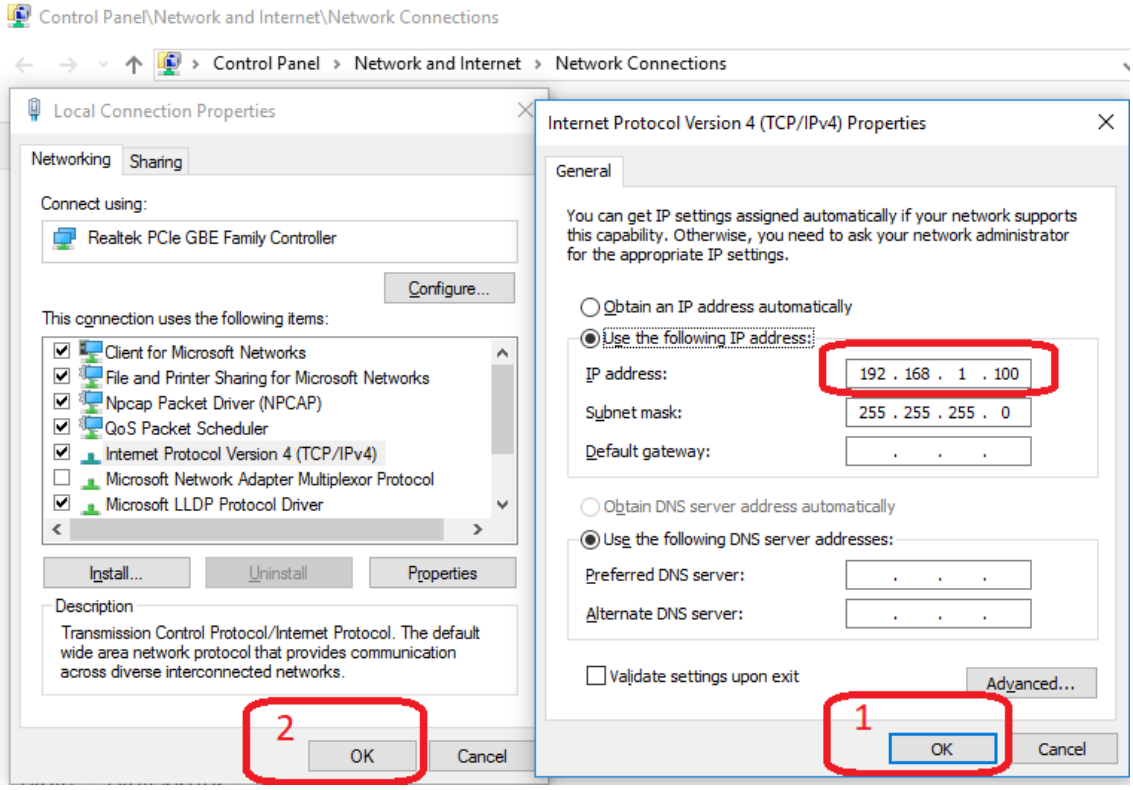


Figure 3 – Windows 10 Ethernet Address Setup

Power up your EdgeRouter X using the supplied power adapter, and then depress and hold the reset button for about 15 seconds. After releasing the reset button, connect a standard Ethernet cable from the EdgeRouter's eth0 port to the setup computer's Ethernet jack. See Figure 4 – Initial EdgeRouter Hardware Setup.

If your EdgeRouter is ever reset (on-purpose / crash / accidental) you will need to re-start recovery at this section. If you keep a current EdgeRouter configuration-backup-file available, a full restore is then easy.

Note that some setup computers may have an additional Ethernet adapter or have an additional Wi-Fi adapter installed. If any additional adapter(s) are installed, and an adapter is using or connecting to an address within the range of 192.168.1.X, then you will need to temporarily disable that additional adapter. The additional adapter only needs to be disabled while you are trying to access the EdgeRouter at its initial hardware setup address of 192.168.1.1.

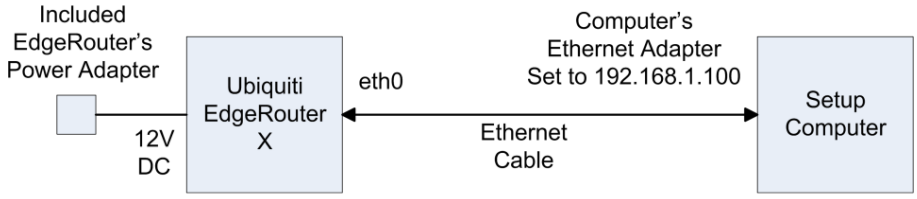


Figure 4 – Initial EdgeRouter Hardware Setup

Reference Quick Start Guide and the User's Guide @Chapter 2:Using EdgeOS.

10. Initial EdgeRouter Login

Wait about three minutes for the EdgeRouter to boot up, then open a web browser of your choice on your setup computer and enter https://192.168.1.1 into the address field.

Note that there are UI community discussions about the EdgeRouter's web page not working correctly with Apple's Safari browser and/or not working correctly with Apple's iPad. I can confirm that my iPad will not show a correct page. One hint of an incorrect page is that "TBD" shows up under the "IP Addr" field on the Dashboard page and lots of items at the top of the page are blank / black.

The browser may issue a security warning. You will need to "Continue to this website" or equivalent. The exact prompts and responses vary by browser. See Figure 5 – IE Security Certificate Example.

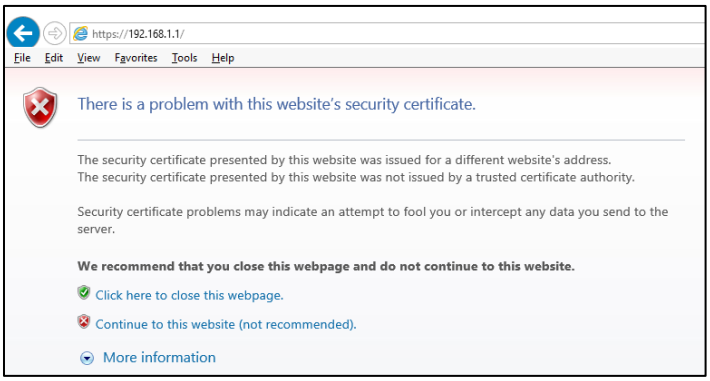


Figure 5 – IE Security Certificate Example

You will likely see a combined login and license agreement dialog. Enter the username and password. The default username is "ubnt" and the default password is "ubnt". Do what you need to do for the agreement. See Figure 6 – Ubiquiti License Agreement Dialog.

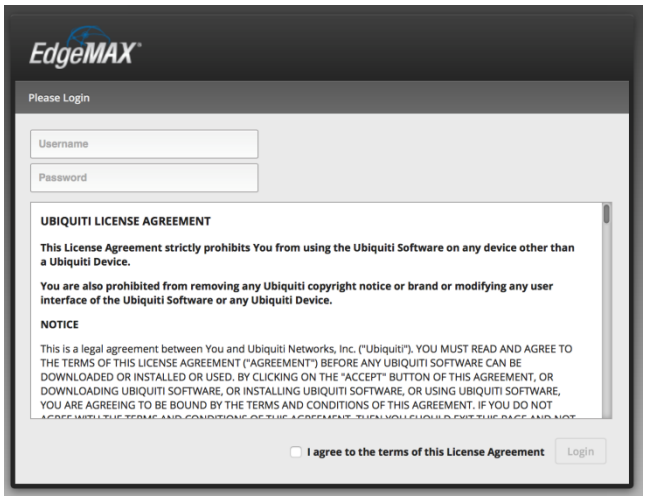


Figure 6 – Ubiquiti License Agreement Dialog

Depending upon the version of firmware that was pre-installed on your EdgeRouter, you may be presented with a dialog box stating that the “Router is in default config. Do you want to start with the Basic Setup wizard?” If presented, answer No. See Figure 7 – Basic Setup Question.

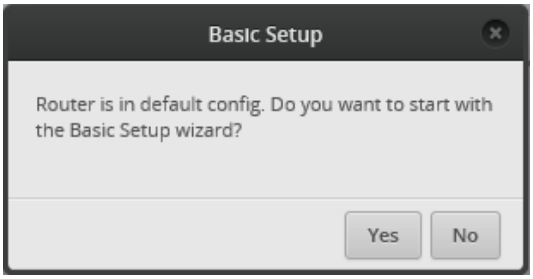


Figure 7 – Basic Setup Question

You will land on the Dashboard screen. See Figure 8 – Initial Dashboard Screen.

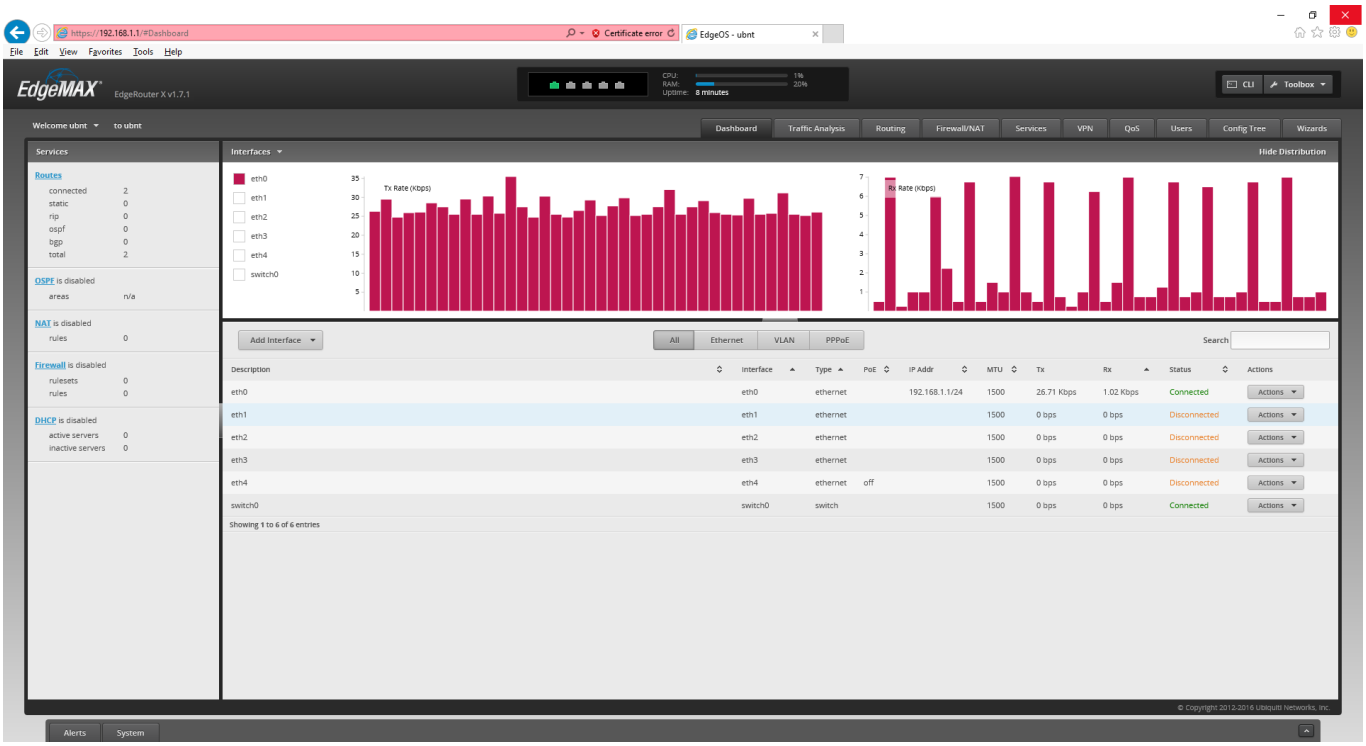


Figure 8 – Initial Dashboard Screen

Reference Quick Start Guide and the User’s Guide @Chapter 2:Using EdgeOS.

11. Update EdgeRouter (System) Firmware

WARNING: As of early 2020, many forum users are reporting that newer versions of Google's Chrome browser may no-longer work for uploading / downloading system images and/or configuration files. Try to use a FireFox browser. Reference https://community.ui.com/questions/Has-Chrome-83-broken-restoring-configuration-backups/c6a2d0e6-5f0d-494e-b588-c477cf5e19e4

Note: Sometimes to download newer system firmware, you might need to first recover more space on your ER-X router. You can issue the CLI command:

```
delete system image
```

to recover more space. Note that this deletes the backup (configuration) image, not the running (configuration) image. Only do this command if you cannot otherwise update. Reference Section 17 - EdgeRouter Command Line Interface (CLI).

On your setup computer, download the firmware from (one of):

https://www.ui.com/download/edgemax/edgerouter-x
https://community.ui.com/releases (click EdgeMax here, UniFi Wireless for UAPs)

2019 Note: Through early 2021, Ubiquiti has maintained two sets / lines of system firmware for the ER-X model. Specific release numbers, below, are as of January 2021:

Firmware v1.10.11
Firmware v2.0.9

The v1.10.x line is highly regarded, and universally seen as stable, but Ubiquiti has stated that there will be no more updates made to the v1.10 series. What a shame.

The v2.0.x line of releases has been a disaster, especially for the ER-X model. Ubiquiti has released firmware which is not even of alpha quality, hardly tested it, and then released it into the stable channel. They have done this again and again and again. I strongly suggest NEVER loading any v2.0 release before v2.0.8-hotfix.1.

2021 Note: I am still running V1.10.11, but am now experimenting with 2.0.9.hotfix.2.

2022 1Q Note1: I am now on 2.0.9.hotfix.2, and do not have any problems

2022 3Q Note2: 2.0.9.hotfix.4 is just out, I have not tried it yet.

For reference, during the initial writing of this document, the firmware was at:

"EdgeRouter ER-X/ER-X-SFP/EP-R6: Firmware v1.9.1".

Some of the ER-X screenshots in this guide have now been taken over many different firmware versions.

Press the "System" button. See Figure 9 – System Button. This button is located near the lower-left corner of the dashboard screen, as shown in Figure 8 – Initial Dashboard Screen.

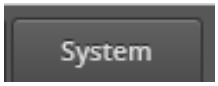


Figure 9 – System Button

Sometimes the System button and/or the Alerts button, which is right next to the System button, don't seem to work for me. I usually just click the other button twice, and then click the button I want.

You might want to join the Ubiquiti community and sign up for notifications about new software / firmware updates. You could also just periodically poll the above link, looking for new updates. It is probably a good idea to keep (somewhat) up to date firmware on your EdgeRouter, for security updates.

The System window will then pop-up an overlay that will cover most of your screen. See Figure 10 – System Pop-up Screen.

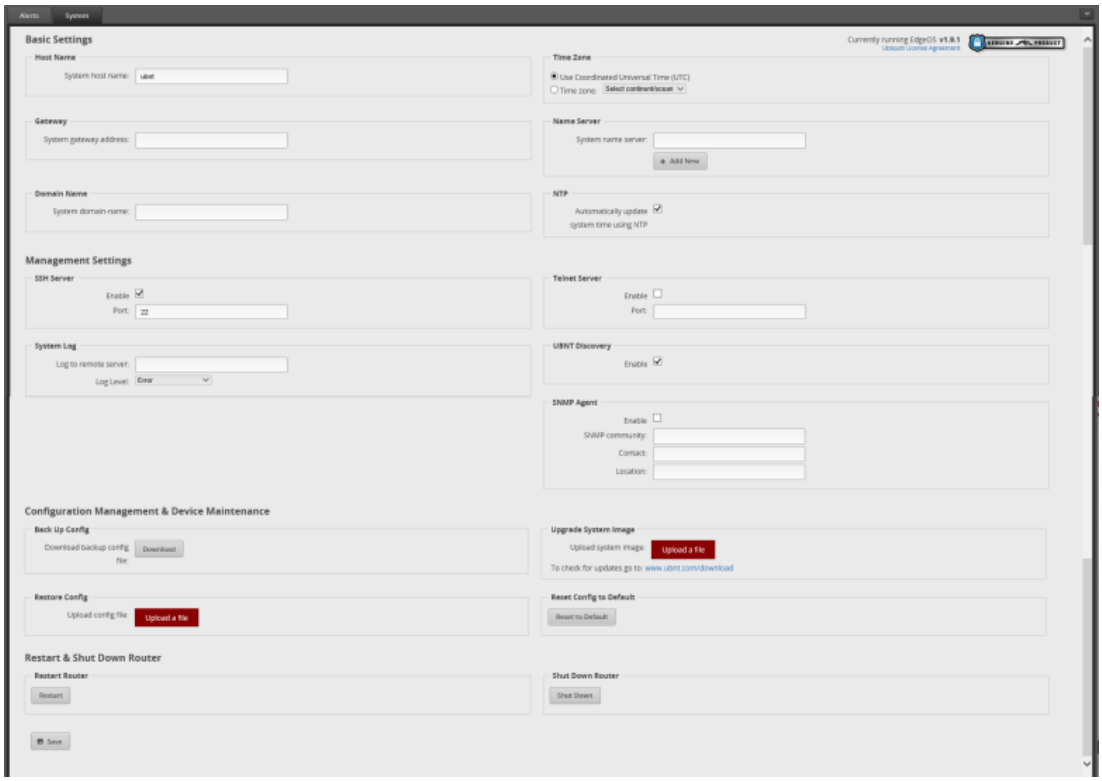


Figure 10 – System Pop-up Screen

Find the "Upgrade System Image" section, and press the "Upload a file" button. See Figure 11 – Upgrade System Image.

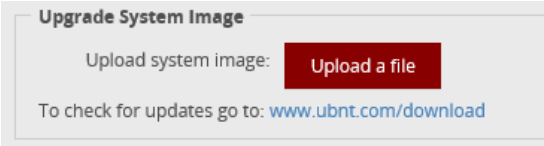


Figure 11 – Upgrade System Image

Choose the firmware file that you downloaded earlier. The EdgeRouter will then install the chosen file. See Figure 12 – Upload a file.

Figure 12 – Upload a file

You will eventually be asked if you want to reboot the EdgeRouter. Press the "Reboot" button. You will then be asked to confirm the reboot, click on the "Yes, I'm sure" button. See Figure 13 – Upgrade Complete Dialog.

The router will inform you that it is rebooting. See Figure 14 – Reboot Process.

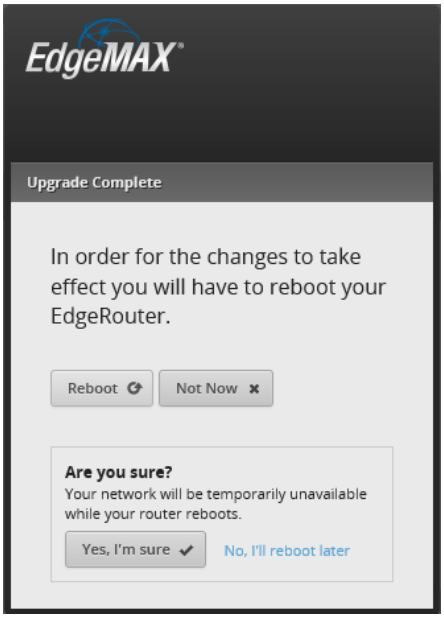


Figure 13 – Upgrade Complete Dialog

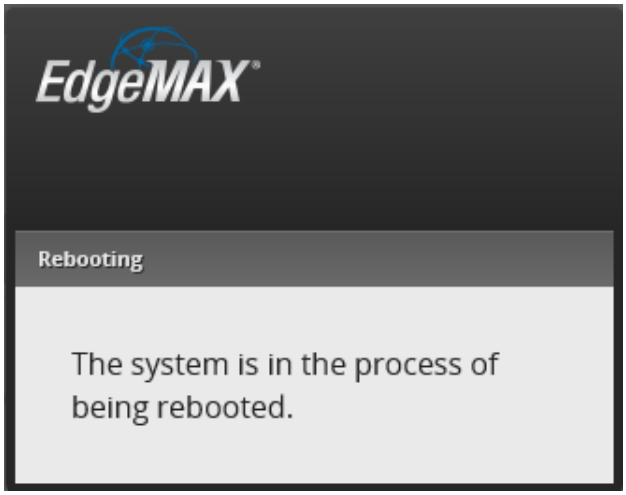


Figure 14 – Reboot Process

While the EdgeRouter is rebooting, the web page will present you with a Lost Connection Dialog. See Figure 15 – Lost Connection Dialog.

Eventually, when the EdgeRouter has fully re-booted, the presented dialog will change to Figure 16 – Timed-Out Dialog. This is a nice touch of web programming from Ubiquiti, so you can easily know when re-booting has completed.

Press the Reload button.

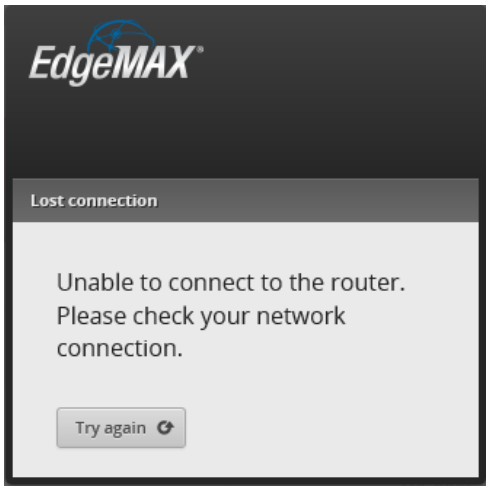


Figure 15 – Lost Connection Dialog

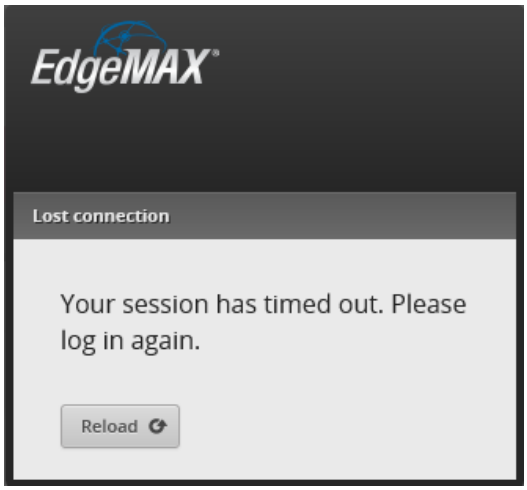


Figure 16 – Timed-Out Dialog

You will be asked to login; please enter the username and password into the dialog. The default username is “ubnt” and the default password is “ubnt”. See Figure 17 – Login Dialog.

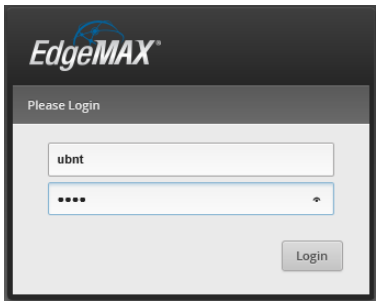


Figure 17 – Login Dialog

You should be presented with a dialog box stating that the “Router is in default config. Do you want to start with the Basic Setup wizard?” Answer “no.” Reference Figure 7 – Basic Setup Question.

You will (again) land at the Dashboard screen. Reference Figure 8 – Initial Dashboard Screen. Check the upper left of the screen and verify that you are presented with the version of code that you just downloaded. See Figure 18 – Example EdgeRouter Version.

Figure 18 – Example EdgeRouter Version

Additional References:

https://help.ubnt.com/hc/en-us/articles/205146110-EdgeRouter-How-to-Upgrade-the-EdgeOS-Firmware

https://community.ui.com/questions/EdgeRouter-X-loses-WAN-IP-around-once-a-week/b183c5a2-e889-4532-9201-43559eed3eaf#answer/faba4035-1105-421a-813e-bba41df9e21f

If you get your EdgeRouter messed up, you might need to factory reset it. Here are some link(s):

https://help.ubnt.com/hc/en-us/articles/205202620-EdgeRouter-Reset-to-Factory-Defaults

https://help.ubnt.com/hc/en-us/articles/360002231073-EdgeRouter-How-to-Use-SSH-Recovery-

https://community.ubnt.com/t5/EdgeRouter/ERX-ERX-SFP-System-Recovery/td-p/2056921

https://community.ubnt.com/t5/EdgeRouter/ERX-ERX-SFP-System-Recovery/m-p/2056921

If you really get your EdgeRouter into a non-booting mode, you could try the new TFTP recovery methods:

https://help.ubnt.com/hc/en-us/articles/360018189493

https://community.ubnt.com/t5/EdgeRouter/TFTP-recovery-images-for-EdgeOS-request/m-p/2676042#M240903

https://community.ubnt.com/t5/EdgeRouter/How-to-connect-ER-X-serial-console/m-p/2607963#M233420

https://community.ubnt.com/t5/EdgeRouter/Updated-Edgerouter-X-to-EdgeMAX-EdgeRouter-software-release-v1/m-p/2711039/highlight/true#M244509

12. About Using Two or More Ubiquiti Access Points

Many people have wanted to connect two (or more) Ubiquiti Access Points (UAPs / APs) to their ER-X to provide more / wider Wi-Fi coverage. The following ideas should work, but I have only tested Methods 1, 1A, and 4. Therefore, the following directions are approximate.

Method 1: Connect an 802.1Q capable switch to eth4, and then connect your Access Points to this switch. I have tested Method 1 using a TP-Link TL-SG105 (Ver 2.1) unmanaged gigabit switch, which was cheap and worked. I am amazed that I just plugged it in and it just worked, as I thought you needed a managed switch to carry VLAN data.

Managed switches will likely need to be specifically configured to pass VLAN 6, 7, 8 data. The HomeNet / trunk / 192.168.3.X data does not appear to need to be specifically configured. I had previously tested Method 1 with a specifically-programmed TP-LINK TL-SG105EV2 managed switch and it worked. For configuration details, for this switch, reference Appendix A. I would now instead use Method1A/1B.

Method 1A: Connect an 802.1Q capable switch to eth3, connect HomeNetwork devices and your additional Access Point(s) to this switch, leaving your original Access Point connected to eth4. This method is lower cost than Method1, as it shares a common switch for both the HomeNet wired items and the extra Access Points(s). It appears that recently-manufactured unmanaged gigabit-switches are 802.1Q compatible. It is likely that old 10/100 (i.e. non-gigabit) switches will NOT be 802.1Q compatible. If you use this method, remember to perform the steps in section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks, when you get to that section. When I did this testing, I used a readily available TP-Link, unmanaged gigabit switch; model TL-SG1005D that I had previously purchased. See also section 92 - So what is the meaning of PVID / VID?

Method 1B: Connect an 802.1Q capable switch to eth3, and then connect HomeNetwork equipment and ALL of your Access Point(s) to this switch, leaving eth4 for a second Separate Network. If you use this method, remember to perform the steps in section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks, when you get to that section. You can also perform the steps in section 101 - Add a Second Separate Network, when you get to that section This method is what I now suggest. See also section 92 - So what is the meaning of PVID / VID?

Method 2: Plug your one or two additional Access Points(s) directly into the ER-X router. You will need to forego the Wired IOT Network and/or the Wired Separate Network, unless you happen to have zero wired devices on the HomeNetwork. This would alternately configure the HomeNet on ports 1,3,4 or 2,3,4 or 1,2,3,4. This saves the cost of needing to purchase an additional 802.1Q capable switch, but delivers fewer features. I would now instead use Method1A/1B.

To include port 1 in HomeNet, instead CHECK the "One LAN" box in section 14 / Figure 21. You will need to figure out the additional associated changes which are later in this document.

To include port 2 in HomeNet, DON'T follow sections 21, 22, 28. You will need to figure out the additional associated changes which are later in this document.

This is a lot of changes / stripping-of-features to save about $20 USD for a gigabit unmanaged switch. I would instead use Method1A/1B.

Method 3: Use an ER-X SFP instead of a “plain” ER-X. This model router has an extra SFP port on it. You will also need an appropriate SFP adapter to use the extra port. Using this Method, just about doubles the cost of this project. I hear that most “copper” SFP modules do not auto-negotiate link speeds. I would now instead use Method1A/1B, as it is much cheaper.

Method 4: Configure the additional Ubiquiti Access Points to Wi-Fi mesh / chain to the original Ubiquiti Access Point. [Update: it appears that multi-hop support has been added in later versions of Access Point’s firmware.] Note that using mesh equipment / modes will likely decrease your wireless bandwidth by at-least half and/or steal (?all of / most of?) your 5GHz channel.

Reference the following:
https://help.ubnt.com/hc/en-us/articles/115002262328-UniFi-UAP-Configuring-Wireless-Uplink

Ubiquiti also makes specific equipment for multi-hop deployments. Some of that equipment is rated for outdoor use. If you can, wire each Access Point back to your EdgeRouter.

General:

Except for method 4, Each Access Point should be Ethernet-wired. When you get there, reference section 77 - Setting UniFi / Access Point's SSIDs, Channels, and Power Levels for configuration details.

See also section 16, the "VLAN References" portion of section 31, and more information in Appendix A.

Ethernet data can be sent over cable TV coax by using "Multimedia over Coax Alliance (MOCA)" adapters. These devices can be used as general purpose Ethernet drops and/or for wiring / placing Access Points within a house. These are discussed in Appendix B.

13. Comments about Network Switches

@shermbug suggests that unmanaged switches not be used for carrying VLAN data.

Most new / gigabit switches will probably work, but at least, ensure your (unmanaged) switches are marked as being 802.1Q capable.

It is probably a good idea, when using (your specific) network switch, to test that all of your Home, Iot, Guest, and Spare Networks are operating correctly.

To test if a specific network switch works, connect some WiFi equipment to the IOT, Guest, Spare Network (one at a time) and see if that equipment connects. Additionally notice if the equipment acquires an IP address in the 6.x, 7.x, or 8.x IP range. For testing, you will need to wait until you reach and follow section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks. Including using the "eth3 vid 6,7,8" portion. See also section 92 - So what is the meaning of PVID / VID?

I am currently using Method1B of section 12 - About Using Two or More Ubiquiti Access Points. I recently purchased a managed 24-port gigabit-switch. It is now the only network switch connected to my ER-X (via eth3) and can provide Ethernet ports for Home, Iot, Guest, and Spare Networks. This single switch replaces all the switches shown in Figure 1 - Overview Diagram and makes for a much cleaner installation.

The model I choose was HP J9803A (Procurve 1810-24G). This was acquired, as used, on eBay for under $60 shipped. This switch support VLANs. If you use this method, remember to perform the steps in section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks, when you get to that section.

The HP J9803A switch is / can-only-be configured via a web page, which is perfect for my home use. I can see why IT professionals may not like this switch, as they cannot be bulk-programmed via command line utilities, in their large commercial settings.

14. EdgeRouter Wizard

Press the “Wizards” button, which is located in the upper-right portion of the Dashboard screen. See Figure 19 – Wizards Button.

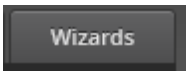


Figure 19 – Wizards Button

You will see the following (portion shown) of the Wizard Screen. See Figure 20 – Wizard Screen Portion.

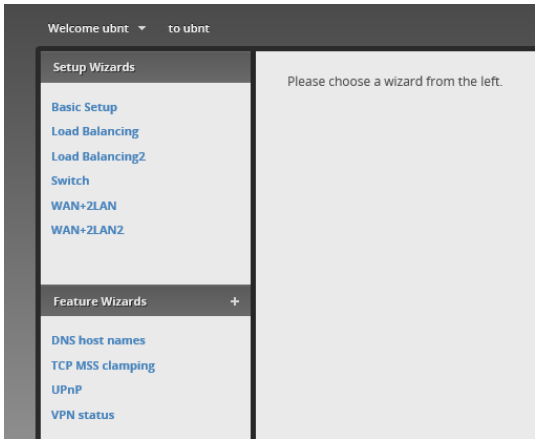


Figure 20 – Wizard Screen Portion

Note that there are various Wizards available, which can turn the EdgeRouter into a network switch, or perform load balancing between two WAN interfaces. Most people will probably be interested in a “standard” setup, as described in this guide, which is “WAN+2LAN2”.

Choose “WAN+2LAN2”. See Figure 21 – Wan+2LAN2 Dialog. You will need to expand / open sections, and make the following selections:

In the “Internet Port” section:

Port:	eth0	
Internet CT:	DHCP	
VLAN:	UN-Checked	(Internet Connection is on VLAN)
Firewall:	CHECKED	(Enable the default firewall)
DHCv6 PD:	UN-Checked	(Enable DHCv6 Prefix Delegation)

In the next (unlabeled) section:

One LAN:	UN-Checked	(Only use one LAN)

In the “(Optional) Secondary LAN port (eth1)” section:

Address:	192.168.4.1 / 255.255.255.0	
DHCP:	CHECKED	(Enable the DHCP server)

In the “LAN ports (eth2, eth3, eth4)” section:

Address:	192.168.3.1 / 255.255.255.0	
DHCP:	CHECKED	(Enable the DHCP server)

If your internet provider uses something other than DHCP (i.e. IP address provided from your cable / dsl modem), you will need to select “Static IP” or “PPPoE”, and then configure those settings accordingly. Some links for dealing with PPoE were given in section 6.

Unchecking the “Only use one LAN” selection informs the Wizard to un-bundle eth1 from eth2-4, allowing for the provision of a separate Network. I used this eth1 Network for Wired IOT devices.

It is important that “Enable the default firewall” is CHECKED. The entire security of this router depends upon this setting.

Under the “User setup” section, either change the default password to something secure / unique or “Create new admin user” with a secure / unique password. If you “Create new admin user”, you will need to also return to this dialog and delete the default “ubnt” login. You will need to remember your login credentials.

[Note you **REALLY** should make a new and unique admin-user login-name and then delete the default ‘ubnt’ login-name for security.]

Press “Apply” at the bottom of the screen.

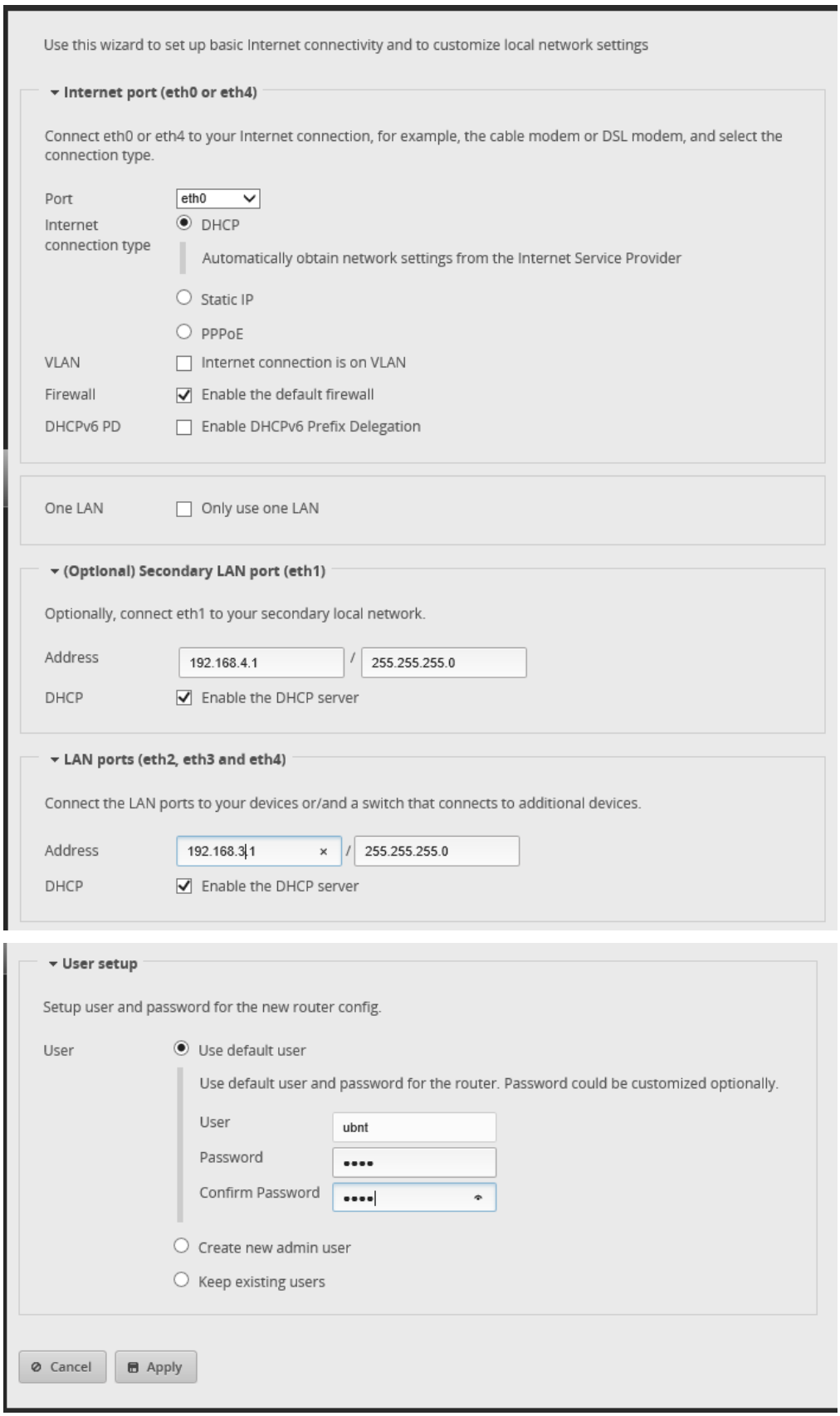


Figure 21 – Wan+2LAN2 Dialog

After Applying, you will be presented with Figure 22 – Replace Configuration. Please study what it says. Press "Apply Changes."

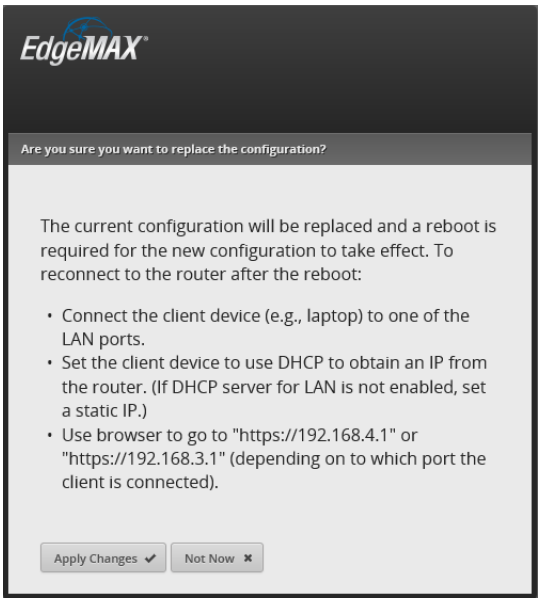


Figure 22 – Replace Configuration

Press Reboot, then confirm the reboot, by pressing the "Yes, I'm sure" button. See Figure 23 – Reboot into New Configuration.

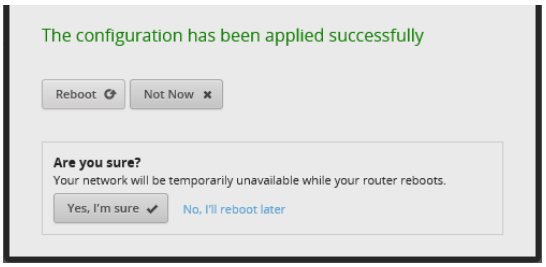


Figure 23 – Reboot into New Configuration

The EdgeRouter will inform you that it is rebooting. Reference Figure 14 – Reboot Process. The EdgeRouter takes several minutes to reboot.

Disconnect your setup computer's Ethernet jack from the EdgeRouter's eth0 connection. Re-configure your setup computer's Ethernet port back to using DHCP. Again, there are many tutorials available on the internet that show how to configure a computer's Ethernet jack to use DHCP. Reference section 9 - Initial EdgeRouter Hardware Setup, but instead choose "Obtain an IP address automatically." Also reference Figure 3 – Windows 10 Ethernet Address Setup.

15. EdgeRouter Re-Connection

Ensure that your existing router's LAN ports are not using any of the addresses utilized by the EdgeRouter, i.e. not using 192.168.3.0 through 192.168.8.255. Reference section "6 - EdgeRouter IP Address Use." Connect the EdgeRouter's eth0 port into your existing router's LAN port with a standard Ethernet cable. Connect your setup computer's Ethernet port (now re-configured for DHCP) into the EdgeRouter's eth3 port. See Figure 2 - EdgeRouter Configuration Setup.

Open a web browser on your computer and enter https://192.168.3.1 into the address field.

Acknowledge the browser's security warning, Reference Figure 5 – IE Security Certificate Example.

Login to your EdgeRouter, as shown in Figure 17 – Login Dialog.

You will be presented with the Dashboard Screen. See Figure 24 – Dashboard Screen.

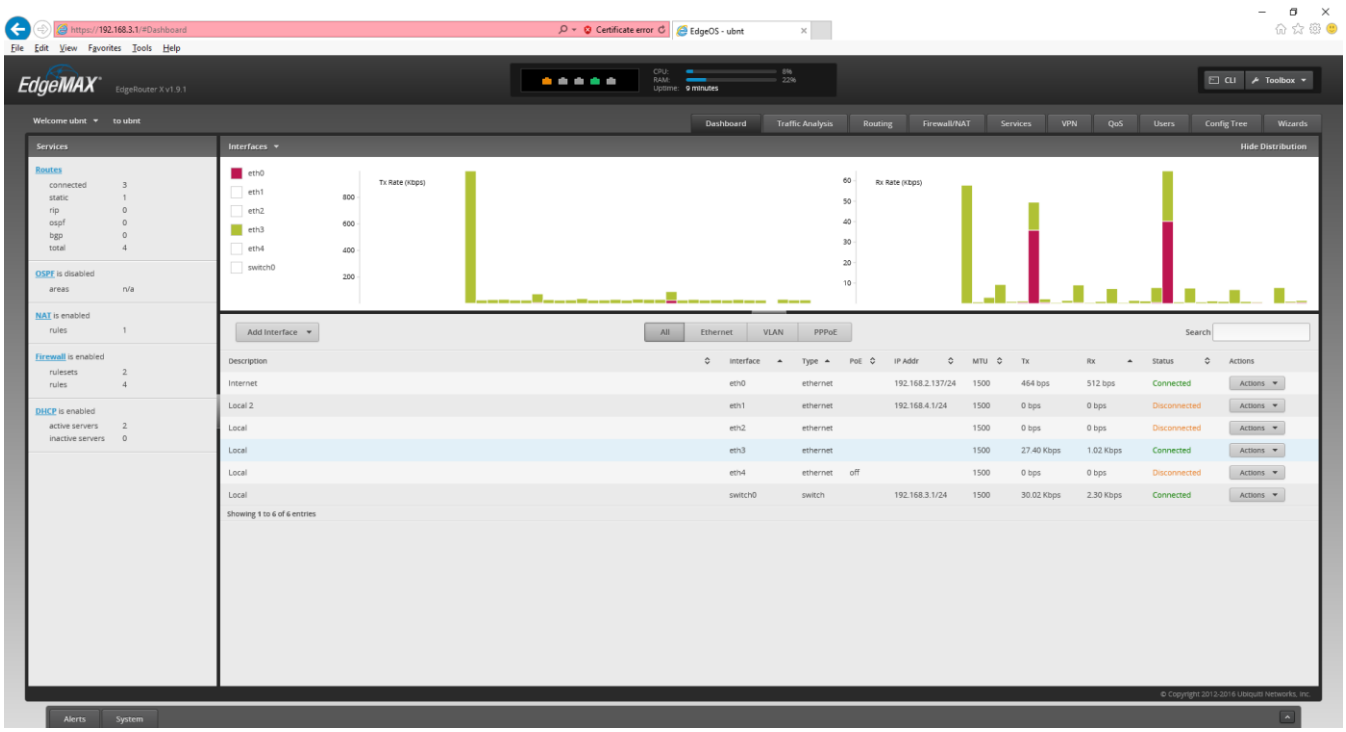


Figure 24 – Dashboard Screen

16. Network Naming

Setting up the EdgeRouter, per this guide, provides for several separate Networks. In this guide, I try to use the word "Network" (capitalized) for these. Each Network has a unique IP address range / subnet. See Table 1 - Table of Networks.

Network Name	IP Address Range	Interface	VLAN
Internet	DHCP	eth0	No
Home Network	192.168.3.X	eth3, eth4	No
(Wired) IOT Network	192.168.4.X	eth1	No
Wired Separate Network	192.168.5.X	eth2	No
Wi-Fi Guest Network	192.168.6.X	-	6
Wi-Fi IOT Network	192.168.7.X	-	7
Wi-Fi Spare Network	192.168.8.X	-	8

Table 1 - Table of Networks

Some of these Networks are on a Virtual LAN (VLAN). VLANs provide the ability for separate network data to be carried over shared Ethernet cables. Data that is "tagged" as belonging to a specific VLAN cannot interact with either non-VLAN data (trunk data) or with data from any different VLAN.

When VLANs are used, all devices involved with this data need to be VLAN aware. Any network switches carrying VLAN traffic will need to be IEEE 802.1Q capable, e.g. a Level 2 switch.

Note that the only VLAN traffic shown in Table 1 - Table of Networks is involved with the Wi-Fi Guest, Wi-Fi Iot, and Wi-Fi Spare Networks. The Ubiquiti AP-AC-LR Access Point is VLAN aware. Eventually the Ubiquiti Access Point will be plugged directly into the EdgeRouter's eth4 interface, so VLAN data will be able to be carried between them. If you are going to deploy multiple Access Points, then the network switch attaching the Access Points to the EdgeRouter's (eth3 and/or) eth4 port MUST be IEEE 802.1Q capable. It appears that recently-manufactured unmanaged gigabit-switches are 802.1Q compatible.

This Wi-Fi VLAN data does NOT need to flow to devices on the Wired Home Network; therefore, the network switch attached to the EdgeRouter's eth3 interface can be an (inexpensive) unmanaged switch. Reference Figure 1 - Overview Diagram. If they are needed, the network switches attached to the EdgeRouter's eth1 and/or eth2 interfaces can also be (inexpensive) unmanaged switches.

Each Network is also customizable to provide functionality and connectivity. The rest of this guide should provide sufficient details on that.

There are many VLAN references on the web. Here is one brief tutorial:
http://www.microhowto.info/tutorials/802.1q.html

More References:
https://help.ubnt.com/hc/en-us/articles/204976664-EdgeRouter-Packets-Processing

I was asked to add a reference for google config to this guide, so here it is:
https://github.com/mjp66/Ubiquiti/issues/31

17. EdgeRouter Command Line Interface (CLI)

In most of Ubiquiti's Edgerouter forum posts, steps to (re-)configure items are given as Command line Interface (CLI) commands. In fact, not very many GUI screenshots are used, and they are typically posted only by novices.

The following steps show how to open and use the built-in CLI interface. Click on the "CLI" button, in the upper-right screen. See Figure 25 – CLI Button.

Figure 25 – CLI Button

The initial CLI window will appear as a semi-transparent overlay. See Figure 26 – Initial CLI Window.

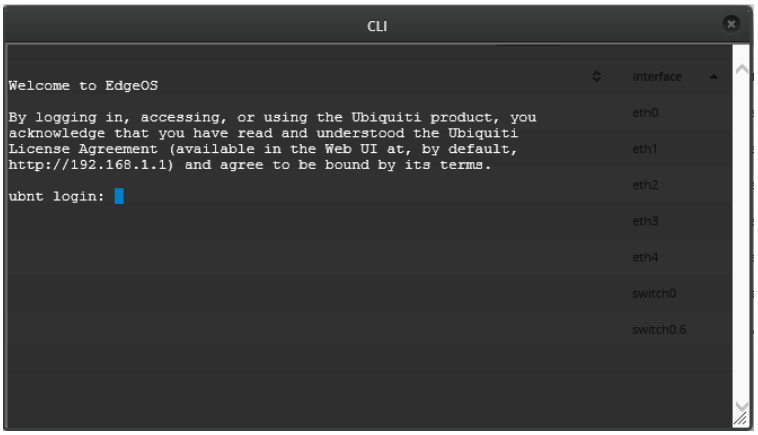


Figure 26 – Initial CLI Window

Login to this window, using your EdgeRouter's user name and password. You will now be presented with a command prompt. See Figure 27 – Logged-In CLI Window.

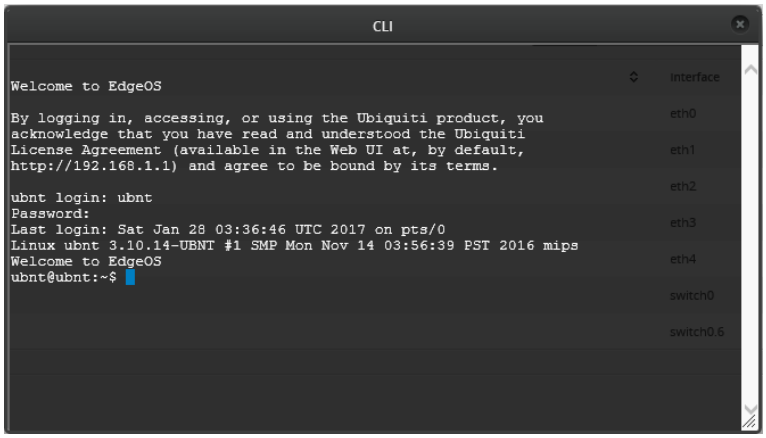


Figure 27 – Logged-In CLI Window

CLI commands are typically divided into configuration commands and non-configuration commands. The CLI interface will accept only configuration commands when in configuration mode. Type the "configuration" command to enter configuration mode. The "exit" command is used to leave configuration mode and return to normal (non-configuration) mode.

If you enter the “configure” command, the CLI window’s prompt will now include “[edit]”, and the prompt will change to ‘#’. See Figure 28 – Configure CLI Window.

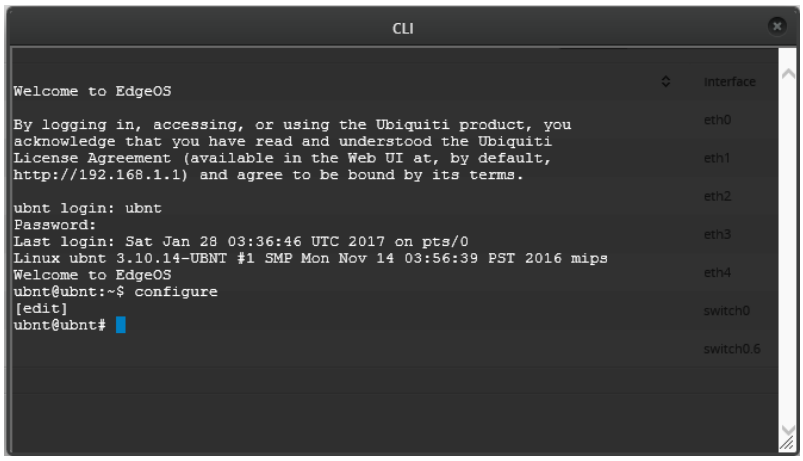


Figure 28 – Configure CLI Window

Many times when doing a commit and/or a save command, the page will need to be refreshed. A refresh dialog box will pop-up on the screen. See Figure 29 – Configuration Change. Press the “Refresh” button.

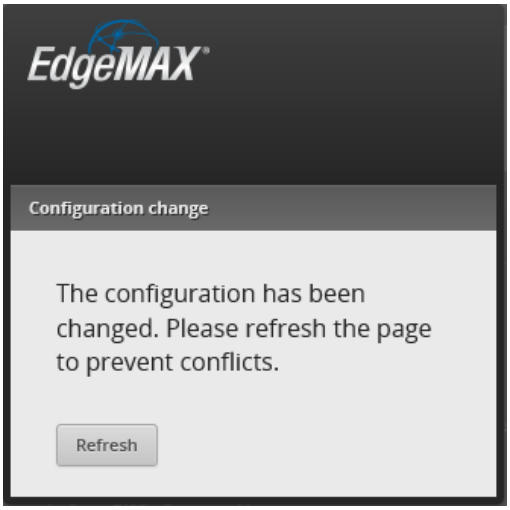


Figure 29 – Configuration Change

You can also use a popular Windows program, called putty.exe, to Secure Shell (SSH) into the EdgeRouter, and then issue CLI commands. Unlike the CLI interface, Putty has the ability to do Copy / Paste. Linux users should already be familiar with how to use SSH. There is also a Windows specific program WinSCP, which is similar to SSH, but easily transfer files between a Windows PC and the EdgeRouter. There is also a “`commit-confirm`” command, described in the next URL.

Here are some CLI references:

https://help.ui.com/hc/en-us/articles/204960094-EdgeRouter-Configuration-and-Operational-Mode
https://dl.ubnt.com/guides/edgemax/EdgeSwitch_CLI_Command_Reference_UG.pdf
https://community.ubnt.com/t5/EdgeMAX/EdgeOS-CLI-Primer-part-1/td-p/285388
https://community.ubnt.com/t5/EdgeMAX-CLI-Basics-Knowledge/tkb-p/CLI_Basics@tkb

18. EdgeRouter Config Tree

There is a neat and alternate way to configure the EdgeRouter. Near the top of the screen is a “Config Tree” button. See Figure 30 – Config Tree Button.

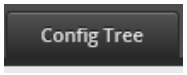


Figure 30 – Config Tree Button

When you press it, the “Configuration” Tree window will appear. See Figure 31 – Config Tree Initial Screen.

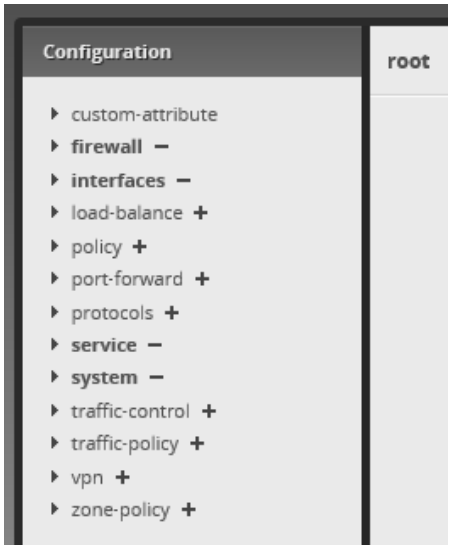


Figure 31 – Config Tree Initial Screen

Using the config tree is an alternate method (for some items) to using the Command Line Interface (CLI).

19. My Command Line Trouble

When I was experimenting with dnsmasq, many internet resources simply gave CLI commands to enable this feature. When I tried some of these commands, my EdgeRouter had problems. I no longer remember what the exact problem was, but I noticed that sometimes when using the Config Tree, multiple commands were issued.

See Figure 32 – Example of Multiple Config Tree Commands.

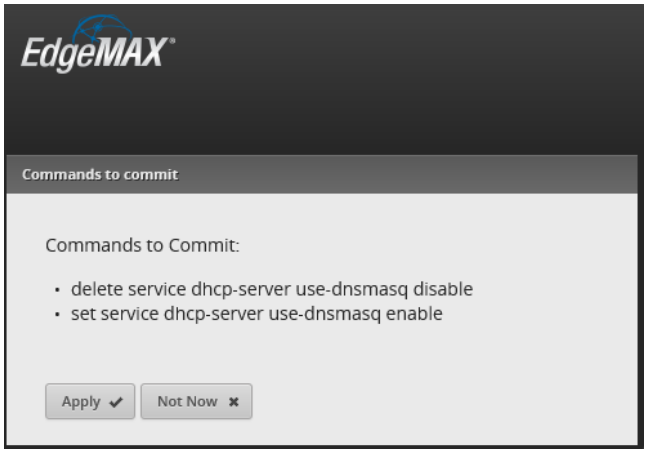


Figure 32 – Example of Multiple Config Tree Commands

20. EdgeRouter Backup / Restore Configuration Files

WARNING: As of early 2020, many forum users are reporting that newer versions of Google's Chrome browser may no-longer work for uploading / downloading system images and/or configuration files. Try to use a FireFox browser. Reference https://community.ui.com/questions/Has-Chrome-83-broken-restoring-configuration-backups/c6a2d0e6-5f0d-494e-b588-c477cf5e19e4

When EdgeRouters are described in most internet forums, their configuration parameters are usually described (in text) by a standard file format. Eventually, you will need to be fluent in reading these files and translating that data into actions taken in the Command Line Interface (CLI), the Config Tree or the GUI.

You can find this configuration data within the config.boot file that is inside of the backup file generated from the system window. The file that is generated is typically named edgeos_ubnt_<date>.tar.gz, with <date> replaced by numbers representing todays date.

To generate a backup file, first press the System button, as shown in Figure 9 – System Button. You will be presented with the System screen, as shown in Figure 10 – System Pop-up Screen.

Find and press the "Download" button under the Configuration Management & Device Management section. See Figure 33 – Back Up Config Download Button.

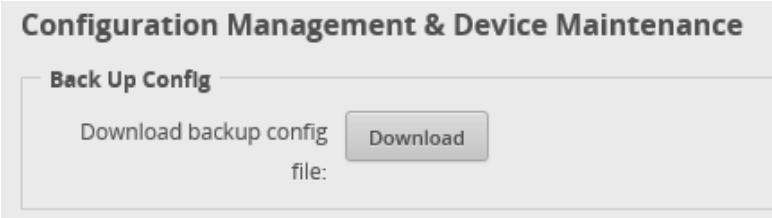


Figure 33 – Back Up Config Download Button

You will be presented with a dialog of where to (open or) save your backup file. This dialog is browser specific. Save your file to a directory of your choice on your setup computer. This file will be needed if you ever need to reload your EdgeRouter. You may want to do this frequently, when setting up this device.

Another way to obtain a relevant portion of this file is to issue one of the following commands into the Command Line Interface (CLI) window. For information about the CLI, reference section "17 - EdgeRouter Command Line Interface (CLI)".

Two different / similar normal-mode CLI command for acquiring the system configuration are:

```
cat /config/config.boot
show configuration | no-more
show configuration | cat
```

I will show as many portions of this config data as possible throughout this guide. One goal of this guide is to teach users enough about this EdgeRouter that they are comfortable reading and understanding the backup files.

You would do well to save / keep multiple backup files, while you are working through this guide.

An alternate method of generating backup data is to issue one of these commands:

```
show configuration commands
show configuration commands | cat
```

which dumps a list of configuration commands which should re-generate your installation. Internally generating this list has to be pretty crazy, since many commands will depend upon other commands having already being entered.

To restore a configuration file, first press the System button, as shown in Figure 9 – System Button. You will be presented with the System screen, as shown in Figure 10 – System Pop-up Screen.

Find and press the "Upload a file" button under the Configuration Management & Device Management section. See Figure 34 – Restore Config Upload a file Button.

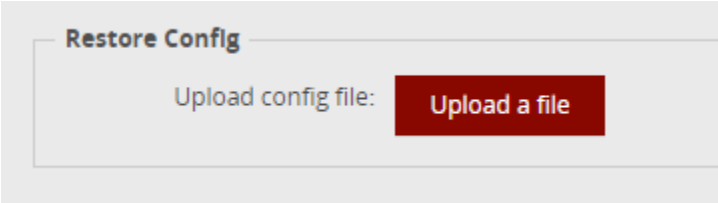


Figure 34 – Restore Config Upload a file Button

You will be asked to select and "Open" a previously generated configuration file.

Note: Sometimes to upload a configuration file, you might need to first recover more space on your ER-X router. You can issue the CLI command:

```
delete system image
```

to recover more space. Note that this deletes the backup (configuration) image, not the running (configuration) image. Only do this command if you cannot otherwise update. Reference Section 17 - EdgeRouter Command Line Interface (CLI).

Link(s):
https://help.ubnt.com/hc/en-us/articles/360002535514

https://community.ubnt.com/t5/EdgeRouter/Edgerouter-CLI-command/m-p/2728959

21. Remove eth2 from the EdgeRouter's Internal Switch

In this optional step, we will manually un-bundle the eth2 interface from the EdgeRouter's internal switch chip to provide for the Wired Separate Network on the eth2 interface. Un-bundling this interface from switch0 enables a separate physical network. An additional network could be achieved by adding a logical VLAN, but we are choosing to implement an additional network on the physical eth2 port. The switch chip will remain enabled for eth3 and eth4 interfaces. Later, we will assign an IP address range to this port, setup DHCP to provide IP addresses to eth2 connected devices, and create firewall rules that will keep this Network isolated from the other Networks. If you choose to not implement the Wired Separate Network, there are other associated steps you will not perform.

Press the Dashboard Button. See Figure 35 – Dashboard Button.

Figure 35 – Dashboard Button

On the right side of the Dashboard screen, select switch0's "Actions" button. See Figure 36 – switch0's Action Button.

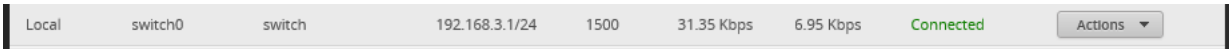


Figure 36 – switch0's Action Button

A sub-menu will appear, Select "Config" from the menu items. See Figure 37 – switch0 Actions Config.

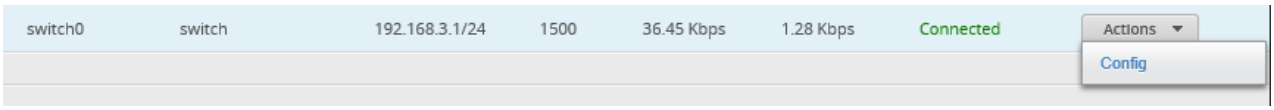


Figure 37 – switch0 Actions Config

You will be presented with the configuration dialog for switch0. See Figure 38 – switch0 Configuration.

Select the VLAN tab. Under the section labeled "Switch Ports", UN-CHECK eth2. See Figure 39 – switch0 Switch Ports.

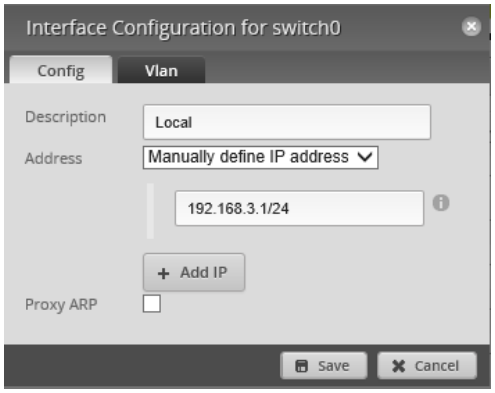


Figure 38 – switch0 Configuration

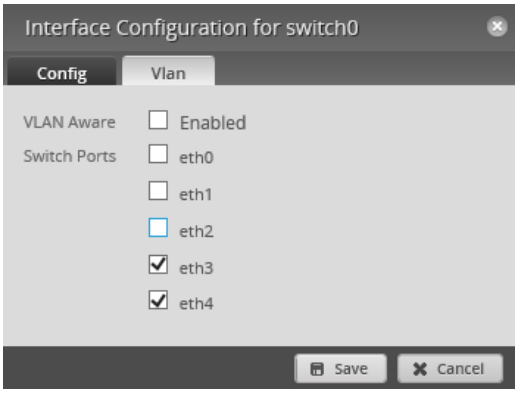


Figure 39 – switch0 Switch Ports

Press “Save”. While the EdgeRouter is completing this task, a busy indicator will spin, in the upper right corner of the dialog. See Figure 40 – Busy Indicator. Wait for the Busy Indicator to finish spinning. It will be replaced by a Green checkmark when the task is completed. See Figure 41 – Finished Checkmark.

Figure 40 – Busy Indicator

Figure 41 – Finished Checkmark

22. Configure EdgeRouter's eth2 IP Addresses

Now that the eth2 interface has been un-bundled, we need to allocate a new IP address range to this interface.

On the right side of the Dashboard screen select eth2's "Actions" button. See Figure 42 – eth2's Actions Button.

Figure 42 – eth2's Actions Button

A sub-menu will appear, See Figure 43 – Interface Actions.

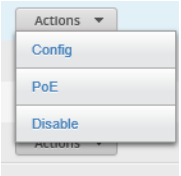


Figure 43 – Interface Actions

Select "Config". You will be presented with Figure 44 – Configuration for eth2 Dialog.

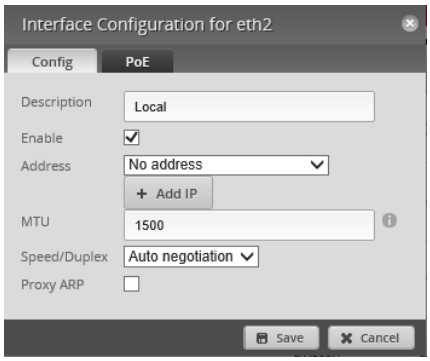


Figure 44 – Configuration for eth2 Dialog

Under the Address selection, choose "Manually define IP address", and enter "192.168.5.1/24" into the address field. See Figure 45 – eth2 Address Dialog.

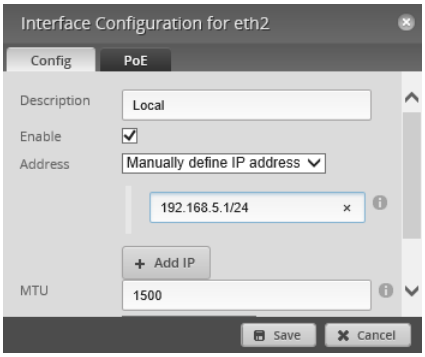


Figure 45 – eth2 Address Dialog

Click the Save button.

23. About DNS settings

I seem to have spent more time investigating DNS settings for the EdgeRouter than in learning firewall rules.

A DNS explanation: https://www.cloudflare.com/learning/dns/what-is-dns/

Within my router, and within this guide, I tried using Quad9 DNS addresses, but have now switched back to Level3 DNS addresses for the Home Network. For training / clarity purposes within this guide, I am using Google DNS resolvers for the Separate Network and within the EdgeRouter Itself. I also optionally forced OpenDNS DNS addresses for the IOT Network. Some people have reported that Quad9 is slower, See Section 75 - Adblocking and Blacklisting as a security alternative.

Change any or all of the listed DNS providers to ones of your own choosing. These are used within this guide:

Level3 (CenturyLink) resolver addresses are	209.244.0.3	209.244.0.4
Google resolver addresses are	8.8.8.8	8.8.4.4
OpenDNS resolver addresses are	208.67.222.222	208.67.220.220

Steve Gibson has a web page that can help you characterize various DNS providers. Since it runs from your computer, the results are localized to your connection / ISP. Until the EdgeRouter is fully setup, you might want to run this from a computer that is currently wired outside of the EdgeRouter. This is shown as "Existing LAN" in Figure 2 - EdgeRouter Configuration Setup. The page is at:

https://www.grc.com/dns/benchmark.htm

Steve Gibson has another web page that tests the "spoofability" (security) of DNS resolvers. It is at:
https://www.grc.com/dns/dns.htm

Here are some alternate DNS resolvers, and additional DNS information pages:
https://en.wikipedia.org/wiki/List_of_managed_DNS_providers
https://dns.norton.com/configureRouter.html,
https://dns.norton.com/faq.html
https://support.opendns.com/hc/en-us/articles/228006047-Generalized-Router-Configuration-Instructions
https://use.opendns.com/#router
https://en.wikipedia.org/wiki/OpenDNS
https://www.quad9.net/ and https://www.quad9.net/faq
https://www.globalcyberalliance.org/initiatives/quad9.html

EdgeRouter DNS References:
https://help.ubnt.com/hc/en-us/articles/115010913367-EdgeRouter-DNS-Forwarding-Setup-Options
https://community.ubnt.com/t5/EdgeMAX/ERL-3-1-9-0-No-DHCP-leases-since-switching-to-DNSMasq/td-p/1644201
https://community.ubnt.com/t5/EdgeMAX/Traffic-Analysis-host-name-resolution/m-p/1774017#M141121
https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/
https://community.ubnt.com/t5/EdgeRouter/DNS-Forwarding-Name-Servers/td-p/1117142
https://community.ubnt.com/t5/EdgeRouter/Setting-up-Local-DNS/td-p/449259
https://community.ubnt.com/t5/EdgeRouter/DNS-forwarding-listen-on-vs-dns-server-on-DHCP-server/m-p/2613931

For more information on Quad9, see:

Security Now Podcast #638 at https://www.grc.com/securitynow.htm
Reference: https://github.com/mjp66/Ubiquiti/issues/13 and https://www.quad9.net/faq

24. dnsmasq

There are two different DNS packages available within the EdgeRouter. They are ISC (default) and dnsmasq. Dnsmasq was incomplete as of firmware 1.9.0 and had an additional bug added in firmware 1.9.1, I think it was re-broken and fixed during the hoxfixes of 1.9.7. I now suggest that you DON'T use ISC and that you DO use dnsmasq. See link "ER-X doesn't block dhcp server" further down in this section. Dnsmasq seems to be more DHCP than DNS.

To enable dnsmasq, enter the Config Tree. Reference section "18 - EdgeRouter Config Tree." Select and open up the following config tree sub-menu items from the configuration screen:

service
dhcp-server

You should see some DHCP settings, including use-dnsmasq and hostfile-update. (Note, your screen will still show "disable"). See Figure 46 – use-dnsmasq.

Configure

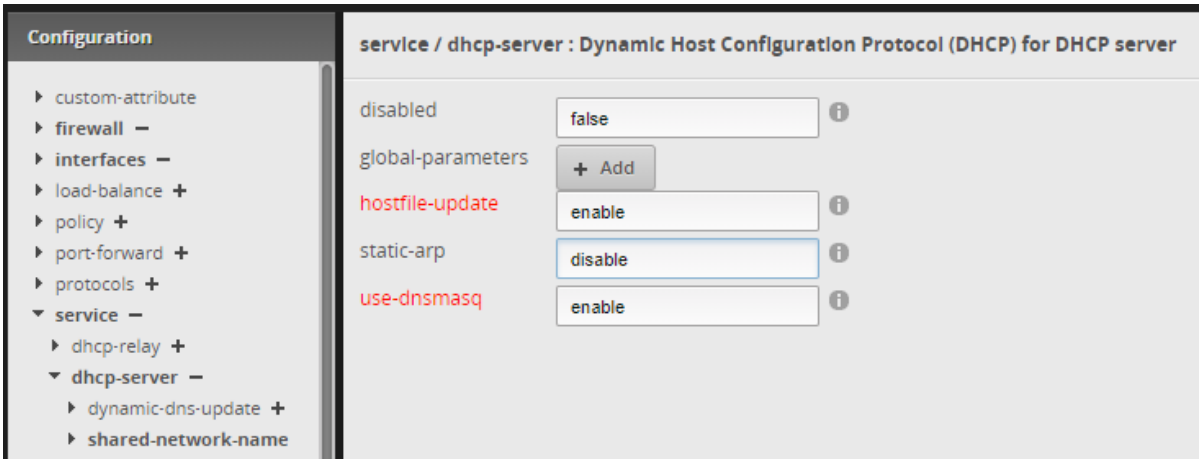


Figure 46 – use-dnsmasq

Type "enable" in the use-dnsmasq box and in the hostfile-update box. Then press the "Preview" button. See Figure 47 – commit-dnsmasq.

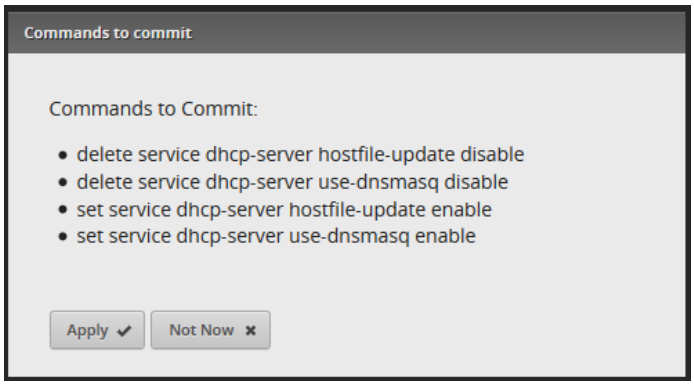


Figure 47 – commit-dnsmasq

Press "Apply." You should see the message "The configuration has been applied successfully", in green, near the bottom of the screen.

With local hostname resolution, you can lookup different devices / PCs on your Network by just referencing the name of the device / PC. For instance, you can look up a second PC on your Home Network from another PC on your Home Network by referencing its name, i.e. by typing (example) "ping DifferentPcName" or by entering "http://DifferentPcName" (if it is a web server), etc.... You may need to add ".local" to the end of the name.

To allow local hostname resolution, perform the following changes. Drop into the Command Line Interface (CLI) and issue the following commands:

```
configure
set system name-server 127.0.0.1
set service dns forwarding listen-on switch0
set system domain-name home.local
commit
save
exit
```

You should see a yellow "The configuration has been changed and is in the process of being committed" message. See Figure 48 – The Configuration has been changed message

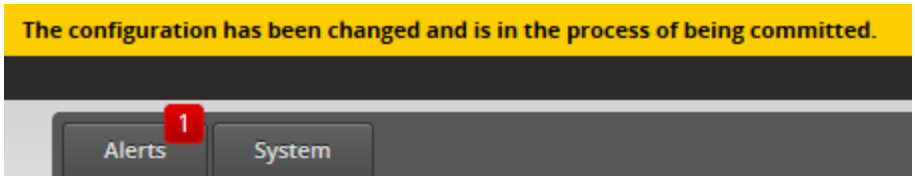


Figure 48 – The Configuration has been changed message

ER-X doesn't block dhcp server:
https://community.ui.com/questions/ER-X-doesnt-block-dhcp-server/e2c9b13c-8bdf-43eb-8bdc-26637edbc648

References:

https://help.ui.com/hc/en-us/articles/115002673188-EdgeRouter-DHCP-Server-Using-Dnsmasq

https://help.ubnt.com/hc/en-us/articles/115002673188-EdgeRouter-Using-dnsmasq-for-DHCP-Server

https://community.ubnt.com/t5/EdgeRouter/vlan-can-not-connect-to-management-plane-or-internet/m-p/2724332/highlight/true#M245769

https://community.ubnt.com/t5/EdgeRouter/Help-with-dnsmasq-on-ER-X/m-p/2477434

Additional and external:
https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/

25. Aliases for devices on your Network

The Edgerouter provides commands which allow you to generate an alias for addressing / accessing equipment on your local Network using a different / additional name. This equipment will need to have its IP address reserved. To reserve the devices IP address, see section 87 - Reserving Device Addresses via DHCP.

I originally saw this posing:
https://community.ui.com/questions/dnsmasq-dhcp-hostnames-and-aliases/2e736a97-9f23-4ff0-a624-4ace4a6a7a2f

Which led me to this help page:
https://help.ui.com/hc/en-us/articles/115002673188

Where I saw the following (example) commands:

set system static-host-mapping host-name uap-pro.ubnt.local inet <ip-address>
set system static-host-mapping host-name uap-pro.ubnt.local alias uap-pro

See section 15 - EdgeRouter Command Line Interface (CLI) for how to issue commands.
To play with this, I issued the following commands via CLI:

set system static-host-mapping host-name router.local inet 192.168.3.1
set system static-host-mapping host-name router.local alias router2.local

Using this example, I can now access my ER-X router using any of the following URLs:

https://192.168.3.1/
https://router.local/
https://router2.local/

FYI, the backup file now contained this additional text:

```
static-host-mapping {
    host-name router.local {
        alias router2.local
        inet 192.168.3.1
    }
}
```

26. System DNS Settings

This step instructs the EdgeRouter ITSELF to use specific DNS servers to resolve web URLs into IP addresses. These DNS servers are specified under the System widow.

Press the “System” button. Reference Figure 9 – System Button.

On the system window, find the Name Server Box. See Figure 49 – Initial System Name Server.

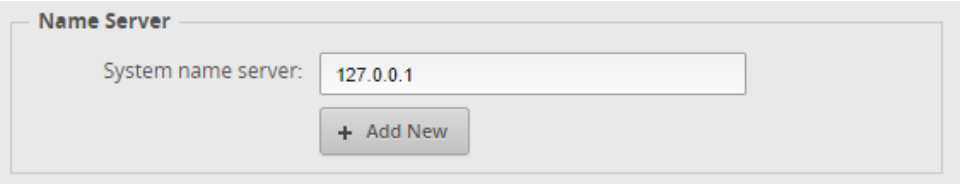


Figure 49 – Initial System Name Server

Your box should already be filled-in with 127.0.0.1, as this was set by CLI in the previous section. You can leave it, or change it (as I did) to two DNS resolver addresses of your choice. I used Google addresses for this guide. Most external DNS resolver systems have multiple resolver addresses, in case of failure; ensure that you add both the primary and secondary resolver addresses by (erasing what is already there and/or) pressing the “+ Add New” button. See Figure 50 – Example Google DNS System DNS Entries.

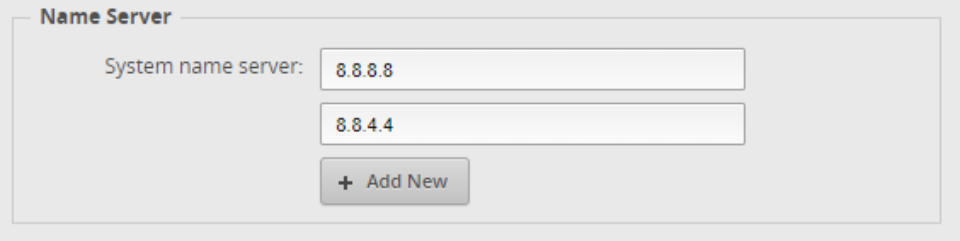


Figure 50 – Example Google DNS System DNS Entries

When you are done editing, press the Save button near the bottom of the system page. See Figure 51 – System Save Button.

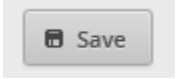


Figure 51 – System Save Button

27. Remove ISP Provided DNS Resolvers

I don't want to depend upon the DNS servers that are provided by my dsl / cable modem. The specific DNS resolver addresses are specified as part of the DHCP data, which is given to the EdgeRouter's eth0 WAN port from the dsl / cable modem. Performing the commands in this section is optional / up to you.

These ISP DNS servers are probably OK, but I don't trust the security of phone-company/cable-company provided modems. Consumer modems are typically full of unpatched security holes, and many have programmed backdoors in them. Commercial modems bulk produced by the lowest bidder and externally controlled by large, uncaring companies have got to be even worse.

In particular, there are DNS changer worms, which attack consumer / commercial routers and change their DNS resolver settings. The way to help circumvent this problem is to instruct the EdgeRouter to ignore the DHCP provided DNS resolver address from your commercial router / ISP.

Since the DNS changer worm could attack an EdgeRouter, remember to change the EdgeRouter's default password to something strong. You don't want to end up like these people:
https://www.routersecurity.org/bugs.php,

-> January 2018, -> MikroTik and Ubiquiti Routers defaced due to default passwords

To see the DNS resolvers being used by the EdgeRouter, issue the CLI command:

```
show dns forwarding nameservers.
```

(For information on the CLI, reference section "17 - EdgeRouter Command Line Interface (CLI)")

The following text shows the Google resolver addresses that were entered into the system page, and an ISP-provided resolver, delivered via my existing / upstream router, which has an address of 192.168.2.1:

```
------------------------------------------------
   Nameservers configured for DNS forwarding
------------------------------------------------
8.8.8.8 available via 'system'
8.8.4.4 available via 'system'
192.168.2.1 available via 'dhcp eth0'
```

To remove the ISP-provided nameserver, drop into the Command Line Interface (CLI) and issue the following commands:

```
configure
set service dns forwarding system
commit
save
exit
```

To see if this worked, re-issue the CLI command "`show dns forwarding nameservers`". This is what I got:

```
-----------------------------------------------
   Nameservers configured for DNS forwarding
-----------------------------------------------
8.8.8.8 available via 'optionally configured'
8.8.4.4 available via 'optionally configured'

-----------------------------------------------
 Nameservers NOT configured for DNS forwarding
-----------------------------------------------
192.168.2.1 available via 'dhcp eth0'
```

Reference https://community.ubnt.com/t5/EdgeMAX/Change-WAN-DNS-Server/td-p/977885

According to https://github.com/mjp66/Ubiquiti/issues/11, you would restore using your ISP's resolvers with the following commands:

```
configure
delete service dns forwarding system
set service dns forwarding listen-on eth0
commit
save
exit
```

Some DNS references:
https://community.ui.com/questions/Check-if-DNS-is-not-leaking-ISP-transparent-DNS/ad58975d-c21a-4c5b-9c99-c557abfdfb04

28. Configure EdgeRouter's eth2 DHCP Server

Now that eth2 has been un-bundled, and has a unique IP subnet assigned to it, we need to provide a DHCP server on this port. Near the top of the screen select the "Services" button. See Figure 52 – Services Button.

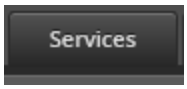


Figure 52 – Services Button

Ensure that the "DHCP Server" tab is selected. See Figure 53 – DHCP Server Screen.

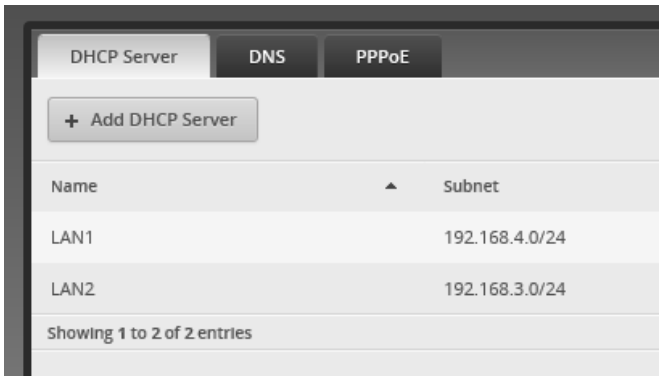


Figure 53 – DHCP Server Screen

Note that I am using Google resolver addresses for DNS1 and DNS2 (below). You can change these to providers of your choice.

Click on the "+ Add DHCP Server" button. You will be presented with a Create DHCP Server dialog. See Figure 54 – Create eth2 DHCP Server Screen. Fill in the form as follows:

DHCP Name:	SecureNetDHCP
Subnet:	192.168.5.0/24
Range Start:	192.168.5.38
Range Stop:	192.168.5.243
Router:	192.168.5.1
DNS 1:	8.8.8.8
DNS 2:	8.8.4.4
Unifi Controller:	<Leave Blank>
Enable:	CHECKED

Click "Save."

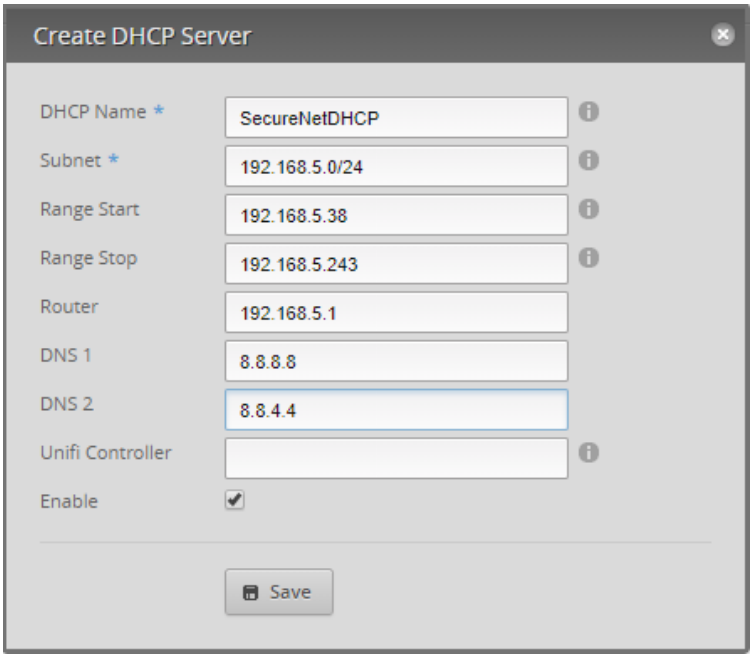


Figure 54 – Create eth2 DHCP Server Screen

I used the same range start and range stop values (38 and 243) that the wan+2lan2 wizard used within the DHCP servers for LAN1 and LAN2.

For some reason, the Ubiquiti GUI programmers seem to have forgotten to include the setting of "authoritative enable" and "domain" from this GUI interface. Setting of those will come later.

29. Configure EdgeRouter's Time Zone

Near the bottom of the screen select the "System" button. Reference Figure 9 – System Button. Find the section titled "Time Zone" and configure the data in these fields according to the time zone you are in, unless you want your router to remain in UTC. See Figure 55 – Time Zone.

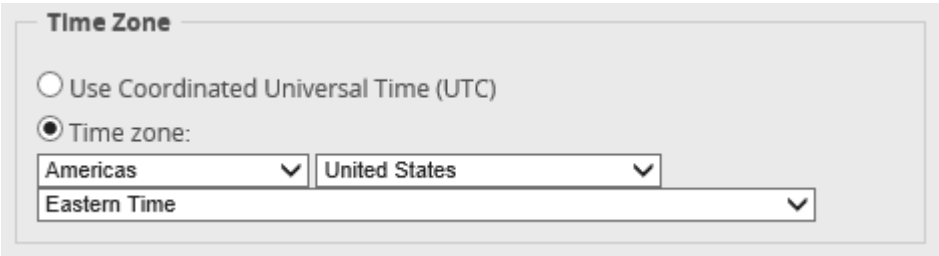


Figure 55 – Time Zone

Press the Save button, Reference Figure 51 – System Save Button.

30. DNS Forwarding

Press the “Services” button, near the top right of the window. Reference Figure 52 – Services Button. Ensure that the “DNS” Tab is selected. See Figure 56 – DNS Tab.

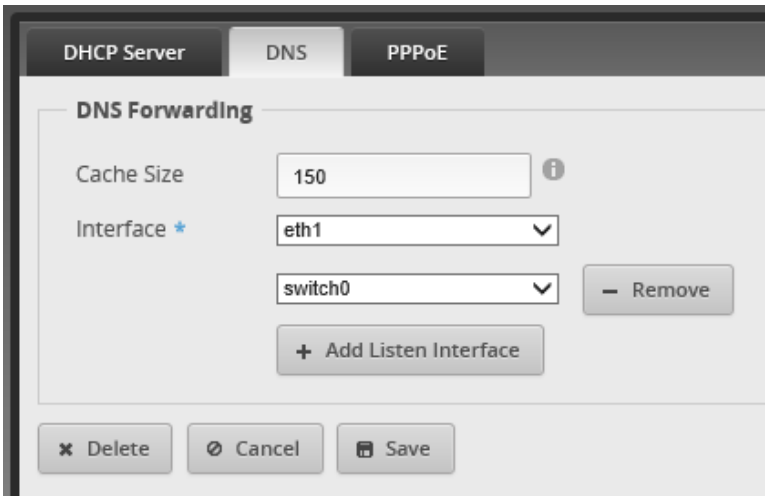


Figure 56 – DNS Tab

I changed my cache size to 400. We want to remove eth1 from this list. Change the first item (which can’t be removed) to “switch0”. Then press the “- Remove” button to the right of the second item. The result should look like Figure 57 – Remove eth1 from DNS. Press “Save.”

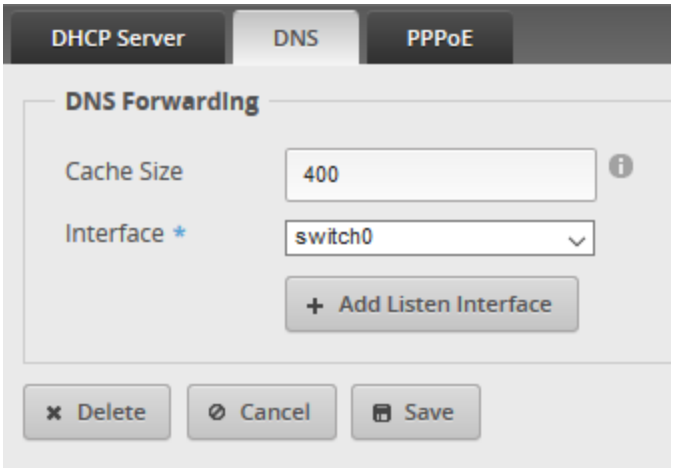


Figure 57 – Remove eth1 from DNS Forwarding

31. Add VLAN Networks to the EdgeRouter

The Ubiquiti AC-AP-LR Wi-Fi Access Point can manage up to four separate Networks / SSIDs, by using VLANS. VLANS allow separated IP data to flow over one Ethernet cable, without the data being mixed together. This section will create three new Networks using VLANs.

Press the Dashboard button near the top of the Screen. Reference Figure 35 – Dashboard Button. On the upper left side of the Dashboard screen select the Add Interface button. See Figure 58 – Add Interface Button

Figure 58 – Add Interface Button

The Add Interface menu will appear. Select “Add VLAN”. See Figure 59 – Add Interface Menu

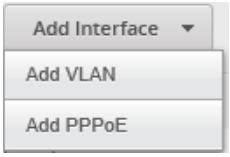


Figure 59 – Add Interface Menu

You will be presented with the “Create New VLAN” dialog. Fill in the information as follows:

VLAN ID:	6
Interface:	switch0
Description:	“Wifi Guest Net”
MTU:	1500
Address:	Manually define IP address
	192.168.6.1/24

The AC-AP-LR access point will eventually be connected to the eth4 interface. The eth3 and eth4 interfaces are internally using the switch0 chip. Therefore, this VLAN needs to be attached to switch0, not to eth3 or to eth4. See Figure 60 – Create New VLAN Example. Press the “Save” button.

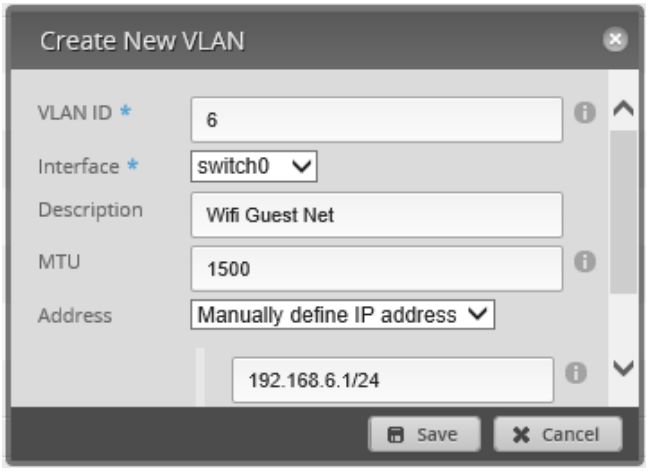


Figure 60 – Create New VLAN Example

Repeat the above steps two more times, for adding two more VLANs. Fill in the information as follows:

VLAN ID:	7
Interface:	switch0
Description:	“Wifi Iot Net”
MTU:	1500
Address:	Manually define IP address 192.168.7.1/24

VLAN ID:	8
Interface:	switch0
Description:	“Wifi Spare Net”
MTU:	1500
Address:	Manually define IP address 192.168.8.1/24

There are the relevant sections from the backup file:

```
vif 6 {
    address 192.168.6.1/24
    description "Wifi Guest Net"
    mtu 1500
}
vif 7 {
    address 192.168.7.1/24
    description "Wifi Iot Net"
    mtu 1500
}
vif 8 {
    address 192.168.8.1/24
    description "Wifi Spare Net"
    mtu 1500
}
```

Here is a link discussing using VLANs and managed switches to reduce the number of network cables in a home: https://community.ubnt.com/t5/EdgeMAX/Need-recommendation-on-tweaking-config-to-support-some-VLAN/td-p/2155404

When originally writing this guide, I was not able to figure out how to combine the Wired IOT Network (as 192.168.4.X) and the Wi-Fi IOT Network (as 192.168.7.X) as a single Network / Subnet. I now enable the internal ER-X switch chip to be VLAN aware, which solves this. Those steps are in section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks. You should just wait to do this until you get to that section, or you might not be able to follow-along in this guide. For me to have instead performed those steps now, now that I know what to do, I would have had to re-write most of this guide and re-take way-too-many screenshots. So that section is still much later in this guide.

VLAN References:

https://help.ubnt.com/hc/en-us/articles/222183968-Intro-to-Networking-Introduction-to-Virtual-LANs-VLANs-and-Tagging

https://community.ubnt.com/t5/EdgeMAX-Stories/Do-people-use-VLANs-for-the-right-things-Pt-1/cns-p/1443246

https://community.ubnt.com/t5/EdgeMAX-Stories/Do-people-use-VLANs-for-the-right-things-Pt-2/cns-p/1443259

https://community.ubnt.com/t5/EdgeMAX/Adding-a-new-subnet-to-an-Edge-Router-X/td-p/2197809

https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch0-with-Inter-VLAN-Firewall-Limiting

https://help.ubnt.com/hc/en-us/articles/205197630-EdgeSwitch-VLANs-and-Tagged-Untagged-Ports

https://help.ubnt.com/hc/en-us/articles/222183968-Intro-to-Networking-Introduction-to-Virtual-LANs-VLANs-and-Tagging

32. Add DHCP Servers to the VLANs

Following the directions that are in the section titled “28 - Configure EdgeRouter’s eth2 DHCP Server”, add DHCP servers for the three VLANs that were just created. Note that I am using Open DNS servers for these networks. If you change them here, you will also need to manually modify some firewall / NAT rules, presented later within this guide.

The information for VLAN 6, is as follows:

DHCP Name:	WifiGuestDHCP
Subnet:	192.168.6.0/24
Range Start:	192.168.6.38
Range Stop:	192.168.6.243
Router:	192.168.6.1
DNS 1:	208.67.222.222
DNS 2:	208.67.220.220
Unifi Controller:	<Leave Blank>
Enable:	CHECKED

The information for VLAN 7, is as follows:

DHCP Name:	IotDHCP
Subnet:	192.168.7.0/24
Range Start:	192.168.7.38
Range Stop:	192.168.7.243
Router:	192.168.7.1
DNS 1:	208.67.222.222
DNS 2:	208.67.220.220
Unifi Controller:	<Leave Blank>
Enable:	CHECKED

The information for VLAN 8, is as follows:

DHCP Name:	WifiSpareDHCP
Subnet:	192.168.8.0/24
Range Start:	192.168.8.38
Range Stop:	192.168.8.243
Router:	192.168.8.1
DNS 1:	208.67.222.222
DNS 2:	208.67.220.220
Unifi Controller:	<Leave Blank>
Enable:	CHECKED

You should now have six DHCP servers.

33. Set Domain Names for Networks

Near the top of the screen select the “Services” button. Reference Figure 52 – Services Button. Ensure that the “DHCP Server” tab is selected. Reference Figure 53 – DHCP Server Screen

Find the LAN1 line, and follow it to the right side, to the line’s “Actions” button. Click the “Actions” button. You will be presented with a list of actions. Choose “View Details”. See Figure 61 – DHCP Actions.

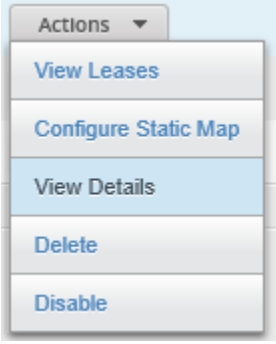


Figure 61 – DHCP Actions

A dialog will open. See Figure 62 – DHCP Server Details Dialog.

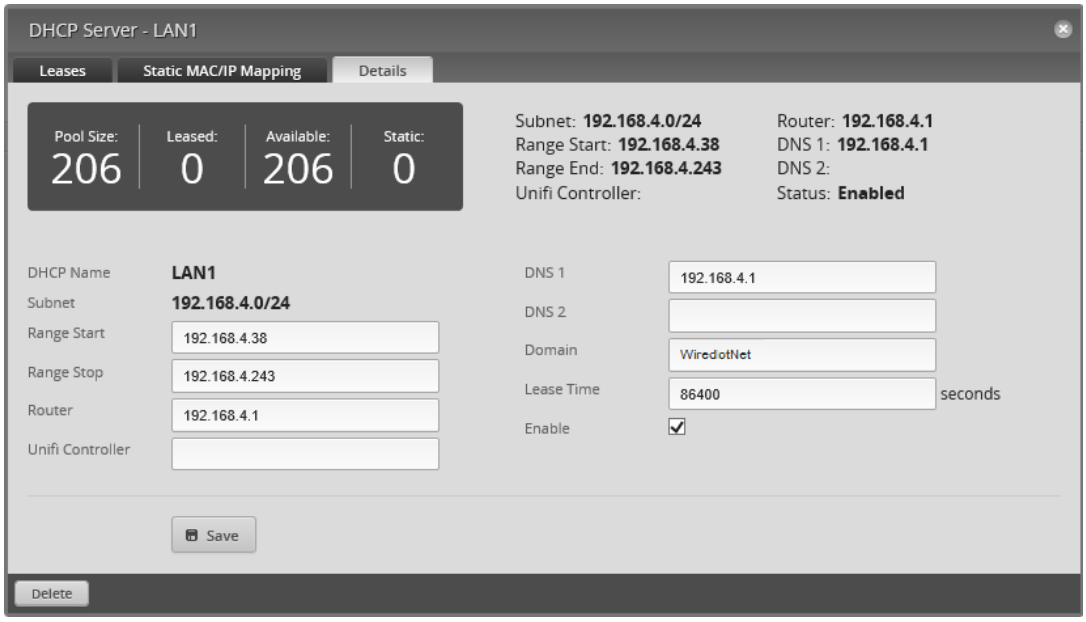


Figure 62 – DHCP Server Details Dialog

Fill-in the “Domain” field with:

WiredIotNet

and then click “Save.” When it is done updating, close the dialog.

Repeat these steps for the following DHCP Servers as show in Table 2 - Table of Domain Names (You have just done the first one of them):

DHCP Servers	Domain
LAN1	WiredIotNet
LAN2	HomeNet
SecureNetDHCP	SeparateNet
WiFiGuestDHCP	WifiGuestNet
IOTDHCP	IotNet
WifiSpareDHCP	WifiSpareNet

Table 2 - Table of Domain Names

34. Modify EdgeRouter's eth1 DHCP Server

Select the "Services" button. Reference Figure 52 – Services Button.

Ensure that the "DHCP Server" tab is selected. Reference Figure 53 – DHCP Server Screen

Select the "Action" button to the right of the "LAN1" line. Reference Figure 61 – DHCP Actions.

Choose "View Details." Reference Figure 62 – DHCP Server Details Dialog.

Modify / enter the following information:

DNS 1: 208.67.222.222
DNS 2: 208.67.220.220

These DNS addresses have the equipment on the Wired Iot Network use Open DNS resolvers. If different resolver addresses are used here, then some firewall rules (and probably group addresses) will also need to be modified. Covered later in this guide.

35. Rename DHCP Servers

When the Wizard setup our EdgeRouter, it named the two original networks as LAN1 and LAN2. To rename them, enter the CLI. Reference section 17 - EdgeRouter Command Line Interface (CLI).Type the following commands into the CLI window:

```
configure
edit service dhcp-server
rename shared-network-name LAN1 to shared-network-name WiredIotDHCP
rename shared-network-name LAN2 to shared-network-name HomeNetDHCP
commit
save
exit
```

Exit the CLI interface.

36. Make DHCP Servers “authoritative”

The EdgeRouter does not default any newly created DHCP servers to “authoritative.” This means that devices on the added Networks can take a long time to acquire an IP address. The Networks that were added by the Wizard (LAN1 and LAN2) are made authoritative by default.

Enter the Config Tree. Reference section “18 - EdgeRouter Config Tree.” Select and open up the following config tree sub-menu items from the configuration screen:

service
dhcp-server
shared-network-name

Click on the DHCP server you want to configure; in this case, it is:

SecureNetDHCP

You should see some DHCP settings, including authoritative. (Note, your screen will still show “disable”). See Figure 63 – Authoritative Example.

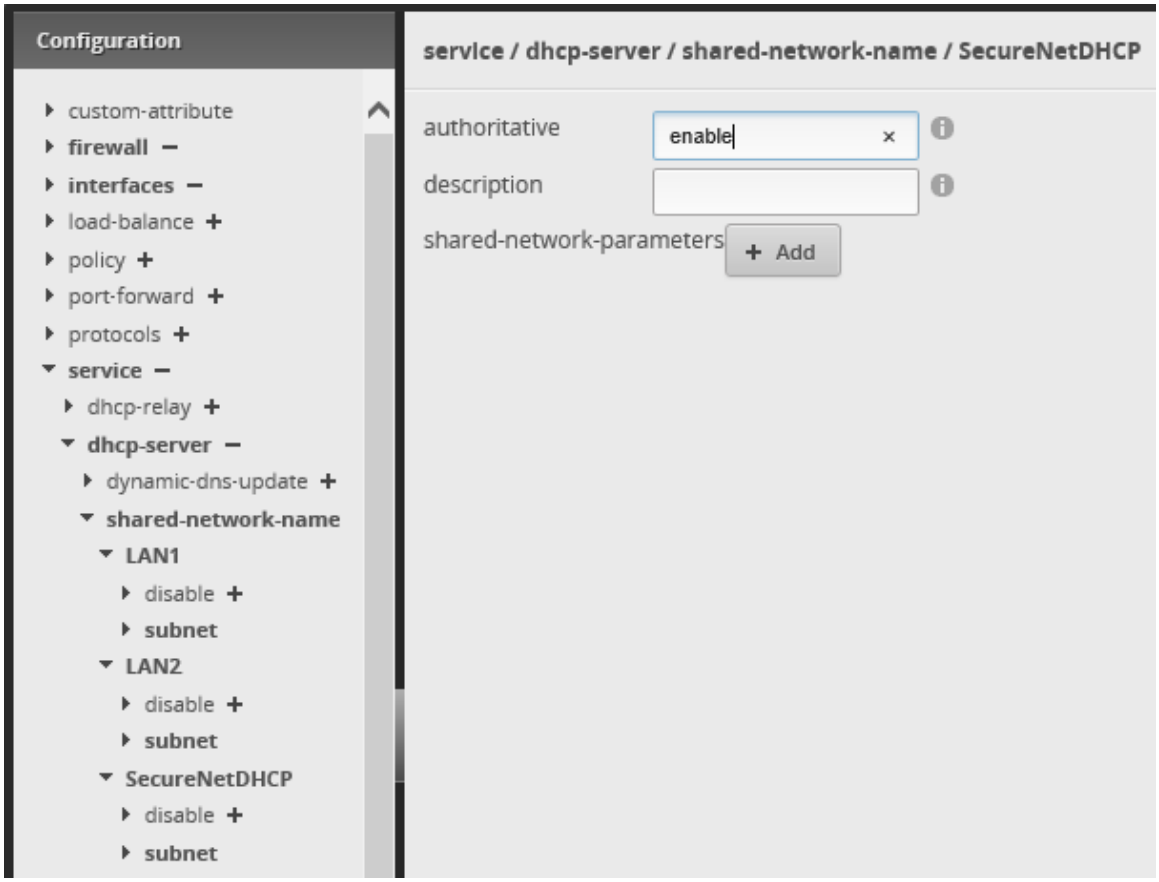


Figure 63 – Authoritative Example

Type “enable” in the authoritative box. Then press the “Preview” button. See Figure 64 – Authoritative Commit.

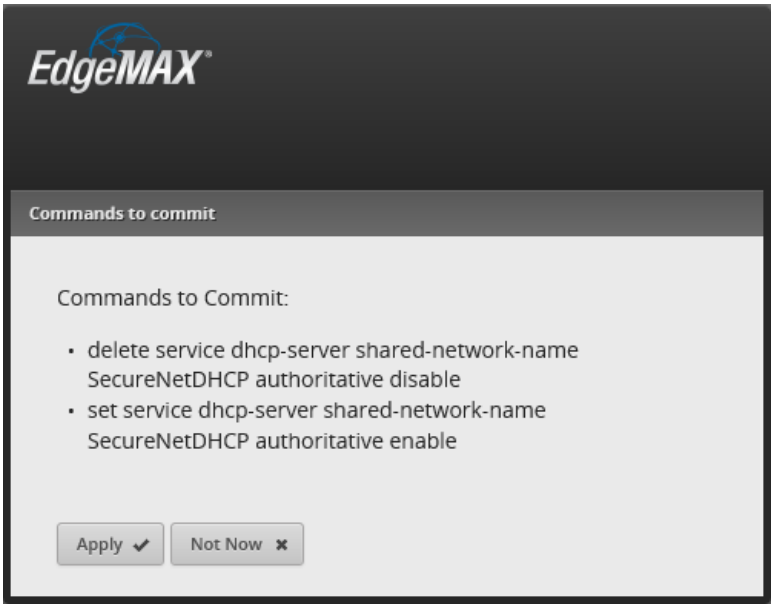


Figure 64 – Authoritative Commit

Press “Apply.” You should see the message “The configuration has been applied successfully”, in green, near the bottom of the screen.

Repeat these steps for the following Authoritative DHCP Servers as shown in Table 3 - Table of Authoritative DHCP Servers. (You have just done the first one of them):

Authoritative DHCP Servers
SecureNetDHCP
WiFiGuestDHCP
IotDHCP
WifiSpareDHCP

Table 3 - Table of Authoritative DHCP Servers

Shown below are excerpts of three of the five DHCP sections from the backup file:

```
dhcp-server {
    disabled false
    hostfile-update disable
    shared-network-name HomeNetDHCP {
        authoritative enable
        subnet 192.168.3.0/24 {
            default-router 192.168.3.1
            dns-server 192.168.3.1
            domain-name HomeNet
            lease 86400
            start 192.168.3.38 {
                stop 192.168.3.243
            }
        }
    }
    shared-network-name SecureNetDHCP {
        authoritative enable
        subnet 192.168.5.0/24 {
            default-router 192.168.5.1
            dns-server 209.244.0.3
            dns-server 209.244.0.4
            domain-name SeparateNet
            lease 86400
            start 192.168.5.38 {
                stop 192.168.5.243
            }
        }
    }
    shared-network-name WifiGuestDHCP {
        authoritative enable
        subnet 192.168.6.0/24 {
            default-router 192.168.6.1
            dns-server 208.67.222.222
            dns-server 208.67.220.220
            domain-name WifiGuestNet
            lease 86400
            start 192.168.6.38 {
                stop 192.168.6.243
            }
        }
    }
    use-dnsmasq enable
}
```

37. EdgeRouter Enable HW NAT Assist

Enabling “hwnat” turns on some features of a hardware switching chip that is within the EdgeRouter. This chip assists the EdgeRouter’s CPU with routing and NAT functionality, speeding up the operation of the EdgeRouter X.

Without this hardware assist, routing of packets is relatively slow. Be warned; if Quality of Service (QoS) functionality is enabled, then this hwnat assist is internally / automatically disabled. You also don’t want to enable bridging, since bridging is implemented via the CPU of the EdgeRouter X and is also relatively slow.

With hwnat enabled, many people report 800 – 900Mbps throughput.

Open up the Configuration Tree. Reference section 18 - EdgeRouter Config Tree.

Select and open up the following config tree sub-menu items from the configuration screen:

system
offload

In the hwnat setting area, type:

enable

then select the “Preview” button at the bottom of the page.

See Figure 65 – System Offload Hwnat Selection (Partial).

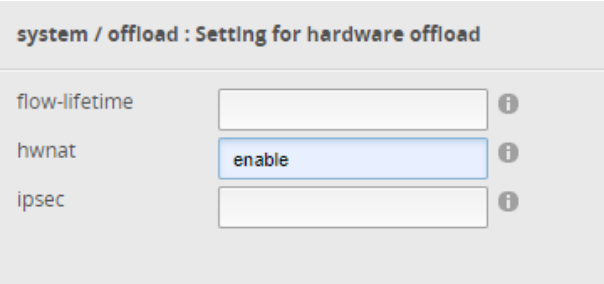


Figure 65 – System Offload Hwnat Selection (Partial)

The Edgerouter will preview what command(s) it will issue. See Figure 66 – Preview hwnat Config.

Figure 66 – Preview hwnat Config

Press “Apply.” The system will inform you that, “The configuration has been applied successfully”. See Figure 67 – hwnat Success

Figure 67 – hwnat Success

The above config-tree hwnat-enable could have been performed with the following CLI commands:

```
configure
set system offload hwnat enable
commit
save
exit
```

Compare the above command(s) with the command that the conifg-tree automatically issued in Figure 66 – Preview hwnat Config.

Remember that different models of EdgeRouters have different abilities / hardware assisting chips within them. Their commands may be different.

Reference: https://help.ubnt.com/hc/en-us/articles/115006567467-EdgeRouter-Hardware-Offloading-Explained

38. EdgeRouter ER-X Speed

The ER-X router seems capable of routing about 1Gbit/second aggregate/total, i.e. the sum of all input/output is 1Gbit/second. Note that most speed tests run separate download and separate upload tests.

The following article is well worth reading about the internals of the ER-X hardware:
http://kazoo.ga/re-visit-the-switch-in-edgerouter-x/

Other performance references:
https://community.ubnt.com/t5/EdgeMAX/Performance-of-EdgerouterX-vs-Edgerouter-Lite/td-p/1230924
https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-low-throughput-slow/td-p/1392229
https://community.ubnt.com/t5/EdgeMAX/ER-X-vs-ER-Lite-Head-to-Head-Speed-Results-on-Google-Fiber/td-p/1839844
https://www.stevejenkins.com/blog/2017/02/edgerouter-x-vs-edgerouter-lite-google-fiber-speed-tests/
https://community.ubnt.com/t5/EdgeMAX/Edgerouter-X-Fios-Gigabit-Won-t-go-over-500-Mbps/td-p/1910761

39. EdgeRouter Enable Traffic Analysis

This step will enable the EdgeRouter to perform Deep Packet Inspection (DPI) / Traffic Analysis. If you have any speed issues with your ER-X, then this may need to stay off.

Press the “Traffic Analysis” button, near the top right of the screen. See Figure 68 – Traffic Analysis Button.

Figure 68 – Traffic Analysis Button

In the upper-right area of the traffic analysis screen, is an “Operational Status” selection. Select “Enabled.” See Figure 69 – Enable Operational Status

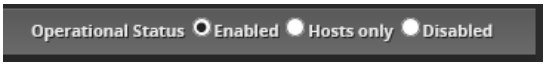


Figure 69 – Enable Operational Status

You will be presented with a confirmation dialog. See Figure 70 – Operational Status Confirmation.

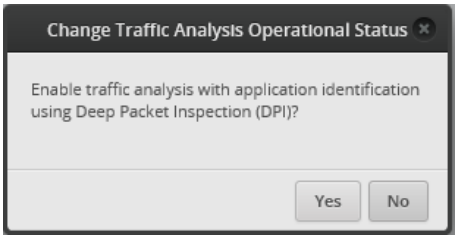


Figure 70 – Operational Status Confirmation

Select “Yes.” The software will (for some reason) present you with an Alert. This is seen in the lower-left of the screen. See Figure 71 – Active Alert.

Figure 71 – Active Alert

Click on the “Alerts” button. You will be presented with the Alert message(s). See Figure 72 – Active Traffic Analysis Message.

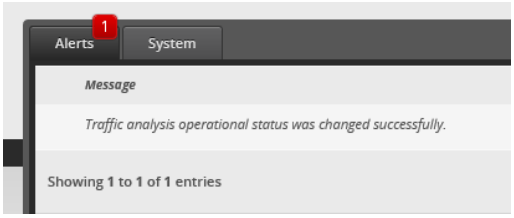


Figure 72 – Active Traffic Analysis Message

To remove this Alert message, press the “Remove” button, located on the right side of the screen. See Figure 73 – Remove Alert Button

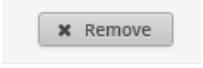


Figure 73 –Remove Alert Button

40. EdgeRouter Traffic Analysis

The Traffic Analysis performed by the EdgeRouter X initially looks pretty neat. The following screen shot was taken when the Edgerouter was at this configuration step in generating this configuration document. The EdgeRouter had been booted for 41 minutes.

The only thing I had done, since I booted the "setup" computer, was to configure the EdgeRouter. I NEVER purposefully go to MSN.com, or to the Financial Times News. I only assume that those web lookups are from Microsoft's Internet Explorer / Microsoft performing their Windows 10 monetization of their users, sometimes referred to as "spying." See Figure 74 –Sample Traffic Analysis

In real use, this feature there seems to puta lot of uncharacterized traffic under "Other."

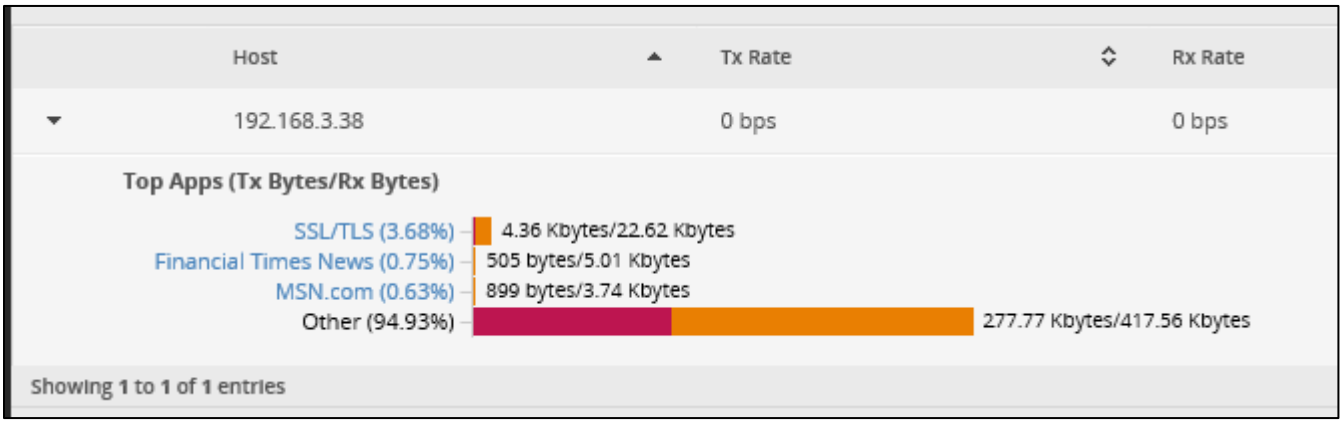


Figure 74 –Sample Traffic Analysis

Note that when HW NAT Assist is enabled, some traffic, which is handled by the internal switch chip, is not shown in traffic analysis. That is because Traffic Analysis is a CPU function, and the traffic that is being handled internally by the switch chip is not visible to the CPU. Note that traffic which is between two devices on the same Network does not even transit to the EdgeRouter, so this traffic will never be shown. The configuration used in this guide has setup the switch0 chip to only move traffic between eth3 and eth4, which is the Home Net (Network).

Trafffic Analysis data cannot be exported out of the EdgeRouter.

Turns out that some of this Traffic Analysis data can trigger firewall rules:
https://www.youtube.com/watch?v=tNG_Fq5Sjcg
https://www.youtube.com/watch?v=d2Mz7Nin4vQ

41. EdgeMAX EdgeRouter X/X-SFP bootloader update

ER-X's, which have firmware versions of 1.10.7 or above, have a newer bootloader available and/or newer method of bootloader update. You will want to update your bootloader. Reference:

https://help.ubnt.com/hc/en-us/articles/360009932554-EdgeRouter-How-to-Update-Bootloader

Per the above link, I ran the following CLI / SSH / PuTTY command:

```
show system boot-image
```

and got the following text:

```
The system currently has the following boot image installed:
Current boot version: UNKNOWN
Current boot md5sum : 7580ebd7ce9303243292f586ab7c6daf
New uboot version is available: boot_e50_001_1e49c.tar.gz
New boot md5sum : 2146fb2e3b2cd543efaa0a687e2ad0ce
Run "add system boot-image" to upgrade boot image.
```

I updated my bootloader with `add system boot-image` (and `yes`) and then got the following text:

```
Uboot version [UNKNOWN] is about to be replaced
Warning: Don't turn off the power or reboot during the upgrade!
Are you sure you want to replace old version? (Yes/No) [Yes]: yes
Preparing to upgrade...Done
Copying upgrade boot image...Done
Checking boot version: Current is UNKNOWN; new is e50_001_1e49c ...Done
Checking upgrade image...Done
Writing image...Done
Upgrade boot completed
```

I then re-ran the following command: `show system boot-image` and got the following text:

```
The system currently has the following boot image installed:
Current boot version: e50_001_1e49c
Current boot md5sum : 2146fb2e3b2cd543efaa0a687e2ad0ce
```

Next, issue the `reboot` command and when prompted with the prompt:

```
Proceed with reboot? [confirm]
```

Type a single `y` character to confirm the reboot.

You will need to wait about 3 to 5 minutes.

After the re-boot, I re-ran the following command: `show system boot-image` and got the following text:

```
The system currently has the following boot image installed:
Current boot version: e50_001_1e49c
Current boot md5sum : 2146fb2e3b2cd543efaa0a687e2ad0ce
```

42. EdgeRouter X/X-SFP Legacy Bootloader Information

Part 1

Older bootloaders have an initialization issue in the bootloader for the ER-X and ER-X-SFP models that causes all ports to act as a "switch" during a brief period of time when the router is booting up.

When this guide was written, Ubiquiti had still not updated their production line to incorporate the patched bootloader.

Reference https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-acts-as-switch-during-boot/td-p/1393679

Part 2

For pre 1.10.6 firmware, check the version of your bootloader per:

https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-X-SFP-check-bootloader-version/td-p/1617287

Some postings may be missing the “s” in “firmwares”.

Part 3

Older bootloader (pre 1.10.6) updating is follows:

If your bootloader is not the newest, update your bootloader per:

http://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-X-X-SFP-bootloader-update/ba-p/1472216

https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/DEPRECATED-EdgeMAX-EdgeRouter-X-X-SFP-bootloader-update/ba-p/1472216

It is much easier to update the EdgeRouter’s bootloader when the EdgeRouter is connected to the internet.

You may need to prepend “sudo” to one for more of the following commands, to get this to work:

https://community.ubnt.com/t5/EdgeMAX/ERX-bootloader-update/td-p/1892923

https://community.ubnt.com/t5/EdgeRouter/ER-X-bootloader-update-versions/td-p/2134544

43. EdgeOS file system layout and firmware images

@BranoB made the following interesting posting:

https://community.ubnt.com/t5/EdgeRouter/EdgeOS-file-system-layout-and-firmware-images/m-p/2377075

44. EdgeRouter Power Cycle Warning

Generally, you should use the reboot button that is located on the system screen to restart the EdgeRouter; don't simply remove power to the EdgeRouter, if you can help it.

Reference TBD

45. EdgeRouter UPnP

Don't enable UPnP. UPnP allows anything on your network (PCs / PCs with malware / Chinese IOT devices) to silently open ports in your firewall and let their friends and servers back in to feast on your private data.

If you need to connect devices like an Xbox behind your EdgeRouter, then manually open / forward the firewall ports by hand. If you really want UPnP, I've got a slightly used D-Link router for sale, which probably has lots of holes already in its firewall. Just ask the Federal Trade Commission who is suing D-Link.

References (I have not tried any of these and I don't have an Xbox):

https://help.ui.com/hc/en-us/articles/217367937-EdgeRouter-Port-Forwarding

https://www.reddit.com/r/HomeNetworking/comments/8a8ljb/another_xbox_one_nat_edgerouterx_help_post/

https://support.microsoft.com/en-us/help/4026770/xbox-open-these-network-ports-for-xbox-one

46. Extended GUI Access / Use May Crash the EdgeRouter

Leaving the EdgeRouter's GUI interface up for extended periods of time (maybe like a day or so) may crash the Edgerouter.

I can't find my original reference, so here is a related one:

> One specific example is leaving the GUI open which can cause an unexpected reboot.
> We are currently working on a fix for this. It's not convenient,
> but saying out of the GUI may prevent these reboots assuming it is the same cause.

https://community.ubnt.com/t5/EdgeMAX/ER-PRO-8-random-reboots-1-9-7-hotfix-1/td-p/2033684

47. EdgeRouter Toolbox

In the upper right side of the main page, is a Toolbox button. When you click on it, you will see some nice utilities. See Figure 75 –Toolbox Items.

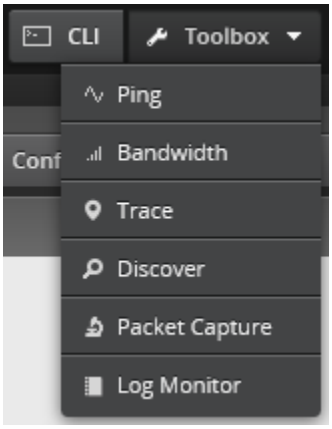


Figure 75 –Toolbox Items

There is a handy log monitor here:
https://community.ubnt.com/t5/EdgeRouter/Viewing-Firewall-Logs-in-GUI/m-p/2686126/highlight/true#M241809

48. Address Groups

The software in the EdgeRouter allows the user to define Address Groups. These groups are used for convenience. We will define a couple of address groups. This guide previously used multiple address groups, one for each Network. Those address groups have recently been converted into simpler “Interface Networks”. This change will be explained later.

Select the “Firewall/NAT” Button from the top of the screen. See Figure 76 – Firewall/NAT Button.

Figure 76 – Firewall/NAT Button

From the tabs that are shown, select “Firewall/NAT Groups”. See Figure 77 – Firewall/NAT Groups Tab.

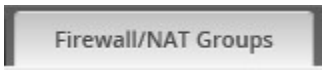


Figure 77 – Firewall/NAT Groups Tab

Find the “+ Add Group” button and click it. See Figure 78 – Add Group Button.

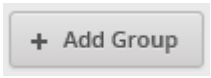


Figure 78 – Add Group Button

You will see the “Create New Firewall/NAT Group” dialog. Fill in this form as follows:

Name:	OPENDNS_SERVERS_GROUP
Description:	OpenDNS Servers
Group Type:	Address Group.

See Figure 79 – Example New Address Group Dialog. Press “Save.”

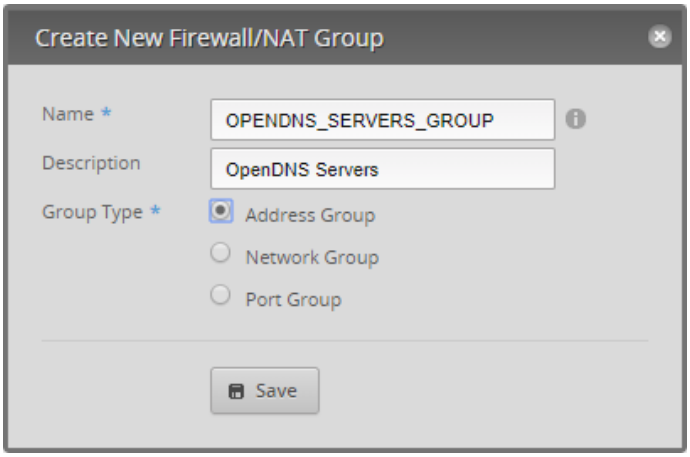


Figure 79 – Example New Address Group Dialog

An empty Address group will have been added. Note that the “Number of group members” is 0. See Figure 80 – Added Address Group.

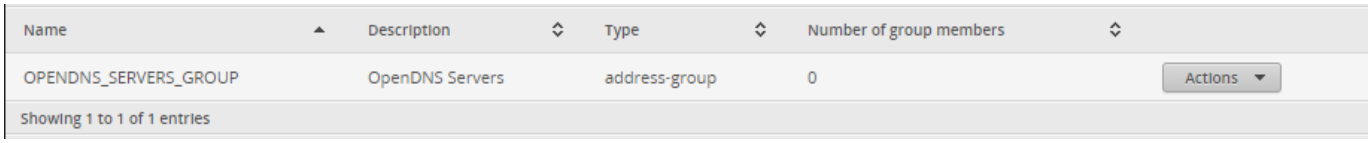


Figure 80 – Added Address Group

Press the OPENDNS_SERVERS_GROUP ‘s Action button and select Config. See Figure 81 – Address Group Actions

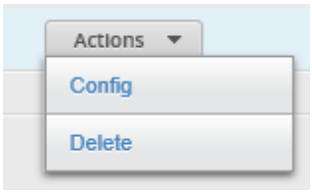


Figure 81 – Address Group Actions

Enter the address specifier of:

```
208.67.222.222
```

Press the “+ Add New” button and then add

```
208.67.220.220
```

See Figure 82 – Example Edit Address Group. Press “Save.” When it is finished updating, close the dialog.

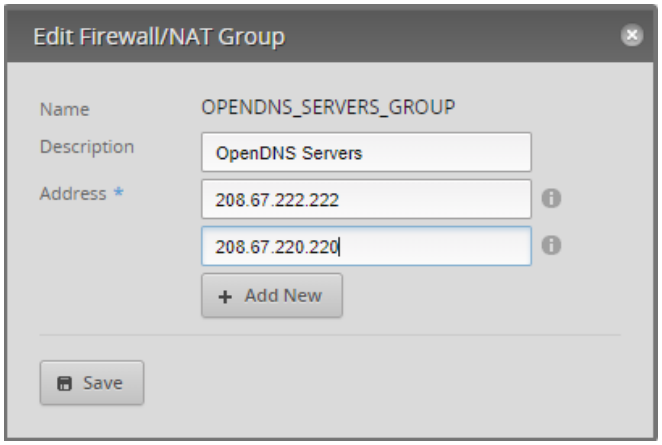


Figure 82 – Example Edit Address Group

Repeat the above steps for the following address groups. If there is more than one address listed in a group, then you will need to use the "+ Add New" button to add additional address(es) to the group. You have just done the OPENDNS_SERVERS_GROUP.

```
group {
    address-group OPENDNS_SERVERS_GROUP {
        address 208.67.222.222
        address 208.67.220.220
        description "OpenDNS Servers"
    }
    address-group RFC-1918_GROUP {
        address 192.168.0.0/16
        address 172.16.0.0/12
        address 10.0.0.0/8
        description "RFC-1918 Group"
    }
}
```

The above text section is from the backup file.

49. EdgeRouter Layman's Firewall Explanation

I initially had trouble understanding the EdgeRouter's firewall rules. The firewall rules that I saw on the internet appeared backwards (in direction) to me. I also didn't understand what "local" rules meant or applied to. Then I found the article "Layman's firewall explanation".

Reference: https://community.ubnt.com/t5/EdgeMAX/Layman-s-firewall-explanation/td-p/1436103

I highly recommend that you stop and read that entire posting now.

I have re-produced the main diagram, from that article, as Figure 83 – Layman's Firewall Explanation Diagram. Note that this diagram is for an EdgeRouter Lite, which has its WAN port on eth1. The WAN interface is therefore shown in the middle of this diagram.

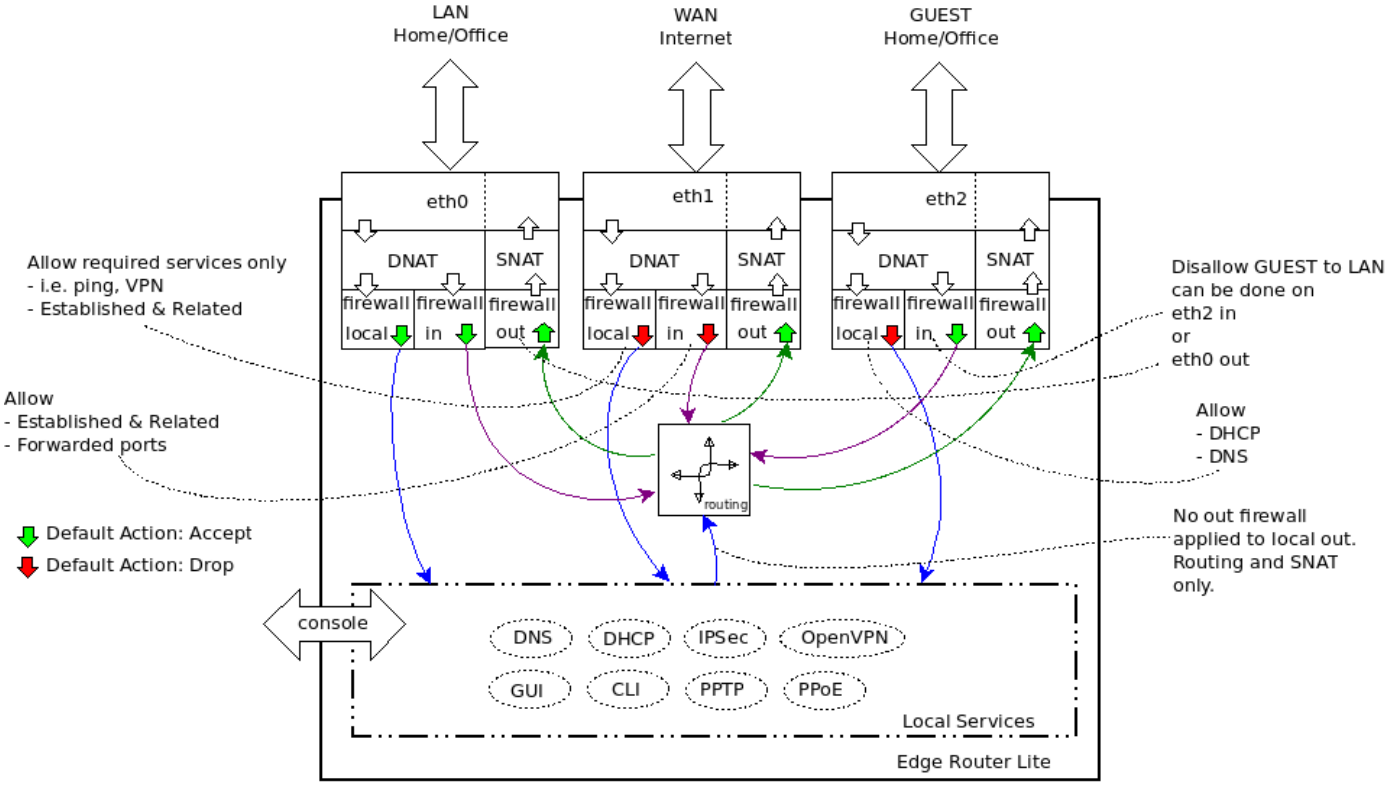


Figure 83 – Layman's Firewall Explanation Diagram

A firewall policy (ruleset) is a set of firewall rules along with a default action. The default action can be "accept," "reject," or "drop." A firewall ruleset is applied to a specific interface as well as applied to a specific "direction." For an EdgeRouter, the directions are "In," "Out," and "Local." The **"In" direction is** input IP packets from the internet, as well as **input into the EdgeRouter** from devices on a Network (LAN). The **"Out" direction** consists of IP packets **output from the EdgeRouter** destined for the internet, as well as output to your Network devices from the EdgeRouter. "Local" refers to IP data coming into the EdgeRouter destined for (services on the) EdgeRouter itself. Reference Figure 83 – Layman's Firewall Explanation Diagram. **The In and Out directions are referenced as viewed from the EdgeRouter.**

Each firewall rule, within a ruleset, also has an action of "accept," "reject," or "drop." Each IP packet attempting to traverse an interface that has firewall rules will be tested by the individual firewall rules, in the ruleset order, until a firewall rules matches the rule's condition criteria. The individual firewall rules contain conditions that need to all be matched for that firewall rule to perform its action. If no firewall rules match an IP packet, then the ruleset's default action is taken for that packet. Once an IP packet matches an individual firewall rule, no other firewall processing is needed for that IP packet.

Firewall rules within the ruleset are applied (tested) in the specific order that they were arranged. Therefore, it is important to order the firewall rules so that the most frequently used rules are arranged at or near the top of the set of rules, allowing for efficiency within the EdgeRouter.

Sometimes the firewall rule numbers seem to increment by one and sometimes they increment by ten. I think that different versions of EdgeRouter firmware have implemented numbering differently, so don't worry if your firewall rule's absolute numbers don't match this guide, only the rules ordering matters. Firewall processing is ordered by lowest number to highest number.

Firewall policies are applied before SNAT (Source Network Address Translation) and after DNAT (Destination Network Address Translation).

The descriptions above are by no means exact regarding what is happening internally. These descriptions are just meant to convey enough information to help understand these firewall rules, their design, and their operation.

Additional References:
https://help.ubnt.com/hc/en-us/articles/204976664-EdgeMAX-How-are-packets-processed-by-EdgeRouter

You can issue a CLI command to view the firewall's connection table with:

```
sudo conntrack -L
```

50. Firewall State

There are many conditions available that can constitute a firewall rule. One of the most important conditions is "State." States are maintained internally by the underlying firewall code that is within the EdgeRouter, and are:

New – a packet starting a new connection
Invalid – packets that have invalid data in them
Established – packets associated with an existing connection (conversation)
Related – packets related to an existing connection (conversation)

51. WAN Firewall Rules

The most important firewall rules in an EdgeRouter, from a security standpoint, are the default WAN_IN and WAN_LOCAL rulesets. These rulesets were generated by the WLAN+2LAN2 Wizard. The firewall rules with these rulesets provide the "firewall" protection associated with (consumer) Network Address Translation (NAT) routers. The WAN_IN and WAN_LOCAL rulesets are identical, except for naming, and for the interface that they are applied to. This is the WAN_IN ruleset, from the backup file:

```
name WAN_IN {
    default-action drop
    description "WAN to internal"
    rule 10 {
        action accept
        description "Allow established/related"
        state {
            established enable
            related enable
        }
    }
    rule 20 {
        action drop
        description "Drop invalid state"
        state {
            invalid enable
        }
    }
}
```

The name of this ruleset is WAN_IN. The rules in this ruleset are applied (not shown here) to the input side of the eth0 interface, i.e., to IP packets that are entering the EdgeRouter from the internet.

This ruleset has a default action of drop. If a packet destined for this interface doesn't match any firewall rule, then the packet will be dropped.

The first rule (rule 10) in the ruleset has an action of "accept," and will allow packets that are "established" and "related" (i.e. associated) to an existing IP conversation to enter eth0. The only way to have an existing connection on eth0 is for the connection to have been started from within the EdgeRouter's system, i.e., from the EdgeRouter itself, or from a device on one of the EdgeRouter Networks. Note that there are no other / additional qualifiers on this rule(s), so it is applied to every IP packet entering from the internet.

The second rule (rule 20) has an action of "drop." Any packet matching this rule: "invalid state" will be dropped.

52. EdgeRouter Detailed Firewall Setup

I have adapted Figure 83 – Layman's Firewall Explanation Diagram to my own diagram. See Figure 84 – Detailed Firewall Setup Diagram.

The FireWall Rules (FWR) that are described in this guide are numbered (as FWR*) in Figure 84 – Detailed Firewall Setup Diagram. Each is associated with a named firewall ruleset that will be described in the following sections. FWRs that are colored red means a ruleset terminates with a default of drop, while FWRs colored green mean a default of accept. The firewall rule sets are:

FWR1 = WAN_LOCAL.
FWR2 = WAN_IN.
FWR3 = WIRED_IOT_LOCAL.
FWR4 = WIRED_SEPARATE_LOCAL.
FWR5 = WIRED_SEPARATE_IN.
FWR6 = WIRED_SEPARATE_OUT.
FWR7 = HOME_OUT (same single set of rules, but shown in two places).
FWR8 = WIFI_GUEST_LOCAL.
FWR9 = WIFI_IOT_LOCAL.
FWR10 = WIFI_SPARE_LOCAL (identical to FWR8, but not shown).

The descriptions below are by no means exact regarding what is happening internally. These descriptions are just meant to convey enough information to help understand these firewall rules, their design and their operation.

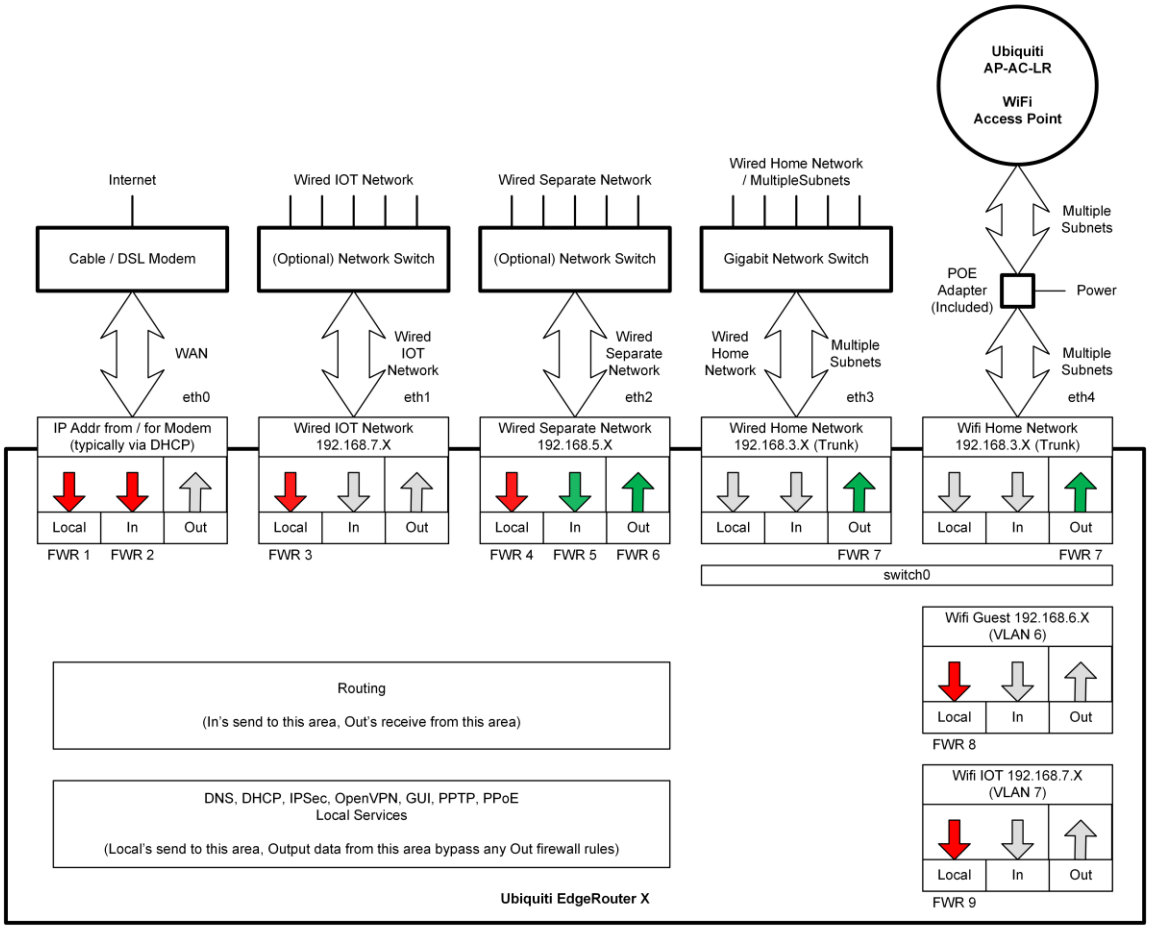


Figure 84 – Detailed Firewall Setup Diagram

53. WAN_LOCAL Firewall Rules

The basic operation of these firewall rules is described above, in the section titled “51 - WAN Firewall Rules”. These rules are FRW1 as shown in Figure 84 – Detailed Firewall Setup Diagram.

54. WAN_IN Firewall Rules

The basic operation of these firewall rules is described above, in the section titled “51 - WAN Firewall Rules”. These rules are FRW2 as shown in Figure 84 – Detailed Firewall Setup Diagram.

Add port forwarding, etc…

Debugging port forwarding:
https://community.ui.com/questions/SOLVED-Port-forwarding-to-IP-camera/f3384ddf-c2f5-4619-ae4c-0042f7349928#answer/4b4fad3e-4e88-4f0a-b142-4cf5929f34f9

55. HOME_OUT Firewall Rules

There are five firewall rules in this ruleset. These firewall rules inspect IP packets that are exiting the EdgeRouter towards devices on the Home Network. Reference “FWR7,” shown as two instances, in the upper-right of Figure 84 – Detailed Firewall Setup Diagram.

These five rules are maintained as four accept rules (one rule per interface), followed by one general-purpose drop rule. Each interface is a separate Network. Except for naming and the Network that they are applied to, the accept rules are identical. The four Networks, which these are applied-to, are: Wired Iot Network, Wifi Iot Network, Wifi Guest Network, and Wifi Spare Network.

The following section of backup file will be referenced later, so it was given a reference tag of Equation 1 – A Portion of the HOME_OUT Firewall Ruleset.

Note that when Ubiquiti uses the term “`address-group`” in a backup file, it can instead/also mean “Interface Network”.

This is a portion from the backup file:

```
name HOME_OUT {
    default-action accept
    description "Home Out"
    rule 10 {
        action accept
        description "Allow Wired Iot Established Replies"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_eth1
            }
        }
        state {
            established enable
            invalid disable
            new disable
            related enable
        }
    }
    ...
    rule 50 {
        action drop
        description "Drop RFC-1918 Traffic"
        log disable
        protocol all
        source {
            group {
                address-group RFC-1918_GROUP
            }
        }
    }
}
```

Equation 1 – A Portion of the HOME_OUT Firewall Ruleset

The name of this ruleset is HOME_OUT. The rules in this ruleset are applied (not shown here) to the output side of both of the eth3 and eth4 interfaces, i.e., switch0. These interfaces are also known as the Home Network. IP packets that are exiting the EdgeRouter (on eth3/eth4) towards equipment on the Home Network are inspected and potentially dropped by these firewall rules. Remember that eth3 and eth4 are still bound together by the switch hardware within the EdgeRouter. In Figure 84 – Detailed Firewall Setup Diagram, this information is shown as duplicated in two blocks (in the upper-right portion of the diagram), each labeled with FWR7.

This ruleset has a default action of “accept.” If a packet destined for this interface doesn’t match any individual firewall rule, then the packet will be accepted, i.e., passed along to devices attached to the Home Network.

The first rule (rule 10) in this ruleset has an action of “accept,” and will allow IP packets that are “established” and “related” (i.e. associated) to an existing IP conversation, to exit the EdgeRouter to devices that are on the Home Network. Note that this rule has an additional qualifier that the source must be from eth1, i.e., this rule only applies to traffic that originates from the Wired IOT Network. The only way to have an existing connection between Wired IOT Network and the Home Network is for the conversation to have been started from devices within the Home Network. The name associated with this rule is "Allow Wired Iot Established Replies."

Rules 20, 30, and 40 are also “accept”, “established / related”, operate identical to Rule 10, but are applied to different Networks.

Rule 50 in this ruleset has an action of “drop,” and will drop all other IP packets that originate from any RFC-1918 address. This address set include all of the Networks used in this project. This is a change from earlier versions of this guide, as there was separate “drop” rule for each Network. Reference section 97 - Simple Service Discovery Protocol (SSDP) / igmp-proxy for what I found that slipped around the previous rules.

The two rules, number 10 and number 50, treated as a set, describe the IP connections (conversations) that can occur between equipment on the Wired IOT Network and the Home Network.

If the conversation was started by devices in the Home Network and directed to devices residing on the Wired IOT Network, then replies to those conversations will be allowed back into the Home Network by firewall rule number 10. Internally, the firewall code keeps track of IP connections, which are entering the EdgeRouter (the “In” side) and then allows traffic that is related to that data to exit the EdgeRouter towards the Home Network devices.

If a conversation was instead started by devices within the Wired IOT Network and directed towards the Home Network, firewall rule 10 will have no prior knowledge about this conversation (because it is not “established”/”related”). Therefore, firewall rule number 10 will not match, and firewall rule processing will then proceed to rule number 20. Rules number 20, 30, and 40 do not apply to traffic from the Wired IOT Network, so those rules do not apply, and no action is taken for them. When this traffic is inspected by rule number 50, this rules condition will match, and the “drop” action will be taken. This data will be discarded by the EdgeRouter, and will therefore NOT reach any device on the Home Network.

Remember that the default action for this ruleset is “accept.” You want the Home Network to be able to operate on its own, i.e. over the Internet, when it is not conversing with just these internal Networks.

Note that every IP packet attempting to exit the EdgeRouter towards devices on the Home Network will need to be inspected by these six firewall rules. Most of the traffic destined for the Home Network will not be from one of the IOT or Guest Networks.

Alternate firewall description:
https://community.ui.com/questions/Sanity-check-for-WAN-Firewall-rules/e82408d3-e8c9-470c-a284-e28528678fde#answer/71475b15-8623-41f1-ab93-5e723018c1aa

56. Firewall Conditions

The following figures are from the “Add New Rule” firewall dialog. We will explain how to get to these in the next section. There are several Tabs in this dialog for entering firewall conditions. You might want to study the following figures, and familiarize yourself with what firewall conditions are available. See the following figures:

Figure 85 – Firewall Conditions, Basic Tab.
Figure 86 – Firewall Conditions, Advanced Tab.
Figure 87 – Firewall Conditions, Source Tab.
Figure 88 – Firewall Conditions, Destination Tab.
Figure 89 – Firewall Conditions, Time Tab.

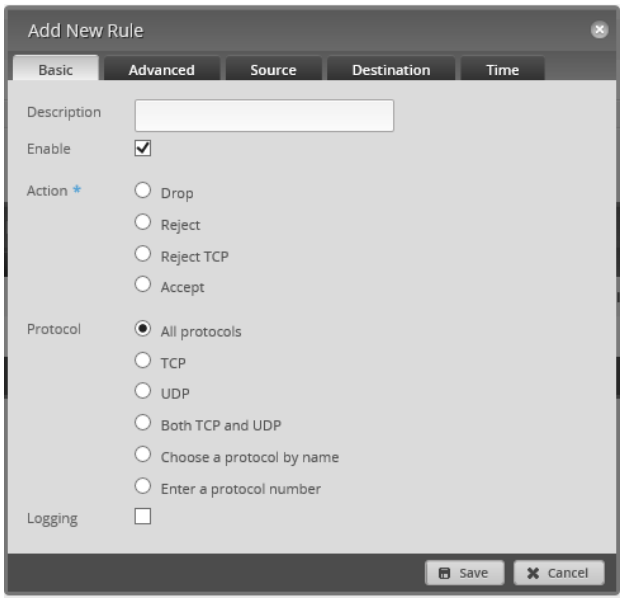


Figure 85 – Firewall Conditions, Basic Tab

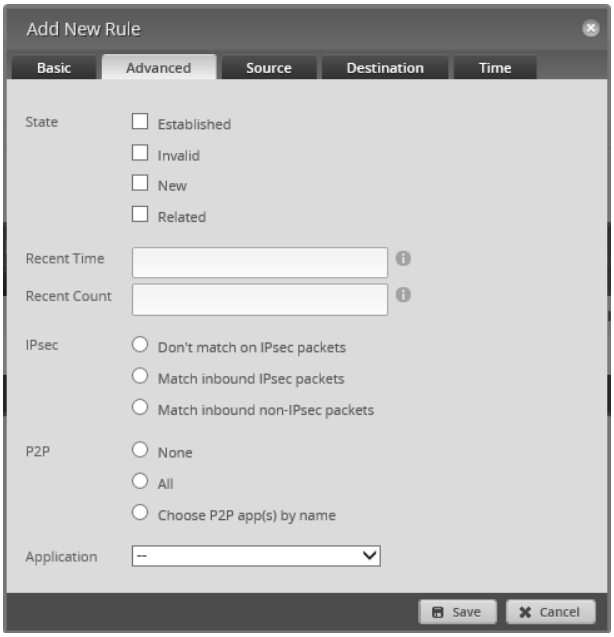


Figure 86 – Firewall Conditions, Advanced Tab

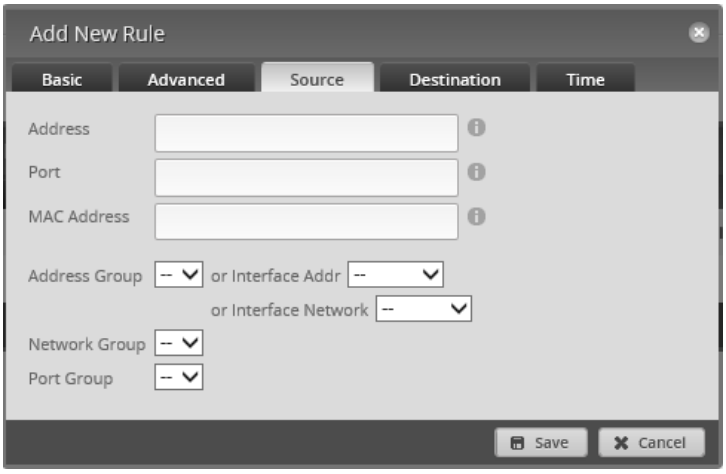


Figure 87 – Firewall Conditions, Source Tab

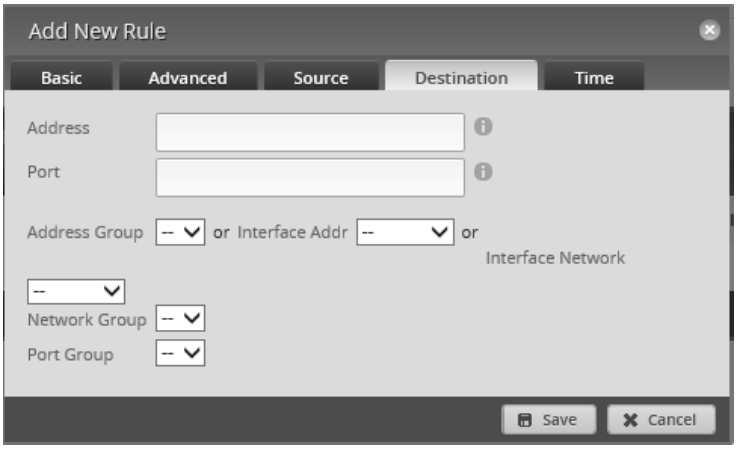


Figure 88 – Firewall Conditions, Destination Tab

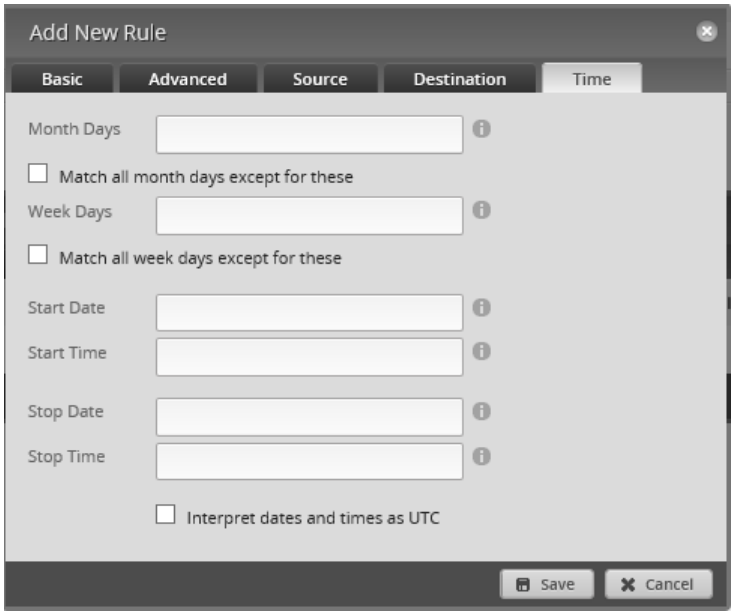


Figure 89 – Firewall Conditions, Time Tab

57. Adding Firewall Rules

Hopefully, you now understand the design of the HOME_OUT firewall rules. Now it is time to actually add these rules. This section will use a portion of HOME_OUT rules as an example of how to add firewall rules using the GUI interface.

While you are using the GUI to add these rules, please frequently reference the backup file segment labeled "Equation 1 – A Portion of the HOME_OUT Firewall Rules", which is in section "55 - HOME_OUT Firewall Rules." This should help you better relate between the two forms - that of the backup text description versus that of GUI entry.

Select the "Firewall/NAT" button from the top of the screen. Reference Figure 76 – Firewall/NAT Button.

Ensure that the "Firewall Policies" tab is selected. See Figure 90 – Firewall Policies Tab.

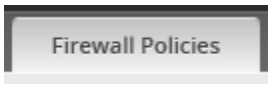


Figure 90 – Firewall Policies Tab

The two WAN rulesets, which were added by the Wizard, should be shown. Press the "+ Add Ruleset" button. See Figure 91 – Add Ruleset.

Figure 91 – Add Ruleset

You will be presented with a "Create New firewall Ruleset." See Figure 92 – Blank Create New Firewall Ruleset.

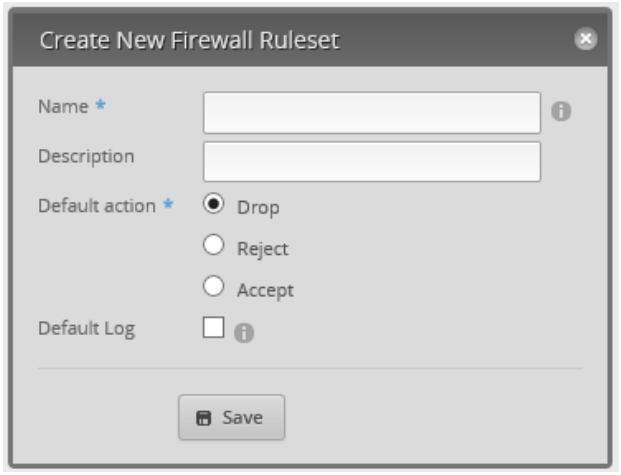


Figure 92 – Blank Create New Firewall Ruleset

Enter the following into the Create New Firewall Ruleset dialog:

Name	HOME_OUT
Description	Home Out
Default action	Accept

See Figure 93 – HOME_OUT Example New Ruleset.

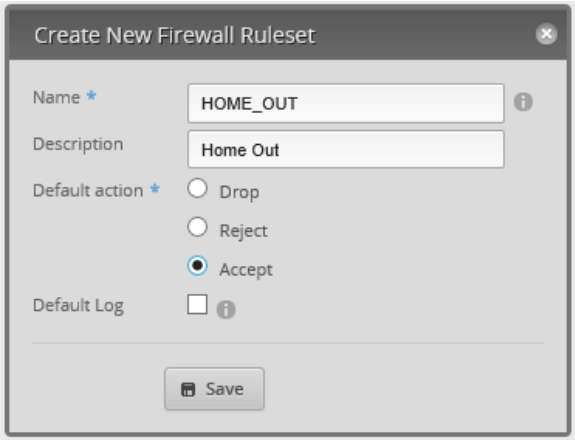


Figure 93 – HOME_OUT Example New Ruleset

Press "Save." A HOME_OUT ruleset will be created. Note that no interfaces have been selected, and the number of rules is 0. See Figure 94 – Empty HOME_OUT Ruleset.

Name	Interfaces	Number of Rules	Default Action
HOME_OUT		0	accept
WAN_IN	eth0/in	2	drop
WAN_LOCAL	eth0/local	2	drop

Showing 1 to 3 of 3 entries

Figure 94 – Empty HOME_OUT Ruleset.

Find the "Actions" button at the right end of the HOME_OUT line (not shown) and press it. You will be presented with a "Firewall Actions Menu." See Figure 95 – Firewall Actions Menu.

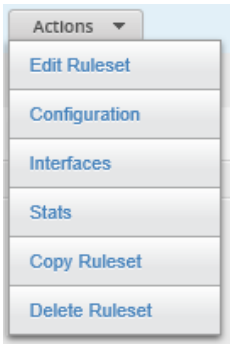


Figure 95 – Firewall Actions Menu

Choose “Edit Ruleset.” A dialog for editing firewall rules appears. The “Rules” Tab should already be selected. See Figure 96 – Edit Ruleset Dialog.

Note that this dialog also contains Tabs of “Configuration,” “Interfaces,” and “Stats.” These match the handy shortcuts that are also in the previously shown Actions menu, reference Figure 95 – Firewall Actions Menu.

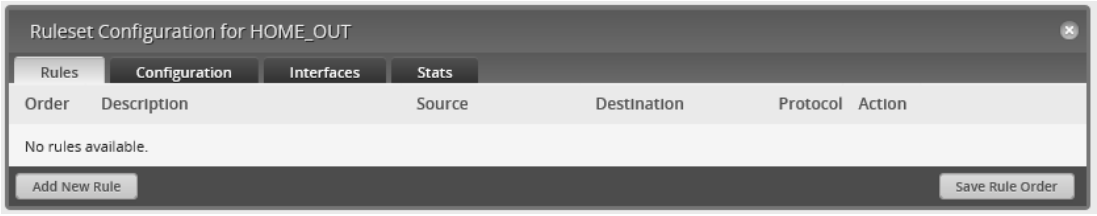


Figure 96 – Edit Ruleset Dialog

Choose the “Configuration” Tab. You should see the information that was entered earlier. See Figure 97 – Firewall Rule Configuration Tab.

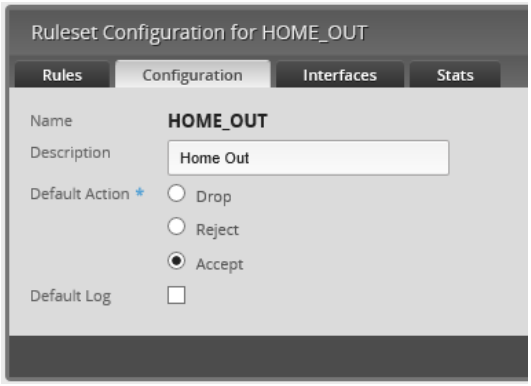


Figure 97 – Firewall Rule Configuration Tab

Choose the “Interfaces” Tab. Select the following information in the dialog:

Interface	switch0
Direction	out

Then press the “Save Ruleset” button.

A lot of problems occur because a ruleset is created and the interface / direction is never set and/or saved.

Since the Home Network is governed by switch0 (i.e. switch0 contains interfaces of eth3 and eth4), we need to choose “switch0” for the Interface, not the individual eth3 or eth4. If an interface is not part of switch0 (eth0, eth1, or eth2) then we would just select that individual interface. See Figure 98 – Firewall Rule Interface Tab.

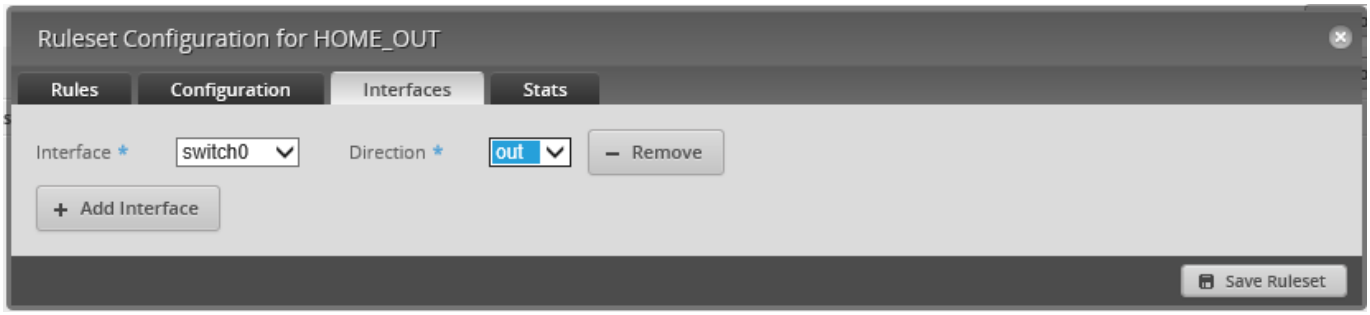


Figure 98 – Firewall Rule Interface Tab

Re-select the “Rules” Tab, and press the “Add New Rule” Button, that is shown in Figure 96 – Edit Ruleset Dialog. An “Add New Rule” dialog will be shown. See Figure 99 – HOME_OUT Firewall, Rule1, Basic. Enter the following into the Basic Tab:

Description	Allow Wired Iot Replies
Enable	CHECKED
Action	Accept
Protocol	All protocols

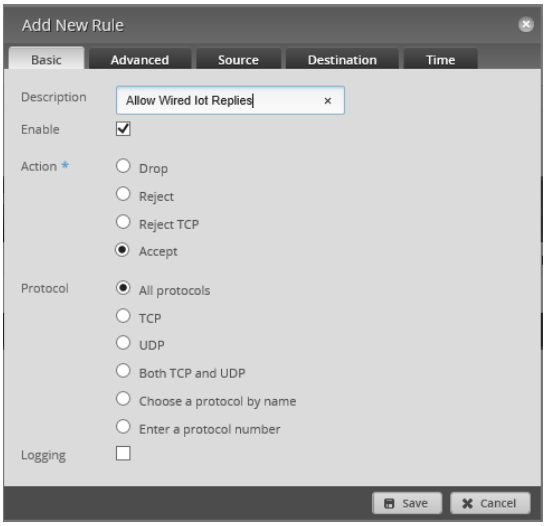


Figure 99 – HOME_OUT Firewall, Rule1, Basic

Click on the Advanced Tab. See Figure 100 – HOME_OUT Firewall, Rule1, Advanced. Enter the following information into the Advanced Tab:

State, Established	CHECKED
State, Invalid	Un-checked
State, New	Un-checked
State, Related	CHECKED

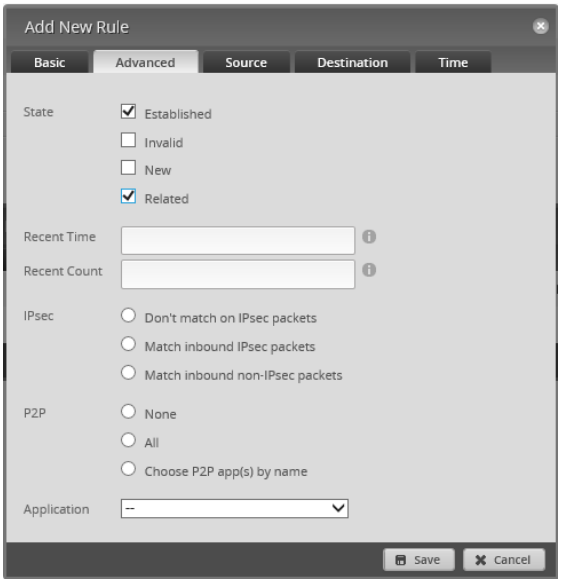


Figure 100 – HOME_OUT Firewall, Rule1, Advanced

Click on the Source Tab. See Figure 101 – HOME_OUT Firewall, Rule 1, Source. Select the following information for the Source Tab:

Interface Network eth1

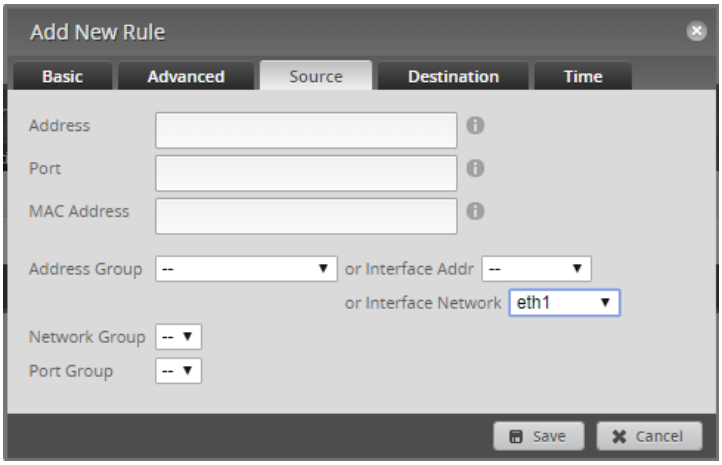


Figure 101 – HOME_OUT Firewall, Rule 1, Source

Press the "Save" button.

Earlier versions of this guide used an "Address Group" instead of "Interface Network". These two methods are equivalent, but there was more setup involved in using an "Address Group". Reference https://community.ubnt.com/t5/EdgeRouter/Firewall-Interface-Addr-vs-Interface-Network/td-p/2238960

You now have a new rule in the HOME_OUT ruleset. See Figure 102 – HOME_OUT Firewall, Rule 1. Note that you used an "Interface Network", but "address-group" is instead / still shown.

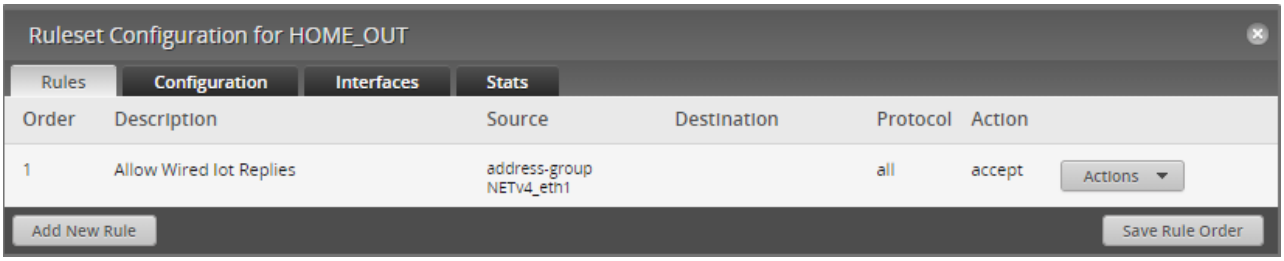


Figure 102 – HOME_OUT Firewall, Rule 1

58. Adding More HOME_OUT Firewall Rules

We now need to add three more rules to the HOME_OUT Ruleset. These rules have identical composition to the rule that was already added, only the names and sources are different. Using the steps that are shown in the above section “57 - Adding Firewall Rules”, add three more rules per the backup data that is shown below. Note that the following three instances of “`address-group`” really mean “Interface Group”. Reference Figure 101 – HOME_OUT Firewall, Rule 1, Source.

```
rule 20 {
    action accept
    description "Allow Wifi Guest Established Replies"
    log disable
    protocol all
    source {
        group {
            address-group NETv4_switch0.6
        }
    }
    state {
        established enable
        invalid disable
        new disable
        related enable
    }
}

rule 30 {
    action accept
    description "Allow Wifi Iot Established Replies"
    log disable
    protocol all
    source {
        group {
            address-group NETv4_switch0.7
        }
    }
    state {
        established enable
        invalid disable
        new disable
        related enable
    }
}

rule 40 {
    action accept
    description "Allow Wifi Spare Established Replies"
    log disable
    protocol all
    source {
        group {
            address-group NETv4_switch0.8
        }
    }
    state {
        established enable
        invalid disable
        new disable
        related enable
    }
}
```

We now need to add the final “drop” rule to the HOME_OUT Ruleset. This rule consists of:

Basic Tab has an Action of “drop”.
Advanced Tab has nothing selected (i.e. no state.)
Source Tab uses a (really this time) Address Group of “RFC-1918 Group”.

Using the steps that are shown in the above section “57 - Adding Firewall Rules”, add the last rule per the following backup data that is shown below (which matches the above settings):

```
rule 50 {
    action drop
    description "Drop RFC-1918 Traffic"
    log disable
    protocol all
    source {
        group {
            address-group RFC-1918_GROUP
        }
    }
}
```

Here is a recap of how the HOME_OUT ruleset works.

The first rule allows traffic that is “established” and “related” (i.e. associated) to go out FROM the EdgeRouter, towards devices on the Home Network that have a SOURCE address that matches (originated from) the Wired IOT Network. The association would be to traffic that previously went IN (towards the EdgeRouter) destined for the Wired IOT Network. This would typically be a request to a device on the Wired IOT Network from a device on the Home Network.

The last rule (which we just configured) drops all traffic from all the local Networks that was not matched by any of the established / related rules, i.e., any non-requested traffic that was initiated by a device on one of the non-home Networks.

The default action for the HOME_OUT ruleset is “accept,” allowing traffic that is not SOURCED from the Wired IOT Network to pass OUT to devices on the Home Network. This would be traffic coming from the internet, or from the EdgeRouter itself.

Remember that the order of firewall rules really matters in what happens to traffic. The current HOME_OUT rules are shown in Figure 103 – Firewall Ruleset Original Ordering

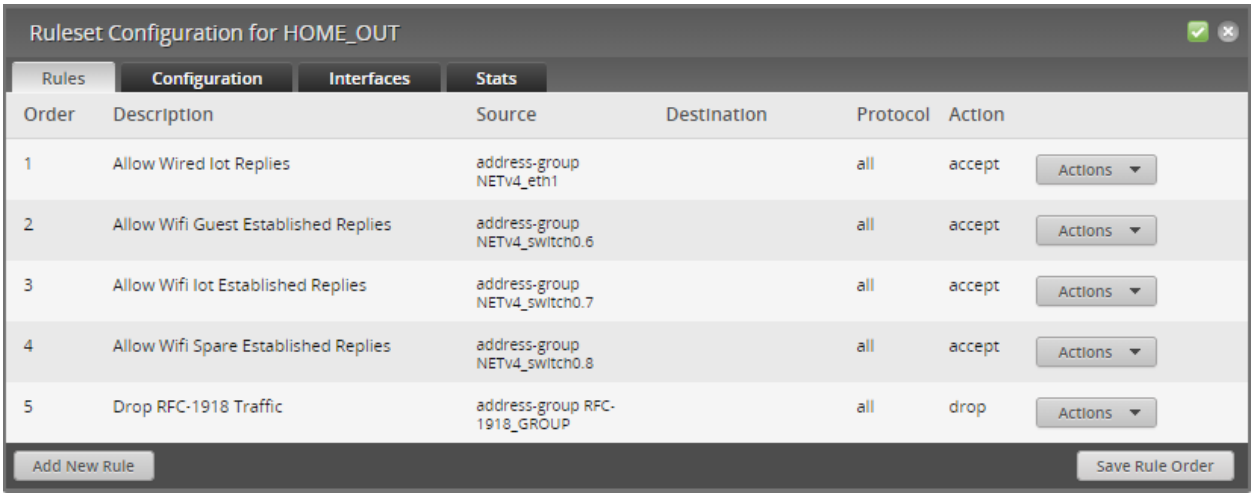


Figure 103 – Firewall Ruleset Original Ordering

To change the order of firewall rules, you simply drag a row up or down and let go. The numbers will change to show you what the order *will be* when you press the “Save Rule Order” button, which is in the lower right. To cancel a move, select the “X” in the upper right.

Drag the row `"Allow Wifi Iot Established Replies"` to the top of the entries, and let go of the mouse button. Your screen should look like Figure 104 – Firewall Ruleset Drag Order.

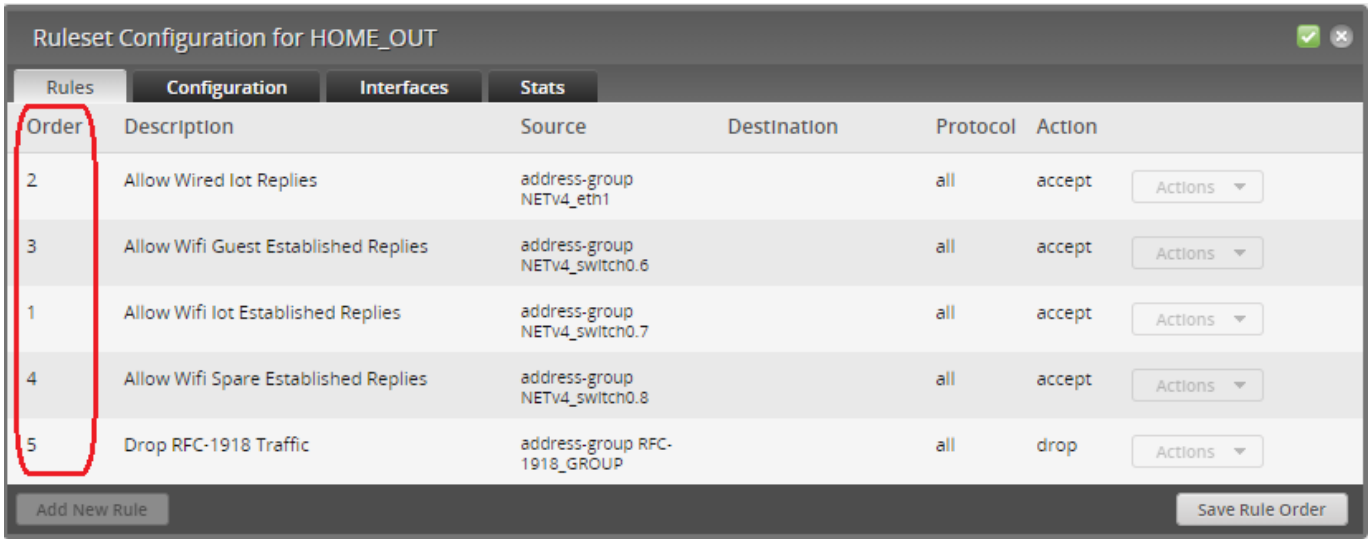


Figure 104 – Firewall Ruleset Drag Order

I am doing this, as I expect there will be more replies from Iot equipment than replies from equipment on any other Network(s), so this processing order should be more efficient. Press the “Save Rule Order” button. Your screen should now look similar to Figure 105 – Firewall Ruleset New Order.

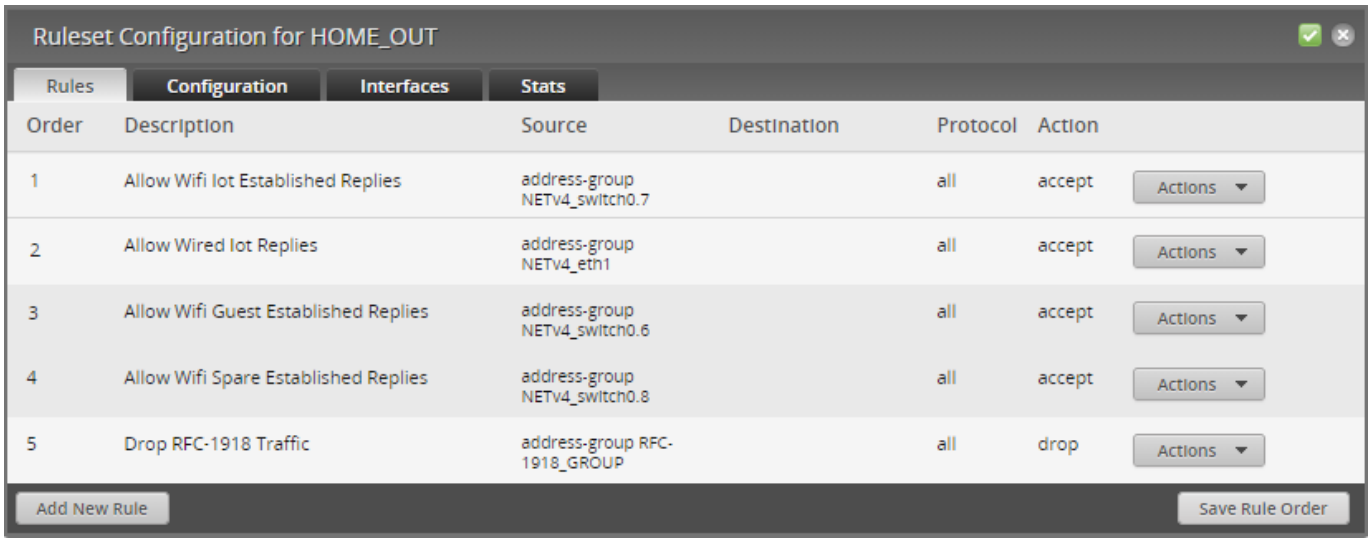


Figure 105 – Firewall Ruleset New Order

59. WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules

These rules are FWR3 and FWR9 as shown in Figure 84 – Detailed Firewall Setup Diagram.

The purpose of these rules is to block the use of EdgeRouter local services from these two IOT Networks, except for the use of DNS and the operation of DHCP.

The DHCP protocol uses a source UDP port of 68 and a destination UDP port of 67.

The DNS protocol uses port 53 of both TCP and UDP.

It has been brought up in https://github.com/mjp66/Ubiquiti/issues/54 that the (allow) DNS rule may not be needed, depending upon how you have configured your Network's DNS provider. If you use your ER-X as the DNS provider, then this rule is needed, to allow your equipment to access your ER-X as the DNS resolver. If you instead point your equipment to use an external DNS resolver, then the equipment will bypass asking the ER-X for DNS, and the DNS allow rule is no longer needed. This insight will impact the rules in this and the next several sections, including the Guest Network, below. Thanks @scottj97 for bringing this issue up. I'm going to leave these local "Allow DNS" rules enabled, for the readers which use the EdgeRouter's own address as a DNS resolver.

We now need to add two more rulesets, with each ruleset containing two firewall rules. Using the steps that are shown in the above section "57 - Adding Firewall Rules", add the following two rulesets, each containing two firewall rules, with a real address-group, per the backup data that is shown below:

When adding the following WIRED_IOT_LOCAL ruleset, remember to also set and SAVE the following:

Interface: eth1
Direction: local

```
name WIRED_IOT_LOCAL {
    default-action drop
    description "Wired Iot Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67
        }
        log disable
        protocol udp
        source {
            port 68
        }
    }
    rule 2 {
        action accept
        description "Allow DNS"
        destination {
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

When adding the DNS rule, the above "tcp_ucp" description is shown in the GUI as "Both TCP and UDP."

Note that there is an “Actions” / “Copy Ruleset” available, that can be used to clone an existing ruleset.

When adding the following WIFI_IOT_LOCAL ruleset, remember to also set and SAVE the following:

Interface: switch0.7
Direction: local

```
name WIFI_IOT_LOCAL {
    default-action drop
    description "WiFi Iot Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67
        }
        log disable
        protocol udp
        source {
            port 68
        }
    }
    rule 2 {
        action accept
        description "Allow DNS"
        destination {
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

When adding the DNS rule, the above “tcp_ucp” description is shown in the GUI as “Both TCP and UDP.”

60. WIFI_GUEST_LOCAL Firewall Rules

These rules are FWR8 as shown in Figure 84 – Detailed Firewall Setup Diagram.

The purpose of these rules is to block the use of EdgeRouter local services from the Wi-Fi Guest Network, except for the use of DNS and the operation of DHCP.

To add the following ruleset and rules, follow what was done in the above section “57 - Adding Firewall Rules”.

When adding the following WIFI_GUEST_LOCAL ruleset, remember to also set and SAVE the following:

Interface: switch0.6
Direction: local

```
name WIFI_GUEST_LOCAL {
    default-action drop
    description "Wifi Guest Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67
        }
        log disable
        protocol udp
        source {
            port 68
        }
    }
    rule 2 {
        action accept
        description "Allow DNS"
        destination {
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

61. WIFI_SPARE_LOCAL Firewall Rules

These rules are designated as FWR10 but are not shown in Figure 84 – Detailed Firewall Setup Diagram. You can instead look at the similar FWR8.

The purpose of these rules is to block the use of EdgeRouter local services from the Wi-Fi Spare Network, except for the use of DNS and the operation of DHCP.

To add the following ruleset and rules, follow what was done in the above section “57 - Adding Firewall Rules”.

When adding the following WIFI_SPARE_LOCAL ruleset, remember to also set and SAVE the following:

Interface: switch0.8
Direction: local

```
name WIFI_SPARE_LOCAL {
    default-action drop
    description "WiFi Spare Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67
        }
        log disable
        protocol udp
        source {
            port 68
        }
    }
    rule 2 {
        action accept
        description "Allow DNS"
        destination {
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

62. Optional DNS Forcing of the WIFI_IOT_LOCAL Network

Performing the steps within this section is optional. This forcing of DNS is NOT really needed, but was a good exercise in learning how NAT rules operate. Details within this section previously forced DNS requests within the Guest Network, but now forces DNS requests within the IOT Network.

If you setup the NAT rules in this section, ensure you actually used OpenDSN addresses for VLAN.7 in section 32 - Add DHCP Servers to the VLANs

The destination Network Address Translation (NAT) rules, presented here, will force any devices on the IOT Network to only be able to use Open DNS resolvers. This is regardless if the devices specify their own DNS resolver addresses and ignore the DNS resolver addresses suggested by the EdgeRouter's IOT DHCP server.

The two rules presented here work with each other. Rule #1 will exclude NAT from being performed on DNS requests directed towards either of the OpenDNS resolver addresses, i.e. normalDNS and BackupDNS. These two addresses are in an address group. This allows both the primary and secondary resolver addresses to pass-through the EdgeRouter from the IOT Network. Note that If the primary DNS resolver is unavailable, then the requesting device will instead (internally) query the backup DSN address. Rule #1 allows both primary and backup addresses.

Rule #2 will act upon any remaining port 53 (DNS) requests (that did not match Rule #1) from the IOT network, and translate the associated IP address into the address of the primary OpenDNS resolver. Note that any IOT device using their own (Non-suggested-OpenDNS) resolver address will not operate, when the primary OpenDNS resolver / server is unavailable.

Press the Firewall/NAT button near the top of the screen. Reference Figure 76 – Firewall/NAT Button.

Ensure that the NAT tab is selected and then press the "+ Add Destination NAT Rule" button. See Figure 106 – NAT Tab.

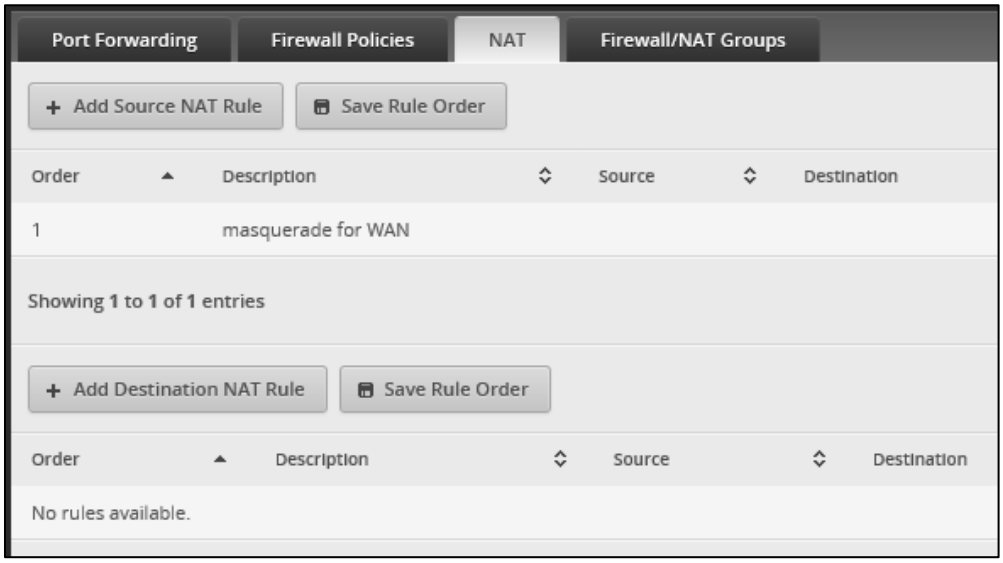


Figure 106 – NAT Tab

You will be presented with a “Destination NAT Rule Configuration” dialog.

Enter the data for NAT rule #1, as follows:

Description	Exclude OpenDNS Wifi IOT
Enable	CHECKED
Inbound Interface	switch0.7
Translations, Port	53
Exclude From NAT	CHECKED
Protocol	Both TCP and UDP
Dest Port	53
Dest Address Group	OpenDNS Servers

and save it. See Figure 107 – NAT Rule Number 1.

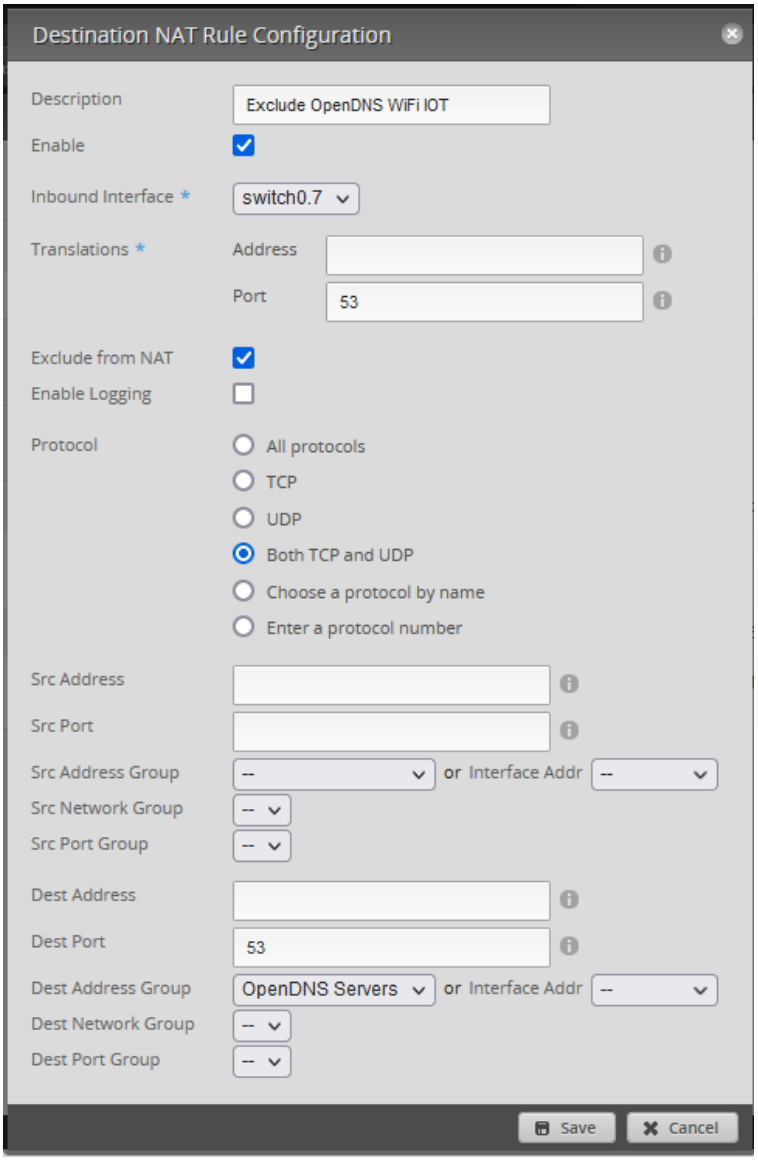


Figure 107 – NAT Rule Number 1

Press the “+ Add Destination NAT Rule” button and enter the data for NAT rule #2, as follows:

Description	Force OpenDNS Wifi IOT
Enable	CHECKED
Inbound Interface	switch0.7
Translations, Address	208.67.222.222
Exclude From NAT	Un-Checked
Protocol	Both TCP and UDP
Dest Port	53

and save it. See Figure 108 – NAT Rule Number 2.

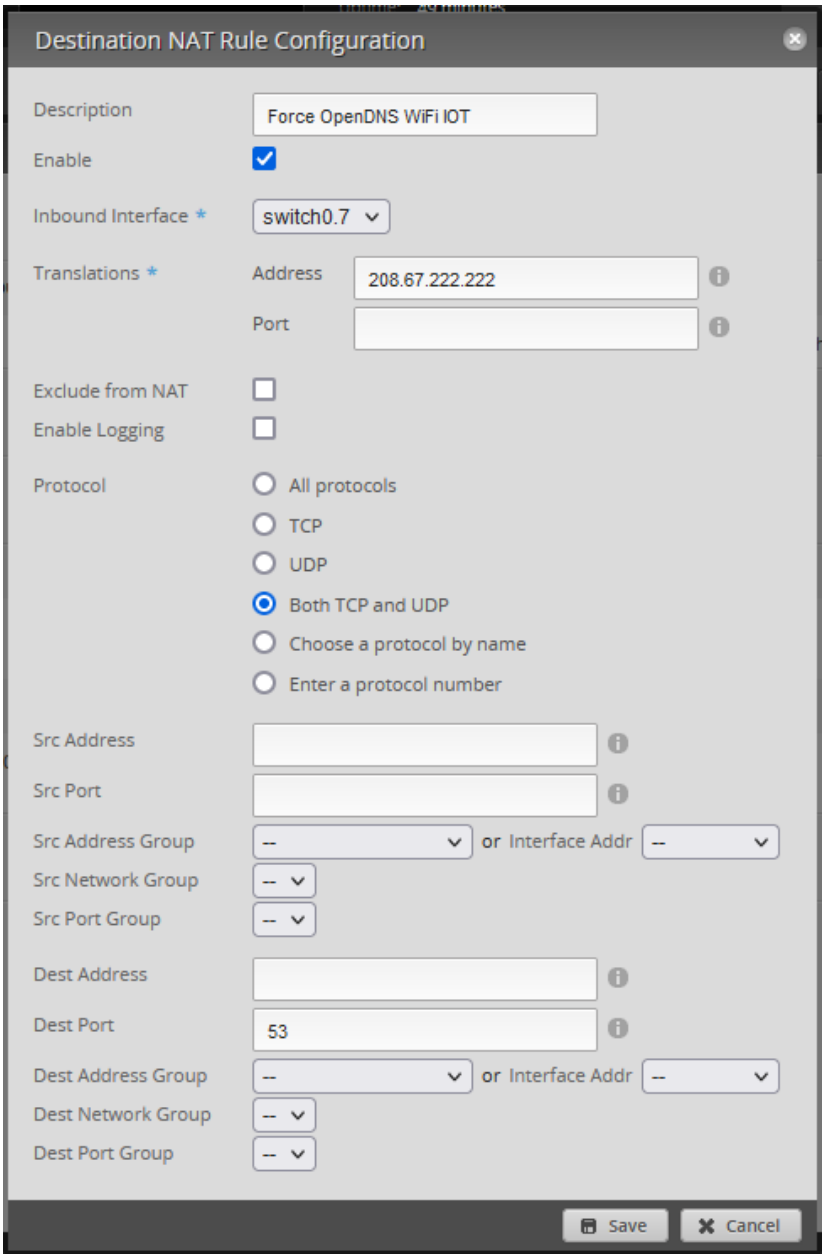


Figure 108 – NAT Rule Number 2

This is the relevant portion from the backup file. Rule 5010 is an existing Source NAT rule for handling the WAN port (eth0).

```
    nat {
        rule 1 {
            description "Exclude OpenDNS WiFi IOT"
            destination {
                group {
                    address-group OPENDNS_SERVERS_GROUP
                }
                port 53
            }
            exclude
            inbound-interface switch0.7
            inside-address {
                port 53
            }
            log disable
            protocol tcp_udp
            type destination
        }
        rule 2 {
            description "Force OpenDNS WiFi IOT"
            destination {
                port 53
            }
            inbound-interface switch0.7
            inside-address {
                address 208.67.222.222
            }
            log disable
            protocol tcp_udp
            type destination
        }
        rule 5010 {
            description "masquerade for WAN"
            outbound-interface eth0
            type masquerade
        }
    }
```

These rules can be tested, if you are implementing this DNS forcing using actual OpenDNS resolvers. This is because OpenDNS has a test page:

http://welcome.opendns.com

that can show if you are using OpenDNS as a resolver.

To perform this test, first temporarily change the DNS resolvers associated with the IOT Network's DHCP server (switch0.7) to something else. I used addresses of 8.8.8.8 and 8.8.4.4 from Google. Reference section 32 - Add DHCP Servers to the VLANs. Then, using a device attached to the IOT Network, visit the OpenDNS test page. If you get their success page, then these two rules translated the Google DNS addresses into OpenDNS addresses. You may have to reboot the EdgeRouter and/or the IOT device to ensure that the changed DNS resolver addresses propagated to the IOT device. Remember to return the IOT Network's DNS resolver addresses (in the DHCP area) back to the OpenDNS addresses and reboot your equipment.

Reference this OpenDNS page about testing:
https://support.opendns.com/hc/en-us/articles/227986567-How-to-Test-for-Successful-OpenDNS-Configuration-

Additional Reference: EdgeRouter DNS Redirection: https://www.youtube.com/watch?v=EFWbYQPe3XI

63. WIRED_SEPARATE Firewall Rules

The Wired Separate Network is meant to be kept separate from the other Networks, i.e., not allow communications with anyone except with the Internet.

There are two usage scenarios, which I can think of, for the Separate Network.

1. You might want to put your banking computer on this Separate Network.
   In this instance, people and devices on the other Networks cannot get to your banking computer.
2. You might want to provide internet access to the friend's kid (i.e. tenant) who lives in your basement.
   In this instance, you don't want any people or devices on the Separate Network
   to be able to access any of your other Networks, OR be able to access the internals of the EdgeRouter.

I'm thinking that eth2 needs to be removed from the ER-X's switch to ensure that tagged VLAN data does not leak out the eth2 port from the switch usage.

Reference Figure 84 – Detailed Firewall Setup Diagram, for FWR numbers and Network routing / interactions

Reference Table 1 - Table of Networks, for Network subnet addresses

To block instance number 1, we need to block traffic from exiting OUT of the EdgeRouter that was initiated from another Network / subnet, and then allow other traffic (from the Internet.)

To add the following ruleset and rules, follow what was done in the above section "57 - Adding Firewall Rules".

When adding the following WIRED_SEPARATE_OUT ruleset, remember to also set and SAVE the following:

Interface: eth2
Direction: out

```
name WIRED_SEPARATE_OUT {
    default-action accept
    description "Wired Separate Out"
    rule 1 {
        action drop
        description "Drop Non-Separate Traffic"
        log disable
        protocol all
        source {
            group {
                address-group RFC-1918_GROUP
            }
        }
    }
}
```

To block the first part of instance number 2, we need to block traffic from entering IN the EdgeRouter and going to devices that are on any of the other Networks. This ruleset will be labeled WIRED_SEPARATE_IN and is denoted as FWR5.

When adding the following WIRED_SEPARATE_IN ruleset, remember to also set and SAVE the following:

Interface: eth2
Direction: in

```
name WIRED_SEPARATE_IN {
    default-action accept
    description "Wired Separate In"
    rule 1 {
        action drop
        description "Block RFC-1918 Traffic"
        destination {
            group {
                address-group RFC-1918_GROUP
            }
        }
        log disable
        protocol all
    }
}
```

To block the second part of instance number 2, we need to block traffic from entering the EdgeRouter itself (LOCAL) except for DNS and DHCP requests. This ruleset will be labeled WIRED_SEPARATE_LOCAL and is denoted as FWR4.

When adding the following WIRED_SEPARATE_LOCAL ruleset, remember to also set and SAVE the following:

Interface: eth2
Direction: local

```
name WIRED_SEPARATE_LOCAL {
    default-action drop
    description "Wired Separate Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67
        }
        log disable
        protocol udp
        source {
            port 68
        }
    }
    rule 2 {
        action accept
        description "Allow DNS"
        destination {
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

64. EdgeMax Change Interface Names

Press the Dashboard Button. Reference Figure 35 – Dashboard Button.

Find the line with an Interface of “switch0”. Click on the Action button to the right of this line. Select “Config” from the Actions Menu. You will see a dialog similar to Figure 38 – switch0 Configuration. Change the Description field to “Home Net.”

Repeat these steps for the following Interfaces as shown in Table 4 - Table of Interface Names:
(You have just done the last one)

Interface	Description
eth1	Iot Net
eth2	Wired Separate Net
eth3	Home Net
eth4	Home Net
switch0	Home Net

Table 4 - Table of Interface Names

65. SmartQueue Setup

This section is optional. Turning on SmartQueue (on your WAN port) can help solve the issue of "bufferbloat". Reference the internet for "bufferbloat" if you are unfamiliar with it. Smart Queue is a variety of Quality of Service (QoS.) Enabling QoS may disable the hardware acceleration that was enabled in section 37 - EdgeRouter Enable HW NAT Assist. I think that if you only enable QOS on the WAN port, that HW acceleration will stay enabled.

One place to test connection speeds (and bufferbloat), to see if you should setup QoS, is:

http://www.dslreports.com/speedtest

To enable SmartQueue, press the QoS button, located near the top of the page. See Figure 109 – QoS button.

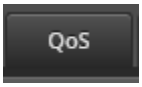


Figure 109 – QoS button

Ensure that the Smart Queue tab is selected. You may not need to press the "+ Add Smart Queue" button.

QOS needs to know your maximum upload rate and/or your maximum download rate to be able to manage the data. Since we will be selecting eth0, which is your WAN, you can run a speedtest to acquire these numbers. From what I understand, QOS kicks-in when you reach (approximately 90% to 95% of) these maximum rates. This means that you lose about 10% of your internet bandwidth when enabling QOS. If you make the number(s) too high, then QoS will not take effect, and you lose the benefit of having QOS. If you make the number(s) too low, then you are throwing away more bandwidth.

There are also posting / indications that you should only implement SmartQueue in the Upload direction. My (example) connection speeds are 26 down and about 5 up, so that is what I show here.

To enable QOS on your WAN connection:

Choose a Policy name, like "Internet QOS".
Choose WAN Interface of eth0.
Check "Apply to upload traffic".
Enter your own upload speed (probably Mbits/sec) into the Upload Rate box.
Press Apply.

If Download filtering is desired:
Check "Apply to download traffic".
Enter your own download speed (probably Mbits/sec) into the Download Rate box.
Press Apply.

If Download filtering is NOT desired:
Ensure "Apply to download traffic" is UnChecked.

Optionally, you can check "Show advanced options". I know nothing about these options.

See Figure 110 – Example SmartQueue Settings

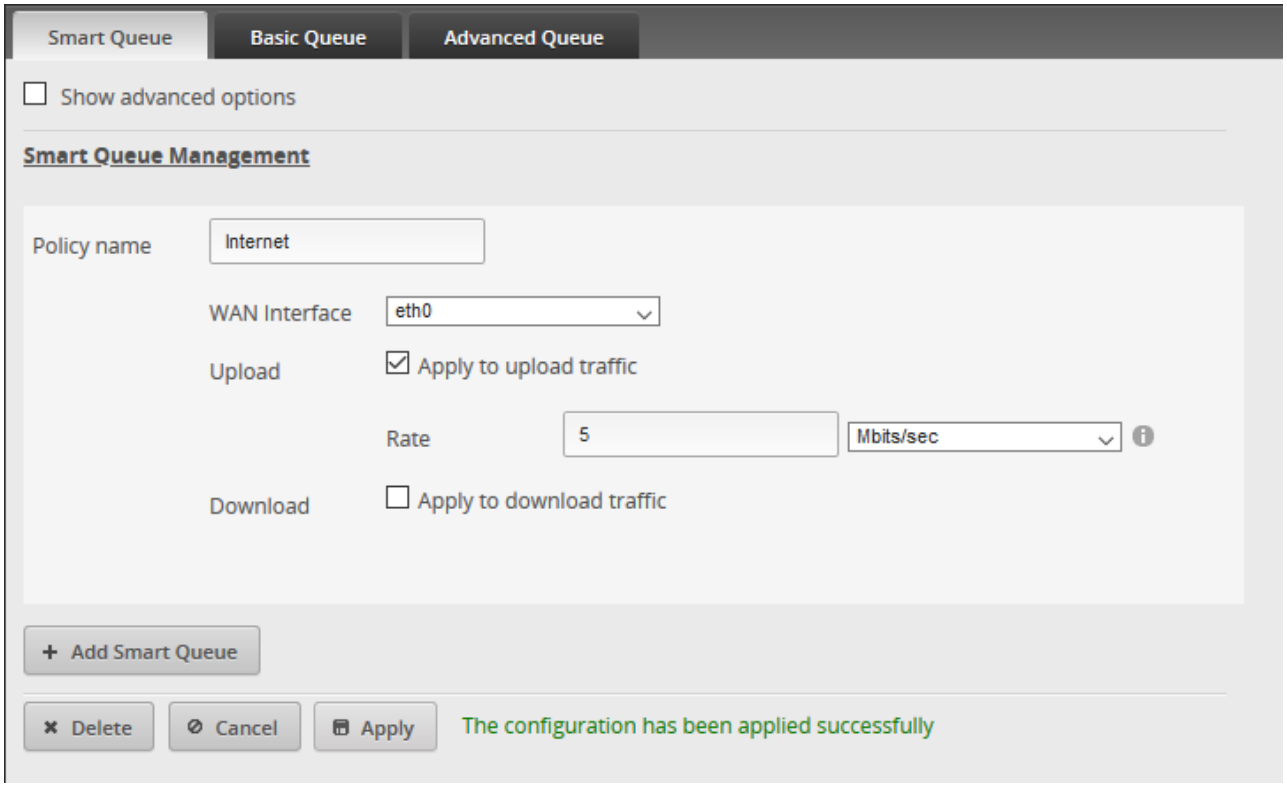


Figure 110 – Example SmartQueue Settings

References:

QC Ubiquiti EdgeMAX - Basic Smart Queue Quality of Service (QoS)
https://www.youtube.com/watch?v=8NGlzMGd_IA

EdgeRouter Quality of Service
https://help.ui.com/hc/en-us/articles/216787288-EdgeRouter-Quality-of-Service-QoS-

How to Set Up EdgeRouter QoS:
https://www.youtube.com/watch?v=3hvmzEv8iNQ

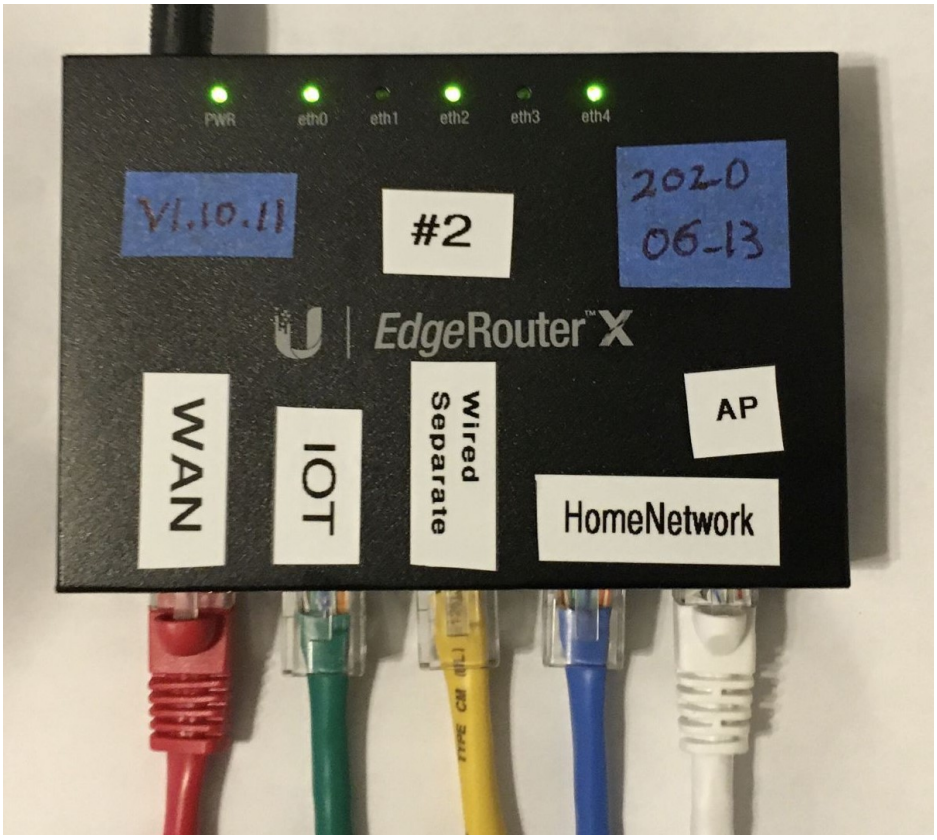
Edgerouter X - Smart Queue:
http://kazoo.ga/edgerouter-x-smart-queue/

Gaming QoS for League of Legends:
https://community.ui.com/questions/Gaming-QoS-for-League-of-Legends-LoL/32392060-627f-40cc-9d48-32d1113ebd44

66. ER-X Marking

This is how I typically mark my ER-X routers:

- Labels for permanent items
- Blue (masking type) Tape for temporary labels



I also try and use colored patch cables to denote different Networks (at least at the router).

67. End of ER-X Basic Setup

This is the end of the ER-X Basic setup. There are additional / optional ER-X setup steps later.

68. Ubiquiti AP-AC-LR Access Point Setup

This guide utilized Access Point software (UniFi) installed on a Windows PC. This software ONLY needs to be running when you are adopting or making configuration changes to your Access Point(s). The software does NOT need to be running all the time, unless you want the optional guest portal / data-collection features. These features might be found in a Motel/Hotel WiFi system, or a school building / library.

Other Ubiquiti Access points should work; the Ubiquiti AP-AC-LR model is just the model that I purchased.

I would **never** install this software on a PC again, because it requires buggy Java. There are also clients available for Linux, Macs, Android phones and Apple phones. I have heard that the phone Apps are rather limited. Ubiquiti makes dedicated device(s) called Cloud-Key (Generation 1, and now Generation 2) which runs this software. Pricing for Generation 1 seems about $100. If you can afford it, the Cloud-Key device or the Raspberry Pi solution discussed below, is well worth the hassle of loading Java on your PC. If you are very cost sensitive, loading software on your PC is free.

I purchased a Cloud-Key (now Generation 1) and used it for years. Having this device saves the hassle of installing the UniFi Software (and insecure Java) software on a PC. The configuration steps look the same / similar. The Cloud-Key Generation 1 devices may not be usable and may need manual recovery after power is interrupted / restored. This probably applies to the Raspberry Pi solution also.

You can also install the UniFi Software onto a Raspberry Pi computer, see details below. This is more cost effective than purchasing a real Cloud-Key. Remember the UniFi Software does not need to be run continuously, so you can repurpose your Raspberry Pi if you want. I am now running my UniFi controller software on a Raspberry Pi. I loaded the Raspberry Pi, per the following directions, acquired my most recent Cloud-Key backup image and restored that backup image to this Raspberry Pi installation. It found my Access Point(s) and worked just fine. You do not want to access the UniFi Software using a browser on the Raspberry Pi, access it remotely using a PC, as the Raspberry Pi may not have enough memory to support both UniFi Software and a browser at the same time.

I will try to call all of these installations (that run UniFi Software) a generic name of “UniFi Controller” or just UniFi, within this guide. For my uses, I typically only power-up / run the UniFi Controller / PC Software / Cloud Key / Raspberry Pi when I need to make a configuration change to an Access Point, so I have little experience with long-term / always-on usage. It is import that power is not cut unexpectedly to your UniFi Controller, as some internal database can get corrupted, and then your controller will not boot.

Version note 1: As of 2020 and early 2021, Ubiquiti has released 6.X version(s) of the Unifi Controller software. There are many Ubiquiti community posts advising that users, for various bugs, downgrade to (the latest 5.X) 5.14.23 version. Downgrading actually consists of resetting your controller, and then reloading a backup file made from that specific version. So backup your UniFi installation, frequently and often. Reference https://community.ui.com/questions/How-to-downgrade-from-UniFi-Network-Controller-6-0-23-to-5-14-23/625ff0ef-97f8-4579-8293-6f3b6517d483

Version note 2: As of late 2020 and early 2021, there are even more Ubiquiti community posts advising users, because of many severe bugs, to downgrade their AP firmware to version 4.3.20. Reference https://help.ui.com/hc/en-us/articles/204910064-UniFi-Upgrade-the-Firmware-of-a-UniFi-Device

Version note 3: As of late 2021, I’m trying the new newest Unifi Controller software on a spare CloudKey Ver 1, and am testing new firmware on a U6-Lite-US. System seems to work fine. Ubiquity is still releasing tons of beta and non-beta software / firmware updates (at a furious rate). The U6 APs require a newer software base (than above) to operate.

Version note 4: As of 1Q 2022, I'm now running UniFi controller software 6.5.55 on a Raspberry Pi. UniFi version 7.X was also available, but I'll wait a while on that 'Beta' version. While (temporarily) running my house on my existing AP-AC-LR, I started completely-over by factory resetting my U6-Lite-US and U6-LR-US and re-adopting (only) those into this new controller instance. The U6 APs are running firmware 6.0.15.13647 (latest when this was written). Wi-Fi seems pretty stable, but I only have about a month of time on these U6 APs. It is likely that only one of these U6 APs is actually needed for my home. I also needed to disable "System" / "New User Interface" within my Unifi controller software, to be able to configure many of the settings used within this document. This UI looks a lot different, but I was able to generate a configuration which matched the ER-X's VLAN structure.

Version note 5: As of 2Q 2022: I'm now running Unifi 7.1.61 on a Raspberry Pi and 6.0.19.13671 (latest when this was written) on my two U6 APs. I've re-boxed (i.e. unpowered spare) my original AP-AC-LR and left it at AP firmware version 4.3.20. I don't think I'm experiencing any (real) Wi-Fi problems, but I see a lot of device disconnections, immediately followed by a device (re-)connection, typically to the same AP. It also seems that UniFi is dropping / not reporting events within the "Events" tab. I don't know when those problems started, because I typically have not (in the past), continuously run the Unifi software.

Version note 6: As of 3Q 2022: I'm still running Unifi 7.1.61 on a Raspberry Pi and downgraded to 6.0.15 on my two U6 APs. I've relegated my U6-LR to the basement, and re-introduced my AP-AC-LR at 4.23.20. I later un-plugged the U6-LR, because roaming clients were still impacted.

Version note 7: As of 4Q 2022: I'm still running Unifi 7.1.61 on a Raspberry Pi and now upgraded to 6.2.41 on both the U6-Lite and U6-LR. The AP-AC-LR is now boxed up as a cold spare (i.e. unplugged). Let's see how long they can achieve stability with the U6-LR.

If you are starting fresh, with a new UniFi, you may need to perform:

```
Settings -> System -> Advanced -> Interface: Legacy; Deactivate
```

to try and follow this guide.
https://community.ui.com/questions/Mike-Potts-Ubiquiti-AP-AC-LR-Access-Point-Setup-new-changed-interface-Unify-Network-7-2-95-2022/d65fea97-2611-477e-b98d-ecde748dbbd1

@rpoppes
Never turn on auto update with ubiquiti. They use customers for their testing, which is fine, but they need to state that very clearly. Nearly all updates have serious issues where people spend many hours and sometimes days trying to figure out what is going on. And yes downgrade is often the only option.

UniFi / Cloud-Key Help Links

UniFi-Installation-Scripts [Stated Ubuntu/Debian Machines]
https://community.ui.com/questions/UniFi-Installation-Scripts-or-UniFi-Easy-Update-Script-or-UniFi-Lets-Encrypt-or-UniFi-Easy-Encrypt-/ccbc7530-dd61-40a7-82ec-22b17f027776

https://help.ui.com/hc/en-us/categories/200320654-UniFi-Wireless

https://help.ui.com/hc/en-us/articles/360012192813

https://help.ui.com/hc/en-us/articles/360000128688-UniFi-Troubleshooting-Offline-Cloud-Key-and-Other-Stability-Issues

https://help.ui.com/hc/en-us/articles/360006634094

https://help.ui.com/hc/en-us/articles/204911424-UniFi-How-to-Remove-Prune-Older-Data-and-Adjust-Mongo-Database-Size

Other UniFi / Cloud-Key Links

Cannot log in to Cloud Key WebUI
https://community.ui.com/questions/Cannot-log-in-to-Cloud-Key-WebUI/e31a1fc1-7e19-40a7-a266-4d36c35825e4#answer/cf3de5ce-ed9c-4cef-90cd-cdbcceb6da3e

Unifi Cloudkey invalid username password
https://community.ui.com/questions/Unifi-Cloudkey-invalid-username-password/a8d87d40-50ad-4bc9-9a1b-2a5eb68694df#answer/82d80371-a9ac-484d-b293-19ad9ec44ec1

Repairing Database Issues on the UniFi Controller
https://help.ui.com/hc/en-us/articles/360006634094-UniFi-Network-Controller-Repairing-Database-Issues-on-the-UniFi-Controller

Re-purposing a consumer router as an Access Point.

If you are going to re-purpose a consumer router as an Access Point, instead of using an Ubiquiti Access Point, remember that some of the Network security is achieved via VLANS and Guest options within the Access Point. Firewall rules within the EdgeRouter may need to be adjusted, probably additional Guest Control Post-Authorization Restrictions. See near Figure 143 –Unifi Guest Control. I suggest acquiring real Ubiquiti Access Point(s).

UniFi on Raspberry Pi Information.

This is the Raspberry Pi installation I tried (I have not gotten to the Pi-Hole portion, yet):
https://community.ui.com/questions/Step-By-Step-Tutorial-Guide-Raspberry-Pi-with-UniFi-Controller-and-Pi-hole-from-scratch-headless/e8a24143-bfb8-4a61-973d-0b55320101dc

For completeness and caching, here is the main command to install UniFi Software onto a Raspberry Pi:
(Check the above link for updates, and this is a single, very long line)

```
wget "https://github.com/SmokingCrop/UniFi/raw/master/install-unifi-pihole-English.sh" -O install-unifi-pihole.sh && chmod +x install-unifi-pihole.sh && ./install-unifi-pihole.sh no-pihole
```

You may need to wait a couple of minutes (after rebooting the Raspberry Pi) for the software to finish starting. You do not want to access the UniFi Software using a browser on the Raspberry Pi, access it remotely using a PC, as the Raspberry Pi may not have enough memory to support both UniFi Software and a browser at the same time.

To upgrade the UniFi Software, that is running on a Raspberry Pi:
(These are not exact directions, because this is from memory)

Click on the download-new-software popup-box.
Find the browser download notification or the downloaded file.
Run the downloaded .deb file.
Software should restart, wait a couple of minutes for installation / restart.

Here are some other Raspberry Pi links:

Article first seen here:
https://community.ui.com/questions/Newbie-need-help-on-setup/28cb82b2-4b6a-4485-b115-779b9eead7a8#answer/68f1358e-c560-4096-860c-2ba0c89e9dff

https://lazyadmin.nl/home-network/installing-unifi-controller-on-a-raspberry-pi-in-5-min/

https://www.youtube.com/watch?v=XIn-39o0g2M

https://pimylifeup.com/rasberry-pi-unifi/

https://dougrathbone.com/blog/2018/03/31/configuring-a-ubiquiti-unifi-controller-to-run-on-raspberry-pi

69. Hookup the Ubiquiti AP-AC-LR Access Point

The following information is specific to the AP-AC-LR Access Point. Other models of Access Points may-be / are-powered differently and/or use different POE standards and voltages, so use caution.

Using two standard Ethernet cables:

Wire the EdgeRouter's eth4 port to the LAN port of the included Power-Over-Ethernet (POE) Adapter.
Wire the POE port of the POE adapter to the Ethernet port on the Ubiquiti AP-AC-LR Access Point.

See Figure 111 – AP-AC-LR Access Point Wiring.

Plug the POE adapter into your main electrical power.

WARNING: Connecting the POE port of the POE adapter to any other device will probably burn-up that other device.

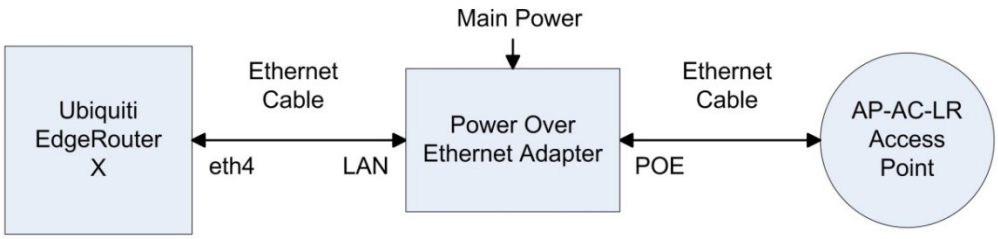


Figure 111 – AP-AC-LR Access Point Wiring

You can also have the AP-AC-LR POE adapter powering both the ER-X and the AP-AC-LR Access Point. I am not powering my devices that way, as some people have reported instability. There is also the possibility of forgetting that eth4 is POE enabled, and plugging in some other equipment and burning that equipment up. I like to keep the POE adapter next to the Access Point. For 24V POE adapters, there appears to be both 12W (24V * 0.5A) and 24W (24V * 1A) varieties.

References (also see parent discussions)**:**

https://community.ui.com/questions/PoE-does-not-work-on-ER-X-with-AP-AC-LR/165d1a73-1dff-467c-9c70-9efc8085d9ed#answer/2ea39394-72de-4955-a174-d1943fc428fa

Don't mix up power adapters between UAPs. Some models are 24V passive and some are 48V.

70. Download and Install the UniFi Software

[The UniFi screenshots, in the following sections, were taken over several years, across several different UniFi versions and also from different platforms. I now suggest installing the Unifi Software on a Raspberry Pi. You should still be able to follow along and get your Access Point(s) configured from what is here. Cloud-Key / Raspberry Pi users should be able to jump to section 72 - Initial Setup of the UniFi Software. Now back to the legacy directions.]

For Windows users, you will need to be an Administrator, or the installation will install (somewhere else) in the area belonging to the admin's account that was used.

Browse to:

https://www.ubnt.com/download/unifi/

Under the SOFTWARE section, download a version of the "Unifi Controller for Windows" software (Unifi-installer.exe). [See Version notes in section 68 - Ubiquiti AP-AC-LR Access Point Setup.]

Under the DOCUMENTATION section, you might also want to download:

UniFi Controller v5 Users Guide (or later version)
UniFi AC-LR-AP Quick Start Guide.

The following install items may be slightly out of order between your installation and that of this guide. I had to re-start my UniFi Setup. You might also reference https://github.com/mjp66/Ubiquiti/issues/7

Run the Unifi-installer.exe. Acknowledge any Windows admin prompts. See Figure 112 – UniFi Setup Welcome Screen.

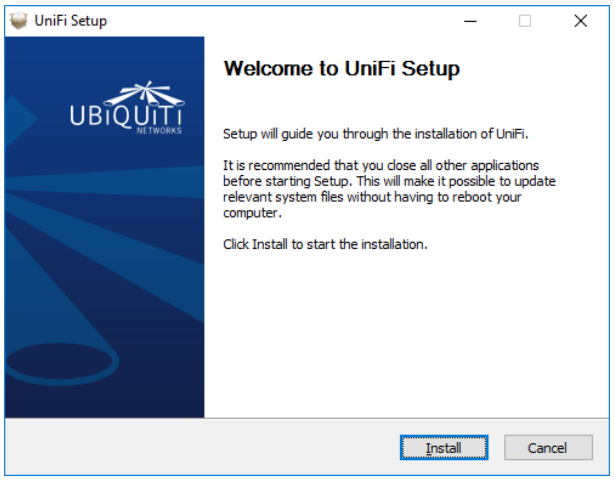


Figure 112 – UniFi Setup Welcome Screen

If Java is not installed on your your PC, you will be prompted to install Java. See Figure 113 – UniFi Java Required. Click "OK".

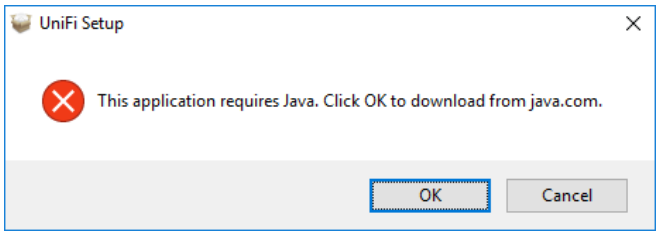


Figure 113 – UniFi Java Required

You will be taken to an Oracle site to download Java. Click on the “Free Java Download” button. See Figure 114 – Unifi Download Oracle Java. Note that Oracle asks “Why download Java?” My only answer is “Because I have to”.

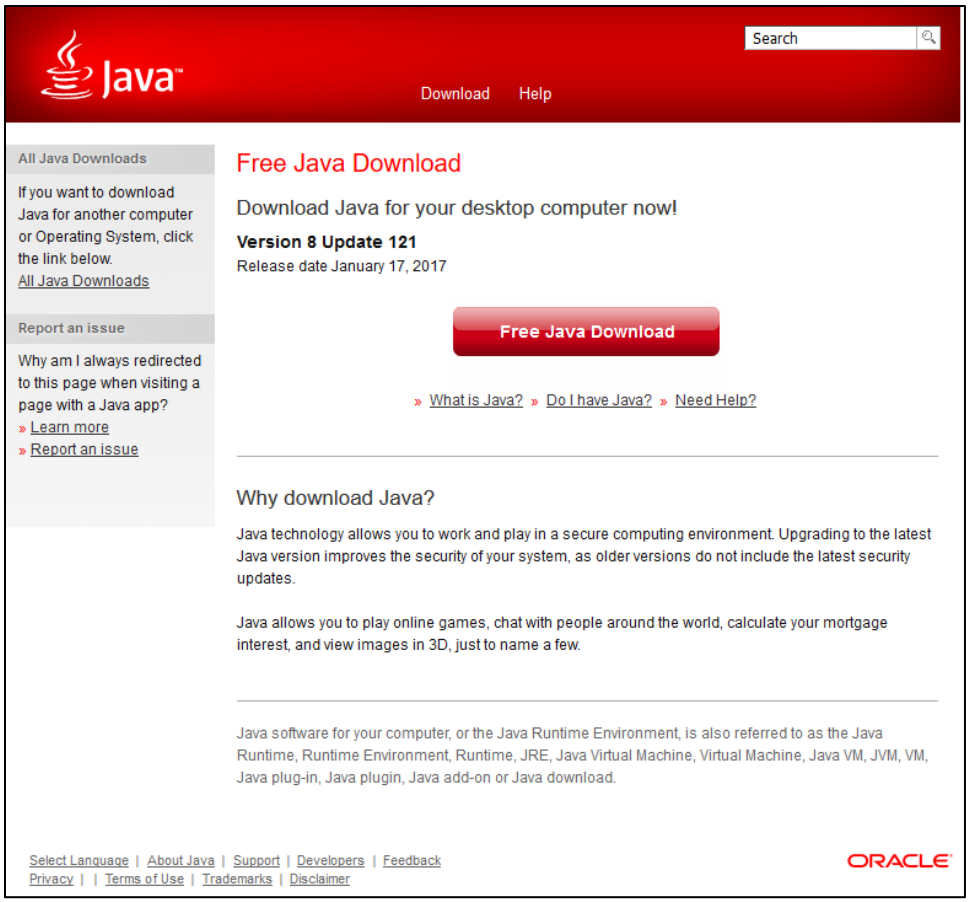


Figure 114 – Unifi Download Oracle Java

While downloading, Oracle will inform you that their security holes are found everywhere, and that you can experience that also. See Figure 115 – UniFi Downloading Oracle Java.

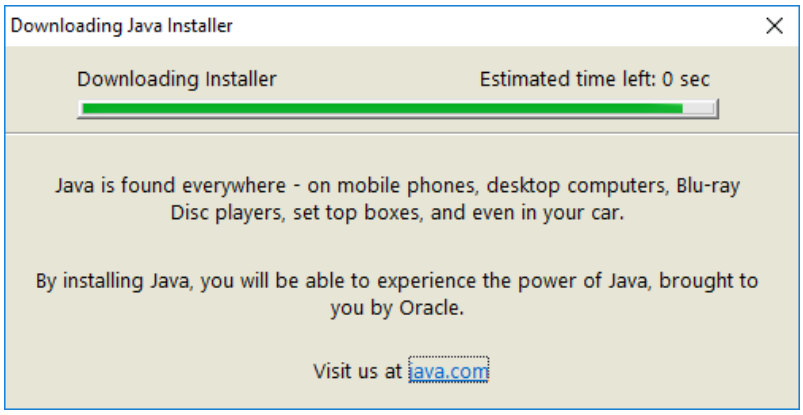


Figure 115 – UniFi Downloading Oracle Java

When done downloading, they will try and monetize you by setting up crapware. Select “Do not update browser settings”, unless you like this type of stuff. See Figure 116 – UniFi Oracle Crapware.

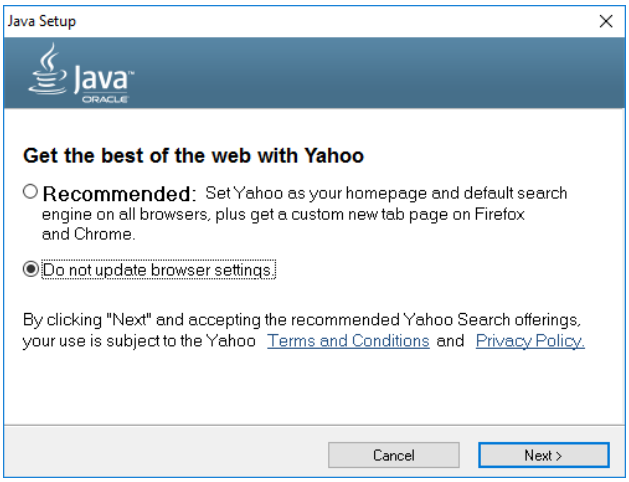


Figure 116 – UniFi Oracle Crapware

Run the downloaded JavaSetup*.exe executable. Java will install. Oracle will again inform you that they are probably responsible for hundreds of billions of accumulated security holes, with billions of them in internet connected devices that will never be patched. See Figure 117 –UniFi Java Installing.

When Java is done installing you will see the dialog of See Figure 118 – UniFi Java Done. Press “Close”. When the next browser window opened (to verify Java is working), I closed that browser verify page.

Figure 117 –UniFi Java Installing

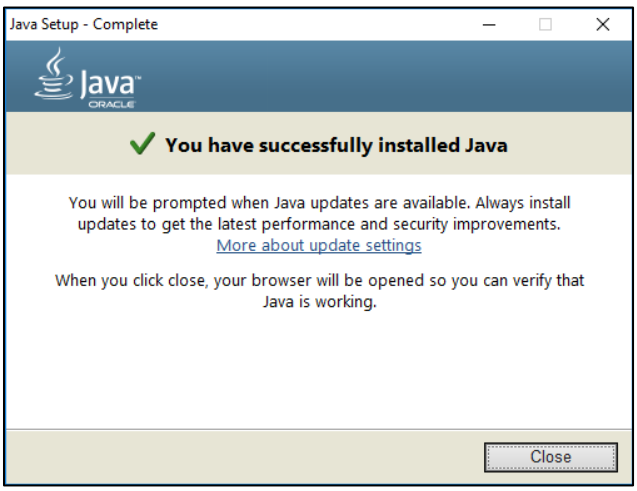


Figure 118 – UniFi Java Done

Press the Windows Start button; Go to the list of programs, select Java, then select “Configure Java”. Press the “Security” tab, and UNCHECK the”Enable Java content in the browser” checkbox. See Figure 119 – UniFi Java Control Panel. Without this you will be live-bait for any drive-by browsing malware.

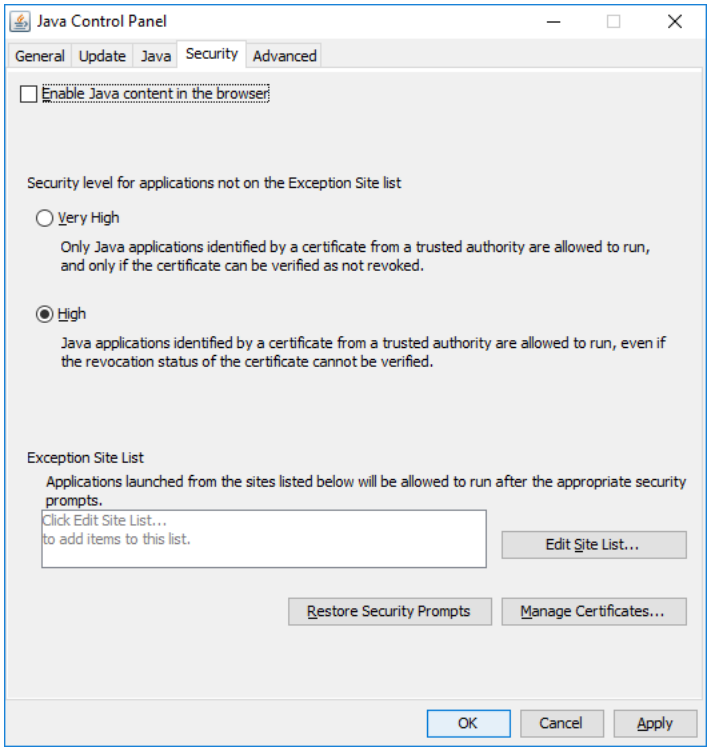


Figure 119 – UniFi Java Control Panel

I had to restart the UniFi installer. See Figure 120 – UniFi Installing.

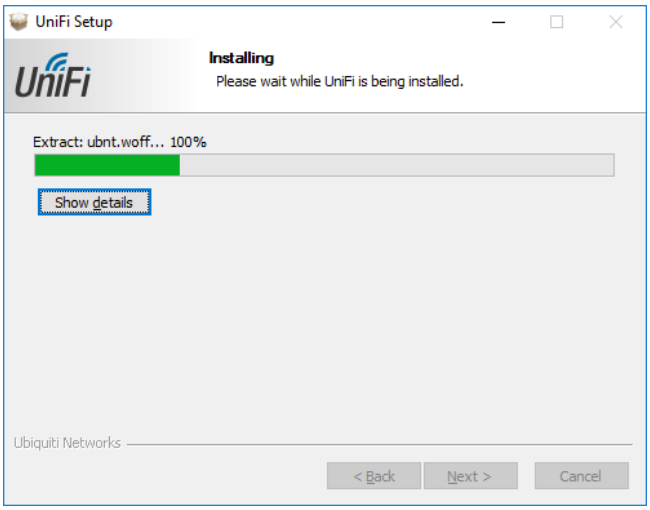


Figure 120 – UniFi Installing

The UniFi Software will finish installing. See Figure 121 – UniFi Done Installing

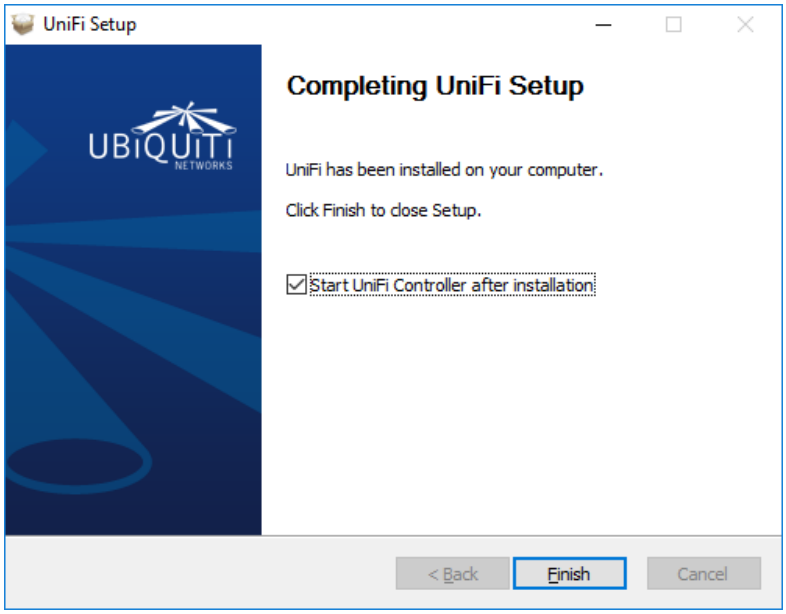


Figure 121 – UniFi Done Installing

71. Running the UniFi Software

Double click the Unifi icon on your desktop. See Figure 122 – UniFi Icon

Figure 122 – UniFi Icon

The UniFi controlling software will start to initialize. See Figure 123 – UniFi Controller Software Initializing.

Figure 123 – UniFi Controller Software Initializing

When it has fully started, it will look like Figure 124 – UniFi Controller Software Running.

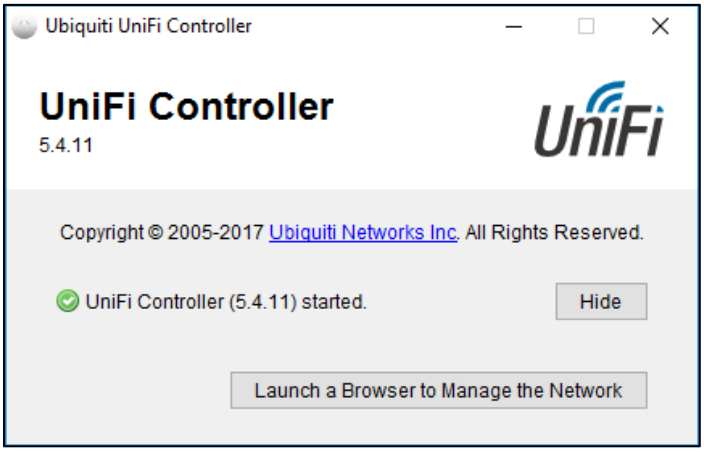


Figure 124 – UniFi Controller Software Running

When the UniFi Software started for the first time, a Windows Firewall dialog popped up. See Figure 125 – Windows Initial Firewall - UniFi.

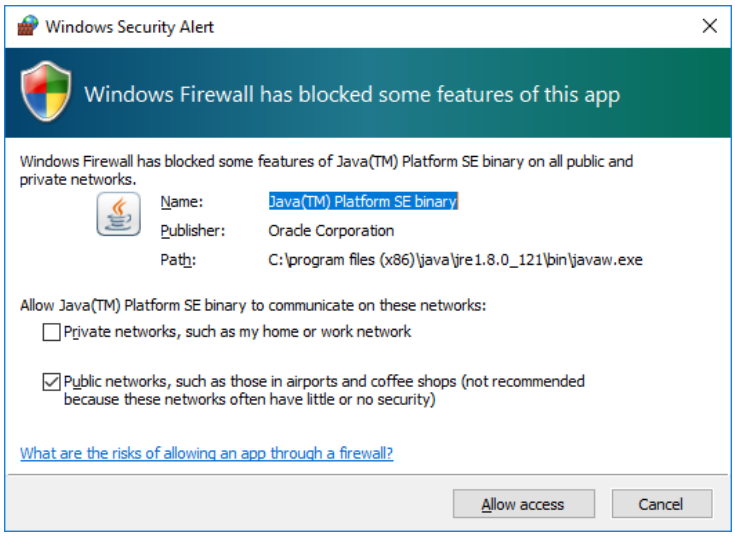


Figure 125 – Windows Initial Firewall - UniFi

The wording and default selections seem backwards to me. I reversed the selections and pressed “Allow access”. See Figure 126 – Windows My Firewall Settings - UniFi.

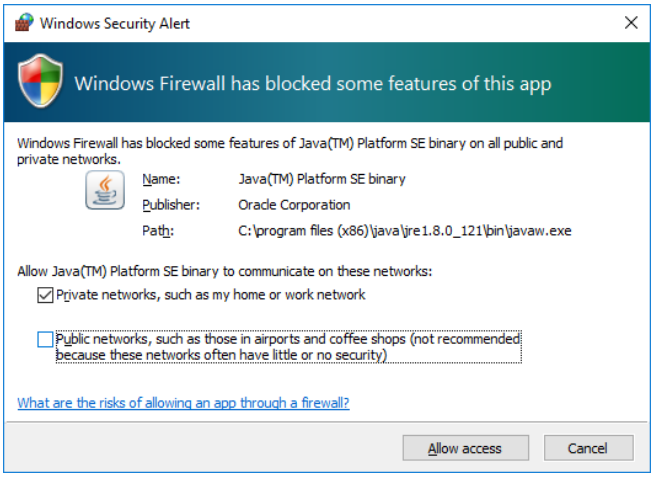


Figure 126 – Windows My Firewall Settings - UniFi

72. Initial Setup of the UniFi Software

To start the UniFi Software, perform one of the following:

"Launch a Browser to Manage the Network" button	(PC Install)
https://localhost:8443/manage	(PC Install)
https://localhost:8443/	(PC Install)
https://<UniFi_Controller_IP_Address_Here>:8443	(Replace <…> with the real IP address)

URL's go into a browser. If using a Raspberry Pi, don't use a browser which is local to the Raspberry Pi, as you may not have enough memory available to run both the UniFi Software and a browser at the same time.

Most of the following screenshots are portions of the full browser screen.

Select your country, time zone, and enable Auto Backup", then press Next. See Figure 127 – UniFi Setup Wizard.

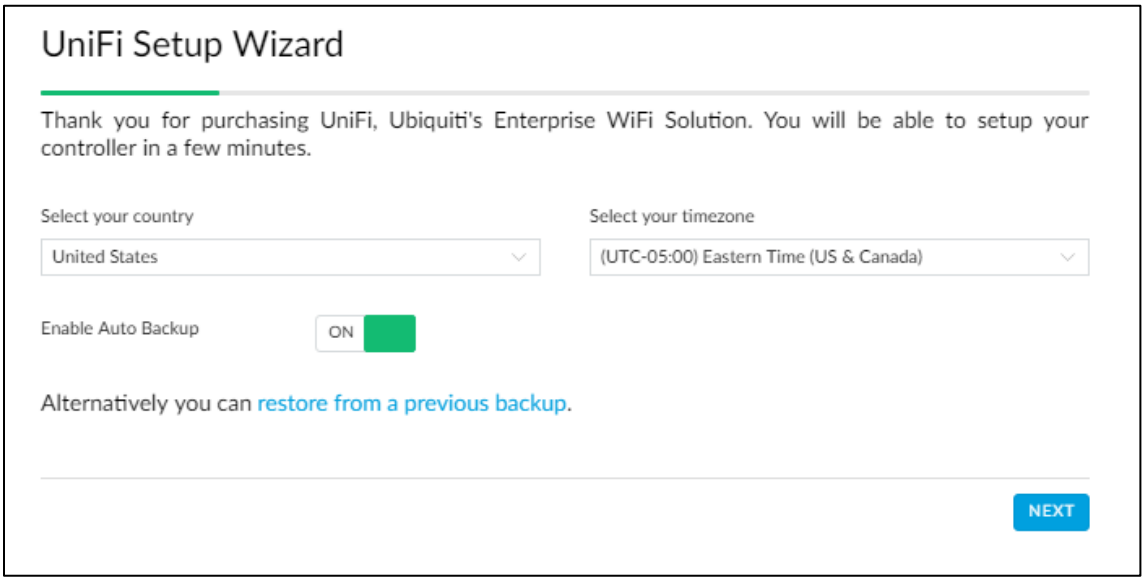


Figure 127 – UniFi Setup Wizard

Your Ubiquiti Access Point should show up in the list. Check it and then press Next. See Figure 128 – UniFi Configure Devices.

Figure 128 – UniFi Configure Devices

You will see the initial configure Wi-Fi screen. See Figure 129 – UniFi Initial Configure Wi-Fi.

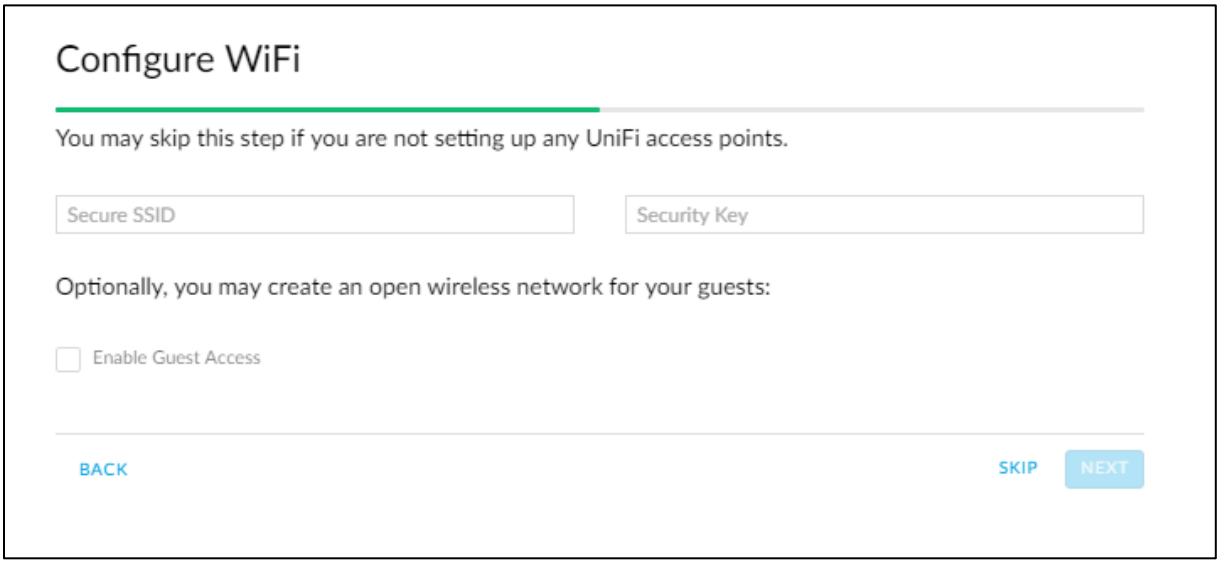


Figure 129 – UniFi Initial Configure Wi-Fi

Fill in your main network's SSID and your Wi-Fi password. I used the name "HomeNet "for this guide. This is the Wi-Fi network that most of your computers, tablets, and cell phones will connect to. Leave the Enable Guest Network as UNCHECKED, and then press Next. See Figure 130 – UniFi Configure Wi-Fi SSID.

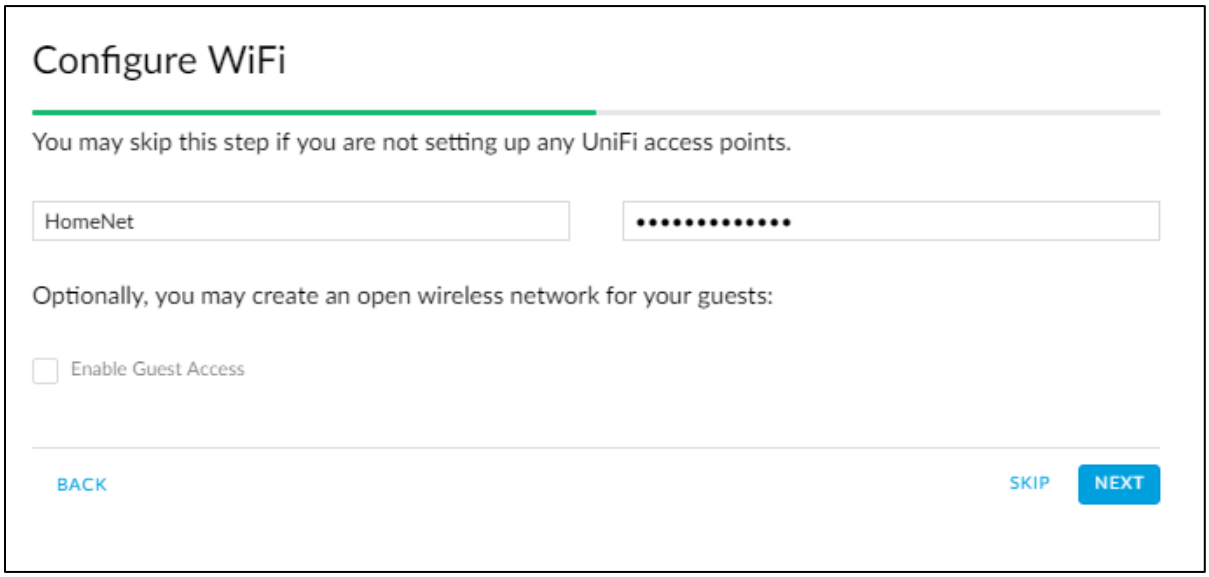


Figure 130 – UniFi Configure Wi-Fi SSID

To access this UniFi software later on, fill in the following information:

Admin Name
Admin Email
Password

You will want to write these down and/or put them in your password safe. The email address is used for password recovery. When finished, press Next. See Figure 131 – UniFi Controller Access.

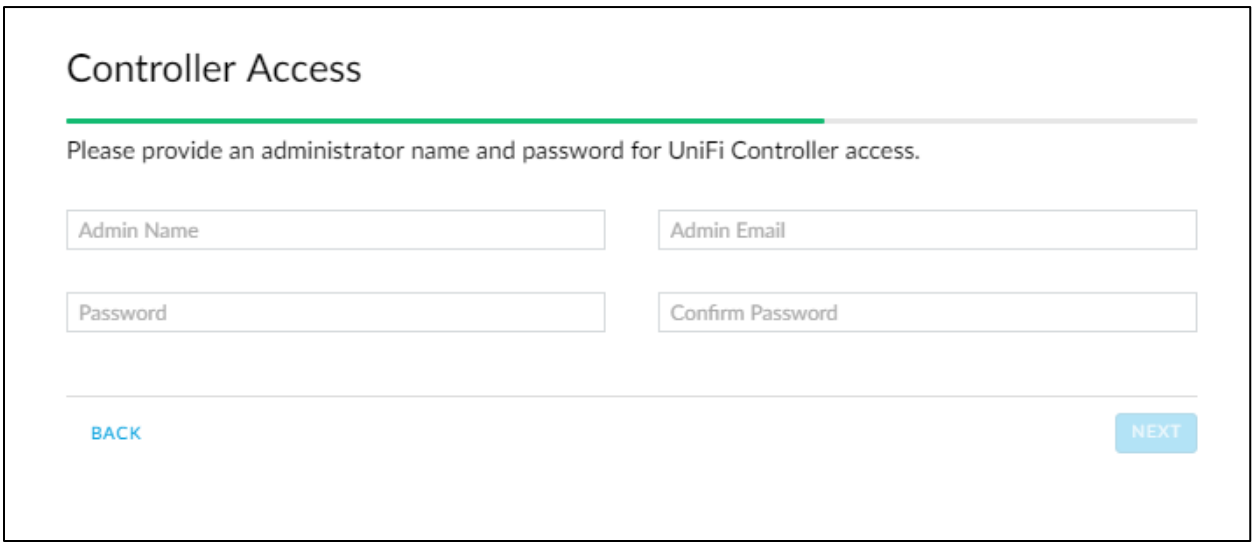


Figure 131 – UniFi Controller Access

Since I am not using Cloud Access, I pressed Skip. See Figure 132 – UniFi Cloud Access.

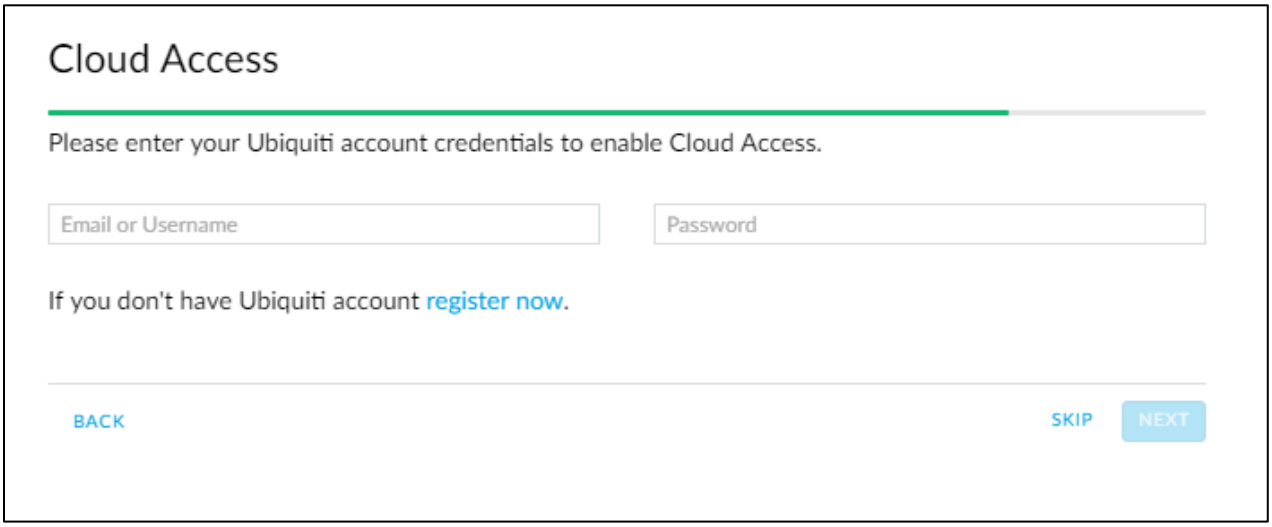


Figure 132 – UniFi Cloud Access

You are then asked to confirm the above information. If it is correct, press Finish. See Figure 133 – UniFi Confirm Setup.

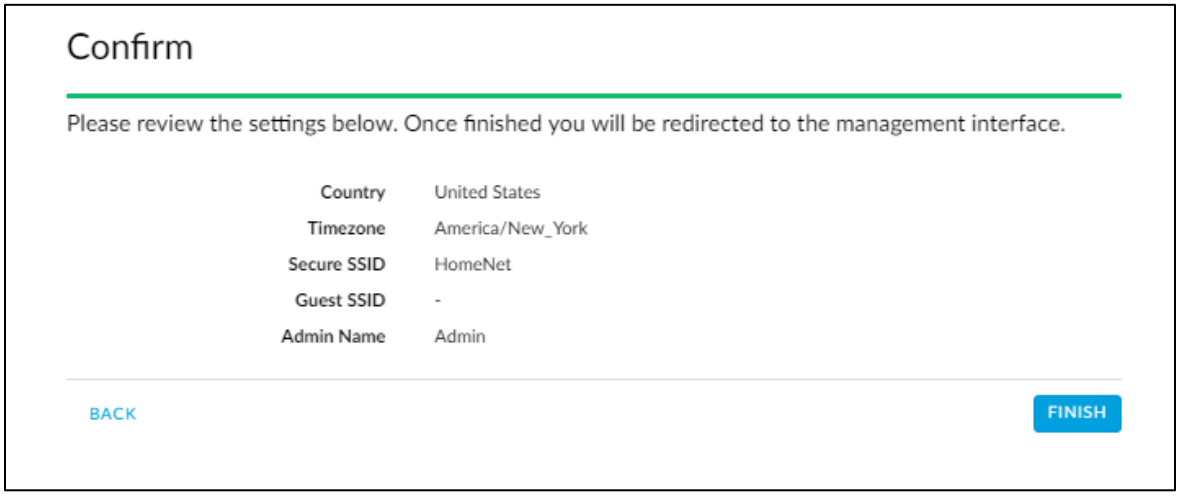


Figure 133 – UniFi Confirm Setup

73. Login to the UniFi Software

You will be asked to login to the UniFi Software. See Figure 134 – UniFi Login. Use your newly created credentials that were entered at Figure 131 – UniFi Controller Access.

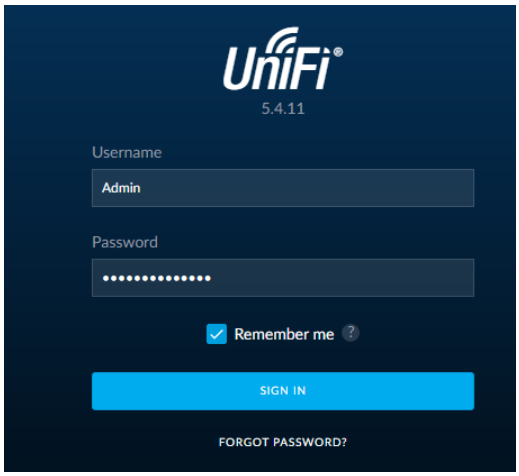


Figure 134 – UniFi Login

You will land on the Dashboard page. See Figure 135 – Initial UniFi Dashboard Page

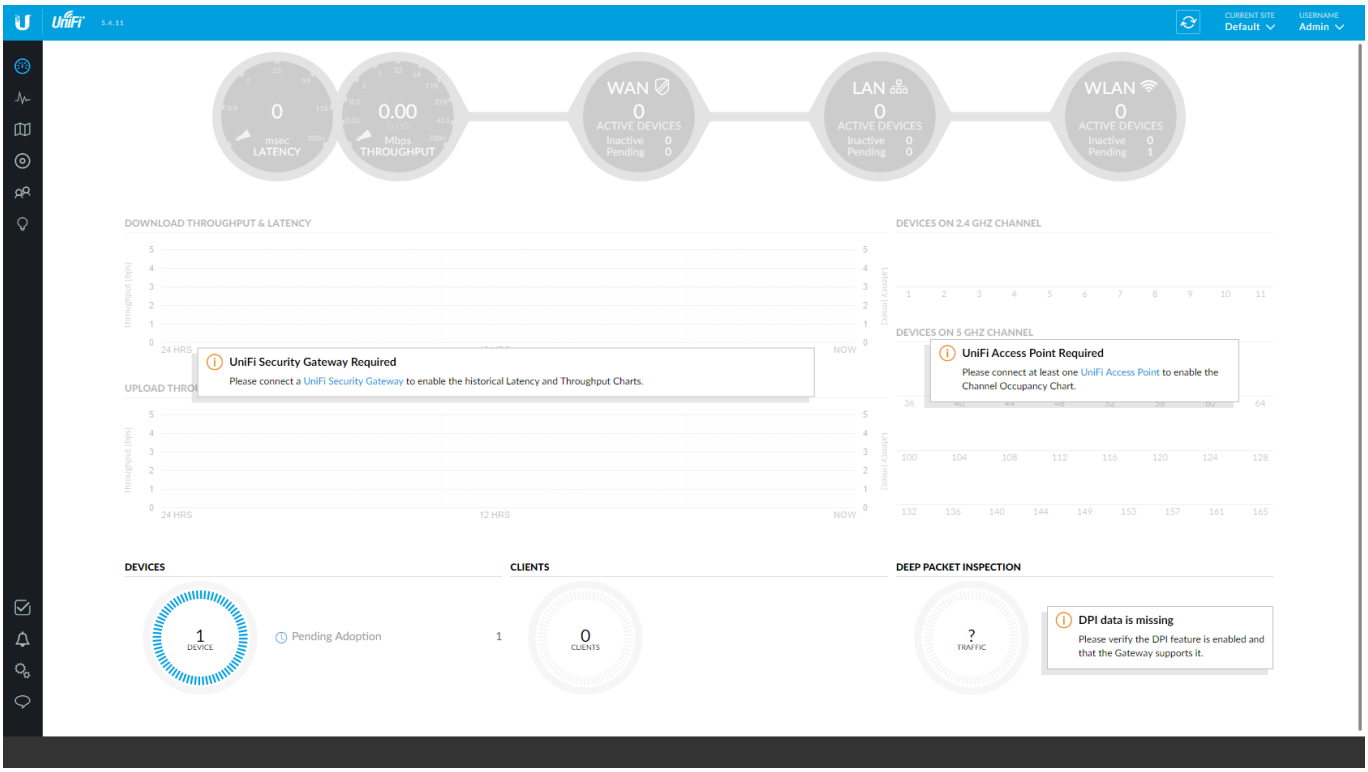


Figure 135 – Initial UniFi Dashboard Page

From the upper left hand side choose Devices. See Figure 136 – UniFi Devices Button.

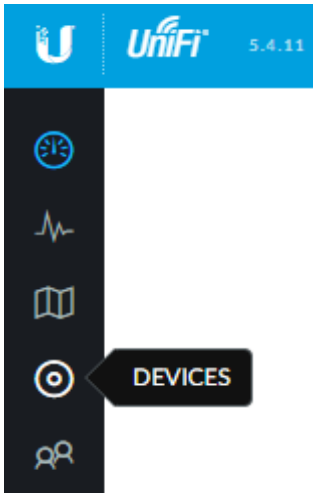


Figure 136 – UniFi Devices Button

74. UniFi Devices

You will see the devices page, and the Access Point should be Pending Adoption. See Figure 137 – Initial UniFi Device Screen. Note that this screenshot / figure was cut into two pieces and folded into one image.

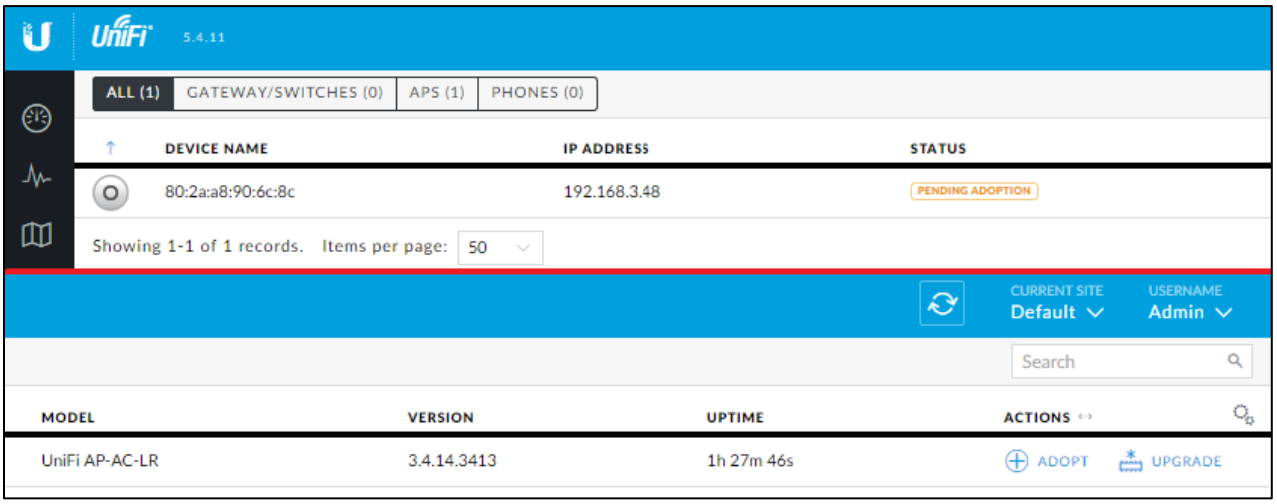


Figure 137 – Initial UniFi Device Screen

[First see version notes in section 68 - Ubiquiti AP-AC-LR Access Point Setup] Press the Upgrade button on the right side of the device line. Reference Figure 137 – Initial UniFi Device Screen. You will be presented with an upgrade confirmation dialog. Press Confirm. See Figure 138 – UniFi - Upgrade Access Point

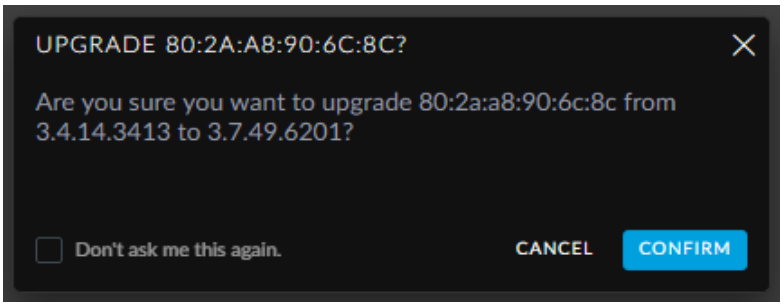


Figure 138 – UniFi - Upgrade Access Point

You should see acknowledgement of the upgrade. See Figure 139 – UniFi – Upgrading.

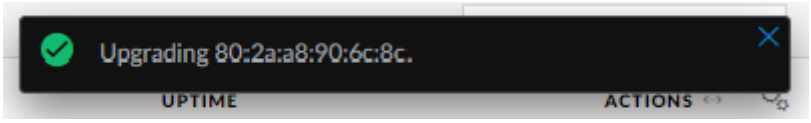


Figure 139 – UniFi – Upgrading Access Point

When the upgrade is finished, press the Adopt button on the right side of the device line. Reference Figure 137 – Initial UniFi Device Screen. You should see acknowledgement of the Adoption. SeeFigure 140 – UniFi – Adopting.

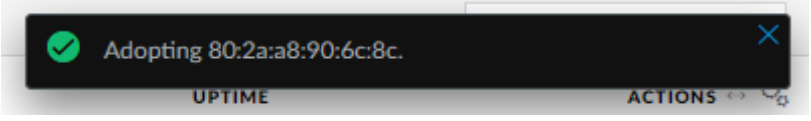


Figure 140 – UniFi – Adopting Access Point

Your device should now say Connected. The buttons on the right now allow you to locate, restart, and upgrade the Access Point. See Figure 141 – UniFi Access Point Connected. Note that this screenshot / figure was cut into two pieces and folded into one image.

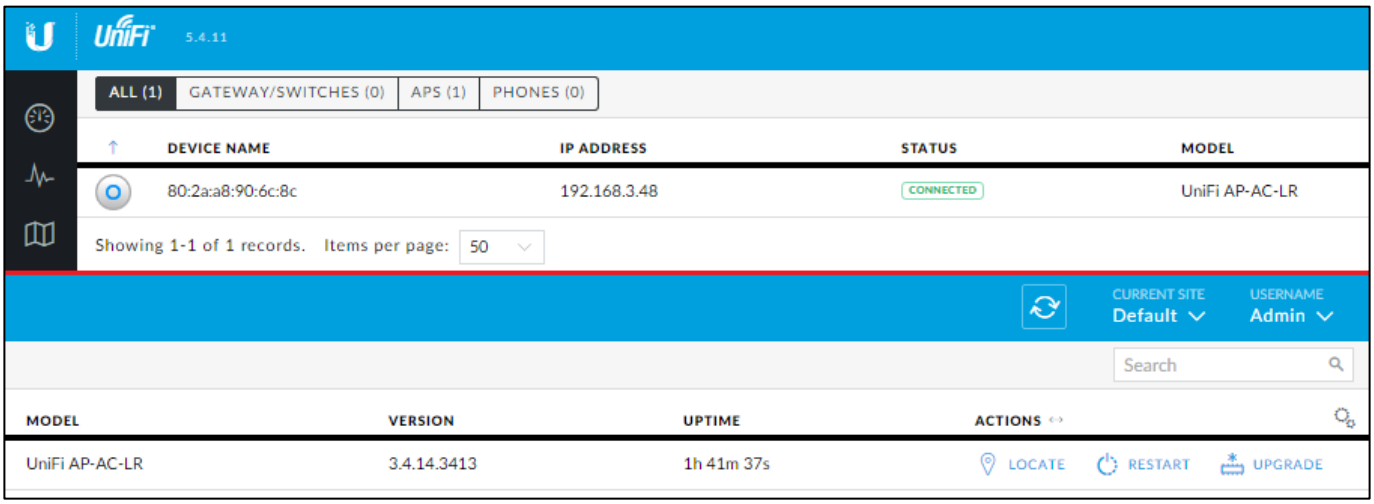


Figure 141 – UniFi Access Point Connected

Find the Settings button, near the lower left side of the screen, and press it. See Figure 142 – Settings Button

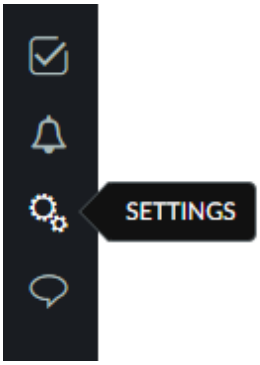


Figure 142 – Settings Button

75. UniFi Settings

You should see the Site Tab of the Settings page.

Uncheck: Automatically upgrade firmware

Uncheck: Enable connectivity monitor and wireless uplink (only if all APs are hardwired)

Ensure that you specify and save AP login credentials under 'Device Authentication', so that you can recover your APs if there are any future problems.

Press Apply Changes. See Figure 143 – UniFi Site Configuration.

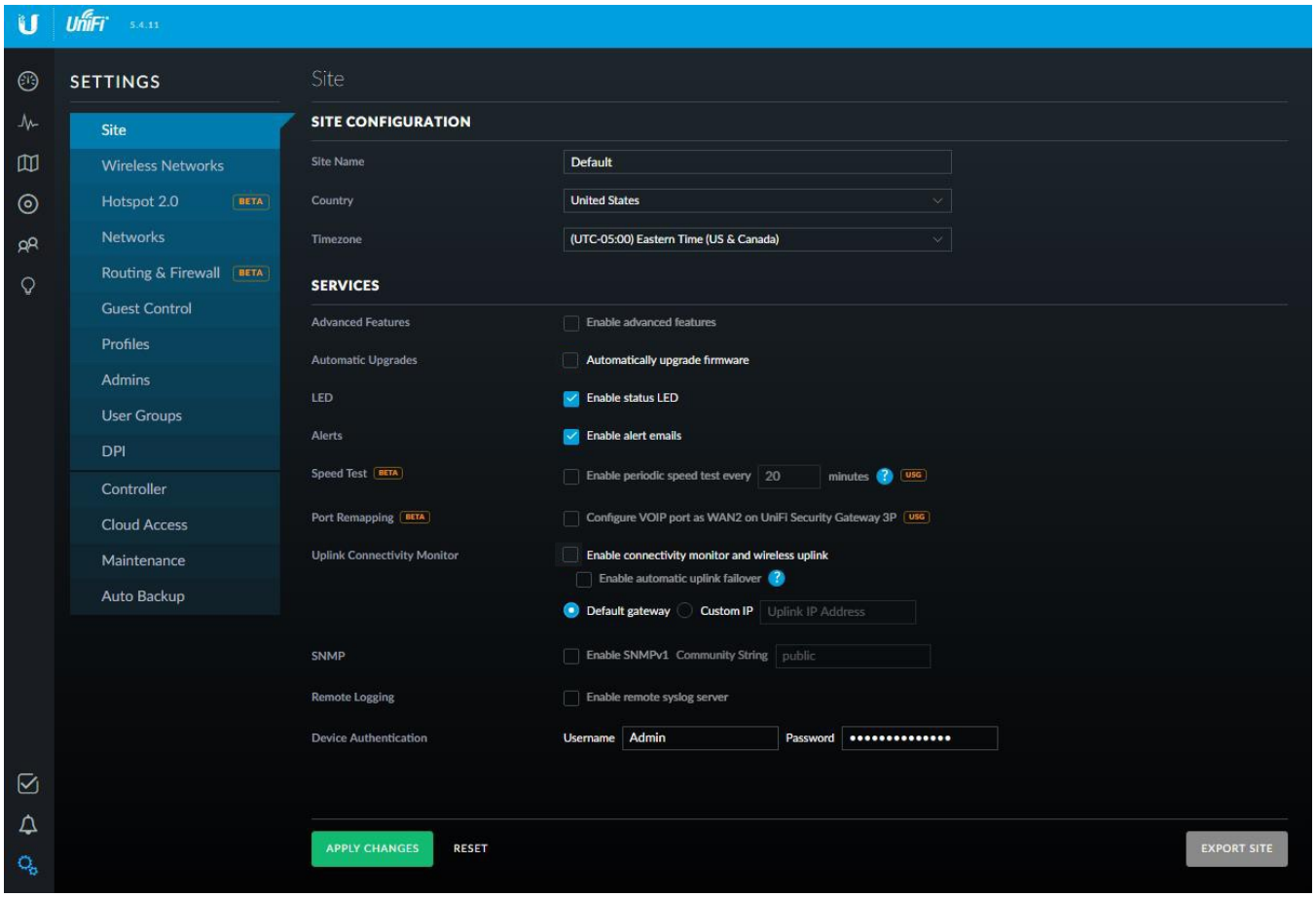


Figure 143 – UniFi Site Configuration

Click on the Guest Control tab. Under the Access Control section, add:

192.168.3.0/24

to Pre-Authorization Access, then press Apply Changes. See Figure 144 –Unifi Guest Control.

This will allow devices on a Wi-Fi Network designated as using "Guest Policy to (respond to) communications from the Home Network. Remember that the EdgeRouter has firewall rules prohibiting Guest network devices from directly initiating communications with the Home Network. This allows Guest devices to RESPOND to Home Network initiated conversations.

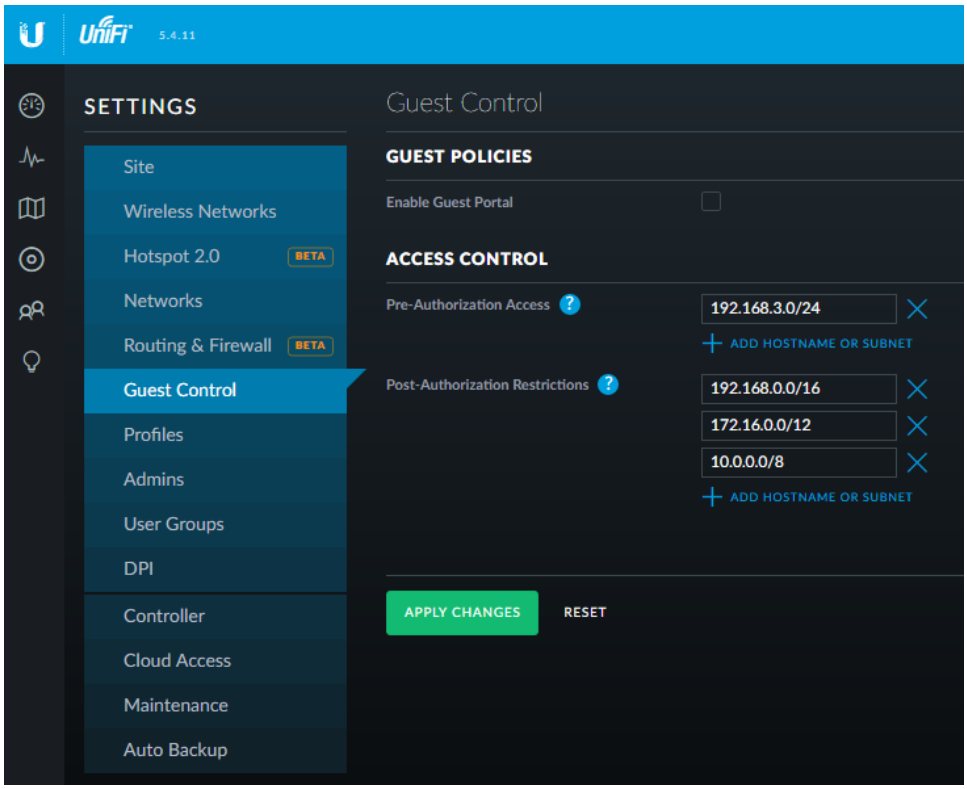


Figure 144 –Unifi Guest Control

Click on the User Groups tab, and then press Create New User Group. See Figure 145 – UniFi Initial User Groups.

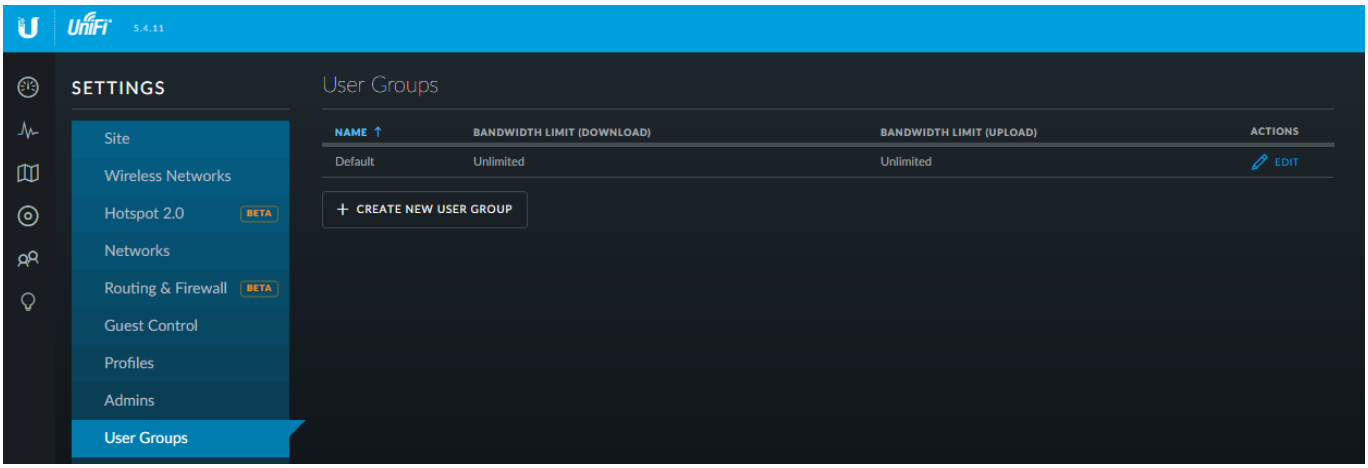


Figure 145 – UniFi Initial User Groups

The following settings allow the Access Point to limit the bandwidth used by users within the guest networks. You may choose to enter different limit values and/or leave either or both of the settings as unchecked. Unchecked is unlimited. The values used here are:

download speed is limited to 10 Mbps
upload speed is limited to 2 Mbps.

I believe that the limits are per user, not per network. Reference:
https://community.ubnt.com/t5/UniFi-Wireless/User-Group-Bandwidth-limit-group-or-user/td-p/1828127

To use the values that are in this guide, complete the form as follows:

Name	GuestGroup	
Bandwidth Limit (Download)	Checked	10000
Bandwidth Limit (Upload)	Checked	2000

then press Save. See Figure 146 – UniFi Guest Group

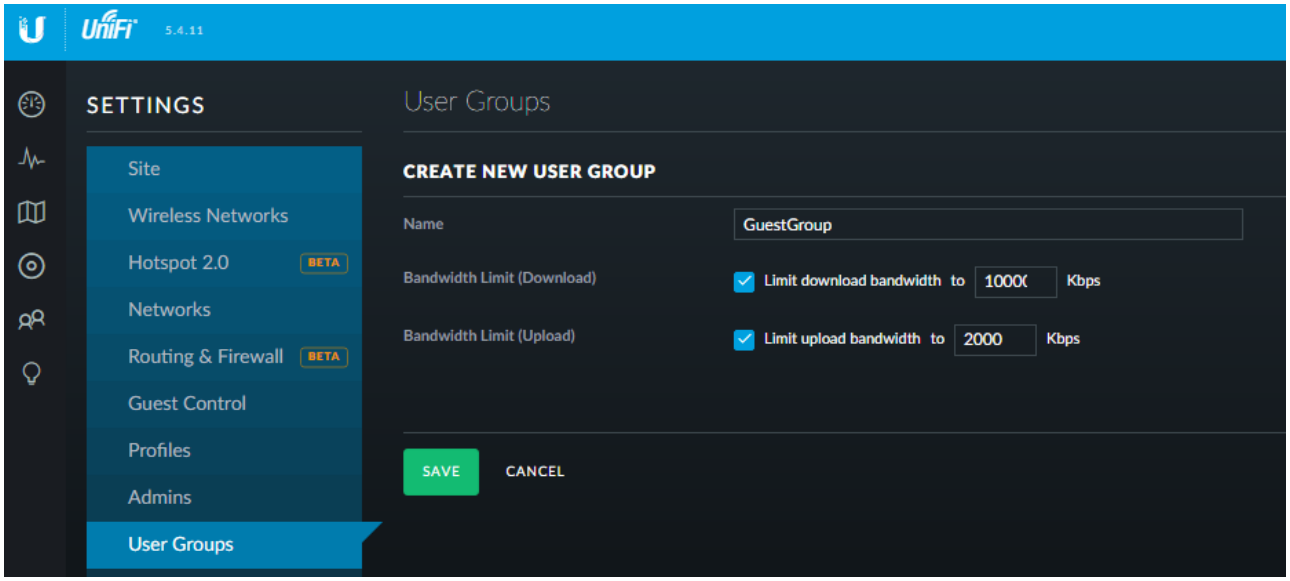


Figure 146 – UniFi Guest Group

You should now see the newly created group. See Figure 147 – UniFi New User Groups.

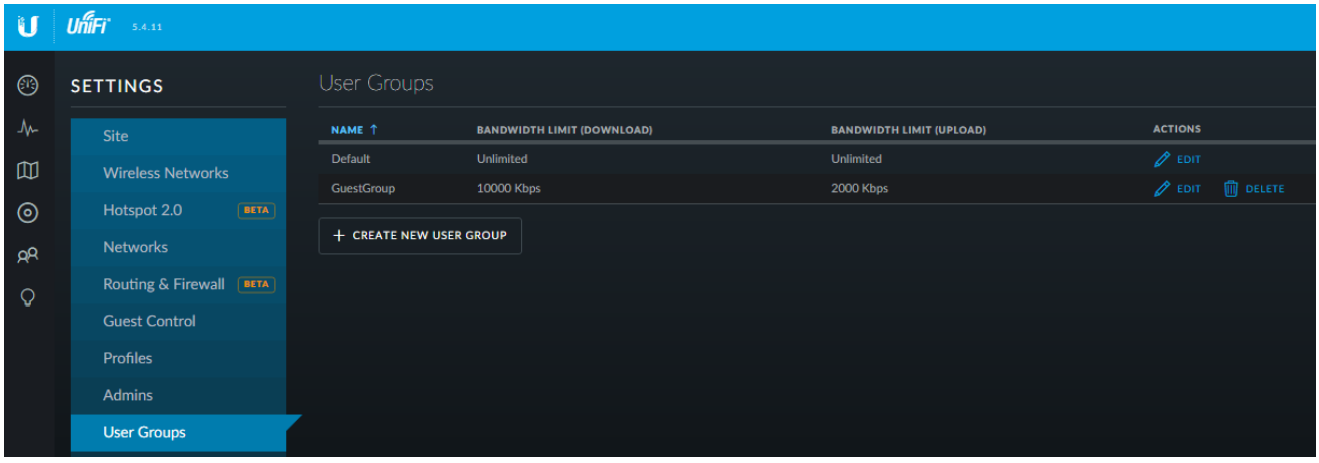


Figure 147 – UniFi New User Groups

Additional Link:
https://help.ui.com/hc/en-us/articles/204911354-UniFi-How-to-Set-Traffic-Bandwidth-Limits

2022 Note: Newer versions of UniFi might need the following “Settings -> Networks” setup step(s) performed. See Figure 148 – Newer UniFi Networks Setup.

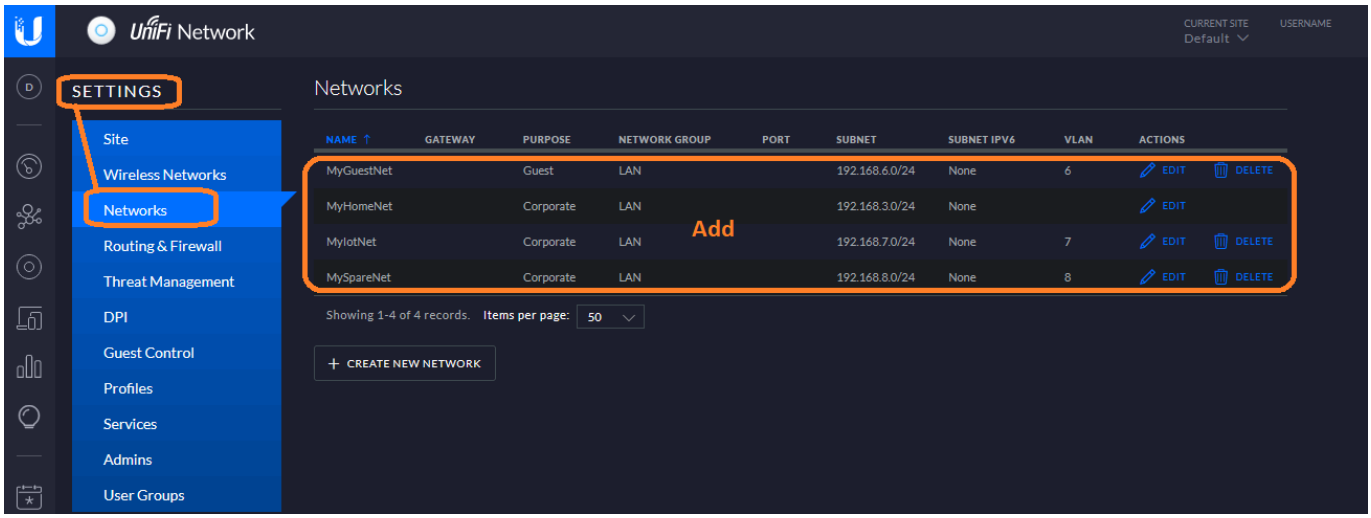


Figure 148 – Newer UniFi Networks Setup

Click on the Wireless Networks tab, you should see the Home Network that was setup earlier. See Figure 149 – UniFi Wireless Network Setup. Click on Create New Wireless Network button

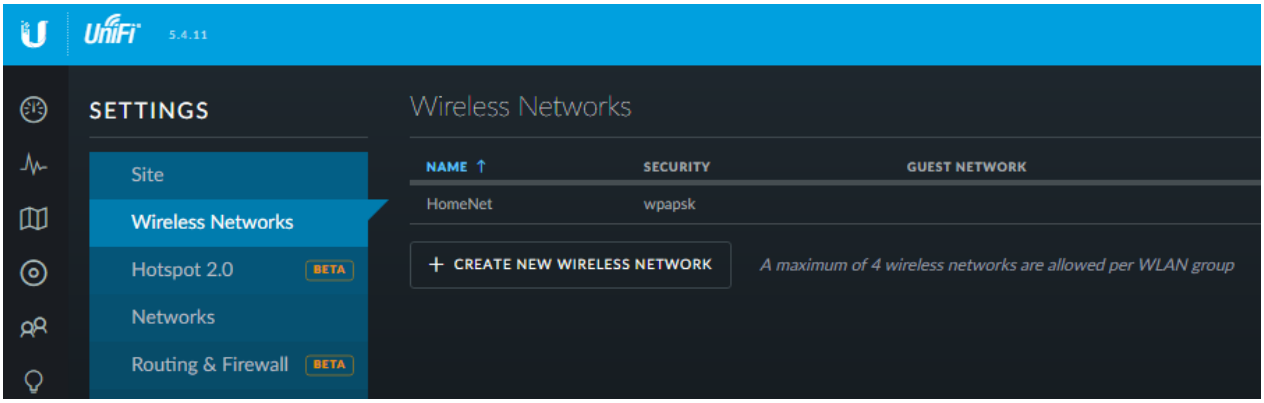


Figure 149 – UniFi Wireless Network Setup

Click on Create New Wireless Network button. You may need to open up “Advanced Options”. You will be presented with the Create New Wireless Network dialog. See Figure 150 – UniFi Create New Wireless Network.

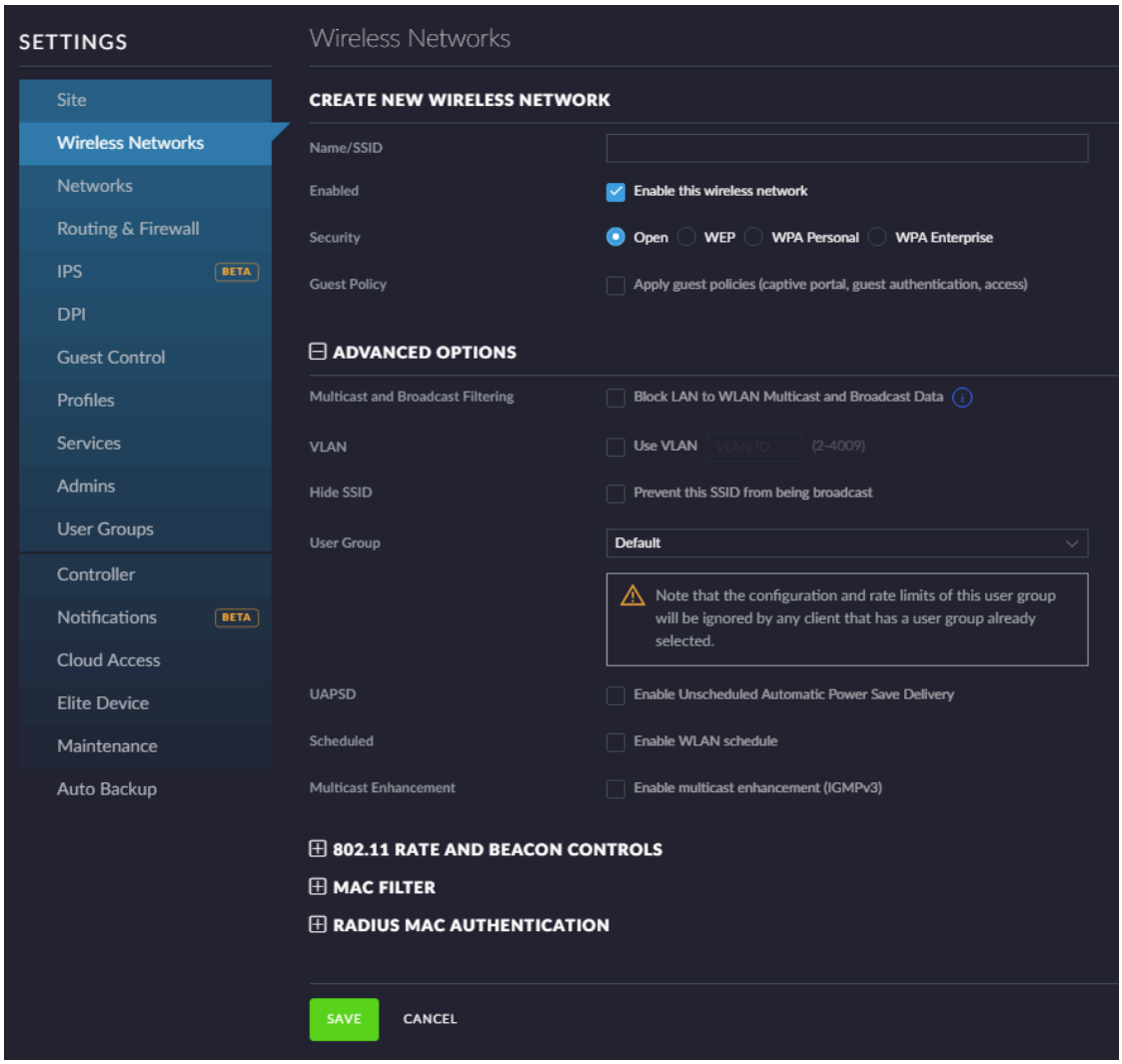


Figure 150 – UniFi Create New Wireless Network

Note that any wireless network which has checked the “Guest Policy” checkbox will isolate ALL devices from every other device on that wireless network.

Many people do have (groups of) IOT devices which need to communicate with each other to function. Examples are multiple Amazon devices, video cameras and their (storage) servers, etc. Newer versions of the UniFi Software have an additional checkbox “Multicast and Broadcast Filtering” (not shown), which also needs to be unchecked to enable the Wi-Fi clients to communicate with each other. See also related sections: 96 - Multicast DNS and 94 - What devices should be placed on which Network?.

Maybe a good compromise for security vs convenience is to:

Enable “Guest Policy” and Enable Broadcast Filtering for the Wi-Fi Guest Network and
Disable “Guest Policy” and Disable Broadcast Filtering for the Wi-Fi IOT Network.

You will need to choose these settings for yourself, based upon your own installed IOT devices.

In the following Wi-Fi setups, I don't know what to do with the "Multicast Enhancement" checkbox. Mine is Un-Checked, maybe because it was setup so long ago. Here are some References:

https://help.ubnt.com/hc/en-us/articles/115001529267-UniFi-Managing-Broadcast-Traffic

https://community.ubnt.com/t5/airOS-Software-Configuration/quot-Multicast-Enhancement-quot-checkbox/td-p/550452

https://community.ui.com/t5/UniFi-Wireless/Enable-multicast-enhancement-IGMPv3-feature/td-p/2249142

You can change the following settings as suites you. Change / Enter the following information:

Name/SSID	GuestWifi		
Security	WPA Personal		
Security Key	<Enter your own password for the guest Wi-Fi network >		
Guest Policy	CHECKED	Apply guest policies	
Multicast … Filtering	CHECKED	Block LAN to WLAN Multicast … Data	
VLAN	CHECKED	Use VLAN	6
WPA Mode	WPA2 Only	Encryption	AES/CCMP Only
User Group	GuestGroup		

Press Save. See Figure 151 – UniFi Guest Wif.

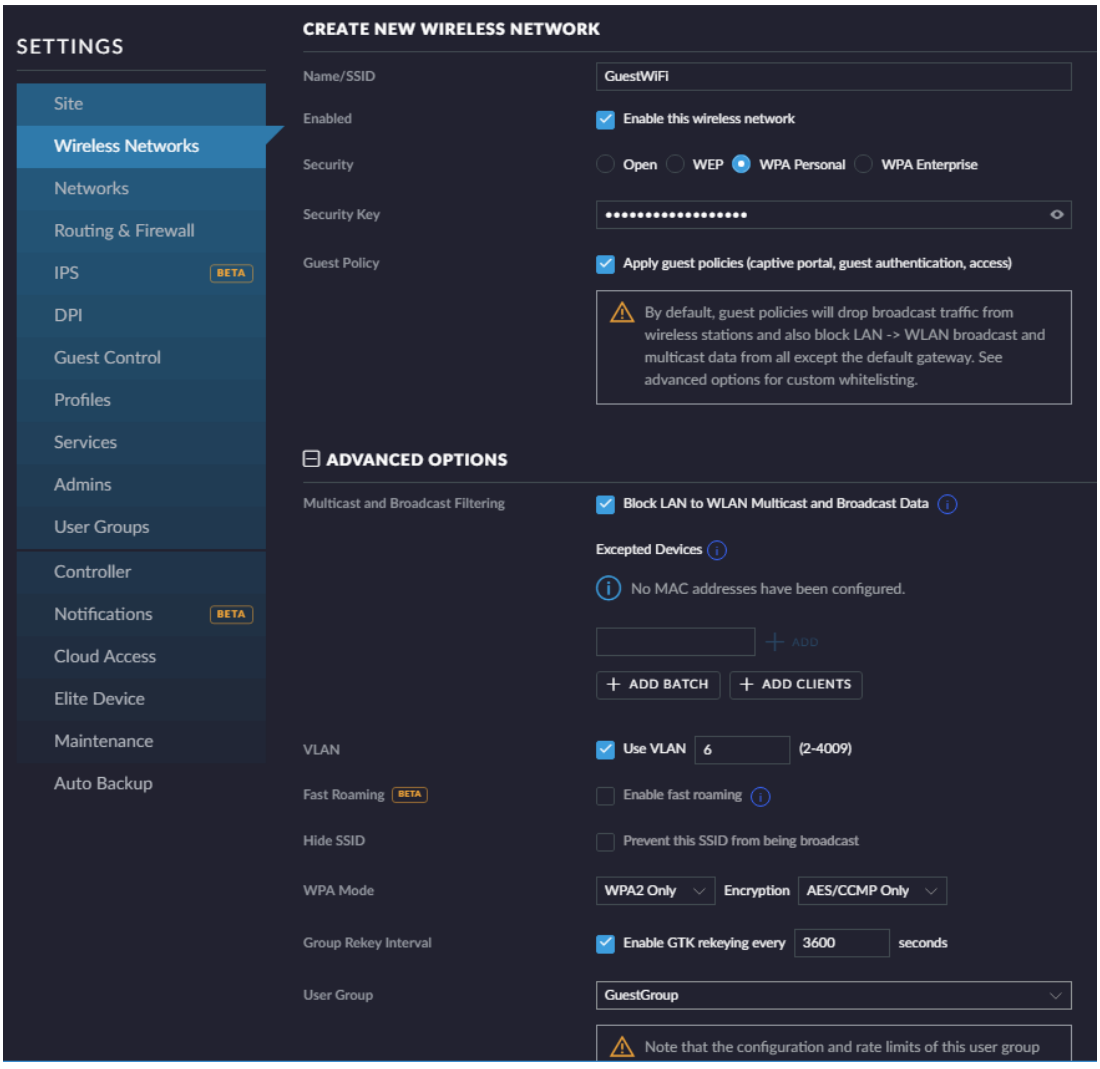


Figure 151 – UniFi Guest Wif

Click on Create New Wireless Network button.

You can change the following settings as suites you. Change / Enter the following information:

Name/SSID	IotWifi		
Security	WPA Personal		
Security Key	<Enter your own password for the iot Wi-Fi network >		
Guest Policy	Un-Checked	Apply guest policies	
Multicast … Filtering	Un-Checked	Block LAN to WLAN Multicast … Data	
VLAN	CHECKED	Use VLAN	7
WPA Mode	WPA2 Only	Encryption	AES/CCMP Only
User Group	Default		

Press Save. SeeFigure 152 – UniFi Iot Wi-Fi.

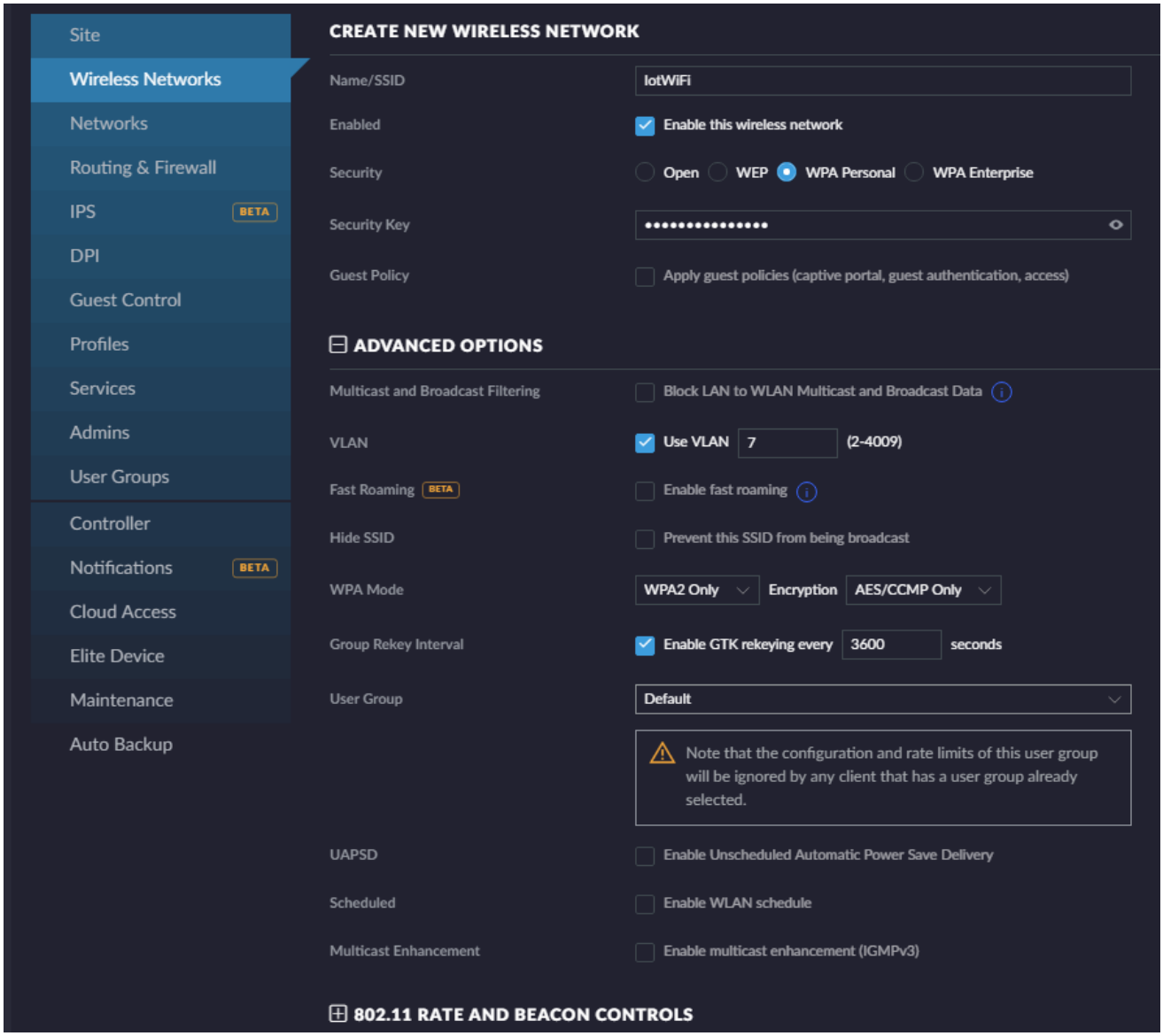


Figure 152 – UniFi Iot Wi-Fi

You should now have the following networks. Note that:

GuestWifi	Checked as Guest	VLAN 6
HomeNet	(Unchecked Guest)	(no VLAN)
IotWifi	(Unchecked Guest)	VLAN 7

See Figure 153 – UniFi Three Wi--Fi Networks.

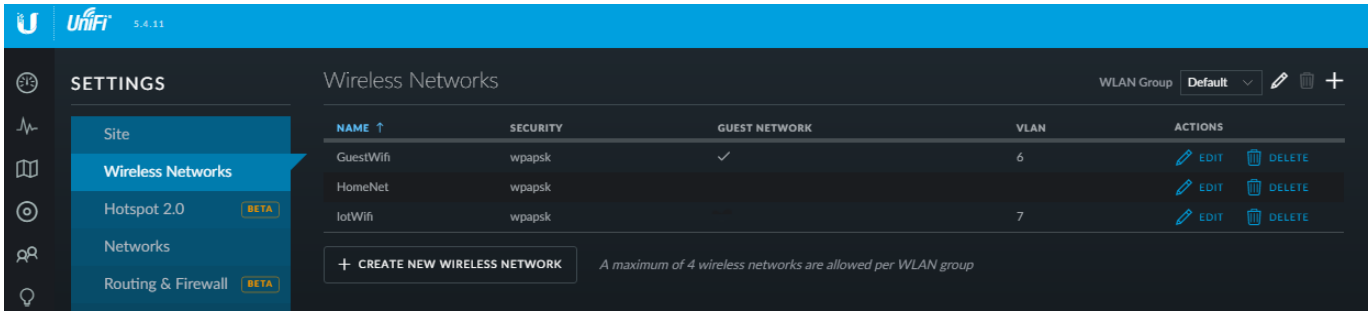


Figure 153 – UniFi Three Wi--Fi Networks

If you want to implement another "Spare" Wi-Fi network, you would do that now, following the above steps, but instead specifying:

VLAN	CHECKED	Use VLAN	8.

Click on the DPI tab, and set:

Enable Deep Packet Inspection (DPI)	On

Press Apply Changes. See Figure 154 – UniFi Deep Packet Inspection

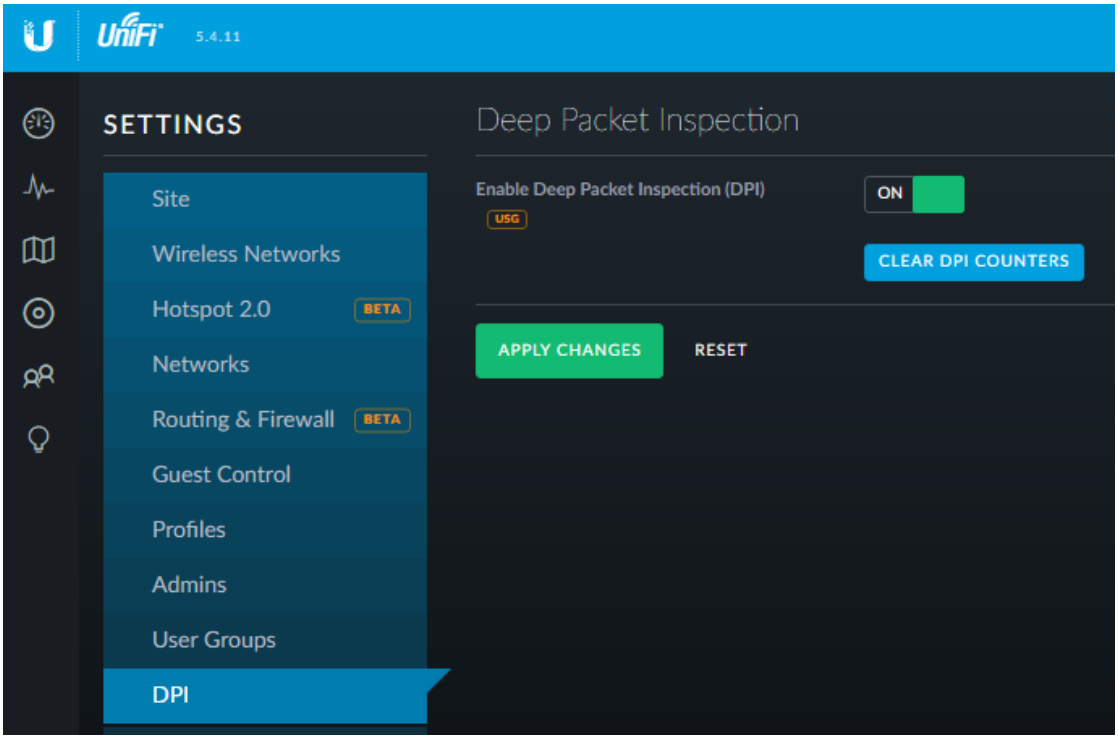


Figure 154 – UniFi Deep Packet Inspection

Return to the Dashboard screen by pressing the Dashboard button. See Figure 155 – UniFi Dashboard Button.

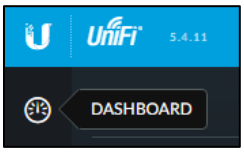


Figure 155 – UniFi Dashboard Button

In the upper right part of the dashboard screen is the Open Properties button. Press the button. See Figure 156 – UniFi Open Properties Button

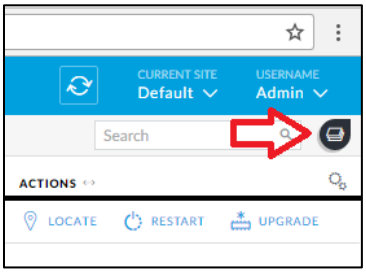


Figure 156 – UniFi Open Properties Button

These are the Properties of the Access Point. There are some nice settings in here. See Figure 157 – UniFi Access Point Properties.

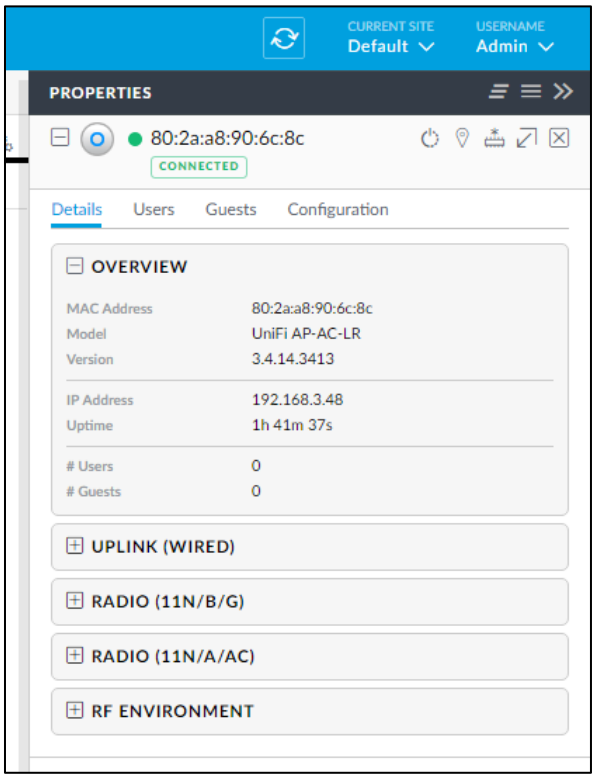


Figure 157 – UniFi Access Point Properties.

76. UniFi WLAN Groups

This section is optional. I have setup, and am managing a couple of Access Points for other people / installations, and do not want all these installations to be using the same set of SSIDs and passwords. A WLAN Group holds a group of settings for a single or for multiple Access Points. An Access Point can only belong to one WLAN Group.

I could have instead made multiple sites, one for each location.

To setup a (new) WLAN Group, first select the Settings button, near the lower left side of the screen, and press it. Reference Figure 142 – Settings Button. Next, click on the Wireless Networks tab, and (in the upper right) select the large "+" sign to the right of the WLAN Group text. See Figure 158 – UniFi Add WLAN Group.

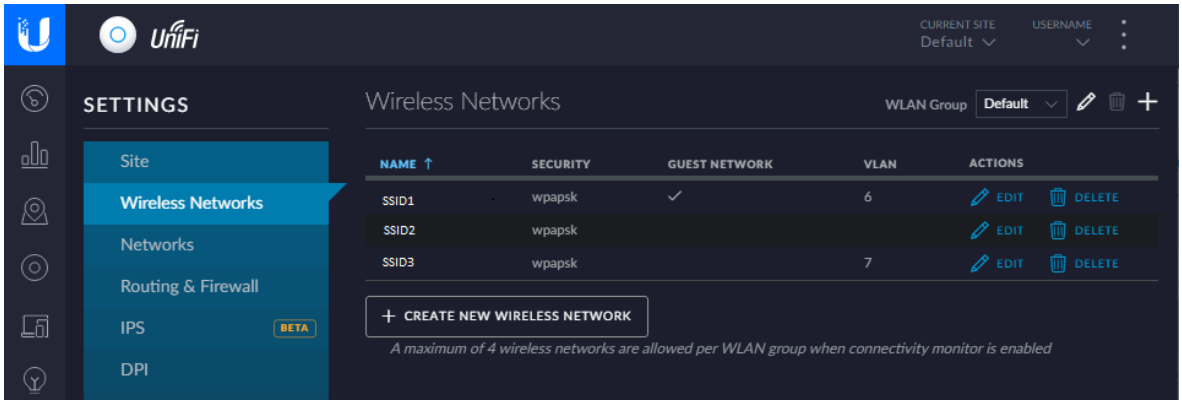


Figure 158 – UniFi Add WLAN Group.

You will now see a dialog allowing you to create a new WLAN Group. Fill in the following information:

Name	<Name of new WLAN Group>
Duplicate WLANs	Check this if you want to copy an existing WLAN Group to this new group

Press Save when done. See Figure 159 – UniFi Create New WLAN Group.

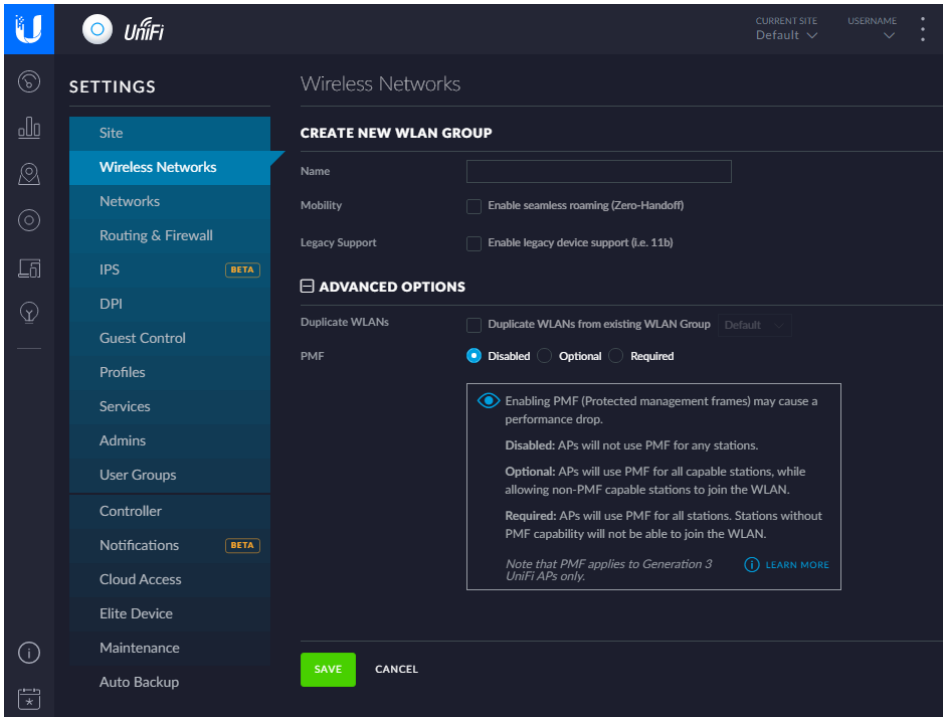


Figure 159 – UniFi Create New WLAN Group.

Select the new WLAN Group you just created, and edit all the group's items as desired. See Figure 160 – UniFi Select Newly Created WLAN Group.

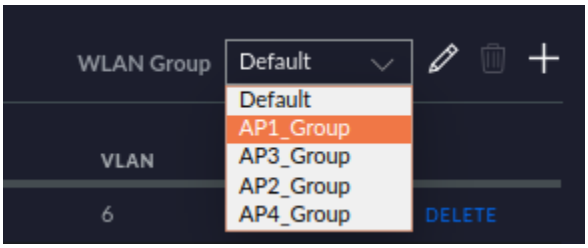


Figure 160 – UniFi Select Newly Created WLAN Group.

Now we need to select a particular Access Point, and set it to belong-to / have-it-use the newly defined WLAN group. Select:

1. Devices.
2. <Your Access Point>.
3. Configure Tab.
4. Expand the WLANS Item.
5. For the 2.4 GHz WLAN Group, select which group you want (Shown selecting "AP1_Group".)

5A. Queue the changes (not shown)

6. For the 5 GHz WLAN Group, select the same group as was chosen for 2.4GHz WLAN Group.

6A. Queue the changes (not shown)

6B. Apply the changes (not shown)

See Figure 161 – UniFi Utilize a WLAN Group.

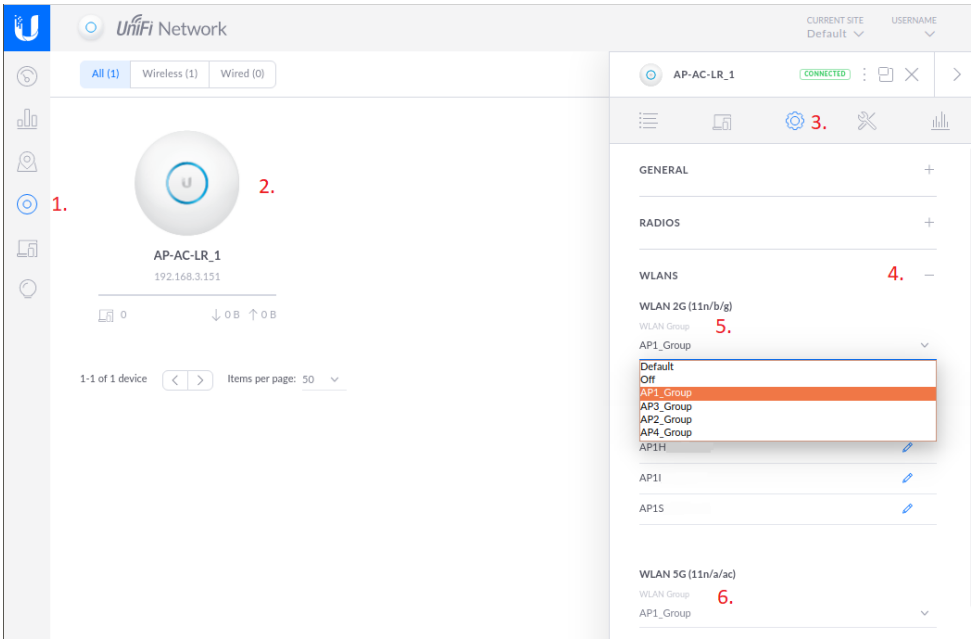


Figure 161 – UniFi Utilize a WLAN Group.

References:

https://help.ubnt.com/hc/en-us/articles/205204020-UniFi-WLAN-Groups

An Alternate Method: https://community.ui.com/questions/Need-different-SSIDs-for-each-Access-Point-/133c3eb7-7730-40fa-98e6-695d8a92aa8e

77. Setting UniFi / Access Point's SSIDs, Channels, and Power Levels

Your Access Point should now be running. You may have one or multiple Access Points in your installation. Everything that I have read, says that all Access Point(s), of a particular WLAN group, should be provisioned with the same set of SSIDs. This should allow for mobile client devices (Cellphones, tablets, etc.) to transition from one physical Access Point to another Access Point when they are roaming around this WLAN Group's installation area.

Now we come to channel assignments and power levels. This is only what I have read and/or done for my installation. Specifics may apply to U.S.A only, others countries will likely vary.

77.1 The best link on Wi-Fi details.

https://www.duckware.com/tech/wifi-in-the-us.html **Wow! Must See!**

77.2 Channel assignment for the 2.4GHz band.

Only choose channels 1 or 6 or 11. Fix the channel; don't set to "Auto". Set channel width to HT20. These three channels are the only clear / non-overlapping frequencies. See (borrowed from the Internet) Figure 162 – 2.4 GHz Channel Frequencies. I don't think that this figure's overlapping frequencies are shown exactly to scale. U.S.A. does not have channels 12, 13, 14.

I think that channel 1 can be "interfered with" by any of your neighbors using an overlapping channel of 2, 3, or 4. Similarly, I think that channel 11 can be "interfered with" by anyone nearby using an overlapping channel of 8, 9, or 10. I also contend that channel 6 should be used last, since it appears that channel 6 can be "interfered with" by anyone nearby using any overlapping channel(s) of 3, 4, 5, 7, 8, or 9.

If you have four or more Access Points, you will need to take your layout / geometry into account for the 2.4 GHz channel assignments, because at-least two Access Points will need to share the same channel.
A different alternative is to disable the 2.4GHz band on some of your (strategically placed) APs.

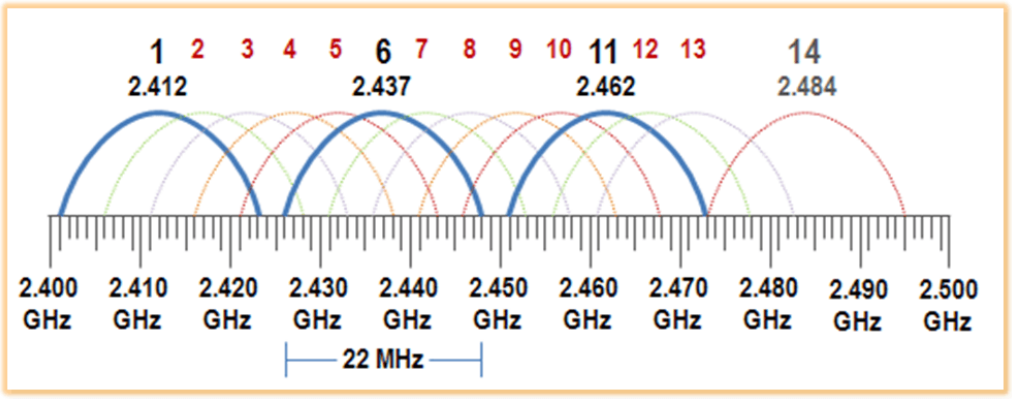


Figure 162 – 2.4 GHz Channel Frequencies.

How to set channel assignments is described in section 76.12.

77.3 Channel assignment for the 5GHz band.

Set channel width to VHT40. Only choose channels 36/44/149/157 (base frequencies). Alternately, you might see these channels listed as 38/46/151/159 (center frequencies). Fix the channel; don't set to "Auto". Try to avoid DFS channels, but never use 120 - 128. When using a VHT40 width, which is double that of VHT20, use only every other VHT20 channel in nearby Access Points or you will be interfering with yourself, similar to what is described in the above 2.4GHz section. See (borrowed from the Internet) Figure 163 – 5 GHz Channel Frequencies Number One. Also see (borrowed from the Internet) Figure 164 – 5 GHz Channel Frequencies Number Two.

If the above settings work for your installation, you might instead try setting the width to VHT80 and the channel to (36 base) 42 center or to (149 base) 155 center. Using VHT80 achieves a higher 5G data rate, at the potential cost of being susceptible to more interference. Similarly, if the VHT40 settings are not working for your installation, you might need to drop-back to 5 GHz VHT20 widths / channels.

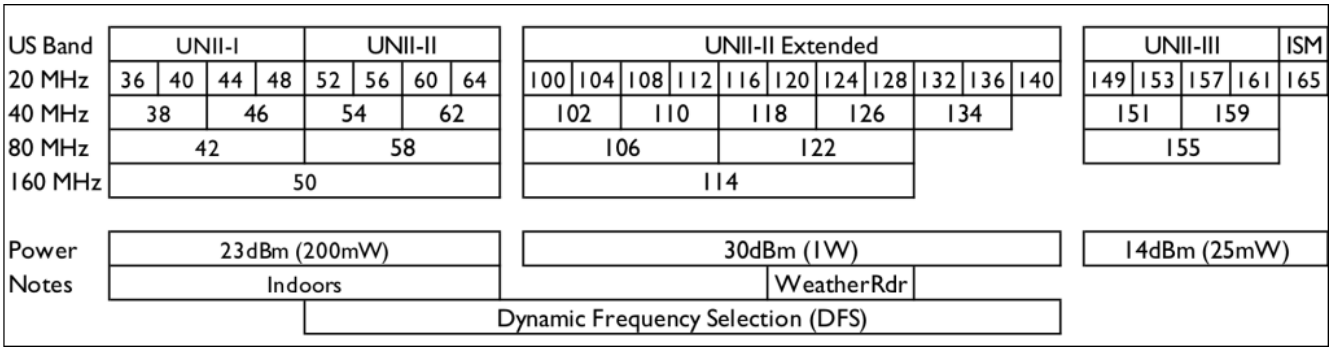


Figure 163 – 5 GHz Channel Frequencies Number One.

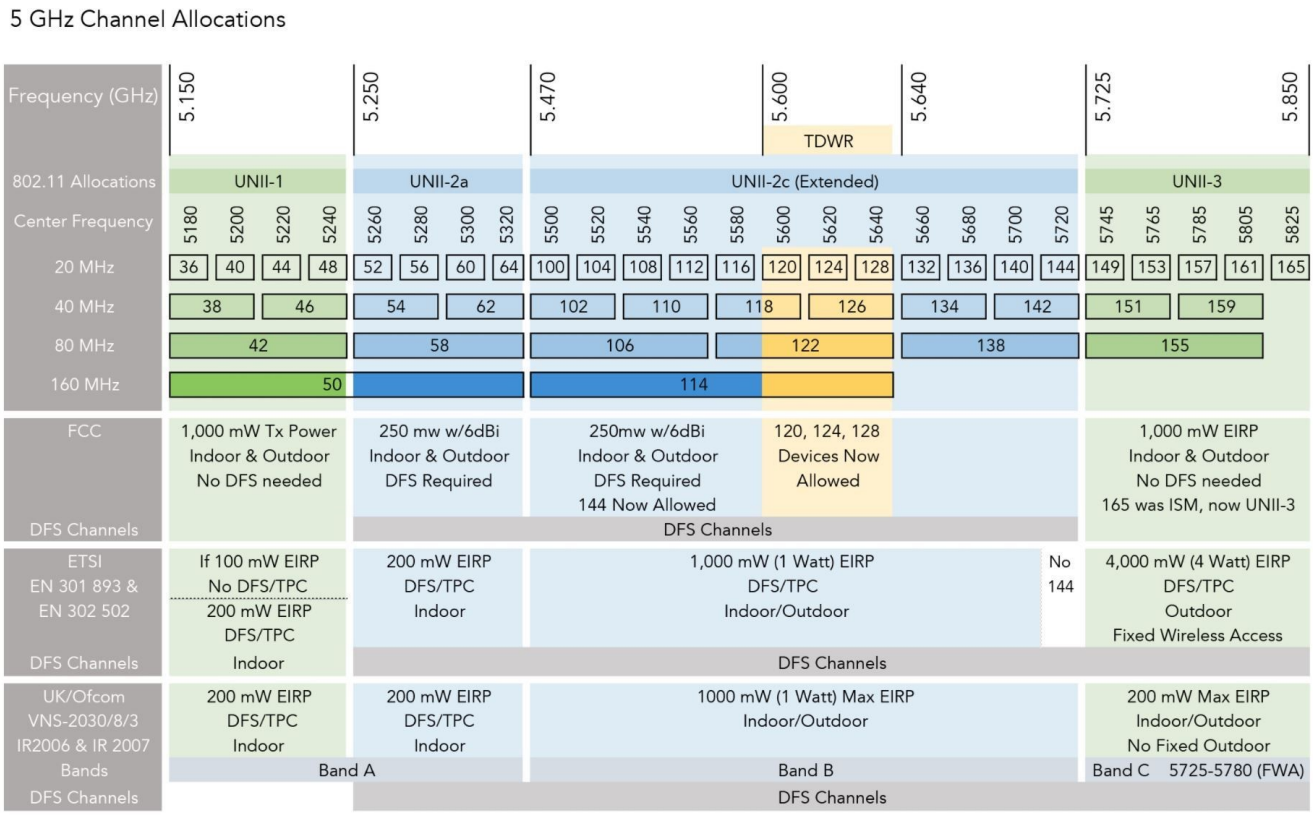


Figure 164 – 5 GHz Channel Frequencies Number Two.

@lcire1
DFS Channel Availability Check
When support for DFS is enabled, it will be necessary for WiFi access points to verify that any radar in proximity is not using DFS frequencies. This process is called Channel Availability Check, and it's executed during the boot process of an access point (AP) as well as during its normal operations.
If the AP detects that a radar is using a particular DFS channel, then it will exclude that channel from the list of available channels. This state will last for 30 minutes, after which the AP will check again if the channel can be used for WiFi transmissions.
The Channel Availability Check performed during the boot process can take anywhere between 1 and 10 minutes, depending on which country you're in. For this reason, DFS channels are not immediately available when an AP boots.
As I just wrote, if the AP detects during the boot process that a DFS channel is currently used by a radar, it will mark it as non-available and exclude it from the list of available channels. This process will have little impact on the WiFi clients.
https://community.ui.com/questions/Possible-bug-seen-in-setting-AP-Channel-against-Access-Points/7eb797e7-f30d-4bb0-b2be-71aec0eb1401#answer/c979436b-b24f-438e-8ebc-0c39a9fa6040.

@AlexWilsonsBlog
You really do not need 80MHz channels in a residential setting. In fact, most times, 80MHz causes more problems due to higher risk for interference, less channels to use internally to avoid overlap / reuse. Plus you lose 3dBm of strength everytime you double channel width. Most professionals, myself included, use 20 and 40MHz only to avoid these issues. Use 40MHz. You have 4 non-DFS ones to use... 36, 44, 149, 157. If by chance you need an extra channel, you always have a 20MHz channel on 165.
https://community.ui.com/questions/Setting-up-3-home-APs-5G-question/bceb113f-797d-4180-bde3-ad2c0423e537#answer/a572ad70-71b2-409f-b6d3-637562b19c9f

77.4 Power Levels.

When I was running a **single** Access Point, I traditionally set my 2.4GHz power level to Medium; and the 5GHz power level to High. Running lower power levels on the 2.4GHz band should help dual band devices migrate towards the 5GHz band. I recently experimented by setting each power level to Custom and maxing-out the dBm settings, this temporary experiment showed that High power is equal to 23 dBm (at least on my AP models / in the U.S.A.). Per the 7 dBm delta comments below, maybe the 5GHz power level should be set to Custom / 23dBm, and the 2.4 band should instead be set to Custom / 16 dBm and not be set to Medium.

When I am running **multiple** Access Points, I find it better to perform customized tuning of your AP(s) transmit power levels, which is better for roaming. Consider initially setting each 2.4GHz power level to a Custom level of 13dBm; and set each 5GHz power level to Custom / 20dBm. This should help mobile devices more-efficiently transition / roam to different Access Points (and also stay on the 5 GHz band) as the devices move around. These dBm values can later be adjusted to suite your own particular site and/or a potential mix of UAP models, which may have different antenna gains.

[2022 Note] Newer firmware for AP-AC-LRs may be limiting power levels
https://community.ui.com/questions/AP-AC-LR-TX-Power-Neutered/bb383790-a09e-4f0e-87ed-d100cf9c82bd

How to set power levels is described in section 77.12. See also section 77.13.

@gregorio
Too much power and devices will stick to distant Access Points. Too little power and you will have gaps.

@gregorio
Mobile devices are 15-30mW EIRP and APs can be 1000mW. If your AP Tx power is too high, the clients can hear the AP screaming at them but the AP cannot hear the client whispering back. This results in high retries and packet loss.

@gregorio
[Could you please just further explain why lower powered APs is better?]
There are many technical reasons. The biggest thing to remember is that WIFI is bi-directional and for the most part, serial in nature (one device uses the airwaves at a time). The link between any device and the AP must be somewhat in balance or it will reduce performance for all devices. U6-Pro can blast out roughly 1000mW of power but the average client device is limited to about 15-30mW. When APs are on AUTO (equal to HIGH) mobile devices can hear many APs screaming "pick me! pick me!" and will connect to the first one that meets the device WIFI requirements for minimum signal level. The problems start because the WIFI standards do not really include the ability for the AP to tell the client "I don't want you because you do not meet MY minimum signal requirement".
The device thinks it has a solid connection TO the AP based only on the received signal strength it is getting FROM the AP. There is really no other mechanism to report this. Operationally, the device will transmit something to the AP over a very low and slow data rate either getting no response or be told that the message was not properly received. Either way, the device must try again to transmit the data. These retries, especially over slow data rates eat up the available shared airtime for **all** devices.
Getting the APs closer to the clients is the only way to improve the signal strength TO the AP. After all, you cannot increase the Tx power of your cellphone. Having more APs closer to the clients is also the best way to deal with outside interference but that is getting into lesson two.
There is a lot more to it, but this is probably the most important aspect for the average home user to consider.
https://community.ui.com/questions/U6-lite-vs-U6-pro/bd3320c0-b0f7-4785-95f2-ee8e4fa2f025#answer/7255cc46-643f-4d4a-b995-b52796cdcaab

@gregorio
We are starting with 13dBm 2GHz and 20dBm 5GHz Tx power and moving up or (more often) down slightly. 13 is very close to what mobile clients use and the 5G spread is acceptable in this direction. Regardless, always maintain at least 7dBm delta or your dual band mobiles will always seek 2G.
https://community.ui.com/questions/U6-LR-Clients-keep-dropping-off-5Ghz-and-on-to-2-4-Ghz/d7449d8e-46c4-4bd7-a14b-5ce34828aa03#answer/4066717d-b545-46a5-bdf0-00969135e589

@ChessMck
While I agree with @gregorio on power settings and matching current devices, I have 5 APs at the house and use 10 dBm on 2G and 17 dBm on 5G as I want the client roaming sooner and not running 2G power that can attract neighbor devices. And I have some older IoT 2G devices that seem to run less than current IoT 2G devices. YMMV and every site is different. I'd definitely suggest you not be higher than what @gregorio suggested..... as to why the approx 7 dBm difference 2/5G – HERE
https://community.ui.com/questions/What-are-reasonable-packet-error-rates-on-a-wireless-access-point/e85ecefb-850c-4828-8220-400e52de6b78#answer/10a0122e-6444-44ff-a92a-b548af9199af
Editorial Comment: @ChessMck is using 5 APs, and has therefore set each AP to transmitting less power i.e. a smaller cell size, than what @gregorio suggests doing, in the previous comment.

@lcire1
So the issue you have in a multi AP network is finding the right overlap so your clients will roam between AP's . Because when to roam is an exclusive decision made only by the client, the best you can do is set up the right conditions to encourage them to jump to a new AP as they move closer to it. Most clients will start looking for a new AP between -70 and -72dBm. If the signal is stronger than this at the adjacent AP, Client will be highly unlikely to jump even if right under the new AP. So download something like wifiman on an android device, (won't work with apple phones) and walk around measuring the signal from each AP. Adjust 5Ghz first to set each radio to be less than that value at the next AP. Maybe shoot for -77dBm under the AP but this is something you will need to play with a bit based on your client mix. Once you have all the 5Ghz set, just go though and lower the 2.4ghz to be 7dBm less than the same AP 5Ghz radio. Lastly you want to remove the option for the client to just keep asking for a slower data rate as the signal drops when they move away. Use the minimum rate controls to remove the lowest rates. This will cause the beacon to not advertise the slowest rates meaning the client needs to start looking earlier as signal drops.
https://community.ui.com/questions/U6-LR-Clients-keep-dropping-off-5Ghz-and-on-to-2-4-Ghz/d7449d8e-46c4-4bd7-a14b-5ce34828aa03#answer/b87afd85-266c-4fda-8cbf-66b5520ac53e
Editorial Comment: I believe you would measure the “other” AP at -77dBm under “this” AP.

@mjp66
1. Disable wireless mesh / connectivity monitor. Disable Band Steering. Disable Minimum RSSI.
2. Remove all auto power and channel settings. You want to set these manually, which is always better than what can be accomplished by the auto settings.
3. Set the 2.4GHz radios to only channels 1, 6, or 11, and to a channel span of 20. If two AP's need to use the same channel number, make sure those are the two that are farthest away from one another. Initially set the 2.4GHz power to custom / 13dBm.
4. Set each 5GHz AP radio to a channel span to 40, and then to a unique / separate channel from the following list: 36, 44, 149, and 157. Initially set each 5GHz power to custom / 20dBm.
5. Download and run WiFiman (only useful for a site survey on an android device).
6. Start with your most important AP. The order, of which APs are tested against each other, depends upon your installation geometry. Let the WiFiman app link to this first AP. Go to the display that shows -dBm power Stand under the next closet AP and read the 5GHz power from the first AP. On the first AP, set a custom 5GHz power value, that will yield a value of -76 to -77 dBm when measuring (this first AP's power) while standing right under the second AP.
6A. Measure the signal level at the midpoint between APs. We like to see -65dBm as the crossover. In other words, when your connected AP signal drops to -65dBm, you can hear at least one other AP at -65dBm.
7. When you have the first AP's 5GHz power level set, now measure the second AP's power, when standing right under its closest neighboring AP. This closest neighbor may the first AP or may be a third AP. Try to achieve the same -76 to -77 dBm value, when measuring the second AP's power while under the third AP.
8. Continue to the last AP doing the same process. Depending upon your installation geometry, this may involve multiple combinations.
9. Go back to each AP and reset the 2.4GHz power to 7 dBm less than that APs 5GHz power level.
10. Set minimum rate control to 12 for all 5GHz radios. Check "Also require clients to use rates at or above the specified value". If your installation is working well, you can later try setting this value to a more aggressive value of 24.
11. Set minimum rate control to 6 for each 2.4 GHz radio. Check "Disable CCK rates ...", some later Unifi versions may later automagically uncheck this CCK checkbox. Check "Also require clients to use rates at or above the specified value".
See thread at https://community.ui.com/questions/Performing-a-Home-Wi-Fi-Site-Survey-for-Better-Roaming/599f3ae9-499c-4e33-8c6a-21bbf8a0e122
Based upon https://community.ui.com/questions/Disappointed-with-UAP-AC-PRO-WiFi/d011c2a4-8b14-4ed4-85aa-e364f2c5e228#answer/edb425d5-99d5-4dac-a0b1-be573a1d78a0

@gregorio
LOW is too low (typically 6dBm) especially when compared to the high power being used on 5G.
2GHz should be 7dBm lower than 5GHz to promote devices to the latter band. We prefer to start the process at 13dBm and 20Dbm for 2/5GHz. This puts the AP output close to the mobile device output.
We find that AC class APs can go up a couple dBm and AX class sometimes need to go down. The higher gain of the U6-LR and Pro models have been a real challenge in retrofits.
Setting overlap at the AP might result in too much in the middle with U6 APs. Also look at it in the middle where both AP should be seen around -65dBm.
https://community.ui.com/questions/Devices-wont-roam-connect-when-walking-between-APs-anymore/5ba39920-1395-491e-88dc-08bfa1a5679b#answer/d391595f-2a21-4b6b-8d69-2a36e82abc81
Editorial Comment: I assume that "Pro" is probably the U6-Pro model.

Here is a nice article on sticky clients / data rates:
http://wifinigel.blogspot.com/2015/03/what-are-sticky-clients.html

Here is a (somewhat generic) tuning video, which is referenced somewhat frequently:
https://www.youtube.com/watch?v=QE-jw1Bu0T8

77.5 Band Steering.

In the same settings area, you have the choice of:

Prefer 5G, Balanced, Off

I left mine set to the default of Off. I hear that Prefer 5G or Balanced settings may cause roaming problems.

77.6 DTIM Settings.

Changing this should help mobile devices, especially Apple, save power. For at-least the SSID which is assigned to the Home Network, for each WLAN Group, change the "DTIM 2G period" to "1" and the "DTIM 5G period" to "3", per "Modifying the DTIM Period" section of

https://help.ui.com/hc/en-us/articles/221029967

I just changed all my SSIDs. For completeness / caching, here are abbreviated directions:

Settings -> Wireless Networks -> "Your HomeNetwork SSID" -> Edit
(Open) Advanced Options -> (Open) 802.11 Rate and Beacon Controls
Uncheck "DTIM Mode / use default values"
Set "DTIM 2G period" to "1" and "DTIM 5G period" to "3".
Save

These are also shown in Figure 165 – ChessMck's Minimum Data Rate Settings.

2022 Note: 2G=1, 5G=3 appears to be the new UniFi default. This document previously said 2G=3, 5G=3. The section "Modifying the DTIM Period" appears to have been removed, by Ubiquiti, from the above link.

77.7 Enable minimum data rate controls.

Having 802.11b devices connected to your AP slows everybody else down. Having any device which transmits its data slowly, takes time away from all the faster Wi-Fi clients.

See also section 77.13 - Expanded UI.com AP References.

@lcire1
Auto [power] is basically high. To roam correctly, most clients will start looking between -70 and -72dBm. You want them to see that value before they physically get to the adjacent AP, otherwise they will [do as your wife's phone does and] cling to the AP they have. Minimum RSSi is not effective because it is something the AP controls, while which AP a client connects to, is entirely a decision the client controls. The behavior of the client when signal drops is to simply request a slower data rate which is more tolerant of the low signal. This then slows all connected clients as they must wait for data to be sent at much lower rates. To counteract this, go to the minimum rate controls and disable lower rates. On a single AP system you can't do this as the client has but one AP to cling to. With multiple AP's, it is desirable to remove the lowest rates to "encourage" the client to probe for a new AP at a higher signal. I.e. to roam and keep overall data rates high.
https://community.ui.com/questions/WiFi-6-LR-trouble-Roaming-with-Android/5310ba4b-4475-4ff4-9647-8f85a2ef0303#answer/dbe1c75e-b747-49c6-aaf5-646c93c52a2d

These are the settings I'm now using for the above two reasons:

DTIM 2G Period:	1
DTIM 5G Period:	3
2G Data Rate Control:	Checked / 6 Mbps
Disable CCK Rates …:	Checked (may later uncheck itself in newer UniFi versions)
Also require clients to use [2] rates …:	Checked
5G Data Rate Control:	Checked / 12 Mbps
Also require clients to use [5] rates …:	Checked

These setting are under Wireless Networks, <Each SSID>, "802.11 Rate and Beacon Controls" section.

See Figure 165 – ChessMck's Minimum Data Rate Settings.

2022 Notes: I now believe the "Disable CCA rates" button is no longer (needed or) operable in newer (V 6.x or V7.X) UniFi installations. There is now a checkbox "Legacy Support" / Enable legacy device support (i.e. 11) that you probably want unchecked, i.e. unchecked disallows slow B devices.

Figure 165 – ChessMck's Minimum Data Rate Settings.

AP-AC-LR-only-giving-40mbps-throughput-on-2-4GHz
https://community.ui.com/questions/AP-AC-LR-only-giving-40mbps-throughput-on-2-4GHz/07246148-beb1-460a-8baa-559aefecdfb8#answer/c72884bb-d762-447f-8665-3749cecd69b3

Slow-2-4-Ghz-Download-speed
https://community.ui.com/questions/Slow-2-4-Ghz-Download-speed/760f4169-9b04-46fc-8b1b-678ccbbdfea0#answer/73bccced-5616-4127-b16f-a052b94cfaaa

@ChessMck
<Regarding moving the sliders all the way to the right>
You can move it fully to the right and if all devices work, then that would be best - however older 2G devices may not work. Some may have problem if you go above 6 Mbps on 2G. Test and use the highest min that works for you. If you have old devices, sometime you cannot check the CCK box, but that will help if you can check that box as the CCK is a less efficient protocol.
https://community.ui.com/questions/High-density-Gaming-Setting-AP/43672883-a05f-4c9c-acc1-524b0df0d24c#answer/1bf95377-87b1-44fc-98a4-b9d5b8145288

77.8 Settings Which Could Be ON.

The following settings could help your install by being ON:

UAPSD, Multicast Enhancement, allow BSS and all SSID combined i.e. WIFI bands Both.
https://community.ui.com/questions/High-TCP-latency-for-Clients-intermittent-wifi-latency/7d11ebfa-de42-4184-8c54-c85dd6e6f6ad#answer/9cb30af0-77cd-44b7-8554-b54d179c9d32

77.9 Settings Which Should Probably Be (Mostly) Off.

The following settings are mentioned (when on) as causing problem in many posts. I don't know if any of them have ever defaulted to being on. To see some of them, you may first need to check Settings -> Site -> Enable advanced features. You may also need to refresh the page OR logout and then log back in to view the advanced items.

Try New Settings BETA -> Wi-Fi AI BETA -> Enable Wi-Fi AI -> Off

(Switch to Classic Mode)

Settings -> Site -> Automatically Optimize Network and WiFi performance -> Off

Settings -> Site -> Uplink Connectivity Monitor -> Off

(May need to be on if you are using Mesh-type features)

Settings -> Wireless Networks -> <Your SSID> -> Edit -> Advanced Options -> Fast Roaming -> Off

(Conflicting posts say this may need to be on, for some Apple device stability)

Settings -> Wireless Networks -> <Your SSID> -> Edit -> Advanced Options -> UAPSD -> Off

(Conflicting posts say this may need to be on, for some Apple device stability)

Settings -> Wireless Networks -> <Your SSID> -> Edit -> Advanced Options

-> High Performance Devices BETA -> Off

77.10 Other Settings.

I left them alone. There are lots of different UniFi / Access Point settings and hundreds of postings (and opinions) about them, have fun experimenting.

This may help explain some advanced settings:
https://evanmccann.net/blog/2021/11/unifi-advanced-wi-fi-settings

77.11 Batch Settings.

This allows you to set certain settings for multiple Access Points at one time.

Using BATCH may be faster - if you haven't used batch - this GUIDE may help - so you can change all of them at one time.... Take note of this ==> 1. Navigate to the Devices page and select device type (Wireless) on the top bar (the batch configuration feature will not appear if ALL is selected). So make sure you click on the WIRELESS button, then you can select all the APs together...
https://community.ui.com/questions/Poor-signal-with-11-AP/3380f3cd-6ad5-4caf-90d1-373473d52701#answer/43fc0870-75b8-4b88-9c51-f2ec70d0a9a5

<GUIDE> https://help.ui.com/hc/en-us/articles/115000170548-UniFi-Group-Configuration-and-Tags

77.12 How to set the channel assignment and power.

For context, reference text near, along with Figure 161 – UniFi Utilize a WLAN Group.
To set channels and power levels for a particular Access Point, select the following:

1. Devices. (not shown)
2. <Your Access Point>. (not shown)
3. Configure Tab.
4. Expand the Radios Item.
5. Set the 2.4 GHz Channel Width.
6. Set the 2.4 GHz Channel.
7. Set the 2.4 GHz Transmit Power. (Probably use Custom if using multiple APs).
8. Set the 5 GHz Channel Width.
9. Set the 5 GHz Channel.
10. Set the 5 GHz Transmit Power. (Probably use Custom if using multiple APs).
11. Queue the changes.
12. Apply the changes (not shown, but near the bottom)

See Figure 166 – Setting Access Point's Channel / Power Level.

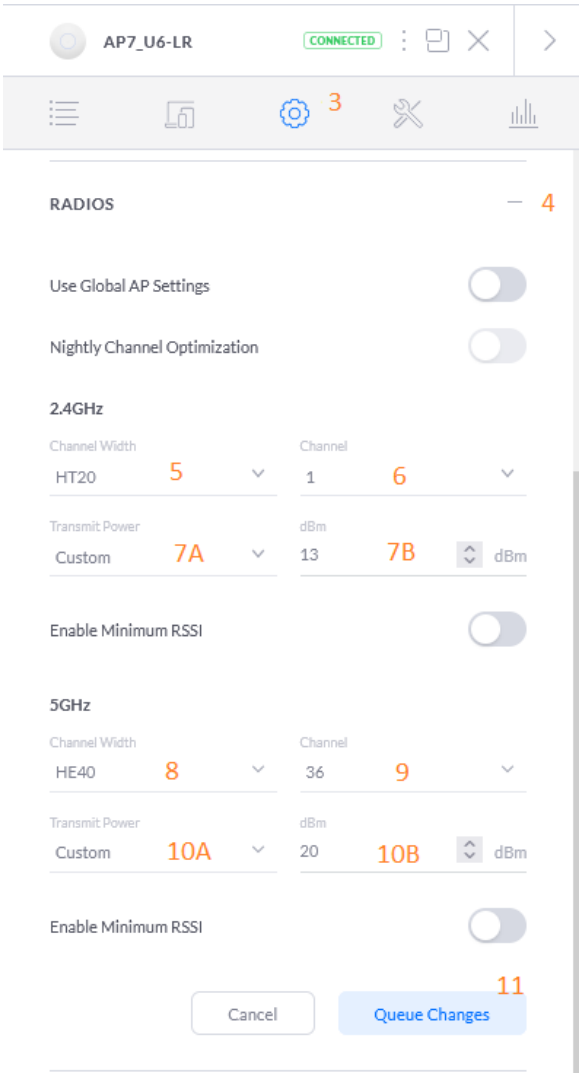


Figure 166 – Setting Access Point's Channel / Power Level.

77.13 Expanded UI.com AP References.

(Original posting data may be slightly edited and/or re-formatted for clarity)

@gregorio
You might try to move away from DFS channels. Devices cannot scan them and therefore need to wait until a beacon is heard. Even though beacons are very often, it does impact roaming. Have you checked RSSI overlap? Do you have anything like Fast Roaming or High Performance Devices enabled in the wireless configs? They, along with Connection Monitor, WiFi AI and Auto Optimize should all be disabled as they can cause problems.
https://community.ui.com/questions/ER-X-and-2-UAP-AC-PRO-hand-over-1-and-Lan-Vlan-access-2/e618495e-7d75-420e-9e8c-9e6537ab3397#answer/d7bb1115-7547-4401-8e26-a4aa79eee6d3

@AlexWilsonsBlog
1. Consumer grade routers are usually running at full power and bristling with high gain antennas designed to flood the place with coverage from a single device. Of course, they rarely flood it well. Then you end up cobbling together a bunch of "extenders" which make it worse usually.
2. Commercial grade, like Ubiquiti, is designed to provide robust, stable coverage in a limited area. It is part of a system of APs that expand that coverage. If done right, no weak spots.
3. The walls you speak of ... they cause about 3dBm loss each. That represents 50% of your signal strength. Then add in some additional loss due to distance. Then add in the next wall (another 50% further). See the problem?
4. Interference. If you are in a noisy area, someone else might be sitting on your channels and thus causing noise which further erodes your performance.
5. Your 80MHz channel is great for throughput, but also picks up more chance for interference since you are using channels 149, 153, 157, and 161 to achieve 80MHz. If you have a neighbor on any of those channels and their signal is -80dBm or better, they could be impacting it. Same happens on 2.4GHz channels.
6. When testing, be sure you are always on the same band when testing to get consistent results. 2.4GHz will usually be less than 5GHz on throughput, sometimes significantly.
7. If you do a channel scan on the AP, keep in mind it is scanning from the AP. The client who is likely further away and maybe on the periphery of the house could be seeing something different and therefore you might not catch problems from neighbors. This is why when we do troubleshooting for clients; we always walk the perimeter with our spectrum gear.

https://community.ui.com/questions/Very-limited-range-on-new-AC-Pro-setup/2f48b246-72e4-4bfe-a33a-ba31913332ba#answer/e7d8e952-6a38-4fec-9030-e38a5b7801f5

@buttersh
I don't care about speed. In today's massively congested 2.4 GHz airspace (at least in my neighborhood), the fact that 5 GHz doesn't go very far is a HUGE benefit. I can see 54 other SSID's on 2.4 GHz, while I can only see 4 on 5 GHz and those are my direct neighbors at a very low signal level. 5 GHz essentially affords you clear airspace, the only drawback being that you need more WAP's. I have managed to purge all 2.4 GHz devices and have been very happy for several years running 5 GHz only. Far fewer headaches. Of course, you have to do your [own] tuning, putting them on non-overlapping channels, and where they must overlap, adjusting power, etc., but that is par for the course.
https://community.ui.com/questions/New-home-looking-for-AP-location-advice/d6afd24e-d46f-4ebd-81a9-158010dc302b#answer/9cf82c04-abc9-4d96-ba32-ec55d86c78a3

@ChessMck
But as wifi is half duplex, there is a lot of overhead between packets including beacons for each SSID every 102ms. Bottom line - expect 55-65% of connected rate if few to one client connected to the AP.
Then normally you will use 40 or 80 MHz bandwidth (yes I know you can run 160, but don't!) and most mobile devices are only 2x2 streams. Then there are marketing numbers using the unachievable connect rates at max streams possible then adding the 2G and 5G together.
And then people run full power creating all kinds of roaming issues and latency.
Do you have Auto Optimize ON? Try turning that off as it will change many settings you may not want to be changed.
If you want to see where I start - my normal copy/paste - all sites are different & YMMV
I would suggest the following settings as a base - some need to be set in the classic menu...and may have newer names in controller 6 as this is from controller 5.14.23 These are based on stability and only using options that don't disrupt clients and options that most clients understand or at least are not ones that can cause issues by being a new setting that older client don't understand - like PMF.
OFF - Any Band steering (including balanced), High Performance (in controller 6.2+ now only in New User under WiFi then SSID then Advanced), Fast Roaming, PMF, Auto Optimize, Radio AI, ATF, RSSI and (on switch) DHCP Snooping.
On - UAPSD, Multicast Enhancement (IGMPv3), allow BSS, all SSID combined i.e. WIFI bands Both and (on switch) IGMP Snooping.
Rates - Push 802 rates on 2G to 6 Mbps and disable the CCK rates and also set 5G rate to 12 Mbps and check the boxes for both bands requiring clients to use (as a min) these higher rates.
Power (Custom) ==> 2G set to 10 dBm and 5G set to 17 dBm for same cell size and good roaming and less retries/latency. (This setting is for when you have multi APs, not just one AP. If you only have one AP, where there is no roaming between APs then for more coverage area - power can be higher - like 2G 5 dBm and 5G 20 dBm.)
DTIM - Set to 3 for 5G and to 1 for 2G SSIDs
https://community.ui.com/questions/Upgraded-ISP-speed-and-EdgeRouter-X-craters-it/26921a4a-8e52-4038-95b5-3bbc4d97f258#answer/b8bde66a-f6d8-4c7f-bb72-611c629637d8
Editorial Comment: I think the stated 5 dBm for 2G [using one AP], should probably be 20 – 7 = 13 dBm.

@seawolf
[MacOS users have wifi / network issues]
When this happened at my house (my GF has all iStuff and I'm Windows/Android), I had to turn off band steering-type settings then her stuff connected and stayed connected. Not mine, but I generally follow this list when iOS is having issues one at a time till they work properly:

- Disable Settings > Site > Auto-Optimize Network
- Disable Settings > Wireless Networks > SSID > Advanced Options > High Performance Devices
- Disable Connect High Performance clients to 5 GHz only
- Disable Prefer 5G
- Disable Fast Roaming
- Set DTIM to 3 on both bands under WiFi > Advanced

https://community.ui.com/questions/MacOS-users-have-wifi-network-issues/15623942-17dc-4b32-82c5-6ac9225ff7ee#answer/fdd068d1-c346-4662-8326-b44fda30c2c6

@ChessMck
[The Minimum RSSI value is set individually on each AP and indicates the minimum signal level required for a client to remain connected.]
Let me explain a bit more. RSSI - when the signal level is hit - actually does a disconnect with the client and then doesn't respond to the client's probes when the client tries to reconnect. The idea is the client will then search for other APs. However this kick-off and then probes without response, delays and can confuse the client. And this can cause a drop in something time sensitive like a VoIP call. On the other hand - the client would already be looking for another AP if the AP power was balanced against the clients (avg 14 dBm) as it is the client that makes the roaming decision and if you are running a lot of power from the AP - the client will not know it is no longer being heard by the AP as it still has a good signal. That's why I suggest 10 dBm for 2G and 17 for 5G as that is a balance of the clients 14 dBm and also 5G is 7 dBm less (physics of RF) than 2G at a given distance - Reference THIS. Also the client does understand min rates and by setting them higher, that frees up beacon air time (2G not sending beacons at 6Mbps, example below, instead of 1 Mbps). So the client will roam based on hitting the min rate too. One newer tool is allowing BBS - as this is the AP telling the client that it is having trouble hearing. And there may be a reason to use RSSI - but normally you are better off to help the client know when to roam rather than kicking it off... Often folks use it when they are running too much power and don't understand lowering the AP power may be a better solution..... But almost everything in WiFi comes as a two edge sword and every site is different....
https://community.ui.com/questions/Looking-for-product-recommendations-for-small-restaurant/4ed2e3ef-3181-4f1a-bc6c-3c3d9234a936#answer/2f750573-34e8-4006-a069-7c6e757b3e6e

@AlexWilsonsBlog
Simply put, roaming is a feature of the client. It is reacting to your network and how it is configured. This is not the fault of the client or the network... it is on you to properly tune the network. No one likes to hear this, but that is the reality of wireless.
It starts with understanding roaming thresholds. For iOS devices, it is -70dBm. This means your client device will not even consider roaming until the RSSI of the client drops below -70dBm. Once that happens, it searches for a suitable option to move to. It does not evaluate and compare options. It takes the first one it finds that meets the criteria. If your APs are on auto power, they are all likely blasting full power on both 5 and 2.4GHZ. This means the 2.4 coverage is likely well beyond the 5GHz coverage and your APs are likely covering way beyond the next one over. Hence nothing ever moves.
Lower the power, improve the performance. Imagine that... less is more!. My go to is low on 2.4 and medium on 5GHz, then tweak using custom, maintaining my 2.4 at 7dBm less than 5GHz where possible. I also shut 2.4 off on some APs to avoid too much overlap. Use natural shielding to help reduce coverage (walls, floors, furnishings, etc.).
https://community.ui.com/questions/Wifi-Roaming/1c3291a4-5e9b-48cc-96ee-bcea38009ca6#answer/3d5aa450-3b06-4d72-a2da-db3e49beece2

@ChessMck
I apply to all APs at a site, as I design for 5G coverage. Each site and needs will be different
 - however the two thing to keep in focus - usually the handheld clients have about 14 dBm of power and you need 7 dBm more power on 5G to have the same signal (free air) 2G/5G.
Therefore this becomes a bit of a balance act. Two things quickly come into play (1) while the client has to be able to talk back, usually there is 10X more data going to the client, so you can allow for a slower connection on the return (client to AP) as long as you don't get into sticky clients. (2) As 2G has more coverage and if you want to balance the two (for area covered) and you need more power for the 5G (but at the same time the client need to talk back) ==> this is the balance of having 5G more than the client and 2G less (the 7 dB) and where the 10/17 power comes from, in the way I design, as I want 5G everywhere for client devices and have the 2G for devices that do not support 5G.
RSSI is disruptive and I avoid using it... last tool I use. Currently I do not have RSSI on at any client location. My first tools are always power and 802 Rates as the client fully understands these and works with them. [Then on the AP I use Cell Size Setting for sites with a lot of RF from neighbors Wi-Fi.] As a rule, if you have to use RSSI - you are running incorrect power (too much).
Basically set the system up correctly (based on your needs) and let the client do what it thinks is best. There may be a good reason the client is connecting to a different AP that you might think.
One last thing for you to consider on using RSSI - it kicks the client OFF and then doesn't respond to probe request, but the client can still "see" the AP and may think the Wi-Fi is simply bad ==> another post of mine with more detail about RSSI and why not use is HERE
The bottom line - many things work together - so this list/suggestion of mine needs to be considered "as a package" with minor adjustments and is what I have found to work well. (Repeating the list below as it may have updates or clearer wording.)
I would suggest the following settings as a base - some need to be set in the classic menu...and may have newer names in controller 6 as this is from controller 5.14.23 These are based on stability and only using options that don't disrupt clients and options that most clients understand or at least are not ones that can cause issues by being a new setting that older client don't understand - like PMF.
OFF - Any Band steering (including balanced), High Performance (in controller 6.2+ now only in New User under WiFi then SSID then Advanced), Fast Roaming, PMF, Auto Optimize, Radio AI, DHCP Snooping, ATF, RSSI
On - UAPSD, Multicast Enhancement, allow BSS and all SSID combined i.e. WIFI bands Both.
Rates - Push 802 rates on 2G to 6 Mbps and disable the CCK rates and also set 5G rate to 12 Mbps and check the boxes for both bands requiring clients to use (as a min) these higher rates.
Power (Custom) ==> 2G set to 10 dBm and 5G set to 17 dBm for same cell size and good roaming and less retries/latency. (This setting is for when you have multi APs, not just one AP, where there is no roaming between APs and power can be higher - like 2G 16 dBm and 5G 21 dBm.)
DTIM - Set to 3 for 5G and to 1 for 2G SSIDs
https://community.ui.com/questions/High-TCP-latency-for-Clients-intermittent-wifi-latency/7d11ebfa-de42-4184-8c54-c85dd6e6f6ad#answer/9cb30af0-77cd-44b7-8554-b54d179c9d32

[How to properly configure APs signals for best performance devices]
@AlexWilsonsBlog
There are a few things you should do. The key to success is to understand that the client decides where to connect. It doesn't evaluate which is best either. It connects to the first one it finds that meets its minimum requirement known as a roaming threshold. That threshold varies based on client. Typically it is around -70 to -75.
The first thing to do is manage the coverage areas by adjusting power and potentially data rates. Lower the power so they just barely overlap. Yeah, tricky to guess without decent measuring gear but generally speaking, use low for 2.4 and medium for 5. Or custom to fine tune it. Try to maintain 2.4 at 7dBm less than 5. This will keep the 2.4 and 5 coverage close to the same. Where this gets complicated is remembering the gain of the antennas plays in here too. If your 2.4 radio has a gain of 3 on the antenna, and you set power to 6dBm, your actual power will be 9dBm. Your 5GHz radio might have a gain of 4. If your target is 16 (7dBm higher than 2.4) you would set the radio to 12dBm.
Adjust accordingly to obtain coverage. Min data rates can further refine it. I usually go with at least 11Mbps as the min on 2.4 which will block all 802.11b devices. Which is good. Then I use 12 or 24Mbps on 5GHz. It used to allow more. Not sure why they changed it but it will help keep things off the AP and will help promote proper roaming.
Do not use min RSSI as that breaks roaming.
The last option is not perfect but helps. Lock to AP. ~~It is a client side feature.~~ Managed in the client settings for each device on your network. Access the settings and you will find the option to set the preferred AP. Now if that AP is off or not usable based on settings being too low, it won't use it. So not perfect, but does help.
I lock to AP all my stationary items like Apple TVs, light switches, HomePods, etc.
https://community.ui.com/questions/How-to-properly-configure-APs-signals-for-best-performance-devices/9aefb34e-68db-4b0f-abd9-ad466f032d10#answer/396e0903-cafc-4504-9e46-a0243cb445e1
@AlexWilsonsBlog [continued in thread]
As for the Lock to AP, that is in the "client" view on the controller. Not the device. Each client that attaches is listed. Find your device, click on it to bring up the device info, click on settings. Scroll down.
@gregorio [continued in thread]
WIFI is bidirectional. Based on client output of 12-15dBm, you should set your AP output power to match. Since most traffic is in the AP to client direction, you can run your links a little hotter in that direction. The problem is for dual band clients. In order to prevent them from sticking to the slower 2.4GHz band, you need to set your 5GHz power 7dBm higher. We start at 13dBm on 2.4GHz and 20dBm on 5GHz and move up or down 1-2dBm depending on AP gain and other local factors. You can reduce the delta to 6dBm to promote 2.4GHz a little more but we prefer to raise 5GHz MDR as high as possible.

@gregorio
Looks like your WIFI is not tuned at all and you are relying on Unifi to do it for you. "Fighting between the two channels" is a clear indicator that it is not working for you.
Your power is the first thing to set manually. We like to start with 13dBm for 2.4GHz and 20dBm for 5GHz. With 6GHz in the mix, logic might say that you need to use 22-24dBm there but this is starting to get too far from the 13dBm (approx) client output. There are not enough clients to worry about this today. In the future, I suspect people will find that the benefits from 6GHz are hard to extract without adding more APs but that is a different subject. These settings will naturally promote band steering to 5GHz without non-standards based gimmicks from the AP controller side. Your clients will automatically shift down from 5>2 without "fighting". These settings also prevent clients from connecting to more distant APs and not be able to talk back resulting in excessive retires.
The right way to start channel selection is RF scans from each AP, one at a time while the others are off. This will give you the external interference picture. This is the stuff you can avoid by selecting other channels. Since there are only three non-overlapping 2.4GHz channels (1, 6, 11), you need to map out their use carefully. Make sure when you re-use them, they are not on adjacent APs.
With 5GHz, you have a lot more flexibility. If you have UNII-3 available, there are four 40MHz channels but also several more in the DFS (UNII-2) range. However, even without DFS, it is pretty easy to use the four primaries (36, 44, 149, 157) and not step on your own toes with overlap.
6GHz has less propagation than the other bands so overlap is even less a problem. What is a problem for many clients is 160Mhz wide channels and link imbalance from using too much power. Don't get too hung up on trying to promote band steering towards 6GHz with 5GHz in the mix. Tests are showing that clients still rely heavily on signal strength when deciding which band to use and trying to increase power 2-4dBm over 5GHz starts to kill 6GHz performance benefits by increasing retires.
Turn off AUTO everything and disable Nightly Scans or you will lose all of this effort. Get here and test. It should result in much improved WIFI.
To see the RSSI and MCS of the clients, go to the Clients page of the controller and select all the right columns.
https://community.ui.com/questions/Help-Requested-Massive-Wifi-Problems-over-the-last-few-weeks-I-need-some-help-badly-with-UDMSE-and-/f8339977-99fc-4254-95de-b7285703015d#answer/7124d014-1681-4e63-be53-82ea4a4bf94f

@gregorio
Devices do not choose based on distance/stronger signal. They connect to the first AP that responds with a connection that fits it needs. How much overlap do you have? Generally, when you walk away from AP1 towards AP2 and signal falls to -65dBm, you should start hearing the new AP at -70dBm. We usually recommend that power be set at 13dBm for 2G and 20dBm for 5G to promote more use of the latter band and keep the links in balance. If this results in coverage gaps, you should consider more APs to fill in rather than use higher power. The reason is that you cannot increase the power of the device and the link needs to be somewhat balanced in both directions.
https://community.ui.com/questions/Clients-lose-connection-for-a-second-on-wifi/1ca6ecf4-d526-4f2b-bed0-2feac3f63f90#answer/37bfc352-465f-4fdc-a429-49deb9ed05d4

77.14 Wi-Fi Modulation Coding Scheme (MCS).

Figure 167 – Wi-Fi Modulation Coding Scheme (MCS) Table. describes what (theoretical) Wi-Fi speeds you should be able to achieve. I think the inputs into this table are: Spatial streams [Top, Mid, Bottom], Channel width [L – R], Data rate [802.11n=400ns, 802.11ac=800ns], and especially RSSI [Row].
Wi-Fi overhead can be estimated as-stealing / at about 40%. This specific table is from https://wlanprofessionals.com/mcs-table-and-how-to-use-it/ More information at that URL.

802.11n and 802.11ac MCS, SNR and RSSI

HT MCS	VHT MCS	Modulation	Coding	20MHz				40MHz				80MHz				160MHz			
				Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI
				800ns	400ns			800ns	400ns			800ns	400ns			800ns	400ns		
1 Spatial Stream																			
0	0	BPSK	1/2	6.5	7.2	2	-82	13.5	15	5	-79	29.3	32.5	8	-76	58.5	65	11	-73
1	1	QPSK	1/2	13	14.4	5	-79	27	30	8	-76	58.5	65	11	-73	117	130	14	-70
2	2	QPSK	3/4	19.5	21.7	9	-77	40.5	45	12	-74	87.8	97.5	15	-71	175.5	195	18	-68
3	3	16-QAM	1/2	26	28.9	11	-74	54	60	14	-71	117	130	17	-68	234	260	20	-65
4	4	16-QAM	3/4	39	43.3	15	-70	81	90	18	-67	175.5	195	21	-64	351	390	24	-61
5	5	64-QAM	2/3	52	57.8	18	-66	108	120	21	-63	234	260	24	-60	468	520	27	-57
6	6	64-QAM	3/4	58.5	65	20	-65	121.5	135	23	-62	263.3	292.5	26	-59	526.5	585	29	-56
7	7	64-QAM	5/6	65	72.2	25	-64	135	150	28	-61	292.5	325	31	-58	585	650	34	-55
	8	256-QAM	3/4	78	86.7	29	-59	162	180	32	-56	351	390	35	-53	702	780	38	-50
	9	256-QAM	5/6			31	-57	180	200	34	-54	390	433.3	37	-51	780	866.7	40	-48
2 Spatial Streams																			
8	0	BPSK	1/2	13	14.4	2	-82	27	30	5	-79	58.5	65	8	-76	117	130	11	-73
9	1	QPSK	1/2	26	28.9	5	-79	54	60	8	-76	117	130	11	-73	234	260	14	-70
10	2	QPSK	3/4	39	43.3	9	-77	81	90	12	-74	175.5	195	15	-71	351	390	18	-68
11	3	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71	234	260	17	-68	468	520	20	-65
12	4	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67	351	390	21	-64	702	780	24	-61
13	5	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63	468	520	24	-60	936	1040	27	-57
14	6	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62	526.5	585	26	-59	1053	1170	29	-56
15	7	64-QAM	5/6	130	144.4	25	-64	270	300	28	-61	585	650	31	-58	1170	1300	34	-55
	8	256-QAM	3/4	156	173.3	29	-59	324	360	32	-56	702	780	35	-53	1404	1560	38	-50
	9	256-QAM	5/6			31	-57	360	400	34	-54	780	866.7	37	-51	1560	1733	40	-48
3 Spatial Streams																			
16	0	BPSK	1/2	19.5	21.7	2	-82	40.5	45	5	-79	87.8	97.5	8	-76	175.5	195	11	-73
17	1	QPSK	1/2	39	43.3	5	-79	81	90	8	-76	175.5	195	11	-73	351	390	14	-70
18	2	QPSK	3/4	58.5	65	9	-77	121.5	135	12	-74	263.3	292.5	15	-71	526.5	585	18	-68
19	3	16-QAM	1/2	78	86.7	11	-74	162	180	14	-71	351	390	17	-68	702	780	20	-65
20	4	16-QAM	3/4	117	130	15	-70	243	270	18	-67	526.5	585	21	-64	1053	1170	24	-61
21	5	64-QAM	2/3	156	173.3	18	-66	324	360	21	-63	702	780	24	-60	1404	1560	27	-57
22	6	64-QAM	3/4	175.5	195	20	-65	364.5	405	23	-62			26	-59	1580	1755	29	-56
23	7	64-QAM	5/6	195	216.7	25	-64	405	450	28	-61	877.5	975	31	-58	1755	1950	34	-55
	8	256-QAM	3/4	234	260	29	-59	486	540	32	-56	1053	1170	35	-53	2106	2340	38	-50
	9	256-QAM	5/6	260	288.9	31	-57	540	600	34	-54	1170	1300	37	-51			40	-48

Figure 167 – Wi-Fi Modulation Coding Scheme (MCS) Table.

I believe that (borrowed from the internet) Figure 168 – Wi-Fi Minimum 802.11 dBm Sensitivity Table. shows what RSSI is needed to achieve which signal modulation scheme. Signal modulation translates into data rates. Reference Figure 167 – Wi-Fi Modulation Coding Scheme (MCS) Table. For my installation, 5GHz is set to a 40 MHz width, so I would use the blue line for 5 GHz.

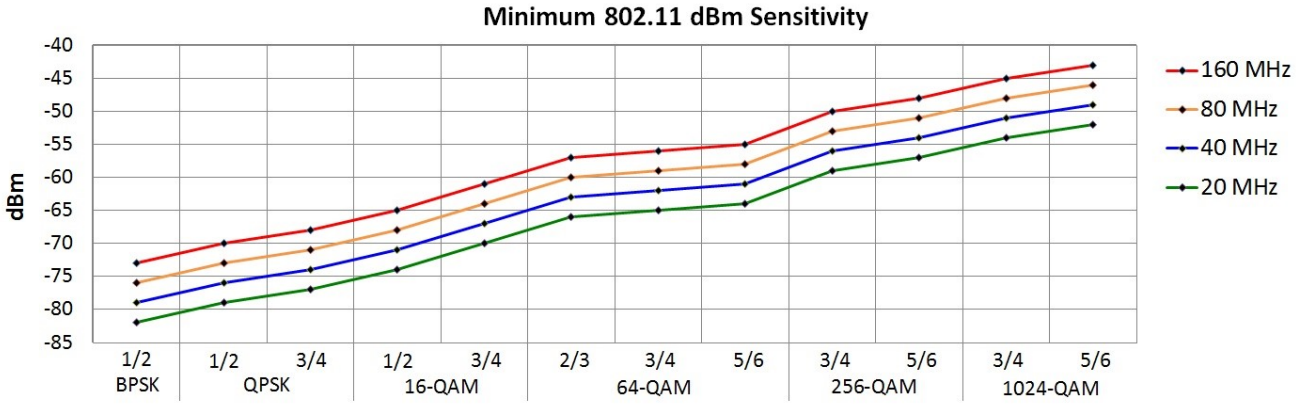


Figure 168 – Wi-Fi Minimum 802.11 dBm Sensitivity Table.

77.15 Measuring AP Power Levels (i.e. Cheap Site Survey).

There is a discussion at
https://community.ui.com/questions/Performing-a-Home-Wi-Fi-Site-Survey-for-Better-Roaming/599f3ae9-499c-4e33-8c6a-21bbf8a0e122

I have tried many Apps on an Android phone to characterize Wi-Fi power levels, as received from an AP. An iPhone will not work for this task. If you typically use an iPhone, you should be able to acquire a used Android phone from a friend, as only 2.4GHz and 5GHz Wi-Fi is needed for this task, i.e. no cell service is needed.
I particularly like two Apps: “WiFi Analyzer” and “WiFiman”.

The first tool is “**WiFi Analyzer**”. See Figure 169 – WiFi Analyzer Channel Screenshots for samples from the Wifi Analyzer App for both 2.4 GHz and 5 GHz. Various graphical and textual screens are available within this App.

Figure 169 – WiFi Analyzer Channel Screenshots

The second tool is "**WiFiman**". WiFiman is published by Ubiquiti. One page on the App, shows a list of available Wi-Fi SSIDs. See Figure 170 – WiFiMan WiFi-List Screenshot. You can also click on these SSID items. Note the SSID item which is circled in orange within the figure. When you click on an SSID, you will then see detailed signal strength(s) for that item. That signal-strength detail will be shown in Figure 171.

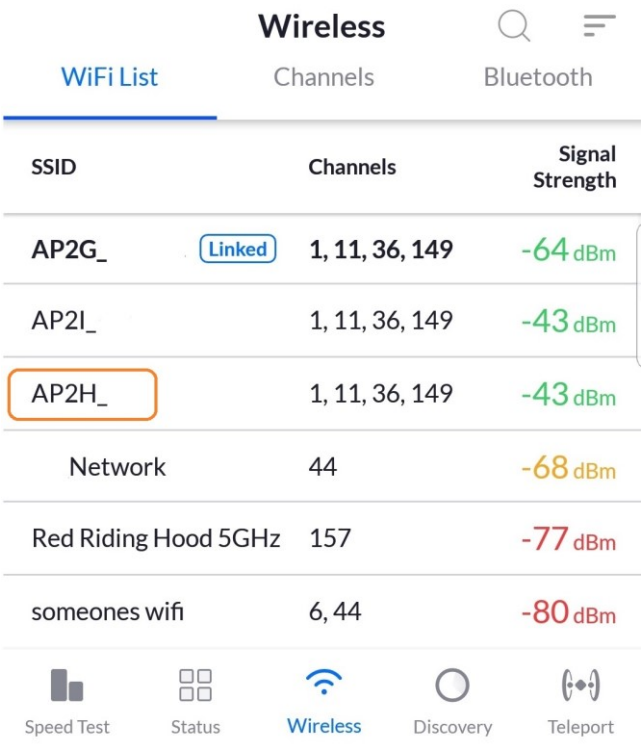


Figure 170 – WiFiMan WiFi-List Screenshot

I have a two story house with a basement. I am currently running two Ethernet-wired APs.
The upstairs AP is mounted near the ceiling of the second floor and is pointing down. This AP is set to Channel 149 / Channel 11. My second AP is positioned on a table in the basement pointing up, and is set to Channel 36 / Channel 1.

I used WiFiman running on an Android phone to perform a household (site) survey. As well as gathering data under / near each AP, I also gathered data at each location within my house which would host either a stationary or a roaming Wi-Fi device. Reference item #7 of @AlexWilsonsBlog's comment on page 150.

At each location, I measured and recorded what dBm signal strength was **received by a device**, from **each U**AP. Examples of this will be shown in Figure 171 – WiFiMan dBm Screenshots. Note that each AP's original transmit power will be attenuated when it finally reaches the device: by walls, floors, & distance.

While at that location, I also recorded the device's signal strength **received at the AP**, from the device, after attenuation by walls, floors, & distance. See Figure 172 – UniFi's Received Signal Value. These dBm signal values can be acquired by clicking on UniFi's Clients tab (circled in Red within the figure) and recording the dBm value under the Signals column (shown underlined in orange within the figure). I like leaving my Clients page sorted by Signal Strength (shown circled by green). Signal strength sorting will put potentially poorly performing devices at the bottom of the list.

Note that each of your Wi-Fi devices may be capable of transmitting a different power level, but since I am using the same mobile device across this site survey, the values provided will be relative-to-each-other / representative dBm values.

For device received signal strength examples, see Figure 171 – WiFiMan dBm Screenshots. , where the:

Left picture: Measurement taken in the basement, basement AP is strongest.

Middle picture: Measurement taken on the first floor, both APs are about equal.

Right picture: Measurement taken on the second floor, upstairs AP is strongest.

For clarity, I have grouped / circled the upstairs AP with orange lines and grouped / circled the basement AP with blue lines.

Per sections above, both of these APs are each set to a 2.4GHz power level of Custom / 13dBm; and each 5GHz power level is set to Custom / 20dBm. Note that on the first floor (middle) screenshot, each AP's power is about equal to the other AP, and there is a 3dBm relative value between each AP's 2.4 GHz and 5GHz power levels, slightly favoring 5GHz.

[It looks like using multiple APs, adjusting the minimum data rates, and lowering the power levels really works for good roaming!]

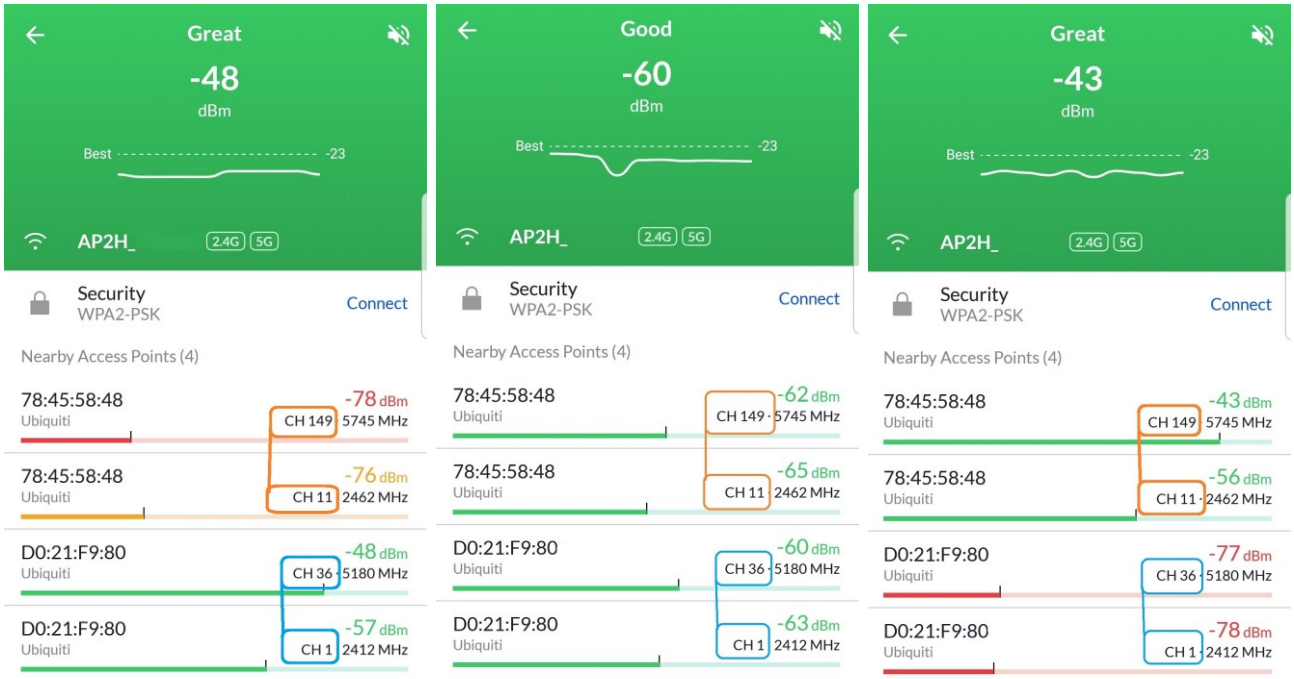


Figure 171 – WiFiMan dBm Screenshots

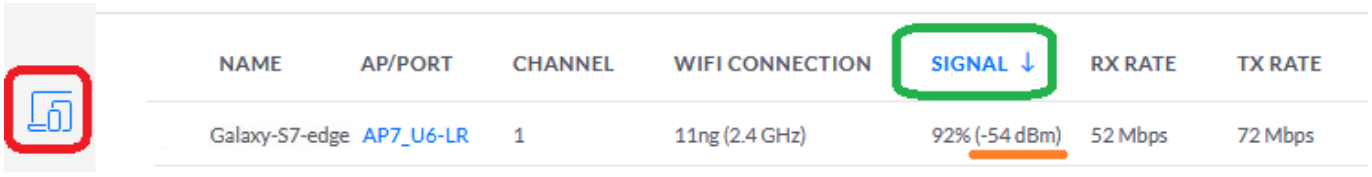


Figure 172 – UniFi's Received Signal Value

77.16 RSSI UI.com References.

UniFi - Understanding and Implementing Minimum RSSI
https://help.ui.com/hc/en-us/articles/221321728

Finding minimum RSSI
https://community.ui.com/questions/Finding-minimum-RSSI/788be046-bb21-44e5-946e-643c0fa3257b#answer/5c5f4997-6803-491e-8ca5-53c4dd9f2016

77.17 More UI.com References.

How do I turn off 2.4Ghz on half my APs?
https://community.ui.com/questions/How-do-I-turn-off-2-4Ghz-on-half-my-APs/8a040c73-eae7-4573-9cbc-6b20c4fb04f5

Some channel number charts
https://community.ui.com/questions/Better-explanation-for-DFS-Radar-channel-width-wanted/46f27c47-926a-476b-8dc0-c92827cb01bc#answer/cb73d31a-b04d-454c-a653-1f566d7c556d

W-Fi speed expectations / speed table [~ 2020]
https://community.ui.com/questions/nanoHD-speed-issues/b617d157-5d56-4a73-bb71-ac0bddd0046a#answer/908e276f-5528-443f-b150-91ac7909b8d2

How to tell which frequency a client is connected too
https://community.ui.com/questions/Unifi-Pro-how-to-tell-which-frequency-a-client-is-connected-too/239748a3-517e-4229-86fe-684ae1f9da96

Band Steering Settings
https://community.ui.com/questions/Band-Steering-Settings/31885afb-9ba1-404d-b2c6-0c4898e5afc3#answer/44c36c99-b037-45c6-a827-06f165c4a303

77.18 Some Other Wi-Fi References.

About wireless roaming for enterprise
https://support.apple.com/en-us/HT203068

https://en.wikipedia.org/wiki/List_of_WLAN_channels

https://metis.fi/en/2018/02/5ghz-channels/

https://www.extremenetworks.com/extreme-networks-blog/2-4-ghz-channel-planning/

https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ac.php

http://www.revolutionwifi.net/revolutionwifi/2013/03/80211ac-channel-planning.html

https://www.silextechnology.com/unwired/changes-to-the-5ghz-wi-fi-band-in-the-uk

78. Troubleshooting UniFi / Wi-Fi Performance

UniFi Help References:

UniFi - Troubleshooting Slow Wi-Fi Speeds
https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Troubleshooting-Slow-Wi-Fi-Speeds

UniFi – Troubleshooting Client Specific Connectivity Issues
https://help.ui.com/hc/en-us/articles/360013106453-UniFi-Troubleshooting-Client-Specific-Connectivity-Issues

UniFi - Troubleshooting Connectivity Issues
https://help.ui.com/hc/en-us/articles/221029967

UniFi - Identifying Wi-Fi Issues with Debugging Metrics
https://help.ui.com/hc/en-us/articles/115012700547

UniFi – Performing a Wireless Site Survey
https://help.ui.com/hc/en-us/articles/360037694253-UniFi-Performing-a-Wireless-Site-Survey

Other References:

iPad cannot connect to Unifi Wi-Fi
https://community.ui.com/questions/iPad-cannot-connect-to-Unifi-WiFi/384e2724-4b22-4678-84e7-9bc35a3685a6#answer/ed584acb-7ccf-43d0-b1aa-132a3628e7e9

Very limited range on new AC-Pro setup
https://community.ui.com/questions/Very-limited-range-on-new-AC-Pro-setup/2f48b246-72e4-4bfe-a33a-ba31913332ba#answer/e7d8e952-6a38-4fec-9030-e38a5b7801f5

iPhone connectivity issues
https://community.ui.com/questions/iPhone-connectivity-issues/289135ff-20ab-4845-b73f-f2c99ac99cde

Unifi Wi-Fi Incorrect password message on client
https://community.ui.com/questions/Unifi-WiFi-Incorect-password-message-on-client/c0dcb5bb-b8b6-4c3e-9c16-b321120ec0b4?page=1

About wireless roaming for enterprise <Apple>
https://support.apple.com/en-us/HT203068

Selecting Columns:

To help with debugging, I selected Clients (on the left) -> ListView -> Menu (i.e. 3 vertical dots). This allows me to select what columns are shown. To see individual connection rates, I selected “Signal”, “Rx Rate” and “Tx Rate”. See Figure 173 – Selecting Client Columns. To make room for these new columns, I un-selected “Activity Up” and “Activity Down”, which I didn’t currently need.

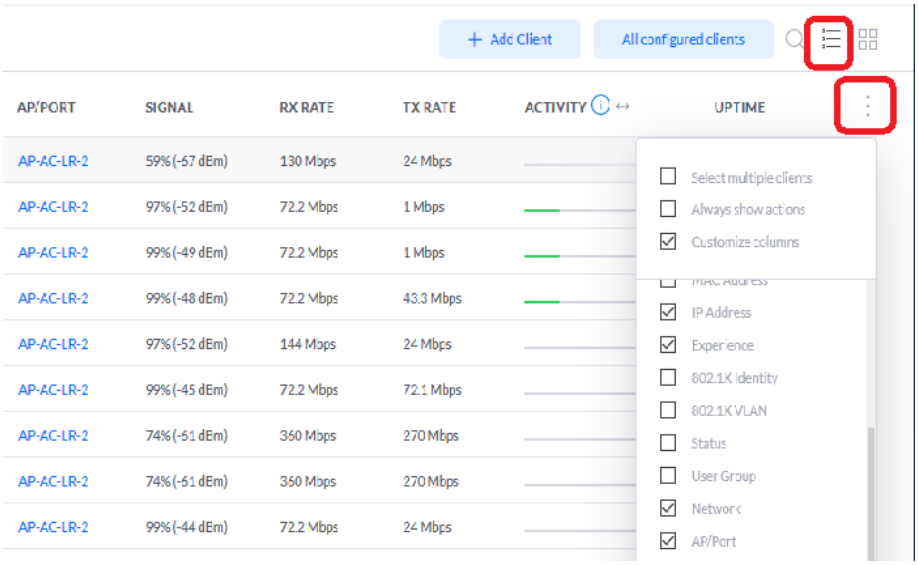


Figure 173 – Selecting Client Columns.

79. UniFi STUN / Channel Scanning

One of the references in section 77 - Setting UniFi / Access Point's SSIDs, Channels, and Power Levels mentioned performing a channel scan to determine the best (most-uncongested) Wi-Fi channel. When I tried to do a channel scan, I got an error similar to "This device is not able to connect to the internal STUN server on your Controller. Please check if the device is able to reach the STUN server on port 3478".

I determined, via a STUN Troubleshooting guide, that a port-forwarding / NAT rule was needed in the ER-X. For this rule to operate, you must first reserve device addresses for your "UniFi Controller" and all of your Access Point(s) per Table 5 - Table of Reserved Address. Reserve the addresses for your "UniFi Controller" and all of your Access Point(s) by following section 87 - Reserving Device Addresses via DHCP. You may need to (cleanly shut-down and) re-boot these devices to ensure that they are using the newly reserved addresses.

To generate the needed Destination NAT rule, perform similar steps as contained in section 62 - Optional DNS Forcing of the WIFI_IOT_LOCAL Network, but enter the information from Figure 174 – STUN DNAT Rule Data.

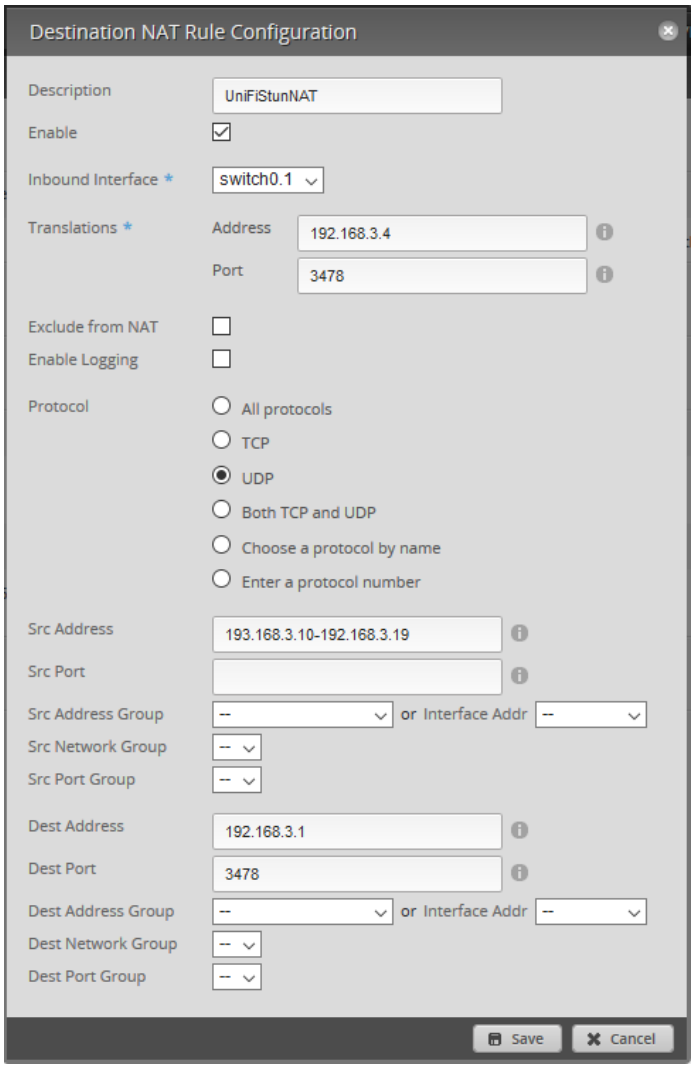


Figure 174 – STUN DNAT Rule Data.

For reference, here is the relevant portion from the backup file:

```
rule 3 {
    description UniFiStunNAT
    destination {
        address 192.168.3.1
        port 3478
    }
    inbound-interface switch0.1
    inside-address {
        address 192.168.3.4
        port 3478
    }
    log disable
    protocol udp
    source {
        address 193.168.3.10-192.168.3.19
    }
    type destination
}
```

With this rule, when the ER-X router sees an incoming UDP packet:

Addressed to 192.168.3.1 (i.e. itself, which is the default gateway device)

With a destination port of 3478

And a source address of 192.168.3.10 through 192.168.3.19, (i.e. from an Access Point)

it re-writes / re-transmits the packet to address 192.168.3.4 (i.e. the UniFi Controller)
with a destination port number of 3478 (i.e. unchanged port). This allows the Access Point's STUN requests / data to be able to be sent (indirectly) to the Unifi Controller, allowing processing.

To Channel Scan

For context on the following, reference text near, and also reference Figure 161 – UniFi Utilize a WLAN Group.
To channel scan, do the following:

1. Devices. (not shown)
2. <Your Access Point>. (not shown)
3. Tools Tab.
4. Expand the RF Environment item.
5. Select Scan.
6. <When the scan is finished> Select the band, 2G or 5G, to view results.

This will take your selected Access Point offline for several minutes while it performs the channel scanning. See Figure 175 – Channel Scanning Context.

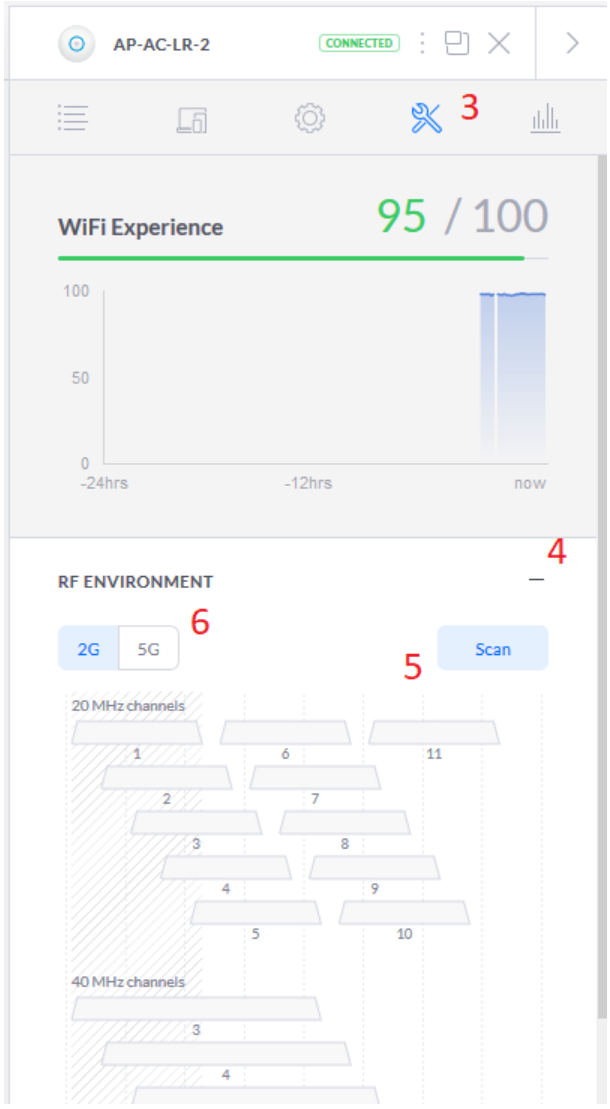


Figure 175 – Channel Scanning Context.

References:

UniFi Troubleshooting STUN Communication Errors
https://help.ui.com/hc/en-us/articles/115015457668-UniFi-Troubleshooting-STUN-Communication-Errors

Other scanning links:

https://community.ui.com/questions/Does-the-RF-Scan-feature-interact-with-Auto-channel-settings-or-not/351abcae-c81d-4fb9-8ce5-9fe1ac7dc8fc#answer/912f7eea-4eba-4638-aaba-6a754985d384

https://community.ui.com/questions/Unifi-AP-AC-roaming-functionality/91462665-59a7-4682-9cf1-df247220b3c9#answer/79f8d1e9-dec7-465f-a016-c9463f516221

80. UniFi Configuration Backup

Find the Settings button, near the lower left side of the screen, and press it. See Figure 142 – Settings Button. You should see the Maintenance Tab of the Settings page. Press it. Reference Figure 176 – UniFi Maintenance Screen.

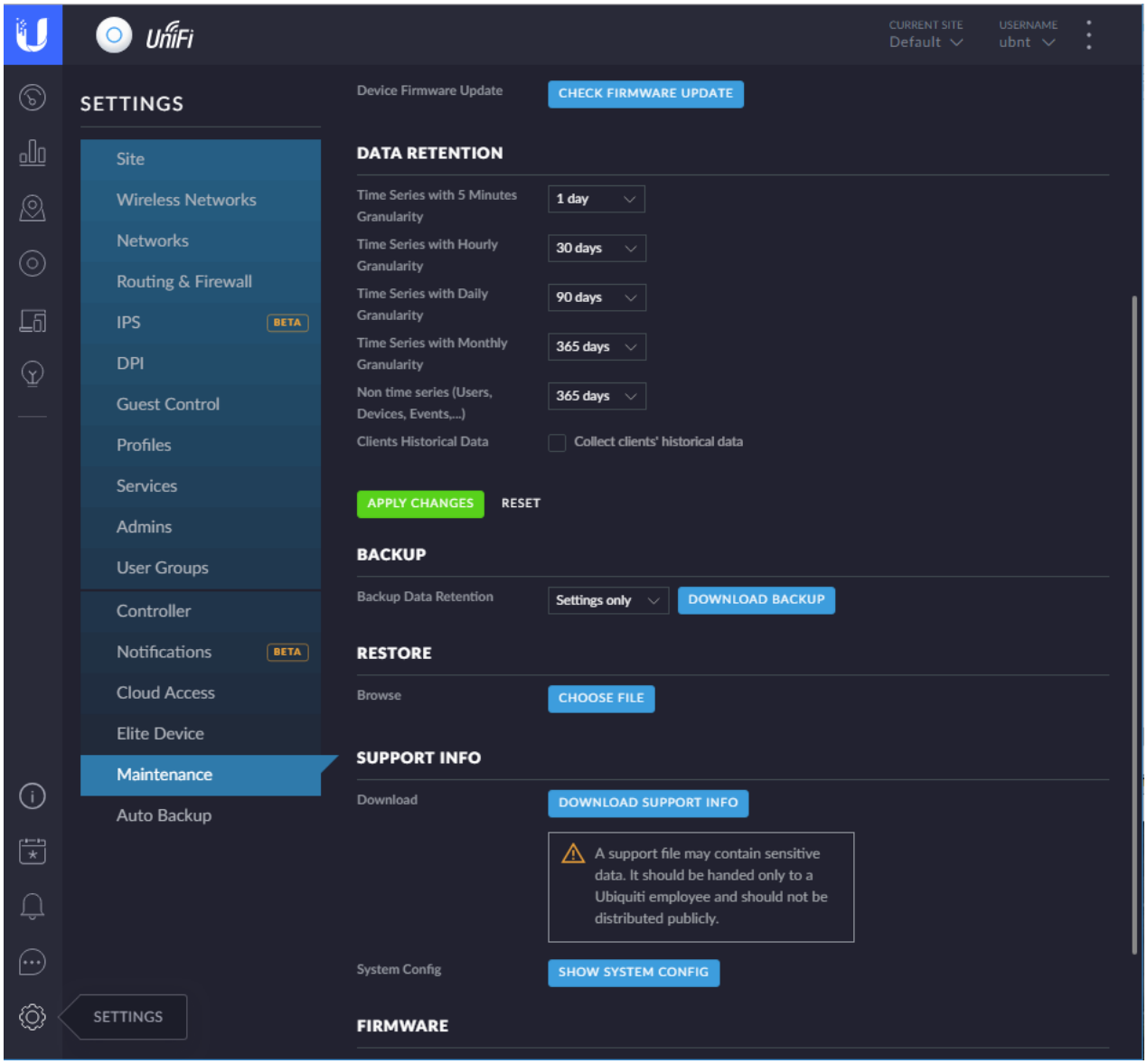


Figure 176 – UniFi Maintenance Screen

In the middle of this screen is a BACKUP section. Before I backup, I change my backup setting to be 'Settings only'. Press the 'DOWNLOAD BACKUP' button and store the resultant file. This is your Access Point configuration backup.

You can now exit the UniFi browser and close the UniFi Controller Software by pressing the X in the upper-right corner, as shown in Figure 124 – UniFi Controller Software Running. If you are running from a Cloud-Key or Raspberry Pi, you will want to shut it down cleanly. The UniFi Software utilizes a database, which does not like to have power abruptly removed.

https://help.ui.com/hc/en-us/articles/204952144

81. UniFi Interesting Links

Some Ui.com Training / Help Links:

UEWA Training Guide V2.1
https://dl.ubnt.com/guides/training/courses/UEWA_Training_Guide_V2.1.pdf

UniFi - 802.11 Basic & Supported Rate Controls
https://help.ui.com/hc/en-us/articles/115006559827-UniFi-802-11-Basic-Supported-Rate-Controls

UniFi - Identifying Wi-Fi Issues with Debugging Metrics
https://help.ui.com/hc/en-us/articles/115012700547-UniFi-Identifying-Wi-Fi-Issues-with-Debugging-Metrics

UniFi - Understanding and Implementing Minimum RSSI
https://help.ui.com/hc/en-us/articles/221321728

UniFi - Methods for Capturing Useful Debug Information
https://help.ui.com/hc/en-us/articles/227129127

More Ui.com Links:

Problems-with-Dropped-and-Retries (Disable the Uplink Connectivity Monitor)
https://community.ui.com/questions/Problems-with-Dropped-and-Retries/1af4f492-a829-4d90-8ea4-5c7dc7caedf4#answer/2b4fdafb-01c1-4dc4-ba1d-d3bc9cd24d83

82. End of UniFi / Access Point Setup

This is the end of the Access Point / UniFi Software / UniFi Controller setup.

The following sections are additional ER-X / EdgeRouter configuration steps.

83. Timed Based ER-X Firewall Rules

Several people have wanted to restrict their children's Internet usage based upon time. Here are some sample links:

https://community.ubnt.com/t5/EdgeMAX/Restrict-WAN-Access-to-from-LAN-Clients-by-Specific-IP-By-Time/td-p/2083140

https://community.ubnt.com/t5/UniFi-Wireless/User-based-time-control-of-wifi-access/td-p/1490803

https://community.ubnt.com/t5/EdgeMAX/Time-control-parental-controll/td-p/1035259

https://community.ubnt.com/t5/EdgeMAX/Set-up-time-limits-for-kids-internet-access/td-p/1824135

https://community.ubnt.com/t5/EdgeMAX/Parental-controls-time-of-day-routing-content-filtering/td-p/1268520

84. Double-NAT

When one firewall/router is behind another firewall/router, that combination is called double-NAT. Each router performs Network-Address-Translation (NAT.) Each router will introduce a small time delay as it processes IP packets. If you are running a server behind your (inner) router, then Double NAT can be particularly difficult to configure. Most people in the Ubiquiti forums hate Double-NAT.

Once the EdgeRouter 's firewall has been enabled / configured, the EdgeRouter can (but does not have to) be your main and only router. Remember to replace and then remove the default 'ubnt' login before using the ER-X as your internet facing router.

85. Configuring a Second / Testing ER-X

It is handy to have a second, already-configured, ER-X on hand as a cold spare. If you are considering using "Adblocking and Blacklisting" from section 88, you could configure one ER-X with Adblocking and one ER-X without Adblocking. Testing that feature is now as easy as the five minutes it takes to swap routers.

To configure a Second/ Testing ER-X, it is important that the IP address presented to the WAN port NOT be within one of our internal IP address ranges. Reference section 6 - EdgeRouter IP Address Use and Table 1 - Table of Networks for that data.

Normally your Setup/Testing PC would be wired directly (or through a switch) to your "Master" ER-X. See Figure 177 – Typical Testing PC Setup.

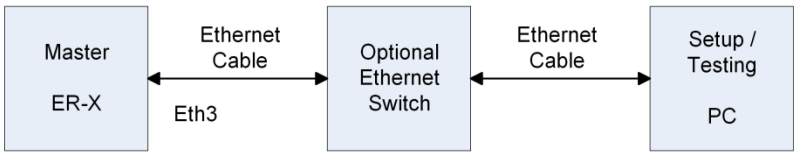


Figure 177 – Typical Testing PC Setup

One way of presenting a different IP address to the Second/Testing ER-X, is to insert your leftover consumer router (with its LAN configured for 192.168.[0,1,2].X) before your Second / Testing ER-X router. The Testing ER-X then connects to your Setup/Testing PC. See Figure 178 – Second / Testing ER-X Wiring.

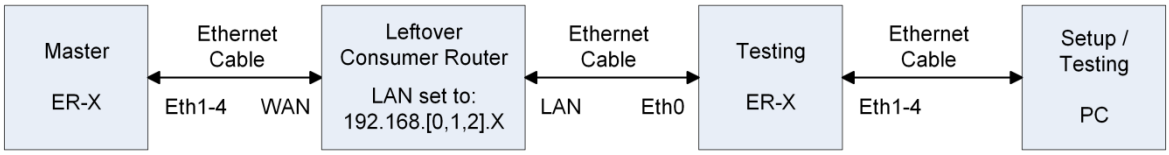


Figure 178 – Second / Testing ER-X Wiring

Another alternative is to use RFC-5737 addresses. @BuckeyeNet posted about them at:

https://community.ui.com/questions/Connecting-Two-ER-X-Routers/7e91a2f5-53c3-4ece-859a-558ab25d4940#answer/017707ac-e0eb-41e0-b58c-c2c30b35969

86. Ubnt Discovery

Recently,the Ubnt Discovery service has shown up in an EdgeRouter Community posting:

https://community.ubnt.com/t5/EdgeRouter/EdgeOS-responds-to-udp-10001-probes-even-if-service-ubnt/td-p/1886105

“The default WAN firewall policies added by the Basic Setup wizard will block all probes to UDP/TCP port 10001 and will prevent the EdgeRouter from being discoverable on the WAN.”
Per https://help.ubnt.com/hc/en-us/articles/204976244

If you still want to disable this service, the following may help you:

[UBNT-discover] - Add CLI command to disable "ubnt-discovery" daemon, thus ER will stop responding to discovery messages on 10001 UDP port. (**set service ubnt-discover-server disable**).
Reference https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-software-release-v1-10-0/ba-p/2233263

[Discovery] - UBNT discovery daemon can be configured to listen to TCP discovery requests (by default it listens to UDP only). This feature can be enbled with "set service ubnt-discover-server protocol tcp_udp" CLI command.
https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-software-release-v1-10-7/ba-p/2513718

87. Reserving Device Addresses via DHCP

DHCP normally issues an IP address to a device, when that device is powered up. Along with issuing an IP address, DHCP usually issues other settings to these devices, including DNS resolver addresses. The IP issued by DHCP is loosely associated with the device's (globally unique) MAC address. These IP addresses are managed by the DHCP server, and are allocated from a pool of addresses. For example, reference "Range Start" and "Range Stop" within Figure 62 – DHCP Server Details Dialog. The issued IP address is usually stays the same per device, but *can* change. Always having the same IP address can be useful for devices like servers, which may have external references to the device's IP address.

ER-X's DHCP server can be instructed to always offer the same IP address to a particular device. This is often referred to as *reserving* a DHCP / IP address. Ubiquiti calls their IP reservation menu "Static MAC/IP Mapping".

Note that you can instead internally configure most IP devices to have a "fixed" IP address. Sometimes fixing an IP address (within that device) is also referred to as setting a static IP address. Although named similarly, these methods are totally different.

Be warned that the router's DHCP server knows nothing about any device, which is internally configured to use a fixed IP address, since these devices do not issue a DHCP request upon powering up. As such, if a device's fixed IP address is within the DHCP's IP allocation range, your network may become unstable, as two devices cannot *legally* have the same IP address. Another disadvantage of Fixing IP addresses within each device, is that DNS resolver addresses also need to be hand-configured for these devices. For modern devices, running under an ER-X router, I see NO need to ever fix an IP address within a device. Instead reserve an IP address.

Reserving addresses (within the Router's DHCP table) has the added benefit that the rest of the DHCP settings continue to be presented to the device, i.e. any changed DNS resolver addresses.

Before you start reserving your own IP Addresses, other sections of this guide may depend upon specific reserved addresses for correct operation. I would suggest that you not reserve any of the addresses shown in Table 5 - Table of Reserved Address for your general purpose devices.

ER-X	(192.168.3.1)
Pi Hole 1	192.168.3.2
Pi Hole 2	192.168.3.3
UniFi Controller	192.168.3.4
Reserved / Future Use	192.168.3.5 - 192.168.3.9
Access Point 1 - 10	192.168.3.10 - 192.168.3.19

Table 5 - Table of Reserved Address

To reserve an IP address for a particular device, ensure that device is powered-on and connected to the Network it will reside on. Select the "Services" button. Reference Figure 52 – Services Button. Ensure that the "DHCP Server" tab is selected. Reference Figure 53 – DHCP Server Screen. Find the correct DHCP line for your Network; follow it to the right side, to the line's "Actions" button. Click the "Actions" button. You will be presented with a list of actions.

Choose “View Leases”, See Figure 179 – View Leases Button.

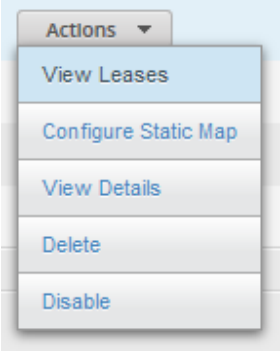


Figure 179 – View Leases Button.

You will be presented with a DHCP Server Dialog. This dialog will contain a list of your devices which have acquired a dynamic DHCP lease. See Figure 180 – DHCP Server Leases Dialog.

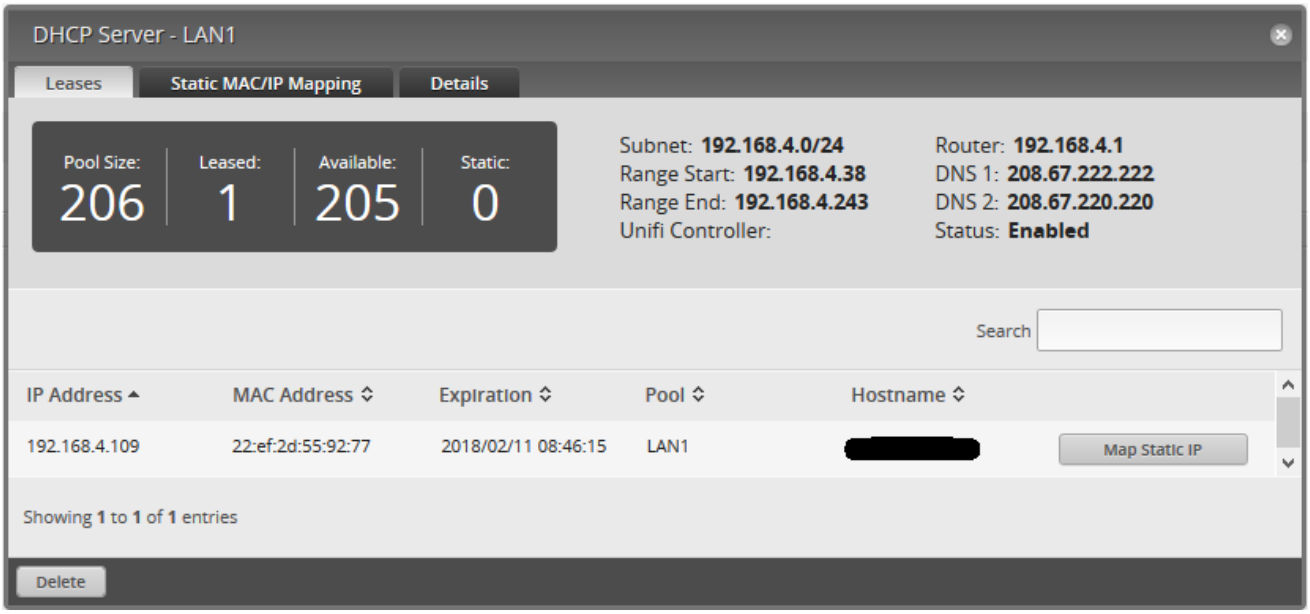


Figure 180 – DHCP Server Leases Dialog.

To reserve an IP address for that device, Press the “Map Static IP” button near the right side of the screen, for the correct device. You will be presented a dialog like Figure 181 – Static IP Mapping Dialog.

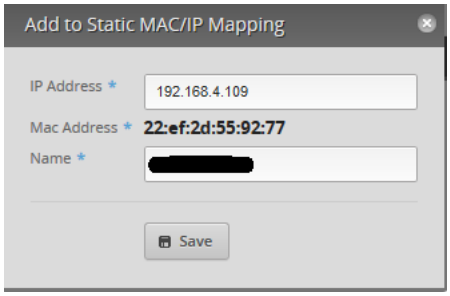


Figure 181 – Static IP Mapping Dialog.

You can modify the IP address to a different one or just leave it as is. If you modify it, only change the last octet (the last number). Press “Save”, then close the DHCP Server Leases dialog. If you modified the presented IP address, you will need to “release” and “renew” the devices IP address and/or reboot that device now. To view static IP reservations, find the Actions button, and click the “Configure Static Map” button. See Figure 182 – Configure Static Map Button.

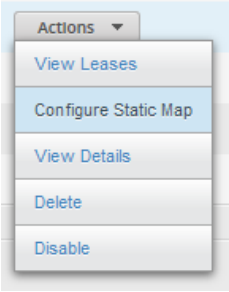


Figure 182 – Configure Static Map Button.

You will be presented with a list of reserved IP addresses for the chosen DHCP server. See Figure 183 – Static IP Mapping Dialog.

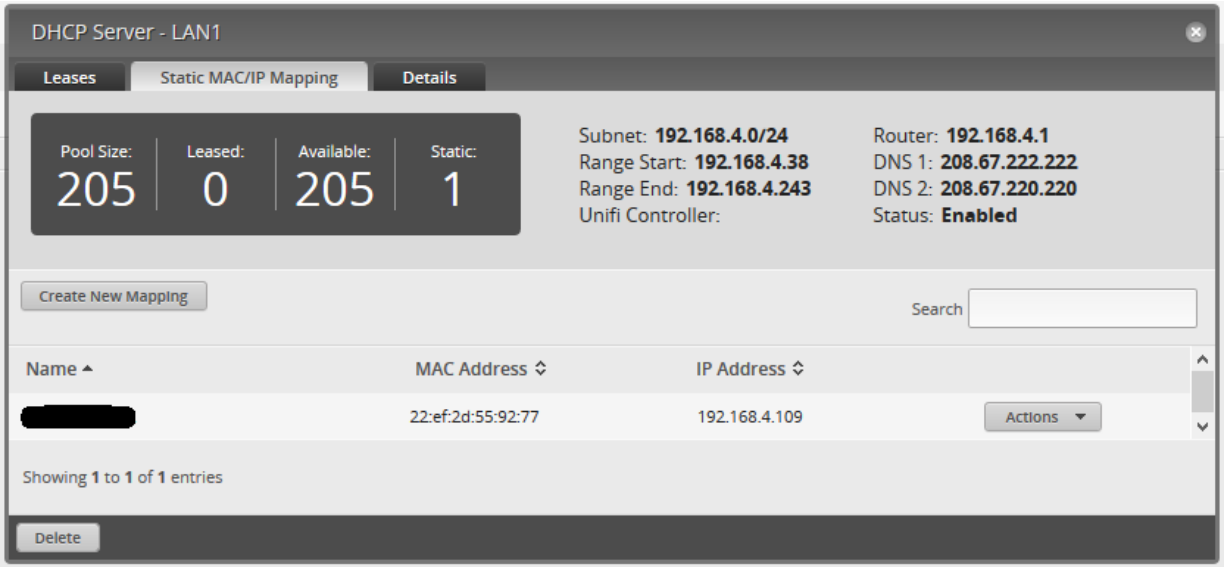


Figure 183 – Static IP Mapping Dialog.

Note also that the IP information presented under the “Static MAC/IP Mapping” dialog is un-changing, unlike the Leases page where devices (and associated lease information) may come and go as your devices are powered / un-powered.

Per the internet, you can use the CLI to issue a “show arp” command within the ER-X and see a list of connected devices. A similar Windows / Linux command is “arp –a”, but this command may not show every device.

88. Adblocking and Blacklisting

This is optional. This seems to work flawlessly. Also reference section 89 - Pi-Hole Network-wide Ad Blocking.

You should note before implementing this section that some web sites / web pages you may wish to visit will be blocked by this code. In some cases you may not be able to determine which URLs in the blocking lists are blocking which sites / page you want to visit, as some website links 'redirect' through advertisers' sites. These advertisers' sites will now be blocked. This includes some Google searches.

There are a number of similar posts with different version numbers. I had to use an SSH package (e.g. putty for Windows) to paste the following commands into the EdgeRouter, as the CLI doesn't seem to support copy / paste.

Reference:

> https://community.ubnt.com/t5/EdgeMAX/DNS-Adblocking-amp-Blacklisting-dnsmasq-Configuration/td-p/2215008
>
> https://community.ui.com/questions/DNS-Adblocking-and-Blacklisting-dnsmasq-Configuration-Integration-Package-v1-2-4-5/eb05f1b2-5316-4a80-8221-5e8b02575da4

See also: https://github.com/britannic/blacklist

The following text is cached from the above URL when the stated version was at V1.2.4.5 (i.e. January 2021). This installation is via a .deb package. An apt-get installation method is also available on that page.
You should check for updated information and use the newest code and any newer directions.

First ensure the router has enough space (2 lines):

```
sudo apt-get clean cache
delete system image
```

Installation (2 lines):

```
curl -L -O
https://raw.githubusercontent.com/britannic/blacklist/master/edgeos-dnsmasq-blacklist_1.2.4.5_mipsel.deb
sudo dpkg -i edgeos-dnsmasq-blacklist_1.2.4.5_mipsel.deb
```

Removal, if ever wanted (1 line):

```
sudo apt-get remove --purge edgeos-dnsmasq-blacklist
```

Upgrade:

> Since dpkg cannot upgrade packages, follow the instructions under Installation and the previous package version will be automatically removed before the new package version is installed

There is much more listed at this post.

When I installed this, I saw the following lines:

Total entries found: 95258
Total entries extracted 68054
Total entries dropped 27204

Some more links:

https://britannic.github.io/blacklist/#frequently-asked-questions

https://github.com/britannic/blacklist/blob/master/CHANGELOG.md

https://britannic.github.io/blacklist/#frequently-asked-questions

There is also an associated project located at: https://github.com/britannic/pixelserv (which I have not tried.)

Reference the following from his post:

dnsmasq may need to be configured to ensure blacklisting works correctly

Here is an example using the EdgeOS configuration shell

```
configure
set service dns forwarding cache-size 2048
set service dns forwarding except-interface [Your WAN i/f]
set service dns forwarding name-server [Your choice of IPv4 Internet Name-
Server]
set service dns forwarding name-server [Your choice of IPv4 Internet Name-
Server]
set service dns forwarding name-server [Your choice of IPv6 Internet Name-
Server]
set service dns forwarding name-server [Your choice of IPv6 Internet Name-
Server]
set service dns forwarding options bogus-priv
set service dns forwarding options domain-needed
set service dns forwarding options domain=mydomain.local
set service dns forwarding options enable-ra
set service dns forwarding options expand-hosts
set service dns forwarding options localise-queries
set service dns forwarding options strict-order
set service dns forwarding system
set system name-server 127.0.0.1
set system name-server '::1'
commit; save; exit
```

For testing, I picked a well-known advertisement site owned by Google. I tried and couldn't get there. Thanks to @britannic for this.

Also reference https://github.com/britannic/blacklist#frequently-asked-questions especially the section titled "EdgeOS dnsmasq Configuration". This appears to be the same text as above.

89. Pi-Hole Network-wide Ad Blocking

I have not (yet) tried this. Looks VERY interesting. Also Reference sections 88 - Adblocking and Blacklisting and 90 - Other Security Items.

Reference:

https://pi-hole.net/

Ubiquiti Links (see also the entire threads, if needed):

https://community.ubnt.com/t5/EdgeRouter/Intercepting-and-Re-Directing-DNS-Queries/td-p/1554378/page/2

https://community.ubnt.com/t5/EdgeRouter/Redirect-Hard-Coded-DNS-w-EdgeRouter/m-p/2354331#M208753

Above links are from: https://community.ubnt.com/t5/EdgeRouter/Redirect-DNS-to-Pi-hole/m-p/2389150/highlight/true#M212068

More Links:

https://community.ui.com/questions/Redirect-all-DNS-requests-to-pi-hole/8da9f082-147f-4185-a647-f4d454ec0ec4

https://community.ui.com/questions/Force-clients-to-use-pihole-as-DNS/8013d6ff-c29a-4c2b-8cd2-89cc15ee763b#answer/2f0843a6-4d19-45ae-b5d4-c98b24b544b8

https://community.ui.com/questions/Help-Setting-up-Pi-Hole/3697b5c4-79d4-4a58-91d8-7409004237a5

https://community.ui.com/questions/SOLVED-Pi-hole-across-VLANs/0b309023-6672-4388-a360-3332594a5da6

https://community.ui.com/questions/Resolving-client-names-with-edge-router-in-pihole/683579ba-1477-4e86-9146-5f99d30e607f

https://community.ui.com/questions/Pi-Hole-DHCP-Behavior-can-ER-X-Do-This/14e9f753-72b0-4b28-abec-98a0de00de16

https://www.myhelpfulguides.com/2018/07/30/redirect-hard-coded-dns-to-pi-hole-using-edgerouter-x/

Other Links:

https://community.ubnt.com/t5/EdgeRouter/Redirect-DNS-to-Pi-hole/m-p/2718992

https://community.ubnt.com/t5/EdgeRouter/Please-help-me-work-out-how-to-set-up-DNS-details-inside/m-p/2745497

https://community.ubnt.com/t5/EdgeRouter/config-for-an-internal-DNS-server-pihole-works-but-client/m-p/2669894

https://community.ubnt.com/t5/EdgeRouter/ER-X-Pi-Hole-and-cross-interface-communication/m-p/2517626\

https://community.ubnt.com/t5/EdgeRouter/Forcing-DNS-to-PiHole-w-DNAT-Allowing-for-Backup-DNS-server/td-p/2458039

https://community.ui.com/questions/ER-4-PiHole-DNS-redirection/00cf6de7-20a2-42ff-b85e-32d37e7114a8

https://community.ui.com/questions/ERX-wont-failover-to-other-DNS-servers-if-Pihole-cant-be-reached/a2f26ae5-4ee9-48b4-84b5-485fe24c66b7

https://community.ui.com/questions/EdgeRouter-4-DNS-and-Pi-Hole/021fc6d7-4b03-4f9f-8dd9-40092c99e20f

https://community.ui.com/questions/Separate-eth1-and-eth2-for-IoT/882fbb23-4889-41c3-9ae2-67374cdba772

External Links:

https://www.derekseaman.com/2019/10/redirect-hard-coded-dns-to-pi-hole-using-ubiquiti-edgerouter.html

https://www.myhelpfulguides.com/2018/07/30/redirect-hard-coded-dns-to-pi-hole-using-edgerouter-x/

https://www.reddit.com/r/Ubiquiti/comments/7p457d/ubiquiti_edgerouter_x_with_a_pihole/

90. Other Security Items

Here are links to other security items. I have not tried any of these.

https://community.ui.com/questions/Emerging-Threats-Blacklist/62a9549e-ddae-4631-941d-b0878b2a13e0

https://community.ui.com/questions/GEO-IP-Blocking/8a641a12-1ed3-463f-9cb4-c685def85bf7?page=2

https://www.ipdeny.com/ipblocks/

91. Coalescing the Wired Iot and Wi-Fi Iot Networks

This section allows the coalescence of the Wired Iot and Wi-Fi Iot Networks. I HIGHLY recommend that this section be followed. Among other items, this combines the Wired IOT Network (as 192.168.4.X) and the Wi-Fi IOT Network (as 192.168.7.X) as a single Network / Subnet. This involves enabling switch0 to be VLAN Aware. There are other advantages to being VLAN Aware, see links, below.

When configuring switch0 to be VLAN Aware, it is important to NOT be connected to an EdgeRouter port which is using switch0. I used the Wired Separate Network (which is not in switch0, if you followed previous sections) for these re-configuration steps. I locked myself out of my ER-X EdgeRouter (and had to factory reset / reload the base configuration) about 4 times while researching and writing this section. You should generate an EdgeRouter backup, right now, if you are going to implement this.

To convert the ER-X to being VLAN Aware, perform the following.

Login to EdgeRouter.

The following (temporarily) allows the Wired Separate Network to access the EdgeRouter itself.

```
Firewall/NAT
    Firewall Policies
        WIRED_SEPARATE_LOCAL -> Actions -> Configuration
            Default Action: Accept
            Save Ruleset
```

Disconnect your computer's Ethernet cable from eth3 / Home Network. Wait 5 to 10 seconds. Re-connect your computer's Ethernet cable to eth2 / Wired Separate Network.

Open a new Browser window/tab and enter a URL of 192.168.5.1 and Login to the EdgeRouter.

Now we are connected to the EdgeRouter without using switch0.

Move the Home Network Address setup from switch0 to vid 1.

```
Dashboard
    Home Net switch0 -> Actions -> Config
        Config Tab
            Address:        No address
            Save

Dashboard
    Add Interface
        Add VLAN
            VLANID:         1
            Interface:      switch0
            Description:    Home Net
            MTU:            1500
            Address:        Manually define IP Address
                            192.168.3.1/24
            Save
```

Remove the address range from Wired Iot Network.

```
Dashboard
    Wired Iot Net / eth1 -> Actions -> Config
        Address:        No address
        Save
```

Remove firewall rules from Wired Iot Network.

```
Firewall/NAT
    Firewall Policies
            WIRED_IOT_LOCAL -> Actions -> Edit Ruleset
                Rules Tab
                    Rule 2-> Action -> Delete Rule, Yes
                    Rule 1-> Action -> Delete Rule, Yes
                Interfaces Tab
                    Set Interface --
                    Set Direction –
                    –Remove
                    Save Ruleset
            WIRED_IOT_LOCAL -> Actions -> Delete Ruleset, Yes
```

Delete the Wired Iot Network DHCP server.

```
Services
    DHCP Server
        WiredIotDHCP
            Actions Delete
            Yes
```

Move Home Network firewall rules from switch0 to vid 1

```
Firewall/NAT
    Firewall Policies
        HOME_OUT Actions -> Interfaces
            Interfaces: switch0.1
            Save Ruleset
```

Enable switch0 to be Vlan Aware.
Note: If the dialog gets stuck, click the Config Tab, then click the Vlan tab to refresh the dialog / size.

Note that I have added "`eth3 vid 6,7,8`" to this configuration, which is suggested but optional. This is needed, if you will ever be wiring extra Access Point(s) through an Ethernet switch connected to eth3. Reference Method1A/1B in section 12 - About Using Two or More Ubiquiti Access Points. This has the potential to "leak" VLAN data out port eth3 to any connected device, dependent upon your type and model of external switch. This should not be a problem; this is a home setup, not an enterprise. If you think devices are snooping / miss-behaving, they should certainly NOT be connect to the Home Network, maybe not even be connected to the IOT Network.

```
Dashboard
    Switch0 Config
        Vlan
            Vlan Aware Enabled checked
            eth0 UNCHECKED
            eth1 checked
            eth1 pvid 7
            eth2 UNCHECKED
            eth3 checked
            eth3 pvid 1
            eth3 vid 6,7,8
            eth4 checked
            eth4 pvid 1
            eth4 vid 6,7,8
            Save
```

Disconnect your computer's Ethernet cable from eth2 / Wired Separate Network. Wait 5 to 10 seconds.
Re-connect your computer's Ethernet cable to eth3 / Home Network. Open a new Browser window/tab and enter a URL of 192.168.3.1 and Login to the EdgeRouter

The following restores the Wired Separate Network firewall restrictions.

```
Firewall/NAT
    Firewall Policies
        WIRED_SEPARATE_LOCAL -> Actions -> Configuration
            Default Action: Drop
            Save Ruleset
```

If you followed an earlier version of this guide and still have WifiIotDHCP, you may want to rename it to be IotDHCP, with the following commands:

```
configure
edit service dhcp-server
rename shared-network-name WifiIotDHCP to shared-network-name IotDHCP
top
commit
save
exit
```

https://community.ui.com/questions/Rename-DHCP-server/4ecc159f-9774-4922-97f2-dc400065c92a#answer/e6cf5a55-9423-42fd-8736-6d6b0c011896

You may also want to change the DNS forwarding to match our now being VLAN aware. Similar to what was done in section 24 - dnsmasq and in section 30 - DNS Forwarding, enter the data shown in Figure 184 – DNS Forwarding, VLAN Aware. You will also need to press the “Apply” button, which is not shown.

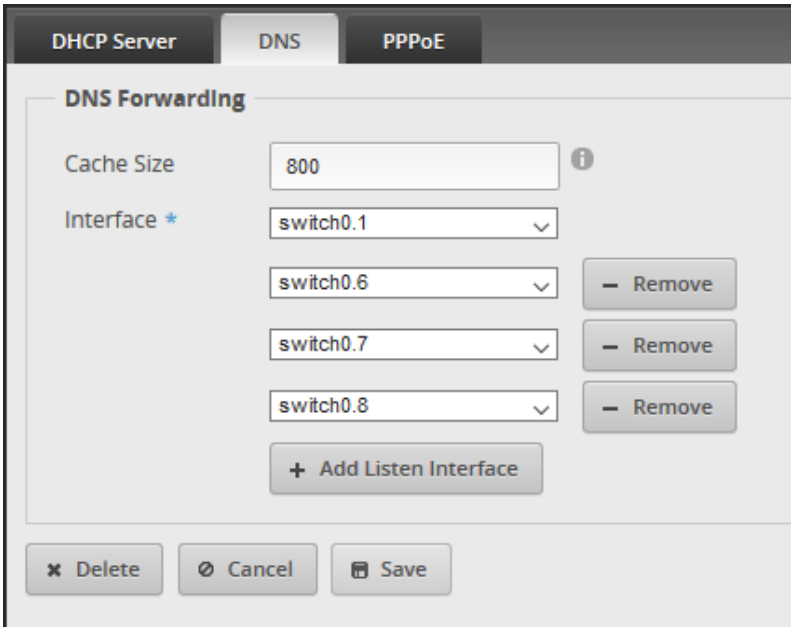


Figure 184 – DNS Forwarding, VLAN Aware.

At this point, I suggest that you backup your new configuration.

See also section 92 - So what is the meaning of PVID / VID?

General References:

https://en.wikipedia.org/wiki/IEEE_802.1Q

Collection of links, incl Ed Harmoush's Practical Networking site:
https://community.ui.com/questions/Setting-up-VLANs-using-Edgerouter-12P-and-Unifi-APs/cacbf252-6937-4665-b30d-a92b99db06b5#answer/a99bfdd3-3c41-4032-ac25-00d445b96853

An interesting switch command:
https://community.ui.com/questions/Edgerouter-X-Port-Mirroring-Issue/fdc37e51-0d3f-4b38-bf15-d92d57f5c84b#answer/4f64288a-2ef8-4310-ae26-37b32a143578

https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch

https://github.com/mjp66/Ubiquiti/issues/5

https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-Inter-VLAN-routing-issues-How-I-solved-it/td-p/1813187

https://help.ubnt.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRouter-as-a-Layer-2-Switch

https://community.ubnt.com/t5/EdgeRouter/Setting-VLAN-s-with-ERX-broke-it-completely/td-p/1917708

https://community.ubnt.com/t5/EdgeRouter/Edge-Router-X-as-Switch-with-VLAN-Need-Help/td-p/1992908

https://community.ubnt.com/t5/EdgeRouter/How-to-configure-EdgeRouter-X-as-switch-reposted-at-differnt/m-p/2635039/highlight/true

https://community.ubnt.com/t5/EdgeRouter/Edge-router-X-SFP-VLAN-s/td-p/1971128

https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch

https://community.ubnt.com/t5/EdgeRouter/riddle-me-this-ER-X-how-do-I-set-a-native-VLAN-on-the-switch/m-p/2667164/highlight/true

https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-VLAN-config-for-switch0-with-LAN-and-VLAN-on-same/m-p/2666616/highlight/true

https://community.ubnt.com/t5/EdgeRouter/locked-out-of-edgerouter-after-vlan-config/m-p/2557366

Differences between being VLAN Aware and NOT being VLAN Aware:

https://community.ubnt.com/t5/EdgeRouter/riddle-me-this-ER-X-how-do-I-set-a-native-VLAN-on-the-switch/m-p/2667164/highlight/true#M240023

https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-VLAN-config-for-switch0-with-LAN-and-VLAN-on-same/m-p/2666758/highlight/true#M239994

https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-VLAN-config-for-switch0-with-LAN-and-VLAN-on-same/m-p/2666758/highlight/true

There is also a discussion at https://github.com/mjp66/Ubiquiti/issues/35

This posting performs similar actions, but all from the CLI interface:
https://community.ubnt.com/t5/EdgeRouter/ERX-Unifi-VLAN-Guest-Portal/m-p/2755024/highlight/true#M249244

92. So what is the meaning of PVID / VID?

Reference these sections:

12 - About Using Two or More Ubiquiti Access Points
13 - Comments about Network Switches
91 - Coalescing the Wired Iot and Wi-Fi Iot Networks
101 - Add a Second Separate Network

Ethernet frames are similar in concept to internet "packets" but are what and how data travels over Ethernet wires. Network switches (hardware) connect devices on an Ethernet network by using packet switching to receive and forward data to destination device(s). This is analogous to using a router for managing the delivery of Internet Protocol (IP) packets.

The 802.1Q standard allows for additional VLAN tag data to be inserted into Ethernet frames. This insertion makes these VLAN –tagged frames slightly larger than the originally specified Ethernet frames. Any network equipment which is not 802.1Q compliant will discard VLAN frames as malformed. Ethernet frames which do not have a VLAN tag are said to be "untagged" i.e. use the original / native Ethernet frame size.

Reference https://en.wikipedia.org/wiki/IEEE_802.1Q

Using VLAN tagged data allows for different *logical-Networks* to be carried across a single Ethernet wire. VLANs are a principal method to accomplish isolation between network segments. The Networks described within this guide are Home Network=Untagged, Guest Network=Vlan6, IOT Network=Vlan7, and Spare Network=Vlan8. Only one group-of-data / Network can be un-tagged at a time, per Ethernet port (or it would not remain isolated).

Not all Ethernet connected equipment is capable of handling VLAN / tagged data. The Edgerouter (obviously) is quite VLAN capable. Ubiquiti Access Points (UAPs) are VLAN capable. UAPs which are configured per this guide expect VLAN tagged data for the handling of Guest, IOT, and Spare WiFi Networks into the UAP's single Ethernet port. VLANs keep the four SSID's data, separate.

Therefore, any network switch which is inserted between the Edgerouter and any / all UAPs needs to be capable of operating with VLAN tagged data, or as stated: be 802.1Q capable. If your APs don't receive any VLAN data, because an intermediate switch threw-away that data, then your Guest, IOT, and Spare WiFi Networks will not operate.

Reference the paragraph about testing network switches in section 13.

In section 91, the Edgerouter's eth3 (and eth4) ports were (identically) configured as:

```
eth3 checked
eth3 pvid 1
eth3 vid 6,7,8
```

This configuration translates to, in respective order:

```
Use the Edgerouter's (internal) VLAN-capable network-switch for eth3.
Direct Vlan 1(Home Network) data through eth3 as un-tagged.
Direct Vlan 6,7,8 data through eth3 tagged with their VLAN number(s).
```

So pvid selects what data goes through a port as un-tagged, while vid selects what-data (including how many VLANs) goes through a port using Vlan tags. Only zero or one `pvid` is allowed, but you can have zero, one, or multiple `vids` per port.

I believe that the ER-X's internal network switch can *only* manage VLAN (tagged) traffic. So all data entering this internal switch has to contain some tag value. In our use case, a (default) VLAN tag value of 1 is used by the ER-X's internal switch in conjunction with the (externally untagged) Home Network's data.

So when `pvid` is specified on a specific port, the VLAN tag data is removed from frames, when that data is transferred from the internal switch and sent out from that port. Similarly, VLAN tag data is added, when data received on that port is internally transferred into the VLAN aware switch. When `vid` value(s) are specified on a specific port, the VLAN tag data is untouched during transfer. If a VLAN is not included in either pvid or vid, that VLAN's data is not included for that specific port.

Reference Figure 1 - Overview Diagram.

In section 91, the Edgerouter's eth1 port was configured with:

```
eth1 checked
eth1 pvid 7
```

This configuration sends VLAN 7 (IOT) data out the eth1 port, but this data is first converted to be un-tagged when transitioning it to the eth1 port. Data received into eth1, will have the VLAN 7 tag inserted into that data before arriving at the ER-X's internal network switch, for correct internal operation. This is due to the specification of `pvid`, not `vid`. This allows any / all equipment wired to eth1, to be able to natively communicate with the eth1 port, even a directly-connected non-802.1Q piece of (cheap) IOT equipment.

With this knowledge, you could instead configure one of the Edgerouter's ports to use only non-tagged Spare Network data.

Want only Home Network data to appear on `eth3` because you can't let some device see VLAN data? Then remove the `eth3 vid 6,7,8` configuration portion, and connect your UAPs to eth4.

Remember that whatever Edgerouter port your UAPs are ultimately connected-to, you need that port to be configured with: `pvid 1` and `vid 6,7,8` to ensure correct UAP operation.

For an example GUI configuration, reference Figure 185 – Example PVID, VID settings. In this example eth1 carries untagged IOT Network data from VLAN 7. eth2 and eth4 are each separate Networks, which don't involve any VLANS. eth3 contains the un-tagged Home Network data, as well as the 3 (tagged) VLANs for connections to the UAPs. Some of this example is discussed in section 101 - Add a Second Separate Network.

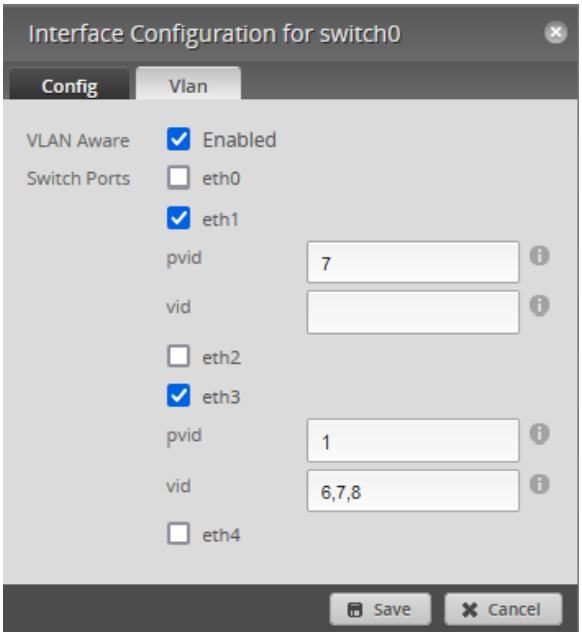


Figure 185 – Example PVID, VID settings

Managed switches are configured, per port, in a similar manner as above. Different configuration terminology may be used, but the concepts are the same:

Selecting what data is presented as un-tagged, per port.
Selecting which VLANs are presented, as tagged data, per port.
Excluding (VLAN Network) data from specific ports, either by specific exclusion rule or simply by omission.

Un-managed network switches give the user NO control over what data is presented to which port. The switch internally manages all transfer of data. A very simplistic view of an un-managed switch is that it transfers all data to everywhere.

Programming the above concepts into a *managed* switch is specific to each vendor. Managed network switches can also do much more than what is stated here.

If you use a *managed* switch, remember that whichever switch-port is connected to the Edgerouter's eth3 port, that switch-port, and all switch-ports connecting to UAP(s), needs to be configured with an equivalent of: `pvid 1` and `vid 6,7,8` to ensure correct UAP operation.

If you need even-more separate Networks (than the two which are available per this guide) or wanted additional /other-types of Networks (e.g. IOT2, etc…), you could expand the Edgerouter's configuration, by internally adding more DHCP servers and associated VLANs to the Edgerouter, then adding those new VLANs to eth3. A configuration like this *requires* an appropriately configured *managed* switch be connected to eth3. This configuration would effectively expand the Edgerouter's number of separately-configurable ports to include those of the *managed* network switch.

This is the power of a real (non-consumer) router. You have full control over which Network data goes to each of the Edgerouter's ports, and if that data is to be tagged or un-tagged. These items are individually controlled for each port. Data separation is maintained, even when multiple Networks share a single Ethernet wire. Additionally, this concept can be expanded to more ports, with the addition of a managed switch.

93. Simple Network Management Protocol (SNMP)

To enable the ER-X to be a source of SNMP data, first press the “System” button. Reference Figure 9 – System Button. Find the SNMP Agent section, fill-in the three fields, and check Enable. Press “Save”. See Figure 186 – Sample SNMP configuration.

The ER-X appears to support both version 1 and version2(c). Version 2 supports 64 bit counters. The only security available is to change the SNMP community string to something hard to guess. Most installations assume “public”.

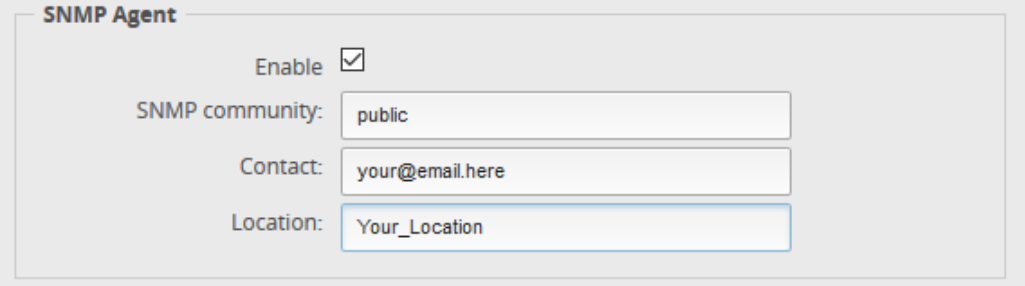


Figure 186 – Sample SNMP configuration.

There is a huge list of SNMP programs which could monitor you router. Some I have seen referenced are:

Snmpwalk	(Referenced in Appendix C)
Cacti	
NetworX / LibreNMS / PRTG	
Nagips / Zabbix / Dude	
OpenNMS	
MRTG	
Grafana / InfluxDB / Telegraf	(See Appendix C)

94. What devices should be placed on which Network?

Some devices could go either on the Home Network or on the Iot Network.

I'll use an Amazon Echo as the first example. The echo can execute just fine from the Iot Network. The Echo typically uses a smart-phone app to control it. Your phone / tablet is typically attached to the Home Network. I presume that the Amazon's app is actually going out to Amazon's mother ship and then back to the Echo. The Echo could also be placed on the Home Network. Since the echo gets regular updates from Amazon, and Amazon is, presumably, smart enough to keep their device secure, I don't see having this device on the Home Network as a real problem.

Then there are devices I would NOT let on my Home Network. These are devices which don't receive firmware updates, devices which likely connect to some web service, or devices which ultimately come from Chinese manufacturers. My examples of these devices would be Baby Monitors / Security Cameras / the proverbial "Light Bulb" / etc... Who knows what is happening inside these devices firmware? Are there hard coded logins-passwords / open telnet ports / etc...? Hackers may be able to easily penetrate these devices, and then they are able to pivot and be inside the Network these devices are connected to.

If you can't tell or test the security of a device, if it is not being actively updated, or if it is from some unknown manufacturer, I'd put that device on the Iot Network. To me, these types of devices are not worth the risk of having them on my Home Network, right alongside my household personal computers.

This is ultimately a convenience vs security trade off. Choose carefully. By even having an Iot network, you can now choose which Network to put your stuff onto.

This is from a discussion at https://github.com/mjp66/Ubiquiti/issues/18

95. Device Discovery Across Networks / Subnets

This subject is complicated. This section and the next couple of sections are all related. Your mileage will vary, as everybody has a different set of equipment, which relies on different discovery methods. The Networks involved will typically be the Home Network and one or more of the Iot Network(s).

Help Link:

https://help.ui.com/hc/en-us/articles/115001529267-UniFi-Managing-Broadcast-Traffic

Related Links:

https://community.ubnt.com/t5/EdgeRouter/IOT-VLAN-multicast-still-not-working/m-p/2739880

https://community.ubnt.com/t5/EdgeRouter/Chromecast-traffic-between-VLANs/m-p/2381712

96. Multicast DNS

The use of MDNS between Networks, was suggested in https://github.com/mjp66/Ubiquiti/issues/29 with a link of: https://www.youtube.com/watch?v=1mjdkki2pIY

I believe MDNS allows clients to resolve host names within a subnet / Network. By adding multiple interfaces, this extends the service across multiple Networks. I don't know what security implications this extending might have.

The following interfaces may be different for you, depending upon what Networks you are trying to repeat / connect and if you choose to implement being VLAN Aware. Reference section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks. This example connects Home Net and Iot Net on a VLAN Aware system.

MDNS can be enabled via the CLI or via the Config Tree. To enable via the Config Tree, open up the service -> mdns -> repeater sub-menus. Enter in your interfaces, and then click Preview. See Figure 187 – MDNS Setup Example.

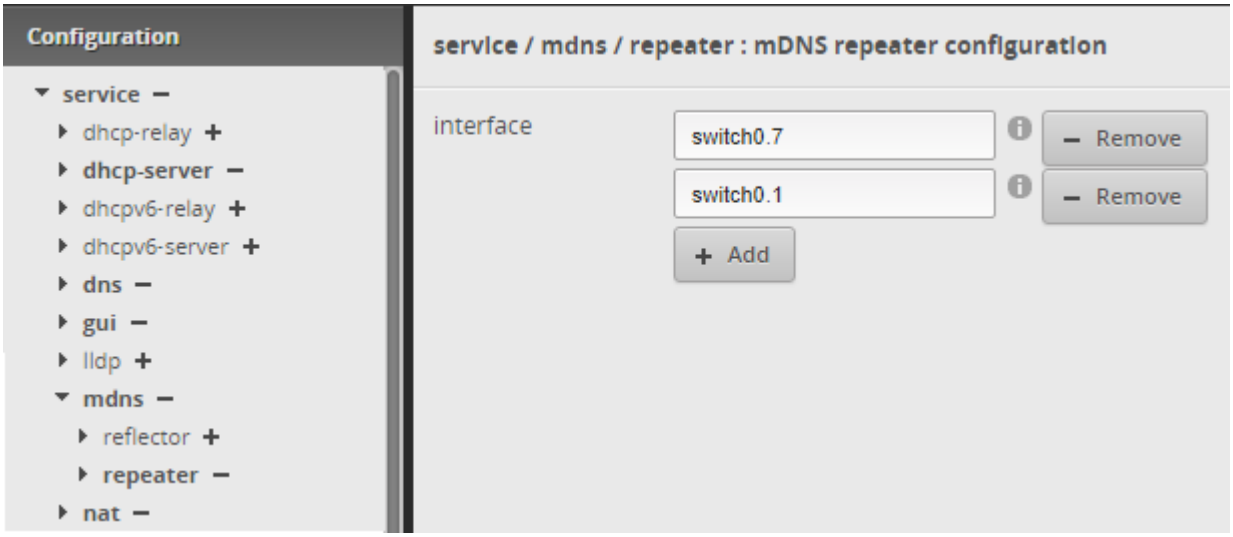


Figure 187 – MDNS Setup Example.

While trying to determine the impact of mdns, I had trouble disabling this feature via the Config Tree, so I used the following commands via the command line interface to disable this service.

```
configure
delete service mdns repeater
commit
save
exit
```

Note there is also a (similar?) mDNS reflector service, which is available.

Seems you will also need to allow UDP port 5353 through theEedgeRouter's firewall, to get mDNS to work. I was able to operate a Google Chromecast attached to the IOT Network, by a smartphone attached to the HOME Network, by allowing a firewall exception.

Attach the following rule to (WIFI_ / WIRED_) IOT_LOCAL:

```
rule 3 {
    action accept
    description "Allow mDNS"
    destination {
        port 5353
    }
    log disable
    protocol udp
    source {
        group {
        }
    }
}
```

See Figure 188 – MDNS Allow Port 5353 for IOT. for a screenshot of the same rule.

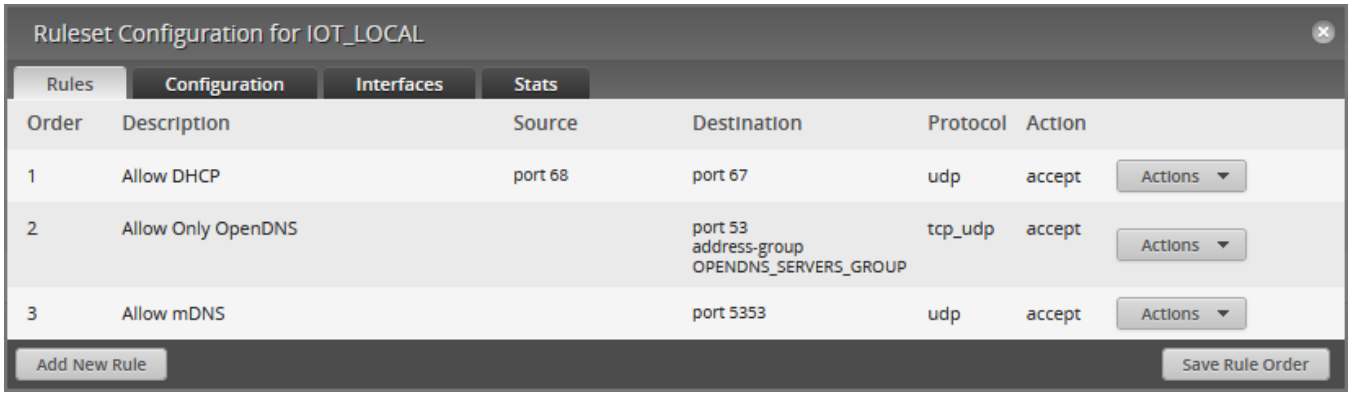


Figure 188 – MDNS Allow Port 5353 for IOT.

At one point while installing the Chromecast, I also added the following rule to HOME_OUT:

```
rule 60 {
    action accept
    description "Allow mDNS Discovery"
    destination {
        port 5353
    }
    log disable
    protocol udp
    source {
        group {
            address-group ADDRv4_switch0.7
        }
    }
}
```

I no longer have this rule enabled, and the Chromecast still seems to work, so this rule is probably not needed.

I have heard that some devices may (also OR instead) need port 1900 opened up, similarly to port 5353.

Reference the following links:

https://community.ui.com/questions/Chromecast-Discovery-Across-VLANs/b4916fcb-5806-4969-a730-9d2d82780b33#answer/1cc831fa-2028-4c76-9f1e-2001879a373a

https://github.com/mjp66/Ubiquiti/issues/47

See also the following posts:

https://help.ui.com/hc/en-us/articles/360035256553-EdgeRouter-mDNS-Repeater

https://community.ubnt.com/t5/EdgeRouter/mDNS-bonjour-forwarding/td-p/414093/

https://community.ubnt.com/t5/EdgeRouter/mDNS-forwarding-so-that-iPhone-can-communicate-with-iTunes-on-a/m-p/1752138/

https://community.ubnt.com/t5/EdgeRouter/Multicast-Sonos-Phorus-amp-Play-Fi-Broadcast-255-255-255-255-lt/td-p/1259616

TTL:
https://community.ui.com/questions/SOLVED-Broadcast-across-vlan-Alexa-mDNS-and-igmp-proxy/32b5244f-0466-40e2-ac82-2e4eceb355b9

Possible multiple interfaces:
https://community.ui.com/questions/MDNS-Repeater/d30f907b-a42c-45ca-848d-dfcf5d307ed0

97. Simple Service Discovery Protocol (SSDP) / igmp-proxy

SSDP is a discovery protocol used by Universal Plug and Play (UPnP.) Note that this protocol (SSDP) does not need to open holes in your WAN firewall to operate. This protocol uses UDP packets sent to a fixed IP address / port for discovering devices. I don't think this protocol was ever expected to work across two subnets i.e. two Networks.

I have been able to get the SSDP discovery packets to be transferred / copied from the Home Network to the Iot Network by using an igmp-proxy service. In order to get the SSDP replies back, I had to open up holes in the firewall from the Iot Network back into the Home Network. Not great, but what is needed if you want to discover devices on the Iot Network from a device on the Home Network. If I were opening up firewall holes, I would reserve IP address for the Iot device(s), and then only open (UDP) holes in the Home Out firewall for those specific device replies. Reference section 55 - HOME_OUT Firewall Rules and section 87 - Reserving Device Addresses via DHCP.

The following interfaces may be different for you, depending upon what Network you are trying to discover from which other Network, and if you choose to implement being VLAN Aware. Reference section 79. This example allows devices on the Iot Net to be discovered from the Home Net, on a VLAN Aware system.

To enable igmp-proxy, use the CLI / putty / SSH to issue the following commands:

```
configure
set protocols igmp-proxy interface switch0.1 role upstream
set protocols igmp-proxy interface switch0.7 role downstream
set protocols igmp-proxy interface switch0.1 threshold 1
set protocols igmp-proxy interface switch0.1 alt-subnet 0.0.0.0/0
set protocols igmp-proxy interface switch0.7 threshold 1
set protocols igmp-proxy interface switch0.7 alt-subnet 0.0.0.0/0
commit ; save
```

To check the igmp-proxy, issue the following commands (you may need to wait several seconds):

```
show ip multicast mfc
show ip multicast interfaces
```

To remove the igmp-proxy services, issue the following commands

```
configure
delete protocols igmp-proxy
commit ; save
```

My ER-X's igmp-proxy seems to restart, with no problems, after a controlled shutdown / restart.
This following link may or may not be relevant:
https://community.ubnt.com/t5/EdgeRouter/IGMP-proxy-not-starting-automatically-after-reboot/td-p/2095339

Reference these specifications (see Discovery sections):

http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf

http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v2.0.pdf

This is a weird protocol. The device doing the discovery sends out a UDP packet, somewhat formatted as HTTP-data, to a non-existing IP address of 239.255.255.250 with a destination port of 1900. SSDP listeners (somehow) receive this packet even though they are actually on a different (for us: 192.168.X.X) Network and (should) respond back to the sender's real (originating) IP address / port number with their "discoverable" information.

Now this gets even weirder. I have a Roku device on my Iot Network. It responded back TWICE, saying it was from address / port:

192.168.7.95 / 60000 (Correct)

and from

192.168.49.1 / 60000 (Incorrect)

The contents of the reply packets from the Roku each contained the correct IP address / port of the Roku:

"LOCATION: http://192.168.7.95:60000/upnp/dev/...".

for the discoverer to be able to contact the Roku device. The second packet (which was addressed to 192.168.49.1) broke through my original Home Out firewall rules. Reference updated rules within section 55 - HOME_OUT Firewall Rules. This is why I have switched over to using the full set of RFC-1918 addresses.

Here are some related links:

https://help.ubnt.com/hc/en-us/articles/360001004034-UniFi-Best-Practices-for-Managing-Chromecast-Google-Home-on-UniFi-Network

https://help.ubnt.com/hc/en-us/articles/204961854-EdgeRouter-Set-up-IGMP-proxy-and-statistics

https://community.ubnt.com/t5/UniFi-Routing-Switching/Configure-Sonos-across-subnets-on-USG/td-p/1979899

Here is a command to see what is going through the firewall on port 1900:

```
sudo tcpdump -i switch0.1 port 1900 -vv
```

98. socat - Multipurpose relay (SOcket CAT)

I have not tried this, but this is another tool for discovery across Networks / subnets.

Reference links:

http://www.dest-unreach.org/socat/

https://linux.die.net/man/1/socat

Other Links:

https://community.ui.com/questions/Howto-HDHomerun-discovery-on-different-LAN-segment/97db52c6-4add-4ba1-ab0d-27ee6f43db8f

http://www.cron.dk/edgerouter-and-chromecast/

99. Insecurity versus Convenience

Otherwise known as “Punching holes in your firewall”.

This example will involve allowing an SSDP reply from a specific IOT device to reach a specific HomeNet device.

Reference section 55 - HOME_OUT Firewall Rules. The HOME_OUT firewall has a bunch of Allow “Established / Related” rules, with one for each Network, followed by a drop of RFC-1918 addresses.

Reference section 97 - Simple Service Discovery Protocol (SSDP) / igmp-proxy. In SSDP, the querying equipment opens a (high) UDP port, sends out a UDP query to a destination port of 1900, and listens / receives replies which are sent back to the original (high) UDP port. The SSDP query data contains the originators IP address and the originators (high) UDP port number, so the responders know where to respond. This (high) port number may-not-be / is-probably-not at a fixed port number.

For the following rule to work, ensure that both devices have had their IP addresses reserved. Reference section 87 - Reserving Device Addresses via DHCP.

The following rule (inserted in HOME_OUT) would allow the 192.168.7.154 IOT device to reply back to the 192.168.3.81 HomeNet device with any UDP data to any UDP port:

```
rule 40 {
    action accept
    description "Allow Example IOT Reply"
    destination {
        address 192.168.3.81
    }
    log disable
    protocol udp
    source {
        address 192.168.7.154
    }
}
```

Related Links:

Secure IoT Network Configuration - YouTube -Crosstalk Solutions
https://m.youtube.com/watch?v=6EII8QeYbZQ

100. Allow Access to Cable/DSL Modem Device

We can punch a hole in our HOME_OUT firewall to allow accessing a Cable / DSL modem device. These devices typically serve web pages that allow you to check upon your modem device's status. You will need to know the IP address of your device. My device address, which will be used in this example, is 192.168.1.254.

To do this, Select:

Firewall/NAT -> Firewall Policies -> HOME_OUT -> Actions -> Edit Ruleset -> Add New Rule

Under `Basic` Tab, populate the following:

```
Description:     Allow Modem
Enable:          Checked
Action:          Accept
Protocol:        All protocols
```

Under `Source` Tab, populate the following:

```
Address:         <use your device's IP Address>
```

Click `Save, Cancel`.

Drag the `Allow Modem` rule above the `Drop RFC-1918 Traffic` rule, and then click the `Save Rule Order` button.

Your HOME_OUT Ruleset should now look similar to Figure 189 – Allow Modem Ruleset Result.

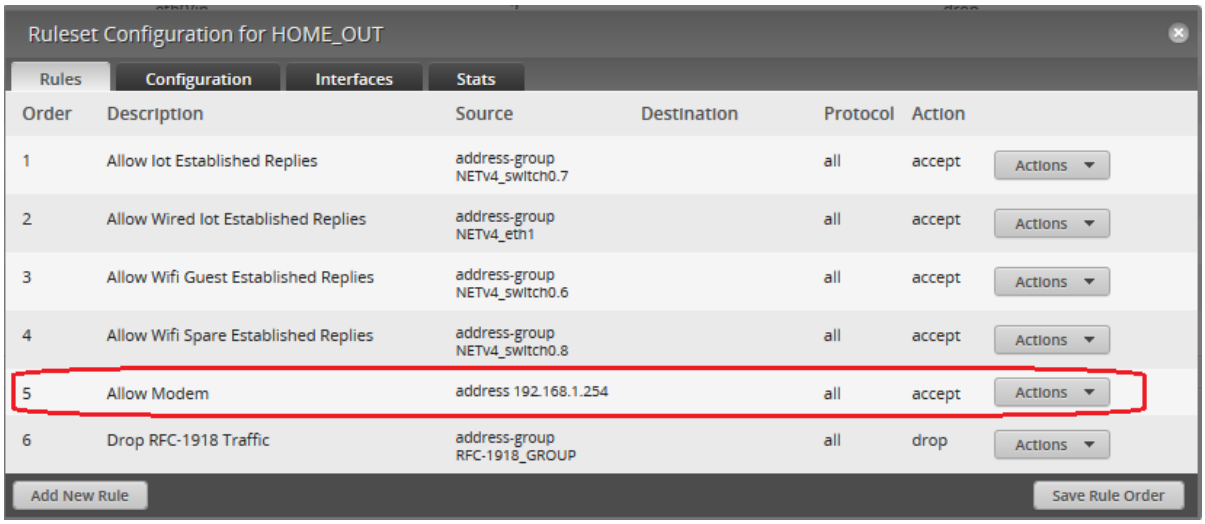


Figure 189 – Allow Modem Ruleset Result.

Here is the relevant HOME_OUT portion from the backup file:

```
        rule 50 {
            action accept
            description Allow Modem
            destination {
            }
            log disable
            protocol all
            source {
                address 192.168.1.254
            }
        }
```

101. Add a Second Separate Network

This is optional.

If you use an 802.1Q compatible network switch connected to eth3 AND you instead connect ALL of your Access Point(s) to this eth3 switch, you can free-up the eth4 port. This is what was described as Method1B in section 12 - About Using Two or More Ubiquiti Access Points. Switches were described in section 13 - Comments about Network Switches. Also reference section 92 - So what is the meaning of PVID / VID?

Eth4 can now become an additional separate network. This is handy for people who are working from home, and want to have two Separate Networks that exist apart from all the other Networks, e.g. have another Separate Network for WorkPCs

The following directions presume you have followed the steps in section 91 - Coalescing the Wired Iot and Wi-Fi Iot Networks. Ensure you backup your configuration *again*.

Go to the Dashboard tab, and select Actions / config for the switch 0 / interface line. Select the Vlan tab and uncheck eth4. This removes eth4 from switch0. Reference Figure 190 – Separate2 – remove eth4 from Vlan.

While on the Dashboard tab, select Actions / config for the eth4 interface line. Change the Description and manually define an IP address of 192.168.9.1/24. Reference Figure 191 – Separate2 – Add Address to eth4.

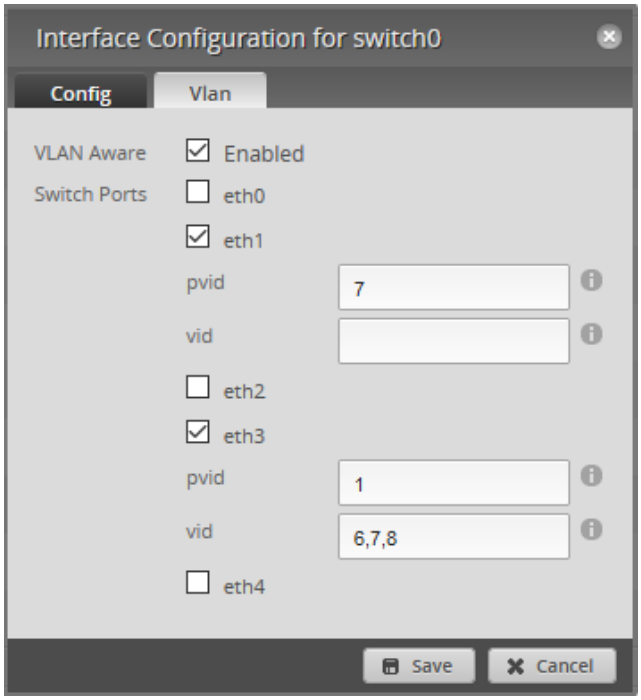


Figure 190 – Separate2 – remove eth4 from Vlan.

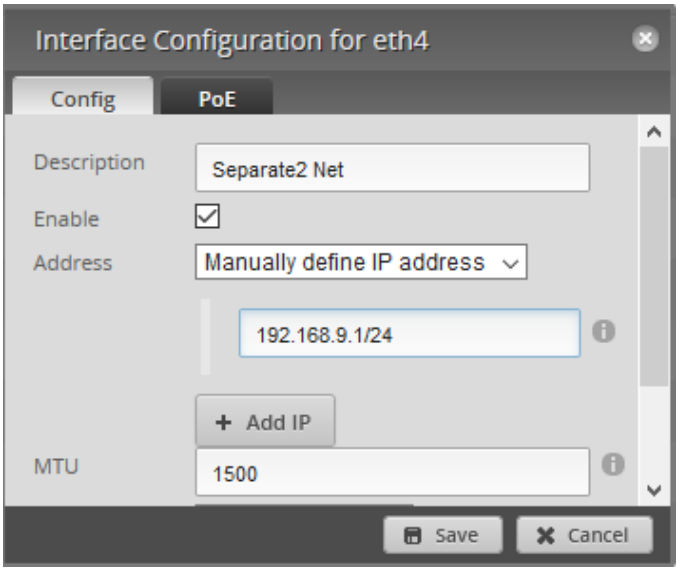


Figure 191 – Separate2 – Add Address to eth4.

Go to Services, DHCP Server tab, click on "+ Add DHCP Server" and fill-in the dialog, as shown in Figure 192 – Separate2 – Add DHCP. Use whatever DNS servers you wish.

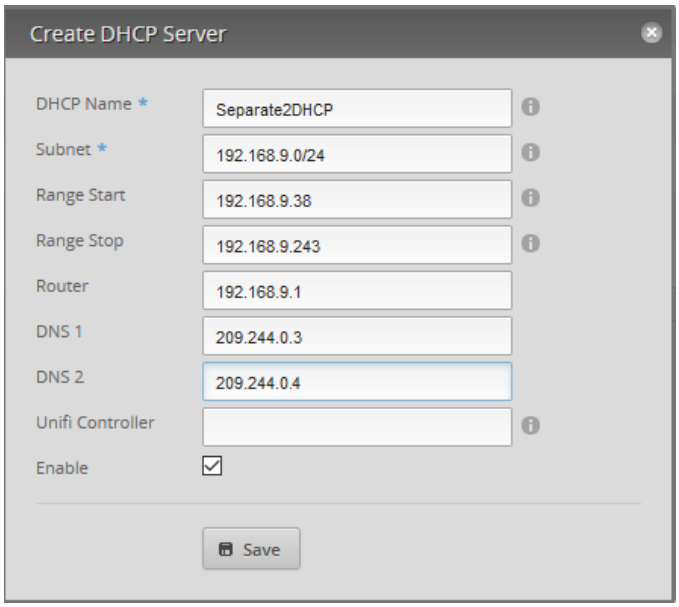


Figure 192 – Separate2 – Add DHCP.

Next, we need to copy three existing "Wired Separate" firewall rules into three new "Separate2" firewall rules. Copying existing rules is a lot easier than writing (the same) rules from scratch.

Start at the Firewall/NAT tab, and then select the Firewall Policies tab. Perform the (following) copy / modify set of steps, one set at a time. Some of the following figures for these modifications will only be shown for one set.

For each of "WIRED_SEPARATE_IN", "WIRED_SEPARATE_LOCAL", and "WIRED_SEPARATE_OUT" rulesets, select Actions / Copy Ruleset. Reference Figure 193 – Separate2 - Copy Ruleset.

You will be presented with a dialog to name the new ruleset. Apply the names "SEPARATE2_IN", "SEPARATE2_LOCAL", or "SEPARATE2_OUT". Reference Figure 194 – Separate2 – Name New Ruleset.

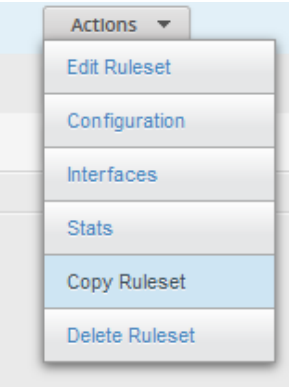


Figure 193 – Separate2 - Copy Ruleset.

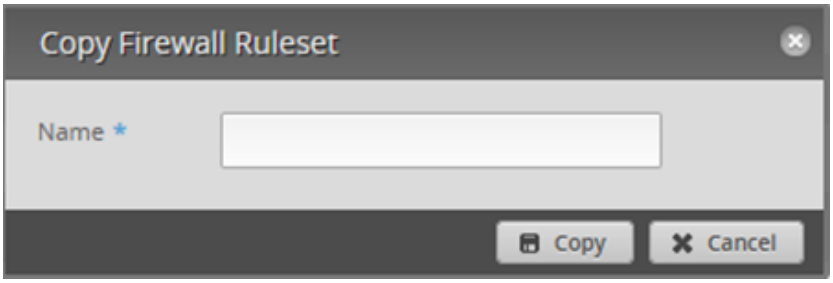


Figure 194 – Separate2 – Name New Ruleset.

For this new rulset, select action / configuration, and change the description. Reference Figure 195 – Separate2 – Edit Ruleset Configuration., which only shows one example.

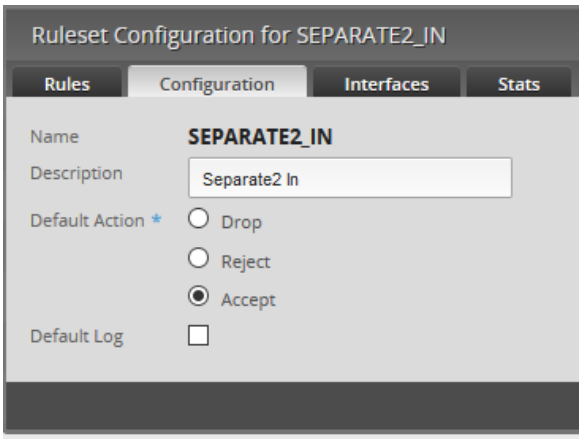


Figure 195 – Separate2 – Edit Ruleset Configuration.

Switch to the Interface tab, change the Interface to eth4 and the Direction as appropriate / matching the rule you are editing, i.e. one of in, local, or out. Reference Figure 196 – Separate2 – Edit Ruleset Interface., which only shows one example.

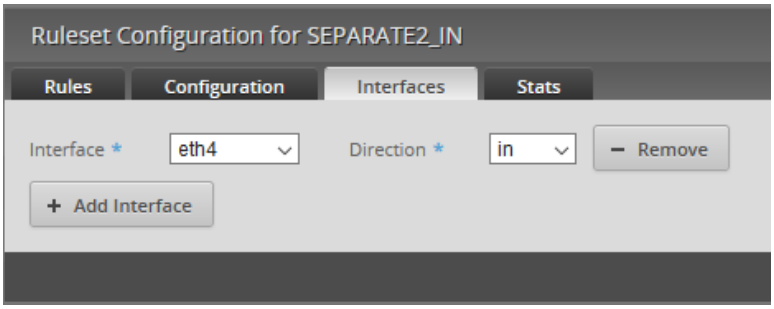


Figure 196 – Separate2 – Edit Ruleset Interface.

The matching configuration data is:

```
    name SEPARATE2_IN {
        default-action accept
        description "Separate2 In"
        rule 1 {
            action drop
            description "Block RFC-1918 Traffic"
            destination {
                group {
                    address-group RFC-1918_GROUP
                }
            }
            log disable
            protocol all
        }
    }
    name SEPARATE2_LOCAL {
        default-action drop
        description "Separate2 Local"
        rule 1 {
            action accept
            description "Allow DHCP"
            destination {
                port 67
            }
            log disable
            protocol udp
            source {
                port 68
            }
        }
        rule 2 {
            action accept
            description "Allow DNS"
            destination {
                port 53
            }
            log disable
            protocol tcp_udp
        }
    }
    name SEPARATE2_OUT {
        default-action accept
        description "Separate2 Out"
        rule 1 {
            action drop
            description "Drop Non-Separate2 Traffic"
            log disable
            protocol all
            source {
                group {
                    address-group RFC-1918_GROUP
                }
            }
        }
    }
```

102. Virtual Private Networks (VPN)

I have not played with or implemented a VPN. There seem to be several types. Here are some VPN links. Note that Wireguard is newer and possibility faster.

EdgeRouter - OpenVPN Server:
https://help.ubnt.com/hc/en-us/articles/115015971688

EdgeRouter - L2TP IPsec VPN Server:
https://help.ubnt.com/hc/en-us/articles/204950294-EdgeRouter-L2TP-IPsec-VPN-Server

EdgeRouter - Site-to-Site VPN Behind NAT
https://help.ubnt.com/hc/en-us/articles/115013382567-EdgeRouter-Site-to-Site-VPN-Behind-NAT

EdgeRouter - EoGRE Layer 2 Tunnel
https://help.ubnt.com/hc/en-us/articles/204961754-EdgeRouter-EoGRE-Layer-2-Tunnel

GUIDE: How to configure Local PPTP VPN:
https://community.ubnt.com/t5/EdgeRouter/GUIDE-How-to-configure-Local-PPTP-VPN-on-1-5-0-Firmware-works-on/m-p/971155

Private Internet Access Open VPN - Step by Step Configuration:
https://community.ubnt.com/t5/EdgeRouter/Private-Internet-Access-Open-VPN-Step-by-Step-Configuration/m-p/1711643

Troubleshooting-Site-To-Site-on-ER-Xs:
https://community.ubnt.com/t5/EdgeRouter/Troubleshooting-Site-To-Site-on-ER-Xs/m-p/2749611

Ubiquiti-edgerouter-ipsec-performance:
https://www.simonmott.co.uk/2018/08/ubiquiti-edgerouter-ipsec-performance/

OpenVPN vs L2TP:
https://community.ubnt.com/t5/EdgeRouter/OpenVPN-vs-L2TP/m-p/2659909

Secure OpenVPN server setup with multi-factor authentication (Google Authenticator): step-by-step:
https://community.ubnt.com/t5/EdgeRouter/Secure-OpenVPN-server-setup-with-multi-factor-authentication/m-p/1240405

OpenVPN configurator for EdgeMax
https://community.ubnt.com/t5/EdgeRouter/Helpful-Tool-OpenVPN-configurator-for-EdgeMax/m-p/2779412#M251490

Wireguard [New]:
https://community.ubnt.com/t5/EdgeRouter/Release-WireGuard-for-EdgeRouter/td-p/1904764

https://github.com/Lochnair/vyatta-wireguard
https://www.wireguard.com/

https://andrew.dunn.dev/posts/wireguard-from-your-isp/

https://www.erianna.com/wireguard-ubiquity-edgeos/

103. UNMS - Ubiquiti Network Management System

Barely played with this:

https://help.ubnt.com/hc/en-us/sections/115003321288-UNMS-Ubiquiti-Network-Management-System

https://help.ubnt.com/hc/en-us/articles/360008732414-UNMS-NetFlow

104. Intrusion Detection Systems

QUESTION: Which one to pick? How to configure it / connect it to the EdgeRouter?

@BuckeyeNet suggests Security Onion. Security Onion is at https://securityonion.net/ and https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecurityOnion

Seems to be rather involved. I have not tried Security Onion yet.

105. BuckeyeNet's link farm

@Buckeyenet invented and is the keeper of the best collection of UI data / links. Due to the materials size, there are multiple postings / links:

General Help and Main Page
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2

Initial Configuration for new users
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/9e65887e-8d98-40b9-868c-8f21023318d4

Troubleshooting Tips: Strategies and Tactics
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/8d61d318-e09a-42a1-b2ad-0d4b112666ec

Known EdgeRouter issues not tracked by Ubiquiti
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/505d87bb-3dc9-480a-87cd-7b96e7f928a7

Misc. Topics
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/a85a5f95-f506-466a-a54b-2b5d5c5f37b8

Some disturbing threads worth reading if you are a Ubiquiti customer.
If you only want good news, skip reading this post.
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/bf2b250d-2731-4838-b877-097d6218a69f

Routing topics
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/89d14ba1-39ec-4838-8571-396cb1b881bd

Unifi Firmware issues
https://community.ui.com/questions/BuckeyeNets-link-farm/d58f154d-8dd7-48a3-aba1-5d35fb84c9d2#answer/698d6513-d447-461c-964f-045d599f2961

106. Miscellaneous Links

This link seems like a wealth of information:
http://wiki.indie-it.com/wiki/Ubiquiti

The following are links I thought might be interesting:

Run script which disable/enables a firewall policy:
https://community.ubnt.com/t5/EdgeRouter/Run-script-which-disable-enables-a-firewall-policy/m-p/2724337

Forward port to PC on IoT Network:
https://community.ubnt.com/t5/EdgeRouter/Forward-port-to-PC-on-IoT-Network/m-p/2709401

UBRSS_Training_Guide_V1.2:
https://dl.ubnt.com/guides/training/courses/UBRSS_Training_Guide_V1.2.pdf

How to set up MTU properly:
https://community.ubnt.com/t5/EdgeRouter/How-to-set-up-MTU-properly/m-p/2337184

EdgeRouter - Configure an EdgeRouter as a Layer 2 Switch (Handy for a remote POE-powered Ethernet switch):
https://help.ubnt.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRouter-as-a-Layer-2-Switch

Measure instantaneous bandwidth usage over time:
https://community.ubnt.com/t5/EdgeRouter/Measure-instantaneous-bandwidth-usage-over-time/m-p/2554597

Help setting up NetFlow :
https://community.ubnt.com/t5/EdgeRouter/Help-setting-up-NetFlow/m-p/464367/highlight/true

Add Debian Packages to EdgeOS:
https://help.ubnt.com/hc/en-us/articles/205202560-EdgeRouter-Add-Debian-Packages-to-EdgeOS

Automating addition/removal of static-host-mapping table entries
https://community.ui.com/questions/Automating-addition-removal-of-static-host-mapping-table-entries/3ac3feee-61e3-43b1-a80a-7cec0d22fcba?page=1

Network configuration with 11 subnets of the same range possible?
https://community.ui.com/questions/Network-configuration-with-11-subnets-of-the-same-range-possible/db77258e-b500-41dd-93ec-a9ac3f79fe17

Edgerouter-X with multiple separate LANs with same IP range, possible?
https://community.ui.com/questions/Edgerouter-X-with-multiple-separate-LANs-with-same-IP-range-possible/778eed2a-875c-474b-b7c2-adfd9f6264f5

Ubiquiti Router Hardening. Note: Free Blog Post, But Paid Expanded Printed Copy, FYI Only.
https://www.manitonetworks.com/ubiquiti/2016/7/26/ubiquiti-hardening

Connecting a Harmony Hub (Disable 5GHz band just for IotWi-Fi)
https://community.ui.com/questions/Help-connecting-Logitech-harmony-ultimate-to-UNIFI-AC-PRO-or-AP-PRO/0cb1094f-a0fc-4bb1-9c10-e0d5784936ec

Troubleshooting rogue DHCP servers:
https://community.ui.com/questions/EdgeRouter-X-SFP-Randomly-Stops-Operating/774507e9-308d-45f7-a962-8488e9a7c922#answer/9067db55-454a-4a1a-9844-51cc9dd68322

How to temporarily disable some of the firewall rulesets in CLI:
https://community.ui.com/questions/How-to-temporarily-disable-some-of-the-firewall-rulesets-in-CLI/16b78471-ce5f-44ea-a1cb-2b83c3e0b501

How to capture packets on ER-X acting as a switch? (i.e. Switch commands)
https://community.ui.com/questions/How-to-capture-packets-on-ER-X-acting-as-a-switch/3a6154a5-04a9-4470-a083-51055e58caaf

QC Ubiquiti EdgeMAX - Capture Packets & Create PCAP Files (TCPdump)
https://www.youtube.com/watch?v=pj-uBX3azac
(Consider using /tmp for file storage, which is stored in DRAM instead of flash.)

Ubiquiti EdgeRouter Packet Capture - How-To:
https://www.youtube.com/watch?v=ei4hhquAd1U

EdgeRouter - Capturing Packets:
https://help.ui.com/hc/en-us/articles/204962304-EdgeRouter-Capturing-Packets

EdgeOS API Documentation
https://community.ui.com/questions/EdgeOS-API-Documentation/5aa67ddb-6480-45d8-8dfa-74c8f38120c5

How to run some commands from a custom script
https://community.ui.com/questions/How-to-run-some-commands-from-a-custom-script-Edge-Router-X/fb1487be-e6b0-4311-a613-d7942aaa52ba

Specific DNS Redirects
https://community.ui.com/questions/Specific-DNS-redirects/bfd23729-85b5-47a9-b030-2746d41a9d70

Tutorial Reconnect PPPoE every day at 6 AM using Task Scheduler only
https://community.ui.com/questions/Tutorial-Reconnect-PPPoE-every-day-at-6AM-using-Task-Scheduler-only/e904c9c4-aa5b-439a-b7d5-eb1134de9bf8

Install pihole on unifi cloudkey v1
https://www.reddit.com/r/pihole/comments/k3hthx/guide_install_pihole_on_unifi_cloudkey_v1/

AT&T blocks NTP
https://community.ui.com/questions/ATandT-Fiber-service-blocks-NTP-123-udp-outbound-Anyway-around-this/a0e90b20-591d-4224-a721-f53966262775

107. Conclusions

I hope that this guide helped you set up your Ubiquiti equipment, and that you have learned a lot.

Enjoy your new network.

-Mike

Appendix A. TP-Link TL-SG105EV2 Switch Setup

This section has nothing to do with the ER-X setup. This section is related to Method 1 of section 12, for using multiple Access Point(s). This section is now outdated, but has been left here as a reference.

[I have now used two different models of gigabit unmanaged switches, instead of configuring a managed switch to carry 802.1Q VLAN data to Access Points(s). I am amazed that I just plugged one in and it just worked, as I thought you needed a managed switch to carry VLAN data. This makes the rest of this section pretty much academic.]

Connect an 802.1Q capable switch to eth4, and then connect your Access Points to this switch. I have recently tested Method 1 using a TP-Link TL-SG105 (Ver 2.1) unmanaged gigabit switch, which was cheap and workedThe inexpensive Netgear switches should also work, I just happened to have Tp-Link models available for use. I believe these switches will need a hardware version of V2 or above to operate correctly. These directions are approximate.

I configured an additional AP-AC-LR Ubiquiti Access Point by referencing the “General” portion of section 12, and then following sections 70 through 75 for this additional Access Point.

I connected the Tp-Link switch to my computer, with the computer configured with a fixed address of 192.168.1.10. Reference section 9 for how to configure a computer’s Ethernet port. Using the Tp-Link software, I then configured this switch to have a specific 192.168.3.X address. After saving the configuration, I re-configured my computer back to DHCP, and re-connected the computer to the Home Network. I also connected the new switch to the Home Network. I then made a static reservation within the ER-X for this switch.

For this example, I will use and connect two Access Points to this switch. I choose port 4 and port 5 for those Access Point connections. I also choose port 1 of this switch to connect to the ER-X’s eth4 port.

Using the Tp-Link software, I selected the VLAN / 802.1Q VLAN page. See Figure 197 – Tp-Link Initial 802.1Q Dialog.

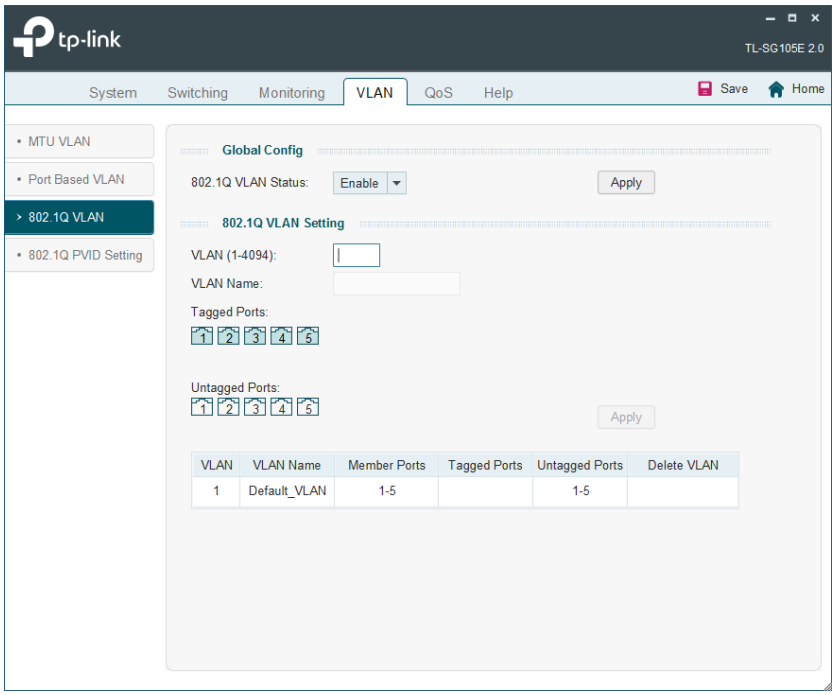


Figure 197 – Tp-Link Initial 802.1Q Dialog.

On the VLAN page, enable the Global Config.

Reference Table 1 - Table of Networks for the VLAN Networks used for this project. Enter the following information into the VLAN Page:

VLAN: 6
VLAN Name: WiFiGuest
Tag the ports: 1, 4, 5

See Figure 198 – Tp-Link VLAN 6 Configuration.

Press Apply

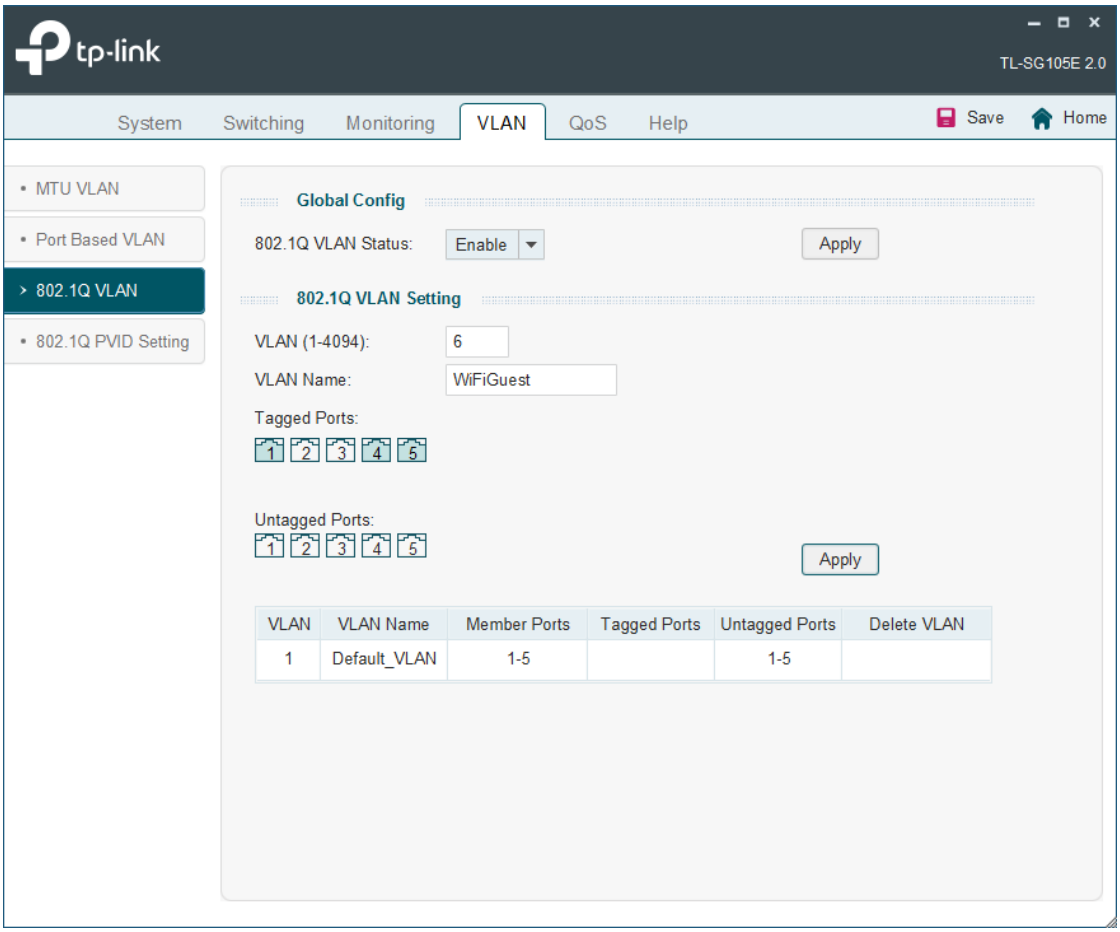


Figure 198 – Tp-Link VLAN 6 Configuration.

Enter the following information into the VLAN Page:

VLAN: 7
VLAN Name: Iot
Tag the ports: 1, 4, 5

See Figure 199 – Tp-Link VLAN 7 Configuration.

Press Apply.

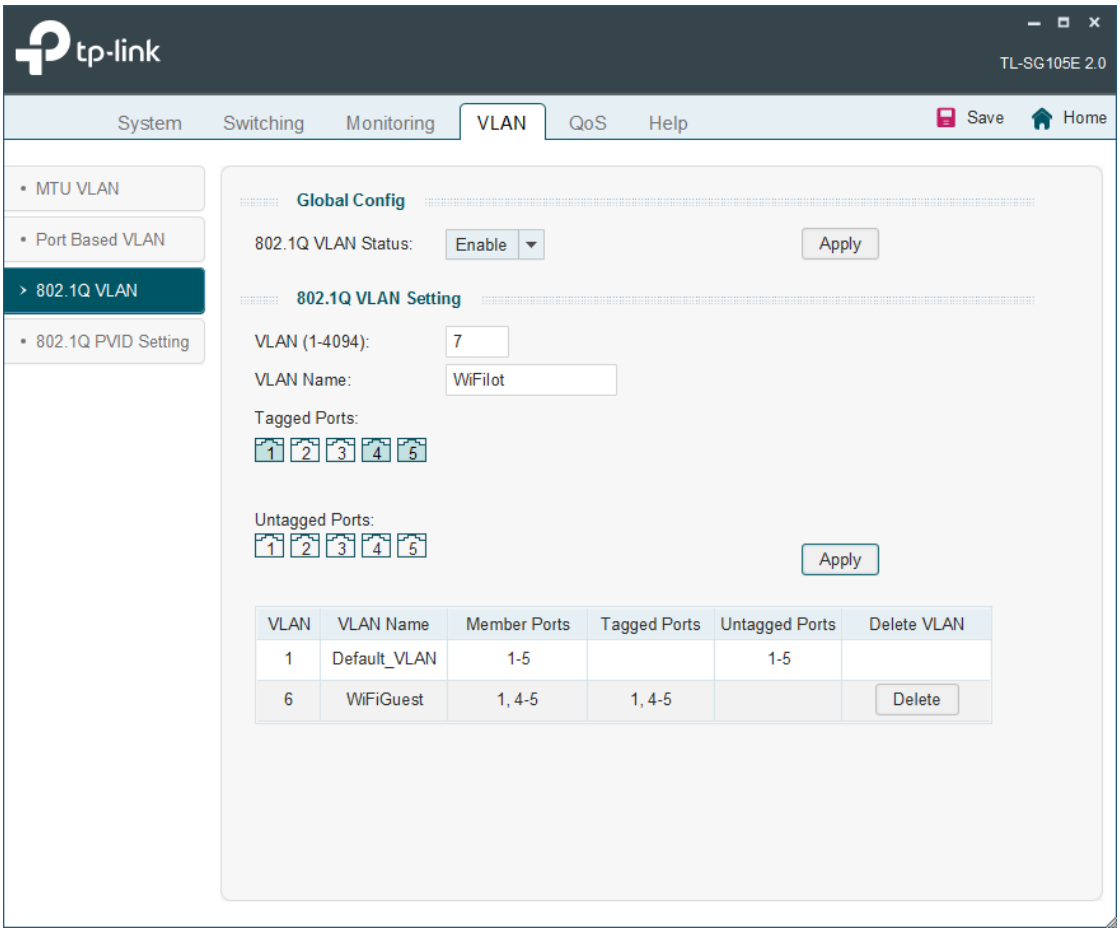


Figure 199 – Tp-Link VLAN 7 Configuration.

When you are finished, your screen should look like Figure 200 – Tp-Link VLAN Final Configuration.

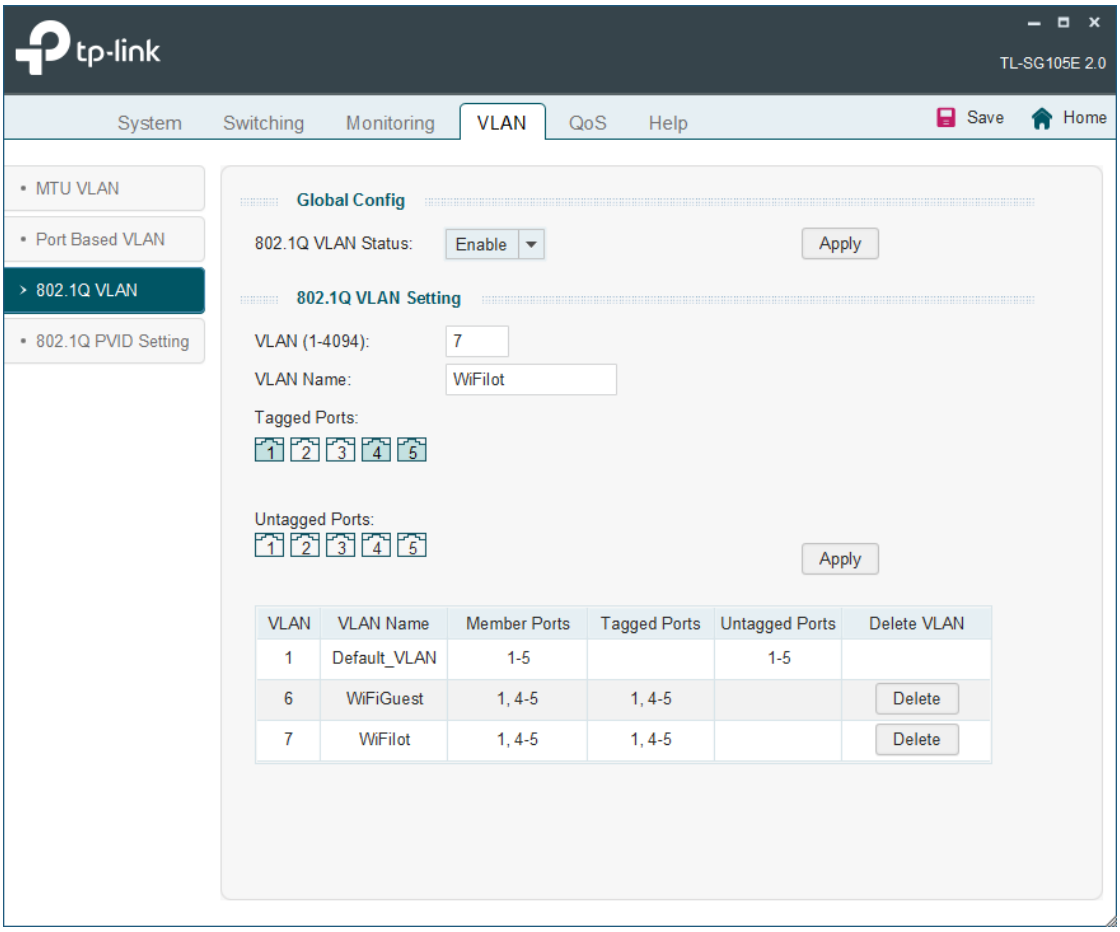


Figure 200 – Tp-Link VLAN Final Configuration.

I you wish to use the "Spare" SSID, enter the following information into the VLAN Page:

VLAN: 8
VLAN Name: WiFiSpare
Tag the ports: 1, 4, 5

There is no screenshot for this entry.

Press Save in the upper right.

After this configuration, I disconnected this switch from the Home Network. I disconnected the original Access Point from the ER-X eth4 port.

I then connected port 1 of the Tp-Link switch to the ER-X's eth4 port. I connected one Access Point (via its Power Over Ethernet (POE) adapter) to the Tp-Link switch port 4 and the other Access Point, via its POE, to the Tp-Link switch port 5. See Figure 201 – Multiple Access Point Wiring. Also reference section 69 and Figure 111 – AP-AC-LR Access Point Wiring. I did nothing with the Tp-Link switch ports 2 and 3.

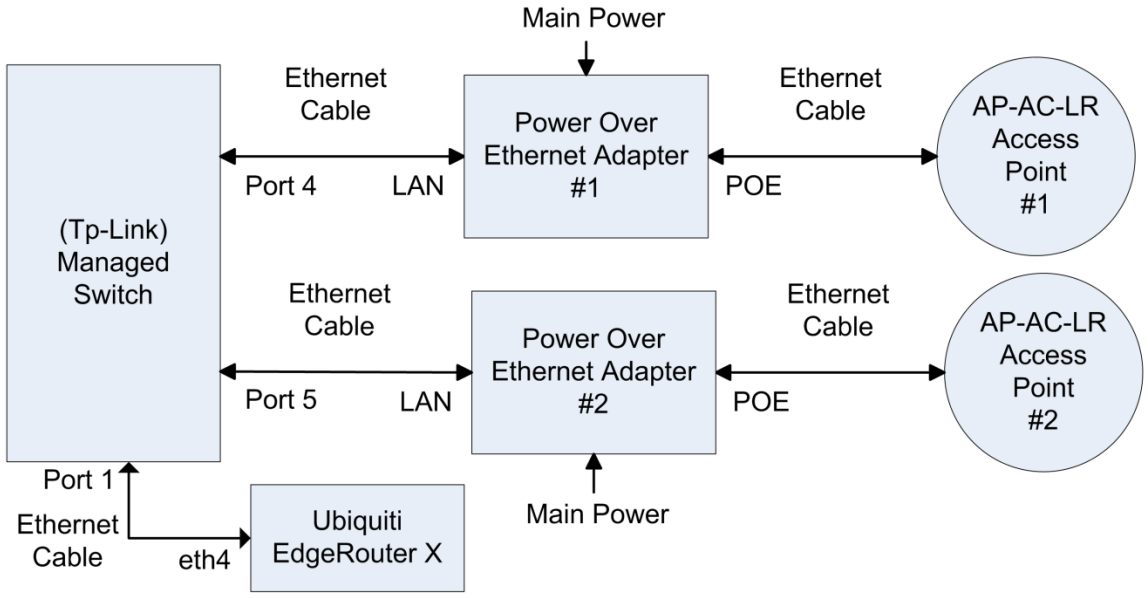


Figure 201 – Multiple Access Point Wiring.

For testing purposes, I configured each of my two Access Points with differently-named-sets of SSIDs. This way I could control and test which Access Points I was actually connecting to.

Appendix B. Multimedia over Coax Alliance (MOCA)

This section has nothing to do with the ER-X setup; this is just general networking information.

If you house is wired for television coax i.e. “Cable TV”, you might be able to use Multimedia over Coax Alliance (MOCA) adapters as an alternative to direct Ethernet cabling. This could be useful if you want to place your Access Point in the center of your house, and don’t have / can’t wire direct Ethernet cabling to that location from your router. These could also be used to positon a second Access Point at that far end of a house, where you can’t run any Ethernet wires. These devices act like a very expensive Ethernet drop. I believe there are also (different) models if you instead have satellite TV

A MOCA adapter will re-broadcast Ethernet traffic over Cable TV wires to another / multiple MOCA adapter. You need at least two MOCA adapters to network together. These adapters can concurrently operate over coax wires which are carrying Cable TV signals. If you use these adapters, you will also want to install a Point of Entry (POE) filter, so that your MOCA signals don’t contaminate the Cable TV provider’s network, i.e. your neighborhood.

A friend of mine had trouble streaming Wi-Fi data to his television set, which was at the far end of his house from his router. He purchased two MOCA adapters to Ethernet connect his Television to his router. He has had no problems and has since purchased two more adapters to provide more Ethernet drops in his house.

You will want at least version 2.0 adapters with version 2.5 now available. You will need MOCA adapters which support 802.1Q if you will be using them to connect Access Points to your ER-X. A pair of these adapters seems to be about U.S. $180. That’s pretty expensive, but might be worth it, if your only other alternative is (typically unreliable) Power-line Ethernet adapters.

References:
http://www.mocalliance.org/
https://en.wikipedia.org/wiki/Multimedia_over_Coax_Alliance

Appendix C. Monitoring an EdgeRouter via SNMP with Grafana running on a RPi

This section has nothing to do with the ER-X setup.

==========

Appendix C - Part 1

The following directions will show how to install and configure Grafana, InfluxDB, and Telegraf on a Raspberry Pi, for monitoring EdgeRouter statistics. Preview pictures are available in one of the below links.

The heavy lifting on this project was done by @waterside. Here are the major references:

https://github.com/WaterByWind/grafana-dashboards
https://github.com/WaterByWind/grafana-dashboards/tree/master/UBNT-EdgeRouter
https://grafana.com/dashboards/1756 (with pictures)
https://community.ubnt.com/t5/UniFi-Wireless/Grafana-dashboard-for-UniFi-APs-now-available/td-p/1833532

Most of the following items will be performed in a command terminal, so you will need to be generally familiar with RaspberryPi / Linux / Rasbian to continue. You will need to enable SNMP on the ER-X, Reference section 93 - Simple Network Management Protocol (SNMP).

To enable the Grafana web page to be remotely accessed by computers other than the Pi (i.e. accessed via PCs on the HomeNetwork), the Pi running these tools will need to be assigned a reserved IP address. Reference section 87 - Reserving Device Addresses via DHCP, for how to do this. Since the Pi is relatively slow, I suggest not browsing directly on the Pi, after the initial setup.

Start with Rasbian Stretch. I used a 32Gig micro SD card, as I expect to collect a lot of data over time.

Configure Pi

- Menu -> Preferences -> Raspberry Pi Configuration
  - Localization Tab
    - Set Locale
    - Set Timezone
    - Set Keyboard
    - Set WiFi Country
  - (You may also want to enable the following)
  - Interfaces Tab
    - SSH: Enable
    - VNC: Enable

Update PI Operating System

```
sudo apt-get update
sudo apt-get upgrade
```

Install SNMP and associated tools

```
sudo apt-get install snmp
sudo apt-get install snmpd
sudo apt-get install dnsutils
```

Test ER-X's SNMP setup by issuing:

```
snmpwalk -v2c -c public 192.168.3.1
```

You should see a lot of data, most of it starting with “iso”.

Download binaries

Go to https://www.influxdata.com/

(The depiction below is what I saw and the commands which I copied from the website and then ran.)

(You will want to check for and use updated instructions / versions / commands.)

(The wget commands are one long line, which is wrapped within this document.)

Select Download tab

Select Telegraf (v1.5.2) button

Find Linux Binaries (ARM) section

```
wget https://dl.influxdata.com/telegraf/releases/telegraf-1.5.2_linux_armhf.tar.gz
tar xvfz telegraf-1.5.2_linux_armhf.tar.gz
```

Select InflluxDB (v1.4.3) button

Find Linux Binaries (ARM) section

```
wget https://dl.influxdata.com/influxdb/releases/influxdb-1.4.3_linux_armhf.tar.gz
tar xvfz influxdb-1.4.3_linux_armhf.tar.gz
```

Select Chronograf (v1.4.2.1) button

Find Linux Binaries (ARM) section

```
wget https://dl.influxdata.com/chronograf/releases/chronograf-1.4.2.1_linux_armhf.tar.gz
tar xvfz chronograf-1.4.2.1_linux_armhf.tar.gz
```

Install (copy) binaries per
https://community.influxdata.com/t/installing-on-a-raspberry-pi/2159
(You will want to adjust directory names for your specific versions.)

```
cd telegraf
sudo cp -rp usr/* /usr
sudo cp -rp etc/* /etc
sudo cp -rp var/* /var
cd ..

cd influxdb-1.4.3-1
sudo cp -rp usr/* /usr
sudo cp -rp etc/* /etc
sudo cp -rp var/* /var
cd ..

cd cronograf-1.4.2.1-1
sudo cp -rp usr/* /usr
sudo cp -rp etc/* /etc
sudo cp -rp var/* /var
cd ..
```

Put the following text into:
/etc/systemd/system/influxdb.service

```
[Unit]
Description=InfluxDB service
After=network.target
[Service]
ExecStart=/usr/bin/influxd
Restart=always
[Install]
WantedBy=multi-user.target
```

Start the service (now) with the following command:

```
sudo systemctl start influxdb.service
```

Check that the service is running with:

```
systemctl | grep influx
```

Auto start the service (after re-boots) with the following command:

```
sudo systemctl enable influxdb.service
```

Put the following text into:
/etc/systemd/system/telegraf.service

```
[Unit]
Description=Telegraf service
After=network.target
[Service]
ExecStart=/usr/bin/telegraf -config /etc/telegraf/telegraf.conf
Restart=always
[Install]
WantedBy=multi-user.target
```

Note that the ExecStart is really one long line, upto the Restart line. It may be wrapped within this document.

Start the service (now) with the following command:

```
sudo systemctl start telegraf.service
```

Check that the service is running with:

```
systemctl | grep telegraf
```

Auto start the service (after re-boots) with the following command:

```
sudo systemctl enable telegraf.service
```

Download and install grafana
Go to https://github.com/fg2it/grafana-on-raspberry
(You will want to check for and use updated instructions / versions / commands.)
(Some instructions / commands will be presented, after you issue the dpkg command.)
Press the raspberry pi 2 and 3 (armv7) Download button in the middle of screen
Save file `grafana_5.0.0_armhf.deb` whose link is near the bottom of the page
Issue the following command:

```
sudo dpkg -i Downloads/grafana_5.0.0_armhf.deb
```

Follow presented instructions, which for my version, included:

```
sudo /bin/systemctl daemon-reload
sudo /bin/systemctl enable grafana-server
sudo /bin/systemctl start grafana-server
```

Acquire needed mib files, by issuing the following command:

```
sudo apt-get install snmp-mibs-downloader
```

Download zip from:

https://github.com/WaterByWind/grafana-dashboards

(Use the green "Clone or download" button, then "Download ZIP" button)

Unzip the file:

```
unzip Downloads/grafana-dashboards-master.zip
```

Configure telegraf

```
cd /etc/telegraf
cp telegraf.conf telegraf.conf.orig
```

Edit `telegraf.conf`

Change the line:	`interval = "10s"`
To:	`interval = "60s"`
Change the line:	`collection_jitter = "0s"`
To:	`collection_jitter = "10s"`
Change the line:	`# username = "telegraf"`
To:	`username = "username"`
Change the line:	`# password = "metricsmetricsmetricsmetrics"`
To:	`password = "password"`
Uncomment:	`# user_agent = "telegraf"`

Append the contents of grafana-dashboards-master/UBNT-EdgeRouter/telegraf-inputs.conf to telegraf.conf. You may want to add separator comment line(s) between the sections.

Change the line:	`agents = [ "edgerouter1", "edgerouter2" ]`
To:	`agents = [ "192.168.3.1" ]`

```
sudo systemctl restart telegraf.service
cd /home/pi
```

Check that the service is running with:

```
systemctl | grep telegraf
```

Test telegraf (this is one long command line)

```
telegraf --config /etc/telegraf/telegraf.conf --config-directory
/etc/telegraf/telegraf.d --input-filter snmp --test
```

You should see a huge block of data, with no error messages.

Only if you see error messages, will you need to acquire additional mib files from your ER-X's
`/usr/share/mibs` directory.
(I used WinSCP, which allows files to be copied to/from a Windows PC against another system.)
(You may instead be able to acquire the mib files by other means or over the internet.)
(See also https://github.com/WaterByWind/grafana-dashboards/issues/3)
(See also https://github.com/WaterByWind/grafana-dashboards/issues/1)

```
mkdir /usr/share/mibs/
mkdir /usr/share/mibs/site
chmod ugo+w /usr/share/mibs/site
cp <mib_files> /usr/share/mibs/site
cd /home/pi
```

Locally login to grafana, by browsing to http://localhost:3000

```
admin
admin
```

Login button

Reference: https://github.com/WaterByWind/grafana-dashboards/tree/master/Extra
(To enable the Grafana web page to be remotely accessed by computers other than the Pi
(i.e. accessed via PCs on the HomeNetwork), substitute the Pi's IP address for the above "localhost".)

Choose Add data source
Enter the following information:

Name	Telegraf
Type	InfluxDB
URL	http://localhost:8086
Access	direct
Database	telegraf
User	username
Password	password
Press the	Save&Test button

Add a dashboard

1. Hover over the upper-left + button
2. Choose Import from the Create section
3. Enter `1756` into the Grafana.com Dashboard box
4. Press the Load Button
5. Under "Options Name", Enter: UBNT EdgeRouter Dashboard
6. Under "Options Telegraf", Select: Telegraf
7. Press the Import button

The new dashboard should then be selected for you
Under Choose Router, select: 192.168.3.1

If the dashboard is not selected, hover over the "4 squares" upper-left icon, and then select Dashboard <dashboard name>.

You should now be viewing your ER-X's SNMP data graphs.

You can change the time scale of the graphs by clicking on the upper-right clock icon.

==========

Appendix C - Part 2

At some point, I was having occasional network problems and suspected dns as the root problem.
Here are some additions to the above grafana setup.

This portion will graph pinging times to web servers, which will test internet access.

Per https://grafana.com/dashboards/2690
Append the following to your telegraf.conf:
(You may want to add separator comment line(s) between the sections.)

```
[[inputs.ping]]
  interval = "60s"
  urls = [ "amazon.com", "github.com", "google.com" ]
  count = 4
  ping_interval = 1.0
  timeout = 2.0
```

Restart telegraf

```
sudo systemctl restart telegraf.service
```

Test new telegraf entry (this is one long command line)

```
telegraf --config /etc/telegraf/telegraf.conf --config-directory
/etc/telegraf/telegraf.d --input-filter ping --test
```

After a few seconds, you should see 3 "> ping" lines.

Add a dashboard

1. Hover over the upper-left + button
2. Choose Import from the Create section
3. Enter `2690` into the Grafana.com Dashboard box
4. Press the Load Button
5. Under “Options Name”, Enter: Ping Monitor
6. Under “Options Telegraf”, Select: Telegraf
7. Press the Import button

As written, this dashboard seems to have trouble displaying the data sometimes.
The following edits seem to help:

1. Select the Ping Monitor dashboard.
2. Hover over the “Ping Average Response Time” title, and then click on the down caret which appears.
3. Choose Edit
4. Ensure you have the Metrics Tab selected (in the middle of the screen)
5. Go to the line
   GROUP BY time($_interval) tag(url) fill(null)
   and click on the word ‘null’, select ‘none’ from the list, as in:
   GROUP BY time($_interval) tag(url) fill(none)
   Click on the X, which is to the right of all of the graph tabs, to exit editing.
   Press the Save Dashboard button, which looks like a floppy icon, at the top of screen.

Perform the same change as above i.e. “fill(null)” -> fill(none)”, for the “Packet Loss Percentage” graph.

You should start collecting data. A portion of the screen should eventually look like Figure 202 – Example Grafana Ping Monitor Portion.

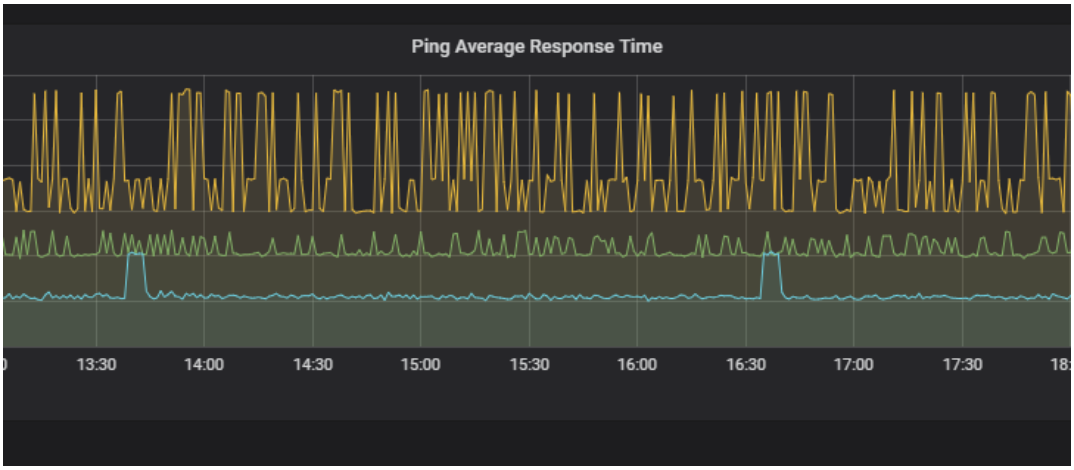


Figure 202 – Example Grafana Ping Monitor Portion

==========

Appendix C - Part 3

This portion will graph dns queries made to multiple dns resolvers.

Per https://github.com/influxdata/telegraf/tree/master/plugins/inputs/dns_query
Append the following to your telegraf.conf:
(You may want to add separator comment line(s) between the sections.)

```
# Dns Query Config:
[[inputs.dns_query]]
  ## servers to query
  servers = [ "192.168.3.1", "209.244.0.3", "8.8.8.8", "9.9.9.9" ]
  ## Network is the network protocol name.
  network = "udp"
  ## Domains or subdomains to query.
  domains = [ "amazon.com", "github.com", "google.com" ]
  ## Query record type.
  ## Posible values: A, AAAA, CNAME, MX, NS, PTR, TXT, SOA, SPF, SRV.
  record_type = "A"
  ## Dns server port.
  port = 53
  ## Query timeout in seconds.
  timeout = 2
```

Restart telegraf

```
sudo systemctl restart telegraf.service
```

Test new entry (this is one long command line)

```
telegraf --config /etc/telegraf/telegraf.conf --config-directory
/etc/telegraf/telegraf.d --input-filter dns_query  --test
```

You should see 12 "> dns_query" lines.

Create a new Dashboard

1. Hover over / click on the “4 squares” upper-left icon, then select Dashboards / Home.
2. Hover over the upper-left + button, choose Create Dashboard
3. Choose Graph
4. Hover over the “Panel Title” title, and then click on the down caret which appears.
5. Choose Edit
6. Select General Tab under Graph
7. In the Title box, enter: ER-X Dns
8. Select Metrics Tab under Graph
9. Under Data Source, select: Telegraf
10. You should see a line which looks like:
    “FROM default select measurement WHERE +”
    Click on “select measurement” and choose “dns_query”
    Click on the + sign and select “server”
    Click on “select tag value” and select “192.168.3.1”, leave the “=” sign alone.
    The line should now look like: “FROM default dns_query WHERE server = 192.168.3.1”

11. You should see a line which looks like:
    "SELECT field(value) mean() +"
    Click on "value" and select "query_time_ms"
    Click on "mean() and select Remove, click on the new + sign and choose max() under Selectors.
    The line should now look like: "SELECT field(query_time_ms) max()"

12. You should see a line which looks like:
    GROUP BY time($_interval) fill(null) +
    Click on the + sign, and select "tag(domain)".
    Select "null" and change into "none"
    The line should now look like: "GROUP BY time($_interval) tag(domain) fill(none)"

13. Leave the "FORMAT AS Time series line alone.

14. In the ALIAS BY box, enter: $tag_domain

15. Select the Graph Axes Tab.
    Under the Left Y group change the following:

Y-Min	auto	to	0
Y-Max	auto	to	100

16 Click on the X, which is to the right of all of the graph tabs, to exit editing.

17. Press the Save Dashboard button, which looks like a floppy icon, at the top of screen.

DNS data should start accumulating. We need a total of four panels, so we will duplicate this panel three times, slightly editing each one.

Duplicate Panel

1. Hover over the "ER-X Dns" title, and then click on the down caret which appears.
2. Select More, then select Duplicate.

Modify New Panel

1. Hover over the NEW "ER-X Dns" title, and then click on the down caret which appears.
2. Select Edit.
3. Select General Tab under Graph
4. In the Title box, change: ER-X Dns to Level3 Dns
5. Select Graph Metrics Tab under Graph
6. In the FROM line, select 192.168.3.1 and then select (change to) 209.244.0.3
7. Click on the X, which is to the right of all of the graph tabs, to exit editing.
8. Press the Save Dashboard button, which looks like a floppy icon, at the top of screen.

Repeat the above "Duplicate Panel" and "Modify New Panel" steps with the following data:

Title	Google Dns
server equals	8.8.8.8

Repeat the above "Duplicate Panel" and "Modify New Panel" steps with the following data:

Title	Quad9 Dns
server equals	9.9.9.9

My graphs eventually looked like Figure 203 – Example Grafana DNS Queries.

How interesting!

I believe that I will need to investigate and adjust dnsmasq settings in the88 - Adblocking and Blacklisting section. What I have seems to work, but is definitely non-optimal.

Figure 203 – Example Grafana DNS Queries

==========

Appendix C - Part 4

This portion may someday graph UniFi Access Point information, per the URLs given in Part 1.