Home-Network Implementation

Using the Ubiquiti EdgeRouter ER-X and a Ubiquiti Access Point

By Mike Potts

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

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 US
- Ubiquiti Wi-Fi Access Point Typically $110 US or $175 US (depending upon model chosen).

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 for 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.

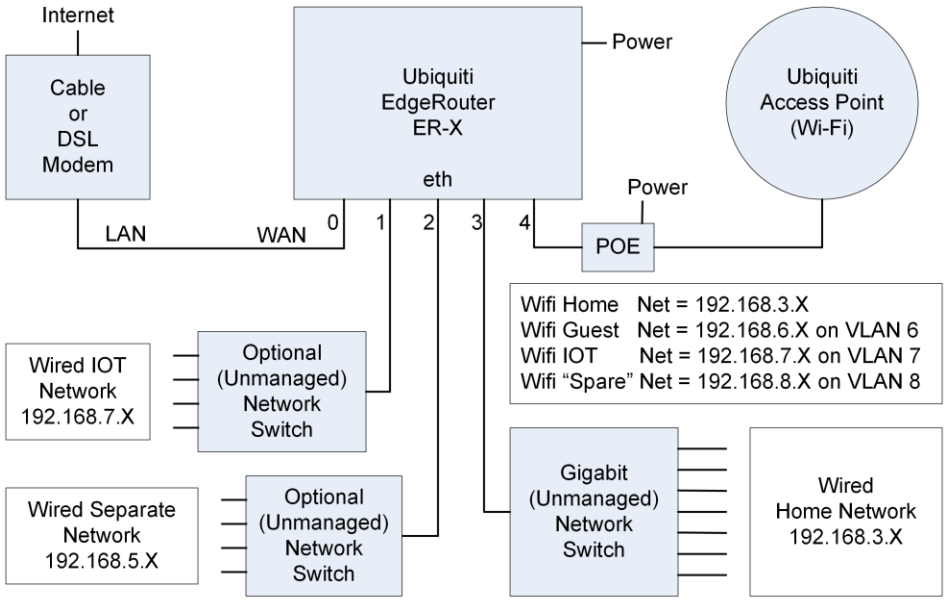


Figure 1 - Overview Diagram

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 a 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. You can also manage / run multiple Access Points for better Wi-Fi coverage.

You will also need to run Ubiquiti's UniFi software for the configuration of the Access Point(s). This is free (Windows / Linux / Mac) software. It only *needs* to run during configuration, but can *also* run permanently to monitor system Wi-Fi health. UniFi runs nicely on a Raspberry Pi.

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. (Don't worry php links are secure for an accessing client.) 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. This guide was first written in 2016, with a total-re-write (equivalent to a Second Edition) occurring early in 2023. 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 EdgeMax and UniFi-Wireless Ubiquiti Communities:

> https://community.ui.com/tags/edgemax/questions?
>
> https://community.ui.com/tags/unifi-wireless/questions?

Other resources are:

> https://www.reddit.com/r/Ubiquiti

When this document was ready, I joined the Ubiquiti community and announced it at:

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 Community links, then look at the resources in section 5 - Web Resources and section 6 - BuckeyeNet's link farm, 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. If you stick with this system, you will eventually want a second ER-X as a backup.

4. Guide Revisions for Previous Users

This section is primarily for users whom have previously used this guide.

The first github commit of this guide was made on Mar 26, 2017. The final "Legacy" guide was committed on Jan 8, 2023. That is 38 commits! The guide was re-written (similar to a Second Edition publication) after that date, and the first publication of the "Second Edition" was published on April 28, 2023.

These re-writes involved me setting up a new ER-X EdgeRouter, with the enabling of the ER-X's VLAN Switch now occurring early in this guide. This change makes for a cleaner, more streamlined sequence, and removed a lot of (original) fumbling-around. This new sequence forced me to re-take almost every ER-X screenshot. I also re-worked the entire firewall. The overall outward-behavior of the firewall remains (approximately) the same, but the internal-operation is completely different, and likely more efficient.

The UniFi installation and setup sections were also completely re-written, now using a single and current UniFi Controller software version. The original UniFi sections had been patched-together over several years of UniFi versions and their changes. If your existing UniFi / Wi-Fi is working, no UniFi / Access Point changes are needed.

@BuckeyeNet has provided valuable guidance, many links, and helped with the many changes in this Second Edition re-write. Thank you. He also persuaded me to try using "IN" rules for the firewall, and for that, Double Thanks.

The bulk of the changes made for the Second Edition were /are:

UAP selection/purchase information:	8.2 - Ubiquiti Access Point Models on page 14.
Early Enabling of ER-X's VLAN Switch.	
Firewall description:	49.1 - Firewall Postings on page 91
New Firewall:	50 - EdgeRouter Detailed Firewall Setup on page 93. (Including description sections 50.1, 50.2, 50.3, & 50.4)
New section on Firewall Design:	61 - Firewall Considerations / Customizations on page 121.
New section on Firewall Testing	62 - Firewall Testing on page 124.
New section on ER-X Customization:	78 - Customizing the ER-X for Your Installation on page 154.
New section on ER-X Deployment:	79 - Preparing the ER-X as Your Primary Router on page 166.
UniFi sections completely updated.	
New section on EOP Adapters:	Appendix B - Ethernet Over Power Adapters on page 251.

For anybody whom has already used prior revisions of this guide, just look over the above cited sections, your current installation should still be good, but note that the new firewall sure looks shiny. If you previously followed this guide, hopefully you purchased a spare / backup unit which you could update per the Second Edition guide and try out the new firewall.

To access earlier revisions of this guide, navigate to the github repository using one of the links which are at the top of page 1. Click on the artifact of interest, e.g. Ubiquiti Home Network.pdf. There should be a "History" button in the upper right. When you click on it, you should get a list of all the artifact's revisions. You can use the "<>" button to "Browse the repository at this point in history". Doing so will allow you access to (view, download) that earlier artifact.

5. Web Resources

These postings perform similar items as this guide does:

https://help.ui.com/hc/en-us/articles/115002531728

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

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.ui.com/questions/EdgeRouter-X-segmentation/44d4aa41-0f23-40e5-87f9-27b07cf6d95f

Ben Pin (sometime Ubiquiti Employee) has a bunch of tutorial videos:

https://www.youtube.com/channel/UC9jUG4FPm9mPM555WOKSl6g

Including “Quick Config Ubiquiti EdgeMAX - UAP with Guest WLAN & VLAN Trunks (VIF)”:

https://www.youtube.com/watch?v=SKeFqFhBwJY

6. BuckeyeNet's link farm

@BuckeyeNet invented and is the keeper of the best collection of Ubiquiti data / links. This is a huge knowledge base. Due to the materials size, he has made 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

These postings are so important, that I have cached the above pages in a (Microsoft Word) document and locally stored that document on my PC.

7. EdgeRouter Models

I chose the Ubiquiti ER-X EdgeRouter for this project. It is inexpensive and still very capable.

Product / Store Link:
https://store.ui.com/collections/operator-edgemax-routers/products/edgerouter-x

7.1 ER-X Routing 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, so speed tests are not accurate for this measuring. Most postings show that this ER-X can do, at least, speeds of 300 Mbit/sec up and 300 Mbit/sec down. With hardware acceleration enabled, and no Quality of Service (QoS) enabled, you should be able to achieve about 900 mbps up / down.

The following (now web archived) article is well worth reading about the internals of the ER-X hardware:

https://web.archive.org/web/20210516080132/https:/kazoo.ga/re-visit-the-switch-in-edgerouter-x/

Other performance references:

https://community.ui.com/questions/Performance-of-EdgerouterX-vs-Edgerouter-Lite/cb11f2e5-eb5e-41c4-968a-9a4a656e1ce9

https://community.ui.com/questions/EdgeRouter-X-low-throughput-slow/b0e2f819-aef7-4fa6-a41f-953b16c701d8

https://community.ui.com/questions/ER-X-vs-ER-Lite-Head-to-Head-Speed-Results-on-Google-Fiber/4490c1a7-a1e7-44ae-8aab-4bff6d4beba3

https://community.ui.com/questions/Edgerouter-X-Fios-Gigabit-Wont-go-over-500-Mbps/a35cf2d2-f4d6-4d68-8b18-24e6d705547d

7.2 Alternate / Similar EdgeRouters

There are now alternate “nicely priced” (more powerful) EdgeRouters available. There are also EdgeRouter models available which are *much* more expensive and *very* powerful. I have no experience with any EdgeRouter models except for the ER-X.

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

EdgeRouter -10X:

https://store.ui.com/collections/operator-edgemax-routers/products/edgerouter-10x

https://community.ui.com/questions/Anyone-want-to-share-their-experience-with-ER-10X/fa9ce2b8-f374-4b86-bb76-e231bfc74a88#M250254

EdgeRouter-12:

https://store.ui.com/collections/routing-switching/products/edgerouter-12

https://community.ui.com/questions/New-ER-12-owner-ER-12-Questions-/e9ebf126-895e-4801-854c-c7e914765def#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.

8. Ubiquiti Access Points Models (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 was that crammed full of IOT devices.

As of 2023, 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 currently being used for my test-system (i.e. the re-writing of this guide) and will eventually become 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 too bad again, I'll shelve the U6-LR and re-deploy the U6-Lite. The U6-Pro is cheaper, more advanced, and more-stable than the U6-LR.

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 (for any UAP).

Access Point AC Long-Range = UAP-AC-LR-US ($110 US with / including 24V passive Power Adapter)

https://store.ui.com/collections/unifi-network-wireless/products/unifi-ac-lr

8.1 Number of Ubiquiti Access Points to Install / Placement

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

**<u>It is better to deploy more (cheaper) Access Points,
than deploy fewer (more expensive) Access Points</u>,**

i.e. walls, floors, and distance seem to make the real difference.

You will want to Ethernet-wire every UAP 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

8.2 Ubiquiti Access Point Models

If you are buying new Access Points, there are Wi-Fi 6 (Dome type) Access Point models available.
See Table 1 – Ubiquiti U6 Access Point Models. The Table is 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 US
U6+ (Was EA)	2x2	2x2		3.0 Gbps	3	5.4		5th	$130 US
U6+ LR (EA)	2x2	3x3		3.0 Gbps	4	5.5		5th	$150 US
U6-Pro-US	2x2	4x4		5.3 Gbps	4	6		6th	$160 US
U6-LR-US	4x4 *	4x4		3.0 Gbps	4	5.5		5th	$180 US
U6-Enterprise-US	2x2	4x4	4x4	10.2 Gbps	3.2	5.3	6	6th	$299 US

* 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.

Table 1 – Ubiquiti U6 Access Point Models

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).** I would *never* purchase an early-access (EA) model; Ubiquiti has abandoned some of their early-access "experiments" in the past. The users whom purchased those EA items were left with semi-worthless / non-supported devices.

If you already have existing UAPs, except non-supported Generation 1 units, just use them for home-use.

This article shows which models belong to which generation:

https://help.ui.com/hc/en-us/articles/4409162471447-UniFi-Identify-your-Access-Point-Model

Before purchasing any new APs, you might also want to read through all of section 8 (here) and also all of section 102 - Channels, Power Levels on page 220. , I suggest also you read community postings, and postings associated with Access Point firmware releases.

Release notes are available at:

https://community.ui.com/releases (click UniFi Wireless on left pane)

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 Ubiquiti adapters (generic industry equivalents are also available / usable):

PoE Injector, 802.3at = U-POE-AT ($12 US, i.e. 30W Power Adapter)

PoE Injector, 802.3af = U-POE-AF ($8 US, i.e. 15W Power Adapter)

You can use an 802.3at adapter for units which only need an 802.3af amount of power. I.e. UAPs which require an AT amount of power, require an AT power source; but UAPs requiring only an AF amount of power, can be powered by either AF or AT power supplies.

Older / non-U6 models are (typically) 24V passive, the above U6 models are 48V 802.11af/at.

2022 Note: The AP-AC-LR model (I originally used) is now four generations old, i.e. in the oldest AP family currently supported.

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

8.3 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.

8.4 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.

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 MOCA adapters can even be used when your coax is in-use. These are discussed in Appendix A - Multimedia over Coax Alliance (MOCA) on page 250.

Similarly, Ethernet Over Power adapters, can carry Ethernet data over your house's existing power lines. These can also be used to "Ethernet Wire" remote UAPs, and are discussed in Appendix B - Ethernet Over Power Adapters on page 251.

Both MOCA and EOP adapters quality as "Ethernet wiring" for purposes of deploying Ubiquiti Access Points.

8.5 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
(above link now re-directs to a stupid marketing link, now listed below)
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://ui.com/wi-fi

Here are some pages comparing Ubiquiti equipment, which seem to provide much better detail than Ubiquiti's own pages. Ubiquiti is now removing some of their useful information. Reference to where I found it, is in section 8.7. If you are purchasing new APs, I suggest you explore (at least) the following pages:
https://evanmccann.net/blog/ubiquiti/unifi-comparison-charts
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

Here are some datasheets which google helped me find:
https://dl.ui.com/ds/u6-lite_ds.pdf
https://dl.ui.com/ds/u6-pro_ds.pdf
https://dl.ui.com/ds/u6-lr_ds.pdf
https://dl.ui.com/datasheets/unifi/UniFi_AC_APs_DS.pdf
https://dl.ui.com/datasheets/unifi/UniFi_AP_DS.pdf
https://dl.ui.com/datasheets/unifi/UniFi_AC_Mesh_DS.pdf
https://dl.ui.com/datasheets/unifi/UniFi_UAP-AC-HD_DS.pdf
https://dl.ui.com/ds/uap-iw-hd_ds.pdf
https://dl.ui.com/datasheets/unifi/UniFi_UAP-AC-SHD_DS.pdf
https://dl.ui.com/datasheets/unifi/UniFi_XG_AP_DS.pdf

8.6 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 than 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

8.7 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

8.8 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

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

9. 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 at the above URL, specific links given below:

https://dl.ui.com/guides/edgemax/EdgeOS_UG.pdf

https://dl.ui.com/guides/edgemax/EdgeRouter_ER-X_QSG.pdf

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 (ER-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.

10. Existing Router's LAN Address Range

For the purposes of this guide, I am assuming that you will, after initial setup, put your Ubiquiti EdgeRouter in-series-with / behind your existing firewall / router, until the configuration of your EdgeRouter has been finalized.

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 on its LAN ports:

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

These are the address ranges which will (after ER-X configuration) be used within the ER-X.

If your existing router uses any of the above address ranges, you need to change your existing router's LAN address range before continuing. The address ranges of 192.168.0.X, 192.168.1.X, or 192.168.2.X are all safe to use.

Most cable / DSL modems seem to be pre-configured for DHCP use, and traditionally have used LAN address ranges of 192.168.0.X or 192.168.1.X. Newer Asus routers seem to instead use the address range of 192.168.50.X (which is also safe to use).

11. EdgeRouter Initialization

Some of the following information is taken from the Quick Start Guide (QSG). The QSG URL was provided in section 9 - Acquire EdgeRouter Documentation on page 23.

> "The EdgeOS configuration interface can be accessed via DHCP or static IP address assignment. By default, eth1 is set up as a DHCP client, while eth0 is assigned a static IP address of 192.168.1.1. To configure the EdgeRouter, proceed to the appropriate section."

The DHCP (eth1) method was developed relatively recently, and is much simpler than the (original) static IP method. You will follow the steps in either section 11.2 - EdgeRouter DHCP Initialization, or in section 11.3 - EdgeRouter Static IP Initialization. The DHCP (eth1) method requires that your existing router must be configured as a DHCP server. Consumer routers are almost universally configured as a DHCP server. You must also be capable of determining the ER-X's assigned IP address. This information would typically be determined by logging-into your existing router and inspecting its DHCP tables / data. You will perform the steps in *either* section 11.2 or in section 11.3.

11.1 EdgeRouter Factory Reset

Perform an EdgeRouter reset, using one of the two methods which are described below. 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.

The following information is taken from the Quick Start Guide (QSG):

There are two methods to reset the EdgeRouter to factory defaults:

- Runtime reset (recommended)

  [Power-up the ER-X router using the supplied 12V Power Supply. Wait about 5 minutes for the ER-X to fully boot.] The EdgeRouter should be running after bootup is complete. Press and hold the Reset button for about 10 seconds until the eth4 LED starts flashing and then becomes solidly lit. After a few seconds, the LED will turn off, and the EdgeRouter will automatically reboot.

- Power-on reset

  Disconnect power from the EdgeRouter. Press and hold the Reset button while connecting power to the EdgeRouter. The port LEDs will light up in sequential order. Keep holding the Reset button until the LED on the last port starts flashing, and then release the button.

Wait about 5 minutes for the EdgeRouter to re-boot, after the factory reset.

11.2 EdgeRouter DHCP Initialization

See Figure 2 - EdgeRouter DHCP Initialization Wiring. Note that your own modem / routing equipment may instead have the “Cable or DSL Modem” portion and “Your Existing Firewall / Router” portion combined into one single unit.

Using an Ethernet cable, wire the ER-Xs eth1 port to a LAN port of your existing router.

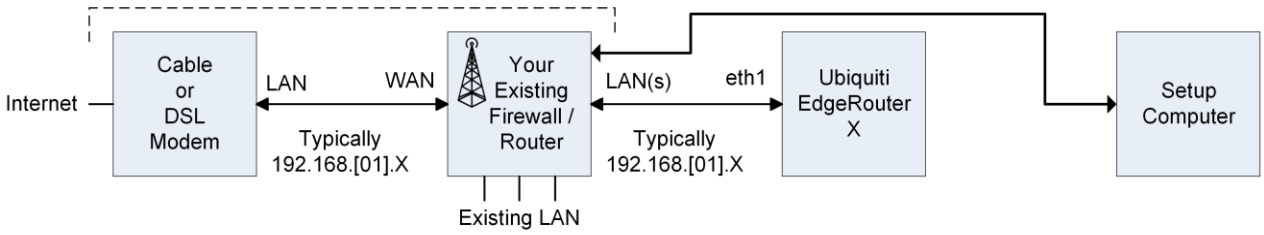


Figure 2 - EdgeRouter DHCP Initialization Wiring

If your Setup Computer is not already connected to your existing router, also connect it to a LAN port

If you run out of router LAN ports, you can connect one port of a Gigabit network-switch to one of your router’s LAN ports, and then connect more devices to the other Gigabit network-switch ports. Gigabit network switches can be acquired for about $20 US from a variety of sources. Popular models are un-managed gigabit network-switches sized at 5-port and 8-port models. If purchasing a new one, assure that it is 802.1Q (VLAN) capable. I believe most (recent models) are 802.1Q capable.

Inspect your existing router to determine the IP address which was assigned to the ER-X. Remember this IP address. Skip the following section: 11.3 - EdgeRouter Static IP Initialization.

11.3 EdgeRouter Static IP Initialization

Using an Ethernet cable, wire your Setup Computer's Ethernet port to the ER-X's eth0 port. See Figure 3 - EdgeRouter Static IP Initialization Wiring.

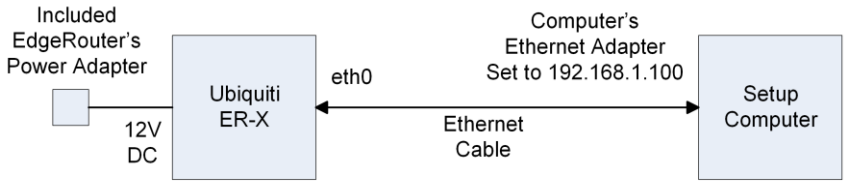


Figure 3 - EdgeRouter Static IP Initialization Wiring

Configure the Setup Computer's Ethernet port to have 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 show how to configure a computer's Ethernet port to use a fixed IP address. If this Setup Computer also has a Wi-Fi adapter or has other Ethernet adapters, they may need to be temporarily disabled for you to be able to access the ER-X.

One way to configure a Windows 10 computer is:

> Control Panel -> Network & Internet -> Ethernet -> Change Adapter Obtions -> <Choose Your Adapter> -> Internet Protocol Version 4 (TCP/IPv4) -> Properties -> <Click> Use the following IP address:
> IP Address: 192.168.1.100, Subnet mask: 255.255.255.0 -> OK -> OK
>
> See Figure 4 – Windows 10 Ethernet Address Setup.
>
> @BuckeyeNet has made the following observation:
> The IP address is not actually changed until you press *both* the #1 OK *and* #2 OK.

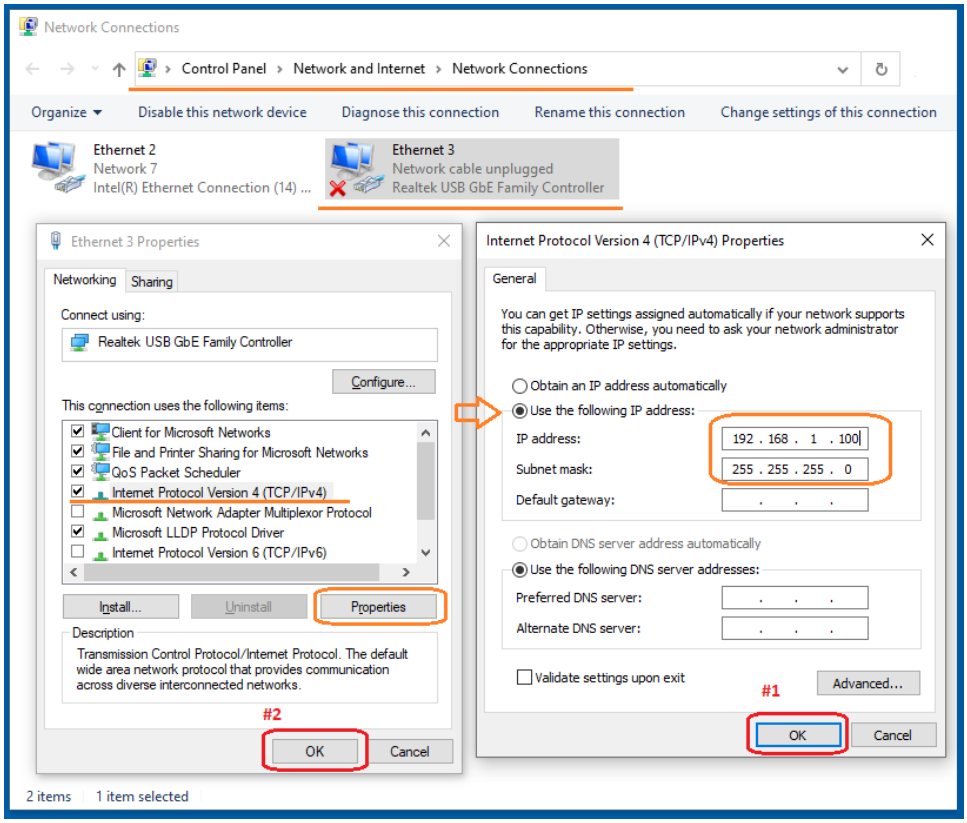


Figure 4 – Windows 10 Ethernet Address Setup

Remember the IP address of 192.168.1.1

12. Initial EdgeRouter Login

On your Setup Computer, open a web browser (of your choice) and enter https://<RememberedIPAddress> into the address field. My example IP address assigned to the ER-X was was 192.168.50.136. So my example browser address was entered as https://192.168.50.136

The browser will likely issue a security warning. You will need to "Accept the Risk and Continue" or equivalent. The exact prompts and responses vary by browser. See Figure 5 – Browser Security Certificate Example

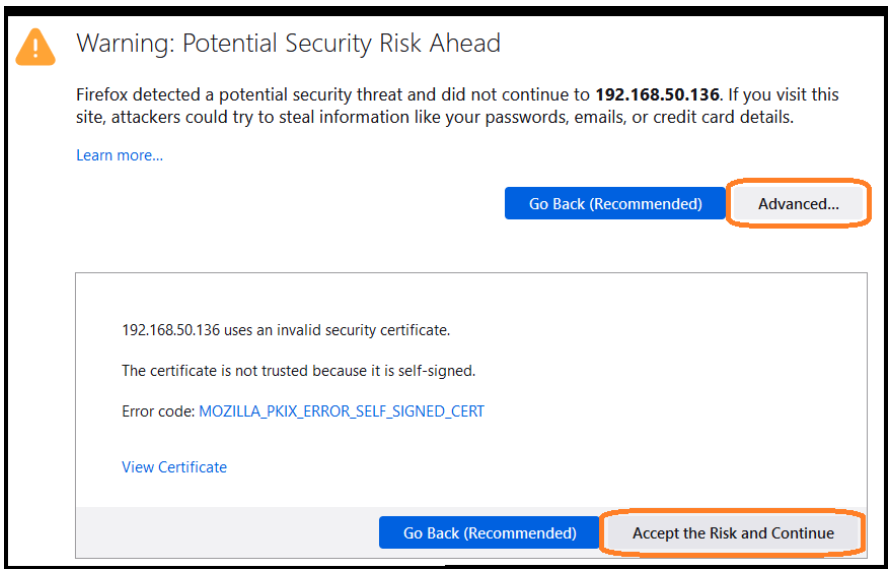


Figure 5 – Browser Security Certificate Example

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

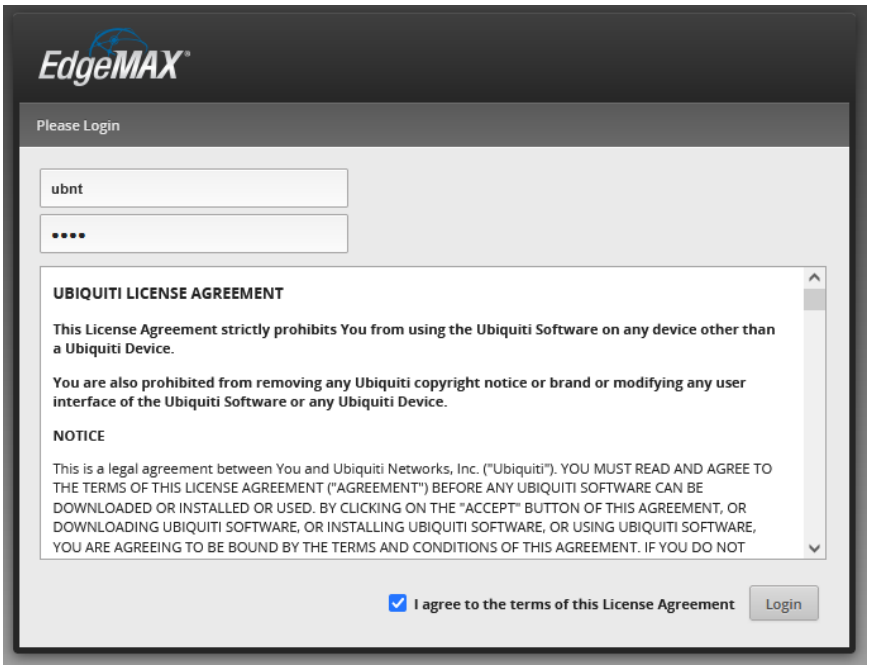


Figure 6 – Ubiquiti License Agreement Dialog

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.

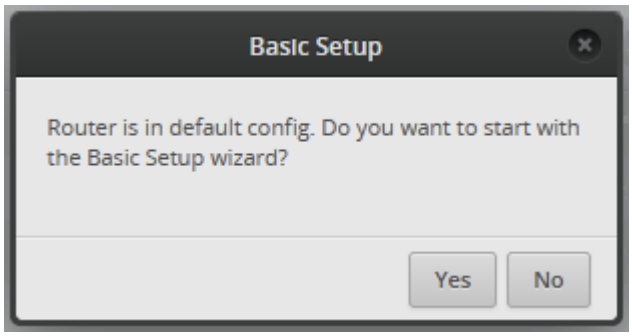


Figure 7 – Basic Setup Question

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

Warning: Do ***not*** enable the POE output on `eth4`, or you will likely destroy any / all equipment which is connected to that ER-X port. This output is an older 24V passive (read as *destructive*) Power Over Ethernet (POE).

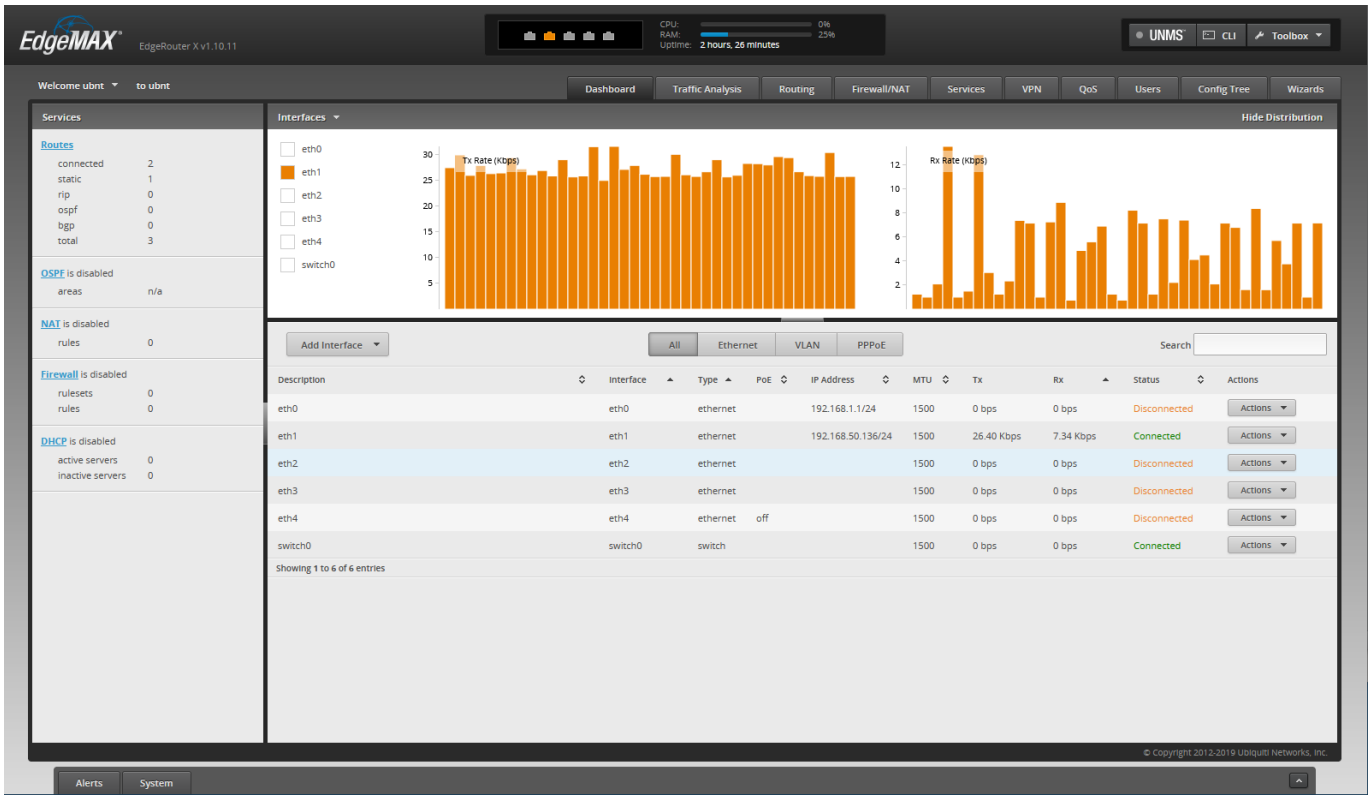


Figure 8 – Initial Dashboard Screen

13. Update EdgeRouter (System) Firmware

Note: Sometimes to successfully 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 18 - EdgeRouter Command Line Interface (CLI).

On your setup computer, download the latest firmware from:

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

Release notes are available at:

https://community.ui.com/releases (click EdgeMax on left pane)

This Edgerouter firmware `v2.0.9-hotfix.5` / `v2.0.9-hotfix.6` were current, and used during the re-writing of the guide.

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(s), looking for new updates. It is probably a good idea to keep (somewhat) up to date firmware on your EdgeRouter, for security purposes.

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.

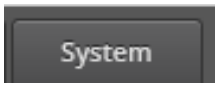


Figure 9 – System Button

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.

The System window will then pop-up an overlay that will cover most of your screen. The resulting dialog is shown here in two screenshots. See Figure 10 – System Pop-up Screen - Top and Figure 11 – System Pop-up Screen - Bottom.

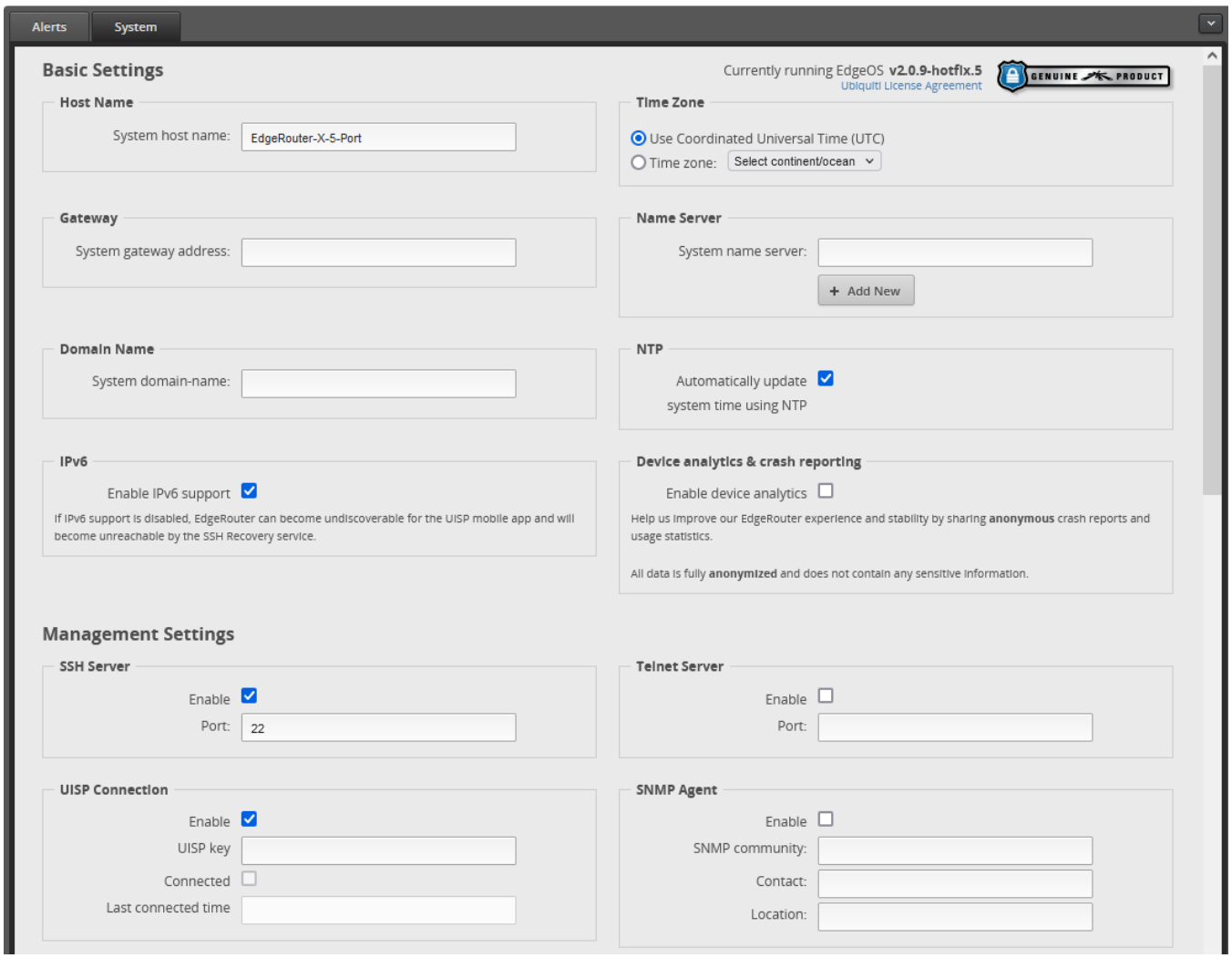


Figure 10 – System Pop-up Screen - Top

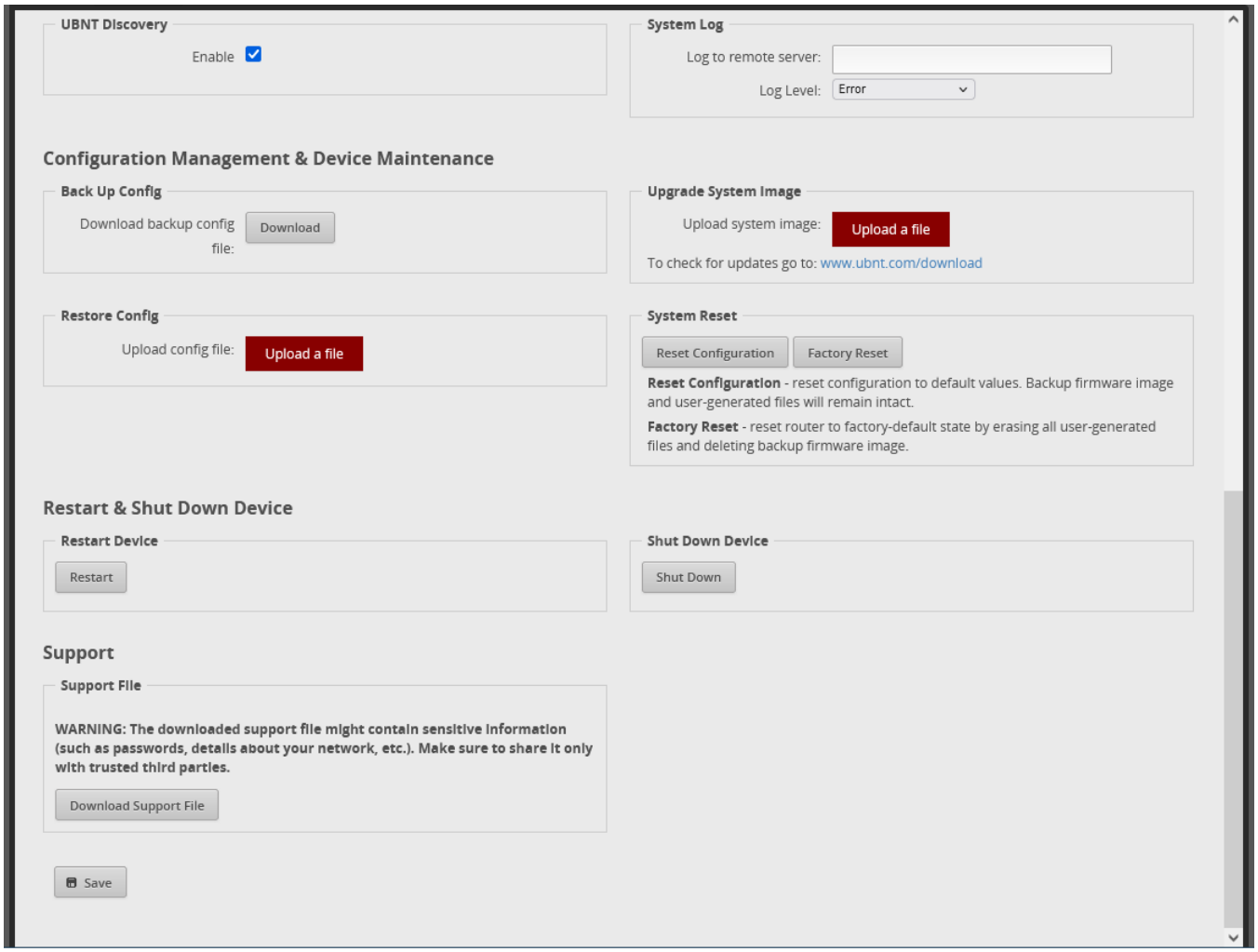


Figure 11 – System Pop-up Screen - Bottom

Find the "Upgrade System Image" section, and press the "Upload a file" button. See Figure 12 – Upgrade System Image.

Figure 12 – Upgrade System Image

Choose the firmware file that you downloaded earlier. The EdgeRouter will then install the chosen file. See Figure 13 – Uploading a System Image.

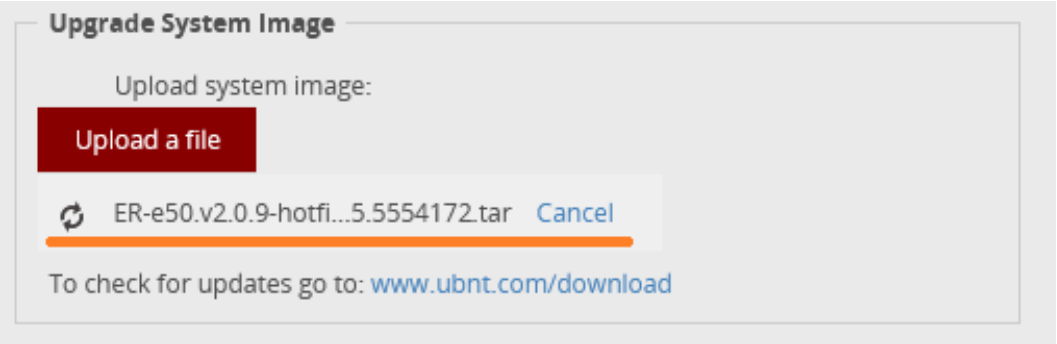


Figure 13 – Uploading a System Image

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 14 – Upgrade Complete Dialog.

The router will inform you that it is rebooting. See Figure 15 – Reboot Process.

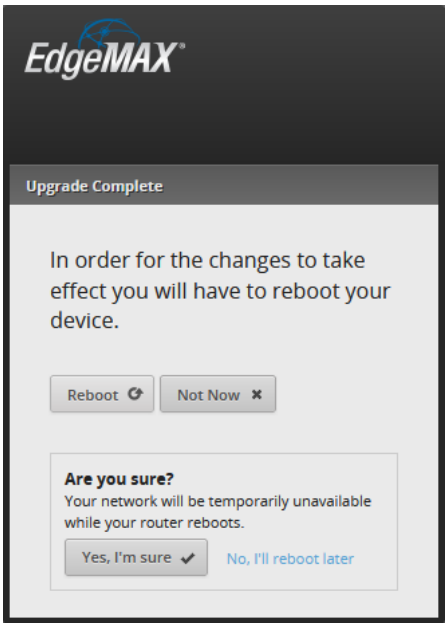


Figure 14 – Upgrade Complete Dialog

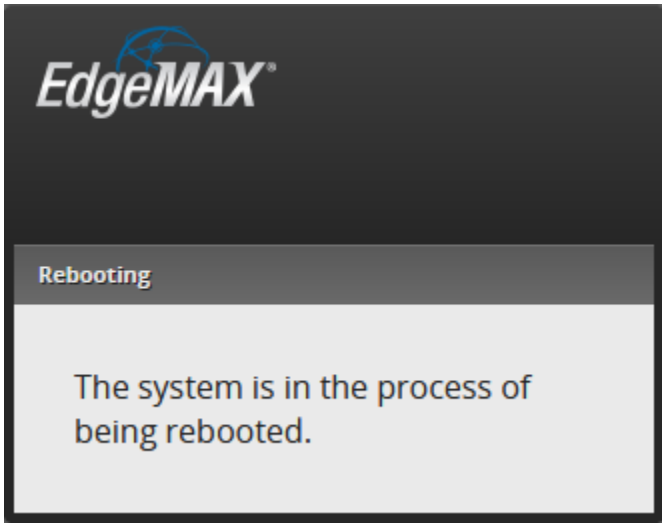


Figure 15 – Reboot Process

While the EdgeRouter is rebooting, the web page will present you with a Lost Connection Dialog. See Figure 16 – Lost Connection Dialog.

Eventually, when the EdgeRouter has fully re-booted, the presented dialog should change to Figure 17 – Timed-Out Dialog. Press the Reload button.

This is a nice touch of web programming from Ubiquiti, so you can easily know when re-booting has completed.

Some browsers may not let this dialog show, because of the invalid security certificate. If you do not see the – Timed-Out Dialog after about 5 minutes of waiting, re-enter the IP address into the browsers address bar and click past the security warning. Details are the same as in section 12 - Initial EdgeRouter Login.

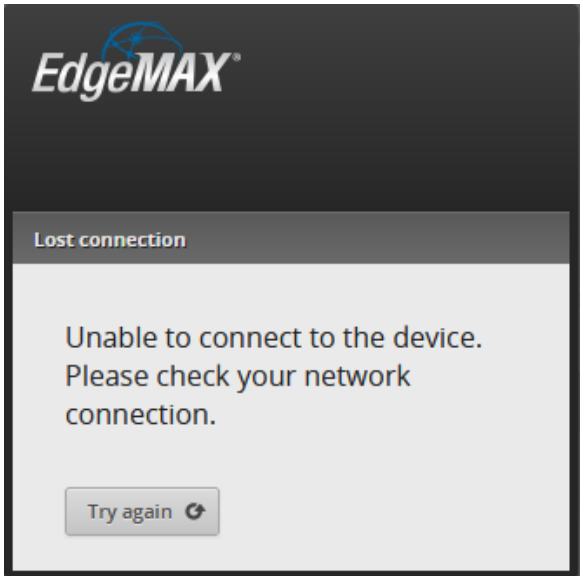


Figure 16 – Lost Connection Dialog

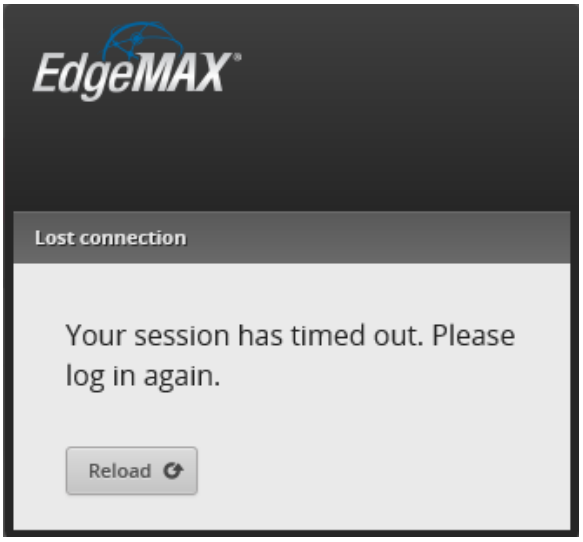


Figure 17 – Timed-Out Dialog

You will be asked to login; please re-enter the username and password into the dialog. The default username is "ubnt" and the default password is "ubnt". See Figure 18 – Login Dialog.

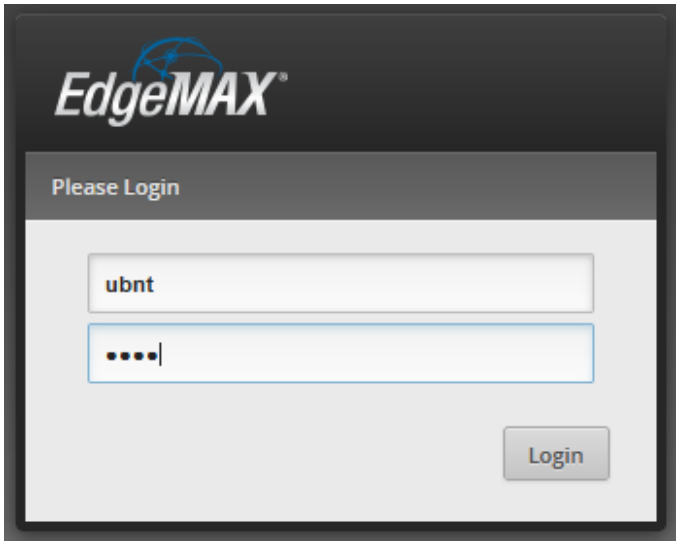


Figure 18 – Login Dialog

I was presented with a “Help Us Improve” dialog; I answered “Do not share”. See Figure 19 – Help Us Improve.

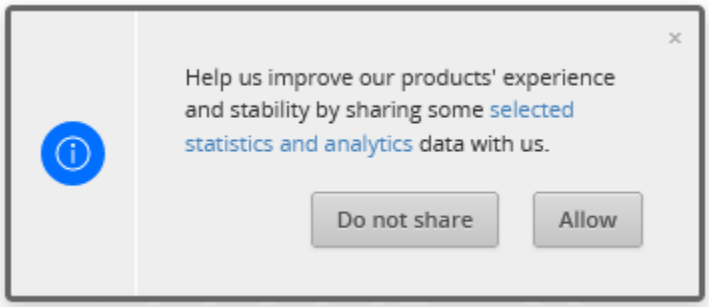


Figure 19 – Help Us Improve

You should (again) land at the Dashboard screen. Reference Figure 8 – Initial Dashboard Screen on page 28. Check the upper left of the screen and verify that you are presented with the version of code that you just downloaded. See Figure 20 – Example EdgeRouter Version.

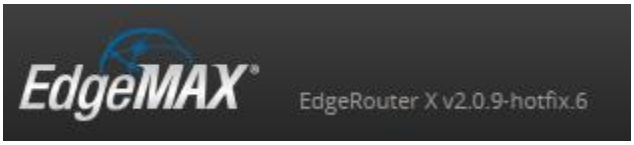


Figure 20 – Example EdgeRouter Version

Additional References:

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

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

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

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

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

https://help.ui.com/hc/en-us/articles/360019289113

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

See also section 22.1 - Emergency SSH Recovery on page 50.

The following postings are for people who want to upgrade without access to the internet, want more control over upgrading or are having problems:

https://community.ui.com/questions/Cannot-upgrade-er-x-firmware/f187730e-1537-4661-8d68-2ef3e312c2cc#answer/37dfb27a-7182-412d-987a-47cac50c8957

https://community.ui.com/questions/ER-X-Windows-server-on-VLAN-10-cant-access-default-gateway-on-router-SOLVED/3af4766d-2ee1-46d9-8914-f73a72f0c270#answer/665f503b-b726-4284-9367-4e0806d2e4ca

https://community.ui.com/questions/Help-in-upgrading-Firmware-ER-X-safely-please/79688d23-6e95-4373-b6f9-cfecda53bd75#answer/4429b51b-c316-442f-94d4-296989f1fbbe

14. About DNS Resolvers

This section is placed early, so you can decide which DNS Resolvers you are going to use within your ER-X EdgeRouter.

A DNS explanation:

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

Many dns resolvers provide malware blocking and other services, which

Within this guide, I am using Level3 DNS addresses for the Home Network and within the EdgeRouter Itself. For training / clarity purposes within this guide, I am using Google DNS resolvers for the Separate Network. I also used OpenDNS addresses for the IOT Network.

Change any or all of the listed DNS resolver addresses within this guide to your own choosing. Note that each provider maintains both primary and backup resolver addresses. Those are typically entered as a set, i.e. DNS 1 and DNS 2.

The following list names some common providers (DNS 1 address are given first, DNS 2 addresses are second):

Level3 (CenturyLink) resolver addresses	209.244.0.3	209.244.0.4
Google resolver addresses	8.8.8.8	8.8.4.4
OpenDNS resolver addresses	208.67.222.222	208.67.220.220
quad9 resolver addresses	9.9.9.9	149.112.112.112

Steve Gibson has a downloadable windows app which can help you characterize various DNS providers. Since it runs from your computer, the results are localized to your own 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 DHCP Initialization Wiring on page 25. The web (download) page is:

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

Steve Gibson has a web page that tests the “spoofability” (security) of DNS resolvers. It is:

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

Ubiquiti Help Articles:

https://help.ui.com/hc/en-us/articles/115010913367-EdgeRouter-DNS-Forwarding-Setup-Options

https://help.ui.com/hc/en-us/articles/115002673188

EdgeRouter DNS References:

https://community.ui.com/questions/ERL-3-1-9-0-No-DHCP-leases-since-switching-to-DNSMasq/7b742c2f-29cd-4a4e-95ae-bc5a14a47e38

https://community.ui.com/questions/DNS-Forwarding-Name-Servers/8a986a94-eae4-4827-bff0-a93af718ab80

https://community.ui.com/questions/Setting-up-Local-DNS/f1ae35c0-07cd-4764-bb12-0d80acb8139d

15. EdgeRouter Wizard

Press the “Wizards” button, which is located in the upper-right portion of the Dashboard screen. See Figure 21 – Wizards Button.

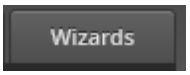


Figure 21 – Wizards Button

You will see the following (portion shown) of the Wizard Screen. See Figure 22 – Wizard Screen Portion.

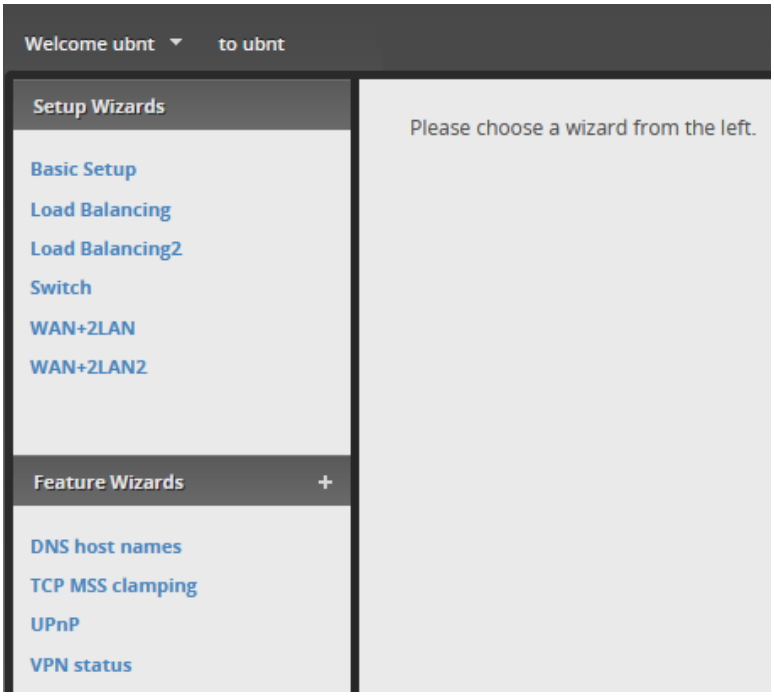


Figure 22 – Wizard Screen Portion

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”. The resulting dialog is shown here in two screenshots. See. Figure 23 – WAN+2LAN2 Dialog - Top and Figure 24 – WAN+2LAN2 Dialog - Bottom. You will need to expand / open sections, and make the following selections:

In the “Internet Port (eth0 or eth4)” section:

Port:	eth0	
Internet CT:	DHCP	(DHCP, since the ER-X is behind your existing router)
VLAN:	UN-Checked	(CHECK if your Internet Connection is on a VLAN)
IPv4 Firewall:	CHECKED	(Enable the default firewall)
IPv6 Firewall:	CHECKED	(Enable the default firewall)
DHCv6 PD:	UN-Checked	(Disable DHCv6 Prefix Delegation)

In the DNS Forwarding section:

Configure DNS servers:

Server #1:	209.244.0.3	(See section 14 - About DNS Resolvers”)
Server #2	209.244.0.4	(See section 14 - About DNS Resolvers”)

In the next (unlabeled) section:

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

Expand the “(Optional) Secondary LAN port (eth1)” section and enter:

Address:	192.168.7.1 / 255.255.255.0	
DHCP:	CHECKED	(Enable the DHCP server)

Expand the “LAN ports (eth2, eth3, eth4)” section and enter:

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

In the User setup section:

Create new admin user:

Note: default user (ubnt) will be removed

User:	<Your New User Name>
Password:	<Your New Password>
Confirm Password:	<Your New Password>

In the Analytics and crash reporting section:

Enable reporting:	UN-Checked	(What I chose)

Unchecking the “Only use one LAN” selection informs the Wizard to un-bundle eth1 from eth 2-4, allowing for the provision of a separate Network. I will use this eth1 Network for Wired IOT devices. We will later manually un-bundle other ports.

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

It is also important that you **generate a new and secure login for your ER-X and remove the default login credentials**; else your router will be attacked and hacked (within minutes!) once you put its WAN port on the internet.

Press “Apply” at the bottom of the screen.

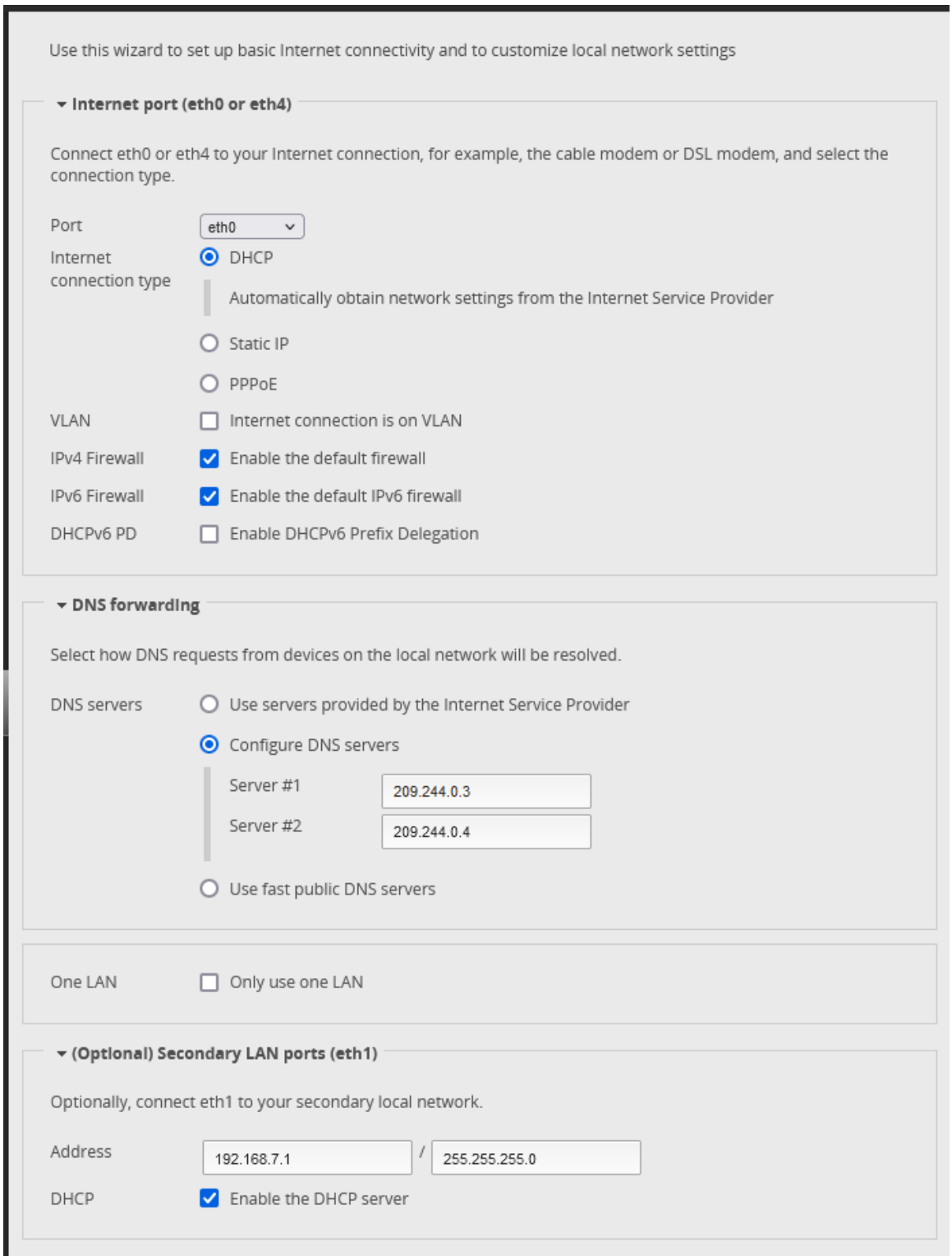


Figure 23 – WAN+2LAN2 Dialog - Top

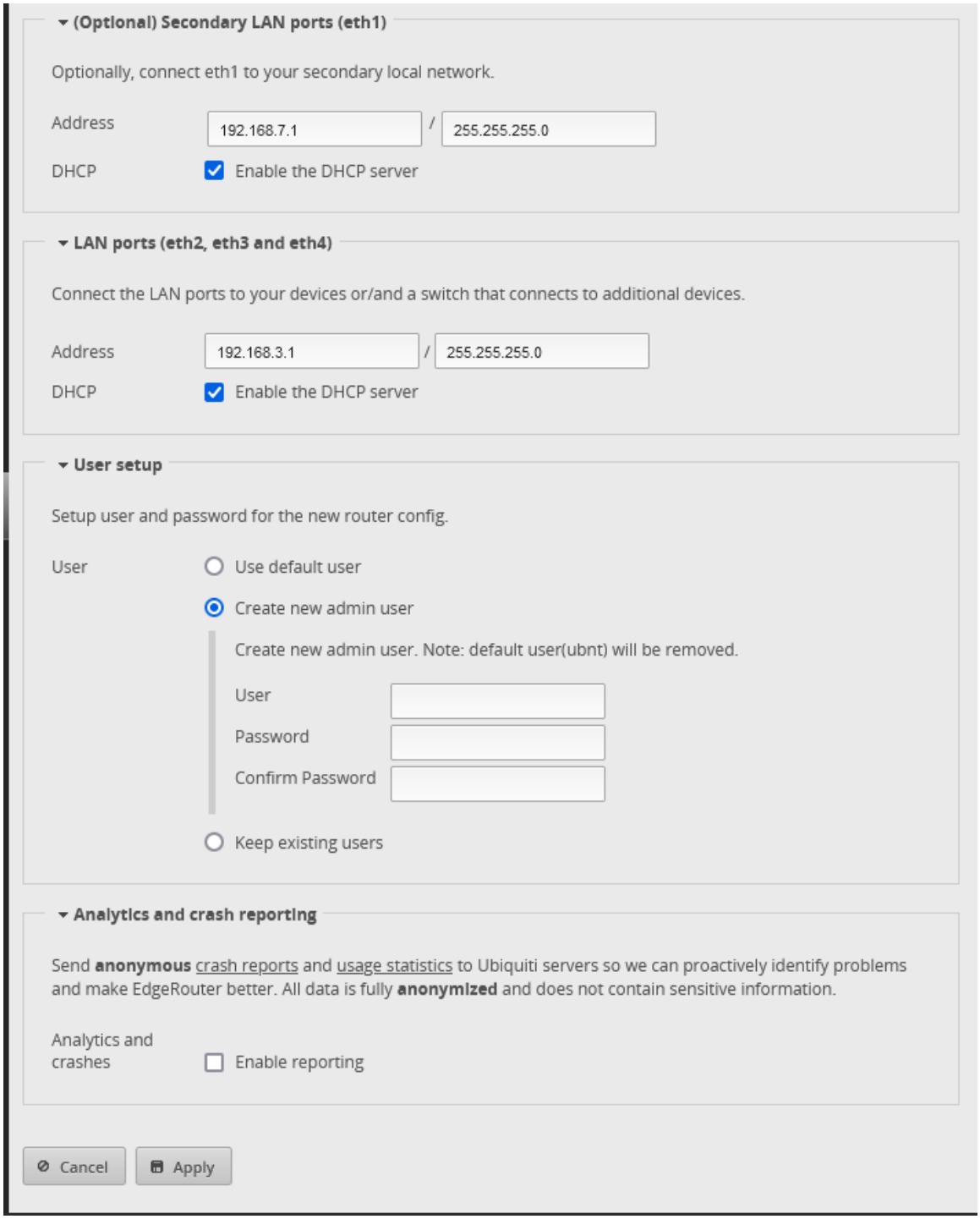


Figure 24 – WAN+2LAN2 Dialog - Bottom

After Applying, you will be presented with Figure 25 – Replace Configuration. Please study what it says. Press "Apply Changes."

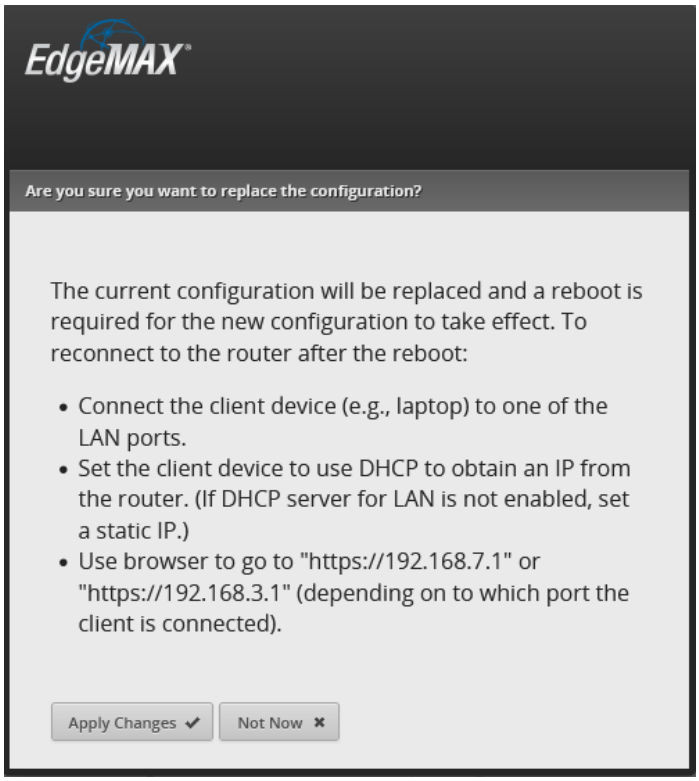


Figure 25 – Replace Configuration

Press Reboot, then confirm the reboot, by pressing the "Yes, I'm sure" button. See Figure 26 – Reboot into New Configuration.

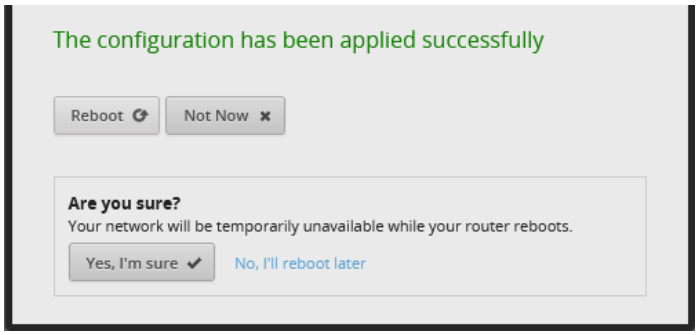


Figure 26 – Reboot into New Configuration

The EdgeRouter will inform you that it is rebooting. Reference Figure 15 – Reboot Process. The EdgeRouter takes about 5 minutes to reboot, before you will be able to login again.

Disconnect the (eth0 or eth1) Ethernet cable from the ER-X. If you followed section 11.3 - EdgeRouter Static IP Initialization, restore your Setup Computer's Ethernet port to DHCP, by re-following section 11.3, but instead using the setting "Obtain an IP address automatically." If any other Setup Computer settings were changed, like disabling Wi-Fi adapters, they can now be restored.

16. EdgeRouter Configuration Setup

Now that the Wizard has been run, we need to re-wire the ER-X's Ethernet connections, per Figure 25 – Replace Configuration on page 40. Now see Figure 27 - EdgeRouter Configuration Wiring. Your existing equipment may instead have the "Cable or DSL Modem" portion and "Your Existing Firewall / Router" portion combined into one single unit.

Connect the ER-X's eth0 (WAN) port to your existing router's LAN. Plug your Setup Computer's Ethernet port into the ER-X's **eth1** port. Note that while connected to either eth1 or eth3, your Setup Computer may not be able to connect to (some or all portions) of your existing Network and the Setup Computer will not be accessible from your existing Network. You can instead connect the Setup Computer's Ethernet port to your existing router's LAN, to restore this functionality, when not actively configuring the ER-X.

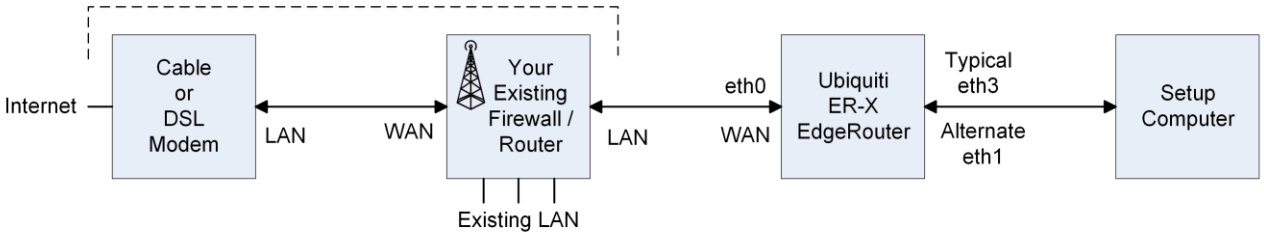


Figure 27 - EdgeRouter Configuration Wiring

Login to the ER-X using the procedure of section 12 - Initial EdgeRouter Login on page 27, but instead use the address of:

https://192.168.7.1

and use your new credentials.

17. 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. A more common term is "subnets". Each Network has a unique IP address range / subnet. See Table 2 – Network Details.

Network Name	IP Address Range	Interface	VLAN	UAP
Internet	DHCP	eth0	No	
Wired / Wi-Fi Home Network	192.168.3.X	eth3	No	*
Wired Separate Network	192.168.5.X	eth2	No	
Wi-Fi Guest Network	192.168.6.X	-	6	*
Wired / Wi-Fi IOT Network	192.168.7.X	eth1	7	*
Wi-Fi Spare Network	192.168.8.X	-	8	*
Wired Separate2 Network	192.168.9.X	(Optional)	No	

Table 2 – Network Details

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 (called trunk data) or with data from any differently numbered 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. 802.1Q is the VLAN specification. It appears that recently-manufactured unmanaged gigabit-switches are 802.1Q compatible.

You might have noticed that Table 2 – Network Details, does not show the ER-X's eth4 port. The eth4 port will eventually connect to our Ubiquiti Access Point(s) and will carry (some via VLANs), the Networks marked in the UAP column.

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.ui.com/hc/en-us/articles/204976664-EdgeRouter-Packets-Processing

18. 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 28 – CLI Button.

Figure 28 – CLI Button

The initial CLI window will appear as a semi-transparent overlay. See Figure 29 – Initial CLI Window.

Figure 29 – Initial CLI Window

Login to this window, using your EdgeRouter's user name and password. You will now be presented with a command prompt ending with a "$" character. See Figure 30 – CLI Non-Configuration Prompt.

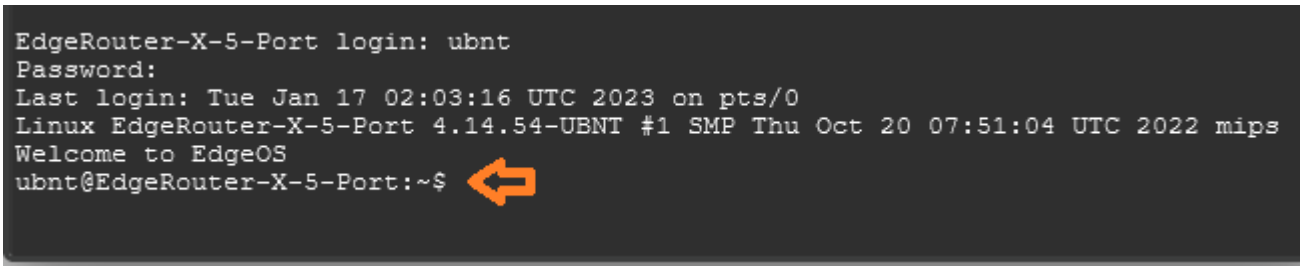


Figure 30 – CLI Non-Configuration Prompt

CLI commands are typically divided into configuration commands and non-configuration commands. The CLI interface will accept only configuration commands when in configuration mode. See Figure 31 – CLI Configuration Prompt. The "configure" command is used to enter configuration mode. If you enter the "configure" command, the CLI window's prompt will now include "[edit]", and the prompt will change to '#'. The "exit" command is used to leave configuration mode and return to the normal (non-configuration) mode.

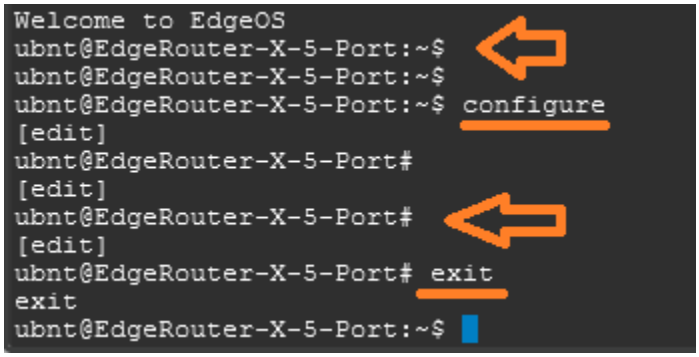


Figure 31 – CLI Configuration Prompt

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 32 – Configuration Change. Press the "Refresh" button.

Figure 32 – 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.

You can also do SSH directly from windows command interface. There is also a Windows specific program WinSCP, which is similar to SSH, but can easily transfer files between a Windows PC and the EdgeRouter.

EdgeRouters also support 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.ui.com/questions/EdgeOS-CLI-Primer-part-1/dc0a7754-1bcf-4ca0-9d02-239100dbc926

19. 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 33 – Config Tree Button.

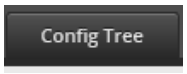


Figure 33 – Config Tree Button

When you press it, the “Configuration” Tree window will appear. See Figure 34 – Config Tree Initial Screen.

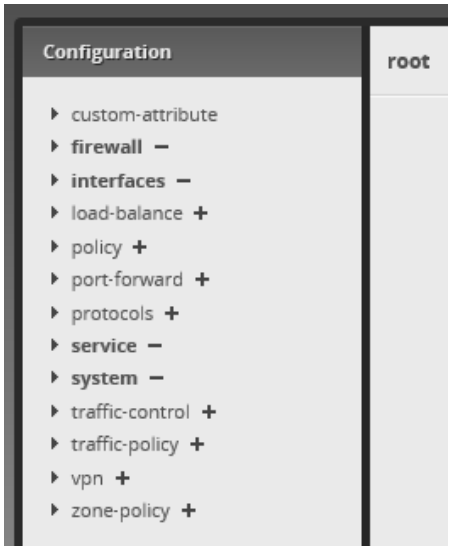


Figure 34 – Config Tree Initial Screen

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

20. 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, and this helped.

See Figure 35 – Example of Multiple Config Tree Commands.

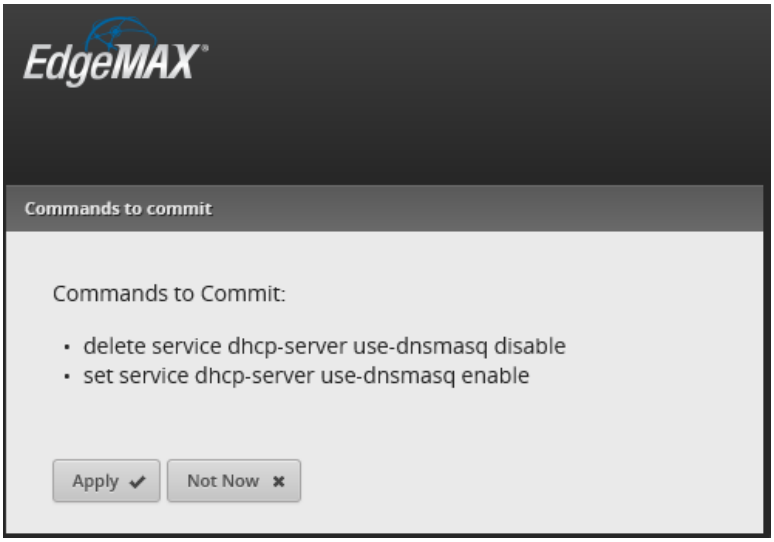


Figure 35 – Example of Multiple Config Tree Commands

21. EdgeRouter Backup / Restore Configuration Files

When EdgeRouters are described in most community / 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 36 – Back Up Config Download Button.

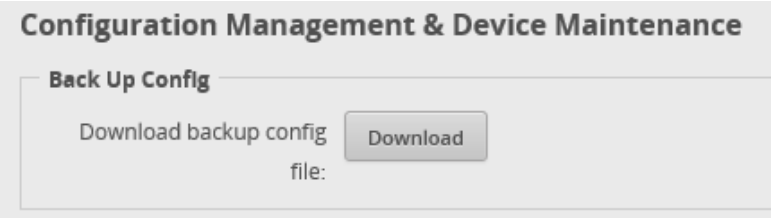


Figure 36 – Back Up Config Download Button

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 should 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 "18 - EdgeRouter Command Line Interface (CLI)".

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. Most experienced Community members will give forum answers as command lines, so learning is pretty much manaditory.

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 which in-turn depends upon …

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 37 – Restore Config Upload a file Button.

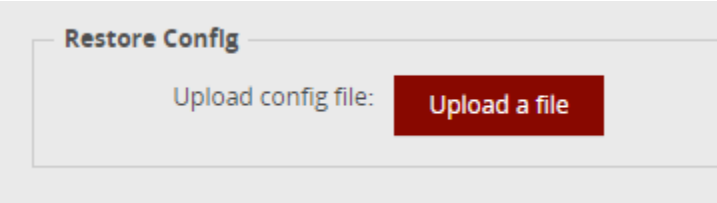


Figure 37 – Restore Config Upload a file Button

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 18 - EdgeRouter Command Line Interface (CLI).

Link(s):

https://help.ui.com/hc/en-us/articles/360002535514

https://community.ui.com/questions/Edgerouter-CLI-command/2d8e5ddd-abd0-4df6-889c-0b6831c78c46

22. ER-X 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 to the newest released version.

Reference:

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

You probably don't want to attempt a bootloader update during a thunderstorm, ice storm, or any other time where power is more likely to go out; you will have increased risk of "bricking" your ER-X.

Per the above link, I ran the following CLI / SSH / PuTTY command on a *new* ER-X:

```
show system boot-image
```

and got the following text:

```
The system currently has the following boot image installed:
Current boot version: e50_003_9a910
Current boot md5sum : 503cf8c994a9b70375287638e035f577
```

That text didn't necessarily confirm that the installed version listed was actually the newest bootloader available, so I issued the following command:

```
add system boot-image
```

I received the following message:

```
Currently installed bootloader version e50_003_9a910 is up to date.
Bootloader upgrade is not needed.
```

The following is what occurred when I was updating the bootloader on an *older* model of ER-X. This update happened a couple of years ago, so the versions below are different than above.

I ran the following CLI / SSH / PuTTY command on an *older* ER-X:

```
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 then updated my bootloader with `add system boot-image` (and `yes`) and received 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 for the ER-X to reboot.

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
```

22.1 Emergency SSH Recovery

Release Notes for EdgeMAX EdgeRouter software release v1.10.0
[Ssh-recovery] - This is new service which starts during early boot stage and provides emergency SSH access via IPv6 link-local address. ssh-recovery can be used to access shell from directly connected neighborif router is not accessible by normal means. By default ssh-recovery service is listening on port 60257 on all Ethernet interfaces and it is automatically terminated 60 seconds after boot. More information is available in this article:
https://community.ui.com/questions/new-feature-explaining-ssh-recovery-service-in-v1-10-0-alpha-1/9c871261-6493-4f06-b78c-3f3560dff552
From:
https://community.ui.com/releases/EdgeMAX-EdgeRouter-software-release-v1-10-0-1-10-0/5433d795-9553-46bc-8607-2415bcfa820d

The following is cached from the above URL:

> Lets assume that ER-EVE is an EdgeRouter which was misconfigured and the admin can't access it by SSH/WebGUI, but he has SSH access to ER-WALLE.
>
> The following steps describe how an admin can reach ER-EVE via ssh-recovery from ER-WALLE:
>
> Login to ER-WALLE:
> Make sure that llssh bash script is present on ER-WALLE
> If ER-WALLE is an EdgeRouter then llssh is already available in /usr/bin/
> Identify eth0 MAC address of ER-EVE or its serial number which is printed on the bottom of the router.
> Lets suppose that eth0 MAC address is "04:18:d6:83:98:F0" (corresponding s/n is "0418D68398F0")
>
> Reboot ER-EVE. This step is needed because by default ssh-recovery service is active only 60 seconds after boot.
> Run following command from ER-WALLE which will search for EdgeRouter with s/n 0418D68398F0 on eth1 interface:
>
> ```
> llssh -m 0418D68398F0 -i eth1 -u ubnt
> ```
>
> User ubnt will reach SSH on ER-EVE after successful authentication:
>
> ```
> Welcome to EdgeOS …
> ```

23. Enabling the ER-X's VLAN Switch

This section will enable the ER-X's internal VLAN switch chip. When configuring switch0 to be VLAN Aware, it is important to NOT be connected to an EdgeRouter port which is actively using switch0. Therefore, ensure your Setup Computer is connected to the ER-X's eth1 port. Un-bundling of eth1 (from the switch) occurred during section 15 - EdgeRouter Wizard.

I locked myself out of my ER-X (and had to factory reset / reload the base configuration) about 4 times while researching and writing this section. You should generate an EdgeRouter backup, now.

Press the Dashboard Button. See Figure 38 – Dashboard Button.

Figure 38 – Dashboard Button

On the right side of the Dashboard screen, select switch0's "Actions" button. See Figure 39 – switch0 Actions Button

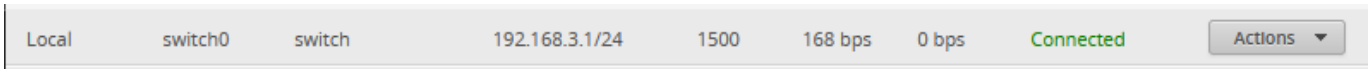


Figure 39 – switch0 Actions Button

A sub-menu will appear, Select "Config" from the menu item. See Figure 40 – switch0 Actions Config.

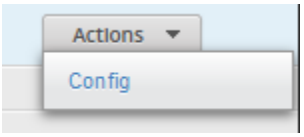


Figure 40 – switch0 Actions Config

Note: If the following dialog(s) gets stuck, gets set too small, or does not refresh, re-click the opposite Tab (Config / Vlan), then re-click the original tab you were on (Vlan / Config) to refresh the dialog / size.

You will be presented with the configuration dialog for switch0. See Figure 41 – switch0 Initial Config.

When the ER-X is configured to be VLAN Aware, switch0 is not allowed to have an IP address. Change the address to “No Address”; see Figure 42 – switch0 New Config.

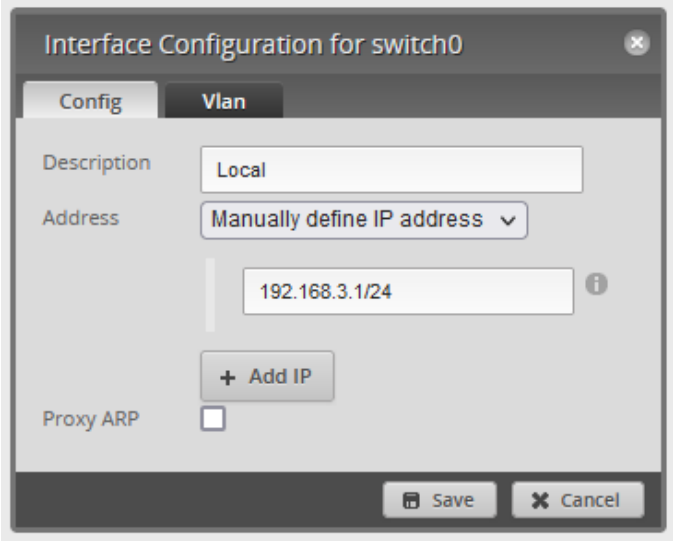


Figure 41 – switch0 Initial Config

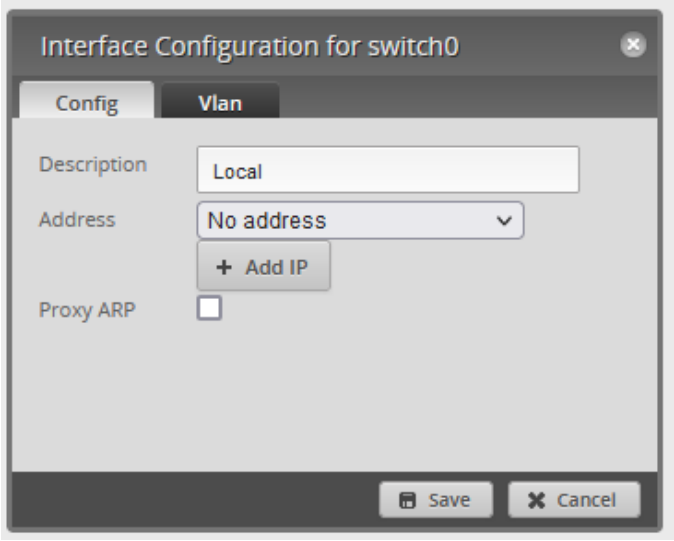


Figure 42 – switch0 New Config

Click on the Vlan Tab, See Figure 43 – switch0 Initial Vlan.

On the Vlan Tab, make the following changes:

```
Dashboard
    Switch0 Actions / Config
        Vlan
            Vlan Aware Enabled CHECKED
            eth0 Un-Checked
            eth1 Un-Checked
            eth2 Un-Checked
            eth3 CHECKED
            eth3 pvid 1
            eth3 vid <Empty>
            eth4 CHECKED
            eth4 pvid 1
            eth4 vid <Empty>
```

See Figure 44 – switch0 New Vlan.
Click `Save`

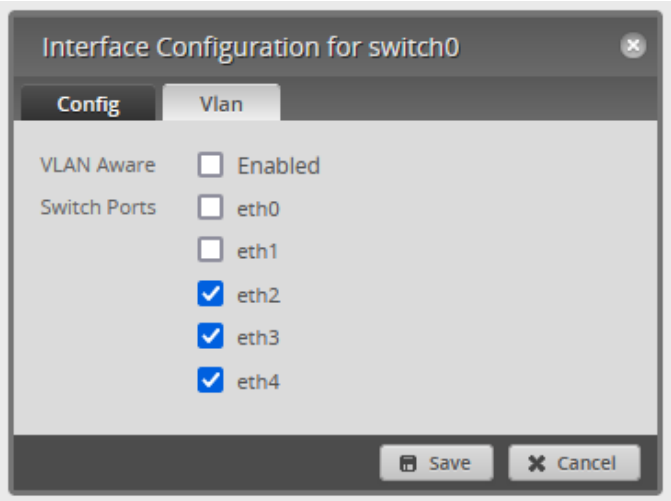


Figure 43 – switch0 Initial Vlan

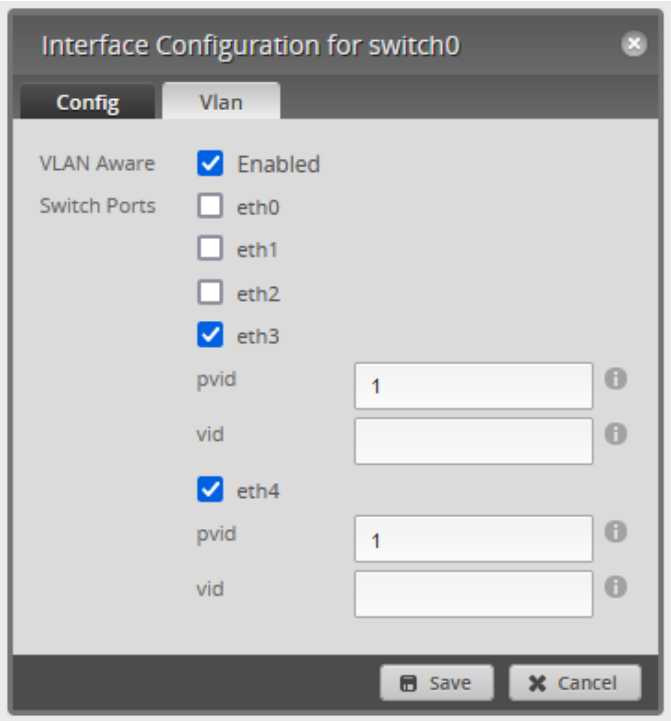


Figure 44 – switch0 New Vlan

While the EdgeRouter is completing this / a task, a busy indicator will spin, in the upper right corner of the dialog. See Figure 45 – 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 46 – Finished Checkmark.

Figure 45 – Busy Indicator

Figure 46 – Finished Checkmark

While enabling VLAN Awareness, we needed to disable the Home Network's IP address range. We will now re-enable that address range, but inside a VLAN.

Press the Dashboard Button. Reference Figure 38 – Dashboard Button. Press the "Add Interface" button; see Figure 47 – Add Interface Button. Select the sub-menu "Add VLAN", see Figure 48 – Add VLAN. You should see Figure 49 – Create New Vlan.

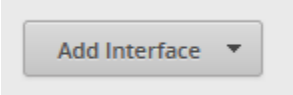


Figure 47 – Add Interface Button

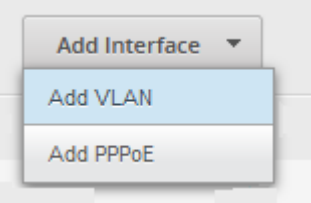


Figure 48 – Add VLAN

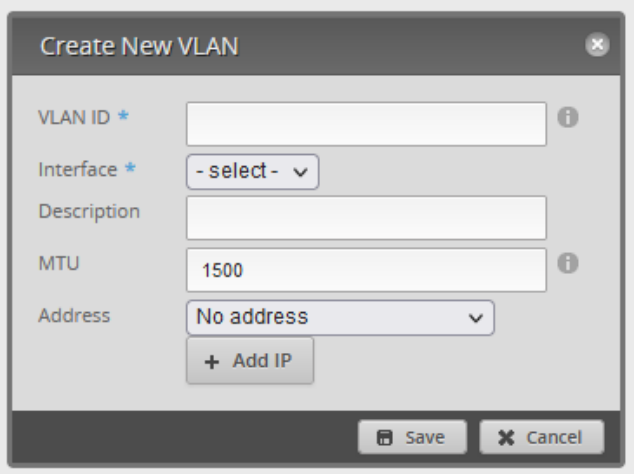


Figure 49 – Create New Vlan

Fill in the form as follows:

```
Dashboard
        Add Interface
            Add VLAN
                VLAN ID:        1
                Interface:      switch0
                Description:    HomeNet
                MTU:            1500
                Address:        Manually define IP Address
                                192.168.3.1/24
                Save
```

A new dashboard line should appear. See Figure 50 – switch0.1 HomeNet.

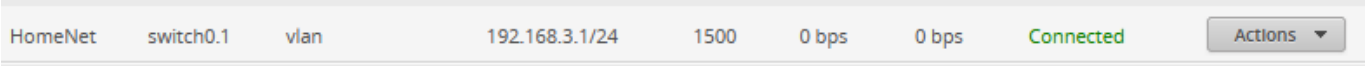


Figure 50 – switch0.1 HomeNet

At this point we should have just been able to disconnect the Setup Computer from eth1 and re-connect it to eth3. When I did this, I did not receive a DHCP address from the ER-X. It is probably an EdgeRouter bug. To circumvent this issue, we will reboot the ER-X, after the following "references" section.

23.1 Networking and VLAN References

Ubiquiti Help Article:

https://help.ui.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch

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

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

A well-referenced VLAN posting: How I solved it.

https://community.ui.com/questions/EdgeRouter-X-Inter-VLAN-routing-issues-How-I-solved-it/6546bf5d-3d92-4580-8bba-13320436735b

General Networking References:

@BuckeyeNet posting of a collection of links, including 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

VLAN References:

https://community.ui.com/questions/riddle-me-this-ER-X-how-do-I-set-a-native-VLAN-on-the-switch/88430200-4660-4721-816f-4e1cb8c2ec00#answer/28f6ebd5-8c78-47a0-b6e1-1fa649db9265

QC Ubiquiti EdgeMAX - Using VLAN 1 on a vlan-aware switch0 Interface
https://www.youtube.com/watch?v=raZHQjaj4iY

QC Ubiquiti EdgeMAX - UAP with Guest WLAN & VLAN Trunks (VIF)
https://www.youtube.com/watch?v=SKeFqFhBwJY

https://community.ui.com/questions/Adding-a-new-subnet-to-an-Edge-Router-X/32a23bd6-6a09-49c8-b4d3-0b9603125026

https://community.ui.com/questions/Need-recommendation-on-tweaking-config-to-support-some-VLAN-trunks-on-a-multizone-network/cc488eec-7c28-48b0-abb4-a4be0cfff284

Differences between being VLAN Aware and NOT being VLAN Aware:

@BuckeyeNet posting
https://community.ui.com/questions/EdgeRouter-X-VLAN-config-for-switch0-with-LAN-and-VLAN-on-same-port/ed673cf2-2b11-46dc-b9a5-a2519d4807d2#answer/51064ee1-87b7-43d6-a5fe-78a29e8442d4

24. Reboot the ER-X

EdgeRouter's don't like having the power unexpectedly removed, it is better to gracefully reboot them.

To re-boot the ER-X, open the System pop-up dialog by pressing the System button (Reference Figure 9 – System Button on page 29). On the lower portion of the System pop-up window (Reference Figure 11 – System Pop-up Screen - Bottom on page 31), find and press the "Restart" button. See Figure 51 – Restart Button .

Figure 51 – Restart Button

You will be presented with a Restart dialog. See Figure 52 – Restart Dialog. Press "Restart". When presented with the confirmation dialog, press "Yes, I'm sure" See Figure 53 – Restart Confirmation.

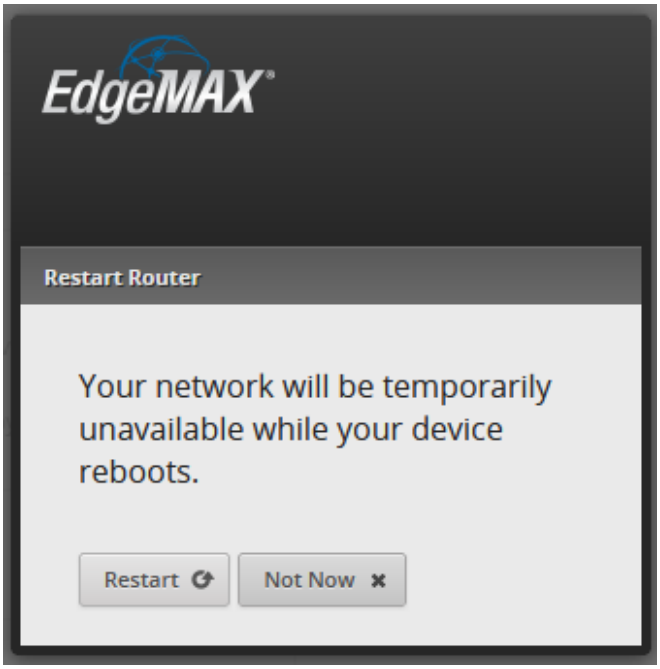


Figure 52 – Restart Dialog

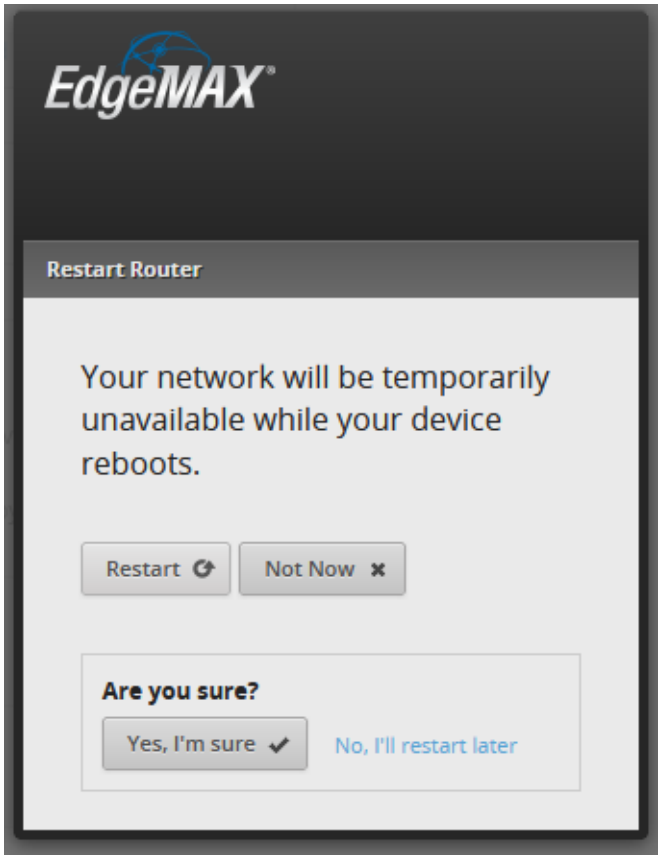


Figure 53 – Restart Confirmation

The ER-X will confirm the reboot, with a “Rebooting” dialog. See Figure 54 – Rebooting Dialog.

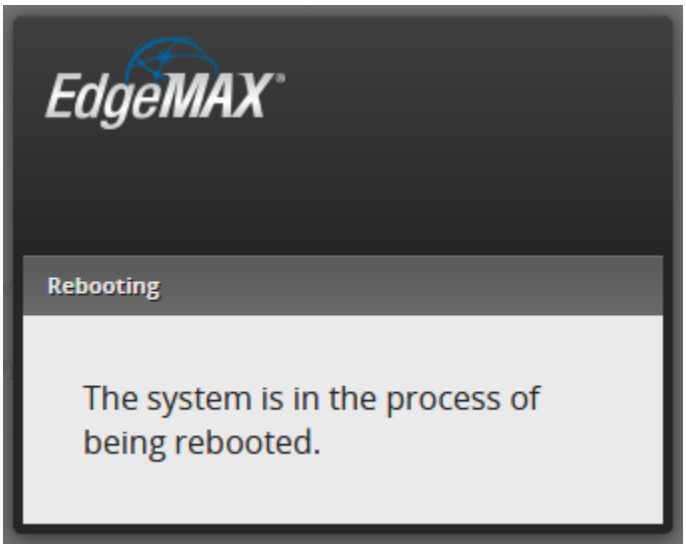


Figure 54 – Rebooting Dialog

It takes about 5 minutes for an ER-X to reboot.

25. Re-Connect to the ER-X

While the ER-X is rebooting, disconnect your Setup Computer's Ethernet cable from eth1. Wait 5 to 10 seconds. Then re-connect your computer's Ethernet cable to **eth3** / Home Network. Reference Figure 27 - EdgeRouter Configuration Wiring on page 41. Open a new Browser window/tab, enter a URL of https://192.168.3.1 and Login to the EdgeRouter.

26. Remove IP address from eth1

Now that we used the ER-X’s (non switch0) eth1 port to enable VLAN Awareness, we need to setup eth1 under switch0, i.e. have eth1 use a VLAN. In preparation for that (later) step, we first need to remove the IP address from the eth1 port.

From the Dashboard screen, find eth1’s line and click on the Actions button. See Figure 55 – eth1 Local line.

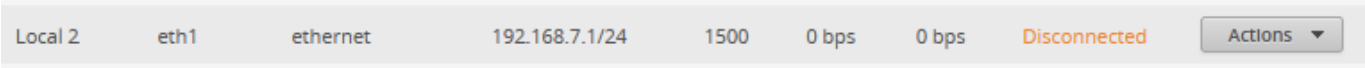


Figure 55 – eth1 Local line

Clicking "Actions", will produce an Action Menu. See Figure 56 – Actions Menu.

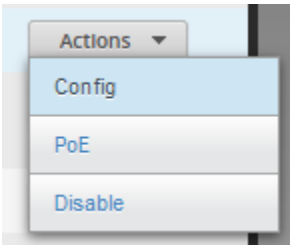


Figure 56 – Actions Menu

Select "Config". You will be presented with an eth1 configuration dialog. See Figure 57 – eth1 Original Dialog.

Fill in the form as follows:

```
Local eth1
    Actions
        Configure
            Description     IotNet
            Enable          <CHECKED>
            Address         No Address
            MTU             1500
            Speed/Duplex    Auto negotiation
            Proxy ARP       <Un-Checked>
```

Your form should look like Figure 58 – eth1 No Address - Named.

Press Save

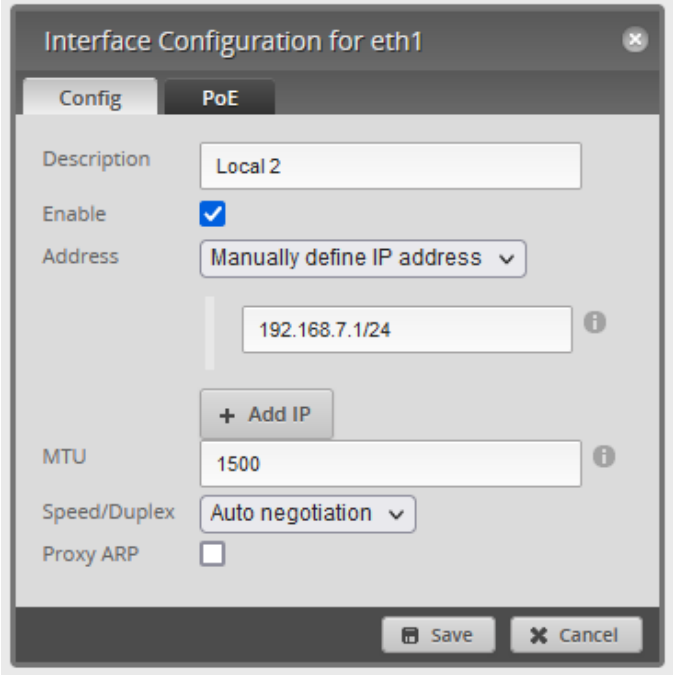


Figure 57 – eth1 Original Dialog

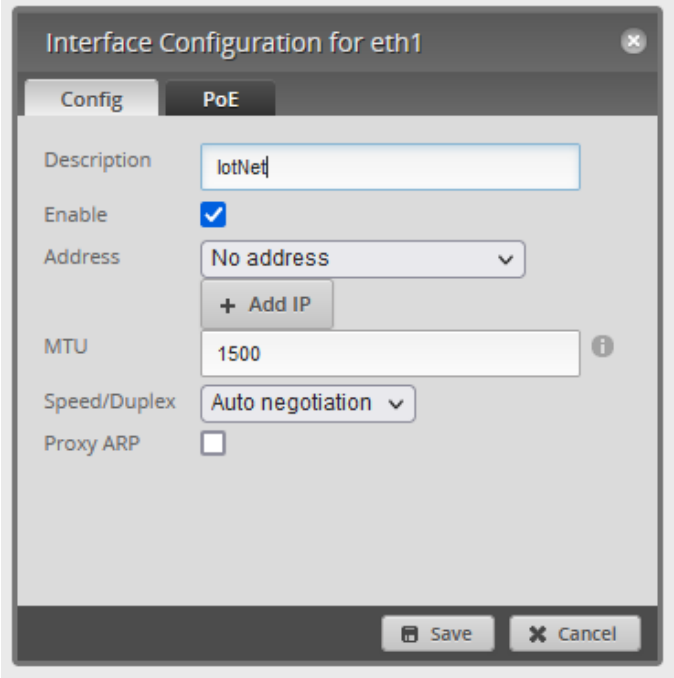


Figure 58 – eth1 No Address - Named

27. Add VLAN Networks to the ER-X

Ubiquiti's Wi-Fi Access Points can manage up to four separate Networks / SSIDs, by using VLANS. VLANS allow (logically) 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", reference Figure 38 – Dashboard Button on page 51. Press the "Add Interface" button; reference Figure 47 – Add Interface Button on page 54. Select the sub-menu "Add VLAN", reference Figure 48 – Add VLAN on page 54. You will be presented with the "Create New VLAN" dialog. Reference Figure 49 – Create New Vlan on page 54.

Fill in the form as follows:

```
Dashboard
        Add Interface
            Add VLAN
                VLAN ID:        6
                Interface:      switch0
                Description:    GuestNet
                MTU:            1500
                Address:        Manually define IP Address
                                192.168.6.1/24
                Save
```

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

```
Dashboard
        Add Interface
            Add VLAN
                VLAN ID:        7
                Interface:      switch0
                Description:    IotNet
                MTU:            1500
                Address:        Manually define IP Address
                                192.168.7.1/24
                Save


Dashboard
        Add Interface
            Add VLAN
                VLAN ID:        8
                Interface:      switch0
                Description:    SpareNet
                MTU:            1500
                Address:        Manually define IP Address
                                192.168.8.1/24
                Save
```

28. Finish configuring the Vlans

Now that we have created our Vlans, we need to inform switch0 about where those Vlan's (data) should be routed. Reference Table 2 – Network Details on page 42.

The ER-X's `eth1` port should carry `Iot` data. We configure this via switch0. Follow the steps in section 23 - Enabling the ER-X's VLAN Switch on page 51, especially Figure 44 – switch0 New Vlan on page 53.

On the Vlan Tab, make **only the following changes**:

```
Dashboard
    Local Switch0    -> Actions / Config
        Vlan
            eth1 CHECKED
            eth1 pvid 7
```

The changed portion should look like Figure 59 – switch0 eth1

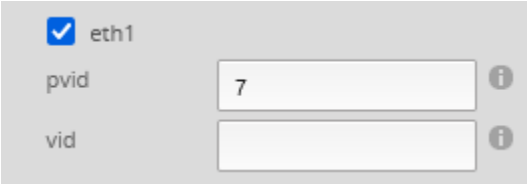


Figure 59 – switch0 eth1 settings

Click `Save`

The ER-X's `eth4` port needs to carry all of: `HomeNet`, `GuestNet`, `IotNet`, and `SpareNet` data. These Networks (sub-nets) need to be provided to our Ubiquiti Access Point(s) via a single ER-X port and be transferred via a single Ethernet cable to the single Ethernet port on the UAP(s). That's why VLANs were invented.

Again, follow the steps in section 23 - Enabling the ER-X's VLAN Switch on page 51, especially Figure 44 – switch0 New Vlan on page 53.

On the Vlan Tab, make **only the following changes**:

```
Dashboard
switch0 switch0    -> Actions / Config
   Vlan Tab
   Eth4 CHECKED
   eth4 pvid 1
   eth4 vid  6,7,8
```

The changed portion should look like Figure 60 – Switch0 eth4 Settings

Figure 60 – Switch0 eth4 Settings

Click `Save`

29. Configure EdgeRouter's eth2 IP Addresses

Note that we un-bundled eth2's interface from switch0 in section 23 - Enabling the ER-X's VLAN Switch on page 51. Now, eth2 needs an IP address assigned to its interface.

On the right side of the Dashboard screen select eth2's "Actions" button. See Figure 61 – eth2's Actions Button.

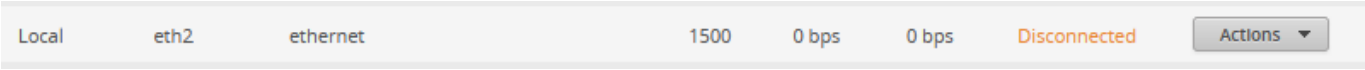


Figure 61 – eth2's Actions Button

A sub-menu will appear, reference Figure 56 – Actions Menu.

Select "`Config`". You will be presented with Figure 62 – Initial Configuration for eth2 Dialog.

Fill in the form as follows:

```
Local eth2
   Actions / Configure
      Description   SeparateNet
      Enable        CHECKED
      Address       Manually define IP Address
                    192.168.5.1/24
      MTU           1500
```

Your form should look like Figure 63 – eth2 Address Dialog.

Press `Save`

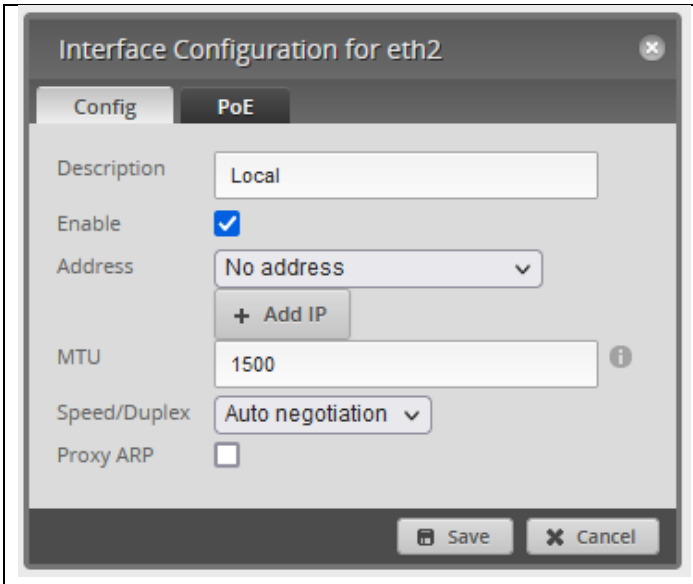


Figure 62 – Initial Configuration for eth2 Dialog

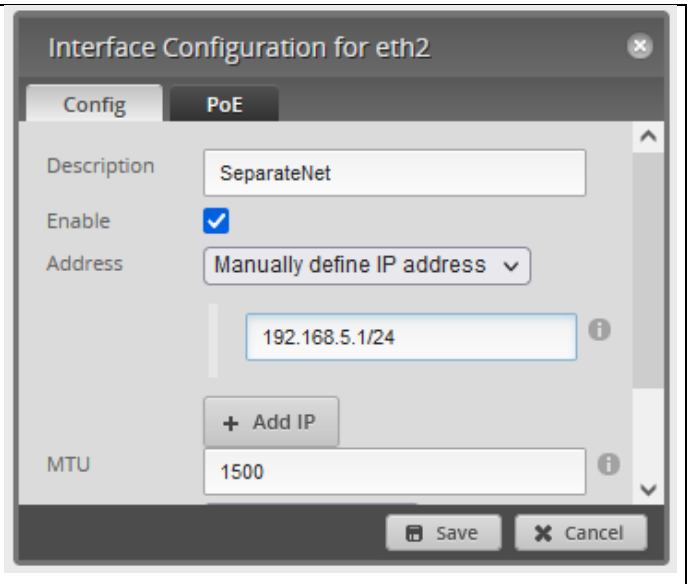


Figure 63 – eth2 Address Dialog

So that you can become familiar with the EdgeRouters config file, (Reference section 21 - EdgeRouter Backup / Restore Configuration Files), see Equation 1 – Example config - interfaces, for a sample interfaces section.

```
interfaces {
    ethernet eth0 {
        address dhcp
        description Internet
        duplex auto
        firewall {
            in {
                ipv6-name WANv6_IN
                name WAN_IN
            }
            local {
                ipv6-name WANv6_LOCAL
                name WAN_LOCAL
            }
        }
        speed auto
    }
    ethernet eth1 {
        description IotNet
        duplex auto
        speed auto
    }
    ethernet eth2 {
        address 192.168.5.1/24
        description SeparateNet
        duplex auto
        speed auto
    }
    ethernet eth3 {
        description Local
        duplex auto
        speed auto
    }
    ethernet eth4 {
        description Local
        duplex auto
        poe {
            output off
        }
        speed auto
    }
    loopback lo {
    }
    switch switch0 {
        description Local
        mtu 1500
        switch-port {
            interface eth1 {
                vlan {
                    pvid 7
                }
            }
            interface eth3 {
                vlan {
                    pvid 1
                }
            }
            interface eth4 {
                vlan {
                    pvid 1
                    vid 6
                    vid 7
                    vid 8
                }
            }
            vlan-aware enable
        }
        vif 1 {
            address 192.168.3.1/24
            description HomeNet
            mtu 1500
        }
        vif 6 {
            address 192.168.6.1/24
            description GuestNet
            mtu 1500
        }
        vif 7 {
            address 192.168.7.1/24
            description IotNet
            mtu 1500
        }
        vif 8 {
            address 192.168.8.1/24
            description SpareNet
            mtu 1500
        }
    }
}
```

Equation 1 – Example config - interfaces

30. Setup eth2's 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 64 – Services Button.

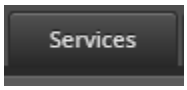


Figure 64 – Services Button

Ensure that the "DHCP Server" tab is selected. See Figure 65 – DHCP Server Screen.

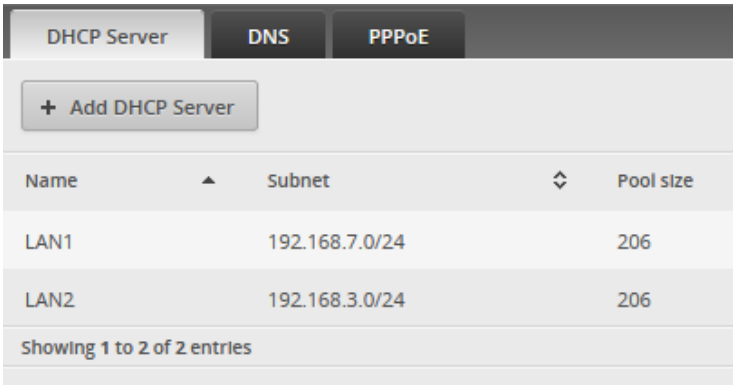


Figure 65 – DHCP Server Screen

Click on the "+ Add DHCP Server" button. See Figure 66 – Add DHCP Server Button.

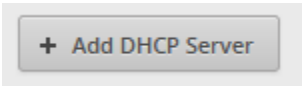


Figure 66 – Add DHCP Server Button

You will be presented with a Create DHCP Server dialog. See Figure 67 – Create DHCP Server Dialog.

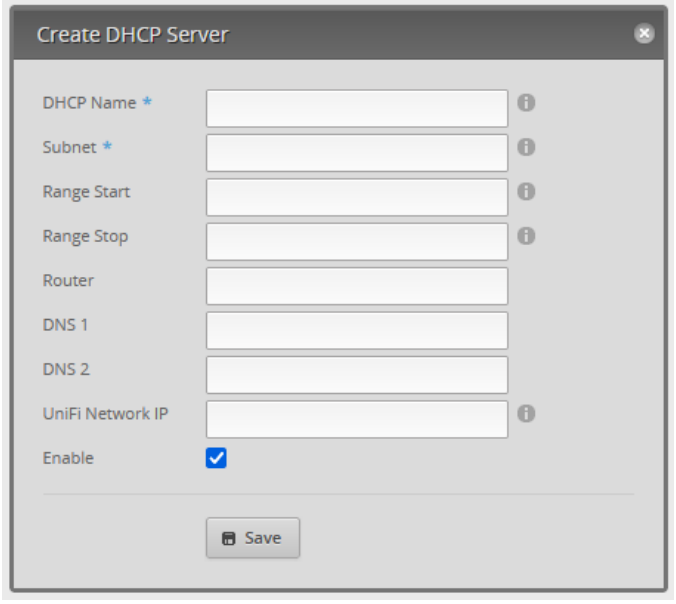


Figure 67 – Create DHCP Server Dialog

Fill in the form as follows:

```
DHCP Name:          SeparateDHCP
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 Network IP:   <Leave Blank>
Enable:             <CHECKED>
```

Your DHCP details should look like Figure 68 – eth2 DHCP Details.

Click `Save`

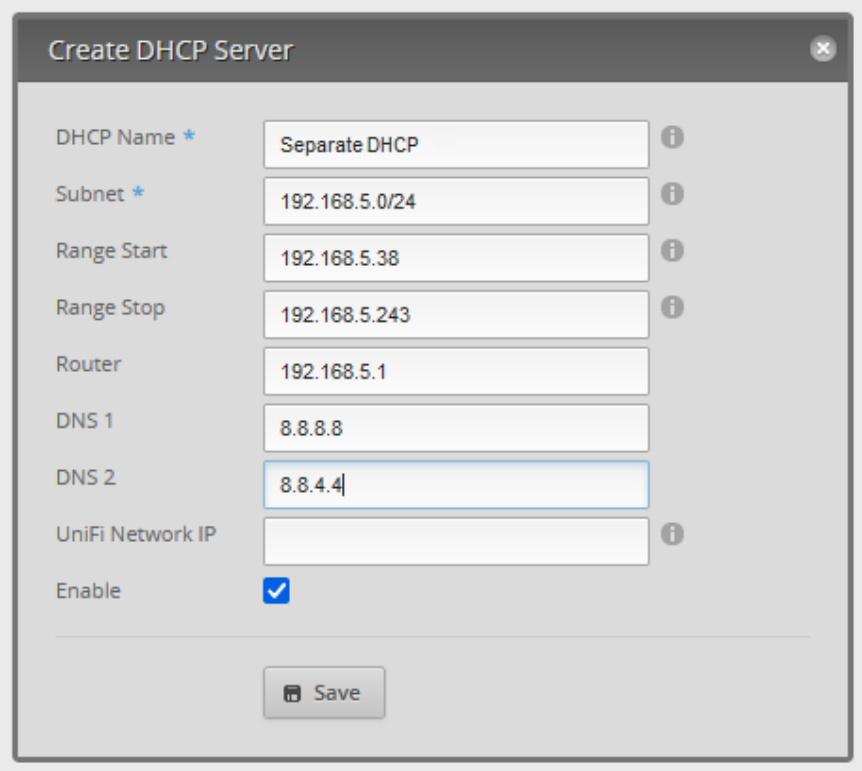


Figure 68 – eth2 DHCP Details

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.

31. Make a DHCP Server 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, or may timeout and never 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 “19 - EdgeRouter Config Tree.” Select and open up the following config tree sub-menu items from the configuration screen:

```
Config Tree
   Service
      dhcp-server
         shared-network-name
```

In the same sub-menu, click on the DHCP server you want to configure; in this case, it is:

```
      SeparateDHCP
```

You should see some DHCP settings, including authoritative. See Figure 69 – Authoritative Example.

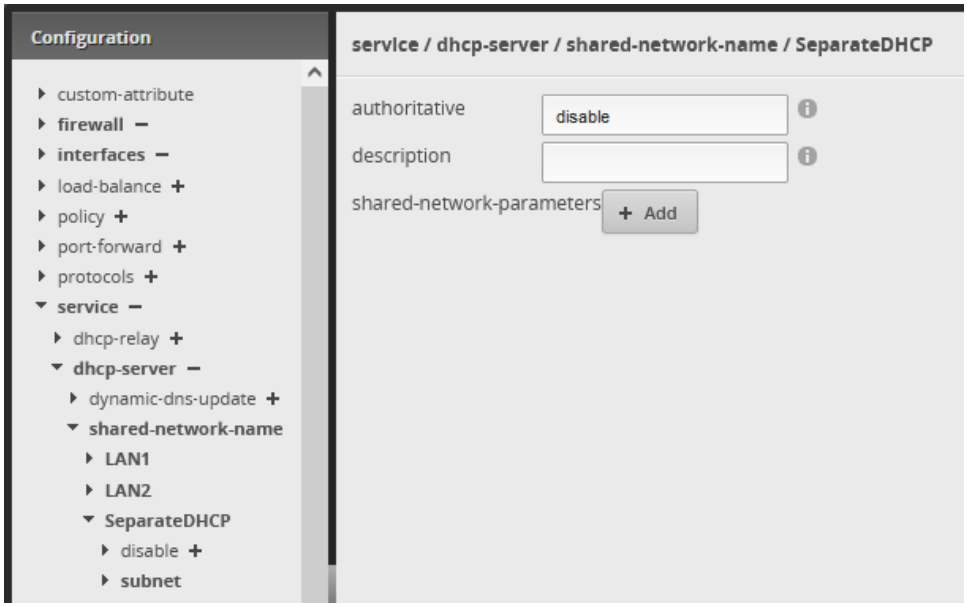


Figure 69 – Authoritative Example

Type “`enable`” in the authoritative box. This action is not shown in a Figure. Then press the “Preview” button. See Figure 70 – Preview Button.

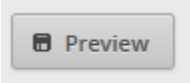


Figure 70 – Preview Button

You will then see a preview of the “Command to commit”. See Figure 71 – SeparateNet DHCP Authoritative Preview. This shows you what command(s) a ConfigTree action will execute.

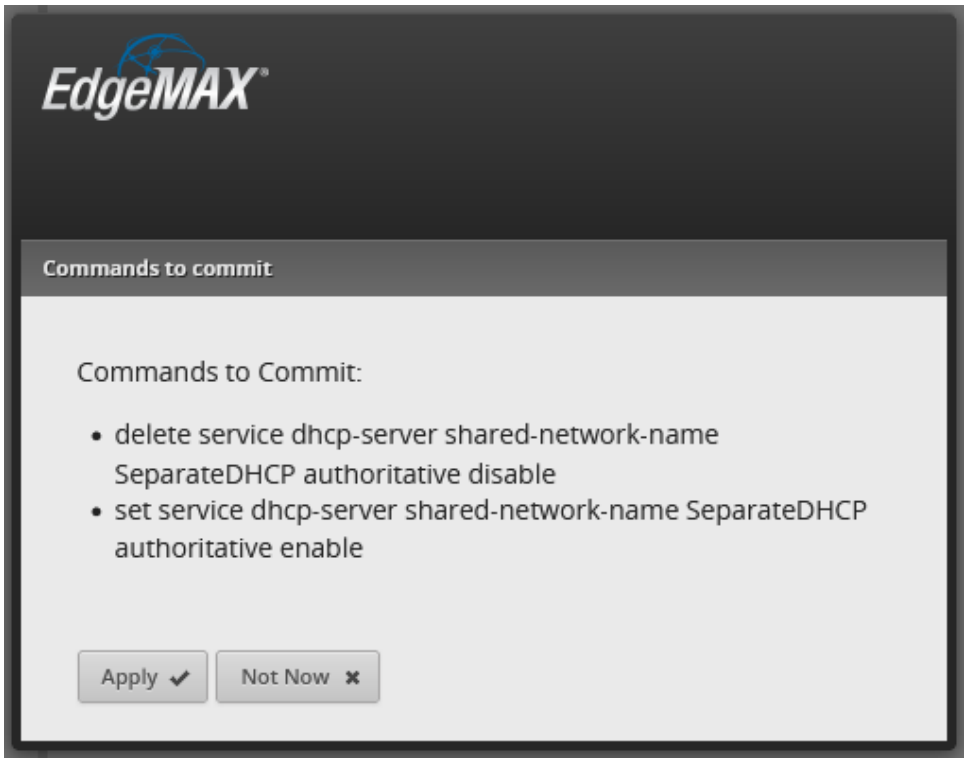


Figure 71 – SeparateNet DHCP Authoritative Preview

Press “Apply.” After a moment, you should see the message “The configuration has been applied successfully”, in green, near the bottom of the screen. See Figure 72 – Configuration Applied Successfully.

Figure 72 – Configuration Applied Successfully

32. Set Domain Name / DNS for a Network

Near the top of the screen select the "Services" button. Reference Figure 64 – Services Button on page 63. Ensure that the "DHCP Server" tab is selected. Reference the example Figure 65 – DHCP Server Screen on page 63.

Find the "LAN2" line, and follow it to the right side, to the line's "Actions" button. See Figure 73 – DHCP LAN2 Line.

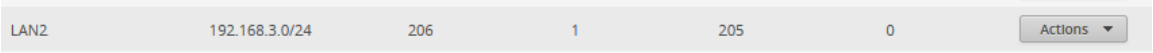


Figure 73 – DHCP LAN2 Line

Click the "Actions" button. You will be presented with a list of actions. Choose "View Details". See Figure 74 – DHCP View Details.

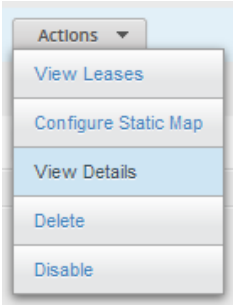


Figure 74 – DHCP View Details

A dialog will open. See Figure 75 – DHCP Lan2 Original.

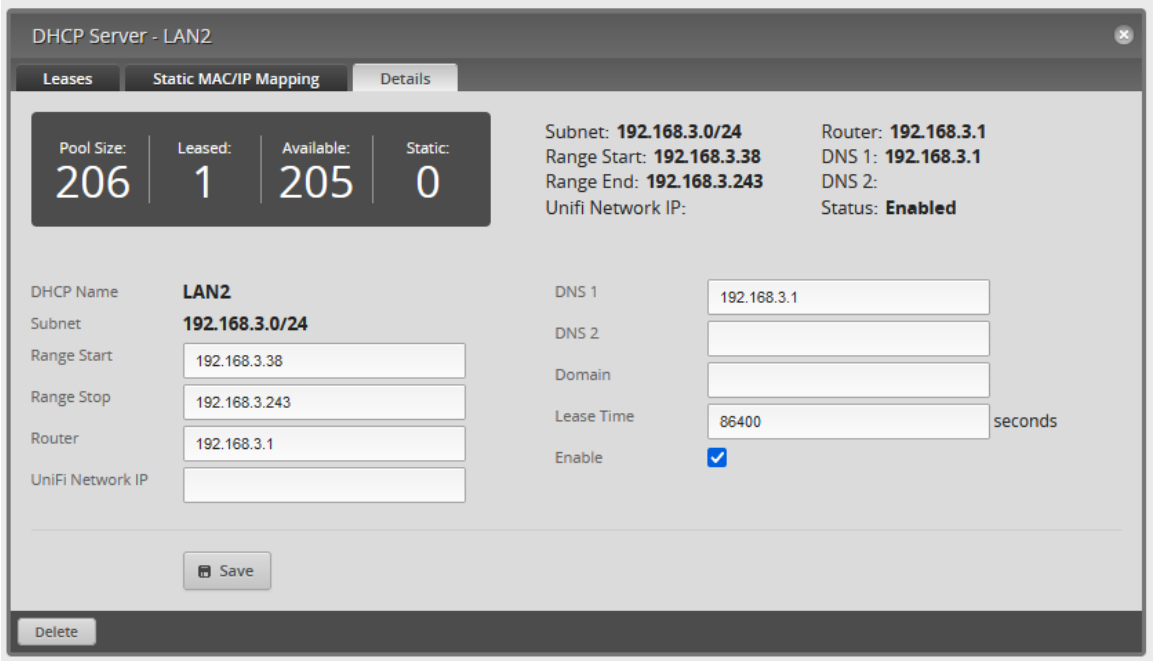


Figure 75 – DHCP Lan2 Original

Replace the DNS1 and DNS2 entries with a resolver pair of addresses of your choice. Reference section 14 - About DNS Resolvers on page 35. Enter the text "`homenet`" into the Domain field. See Figure 76 – DHCP Lan2 New Settings.

Note: Later on, in section 40 - DNS Forwarding on page 78, we will (optionally) put this DNS setting back to this original value. Setting it now, shows you how to change it.

Click `Save`, wait for the green checkmark, and then click the `X` in the upper right corner.

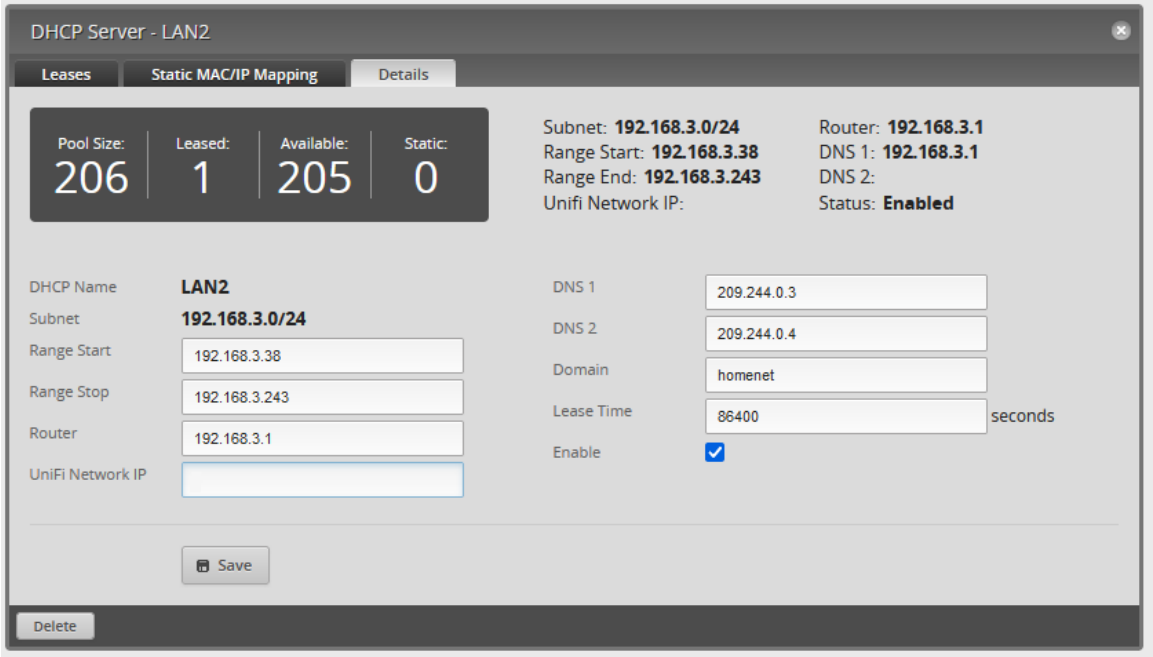


Figure 76 – DHCP Lan2 New Settings

The following are OpenDNS resolver addresses, which can help with any malware that gets on your Iot Network. Future (optional) steps can only be completed if OpenDNS addresses are used here. Reference section 64 - Optional DNS Forcing of the IOT Network on page 128.

Repeat the above steps that you did for LAN2, but with the below data for LAN1:

DNS 1	`208.67.222.222`
DNS 2	`208.67.220.220`
Domain	`iotnet`

Click `Save`, then click the `X` in the upper right corner.

Repeat the above steps that you did for LAN2, but with the below data for SeparateDHCP:

Domain	`separatenet`

Click `Save`, then click the `X` in the upper right corner.

33. Rename Original DHCP Servers

When the Wizard setup our ER-X, it named the two original networks as LAN1 and LAN2. It also named the associated DHCP servers the same. To rename the DHCP servers, enter the CLI. Reference section 18 - EdgeRouter Command Line Interface (CLI). Note that anywhere the CLI can be used, putty or equivalent can instead be used.

Type the following commands into the CLI window (the built-in interface provides no paste):

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

When you enter the `commit` comment, you should see a yellow "The configuration has been changed and is in the process of being committed" message. See Figure 77 – The Configuration has been changed message

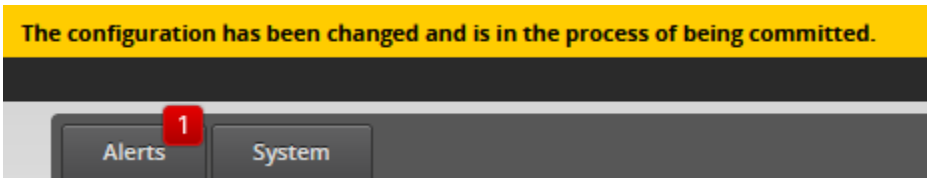


Figure 77 – The Configuration has been changed message

The screen / entire GUI may also refresh.

Exit the CLI interface using the X in the upper right corner of the CLI dialog.

34. Setup Remaining DHCP Servers

We need to add more DHCP servers to the ER-X. These additions are comprised of several steps.

We will be repeating the steps in 30 - Setup eth2's DHCP Server on page 63, but with the data below.

Fill in the "Add DHCP Server" form as follows:

```
Services
   Add DHCP Server
      DHCP Name:          GuestDHCP
      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:              8.8.8.8
      DNS 2:              8.8.4.4
      Unifi Network IP:   <Leave Blank>
      Enable:             <CHECKED>
      Save
```

Fill in the "Add DHCP Server" form as follows:

```
Services
   Add DHCP Server
      DHCP Name:          SpareDHCP
      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:              8.8.8.8
      DNS 2:              8.8.4.4
      Unifi Network IP:   <Leave Blank>
      Enable:           <CHECKED>
      Save
```

We will be repeating the steps in 31 - Make a DHCP Server Authoritative on page 65, but with the data below.

Set the `GuestDHCP` server authorative as follows:

```
Config Tree
   Service
      dhcp-server
         shared-network-name
            GuestDHCP
               Change "disable" to "enable"
               Preview
               Apply
```

Set the `SpareDHCP` server authorative as follows:

```
Config Tree
   Service
      dhcp-server
         shared-network-name
            SpareDHCP
               Change "disable" to "enable"
               Preview
               Apply
```

We will be repeating the steps in 32 - Set Domain Name / DNS for a Network on page 67, **but change only the data below**, i.e. only the Domain, for the following two servers:

```
Services
   DHCP Server (tab)
      GuestDHCP (line) -> Actions -> View Details
         Domain    guestnet
         Save
         X
```

```
Services
   DHCP Server (tab)
      SpareDHCP (line) -> Actions -> View Details
         Domain    sparenet
         Save
         X
```

So that you can become familiar with the EdgeRouters config file, (Reference section 21 - EdgeRouter Backup / Restore Configuration Files on page 47), see Equation 2 – Example config - DHCP, which shows sample DHCP sections.

```
service {
    dhcp-server {
        disabled false
        hostfile-update disable
        shared-network-name GuestDHCP {
            authoritative enable
            subnet 192.168.6.0/24 {
                default-router 192.168.6.1
                dns-server 8.8.8.8
                dns-server 8.8.4.4
                domain-name guestnet
                lease 86400
                start 192.168.6.38 {
                    stop 192.168.6.243
                }
            }
        }
        shared-network-name HomeDHCP {
            authoritative enable
            subnet 192.168.3.0/24 {
                default-router 192.168.3.1
                dns-server 209.244.0.3
                dns-server 209.244.0.4
                domain-name homenet
                lease 86400
                start 192.168.3.38 {
                    stop 192.168.3.243
                }
            }
        }
        shared-network-name IotDHCP {
            authoritative enable
            subnet 192.168.7.0/24 {
                default-router 192.168.7.1
                dns-server 208.67.222.222
                dns-server 208.67.220.220
                domain-name iotnet
                lease 86400
                start 192.168.7.38 {
                    stop 192.168.7.243
                }
            }
        }
        shared-network-name SeparateDHCP {
            authoritative enable
            subnet 192.168.5.0/24 {
                default-router 192.168.5.1
                dns-server 8.8.8.8
                dns-server 8.8.4.4
                domain-name separatenet
                lease 86400
                start 192.168.5.38 {
                    stop 192.168.5.243
                }
            }
        }
        shared-network-name SpareDHCP {
            authoritative enable
            subnet 192.168.8.0/24 {
                default-router 192.168.8.1
                dns-server 8.8.8.8
                dns-server 8.8.4.4
                domain-name sparenet
                lease 86400
                start 192.168.8.38 {
                    stop 192.168.8.243
                }
            }
        }
        static-arp disable
        use-dnsmasq disable
    }
```

Equation 2 – Example config - DHCP

35. dnsmasq

There are two different DNS packages available within the EdgeRouter. They are ISC (default) and dnsmasq. Dnsmasq has many advantages, including being integrated with the DHCP server. We will be needing dnsmasq and hostfile update later.

To enable dnsmasq, enter the Config Tree. Reference section 19 - EdgeRouter Config Tree on page 45. Select and open up the following config tree sub-menu items from the configuration screen (see Figure 78 – Service – dhcp-server):

```
Config Tree
   Service
      dhcp-server
         hostfile-update
            Change "disable" to "enable"
         use-dnsmasq
            Change "disable" to "enable"
         Preview
         Apply
```

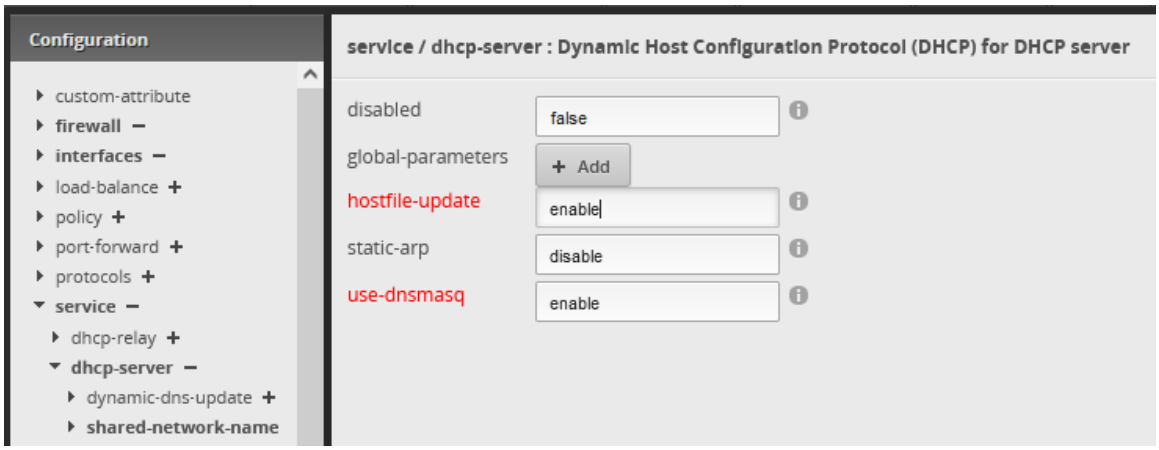


Figure 78 – Service – dhcp-server

Ubiquiti Help References:

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

https://help.ui.com/hc/en-us/articles/115010913367

Link with two videos

https://community.ui.com/questions/vlan-can-not-connect-to-management-plane-or-internet/0f0a4ad6-a2a9-479e-8040-73d83adea23a#answer/d7177b72-60c1-4b53-ab5b-d17610c555e7

36. 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 68 - 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 18 - EdgeRouter Command Line Interface (CLI) on page 43, for how to issue commands.

To play with this, I issued the following commands via CLI:

```
configure
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
commit
save
```

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
    }
}
```

37. 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 page 29.

On the system window, find the Name Server Box. See Figure 79 – Initial System Name Server.

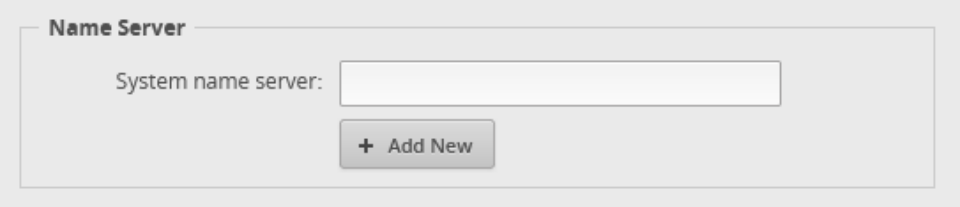


Figure 79 – Initial System Name Server

Into the `System name server:` box enter: `209.244.0.3`

Press the “+ Add New” button shown in Figure 79 – Initial System Name Server.

Into the (new dialog field) enter: `209.244.0.4`

When you are done editing, press the `Save` button near the bottom of the system page. See Figure 80 – System Save Button.

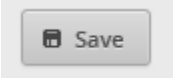


Figure 80 – System Save Button

38. Remove ISP Provided DNS Resolvers

I don't want to depend upon the DNS servers that are provided by my Internet Service Provider's (ISP) / 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 18 - EdgeRouter Command Line Interface (CLI) on page 43.)

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 192.168.50.1:

```
------------------------------------------------
   Nameservers configured for DNS forwarding
------------------------------------------------
209.244.0.3 available via 'system'
209.244.0.4 available via 'system'
192.168.50.1 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
-----------------------------------------------
209.244.0.3 available via 'optionally configured'
209.244.0.4 available via 'optionally configured'

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

Reference https://community.ui.com/questions/Change-WAN-DNS-Server/041bbac7-6de0-44a7-a5ca-165128e4333d

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

39. Configure EdgeRouter's Time Zone

Near the bottom of the screen select the "System" button. Reference Figure 9 – System Button on page 29. 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 81 – Time Zone.

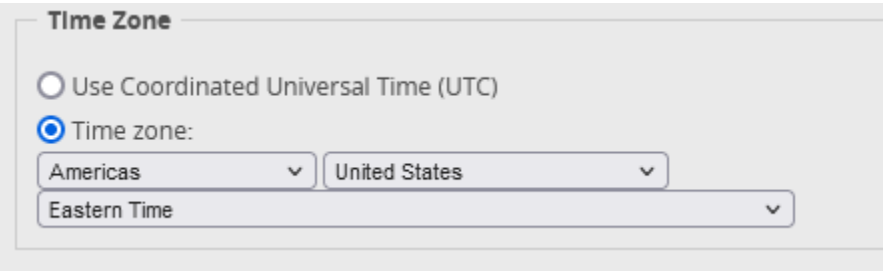


Figure 81 – Time Zone

Press the `Save` button, Reference Figure 80 – System Save Button on page 75.

40. DNS Forwarding

In section 32 - Set Domain Name / DNS for a Network on page 67, we setup the Home Network's DNS resolver addresses to point directly to a pair of (your choice of) public DNS resolver addresses.

The following settings will only work when dnsmasq and hostname-update are enabled. There were enabled in section 35 - dnsmasq on page 73.

If we setup the above two item and setup the ER-X's DNS forwarding system and point the HomeNet's devices to that forwarding system, we also get local hostname resolution.

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 enable local hostname resolution, press the "Services" button, reference Figure 64 – Services Button on page 63. Ensure that the "DNS" Tab is selected. See Figure 82 – DNS Forwarding - Original.

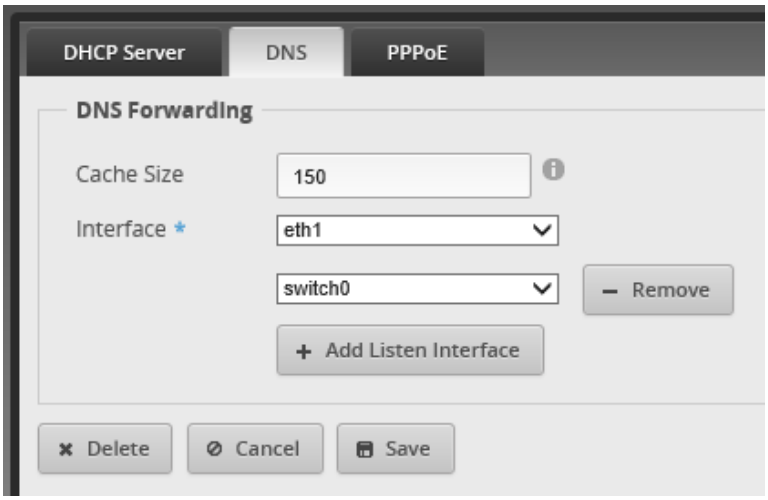


Figure 82 – DNS Forwarding - Original

I changed my cache size from 150 to 400. Don't go crazy here; the ER-X is somewhat memory limited.

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 83 – DNS Forwarding – New Settings. Press "Save."

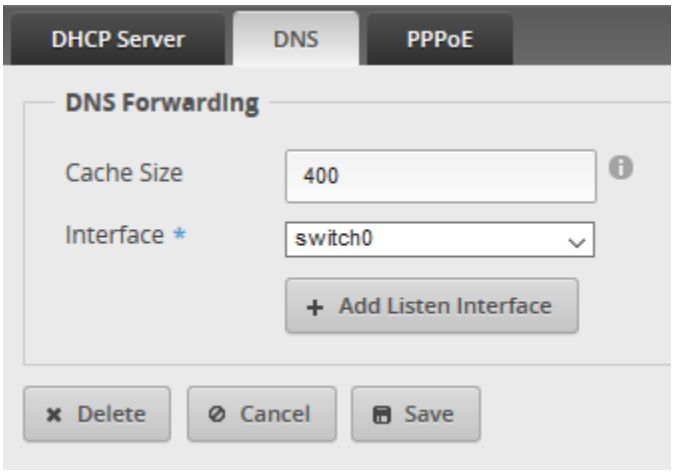


Figure 83 – DNS Forwarding – New Settings

Now we need to inform the HomeNet devices of our forwarding server. To do this follow the steps outlined in section 32 - Set Domain Name / DNS for a Network on page 67, but use the data below:

```
Services
   DHCP Server
      HomeDHCP (line) -> Actions / View Details
```

Change DNS 1: from `<YourPrimaryDNSResolver>` to `192.168.3.1`
Change DNS 2: from `<YourSecondaryDNSResolver>` to <Blank>
`Save`

See Figure 83 – DNS Forwarding – New Settings

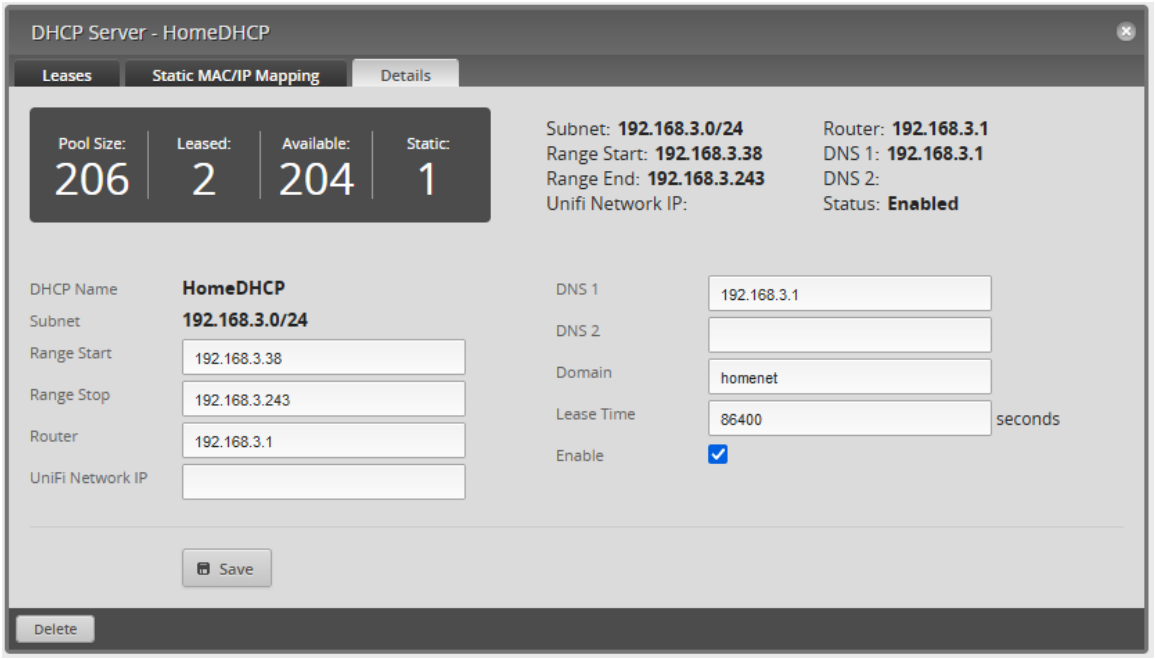


Figure 84 – DHCP Server – HomeNet - Forwarding

We can now use our HomeNet devices names directly, and don't have to look up the device's IP addresses. Command like `ping unifipi`, and `ping unifipi.homenet` now just work.

We can carry this concept further, and do the same for the more Networks. The Iot Network seems like a good candidate for this. If you want to do this, follow the above steps, but instead use this data:

```
Services
   DHCP Server
      IotDHCP (line)  -> Actions / View Details
```

Change DNS 1: from `<YourPrimaryDNSResolver>` to `192.168.7.1`
Change DNS 2: from `<YourSecondaryDNSResolver>` to <Blank>
`Save`

To access Iot devces, you can just append `.iotnet` to the particular device's name, like this example: `ping datalogger.iotnet`.

We setup our dns forwarder to listen-in on dhcp requests which are attached to switch0, which includes HomeNet, IotNet, GuestNet, and SpareNet. Since eth2 / Wired Separate Network is not attached to switch0, it not included (and should not be included since that might leak devices names).

There may be cases, if you re-configuring your ER-X Networks differently than this guide, where you may instead want to have the dns-forwarding system act on all interfaces *except* for one interface. You can perform this step via the Config Tree. Reference section 19 - EdgeRouter Config Tree on page 45. See Figure 85 – DNS Forwarding – Except-Interface Example.

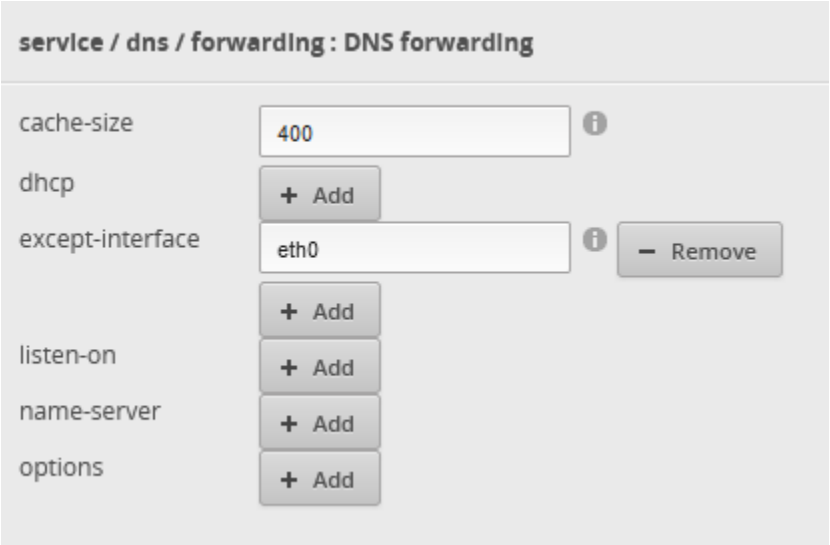


Figure 85 – DNS Forwarding – Except-Interface Example

41. 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.

Note: I think that you can enable QoS (only) on your Internet connection, i.e. eth0 without impacting hwnat.

To enable hwnat, enter the Config Tree. Reference section 19 - EdgeRouter Config Tree on page 45. Before pressing Apply, note the previewed commend. Select / modify the following config tree sub-menu items:

```
Config Tree
   system
      offload
         hwnat
         Enter "enable"
         Preview
         Apply
```

The system should inform you that, "The configuration has been applied successfully".

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 config-tree you had taken note of.

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

Ubiquiti Help Article:

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

42. 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 setting may need to be turned back off.

Press the “Traffic Analysis” button, near the top of the screen. See Figure 86 – Traffic Analysis Button.

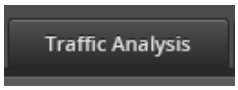


Figure 86 – Traffic Analysis Button

In the upper-right area of the traffic analysis screen, is an “Operational Status” selection. Select “Enabled.” See Figure 87 – Enable Operational Status

Figure 87 – Enable Operational Status

You will be presented with a confirmation dialog. See Figure 88 – Operational Status Confirmation.

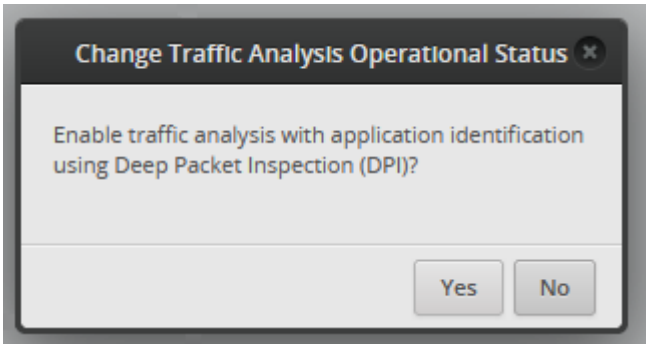


Figure 88 – Operational Status Confirmation

Select “Yes.” The software will (for some reason) present you with a green “changed successfully” message **and** a red Alert. This is seen in the lower-left of the screen. See Figure 89 – Success and Alert.

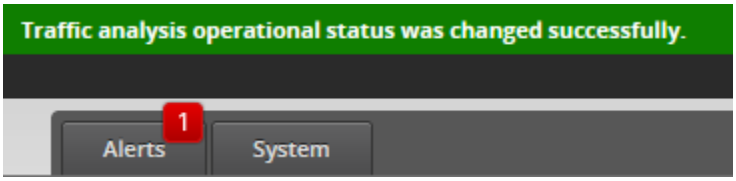


Figure 89 – Success and Alert

Click on the “Alerts” button. You will be presented with the Alert message(s). See Figure 90 – Active Traffic Analysis Message.

Figure 90 – Active Traffic Analysis Message

To remove this Alert message, press the “Remove” button, located on the right side of the screen. See Figure 91 – Remove Alert Button

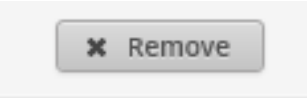


Figure 91 –Remove Alert Button

43. 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 forabout 2 hours.

See Figure 92 –Sample Traffic Analysis. In real use, this feature seems to put a lot of uncharacterized traffic under “Other.”

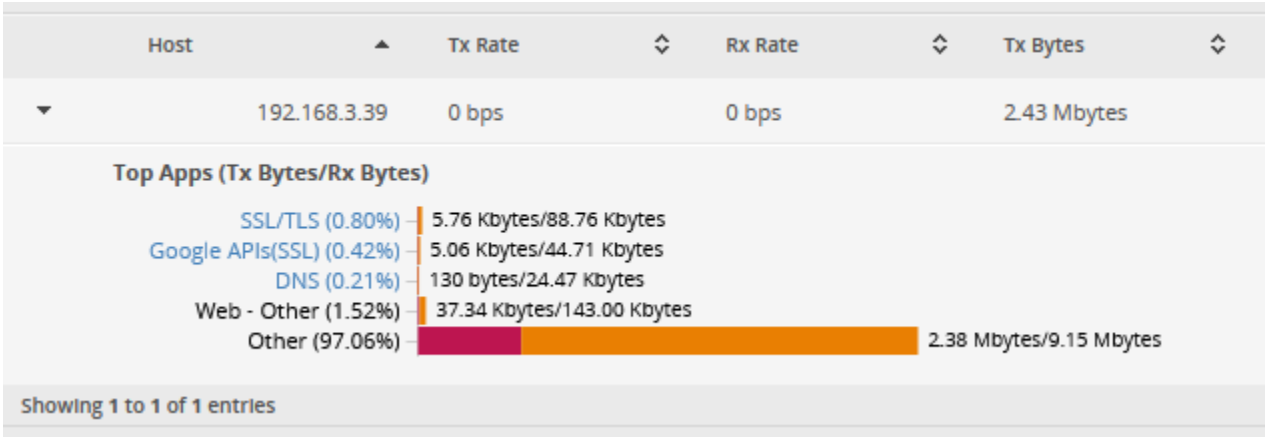


Figure 92 –Sample Traffic Analysis

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. 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

44. 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

45. 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 posting made by Ubiquiti:

> @UI-Team
> 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.ui.com/questions/ER-PRO-8-random-reboots-1-9-7-hotfix-1/e7c9a38b-ff54-4397-bc87-181c675e89bf

This posting was made about 2017 – 2018, and it doesn't appear to be fixed (yet).

46. 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 93 –Toolbox Items.

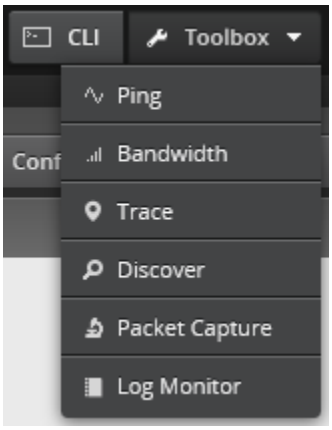


Figure 93 –Toolbox Items

There is a handy log monitor inside:

https://community.ui.com/questions/Viewing-Firewall-Logs-in-GUI/94eb749b-54bf-4706-9bbb-71e5ceb6b303#answer/072b6356-2518-4ac0-b594-c3d19d72214a

47. 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.

Select the “Firewall/NAT” Button from the top of the screen. See Figure 94 – Firewall/NAT Button.

Figure 94 – Firewall/NAT Button

From the tabs that are shown, select “Firewall/NAT Groups”. See Figure 95 – Firewall/NAT Groups Tab.

Figure 95 – Firewall/NAT Groups Tab

Find the “+ Add Group” button and click it. See Figure 96 – Add Group Button.

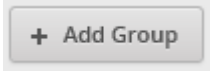


Figure 96 – Add Group Button

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 97 – Example New Address Group Dialog. Press “`Save`.”

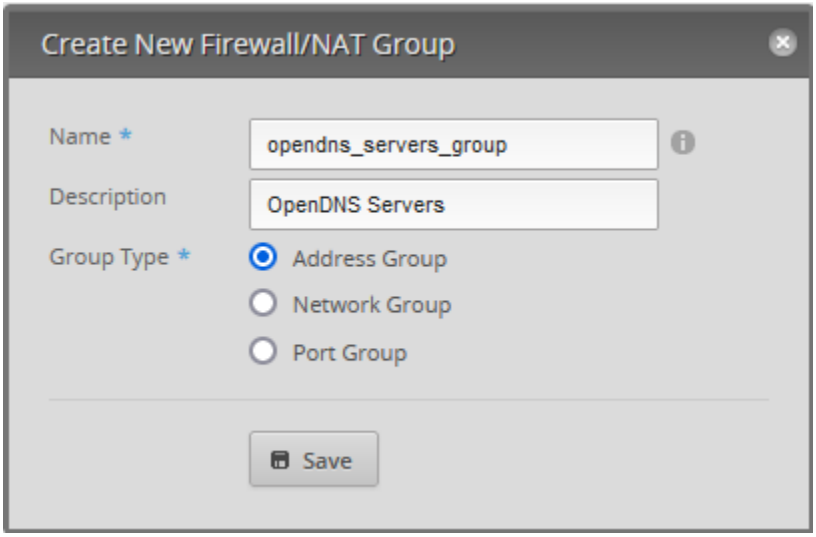


Figure 97 – Example New Address Group Dialog

An empty Address group will have been added. Note that the “Number of group members” is 0. See Figure 98 – Added Address Group.

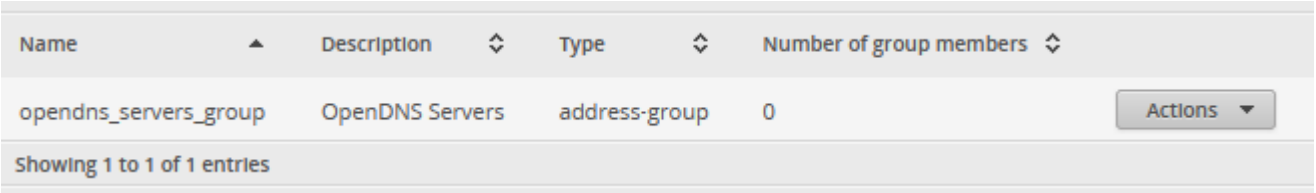


Figure 98 – Added Address Group

Press the `opendns_servers_group`‘s `Actions` button and select `Config`. See Figure 99 – Address Group Actions

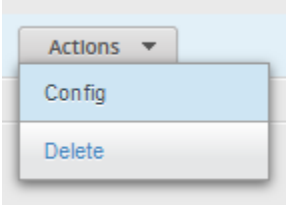


Figure 99 – Address Group Actions

Enter the address specifier of:

`208.67.222.222`

Press the “+ Add New” button and then add

`208.67.220.220`

See Figure 100 – Example Edit Address Group. Press “Save.” When it is finished updating, close the dialog.

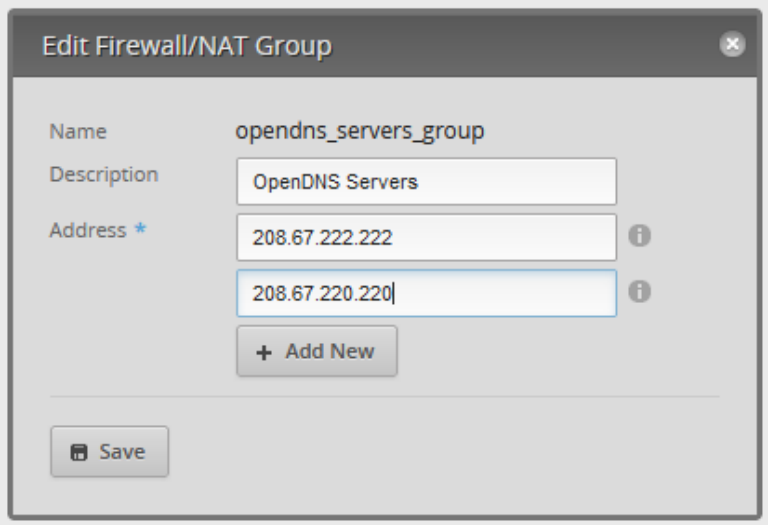


Figure 100 – Example Edit Address Group

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.

RFC-1918 addresses (see values above) are reserved for use within a *private* Network. Every public router on the internet will immediately drop any packet addressed to any of these IP addresses. What is brilliant about this idea is that *every* private network can uniquely reuse these addresses. Within a private network, each IP address must be unique, so each private network is free to use these RFC-1918 addresses as it wishes.

There are approximately 16,777,214 + 1,048,574 + 64,534 private addresses available per private network. This is exactly what virtually every Home-router on the planet is doing, re-using (typically for consumer routers) 192.168.x.x addresses.

Reference:

https://www.rfc-editor.org/rfc/rfc1918

48. 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 @BranoB article "Layman's firewall explanation".

Reference: https://community.ui.com/questions/Laymans-firewall-explanation/2dafa379-3269-4749-b224-0dee15374de9

IN traffic entering the router from an interface (and later exiting via another interface)
OUT traffic exiting the router to an interface (previously entered via another interface)
LOCAL traffic entering the router and destined to the router itself

I have re-produced the main diagram, from that article, as Figure 101 – Layman's Firewall Explanation Diagram. Note that this diagram was originally drawn for an EdgeRouter Lite, which has its WAN port on eth1. The WAN interface is therefore shown in the middle of this diagram.

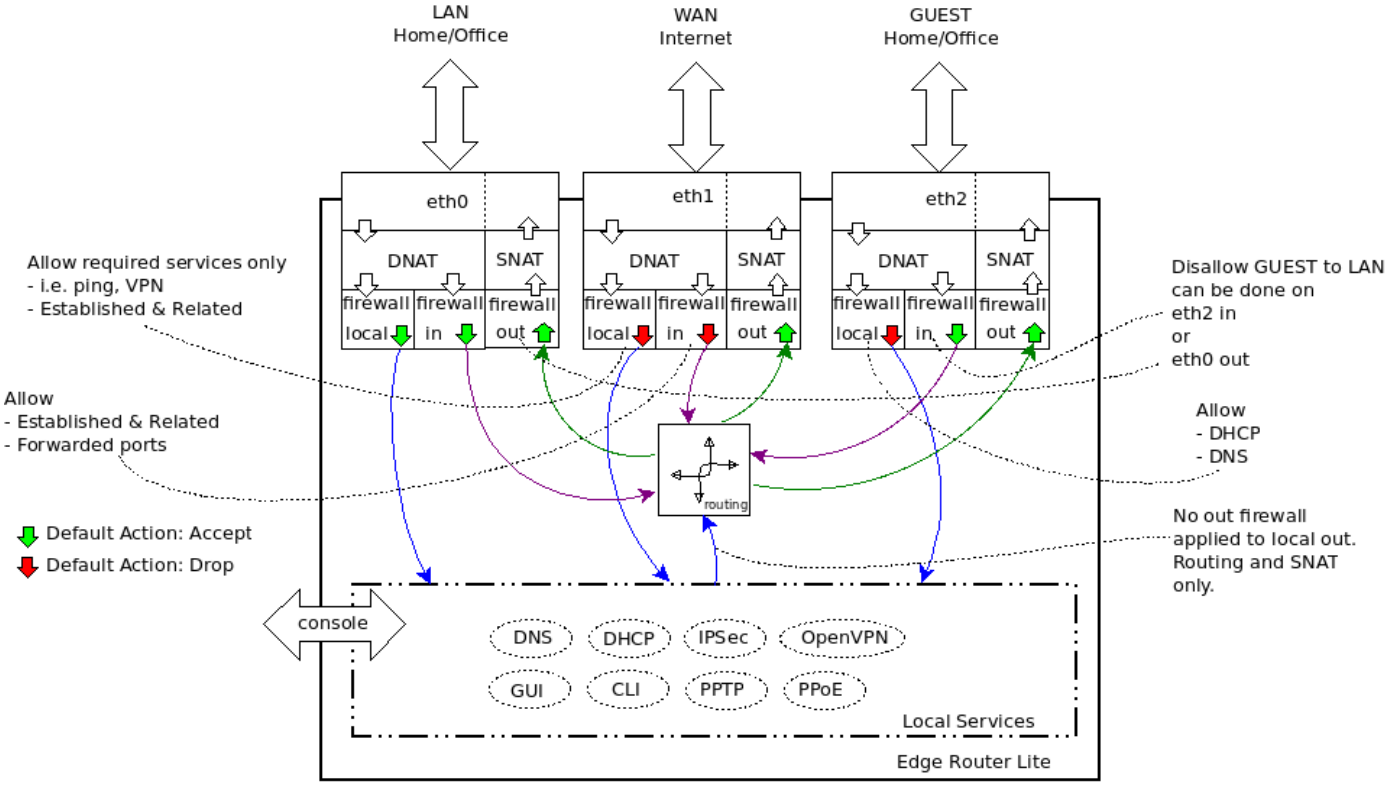


Figure 101 – Layman's Firewall Explanation Diagram

49. EdgeRouter Firewall Basics

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 IP packets INPUT into the EdgeRouter,** from devices on a (LAN) Network as well as IP packets input from the internet (WAN).

The **"Out" direction is IP packets OUTPUT from the EdgeRouter**, to devices on a (LAN) Network as well as IP packets sent to the Internet (WAN).

The **"Local" direction is IP packets input into the EdgeRouter, DESTINED for (services on the) EdgeRouter itself.** These IP packets can be from devices on a (LAN) Network as well as IP packets input from the internet (WAN).

Another way of saying the above is: **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, and its action is taken, no other firewall processing is needed (or taken) for that IP packet.

When designing firewall rules, the design of the *entire* ruleset must be taken into account, in the order presented.

Most rulesets with a default- drop, will have a few individual rules which will allow a few items through the firewall, then the default-drop throws everything else away This type of rule is used on the WAN (internet) interface, and when restricted Network devices s try to access ER-X resources.

Most rulesets which have a default- accept, will have one or more rules which will drop specific items and then the default-accept allows the rest of the data through the firewall. This type of rule is used to disallow one (local) Network from communicating with another (local) Network (e.g. Guest with Iot) and then allow communication with the internet via the default-accept.

Firewall rules within the ruleset are applied (tested) in the specific order that they were arranged.

The firewall rules each have an assigned number. 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, or even if they changes over time, only the rule ordering matters. Firewall processing is ordered by lowest rule number to highest number.

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

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

Ubiquiti help article:
https://help.ui.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
```

49.1 Firewall Postings

The following firewall explanation is so good; I'm going to include it here. These are all postings from the same thread.

@karog

Confidence in firewall security comes from understanding. So begin there. Firewall rules are grouped in ordered rulesets, a list of rules. Each rule has a set of conditions and an action. When a packet is presented to a ruleset, each rule in order has its conditions matched against the packet. If matched, that rule's action is taken and that is the end of it. If not matched, the next rule is considered.

Within a ruleset, rules are numbered from 1 to 9999 though need not be consecutive in numbering, merely ordered. The ruleset default action (drop, accept, reject, etc) actually creates rule 10000, the last rule, and it has no conditions so is always matched. Thus every packet will match some rule, even if it is rule 10000. Most of the conditions of a rule are characteristics of the packet itself like dest ip addr and port, source ip addr and port, protocol. State (new, invalid, est, rel) are part of conntrack, the connection tracker, which keeps state on the flow of related packets. These states are exhaustive and mutually exclusive which means they cover all cases and do not overlap. Thus the two default rules in the WAN rulesets cover all packets of the 3 states est/rel/invalid. Any packet that does not match either of those two rules is then necessarily a new packet. So any rules you put after them can assume new and just deal with other characteristics, namely what sort of packets do you want to allow to create new connection flows eg a tcp connection to a server. With drop as the default WAN action, any packets not matching defined rules are dropped.

A ruleset is attached to an interface (WAN or LAN or VLAN or other) in one of three points: LOCAL, IN, OUT. As all interfaces are on the router, LOCAL is for packets coming to the router on the interface with a dest ip that is the router itself. Note that DNAT occurs before firewall so a packet arriving from the internet on the WAN interface will have a dest ip that is the router, its public ip addr, but that may be changed via DNAT to some other ip address elsewhere on the local network. If it is not so changed, then it is a LOCAL packet. But if DNAT changes it to a non-router ip address then it is an IN packet. IN packets are ones that arrive on the interface (post DNAT) that have ip addrs not for the router and the router merely routes it out the proper interface. OUT packets are the opposite of IN, packets exiting the router on the interface but not originating on the router ie the source address is not a router address hence flowing through the router eg LAN to WAN. There is no LOCAL equivalent for packets exiting the router ie a packet with a router source ip addr. All of this applies to any kind of interface, not just WAN.

So, if you understand all of that, you will see you are well protected from outside packets attacking you to the extent that they are trying to start things. I am leaving aside DDOS ie packet floods. But you still should worry about attacks beginning from inside your network. If you have some compromised device on your network like some IoT thing, it can start packet streams that will get responses. You can guard against these by putting such devices on their own LAN or VLAN and adding LOCAL and IN firewall rulesets on that LAN or VLAN that block where such devices are allowed to send packets

That is the basics. It is not really that hard. Wrap your head around it and grow your confidence. Of course, this is all from the EdgeRouter way of doing things. In reality, the ER config translates these rulesets into the underlying linux iptables rules. These are more flexible but also more complicated.

And I have left out things such as modify rules which actually create rules in the iptables mangle table to mark packets that are then directed to alternative routing tables by ip rules. This way you can control routing of packets by more than just their dest ip addr. So there is more to learn.

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

@karog

Question 1) If the default for both the WAN_IN and WAN_Local is Drop.. why would you need to have any actual "Drop" rules inside of it. Would you not just need to provide the things you want to "allow".

1) If you add no more rules to WAN sets, then yes the drop invalid is redundant. But often more rules are added to accept selected new packets and as I said before the invalid rule filters out such packets so that any rules after can assume new state. If the invalid rule were not there by default, you would need to add it before adding more rules or more likely forget to or have to include new state in every rule. So it is really there as a convenience since outside attacks on the WAN are more likely to throw invalid packets at you than they are to be generated internally.

Question 2) Would it not make more sense for All rulesets to use the default action of "DROP" and then go in and explicitly "Allow" specific things. I thought best practices dictate that you block everything and then open it up.

2) rulesets default are set to accept or drop depending on whether it makes more sense to drop everything but a few accept exceptions OR to accept everything but a few drop exceptions. A guest lan will want to get to the internet with its vast array of addresses so it would be impossible to default drop and then provide accept rules to cover that vast space. Instead you default accept and then drop destination ip addresses to small number of local subnets. You do not need a final drop rule if the default is drop, since that creates such a rule guaranteed to be last.

https://community.ui.com/questions/Sanity-check-for-WAN-Firewall-rules/e82408d3-e8c9-470c-a284-e28528678fde#answer/6da9b3ea-6f33-48b9-8dea-46370f1ab262

@waterside

The 'drop' invalid rule is mostly in place to easily facilitate adding additional 'allow' rules. It makes no sense to further process traffic with an 'invalid' state since it would never match any other rules, so this rule is a common standard.

If you don't have any 'allow' rules then indeed this rule would indeed be redundant, since the default action would drop the traffic anyway.

Having this explicit rule also allows one to enable logging on just 'invalid' traffic if so desired.

https://community.ui.com/questions/Sanity-check-for-WAN-Firewall-rules/e82408d3-e8c9-470c-a284-e28528678fde#answer/84717f84-9fbd-47d4-9ced-b565e58d44d8

49.2 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)

(I don't know the internal difference between Establish and Related, but just use them as a set, either: both turned on, or both turned off).

50. EdgeRouter Detailed Firewall Setup

The firewall design goals are as follows:

- The Home Network should be un-restricted. Devices on the HomeNet, can manage the ER-X Edgerouter, and communicate with devices on the Home, Iot, Guest, and Spare Networks.
- The Iot, Guest, and Spare Networks are Restricted. Their devices cannot interact with the ER-X, except for DNS and DHCP services, and optionally PING. Restricted Network devices can not initiate conversations with devices on any other Network. These are your Restricted Networks
- The Wired Separate Network has the same restrictions as the (above) Iot, Guest, and Spare Networks, but additionally, HomeNet devices cannot communicate with devices on the Wired Separate Network. This Network is also Restricted, but also Protected from other Networks.

I have adapted Figure 101 – Layman's Firewall Explanation Diagram (page 89) to my own diagram. The FireWall RuleSets (FWR) that are described in this guide are numbered (as FWR*) in Figure 102 – Detailed Firewall Setup Diagram on page 93. Each is associated with a named firewall ruleset that will be described in the following sections.

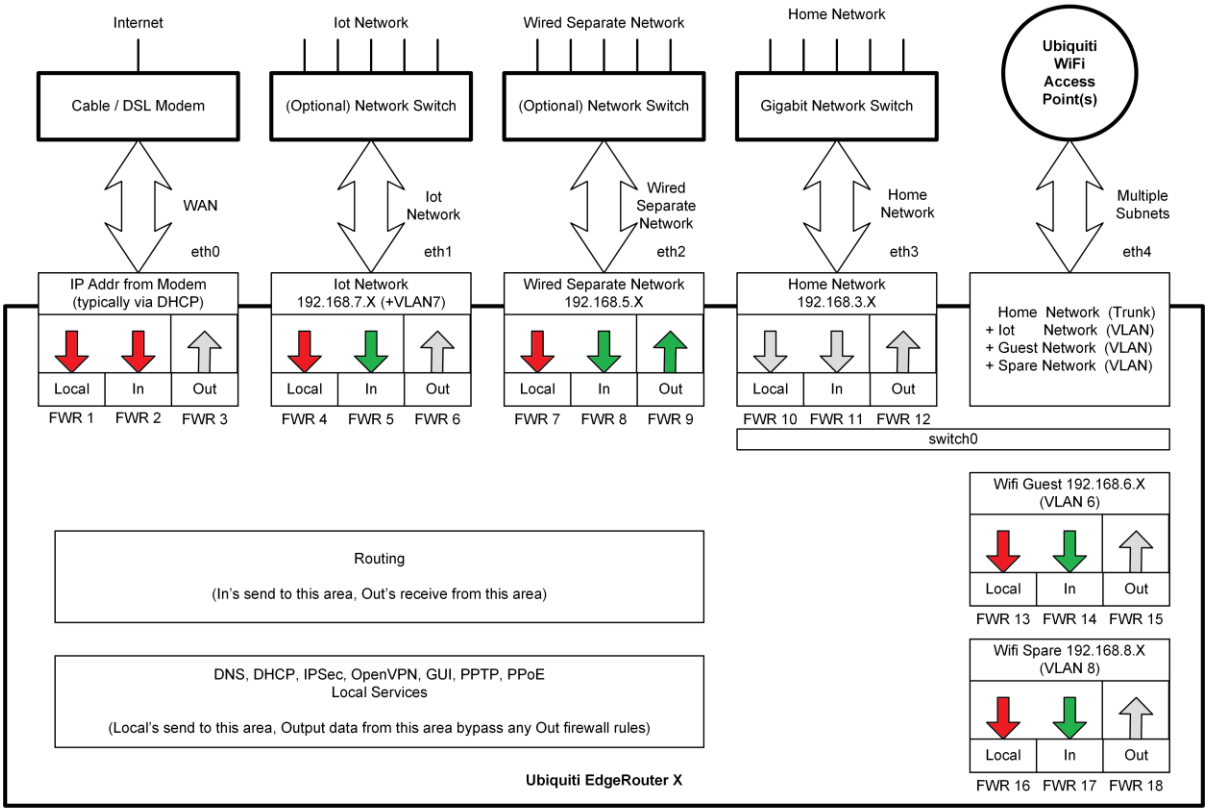


Figure 102 – Detailed Firewall Setup Diagram

FWRs that are colored red means a ruleset terminates with a default of drop, while FWRs colored green mean a default of accept. You might notice that all of the LOCAL rulesets (along with FWR2 / WAN_IN) are red, i.e. are setup as default-drop. All of the remainder of the rulesets are green", i.e. are default-accept. Additionally, some firewall interfaces don't have any firewall rulesets / rules at all. These are shown as gray in the diagram.

These FWRs will each be described in the following sections, but may be described in a different order than given in this diagram. FWR4, FWR7, FWR13, and FWR16 is actually one ruleset, but applied to multiple interfaces. Firewall rulesets FWR5, FWR14, and FWR17 are identical (copies) of a ruleset, except are applied to different interfaces. Rulesets FWR 8 and FWR 9, for "Wired Separate Network", are unique.

The firewall design implemented with this Second Editon re-write is *new*, and is implemented quite differently from the First Edition implementation. This new firewall provides *equivalent* functionality to the older firewall design, but adds a couple of new (minor) protection rules.

Firewall design details are in the following sections

Firewall implementation sections then follow, closing with new sections:

50.1 Firewall Considerations for the “Legacy” Configuration

One.

I switched the order of the “Allow DNS” and “Allow DHCP” rules in IOT_LOCAL, WIFI_GUEST_LOCAL, WIFI_SPARE_LOCAL, and WIRED_SEPARATE_LOCAL. There is a potential for the DNS rule to be used a lot more than the DHCP rule. Even if the DNS rule is unused, the DHCP rule will typically only be used about twice a day, per device.

Two.

There has *never* been any firewall protection between the Iot / Guest / Spare Networks.

I thought of the following three rulesets after publishing the last “Legacy” guide update and before I re-wrote the guide using a newly designed firewall. These rulesets have never been described or implemented in the “Legacy” guide. These added protections are already built-into the newly designed firewall. The protections offered, are minimal, but (I think) are desirable.

If you are staying with the Legacy firewall design, you might want to add the following rulesets. Each of the below Networks will have two IN “drop” rules, one rule blocking each of the other Network(s) listed above.

```
Interface       switch0.7
Direction       in

name IOT_IN {
    default-action accept
    description "Iot In"
    rule 1 {
        action drop
        description "Drop Guest Traffic"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_switch0.6
            }
        }
    }
    rule 2 {
        action drop
        description "Drop Spare Traffic"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_switch0.8
            }
        }
    }
}
```

```
Interface       switch0.6
Direction       in

name WIFI_GUEST_IN {
    default-action accept
    description "Iot In"
    rule 1 {
        action drop
        description "Drop Iot Traffic"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_switch0.7
            }
        }
    }
    rule 2 {
        action drop
        description "Drop Spare Traffic"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_switch0.8
            }
        }
    }
}

Interface       switch0.8
Direction       in

name WIFI_SPARE_IN {
    default-action accept
    description "WiFi Spare In"
    rule 10 {
        action drop
        description "Drop Iot Traffic"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_switch0.7
            }
        }
    }
    rule 20 {
        action drop
        description "Drop Guest Traffic"
        log disable
        protocol all
        source {
            group {
                address-group NETv4_switch0.6
            }
        }
    }
}
```

50.2 Established / Related Rules

The Established / Related (ER) functionality is built around Linux-developed firewall code. The ER firewall rules can be assigned either IN, OUT, or LOCAL directions. The underlying ER code will monitor the stream of IP packets traveling in the *opposite* direction to its assignment, and then remembers relevant details of all those IP packets.

All IP packets traveling in the assigned direction (think “returning”) are checked against the remembered details, and if those checked-IP-packets are related to the opposite stream of data, those IP packets are then allowed back through the firewall via the ER accept rule.

The way I think of these ER rules is in terms of a partially broken phone system. If there is an ER accept rule applied to you, then you can answer the phone and converse with the caller, but you have no dial-tone / cannot initiate your own calls or conversations. Hopefully you know what a dial-tone is.

These ER rules can be assigned to work with data streams in either direction. When ER rules are used in the opposite direction, only you are allowed to initiate conversations, and the other party can only reply to your calls.

Like other firewall rules, ER rules can have specific source and/or destination restrictions applies to them. Since our ER-X router has multiple Networks, multiple ER rules are used to limit specific caller/listener sets. For these ER accept rules to be effective, they are then followed by drop rules. I have never figured-out a use for an ER drop rule, i.e. start some conversation and then don’t listen to the response .

This is a very simplified description of what is happening with ER rules. The internal details are way beyond my pay grade. I also don’t understand the distinction between “established” and “related”. I only know to either check both-of-them or neither-of-them.

All home / consumer routers use this ER type of rule applied to the WAN port. Any IP packets directed to the WAN port from the internet are allowed only if they are (already) associated with an existing conversation. Any IP packets are dropped, if they are not associated with an existing conversation. The only way to (already) be associated with an existing conversation is for that conversation to have been initiated from the LAN (inside) side of the router.

50.3 Alternate Firewall Design

Most Ubiquiti Community members implement IN drop rules. Rules using IN are more efficient, as the packets get dropped (early) before being processed by the EdgeRouter. Rules using OUT get dropped after the EdgeRouter has already processed those (late) drop packets.

For full details on the Legacy firewall, see a legacy revision of this guide. Reference section 4 - Guide Revisions on page 8, for how to access Legacy revisions of this guide.

The bulk of the Legacy HomeNet protection was implemented with three established/related firewall rules which are shown in green, followed by a drop RFC-1918 rule, shown in red. See Figure 103 – Legacy Firewall Design – HomeOut. The established/related (ER) firewall rule(s) monitor the IN data (blue arrow) so that it can allow the "associated" data back into the HomeNet (green arrow). There are three ER allow rules, one for each "Restricted" Network shown in the figure.

Other firewall restrictions, including the Wired Separate Network and EdgeRouter LOCAL restrictions, are not discussed in this section.

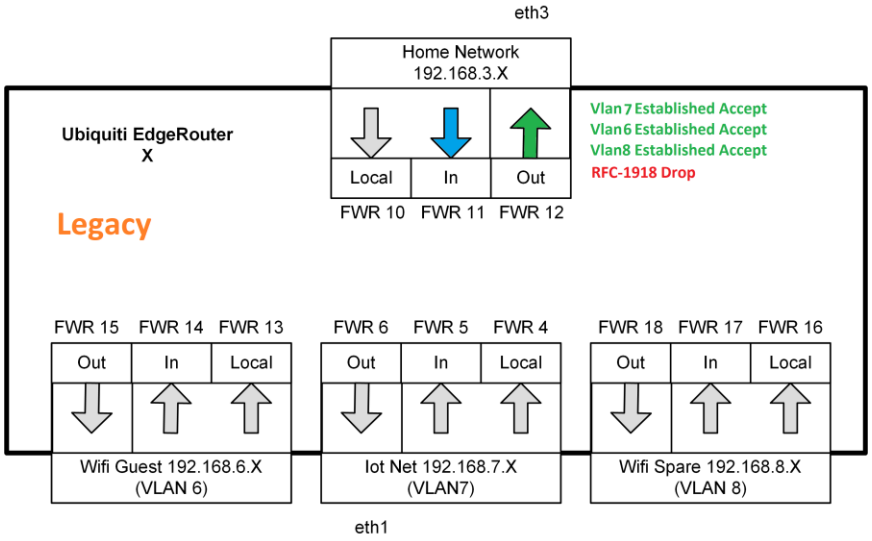


Figure 103 – Legacy Firewall Design – HomeOut

Legacy firewall considerations:

Disadvantage: Less efficient rule processing. The EdgeRouter must process the Restricted Network's IN packets, only to (later) be dropped by Home's OUT rule, i.e. the drop happens late.

Disadvantage: Less efficient HomeNet: every packet leaving the Edgerouter (for every HomeNet device) must traverse a bunch of HOME_OUT rules, slowing down processing. The HomeNet is likely the busiest (and most important) Network in your installationand had the longest ruleset. You may rarely initiate communications with the Restricted Networks, and this (ruleset) burden was incurred by all devices.

Advantage: Home's protection rule is centralized / bundled right with the HomeNet. If you later add a new "restricted" Network, and then forget to add a new established/related rule, your HomeNet is still safe. Since there would be no (new) established/related rule, which allows the new restricted network, the RFC-1918 drop rule safely takes over.

The new firewall design uses smaller / distributed IN rulesets. There are still three established/related rules, one rule for each of the three "Restricted" Networks. See Figure 104 – New Firewall Design – RestrictedIn.

Each of the three established/related firewall rules are shown in green (text) in the figure, each followed by a red (text) drop RFC-1918 rule. In this case, the established/related firewall rule(s) monitor each OUT data stream (blue arrow) so that it can allow the "associated" data back to the HomeNet (green arrow). The HomeNet (was and) is implemented on switch0.1.

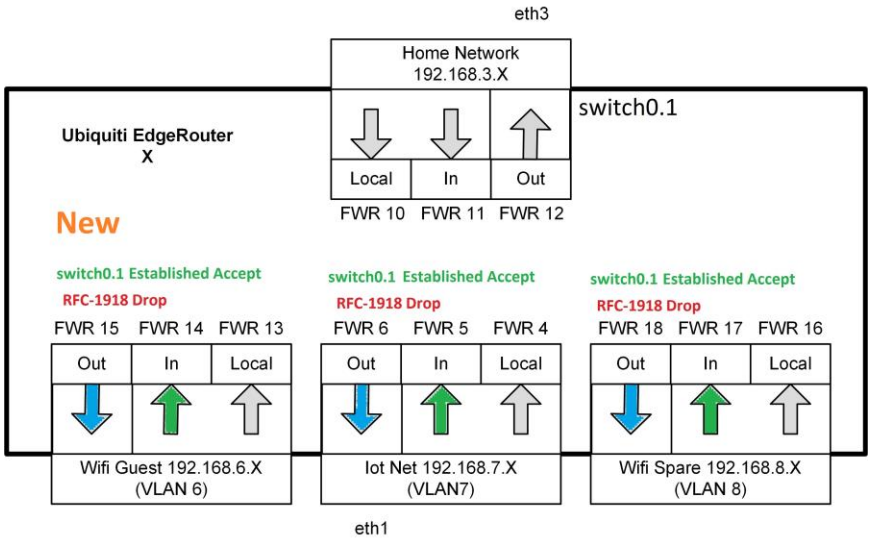


Figure 104 – New Firewall Design – RestrictedIn

New firewall considerations:

Advantage:	More efficient rule processing. The EdgeRouter (immediately) drops non-associated Restricted traffic bound for switch0.1. This is before the EdgeRouter performs any more processing on those packets, i.e. the drop happens early.
Advantage:	More efficient HomeNet: There are *no* firewall rules on the Home Network. Restricted Networks each have an allow established/related firewall rule, and a drop Rfc-1918 rule, which distributes the load.
Disadvantage:	Home's protection rule(s) are de-centralized / scattered, one ruleset per Restricted Network. If you later add a new "Restricted" Network, and forget to add the associated drop Rfc-1918 rule, your HomeNet's firewall is **wide open** to that new Restricted Network. Since I've now mentioned this item, remember to add these rule(s) to any additionally added Restricted Network(s).

Now you know why I chose this new firewall / ruleset method.

50.4 Communication between devices within a Network

Remember that all devices on an Ethernet Network are able to communicate with each other directly. This is via Ethernet Layer 2, and doesn't even require accessing the ER-X, so no firewall rules ever apply.
Reference https://en.wikipedia.org/wiki/Data_link_layer.

51. WAN_LOCAL Firewall Rules

This ruleset is FRW1 as shown in Figure 102 – Detailed Firewall Setup Diagram on page 93.

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_LOCAL ruleset, from the backup file:

```
name WAN_LOCAL {
     default-action drop
     description "WAN to router"
     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 rules in this ruleset are applied to IP packets entering the ER-Xs eth0 interface from the internet. Being a local rule, the destination is within the ER-X, itself.

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. Dropped is another name for discarded.

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 itself. There are no other / additional qualifiers on this rule, so this rule 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. Any packet containing invalid / illegal data will be dropped.

If a packet (entering from the internet) does not match either rule 10 or rule 20, then the listed default action is taken. For this ruleset, that default-action is drop.

52. WAN_IN Firewall Rules

This ruleset is FRW2 as shown in Figure 102 – Detailed Firewall Setup Diagram on page 93.

The difference between WAN_IN and WAN_LOCAL is the data (being applied to the eth0 IN interface) are internet responses returning instead to devices which are attached to the ER-X, and not responses to queries which were made from the ER-X itself.

Note that newer versions of ER-X firmware automatically generate two additional IPv6 rules via running the WAN+2LAN2 wizard. These rules are in the config / backup file and are named WANv6_IN and WANv6_LOCAL.

Rule 20 looks redundant, (because it is a drop rule, which is just above the default-action of drop) but was designed such that it would be positioned *above* any user- added accept rules, to protect those user-added rules. Examples of user-added accept rules would be for port forwarding. Port forwarding could be used for accessing an internal server from the internet. I don't need port forwarding, so those types of rules are not described in this guide.

@16again
Posted about Debugging port forwarding:
See if packets arrive from outside

```
sudo tcpdump -i pppoe0 -n -v tcp port 89
```

And see how they end up on lan

```
sudo tcpdump -i switch0 -n -v tcp port 89
```

Or try

```
sudo tcpdump -ni switch0  -v host 192.168.1.8 and port 89
```

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

53. 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 105 – Firewall Conditions - Basic Tab.
Figure 106 – Firewall Conditions - Advanced Tab.
Figure 107 – Firewall Conditions - Source Tab.
Figure 108 – Firewall Conditions - Destination Tab.
Figure 109 – Firewall Conditions - Time Tab.

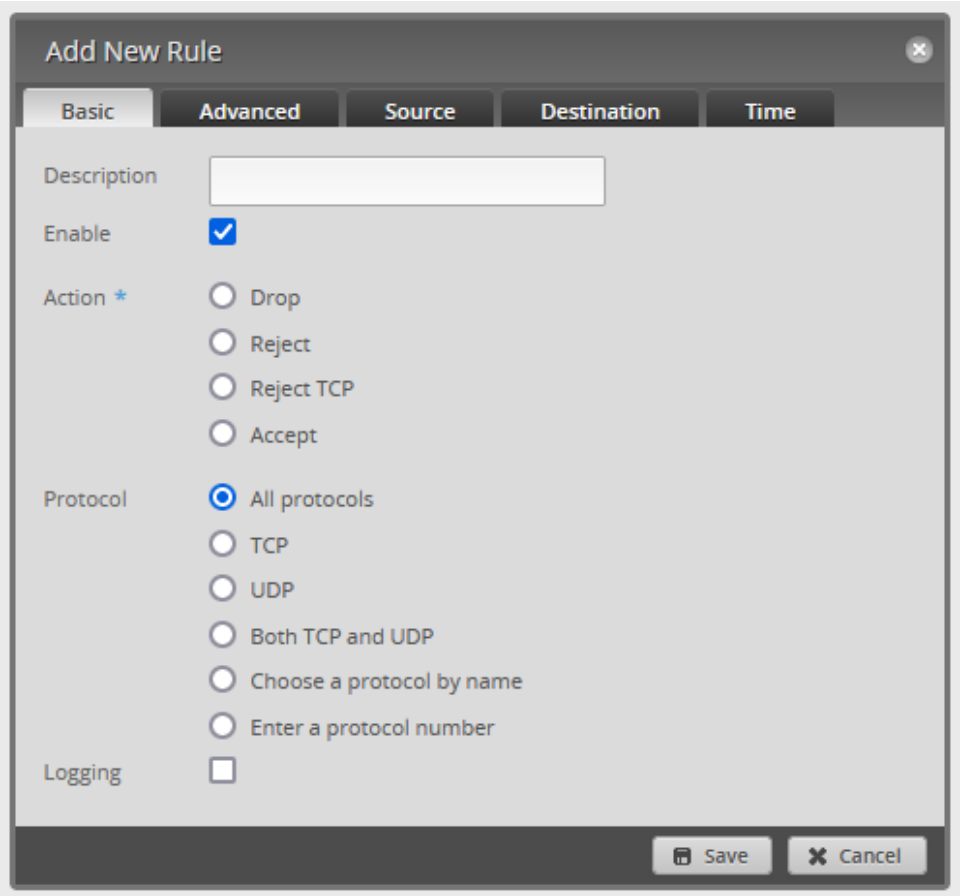


Figure 105 – Firewall Conditions - Basic Tab

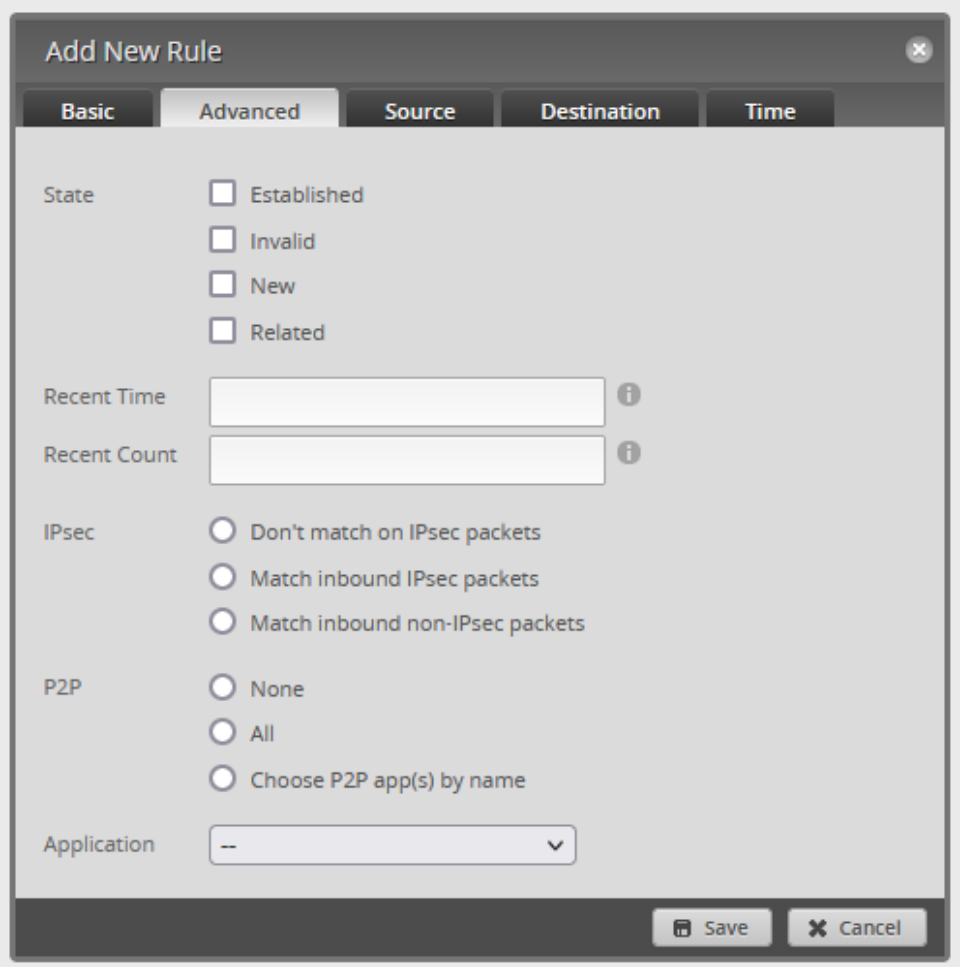


Figure 106 – Firewall Conditions - Advanced Tab

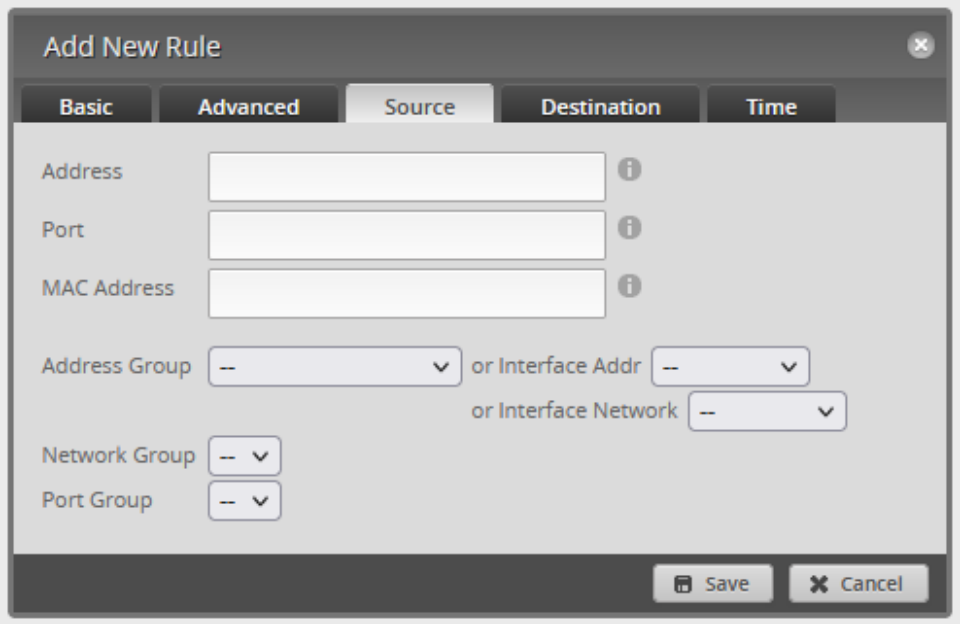


Figure 107 – Firewall Conditions - Source Tab

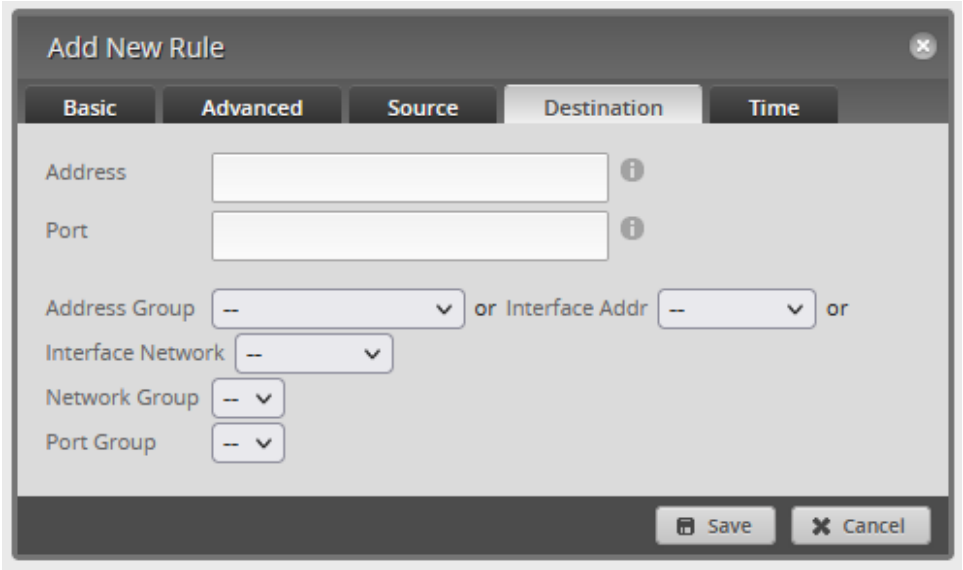


Figure 108 – Firewall Conditions - Destination Tab

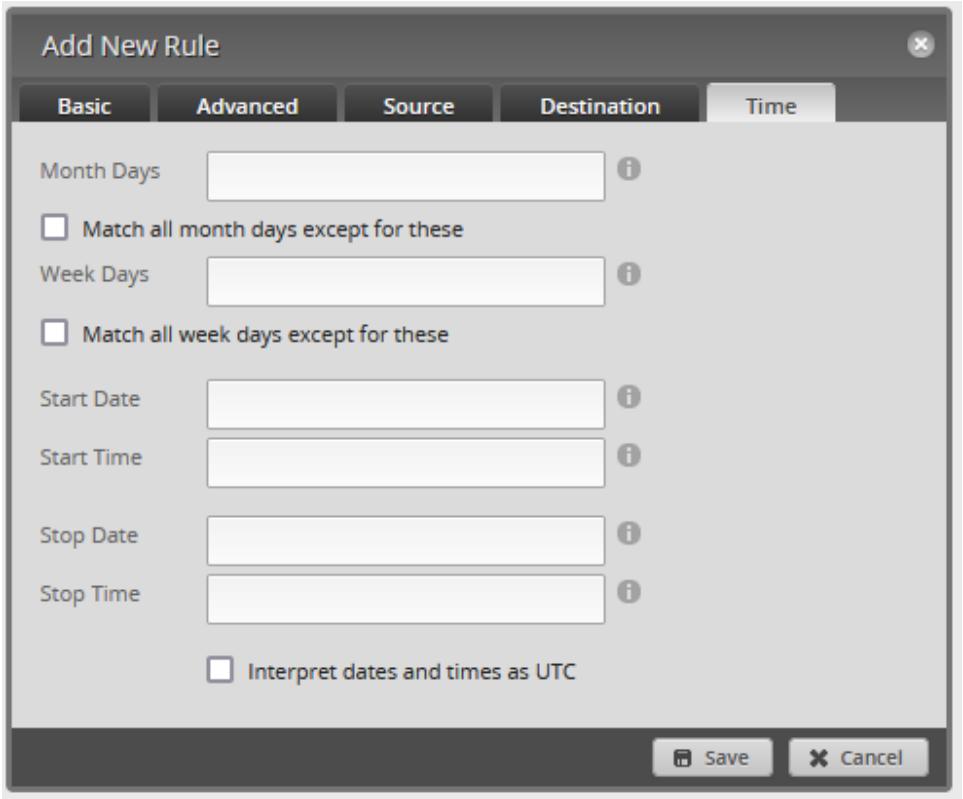


Figure 109 – Firewall Conditions - Time Tab

54. Adding Firewall Rules (IOT_IN)

This ruleset is FWR5 as shown in **Figure 102 – Detailed Firewall Setup Diagram** on page 93.

Hopefully, you now understand how an established / related firewall rule operates. This section will implement the IOT_IN rule, while at the same time; we learn how to use the GUI interface to create a firewall ruleset, containing individual firewall rules.

Select the "Firewall/NAT" button from the top of the screen. Reference Figure 94 – Firewall/NAT Button.

Ensure that the "Firewall Policies" tab is selected. See Figure 110 – Firewall Policies Tab.

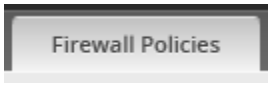
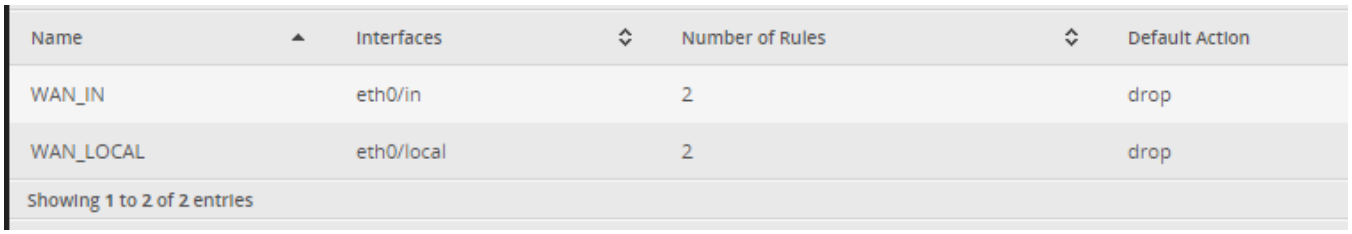


Figure 110 – Firewall Policies Tab

The two WAN rulesets, which were added by the Wizard, should be shown. See Figure 111 – Existing Ruleset. Both of these rulesets contain a stated interface and a non-zero number of rules.



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

Showing 1 to 2 of 2 entries

Figure 111 – Existing Rulesets

Press the "+ Add Ruleset" button. See Figure 111 – Existing Ruleset.

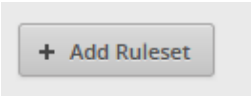


Figure 112 – Add Ruleset

You will be presented a dialog as shown in Figure 113 – Create New Firewall Ruleset - Blank.

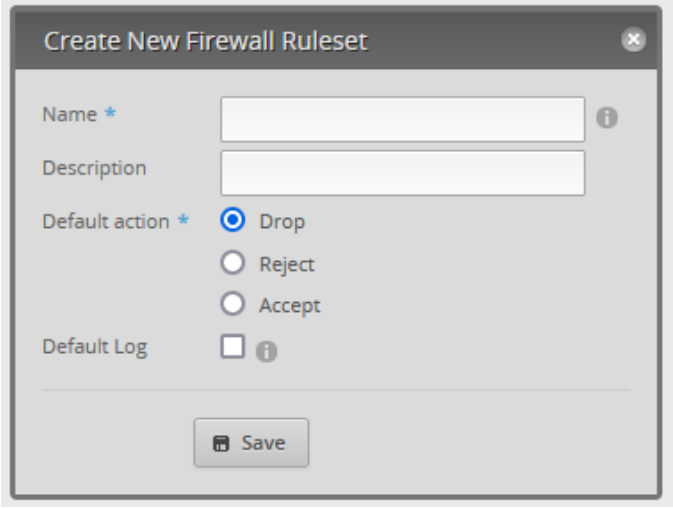


Figure 113 – Create New Firewall Ruleset - Blank

Enter into / change the following in the Create New Firewall Ruleset dialog:

Name	`IOT_IN`
Description	`Iot In`
Default action	`Accept`
Default Log	`Un-Checked`

See Figure 114 – IOT_IN - New Ruleset.

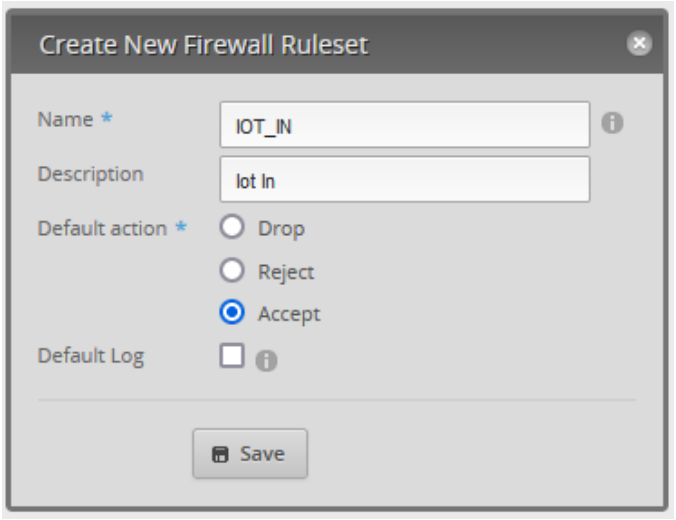


Figure 114 – IOT_IN - New Ruleset

Press "`Save`." An IOT_IN ruleset will be created. Note that no interfaces have been selected, and the number of rules is 0. See Figure 115 – Empty IOT_IN Ruleset.

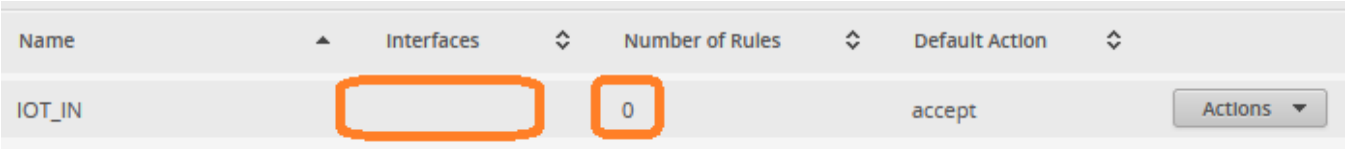


Figure 115 – Empty IOT_IN Ruleset.

Firewall rulesets don't do anything without (individual) firewall rules to operate with, so let's add some rules.

Find the "Actions" button at the right end of the IOT_IN line and press it. You will be presented with a "Firewall Actions Menu." See Figure 116 – Firewall Actions Menu.

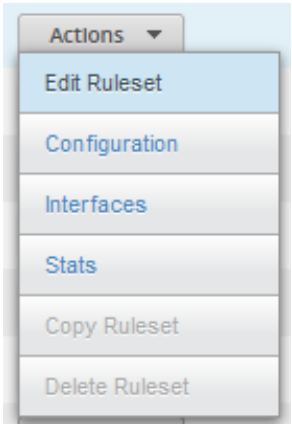


Figure 116 – Firewall Actions Menu

Choose “Edit Ruleset.” A dialog for adding firewall rules appears. The “Rules” Tab should already be selected. See Figure 117 – Firewall 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, shown in Figure 116 – Firewall Actions Menu on page 106.

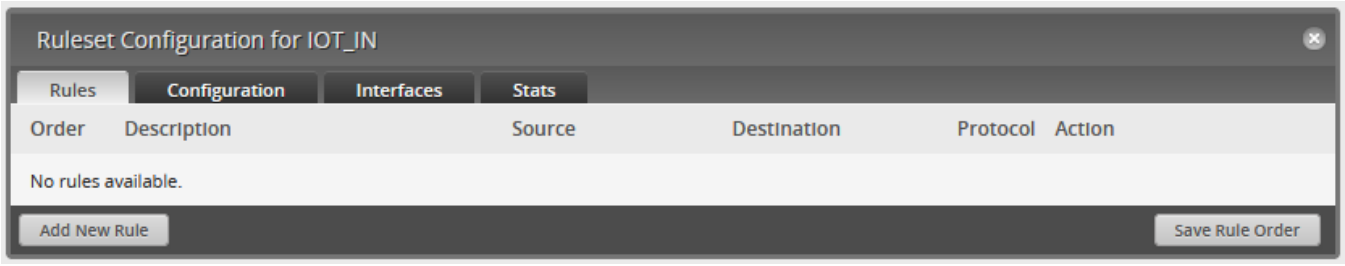


Figure 117 – Firewall Edit Ruleset Dialog

Choose the “Configuration” Tab. You should see the information that was entered earlier. See Figure 118 – Firewall Configuration Tab.

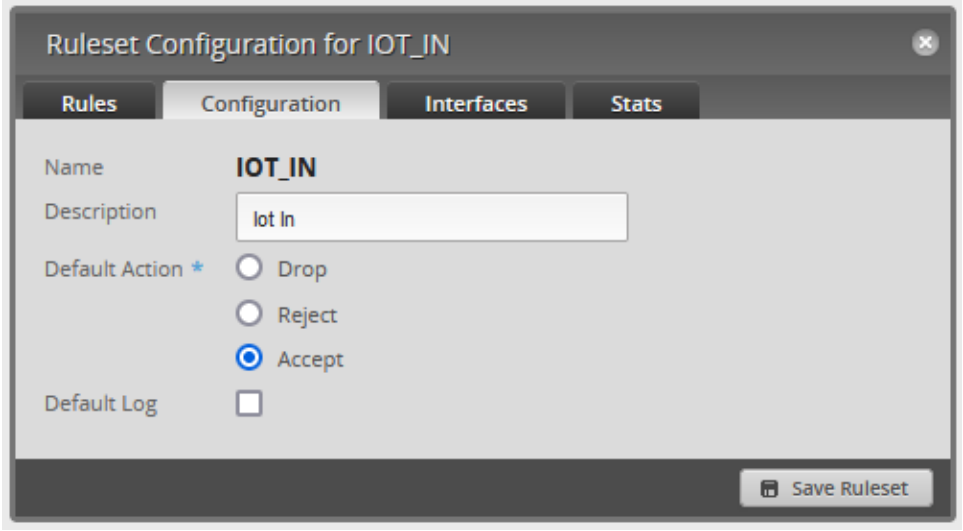


Figure 118 – Firewall Configuration Tab

Choose the “Interfaces” tab. A dialog for setting an interface and a direction appears. See Figure 119 – Firewall Rule Interface Tab - Blank.

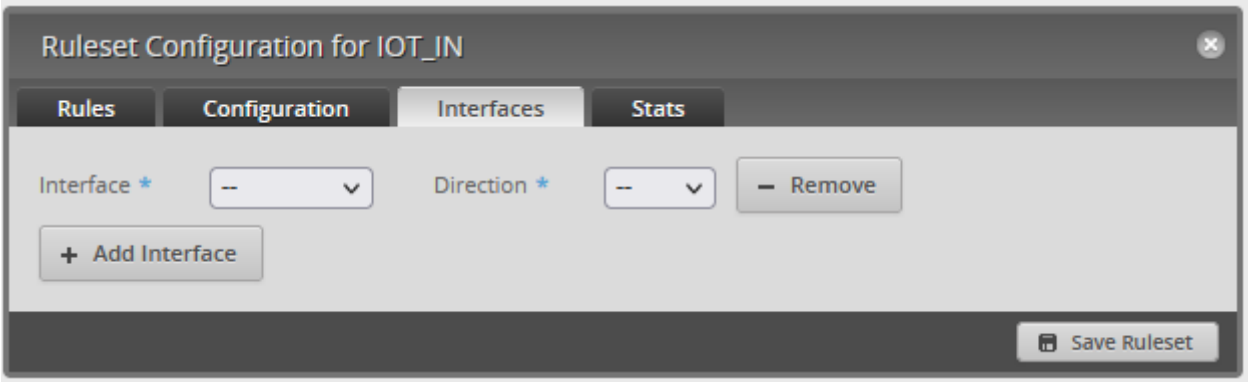


Figure 119 – Firewall Rule Interface Tab - Blank

Enter the following information in the dialog:

Interface	`switch0.7`
Direction	`in`

Figure 121 – IOT_IN Firewall - Rule1 - Basic.

Figure 120 – IOT_IN Interface

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

Re-select the “Rules” Tab, and press the “Add New Rule” Button, that is shown in Figure 117 – Firewall Edit Ruleset Dialog on page 107. An “Add New Rule” dialog will be shown. Reference the dialog shown in Figure 105 – Firewall Conditions - Basic Tab on page 102.

Enter the following into the Basic Tab:

Description	`Allow Home Replies`
Enable	`CHECKED`
Action	`Accept`
Protocol	`All protocols`
Logging	`Un-Checked`

See Figure 121 – IOT_IN Firewall - Rule1 - Basic

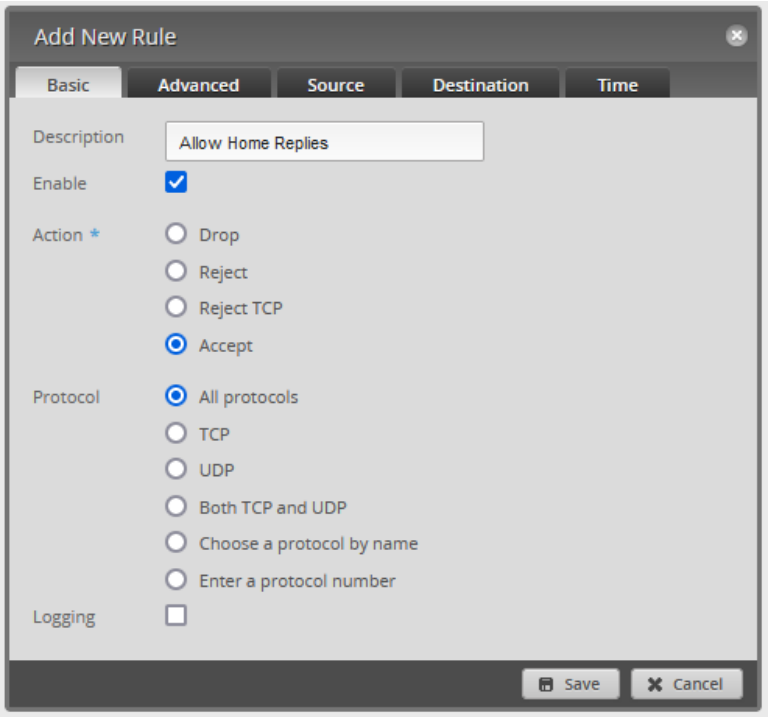


Figure 121 – IOT_IN Firewall - Rule1 - Basic

Click on the Advanced Tab. See Figure 122 – IOT_IN 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`
<Everything Else>	`Blank / Not-Selected`

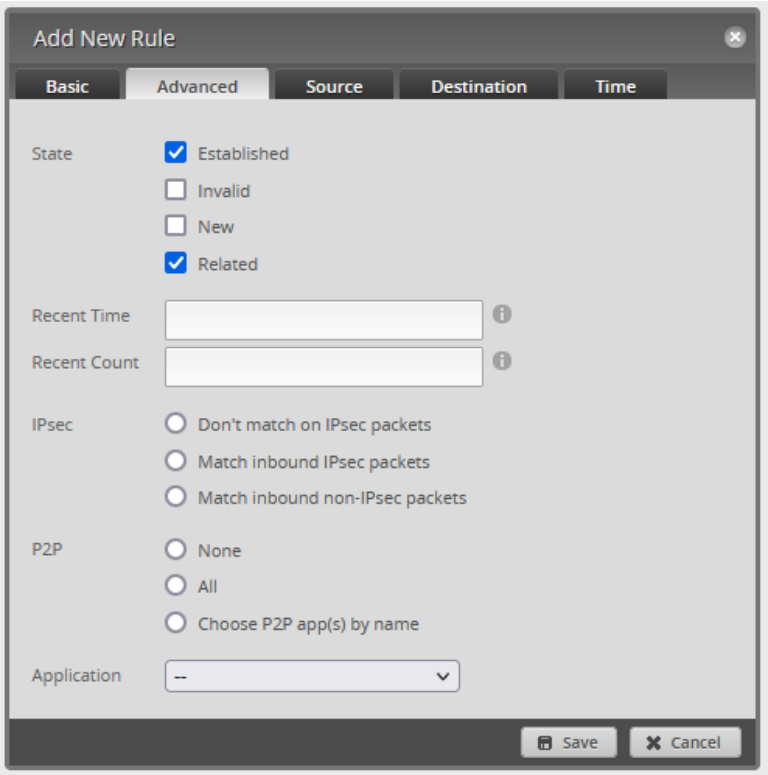


Figure 122 – IOT_IN Firewall, Rule1 - Advanced

Click on the Destination tab. See Figure 123 – IOT_IN Firewall, Rule 1 - Destination.
Enter the following information into the Destination Tab:

Interface Network `switch0.1`

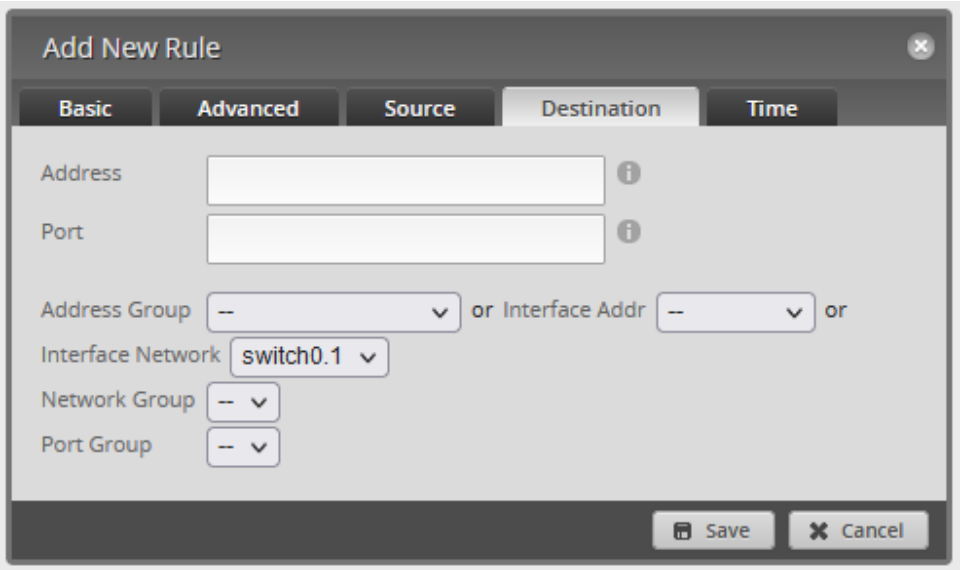


Figure 123 – IOT_IN Firewall, Rule 1 - Destination

We don't need any settings in the Source or Time tabs.

Press the "`Save`" button. Exit the dialog.

Reference https://community.ui.com/questions/Firewall-Interface-Addr-vs-Interface-Network/bdda2a9c-86d1-4339-9c62-22ab5485a60c

You now have a new rule in the IOT_IN ruleset. See Figure 124 – IOT_IN Firewall, Rule 1. Note that you used an "Interface Network", but "address-group" is instead / still shown.

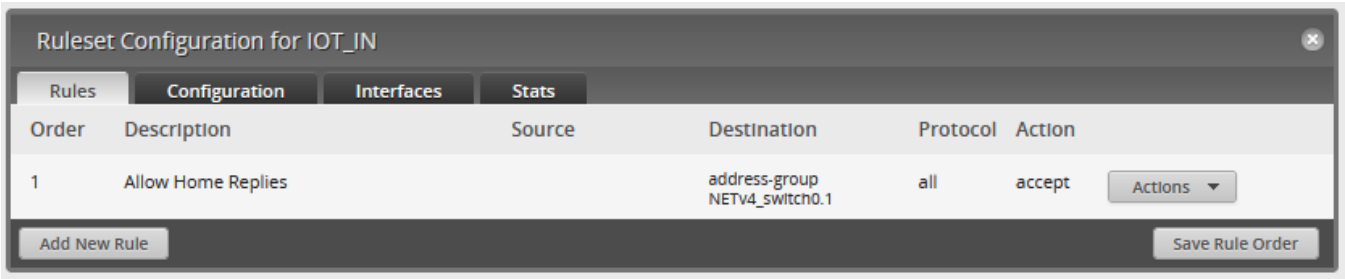


Figure 124 – IOT_IN Firewall, Rule 1 - Finished

54.1 Adding another Rule to IOT_IN

We now need to add another rule to IOT_IN. This rule will "drop" any data destined to an RFC-1918 address, i.e. is addressed to any ER-X Network.

Following the above directions for adding firewall rules, do the following:

```
Firewall/NAT  -> Firewall Policies
IOT_IN (line)    -> Actions  ->  Edit Ruleset  -> Add New Rule
```

Basic Tab:

Description	Drop RFC-1918 Traffic
Enable	Checked
Action	Drop
Protocol	All Protocols

Destination Tab:

Address Group	RFC-1918 Group

Press Save. Close the dialog using the X in the upper right.

Advanced, Source, and Time tabs have all-default / non-changed entries.

54.2 IOT_IN Backup File Portion

The following is a section from the backup file regarding the IOT_IN ruleset we just created.

```
name IOT_IN {
    default-action accept
    description "Iot In"
    rule 1 {
        action accept
        description "Allow Home Replies"
        destination {
            group {
                address-group NETv4_switch0.1
            }
        }
        log disable
        protocol all
        source {
            group {
            }
        }
        state {
            established enable
            invalid disable
            new disable
            related enable
        }
    }
    rule 2 {
        action drop
        description "Drop RFC-1918 Traffic"
        destination {
            group {
                address-group rfc-1918_group
            }
        }
        log disable
        protocol all
    }
}
```

Please study the above backup section, and compare it to the dialogs / screenshots / directions contained within this section, as further firewall rules will be given to you in this “backup file” format.

Note: If you want, you can generate your own backup file and compare the contents of the backup’s “config.boot” file against the above text. You can do this for any firewall section.

55. RESTRICTED_LOCAL Firewall Rules

This ruleset is for FWR4 FWR7, FWR13, and FWR16 as shown in **Figure 102 – Detailed Firewall Setup Diagram** on page 93.

The purpose of this rule is to block the use of EdgeRouter local services from (any) Restricted Networks, except for the use of DNS, the operation of DHCP, and optionally PING.

The DNS protocol uses port 53 of both TCP and UDP.
The DHCP protocol uses a source UDP port of 68 and a destination UDP port of 67.
PING uses the ICMP protocol.

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. Since the default-action is drop, there are no safety issues either way.

I contend you should just leave this rule enabled, so that if you re-configure DNS (years later) you don't need to spend debugging time to get it to work. The other reason is that if no Restricted device is asking the ER-X for DNS, then this rule is simply unused.

RESTRICTED_LOCAL is one ruleset, with the ruleset containing four firewall rules. Using the steps that are shown in section 54 - Adding Firewall Rules (IOT_IN) on page 105, add the following ruleset, per the backup data that is shown below.

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

If you are adding the optional PING rule, the below shown "protocol icmp" term is shown in the GUI as "Choose a protocol by name 'icmp'". Ping can help a lot with debugging a Netwok.

Note that there are no source / destination restrictions on ping, so every device on any Network can ping every Network's Router address. I *don't believe* ping is a security concern, that's why I placed the rule here. Example: A spare-network device can ping 192.168.3.1, …4.1, …5.1, …6.1, …7.1, and …8.1. The Guest Network may have more restrictions, but should always be able to ping 192.168.3.1. Reference "`Guest Network`" setting(s) which are mentioned in section 62 - Firewall Testing on page 124 and section 90.3 - Create New Wifi on page 204.

Add the following RESTRICTED_LOCAL ruleset:

```
name RESTRICTED_LOCAL {
    default-action drop
    description "Restricted Local"
    rule 10 {
        action drop
        description "Drop Invalid Data"
        log disable
        protocol all
        state {
            established disable
            invalid enable
            new disable
            related disable
        }
    }
    rule 20 {
        action accept
        description "Allow DNS"
        destination {
            port 53
        }
        log disable
        protocol tcp_udp
    }
    rule 30 {
        action accept
        description "Allow Ping"
        log disable
        protocol icmp
    }
    rule 40 {
        action accept
        description "Allow DHCP"
        destination {
            port 67
        }
        log disable
        protocol udp
        source {
            port 68
        }
    }
}
```

This ruleset will have multiple interface/direction sets added to it. While on the Interfaces tab, add the following, by using the "+ Add Interface" button:
(Button is shown in Figure 119 – Firewall Rule Interface Tab - Blank)

Interface:	eth2	Direction:	local
Interface:	switch0.6	Direction:	local
Interface:	switch0.7	Direction:	local
Interface:	switch0.8	Direction:	local

Press Save Ruleset.

56. Changing Firewall Rule Ordering.

When adding the rules in section 55 - RESTRICTED_LOCAL Firewall Rules on page113, I deliberately added the "Allow Ping" rule out of order, i.e. as rule #4, so changing rule order could be shown. We want "Allow Ping" as rule #3. See Figure 125 – Rule Order – Before Move. Notice the orange detail.

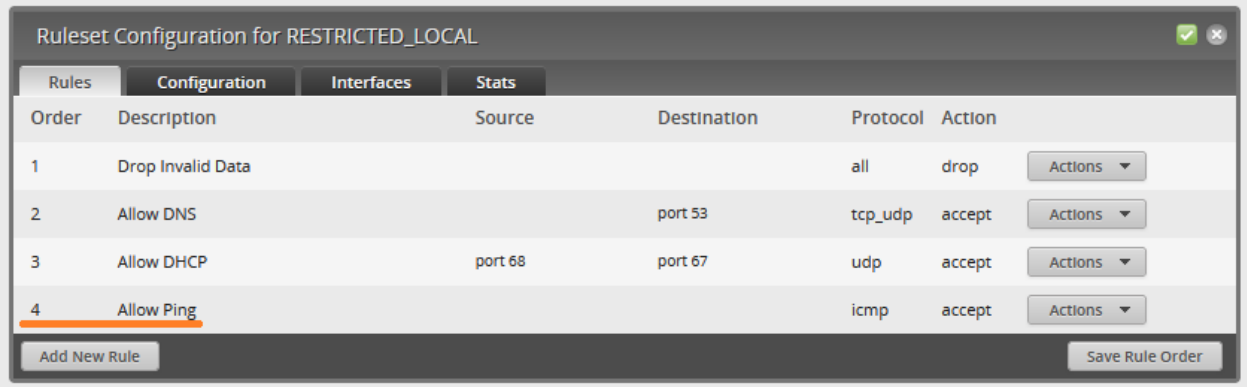


Figure 125 – Rule Order – Before Move

To re-arrange the firewall rule-order within a ruleset, drag a rule from its current position, to its desired positon. I moved "Allow Ping" from the fourth position to the third position. When I let-go of the rule, the dialog will show the new rule order by *only* changing the numbers, not by changing the rule text order. See Figure 126 – Rule Order – After Move, including the orange detail. Ubiquiti only changing the numbers, has confused many people.

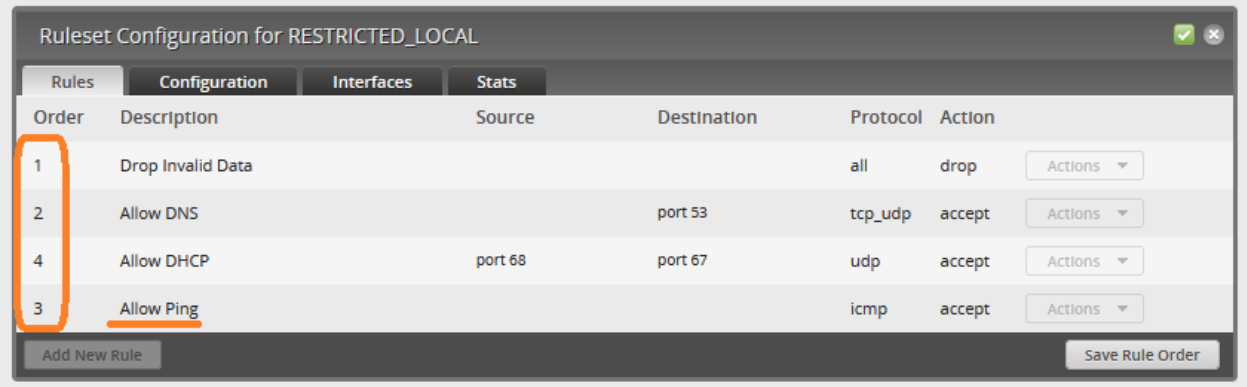


Figure 126 – Rule Order – After Move

Press "Save Rule Order", the dialog will now show the correct / new rule order. See Figure 127 – Rule Order - Finished, notice the orange detail.

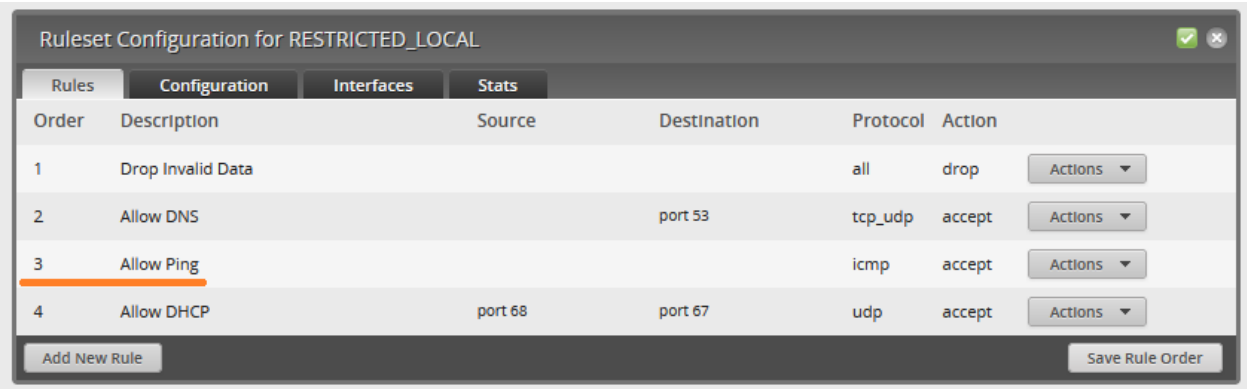


Figure 127 – Rule Order - Finished

57. WIFI_GUEST_IN Firewall Rules

This ruleset is FWR14 as shown in **Figure 102 – Detailed Firewall Setup Diagram** on page 93.

We already made an IOT_IN ruleset in section 54 - Adding Firewall Rules (IOT_IN) on page 105. Ubiquiti has provided a handy “Actions” / “Copy Ruleset” feature which can be used to clone rulesets. We need separate IN rulesets (instead of using a single ruleset applied to multiple interfaces) so we can effectively test the final ER-X firewall.

To copy a RuleSet, Select the “Firewall/NAT” button from the top of the screen. Reference Figure 94 – Firewall/NAT Button on page 86. Ensure that the “Firewall Policies” tab is selected. See Figure 110 – Firewall Policies Tab on page 105.

Select the Actions button at the right side of the IOT_IN line, (the ruleset we want to copy) and then select “Copy Ruleset”. See Figure 128 – Copy Ruleset.

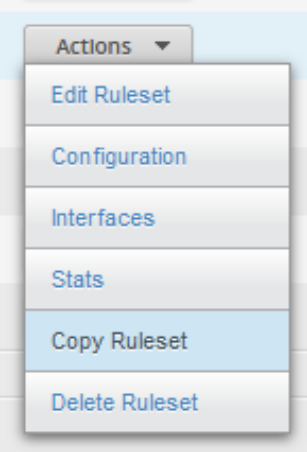


Figure 128 – Copy Ruleset

You should see the dialog of Figure 129 – Copy Ruleset – Enter Name.

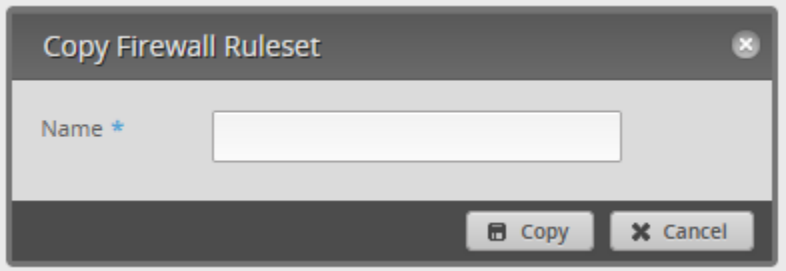


Figure 129 – Copy Ruleset – Enter Name

Enter “WIFI_GUEST_IN” and press Copy.

A new RuleSet was created (with the same internal firewall rules), but with a blank interface / direction.

Set and save the following within the WIFI_GUEST_IN ruleset:

Configuration Tab:
- Description: `WiFi Guest In`

Interfaces Tab:
- Interface: `switch0.6`
- Direction: `in`

For reference, here is the backup-file portion:

```
name WIFI_GUEST_IN {
    default-action accept
    description "WiFi Guest In"
    rule 1 {
        action accept
        description "Allow Home Replies"
        destination {
            group {
                address-group NETv4_switch0.1
            }
        }
        log disable
        protocol all
        source {
            group {
            }
        }
        state {
            established enable
            invalid disable
            new disable
            related enable
        }
    }
    rule 2 {
        action drop
        description "Drop RFC-1918 Traffic"
        destination {
            group {
                address-group rfc-1918_group
            }
        }
        log disable
        protocol all
    }
}
```

58. WIFI_SPARE_IN Firewall Rules

This ruleset is FWR17 as shown in **Figure 102 – Detailed Firewall Setup Diagram** on page 93.

Using the Copy Ruleset method described in section 57 - WIFI_GUEST_IN Firewall Rules on page116:

Copy the IOT_IN ruleset into WIFI_SPARE_IN and set the following:

Configuration Tab:
Description: `WiFi Spare In`
Interfaces Tab:
Interface: `switch0.8`
Direction: `in`

```
name WIFI_SPARE_IN {
    default-action accept
    description "WiFi Spare In"
    rule 1 {
        action accept
        description "Allow Home Replies"
        destination {
            group {
                address-group NETv4_switch0.1
            }
        }
        log disable
        protocol all
        source {
            group {
            }
        }
        state {
            established enable
            invalid disable
            new disable
            related enable
        }
    }
    rule 2 {
        action drop
        description "Drop RFC-1918 Traffic"
        destination {
            group {
                address-group rfc-1918_group
            }
        }
        log disable
        protocol all
    }
}
```

59. WIRED_SEPARATE Firewall Rules

These rules are FWR8, and FWR9 as shown in **Figure 102 – Detailed Firewall Setup Diagram** on page 93.

The Wired Separate Network is meant to be kept separate from the other Networks, i.e., not allow communications with any equipment which is on a different ER-X Network. The Wired Separate Network can only communicate with the Internet.

If you are going to deploy multiple devices on this Network, using a network switch, those devices will natively be able to communicate with each other. Reference section 50.4 - Communication between devices within a Network on page 99. Isolation of these devices will require some sort-of specialized equipment, *maybe* a Layer 3 Network Switch. I have not needed and have not researched this total separation.

There are two usage scenarios (and a requirement), for this 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.
   Similarly, you could instead use the Network for a work-from-home computer.
2. You might want to provide internet access to the friend's kid (i.e. a 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 devices.
3. These two usages also imply another requirement:
   You don't want either of the first two usages to be able to access the internals-of or to modify-the-configuration-of the ER-X.

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

To add the following ruleset and rules, follow what was done previously, in the above firewall rule sections. You should be able to do this by now.

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 RFC-1918 Traffic"
        log disable
        protocol all
        source {
            group {
                address-group rfc-1918_group
            }
        }
    }
}
```

To block usage number 2, we need to block traffic from entering IN the EdgeRouter which is going to devices that are on any of the other (local) Networks.

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 "Drop RFC-1918 Traffic"
        destination {
            group {
                address-group rfc-1918_group
            }
        }
        log disable
        protocol all
    }
}
```

We have already performed the blocking for the above requirement #3 (FWR7), when we previously setup the shared RESTRICTED_LOCAL ruleset in section 55 - RESTRICTED_LOCAL Firewall Rules on page 113.

60. Firewall Setup Conclusion

This concludes the firewall *setup*.

61. Firewall Considerations / Customizations

I hope you now understand the workings of the firewall design of this guide. With that understanding, you should be capable of modifying the described rules to customize them for your own uses, effectively designing your own firewall system.

Some customization items to consider:

1. Maybe you don't like the HomeNet being able to receive responses from other Networks, and want more separation. Example: Maybe you are afraid that if your Iot Network was hacked by a rogue device, a hacker-controlled device could send bogus reply data back into your Home Net to probe or infect it.
2. Maybe you will be running a public server behind this Edgerouter, and don't want there to be any association with your HomeNet.

The easy answer to #1 would be to remove the Iot (or combinations of the three Networks) established/related rule(s) from the Restricted IN ruleset(s).

The easy answer to #2 would be to put your public server on the Wired Separate Network.

61.1 A Network with No Internet Access

What about a Network, maybe populated with cameras, where you don't want those devices to be able to access the internet. One way to achieve this would be to add an "IN" firewall ruleset which defaults to "drop". With no added rules, this would block device communicating with both the internet and all other ER-X Networks (because there is only a ruleset default of "drop"). Any added individual firewall rules within this IN ruleset would (per each added rule) allow a particular (set of) communications between a/some device(s) and a different Network, with the internet being classified as a very-big / sort-of Network.

If you instead had only one particular device on this Network (maybe the camera controller) which required internet access, an individual firewall rule could be added which "allows" only that particular device's IP address to have internet access. This device would need to have a reserved IP address assigned to it, so that the "allow" rule only apples to that particular device. Reference section 68 - Reserving Device Addresses via DHCP on page 135.

The "allow" rule mentioned above, would likely *also* enable that particular device access to other local / ER-X Networks, like HomeNet, IotNet, GuestNet, and/or SpareNet. If you don't also want that access, then add another (higher priority) "drop" rule, dis-allowing access to the local ER-X Networks, like using an "RFC_1918 Group" rule.

Similarly, if you want that device to:

1. Respond to HomeNet queries,
2. But be dis-allowed from other(ER-X) Networks,
3. Access the internet,
4. Where other devices can't communicate outside of its own Network,

then arrange individual firewall rules (in that order) *to do just that*.

Rule number 1 would be "allow" established/related with a specific *source* IP address and a specified *destination* Interface Network. Rule number 2 would be "drop" "RFC_1918 Group" (no specific *source* address needed). Rule number three would be "allow" with a specific *source* IP address. Number 4 is the final *ruleset* default of "drop". If you wanted that device to only access a specific internet (server) IP address, that modify rule number 3 with a specific *destination* IP address. Mix and match the above to what you need / desire.

You may have noticed that to achieve internet access, but to dis-allow local Network access, you need to first drop the list of private IP addresses (RFC_1918 Group), then allow all (other) IP addresses. This is because we know the full list of these private IP addresses, but the list of internet addresses is large (about 3.7 billion routable IP addresses).

61.2 Adding a HOME_OUT Invalid Rule

A more interesting way to answer #1 *might be* to add a drop invalid-state-data firewall rule to a (new) HOME_OUT ruleset. This is optional; I've added this to my own ER-X. If you later have problems with devices receiving replies from either the internet and/or devices on the Guest, Iot, or Spare Networks, you may need to disable this rule. See also postings about "Invalid" rules in section 49.1 - Firewall Postings on page 91.

Following the concepts shown in section 54 - Adding Firewall Rules on page 105, add a new HOME_OUT ruleset.

Firewall/NAT -> Firewall Policies -> +Add Ruleset

Name	HOME_OUT
Description	Home Out
Default action	Accept
Default Log	Un-Checked

HOME_OUT (line) -> Actions -> Interfaces

Interface	switch0.1
Direction	out

Rules Tab -> Add New Rule

Basic Tab

Description	Drop Invalid Data
Enable	CHECKED
Action	Drop
Protocol	All protocols
Logging	Un-Checked

Advanced Tab

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

Press Save

Press Save Ruleset

Now *any* invalid (internet or other-Network-equipment) replies directed to HomeNet devices will be dropped. Remember that every IP packet directed to every HomeNet device will be inspected by this firewall rule.

Discussion about invalid rules:

https://community.ui.com/questions/Rule-of-Drop-invalid-state-in-direction-OUT-of-firewall-polities-Like-WANOUT/53694d7b-403d-4cdf-b666-ca2cc0d86cb0

61.3 Removing "IN"s Established/Related Destination Restriction

You might be able to remove (only) the "Destination switch0.1" restriction from all of Established/Related rules within the IOT_IN, WIFI_GUEST_IN, and WIFI_SPARE_IN rulesets. Those are Restricted Networks (along with the WIRED_SEPARATE Network). The WIRED_SEPARATE Network has no E/R rule within it's IN ruleset.

Reference:

Section 50.3 - Alternate Firewall Design starting on page 98,

Associated Figure 104 – New Firewall Design – RestrictedIn on page 99,

Figure 123 – IOT_IN Firewall, Rule 1 - Destination on page 110.

Note that the following discussions apply to RFC-1918 conversations, i.e. between local Networks, not conversations to the internet.

The stated E/R rules allow replies to conversations (back IN) which have been (externally) started, specifically started by switch0.1, i.e. the Home Network. A device on the HomeNet initiates a query to a Restricted device and expects a reply. Since there are no HOME_IN firewall ruleset/rules, that query is routed to the (designated) Restricted Network.

The associated E/R firewall rule notices the query-data going OUT to devices on the Restricted Network. When the targeted (restricted) device responds, the E/R firewall rule allows those (associated) replies back IN via the rules "accept" clause. Those allowed replies are then routed back to the (originating) Home Network device.

If *all* of your Restricted Networks (IOT_IN, WIFI_GUEST_IN, WIFI_SPARE_IN, and WIRED_SEPARATE_IN) have a "Drop RFC-1918 rule", as we do, then there is *no way* for devices on a Restricted Network to *initiate* a conversation with another RFC-1918 Network. As currently configured, only the HOME Network has no IN rules.

Note that I am only talking about removing the "Destination switch0.1" restriction from the E/R rule. In the current configuration this restriction is redundant. This restriction is to protect against future configuration changes. This section informed you of this fact, and you can now act accordingly to keep or remote that restriction. I'm leaving my "destination switch0.1" restriction intact.

If you were to instead remove the E/R rule from a Restricted Network's IN ruleset, this would disallow the Home Network from receiving a reply from that Restricted Network's device(s). Note this is exactly the design of the WIRED_SEPARATE Network, which has no E/R rule.

If you were to instead remove the "Drop RFC-1918 rule" from a Restricted Network's IN ruleset, then you invite disaster, as you have just ruined a major portion of your firewall's protection. All Restricted network's need to have IN rulesets with a "Drop RFC-1918 rule".

61.4 Adding an Established/Related Rule to RESTRICTED_LOCAL

@BuckeyeNet's EdgeRouter configuration has an additional rule added to his RESTRICTED_LOCAL ruleset. This additional rule is an Established / Related rule, which is now placed as the first rule within his RESTRICTED_LOCAL ruleset. This E/R rule has no further restrictions, and as such, this rule impacts every restricted Network.

This added E/R rule allows restricted devices to reply / respond to queries initiated by the ER-X itself. An example would be "pinging" the device directly from the ER-X. We can already ping restricted devices from the HomeNet, and I can't think of other examples where I could use this added rule, so I haven't added this E/R rule myself.

62. Firewall Testing

I believe I've tested every combination of input-Network vs output-Network, i.e. every combination of the firewall rules. You should rely upon your own testing, especially if you have customized your installation.

If you perform any ER-X firewall testing using a Windows (10) PC, you will need to:

- Configure Windows as a Private Network; for each Ethernet connection / WiFi connection you use.
- Modify Window's internal firewall to allow pings from different Subnets / Networks.
  By default, Windows will only reply to pings within the same subnet / network.

When inventing firewall rules, I don't use "Logging", as those logs are stored in RAM memory, Many Community postings which are asking about un-stable EdgeRouters, almost all turn out to be caused by these logs filling-up all of the EdgeRouter's memory.

Instead, I view the ER-X's internal firewall statistics (counts). To do that:

Select the "Firewall/NAT" button from the top of the screen. Reference Figure 94 – Firewall/NAT Button on page 86. Ensure that the "Firewall Policies" tab is selected. Reference Figure 110 – Firewall Policies Tab on page 105.

Find the desired firewall ruleset of your choice, and on the right side of the line, select "Actions / Stats". See Figure 116 – Firewall Actions Menu on page 106 for the menu.
See Figure 130 – Firewall Stats – Starting. Note the Packets counts. Your counts may not be set to zero.

You can also open-up more than one of these dialogs at the same time.

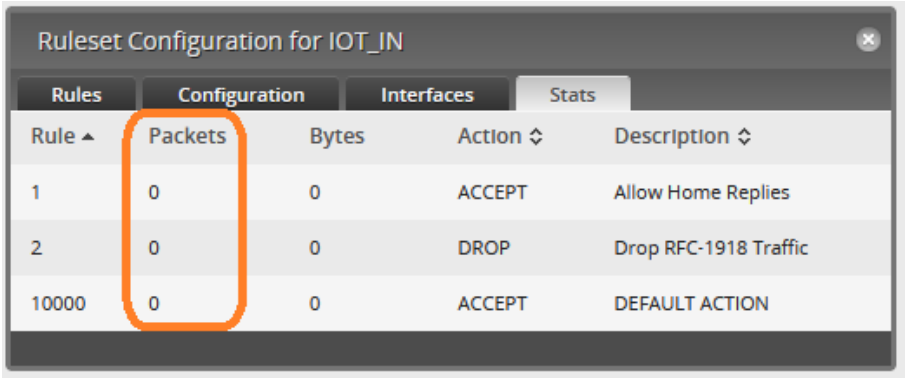


Figure 130 – Firewall Stats – Starting

When a firewall rule matches, the rule's Packet count will be incremented. For most of the following testing, the matching rule will be a "drop", but sometimes the rule will be an "accept". See Figure 131 – Firewall Design – Counted.

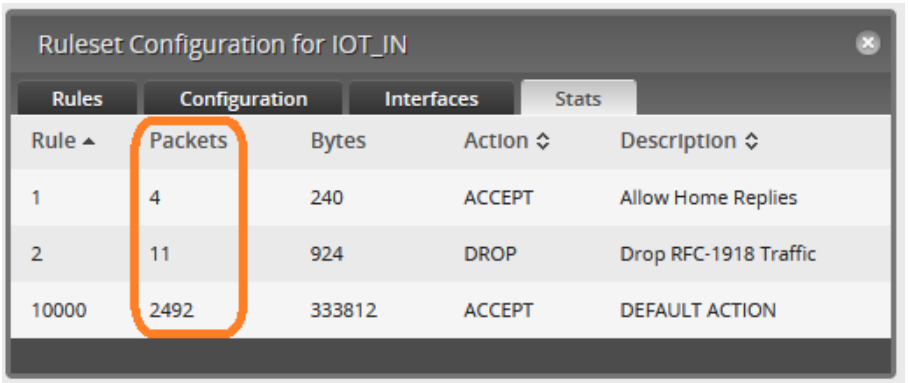


Figure 131 – Firewall Design – Counted

To test the firewall, setup two or more devices, with at least one device on each of the Networks to be tested. Some of these Networks are WiFi only, so this testing can only be executed after the UniFi (WiFi) setup has been completed.

If you are using Windows, the command "`ipconfig`" can be used to determine if your device is connected to the correct network, by viewing the device's DHCP assigned IP address. Similarly, if using Linux for testing, the command "`ifconfig`" can be used. Phones / tablets will have their own method. The device's DHCP address should be checked against Table 2 – Network Details on page 42. Re-check your device's IP address after every change, this also ensures that DHCP has had time to assign an address.

Perform pings between the different Networks. For Networks which have both Ethernet and WiFi components, additionally try all those combinations.

Linux pings execute once per second, by default, until you kill them with ctrl-C. Windows pings default to sending only 4, add a "`-t`" parameter to allow them to run until killed with ctrl-C.

While the "FROM" / source device is pinging, monitor the ping-results / lack-of-ping-results, as that status is what determines the test's pass / fail results. Also monitor the appropriate firewall-rule stats, to ensure that the correct rule is being matched. You want to ensure that the reason a ping is failing, is from an actual firewall rule, and not a faulty test setup. Some of the successful pings will increment accept firewall rules, those should also be checked.

See Table 3 – Firewall Test Results on page 126 and associated Table 3 - Key on page 126.

The UniFi WiFi system has (two) "`Guest Network`" setting(s), which when enabled, can dis-allow all devices on the Guest Network from being able to contact all non-HomeNet devices, including other Guest peer devices. Reference section 90.3 - Create New Wifi on page 204.

In the test-result table, I enclosed in parenthesis characters "()" all the rules which are *internally* blocked by the UAP when the "`Guest Network`" setting(s) are enabled. These are all on the FROM 6.X Guest row. When these WiFi settings are enabled, remember that data packets do not even reach the ER-X firewall, and the firewall counters are therefore not incremented. The underlined text on those special Guest entries is the name of the ER-X firewall rule which would instead block, if those WiFi settings would be turned-off.

You might have noticed that the "6.X Guest" is the only Network where devices cannot (by default) talk to devices on the same Network. Reference section 50.4 - Communication between devices within a Network on page 99. If those UniFi WiFi settings were instead off, Guest devices could talk to other Guest devices. That single cell is marked with "(WiFiGuest)".

Note that the "3.x Home" Network is allowed (via three separate established/related rules) to be able to communicate with devices on the "6.x Guest", "7.x Iot", and "8.x Spare" Networks. Conversations directly initiated from those three Restricted Networks, which are directed to all other ER-X Networks, are blocked by the Rfc-1918 portions of those same three rulesets. This is why the FROM "3.x Home" *row* is different from the TO "3.x Home" *column*.

Also note that the "3.x Home" Network *needs no* firewall rulesets / rules of its own. Optionally there is a drop-invalid rule which *can* be implemented, but is not needed. This is shown in Figure 102 – Detailed Firewall Setup Diagram on page 93. The Home Network is blocked from accessing the Wired Separate Network by the "`Wired Separate Out`" rule (named with WSEP_OUT) as shown in Table 3 – Firewall Test Results.

I've added an Internet testing column in case you have a Restricted Network like that described in section 61.1 - A Network with No Internet Access on page 121. You would also want to test each class of device separately.

		TO					
		3.x Home	**5.x Separate**	**6.x Guest**	**7.x Iot**	**8.x Spare**	**Internet**
FROM	**3.x Home**	✓	✗ WSEP_OUT	✓	✓	✓	✓
	5.x Separate	✗ WSEP_IN	✓	✗ WSEP_IN	✗ WSEP_IN	✗ WSEP_IN	✓
	6.x Guest	✗ GUEST_IN	✗ (GUEST_IN)	✗ (WiFiGuest)	✗ (GUEST_IN)	✗ (GUEST_IN)	✓
	7.x Iot	✗ IOT_IN	✗ IOT_IN	✗ IOT_IN	✓	✗ IOT_IN	✓
	8.x Spare	✗ SPARE_IN	✗ SPARE_IN	✗ SPARE_IN	✗ SPARE_IN	✓	✓

Table 3 – Firewall Test Results

Table 3Key: ✓=Traffic Allowed

✗=Traffic Blocked (Blocking Rule Named)

63. Links for Timed Based Firewall Rules

Several people have wanted to restrict their children's Internet usage based upon time. Here are some sample links:

https://community.ui.com/questions/Restrict-WAN-Access-to-from-LAN-Clients-by-Specific-IP-By-Time-of-Day/9257b80e-46af-4dab-863e-0c3d94a23173

https://community.ui.com/questions/User-based-time-control-of-wifi-access/a95d4e19-db48-4f79-b876-8c91d6375310

https://community.ui.com/questions/Time-control-parental-controll/ce0c0924-9b5d-4eda-be81-6fb83080b753

https://community.ui.com/questions/Set-up-time-limits-for-kids-internet-access/41143a03-96ab-4e76-ba46-45bf2342dd1c

https://community.ui.com/questions/Parental-controls-time-of-day-routing-content-filtering/b0667f8c-309c-43fc-a24f-ab9c95895993

64. Optional DNS Forcing of the IOT 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 force DNS requests within the IOT Network to a specific provider. Note: If you have (Iot) equipment which wants to perform malware / spyware operations, this forcing of DNS will not stop that (determined) level of behavior.

If you setup the NAT rules in this section, ensure you actually used OpenDSN addresses for VLAN.7 (listed as LAN1) in section 32 - Set Domain Name / DNS for a Network on page 67.

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. DNS1 or DNS2, listed in section 14 - About DNS Resolvers on page 35. These two addresses are in the "`OpenDNS Servers`" address group. This allows both the primary and secondary resolver addresses to pass-through the ER-X from the IOT Network unchanged. Note that if the primary DNS resolver is unavailable, then the requesting device will instead (internally) query the backup DSN address.

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 (DNS1) OpenDNS resolver. Note that any IOT device using their own (i.e. non-suggested OpenDNS) resolver address will not operate, when the primary OpenDNS resolver / server is unavailable, as only one destination address is allowed in a DNAT fule.

Press the Firewall/NAT button near the top of the screen. Reference Figure 94 – Firewall/NAT Button on page 86.

The "masquerade For WAN" Source NAT rule was added by the WAN+2LAN2 wizard. Don't mess with it.

Ensure that the NAT tab is selected and then press the "+ Add Destination NAT Rule" button, which is near the middle of the screen. See Figure 132 – NAT Tab.

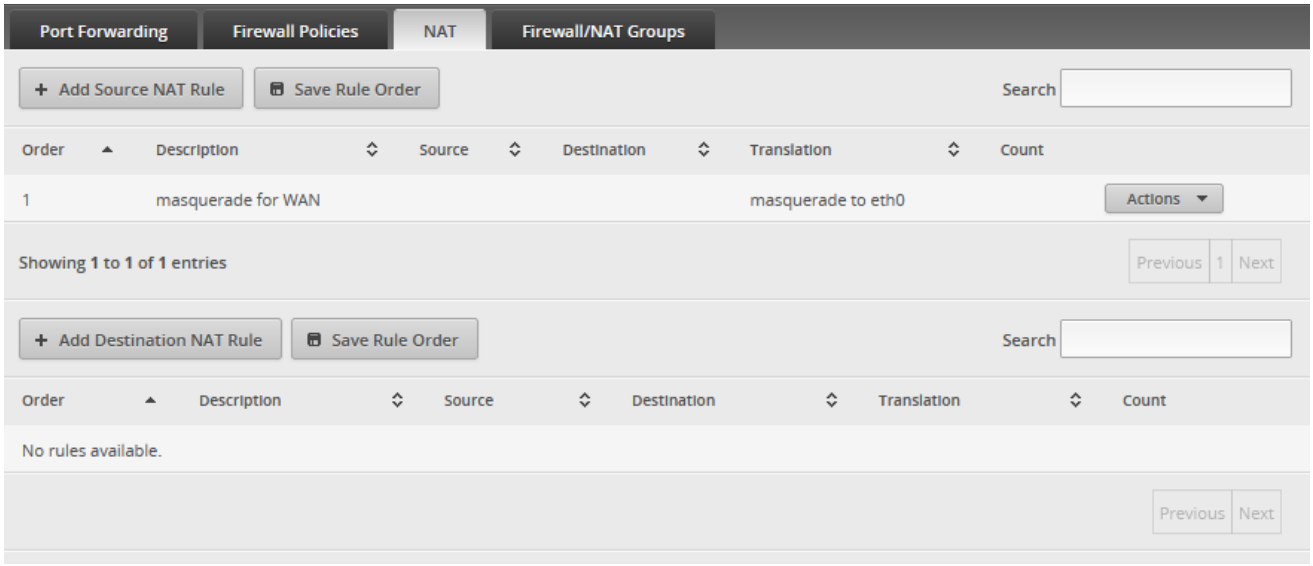


Figure 132 – NAT Tab

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

Enter the data for NAT rule #1, as follows (leave the rest of the fields alone):

Description	`Exclude OpenDNS 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 133 – DNAT Rule Number 1.

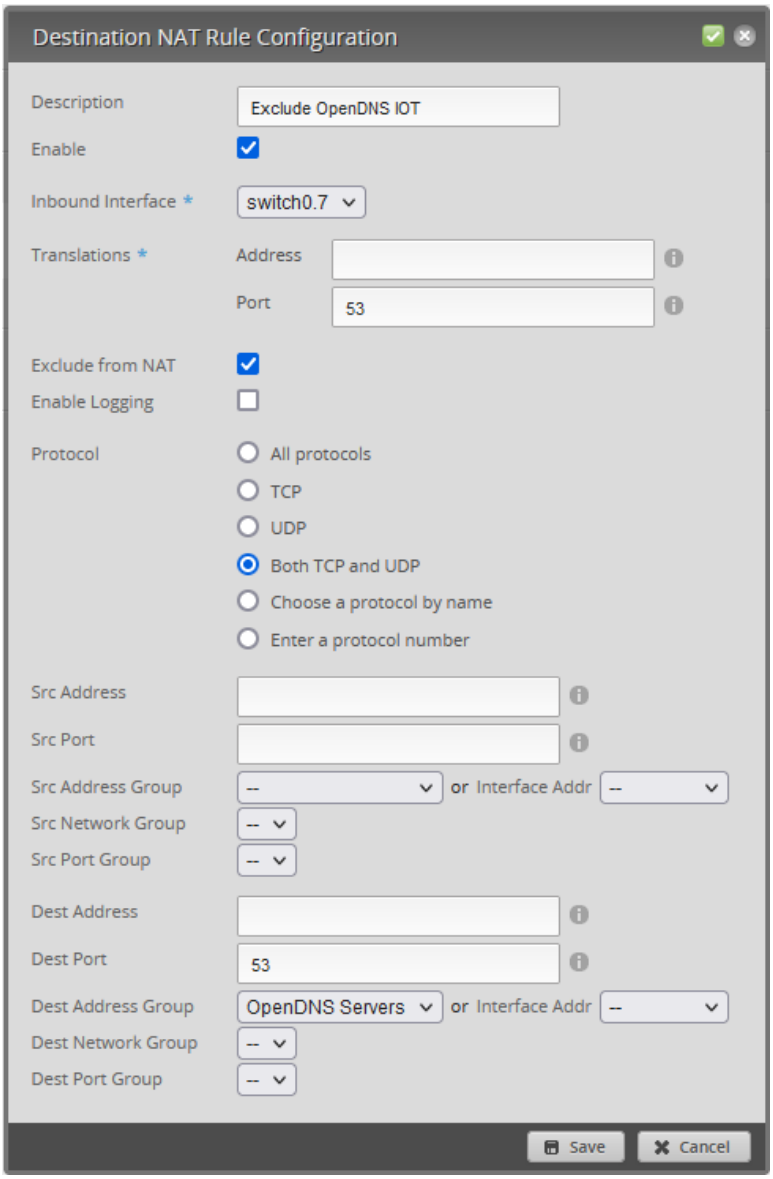


Figure 133 – DNAT Rule Number 1

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

Description	`Force OpenDNS 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 134 – DNAT Rule Number 2.

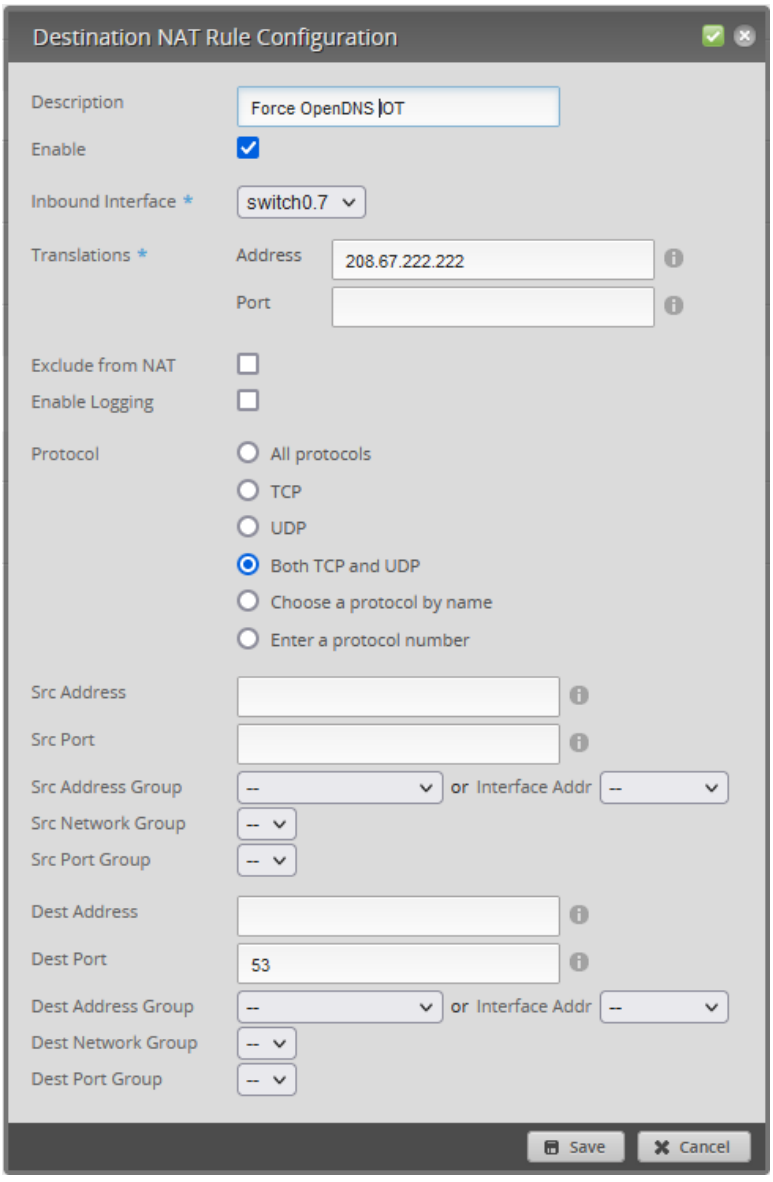


Figure 134 – DNAT Rule Number 2

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 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 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 web page:

http://welcome.opendns.com

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

For reference, I accessed the (above) OpenDNS test page from my Setup Computer, which was not using OpenDNS. I saw Figure 135 – OpenDNS Nope.

To perform this test, first temporarily change the DNS resolver addresses which are sent from the IotDHCP:

```
Services
   DHCP Server
      IotDHCP (line)
         Actions
            View Details
```

Change DNS 1: from `208.67.222.222` to `8.8.8.8`
Change DNS 2: from `208.67.220.220` to `8.8.4.4`
`Save`

On your Iot device, you need to ensure that it is-using / has-been-issued the new (Google) DNS addresses. You could re-boot the Iot device and/or you could issue commands similar to those shown below. You likely also need to close and re-open the web browser used. There is a lot of caching around. Some helpful (windows shown) commands may be (given in order of issuance):

```
ipconfig /release
ipconfig /renew
ipconfig /flushdns
ipconfig /all
```

Check on your Iot device, that the presented DNS resolver addresses are Google's "8s". Access the (above) OpenDNS test page from your Iot device. You should see Figure 136 – OpenDNS Yup. If you got their success page, then these two rules translated the Google DNS addresses into OpenDNS addresses using the DNAT rules.

Return the IOT Network's DNS resolver addresses back to the OpenDNS addresses (shown above) and reboot your Iot equipment.

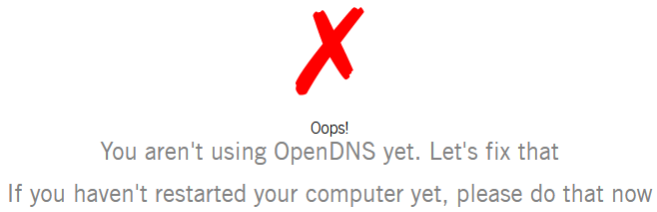


Figure 135 – OpenDNS Nope

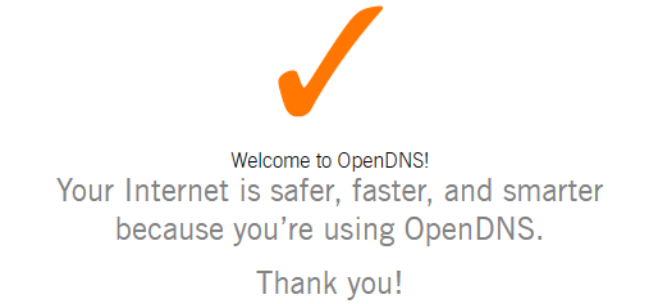


Figure 136 – OpenDNS Yup

Reference this OpenDNS page about testing:

> https://support.opendns.com/hc/en-us/articles/227986567-How-to-Test-for-Successful-OpenDNS-Configuration-

EdgeRouter DNS Redirection Video

> https://www.youtube.com/watch?v=EFWbYQPe3XI

65. Rename your ER-X

To rename your ER-X, first press the "System" button. Reference Figure 9 – System Button on page 29. Find the Host Name section, then change the "System host name" entry, and press "Save" at the bottom of the window. See Figure 137 – ER-X Host Name.

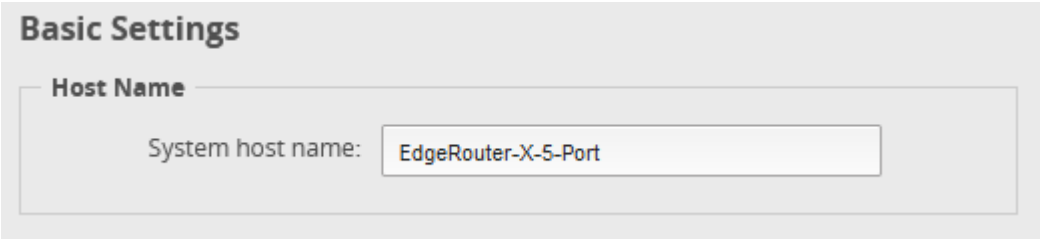


Figure 137 – ER-X Host Name

66. Ubnt Discovery

Way back, the Ubnt Discovery service showed up in an EdgeRouter Community posting:

https://community.ui.com/questions/EdgeOS-responds-to-udp-10001-probes-even-if-service-ubnt-discover-is-disabled/5002a405-1d2e-4d79-9757-dd22c1f9c77f

Per https://help.ui.com/hc/en-us/articles/204976244

> "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."

If you still want to disable this service, the following may help you:

Release Notes for EdgeMAX EdgeRouter software release v1.10.0
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**).
https://community.ui.com/releases/EdgeMAX-EdgeRouter-software-release-v1-10-0-1-10-0/5433d795-9553-46bc-8607-2415bcfa820d

67. Find a Device's IP Address

You can find a device's IP address by selecting the "Services" button. Reference Figure 64 – Services Button. Ensure that the "DHCP Server" tab is selected. Reference Figure 65 – 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 138 – DHCP View Leases Button.

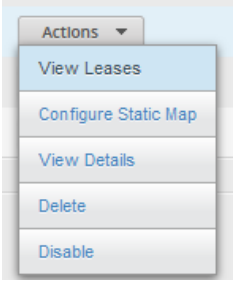


Figure 138 – DHCP View Leases Button

You will then be presented with a DHCP Server Dialog with the Leases tab selected. This dialog will contain a list of your devices which have acquired a dynamic DHCP lease. See Figure 139 – DHCP Server Leases Dialog.

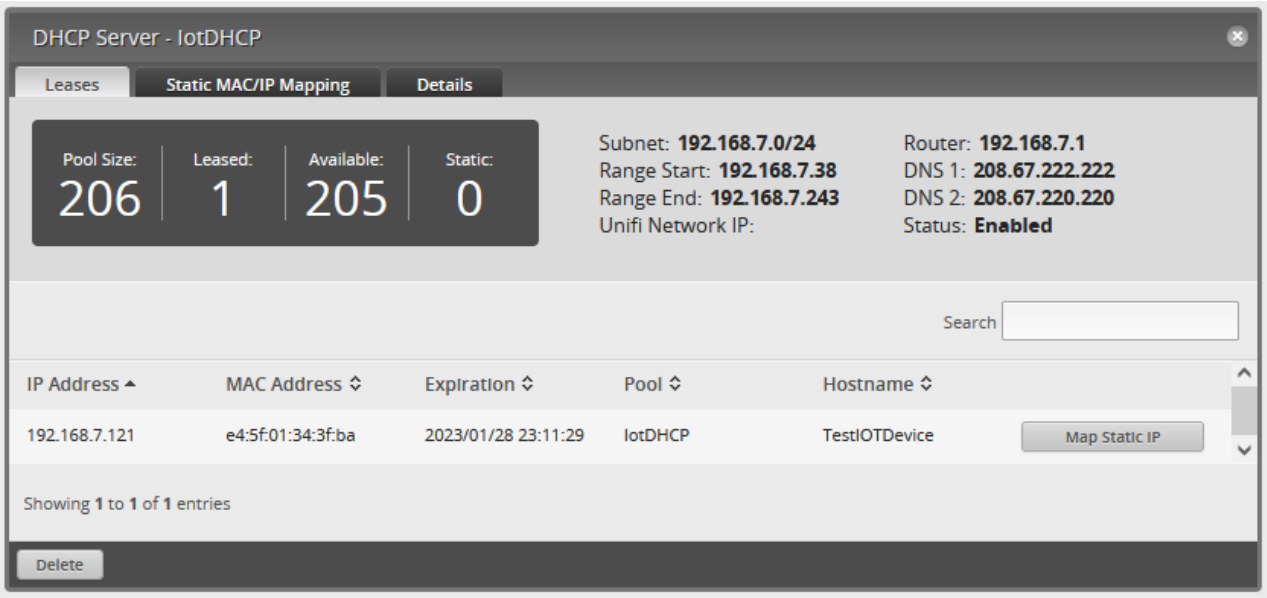


Figure 139 – DHCP Server Leases Dialog

68. 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 75 – DHCP Lan2 Original. The issued IP address 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. Ubiquiti's name, although sounding similar, is actually a totally different method.

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 you should 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 4 - 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 4 - 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. Follow the steps within section 67 - Find a Device's IP Address on page 134. When you see Figure 139 – DHCP Server Leases Dialog, as shown on page 134, 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 140 – Static IP Mapping Dialog

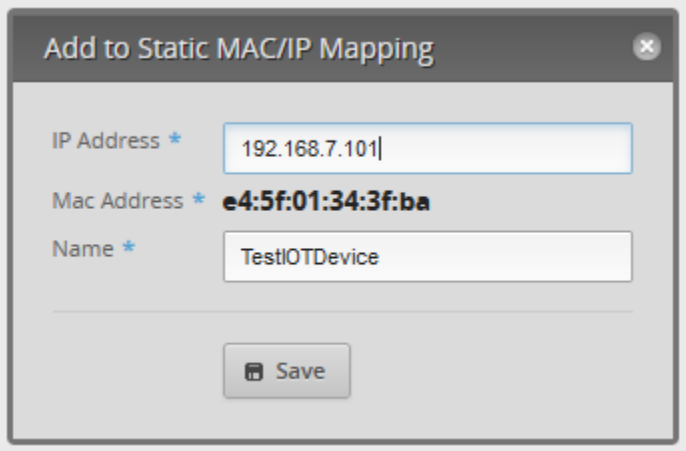


Figure 140 – Static IP Mapping Dialog

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 instead click the "Configure Static Map" button. See Figure 141 – Configure Static Map Button Note that the first three Action items map to the three tabs within Figure 142 – Static IP Mapping Dialog

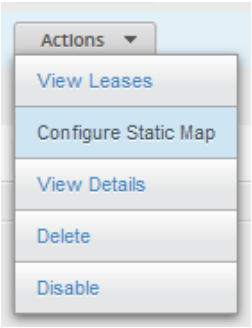


Figure 141 – Configure Static Map Button

You will be presented with a list of reserved IP addresses for the chosen DHCP server. See Figure 142 – Static IP Mapping Dialog

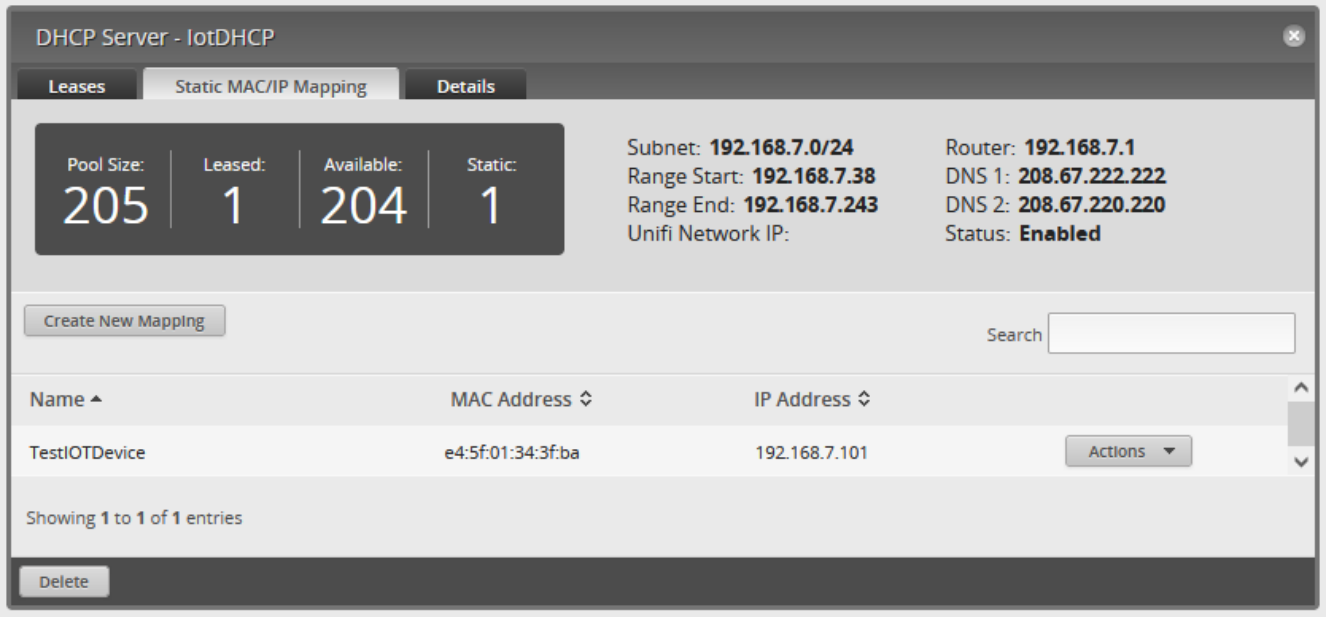


Figure 142 – Static IP Mapping Dialog

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. Said another way: this dialog will not inform you if any reserved device is currently present or absent.

To un-reserve an address, follow the reserved line to the right, and Choose: Actions / Delete, then Confirm.

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.

69. Adblocking and Blacklisting

This is optional. This seems to work flawlessly. I've been using (some version of) this package for about five years. Also reference section 70 - 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.ui.com/questions/DNS-Adblocking-and-Blacklisting-dnsmasq-Configuration-Integration-Package-v1-2-4-8/eb05f1b2-5316-4a80-8221-5e8b02575da4

The above link includes a Frequently Asked Questions section. Change Logs are also available.

See also:

> https://github.com/britannic/blacklist

The following text is cached from the above URL when the stated version was at V1.2.4.8 (at April 2023).

> 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_1.2.4.8_mipsel.deb
>
> sudo dpkg -i edgeos-dnsmasq-blacklist_1.2.4.8_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: 60659
Total entries extracted 58990
Total entries dropped 1669
Successfully restarted dnsmasq
Blacklist update completed.....

69.1 Adblocking / Blacklisting Cached Content

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
```

How do I disable/enable dnsmasq blacklisting?

Use these CLI configure commands:

Disable:

```
configure
set service dns forwarding blacklist disabled true
commit;save;exit
```

Enable:

```
configure
set service dns forwarding blacklist disabled false
commit;save;exit
```

How do I globally exclude or include hosts or a domain?

Use these example commands to globally include or exclude blacklisted entries:

```
configure
set service dns forwarding blacklist exclude cdn.visiblemeasures.com
set service dns forwarding blacklist include www.nastywebsites.com
commit;save;exit
```

How do I exclude or include a host or a domain?

Use these example commands to include or exclude blacklisted entries:

```
configure
set service dns forwarding blacklist domains exclude visiblemeasures.com
set service dns forwarding blacklist domains include domainsnastywebsites.com
set service dns forwarding blacklist hosts exclude cdn.visiblemeasures.com

set service dns forwarding blacklist hosts include www.nastywebsites.com
commit;save;exit
```

70. Pi-Hole Network-wide Ad Blocking

I have not (yet) tried this. Looks VERY interesting. Also Reference sections 69 - Adblocking and Blacklisting and 71 - Other Security Items.

Reference:

https://pi-hole.net/

Best Ubiquiti Community Links:

https://community.ui.com/questions/Intercepting-and-Re-Directing-DNS-Queries/cd0a248d-ca54-4d16-84c6-a5ade3dc3272

https://community.ui.com/questions/Redirect-Hard-Coded-DNS-w-EdgeRouter/a553897c-0675-4ec9-9a59-d1ed82aa9fce

Found from:

https://community.ui.com/questions/Redirect-DNS-to-Pi-hole/6472e3f3-fbc1-4b82-a697-1bad2d7355a4#answer/551d4bfe-3ae3-4527-981c-6394f5804c5c

More Community 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

Even More Community Links:

https://community.ui.com/questions/Redirect-DNS-to-Pi-hole/6472e3f3-fbc1-4b82-a697-1bad2d7355a4

https://community.ui.com/questions/Please-help-me-work-out-how-to-set-up-DNS-details-inside-/55a3cfaa-81f3-43df-9422-d90f71733b1e

https://community.ui.com/questions/config-for-an-internal-DNS-server-pihole-works-but-client-identity-is-obscured-by-having-to-MASQ/d381bf86-877b-4a2d-adf1-6b4a4e8af1d0

https://community.ui.com/questions/ER-X-Pi-Hole-and-cross-interface-communication/818398c0-325e-49bd-986f-e86506cd1f42

https://community.ui.com/questions/Forcing-DNS-to-PiHole-w-DNAT-Allowing-for-Backup-DNS-server/bc8168b3-c6a4-4a05-a18a-48fd90f12ab0

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.reddit.com/r/Ubiquiti/comments/7p457d/ubiquiti_edgerouter_x_with_a_pihole/

71. 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

https://www.ipdeny.com/ipblocks/

72. Configuring a Second / Testing ER-X – Part1

If you have already decided that this ER-X is for you, consider purchasing a second unit. Having a second pre-loaded / pre-configured ER-X is *essential*. A friend had his ER-X taken-out by a power surge / near lightning strike and had to purchase a consumer router, just to get back online. With supply-chain shortages, you can't know when an ER-X will become available for purchase.

If you are considering using "Adblocking and Blacklisting" from section 69, 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.

Since you have been keeping backups (right?), setting up a new ER-X is as simple as swapping the new unit for the old ER-X, loading the firmware / bootloader once, and then loading your backup file.

It is easier to setup a second ER-X now, then after deployment of your main / this ER-X. To do it now, see Figure 143 – Second ER-X Setup - Early. To setup a second ER-X, after this ER-X's deployment, reference section 80 - Configuring a Second / Testing ER-X on page 170.

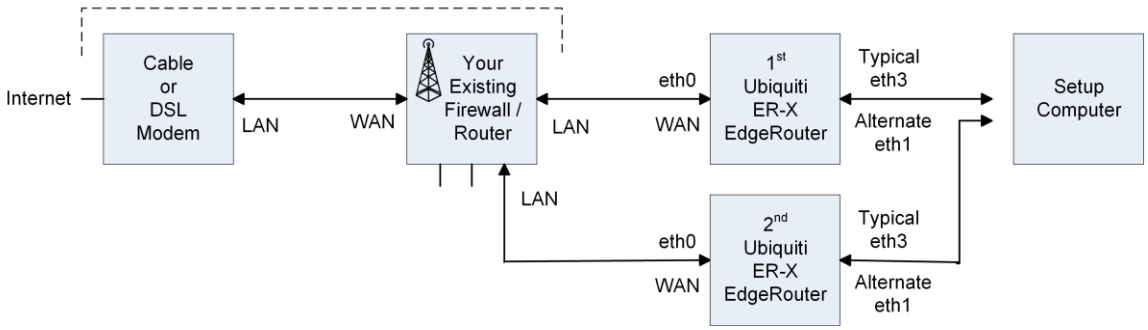


Figure 143 – Second ER-X Setup - Early

73. 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 144 – 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".

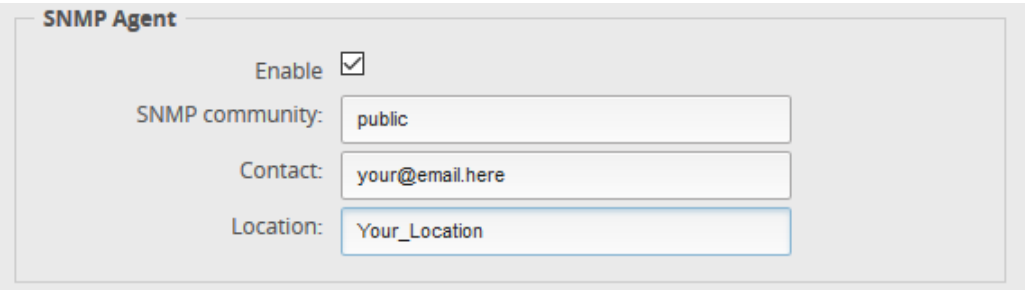


Figure 144 – Sample SNMP configuration.

There is a huge list of SNMP programs which could monitor you router. Some I have seen referenced are:

Snmpwalk
Cacti
NetworX / LibreNMS / PRTG
Nagips / Zabbix / Dude
OpenNMS
MRTG
Grafana / InfluxDB / Telegraf

74. 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 likely the Iot Network.

Note that the following sections were written and tested when the Legacy “Home Out” firewall design was implemented, so some of this data may be out of date, as to specific firewall rules, etc.

Help Link:

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

Related Links:

IOT VLAN multicast still not working

https://community.ui.com/questions/IOT-VLAN-multicast-still-not-working/cdebb828-2ed7-46e9-bee3-55cea4c8cde3

Chromecast traffic between VLANs

https://community.ui.com/questions/Chromecast-traffic-between-VLANs/4a74774e-3a6b-4406-8536-6e034e3f4240

Secure IoT Network Configuration - YouTube -Crosstalk Solutions

https://m.youtube.com/watch?v=6ElI8QeYbZQ

74.1 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. This example connects Home Net and Iot Net.

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 145 – MDNS Setup Example

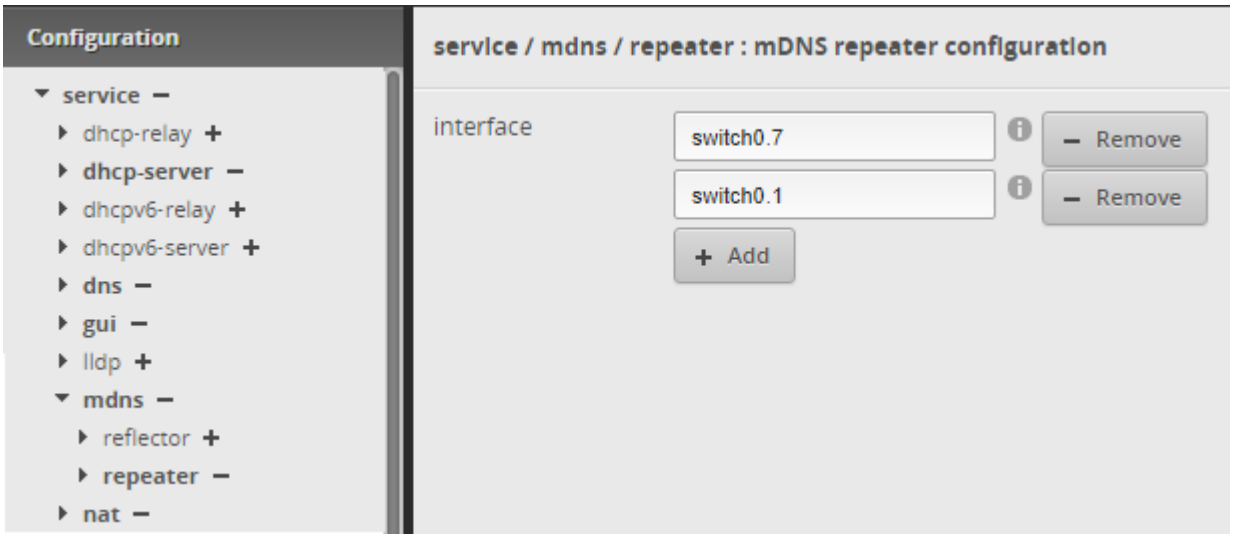


Figure 145 – MDNS Setup Example

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 the EdgeRouter'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 that 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 146 – MDNS Allow Port 5353 for IOT for a screenshot of the same rule.

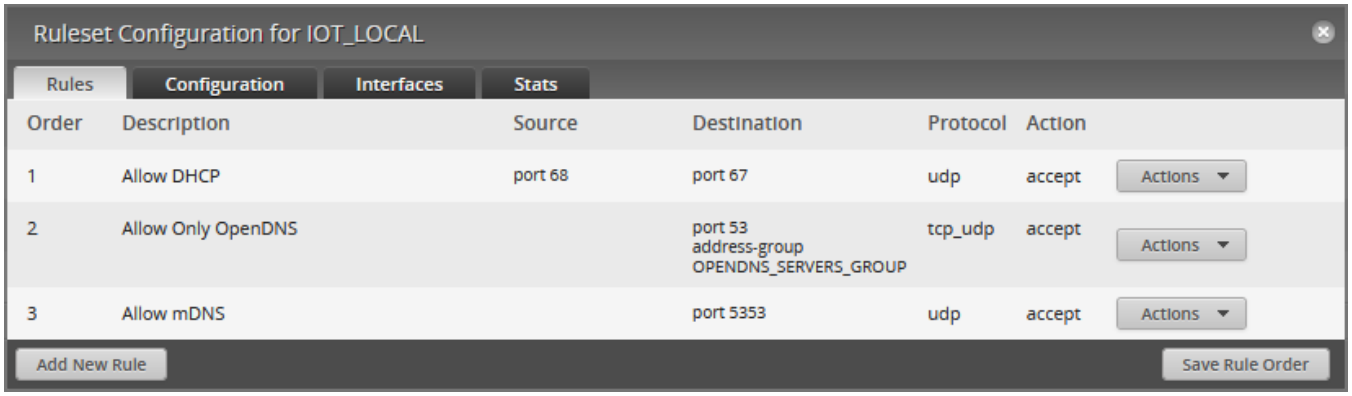


Figure 146 – MDNS Allow Port 5353 for IOT

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 may-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.ui.com/questions/mDNS-bonjour-forwarding/27f7d74f-90f0-4009-bce6-414cff1e859c

https://community.ui.com/questions/mDNS-forwarding-so-that-iPhone-can-communicate-with-iTunes-on-a-PC-over-a-VPN-or-different-subnet/8a17a9e6-3412-4345-abc0-1cf94d222336

https://community.ui.com/questions/Multicast-Sonos-Phorus-and-Play-Fi-Broadcast-255-255-255-255-lessportgreater-Discovery-Solution/1ce890c2-5e7e-4ef2-a42a-e9c59444fd3f

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

74.2 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 associated IN for those specific device replies. All associated devices would need reserved IP addresses, per section 68 - Reserving Device Addresses via DHCP on page 135.

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.ui.com/questions/IGMP-proxy-not-starting-automatically-after-reboot/7758b3bb-b2fe-44af-9d81-1a083c07d9c6

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 had 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 / ancient / incomplete Home Out firewall rules. When I found this, I switched to using the full set of RFC-1918 addresses in the (original) HOME_OUT ruleset.

Ubiquiti Help Links (top link now appears dead):

https://help.ubnt.com/hc/en-us/articles/360001004034-UniFi-Best-Practices-for-Managing-Chromecast-Google-Home-on-UniFi-Network

https://help.ui.com/hc/en-us/articles/4409866388887-Best-Practices-for-Chromecast-and-AirPlay

https://help.ui.com/hc/en-us/articles/204961854-EdgeRouter-Set-up-IGMP-proxy-and-statistics

Community Link(s):

https://community.ui.com/questions/Configure-Sonos-across-subnets-on-USG/a758382b-72e4-446b-90cc-ea353482ff1a

Here is a command to see what is going through the firewall on port 1900:

```
sudo tcpdump -i switch0.1 port 1900 -vv
```

74.3 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/

75. Virtual Private Networks (VPN)

I have not played with or implemented a VPN. There seem to be several types. Here are some VPN links.

ZeroTier appears even newer than Wireguard:

https://community.ui.com/questions/Guide-ZeroTier-on-Ubiquiti-EdgeRouter-as-VLAN/e8974aaf-011d-42ef-8263-3899bbb26462

https://kruyt.org/zerotier-on-a-ubiquiti-edgerouter/

https://community.ui.com/questions/How-to-bridge-two-network-interface/b74f4c6e-dbea-4587-bd53-3ce8acdf9b6b

Wireguard appears newer, better, faster than OpenVPN:

https://community.ui.com/questions/Release-WireGuard-for-EdgeRouter/3765d2a4-1952-4629-948a-3ac9d9c22311

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/

EdgeRouter - OpenVPN Server:

https://help.ui.com/hc/en-us/articles/115015971688

EdgeRouter - L2TP IPsec VPN Server:

https://help.ui.com/hc/en-us/articles/204950294-EdgeRouter-L2TP-IPsec-VPN-Server

EdgeRouter - Site-to-Site VPN Behind NAT

https://help.ui.com/hc/en-us/articles/115013382567-EdgeRouter-Site-to-Site-VPN-Behind-NAT

EdgeRouter - EoGRE Layer 2 Tunnel

https://help.ui.com/hc/en-us/articles/204961754-EdgeRouter-EoGRE-Layer-2-Tunnel

GUIDE: How to configure Local PPTP VPN:

https://community.ui.com/questions/GUIDE-How-to-configure-Local-PPTP-VPN-on-1-5-0-Firmware-works-on-iOS/6474a0e2-ce17-4d8f-a6c5-8c8d677f7108

Private Internet Access Open VPN - Step by Step Configuration:

https://community.ui.com/questions/Private-Internet-Access-Open-VPN-Step-by-Step-Configuration/2489d69e-cdce-4975-87a1-1898be2bb2e0

Troubleshooting-Site-To-Site-on-ER-Xs:

https://community.ui.com/questions/Troubleshooting-Site-To-Site-on-ER-Xs/f6851127-fda7-4f97-86c3-b3e7b838e1dd

Ubiquiti-edgerouter-ipsec-performance:

https://www.simonmott.co.uk/2018/08/ubiquiti-edgerouter-ipsec-performance/

OpenVPN vs L2TP:

https://community.ui.com/questions/OpenVPN-vs-L2TP/7992d6bf-bac1-49a0-a08d-96ffcf162920

Secure OpenVPN server setup with multi-factor authentication (Google Authenticator): step-by-step:

https://community.ui.com/questions/Secure-OpenVPN-server-setup-with-multi-factor-authentication-Google-Authenticator-step-by-step/8b42e255-bd50-41ff-88c6-ad4e0512be7c

OpenVPN configurator for EdgeMax

https://community.ui.com/questions/Helpful-Tool-OpenVPN-configurator-for-EdgeMax/3a8f3655-5513-43aa-943b-21bdcd384626#M251490

76. UNMS - Ubiquiti Network Management System

Barely played with this:

https://help.ui.com/hc/en-us/articles/360008732414-UNMS-NetFlow

77. ER-X Marking

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

Labels for permanent items

Blue (masking type) Tape for temporary labels

See Figure 147 – ER-X Example Marking.

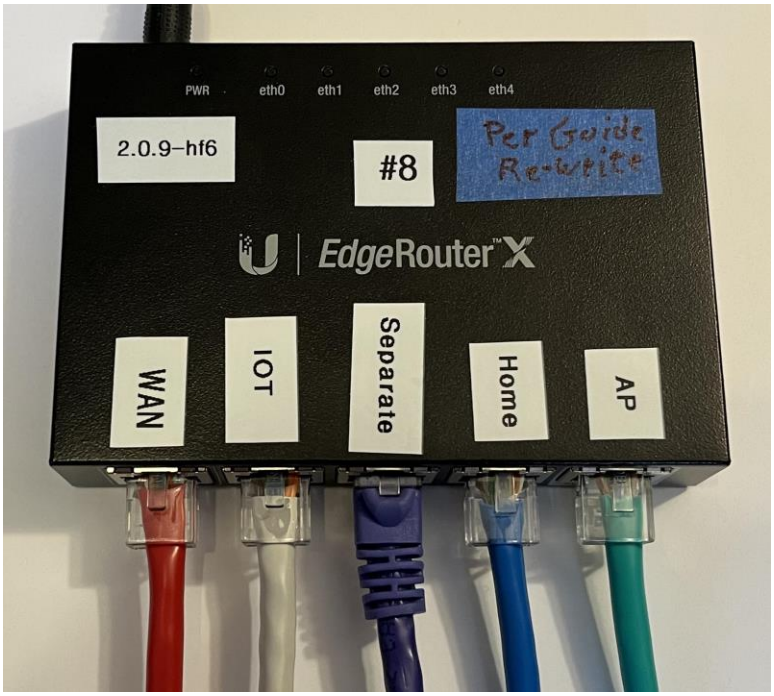


Figure 147 – ER-X Example Marking

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

78. Customizing the ER-X for Your Installation

We have now finished the basic ER-X configuration. There are a number of options / customizations that can occur, to better match your own installation needs. Please re-familiarize yourself with the following:

Figure 1 - Overview Diagram on page 6.

Text preceding and Figure 60 – Switch0 eth4 Settings on page 60.

78.1 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.

78.2 Comments about Network Switches

Figure 1 - Overview Diagram on page 6, shows a bunch of network switches on it, and most are marked optional. If you only need one Ethernet device plugged into any particular ER-X Ethernet port, you don't need a network switch.

Network switch(s) are typically centrally located, near your ER-X EdgeRouter.

Ethernet network switches which are going to carry VLAN data need to be 802.1Q capable. The 802.1Q specification is *how* to carry VLAN data on an Ethernet network. Here is a good article for that specification:

https://en.wikipedia.org/wiki/IEEE_802.1Q

Since the Ethernet frames are now bigger, older network switches will not carry VLAN data.

With the current / base ER-X configuration, the only port carrying VLAN data is eth4, the port which is shown connected to a single Ubiquiti Access Point in Figure 1. Figure 1 doesn't even show a network switch at that location. If you will using more than one UAP, then you will need an 802.1Q capable network switch connected between the ER-X's eth4 port and your multiple UAPs.

@shermbug suggests that unmanaged switches not be used for carrying VLAN data. Every recently-purchased *gigabit* unmanaged network-switch which I have tried, correctly worked with VLAN data. Most unmanaged gigabit network switches seem to be priced at about $20 US.

It is probably a good idea, when using your specific network switch (which is connected to eth4), to test that all of your Home, Iot, Guest, and Spare (3 are VLAN) Networks are operating correctly.

To test if a specific network switch works with VLAN data, connect some WiFi equipment to the Iot / Guest / Spare Network (one at a time) and see if that equipment connects and can send/receive data to the internet. Additionally notice if the equipment acquires an IP address in the IP range according to Table 2 – Network Details on page 42.

Early in 2021, I purchased a *managed* 24-port gigabit-switch. It is now the *only* network switch connected to my ER-X. This managed switch is connected to the ER-X via eth4 and can provide Ethernet ports for Home, Iot, Guest, and Spare Networks, as well as some special functions. This single switch replaces all the switches shown in Figure 1 and makes for a much cleaner installation. My ER-X's VLAN configuration was customized to provide this feature. Customization will be discussed in the next several sections.

The managed network-switch model which I choose was HP J9803A (Procurve 1810-24G). This was acquired as used, on eBay for under $60 US shipped. Early in 2023, I purchased a second used switch, as a spare, which cost under $40 US shipped (it helps to not be in a hurry). This switch supports 802.1Q VLANs. 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.

78.3 About Using Two or More Ubiquiti Access Points

Depending upon your installation site, you may need more than one Ubiquiti Access Point to provide more / better / wider Wi-Fi coverage. There are several ways to achieve this. If you only have one Access Point, a network switch is not needed between eth4 and your single UAP.

Each of Ubiquiti's U6 dome models, which are listed in Table 1 – Ubiquiti U6 Access Point Models on page 14, needs to be provided power. The method used is Power Over Ethernet (POE). Some UAP models actually need POE+ which can supply more power than (regular) POE.

The lowest cost method for maintaining data separation is to use two 802.1Q-capable un-managed gigabit network-switches:

Use the first network switch to connect your HomeNet devices to the ER-X'eth3 port

Use the second network switch to connect your UAPs to the ER-X's eth4 port

This is Method1A, described below.

Method 1A:

Connect an 802.1Q-capable **(managed or unmanaged) network switch to eth4**, and then connect your Access Points to this switch.

- Recently manufactured unmanaged gigabit network switches should work. Reference section 78.2 - Comments about Network Switches on page 155.
- Managed switches will need to be specifically configured to pass Trunk data, as well as VLAN 6, 7, and 8 data to/from ER-X's eth4 connected port and to/from each port connecting to a UAP.
- Managed switch ports which are not connect to a UAP, can be configured for any of Home, Iot, Guest, or Spare Networks.
- You will need a dedicated POE/POE+ power adapter for each UAP. Note that the power adapter's actual POE-marked-port connects *directly* to the UAP.

Method 1B:

Connect an 802.1Q-capable **(managed or unmanaged) POE/POE+ network switch to eth4**, and then connect your Access Points to the POE-enabled ports on this switch. Using a POE(+) network switch eliminates the need for dedicated POE power adapters for each UAP.

- Before purchasing, ensure the POE switch is 802.1Q capable *and* each port is gigabit capable. POE switches are more expensive than non-POE models, so protect your investment.
- Some UAPs need POE+, some only (regular) POE. If purchasing a new POE switch, I suggest acquiring a POE+ model. A POE+ model can also power (the lower powered / regular) POE equipment without harm.
- POE switches typically have an overall/maximum power limit, as well as a limit on the number of POE(+) ports.
- Managed POE switches will need to be specifically configured to pass Trunk data, as well as VLAN 6, 7, and 8 data to/from ER-X's eth4 connected port and to/from each port connecting to a UAP.
- Managed switch ports which are not connect to a UAP, can be configured for any of Home, Iot, Guest, or Spare Networks.

Method 2A:

Connect an 802.1Q capable **(managed or unmanaged) network switch instead to *eth3***.

- See all the bullet points in Method 1A, above.
- **IF** this network switch is un-manged, then VLAN data will be present / available to all HomeNet devices connected to this network switch. This is probably not a concern, but you would need to use a managed switch to not have this happen.
- Needed VLAN customization will be discussed in section 78.4 - VLAN Switch Customization on page 158.
- This method frees-up and allows eth4 to be able to be used as a "Second Wired Separate Network". Described in section 78.5 - Optional Second Wired Separate Network on page 164.

Method 2B:

Connect an 802.1Q capable **(managed or unmanaged) POE/POE+ network switch instead to eth3.**

- See all the bullet points in Method 1B, above.
- **IF** this network switch is un-manged, then VLAN data will be present / available to all HomeNet devices connected to this network switch. This is probably not a concern, but you would need to use a managed switch to not have this happen.
- Needed VLAN customization will be discussed in section 78.4 - VLAN Switch Customization on page 158.
- This method frees-up and allows eth4 to be able to be used as a "Second Wired Separate Network". Described in section 78.5 - Optional Second Wired Separate Network on page 164.

See also section 84 - Hookup your Ubiquiti Access Point(s) on page 178.

78.4 VLAN Switch Customization

Otherwise known as “So what is the meaning of PVID / VID?”

Reference these sections:

23 - Enabling the ER-X’s VLAN Switch on page 51.
78.2 - Comments about Network Switches on page 155.
78.3 - About Using Two or More Ubiquiti Access Points on page 156.

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 Untagged (HomeNet) data, as well as 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.

Two Part VLAN Article:

https://community.ui.com/stories/Do-people-use-VLANs-for-the-right-things-Pt-1/7ab6782d-37d1-4afa-9516-ca1d166c3ede

https://community.ui.com/stories/Do-people-use-VLANs-for-the-right-things-Pt-2/14ab46db-798f-4138-8926-f7ff57d67854

The ER-X's VLAN switch was configured as the following:

```
switch switch0 {
    description Local
    mtu 1500
    switch-port {
        interface eth1 {
            vlan {
                pvid 7
            }
        }
        interface eth3 {
            vlan {
                pvid 1
            }
        }
        interface eth4 {
            vlan {
                pvid 1
                vid 6
                vid 7
                vid 8
            }
        }
        vlan-aware enable
    }
```

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 per port, but you can have zero, one, or multiple `vids` per port.

Per the above switch0 configuration file portion, we have the ER-X ports configured to carry:

Eth0	WAN / Internet	(Not part of switch0)
Eth1	Untagged IOT data	Because of pvid7
Eth2	Wired Separate Network	(Not part of switch0)
Eth3	Untagged HomeNet	Because of pvid 1
Eth4	Untagged HomeNet	Because of pvid 1
	Tagged (VLAN) GuestNet	Because of vid 6
	Tagged (VLAN) IotNet	Because of vid 7
	Tagged (VLAN) SparetNet	Because of vid 8

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 internal switch0's 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.

In section 28 - Finish configuring the Vlans on page 60, 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 "WiFi Spare Network" data.

The default setup only allows (non-VLAN tagged) Home Network data to appear on `eth3` because that should work with all equipment plugged into eth3, even old 10/100 (non-VLAN aware) network switches.

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 148 – Example PVID, VID settings. In this example eth1 carries untagged IOT Network data from VLAN 7. eth2 and eth4 are each (two different) separate Networks, which don't involve using switch 0 or 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 78.5 - Optional Second Wired Separate Network. This is the configuration I am using, since I have now purchased a *managed* network switch.

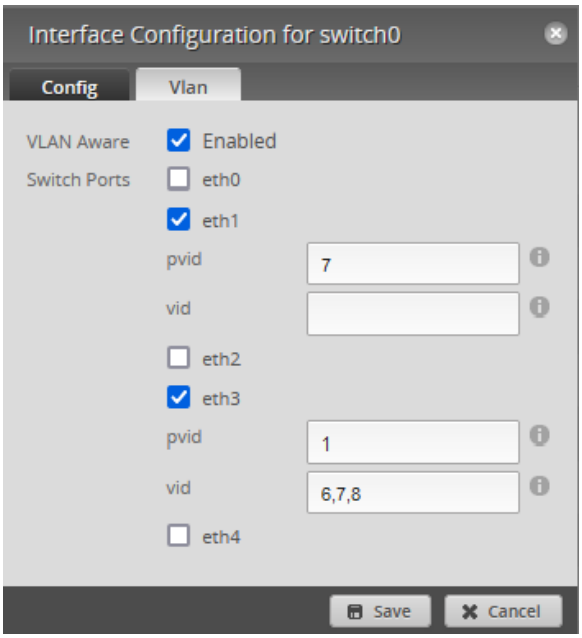


Figure 148 – Example PVID, VID settings

Here is a further example. If you connect a *managed* network switch to eth3, you no longer need Iot data to appear on eth1, since you can connect your Iot devices to (specifically configured ports on) your managed switch. This frees-up eth1, and you could then convert eth1 to a *third* Wired Separate Network.

If you go to this extreme, you might want to purchase and pre-configure an additional managed switch as a backup.

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 (only one `pvid` is allowed).

Selecting which VLANs are presented, as tagged data, per port (zero to multiple `vid`(s) are allowed).

Excluding (VLAN Network) data from specific ports, either by a 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.

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, IOT3, WiredSeparate18, 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 the ER-X's (network switch connection) eth3 and then configure your managed switch to use them.

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. Buy a 24 port *managed* switch and you can have 26 independently configured / managed ports: 3 from the ER-X , plus 23 from the switch.

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.

For my HP managed switch, you configure it using a web page. To configure the port's VLAN usages, you first configure the list of VLANS. This guide's default VLAN list is: `1,6,7,8`. For my own installation, I've added additional Wired Separate Networks of `9` and `10` using additional VLANS.

For each port of the HP's 24-ports, you then configure for the desired trunk / vlan usage. The following nomenclature is used during HP port configuration:

E = **E**xclude from Vlan,
T = participate as **T**agged i.e. `vid`,
U = participate as **U**ntagged i.e. `pvid`.

Remember that Vlan1 is our "trunk", i.e. HomeNet

As an example, this is how I've configured my HP switch ports (ports 21 – 24 are not shown):

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...	
Vlan1	U	U	U	U	U	U	U	X	E	E	E	E	U	U	U	U	U	U	U	U		HomeNet
Vlan6	T	T	T	T	T	E	E	X	E	E	E	E	E	E	E	E	E	E	E	E		Guest
Vlan7	T	T	T	T	T	E	E	X	E	E	U	E	E	E	E	E	E	E	E	E		IOT
Vlan8	T	T	T	T	T	E	E	X	E	E	E	U	E	E	E	E	E	E	E	E		WiFiSpare
Vlan9	T	T	T	T	T	E	E	X	U	E	E	E	E	E	E	E	E	E	E	E		WiredSep3
Vln10	T	T	T	T	T	E	E	X	E	U	E	E	E	E	E	E	E	E	E	E		WiredSep4

The first 5 ports are identical: port 1 is the "uplink" to the ER-X, while ports 2 - 5 are used for Access Points,
all Vlans are present and Vlan1 (trunk) is **U**ntagged, this matches the configuration of the ER-X's port.
Ports 6 – 8 involve port mirroring, not described in this guide.
Ports 9 – 13 are one each: Vlan9, Vlan10, Vlan7, & Vlan8, each as **U**ntagged data.
Ports 13 – 24 are Home Network: as **U**ntagged data, no additional VLAN data is present on these ports.

This is the real power of a (non-consumer) router.

- You have full control over which Network data goes to each of the Edgerouter's ports, and whether 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 (i.e. VLANS).
- Firewall rules have a lot of built-in primitives, which can be combined to generate very powerful specifically-targeted rulesets.
- Expandability can optionally be achieved:
  - Via *un-managed* network switches, with one added switch per specific function, as shown in Figure 1 - Overview Diagram on page 6.
  - Via a *managed*-network-switch; this provides full (tagged / un-tagged) control over each managed port. Having more (controlled) switch ports allows the generation of more / specialized Networks within the EdgeRouter / managed switch combination. Examples:
    - Many (more) wired-separate networks (extension of section 78.5 on page 164)
    - Two (or more) separate Iot Networks (setup similar to section 78.5 on page 164)
    - Camera Network with no internet (see section 61.1 on page 121)
    - Separate RFC-5737 Network for testing a second / backup ER-X (see section 80 on page 170)

    Note: you are still limited to 4 Wi-Fi SSIDs by the design of the Unifi Access Points.

Maybe you have a remote location, with a bunch of different types of equipment, but only have a Single Ethernet Wire connecting to the remote location. See Figure 149 – Example Remote Network Switch. You can use the same VLAN concept(s) as above, but in a different (type of) application.

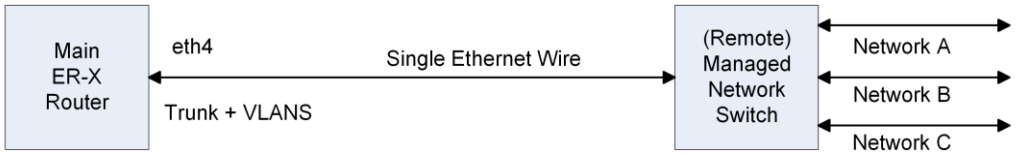


Figure 149 – Example Remote Network Switch

An additional ER-X can also be used as a managed network switch, when configured using "Switch" in the setup wizard. Reference Figure 22 – Wizard Screen Portion on page 36. I have not tried this. Using an ER-X as a network switch is probably too expensive for normal / home applications.

Interesting, you can power a remote ER-X from a local ER-X, when the local ER-X is itself powered via an external 24V Passive POE adapter.

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

Warning: enabling an ER-X's POE output (eth4 only) will apply ***lethal*** voltages to any non-passive-24V-acceping-equipment which is connected to that ER-X's eth4 port. This type of POE is non-forgiving and will destroy any foreign equipment connected. 24V Passive POE is also used in earlier models of Ubiquiti's Access Points, including the AP-AC-LR model.

78.5 Optional Second Wired Separate Network

If you use an 802.1Q compatible (managed or unmanaged) 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. 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. This example will use eth4, but could instead replace the Iot Network on eth1.

If you use an *un-managed* network switch connected to eth3, then all tagged data (VLANs 6,7,8) is also available to any eth3 connected equipment.

Reference the following sections:

78.2 - Comments about Network Switches on page 155

78.3 - About Using Two or More Ubiquiti Access Points on page 156

78.4 - VLAN Switch Customization on page 158.

To do this, go to the Dashboard tab, find the switch0 line, and select Actions / Config. Select the Vlan tab. Un-check eth4. This removes eth4 from switch0. Add vids of "`6,7,8`" to `eth3`. This allows connected UAPs to see VLAN data on eth3. Save. See Figure 150 – Separate2 – Reconfigure Vlan

Go to the Dashboard tab, find the eth4 line, and select Actions / Config. Change the Description to "Separate2Net". Change the Address from "No Address" to "Manually Define IP address" and then enter in 192.168.9.1/24. Save. Reference Figure 151 – Separate2 – Add Address to eth4.

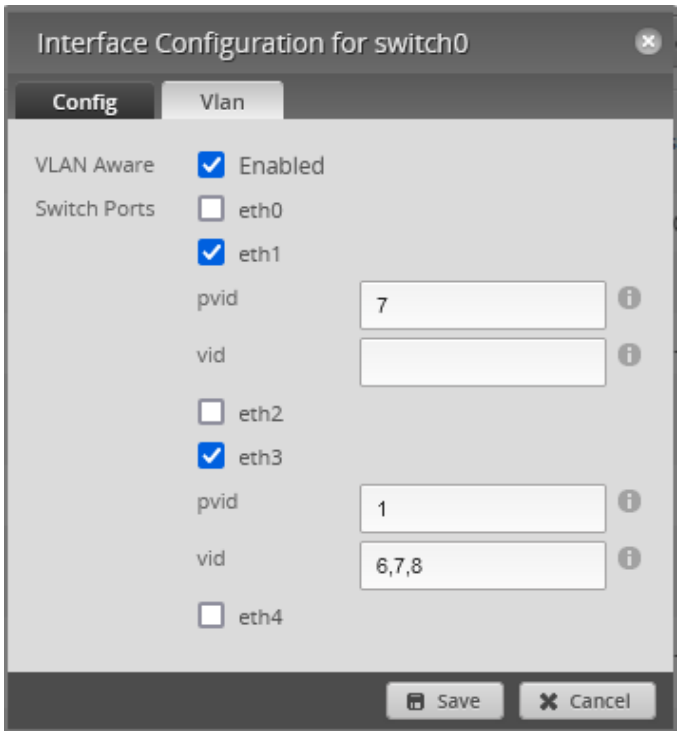


Figure 150 – Separate2 – Reconfigure Vlan

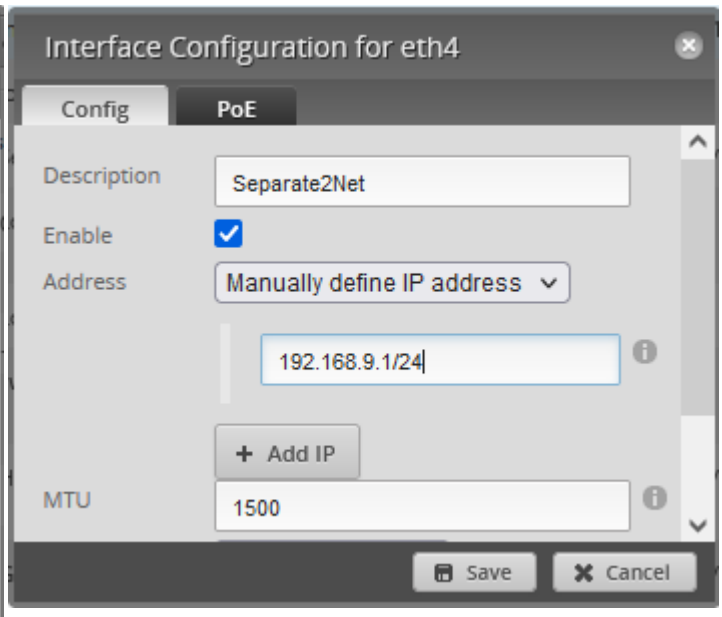


Figure 151 – Separate2 – Add Address to eth4

Go to Services, DHCP Server tab, click on "+ Add DHCP Server" and fill-in the dialog, as shown in Figure 152 – Separate2 – Add DHCP. Use whichever DNS servers you wish. Press "Save".

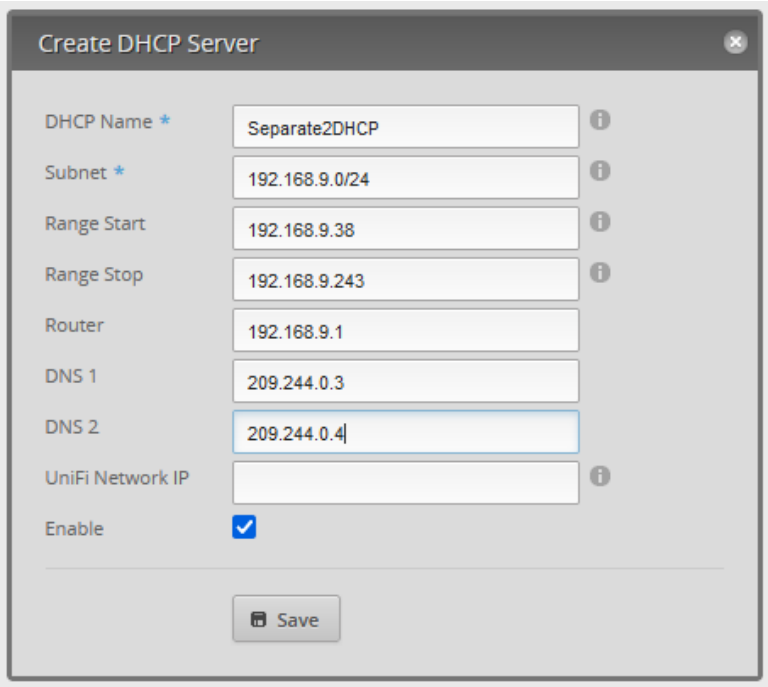


Figure 152 – Separate2 – Add DHCP

Ensure that you make this new DHCP server – "authoritative". Follow the directions in section 31 - Make a DHCP Server Authoritative on page 65.

Next, we need to add new interfaces to three existing "Wired Separate" / "Restricted Local" firewall rules. This is even easier than copying existing rules, which is easier than re-creating (the same) rules from scratch.

Start at the Firewall/NAT tab, and then select the Firewall Policies tab.

On the "WIRED_SEPARATE_IN" line, select Actions / Interfaces.
You will be presented with an Interfaces dialog.
Reference Figure 119 – Firewall Rule Interface Tab - Blank on page 107.
Click on `+ Add Interface`
Set Interface: `eth4` Set Direction: `in`
`Save Ruleset`

On the "WIRED_SEPARATE_OUT" line, select Actions / Interfaces.
You will be presented with an Interfaces dialog.
Click on `+ Add Interface`
Set Interface: `eth4` Set Direction: `out`
`Save Ruleset`

On the "RESTRICTED_LOCAL" line, select Actions / Interfaces.
You will be presented with an Interfaces dialog.
Click on `+ Add Interface`
Set Interface: `eth4` Set Direction: `local`
`Save Ruleset`

79. Preparing the ER-X as Your Primary Router

79.1 Login / Password

Ensure that you are using a unique login name for your ER-X and that the associated password is both long and has enough entropy. This will be useless if you don't also remove the default "ubnt" login credentials, which are widely known.

79.2 Double-NAT

Reference Figure 2 - EdgeRouter DHCP Initialization Wiring on page 25. Note that your own modem / routing equipment may instead have the "Cable or DSL Modem" portion and "Your Existing Firewall / Router" portion combined into one single unit.

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.

You have a decision to make when deploying your ER-X as your primary router, you can:

1. Have the ER-X be your main and only router.
   a) If you have a separate modem device and a separate router device, just replace your existing router device with the ER-X router.
   b) If you modem and router are combined into one physical device, disable the router/firewall portion and effectively change the device into being only a modem. Some consumer "combo" devices allow disabling the firewall portion / some don't allow the firewall to be disabled.

   Disabling the firewall portion typically provides the ER-X's WAN interface with either a public IP address, or some form of carrier-grade-NAT address, per your ISP's operation. These addresses are typically not in the 192.168.X.X address range.
2. Be Double-NATed. You would place your ER-X behind your existing consumer modem/*router*. People on Ubiquiti community forums *hate* being Double-NATed. If you are not running a server or playing time-critical shoot-em-up games, I don't see this as a problem.
3. You may have special ISP-provided modem-type equipment, e.g. fiber. Talk to your ISP about how to connect your ER-X to it.

79.3 Google Fiber WAN Setup

I was asked to add a reference within this guide, for configuring the ER-X for Google Fiber use. So here it is:

https://github.com/mjp66/Ubiquiti/issues/31

79.4 WAN PPPoE Settings

If your Internet Service Provider (ISP) uses PPPoE, you will need to re-configure your WAN / eth0 settings accordingly. Sometimes with PPPoE, your internet may only partially work correctly, You might want to read:

Ubiquiti Community Links:

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

https://community.ui.com/questions/Adjust-the-MSS-value-for-the-PPPOE/72dd3330-9d68-4a38-96ee-fc2ade8e4b84

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

https://community.ui.com/questions/Cant-open-some-webpages/8221b2c2-1dec-4fd5-8a02-b2557e8f817a#M163311

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

External Links:

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

79.5 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 41 - EdgeRouter Enable HW NAT Assist. I think that if you only enable QOS on the WAN port, that HW acceleration will stay enabled.

You should be able to find various speed-testing web sites on the internet:

https://www.speedtest.net/
https://fast.com/
https://www.speedcheck.org/
https://www.spectrum.com/internet/speed-test

If you enable SmartQue on eth0, you should re-visit these settings, if your ISP speed(s) change.

To enable SmartQueue, press the QoS button, located near the top of the page. See Figure 153 – QoS button.

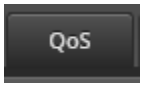


Figure 153 – QoS button

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 postings / indications that you should only implement SmartQueue in the Upload direction.

To enable upload 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 other settings.

See Figure 154 – SmartQueue Settings,

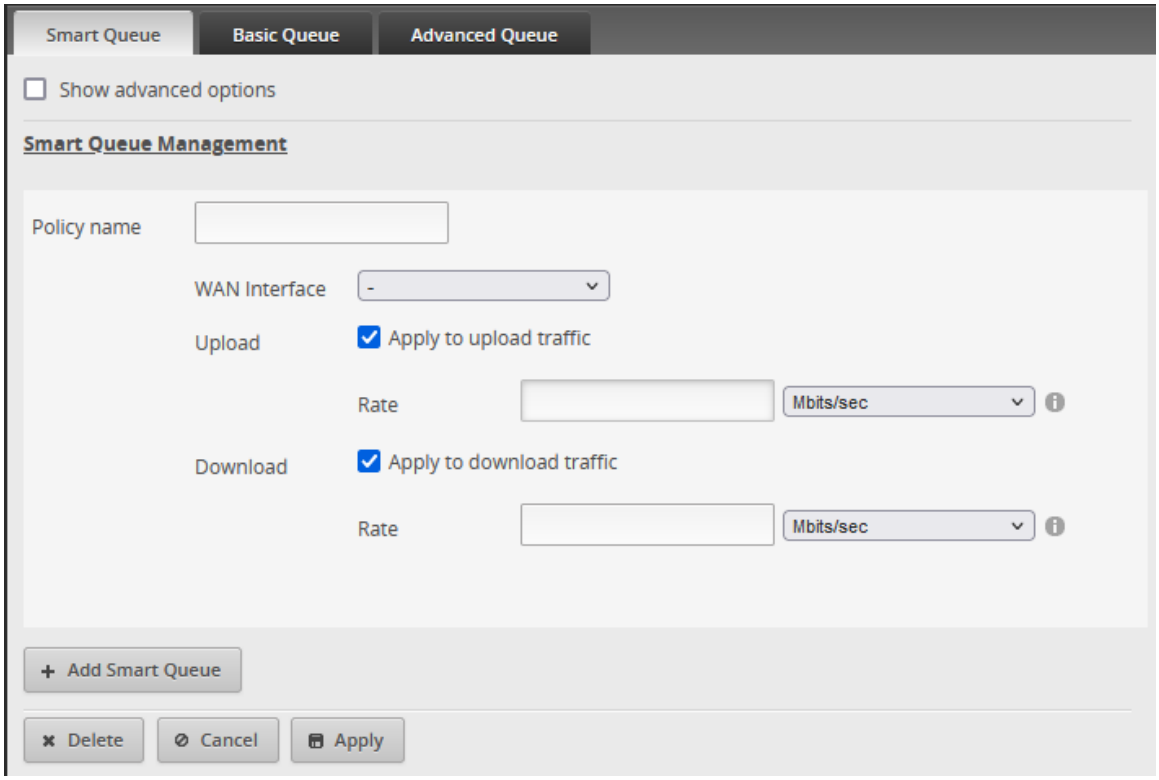


Figure 154 – SmartQueue Settings

References:

QC Ubiquiti EdgeMAX - Basic Smart Queue Quality of Service (QoS)

https://www.youtube.com/watch?v=8NGlzMGd_IA

Ubiquiti Quality of Service help page

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 (now web archived):

http://web.archive.org/web/20210516092055/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

80. Configuring a Second / Testing ER-X - Part2

Once you have deployed the ER-X as your master router, you cannot just connect another ER-X behind it, as the addresses used within the master ER-X will conflict with the (same) addresses used within the second/testing ER-X. These address groups were listed in Table 2 – Network Details on page 42.

That is because the WAN port would be DHCP assigned and be using (one of) the same address sets as one of the testing ER-X's address set. The testing ER-X would get confused, because (with overlapping address sets), it would not know where to route those (overlapping) addresses to.

Example: If you connected the testing ER-X's eth0 (WAN) port into the master ER-X's eth3 (HomeNet), then the testing ER-X would have a 192.168.3.X address assigned to its eth0 interface. Now the WAN address overlaps with the testing ER-X's HomeNet address range. The testing ER-X would now know which port (WAN or HomeNet) to route 192.168.3.X addresses to.

Normally your Setup/Testing PC would be wired directly (or through a switch) to your "Master" ER-X. See Figure 155 – Typical Testing PC Setup.

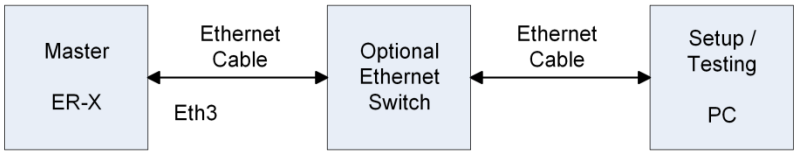


Figure 155 – Typical Testing PC Setup

One way of presenting a different IP address to the testing ER-X, is to insert your leftover consumer router (with its LAN configured for 192.168.[0,1,2].X) before your testing ER-X router. The testing ER-X then connects to your Setup/Testing PC. See Figure 156 – Second ER-X Setup - Late.

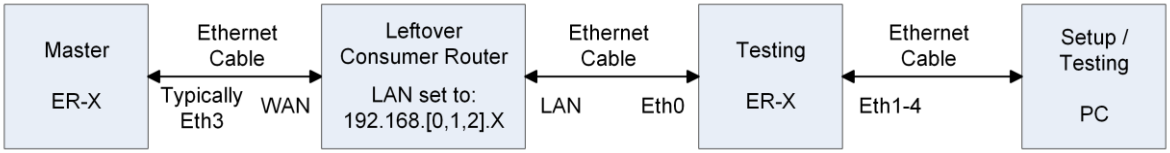


Figure 156 – Second ER-X Setup - Late

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-c2c30b35969a

With this method, you would first need to make a backup of your current/deployed/master ER-X's configuration, and then *temporarily* modify your master ER-X to allocate a different address range to the Wired Separate Network port. Maybe use the RFC-5737 address range of 192.0.2.0/24. You may also need to change the interface address (eth2) on the dashboard page to match the DHCP address set.

You would then connect your second/new/testing ER-X's eth0/WAN port into the master ER-X's eth2/Wired-Separate-Network port using a standard Ethernet cable. When your testing ER-X is fully configured, (remember that backup you just made?), you would then disconnect the testing ER-X and restore the previous address range to the master ER-X's Wired-Separate-Network port.

81. End of ER-X EdgeRouter Setup

This is the end of the ER-X / EdgeRouter setup.

82. Ubiquiti Access Point (UAP) Setup

Ubiquiti Access Point(s) provide the WiFi portion to your installation.

To configure Your Ubiquiti Access Point(s) you will need to install and run Ubiquiti's UniFi (controller) software. This free software runs on Windows, Mac, Linux, iPhone, and Android. I have heard that the phone Apps are rather limited, and may not have enough features for use here.

This software **only** needs to be running when you are adopting or making configuration changes to your Access Point(s). The software *can* run all the time if you want to use the optional guest portal OR use the system-monitoring / data-collection features. The guest portal might be found in a Motel / Hotel WiFi system. System monitoring / data collection might be used in WiFi equipped office spaces or within a school installation.

I would **never** install this software on either a non-dedicated PC or on a Windows PC, because it requires buggy Java. Ubiquiti makes dedicated device(s) which can run this software. Cloud-Key Generation 1 and Cloud-keys Generation 2 are two older examples. If you are very cost sensitive, loading UniFi software on your existing PC is free.

For previous installations, I purchased a Cloud-Key (now named Generation 1) and used it for years. That Cloud-key is no-longer under active support. I only powered-up the Cloud-Key when making UAP changes. It is important that power is not cut unexpectedly to UniFi Controllers, as some internal database can get corrupted, and then your controller will not boot. So make a backup file *every* time you change your configuration.

I have been operating the UniFi Controller software on a Raspberry Pi for several years, and have had it running continuously for over a year. This type of installation uses only a few watts of power. Since the UniFi Software does not need to be run continuously, you can repurpose your (hard to find) Raspberry Pi, if you need to.

The entire/following Unifi installation-directions, were written when the Unifi software version was 7.3.76, and the UAP firmware versions were (for most models) at 6.2.49. The 6.2.49 firmware seems stable for my installation.

Ubiquiti Release Notes (including links to installable(s) / executables):

> https://community.ui.com/releases/UniFi-Network-Application-7-3-76/85c75fc7-3e0f-4e99-aa90-7068af4f1141

Other releases have similar pages.

If you are *not* going to be using a Raspberry Pi, you might look at the following links:

> https://lawrencesystems.com/self-hosted-unifi-network-application-controller-install-tutorial/
>
> https://help.ui.com/hc/en-us/articles/4416276882327-How-to-Set-Up-UniFi
>
> https://help.ui.com/hc/en-us/articles/220066768-Updating-Self-Hosted-UniFi-Network-Servers-Linux-
>
> https://help.ui.com/hc/en-us/articles/205144550-Self-Hosted-UniFi-Network-Server-as-a-Windows-Service-Advanced-
>
> https://help.ui.com/hc/en-us/articles/220066768-UniFi-How-to-Install-and-Update-via-APT-on-Debian-or-Ubuntu
>
> https://lawrencesystems.com/unifi-network-application-7-3-76-changes-and-review/
>
> https://github.com/lawrencesystems/youtubedemos
>
> https://www.youtube.com/watch?v=lkUhWnDPutg

For legacy UniFi directions, see a legacy revision of this guide. Reference section 4 - Guide Revisions on page 8 for how to access Legacy revisions of this guide.

Many of the UniFi settings are customizable, some catastrophically. Many settings I know nothing about, so I assume that Ubiquiti knows what it is doing (not exactly true) and therefore I just accept the defaults for most settings.

After the initial UniFi setup, there are later sections of the guide which contain Community postings about many of these settings. I've tried to provide cross referencing section-links between the install sections and the discussion sections, in each direction.

Ubiquiti Help Links:

https://help.ui.com/hc/en-us/categories/6583256751383-UniFi

https://help.ui.com/hc/en-us/categories/6583256751383-UniFi

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/360006634094

https://help.ui.com/hc/en-us/articles/204910064

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

82.1 UniFi-Controller-Software Upgrade/Downgrade.

Newer U6 UAP models are only supported by recent versions of UniFi Controller software. Obviously, older versions of UniFi controller software were written before the U6 family of UAPs were even invented.

If you generate a UniFi backup file, that backup file is not compatible with earlier versions of the UniFi Controller software. Ubiquiti will load an earlier-version of backup file into a later version of UniFi controller software. This is how you can update an existing installation, to a newer UniFi controller software version.

UniFi controller backup files are binary data, so unlike the ER-X's human-readable backup file, only Ubiquiti knows what each bit / byte of a specific version of a backup file does.

When upgrading UniFi controller software, it is important to preserve your current UniFi controller version's backup files, in case the new controller version has critical bugs which impact your installation. If this disaster happens to you, you would need to re-install the original UniFi controller software version and then re-load your original backup file, as any backup files generated by the newer controller version would not be compatible with your original controller version.

If you use a Raspberry Pi to run your controller software, invest in another / new SD card for running a new version of controller software. Programs are available which will "clone" an SD card to another SD card. Then you can upgrade the cloned card, keeping the original as a backup SD card. You should still keep plenty of backup files.

If you find that your existing UniFi controller software version is working for you, don't be too hasty to update it because a new one has a larger version number. Read the release notes looking for community acceptance / rejection, unless you are looking for a specific fix which already impacts your installation.

82.2 System Stability

@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.

Ubiquiti has a horrible track record of releasing alpha or beta firmware labeled as stable firmware.
One of the hardest objectives about this Ubiquiti configuration is acquiring stable UAP firmware.

@BuckeyeNet
> @joshv918 wrote:
> … updated both devices and they didn't work.
> I was hoping for the newest 4.3.20 magic firmware solution.
> I'm about to go trying one by one rolling back

Does anyone maintain a "UAP Model"/firmware matrix with "ratings" for the firmware. Some firmware turns out to be good and stable, others not nearly as stable. And there may also be some requirements for specific versions of UniFi controller versions as well. Something to let casual users that just want to run a stable version and skip the ones with the problems.
https://community.ui.com/questions/Wifi-Issues-with-Wifi-Devices-Unifi-AP-Firmware/89440a06-170e-41c5-94de-47ea017a9355#answer/7630915f-45b9-4c22-b914-79d874cc6aba

@mjp66 <Reply>
I'd think we would all like to know what firmware is stable, and this includes Ubiquiti's own Software Engineers They should know.
A couple of years ago EdgeRouters went through a horrible string of bad firmware updates, lasting more than a year long. Beta to Release in a day or so, even though the forum was screaming Crashes / Bugs / Dont-do-it. Some "features" introduced via these series of updates will never be fixed.
Unifi software (at least for APs) still seems to be having "the same" stability issues, but just not quite as bad as the EdgeRouter example. AP instability seems (to me) to have been going on for longer. I've been part of this community for about 5 years.
Just look at the amount of daily postings within (this) Unifi-Wireless group. Most of them begging for help. Even after many months, there still seems to be excessive U6-LR instability, just as one AP example. I bought a U6-LR and it had to be disconnected for much of its life, at my residence.
But this is enough ranting for one posting.
I'm still "using", still just-holding-on, and still optimistically (also) searching for the next 4.3.20 magic solution.
https://community.ui.com/questions/Wifi-Issues-with-Wifi-Devices-Unifi-AP-Firmware/89440a06-170e-41c5-94de-47ea017a9355#answer/3fe68517-632e-4675-b01f-59a2cef0e0d5

If you find that your existing UAP firmware is working for you, don't be too hasty to update it because a new one has a larger version number. Read the release notes looking for community acceptance / rejection, unless you are looking for a specific fix which already impacts your installation.

83. Download and Install the UniFi Software

If you are using something other than a Raspberry Pi to run UniFi, install it now.

If you are installing on a Raspberry Pi, follow the indented portion, below:

The Raspberry Pi installation script, which I originally used, no longer works with freshly-updated releases of the Raspberry Pi Operating System (OS). This is per statements made, about 5/27/2023, by the script's author @SmokingCrop. That original installation information has now been placed into Appendix C - Original Unifi Installation Script for Raspberry Pi on page 253.

The installation *did* operate correctly (early in 2023) during the writing of the Second Edition. I successfully *recreated* this installation in June of 2023, by using a now-earlier revision of the Raspberry Pi OS. Details are contained in that Appendix.

This is the suggested replacement script:

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

You will want to check the above web posting and check for any updated information and/or new UniFi supported releases. Following links on that page, I downloaded the following scripts (adjust versions to your own use):

https://get.glennr.nl/unifi/install/unifi-7.3.76.sh
https://get.glennr.nl/unifi/install/unifi-7.4.156.sh

When I tested this installation script, I choose 7.4.156, which was the newest release available, when this section was updated. Installation required using a 64-bit version of the Raspberry Pi Operating System. When the installation finished, UniFi booted, and I successfully loaded my UniFi backup file. I was *unable* to get the 7.3.76 version to correctly install, using either a fresh 32-bit or a fresh 64-bit Raspberry Pi Operating System.

I did *not* investigate any UniFi changes made from 7.3.76 to 7.4.156, as this exercise was simply a test of the above installation script.

After I performed the above, I found the following links, which may be helpful:

https://community.ui.com/questions/Has-anyone-gotten-Unifi-7-4-to-work-on-a-raspberry-pi-running-64-bit-Buster/228a42b9-1158-4d73-a007-e5b9db5c7fa2

https://community.ui.com/questions/Unifi-Network-Application-Raspberry-PI-Migration-32-greater-64-bit-Walkthrough/f7eaaaaf-782a-45ad-9747-c18570577456

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

I chose to change the hostname of my Raspberry Pi to `UniFiPi`. I performed this via `Preferences -> Raspberry Pi Configuration`.

I also enabled VNC and SSH for remote access. I performed this via
`Preferences -> Raspberry Pi Configuration`.
If you do this, a monitor is no-longer required. Within this configuration tool is a "Headless Resolution" setting under "Display" that might be useful for VNC use.

To shutdown UniFi which is being hosted on a Raspberry Pi, I use the terminal command: `poweroff`

For all UniFi Controllers:

Connect you UniFi Controller to the Home Network with an Ethernet cable. If you don't know your UniFi Controller's IP address, find it by following section 67 - Find a Device's IP Address on page 134.

Reserve your UniFi Controller's IP address to `192.168.3.4` by following section 68 - Reserving Device Addresses via DHCP on page 135 and following Table 4 - Reserved Address on page 135.

The UniFi Controller does not like to have power abruptly removed. You should attempt to gracefully shutdown or reboot your UniFi Controller when needed.

84. Hookup your Ubiquiti Access Point(s)

There are a lot of variables for this section:

- Each Ubiquiti Access Point (UAP) needs Power Over Ethernet (POE).
- Each UAP model has specific POE requirements.
- Do not connect non-UAP equipment to a POE output port, especially with older/ passive POE adapters. This includes enabling the POE output on the ER-X's eth4 port.
- You might be using separate POE power adapters or you might be using a POE network switch.
- Using a POE+ power source will not hurt a (regular) POE UAP.
- If you are using a POE/POE+ Network Switch, be mindful of the switch's overall power budget and that some UAPs require POE+.

Reference the following sections:

8.2 - Ubiquiti Access Point Models on page 14
78.2 - Comments about Network Switches on page 155
78.3 - About Using Two or More Ubiquiti Access Points on page 156

WARNING: Connecting a POE port to any Non-UAP device will likely burn-up that Non-UAP device.

If you don't know your UAP(s) IP address(es), find it / them by following section 67 - Find a Device's IP Address on page 134. Reserve your UAP's IP address(es) by following section 68 - Reserving Device Addresses via DHCP on page 135 and following Table 4 - Reserved Address on page 135.

84.1 Trouble Shooting UAPs

Understanding Device LED Status Indicators:

https://help.ui.com/hc/en-us/articles/204910134-UniFi-Network-Understanding-Device-LED-Status-Indicators

Reset Devices to Factory Defaults:

https://help.ui.com/hc/en-us/articles/205143490-UniFi-How-to-Reset-Devices-to-Factory-Defaults

See the following figures:

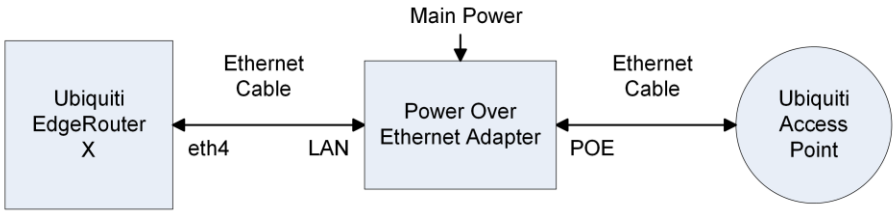


Figure 157 – Ubiquiti Access Point Wiring – Single

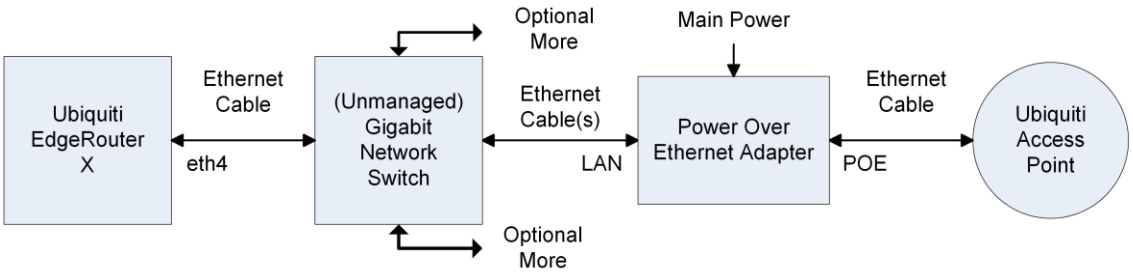


Figure 158 – Ubiquiti Access Point Wiring – Multiple

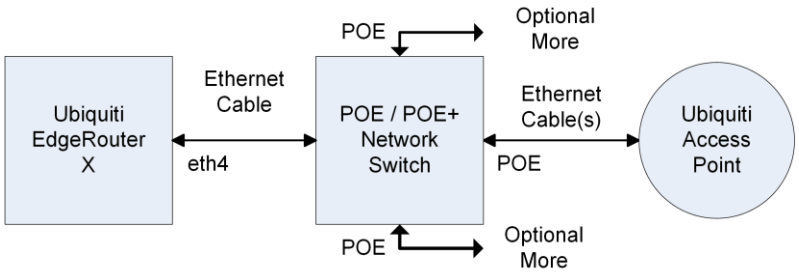


Figure 159 – Ubiquiti Access Point Wiring – POE Switch

85. Initial Setup of the UniFi Software

If you are running UniFi on a Raspberry Pi, you do not want to access the UniFi Software (using a browser) *on* the Raspberry Pi; access UniFi by running the browser *on* your Setup Computer. A typical Raspberry Pi may not have enough memory to support both the UniFi Software and a browser at the same time.

The following **UniFi installation sections** were written when UniFi was at version **7.3.76**

Unifi version 7.3.76 supports both a New Interface and a Legacy Interface, but supports them both badly.

One of the reasons for showing full screenshots of UniFi's pages within this guide is that the developers of UniFi software seem to change the UniFi Controller software with wild abandon. When this guide was re-written, there are items you can only change while in the New Interface, and other items which can only be modified, while using the Legacy interface. Full screenshots may help future users of this guide find some of these settings, if they are again moved around.

After your UAPs are setup (at the competition of this guide) you should be able to switch to whichever interface you prefer.

To start the UniFi Software, open a browser on your Setup Computer and enter the following URL:

`https://192.168.3.4:8443`

If you get a Browser Warning like Figure 5 – Browser Security Certificate Example on page 27, click past it.

You should see the first of six setup pages. See Figure 160 – UniFi Step 1 of 6.

(If you are restoring from backup, including updating to a newer UniFi Controller software version from an earlier controller version, and already have a backup file, then click the "restore" link.)

Choose an installation / application name, and do what you need to do for the checkbox. Press Next.

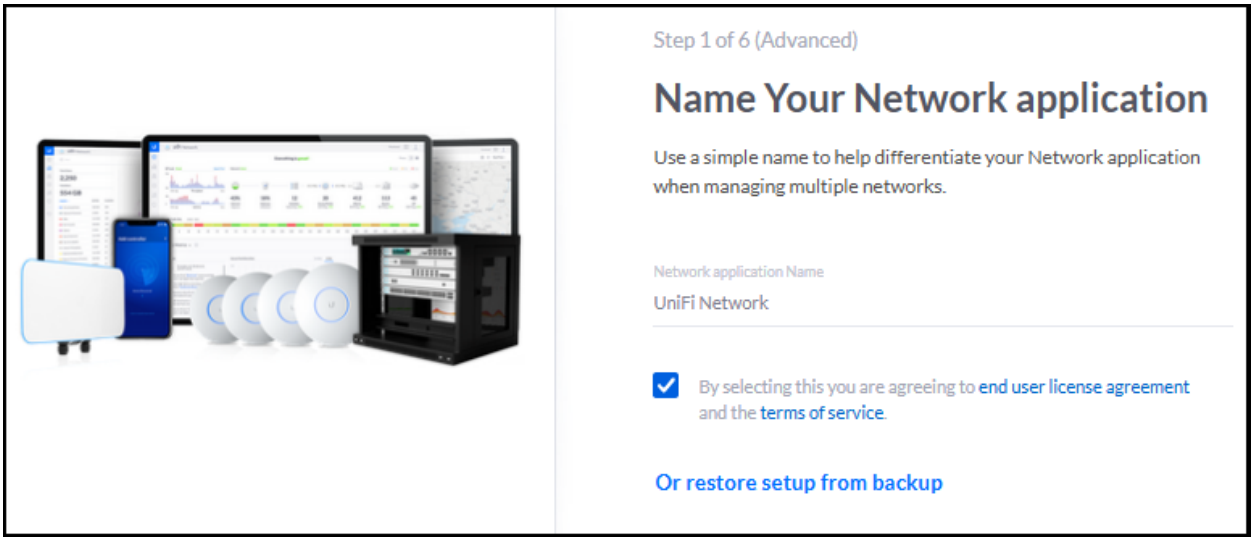


Figure 160 – UniFi Step 1 of 6

If you want to login using a Ubiquiti account, you can just fill in the Username and Password. See Figure 161 – UniFi Step 2 of 6. I did not want to do this, so I instead clicked on" Switch to Advanced Setup".

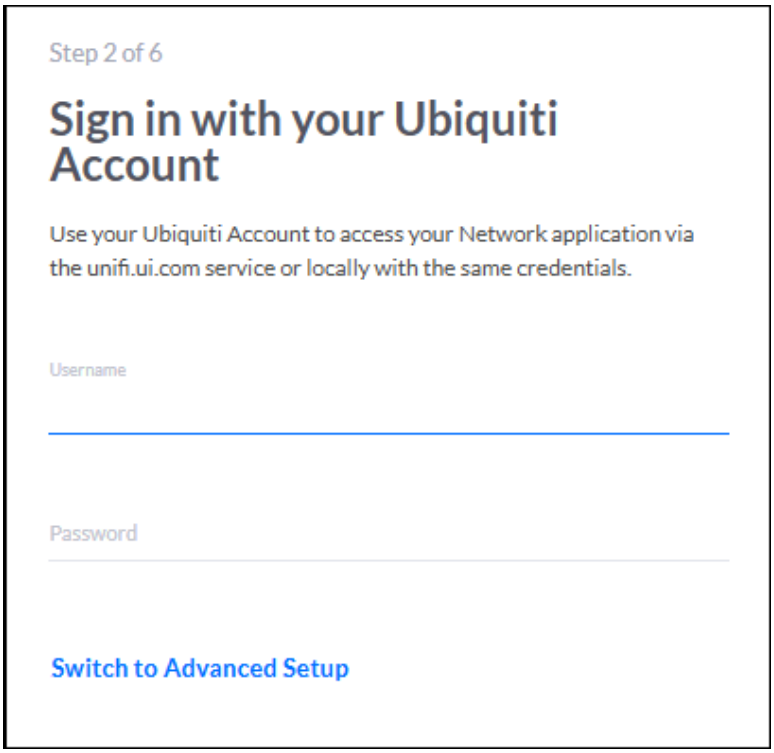


Figure 161 – UniFi Step 2 of 6

See Figure 162 – UniFi Step 2 of 6 - Advanced Setup.

I disabled “Enable Remote Access” and disabled “Use your Ubiquiti account for local access”.

I entered data for the following fields:

- Local Administrator Username
- Local Administrator Password
- Confirm Password
- Local Administrator Email.

You will want to safely store those credentials.

Press Next.

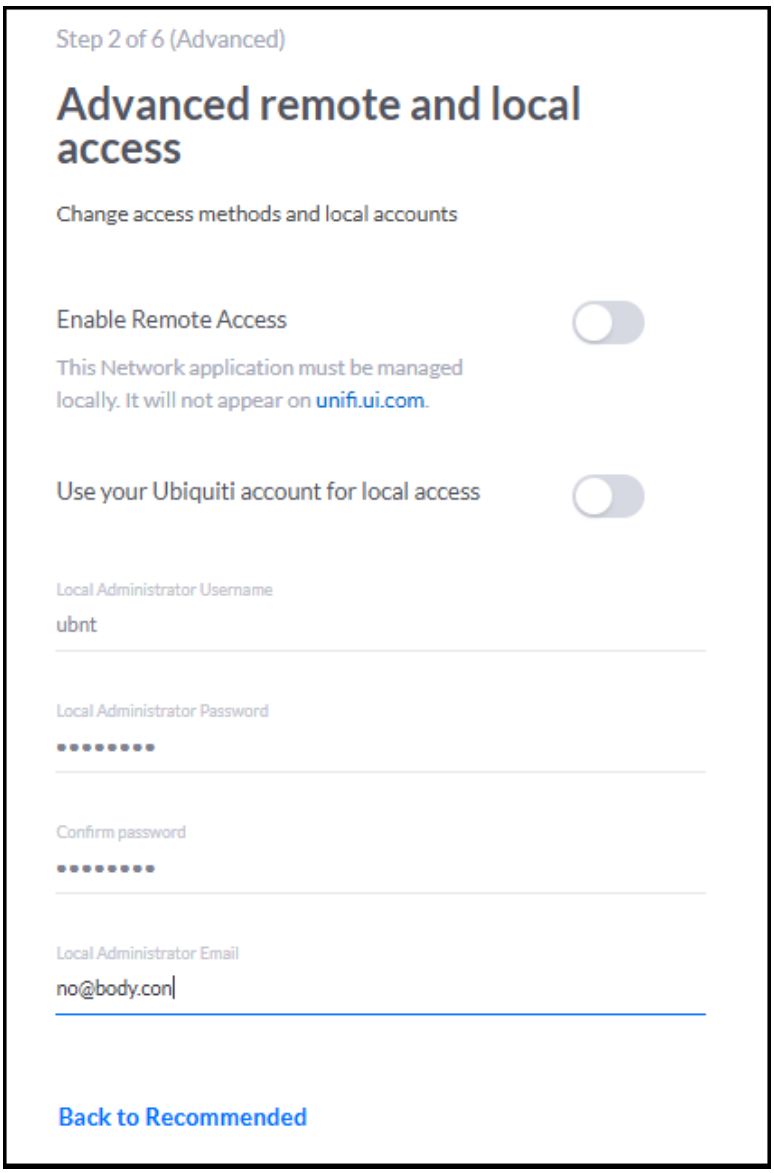


Figure 162 – UniFi Step 2 of 6 - Advanced Setup

I enabled Enable Auto backup. See Figure 163 – UniFi Step 3 of 6.

Press Next.

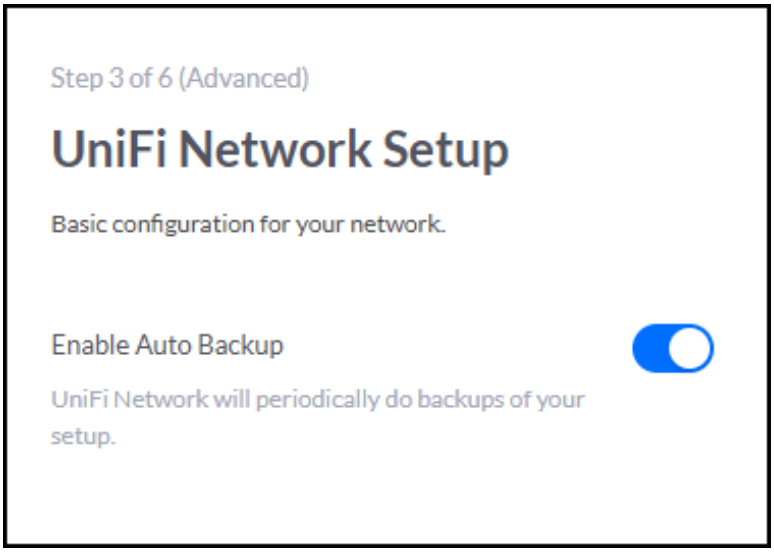


Figure 163 – UniFi Step 3 of 6

The Unifi Controller, found my (single / used-for-testing) UAP, which was on my Home Network waiting for setup.

If (all of) your UAP(s) are not found, you may have to factory reset them. You can hold-down the reset button, for about 15 seconds, with a paperclip or equivalent. Reference section 84.1 - Trouble Shooting UAPs on page 178

Check the appropriate boxes to enable your UAP(s). See Figure 164 – UniFi Step 4 of 6.

Press Next.

Figure 164 – UniFi Step 4 of 6

You should see the dialog shown on Figure 165 – UniFi Step 5 of 6. Enter the following data:

Under WiFi Name `<Your HomeNet WiFi SSID>`

Under WiFi Password `<Your HomeNet WiFi Password>`

Combine 2GHz and 5GHz WiFi Network Names into one `Enable`

Press Next.

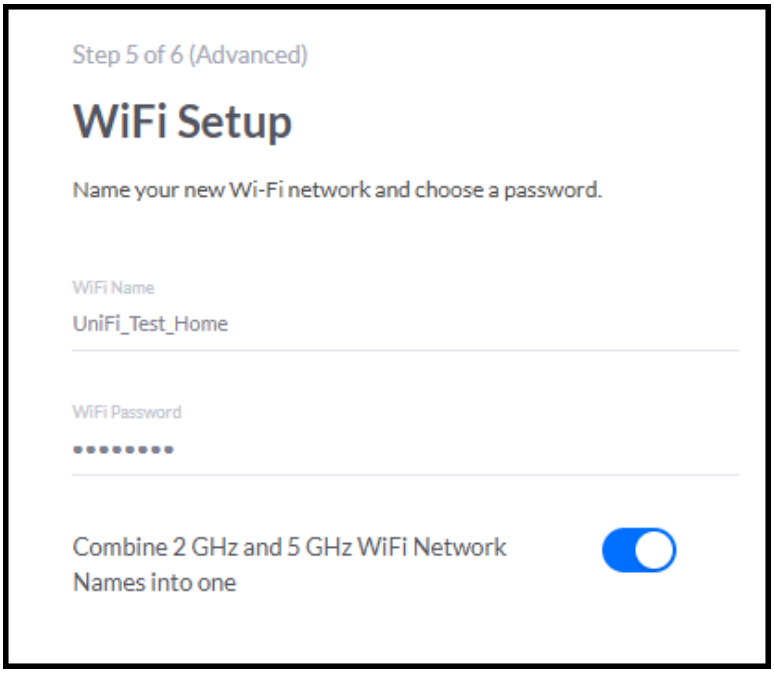


Figure 165 – UniFi Step 5 of 6

You are then asked to confirm the above information. If it is correct, press Finish, else go "Back". See Figure 166 – UniFi Step 6 of 6.

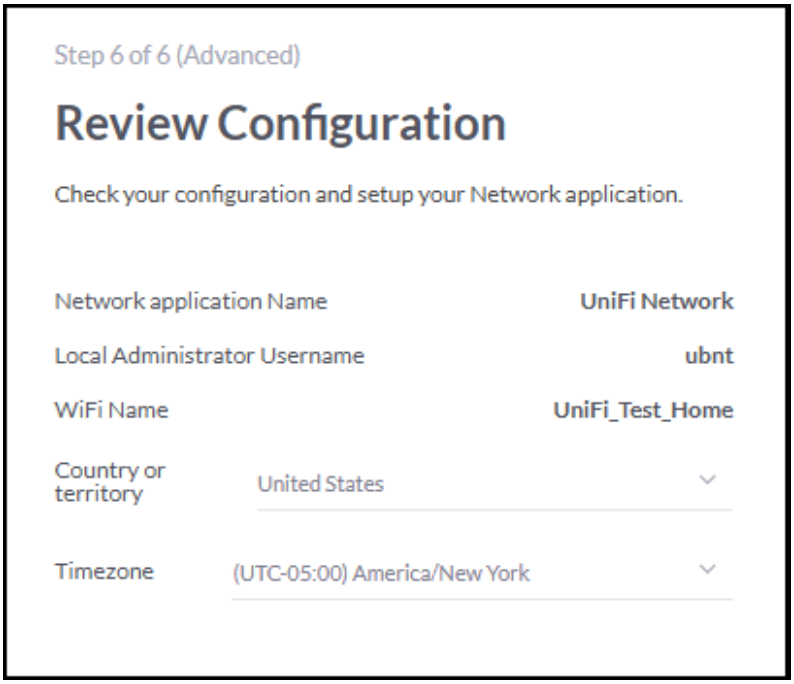


Figure 166 – UniFi Step 6 of 6

The system will then take a few moments to configure itself. See Figure 167 – Configuring UniFi.

Figure 167 – Configuring UniFi

You will then land on the Dashboard page. See Figure 168 – UniFi Dashboard Page – New Interface.

Using the SSID and associated Password, you should be able to connect a WiFi device to your Access Point. This device will appear on the HomeNet, as that is the only WiFi Network which has been setup. The device's IP address should be in the 192.168.3.X range.

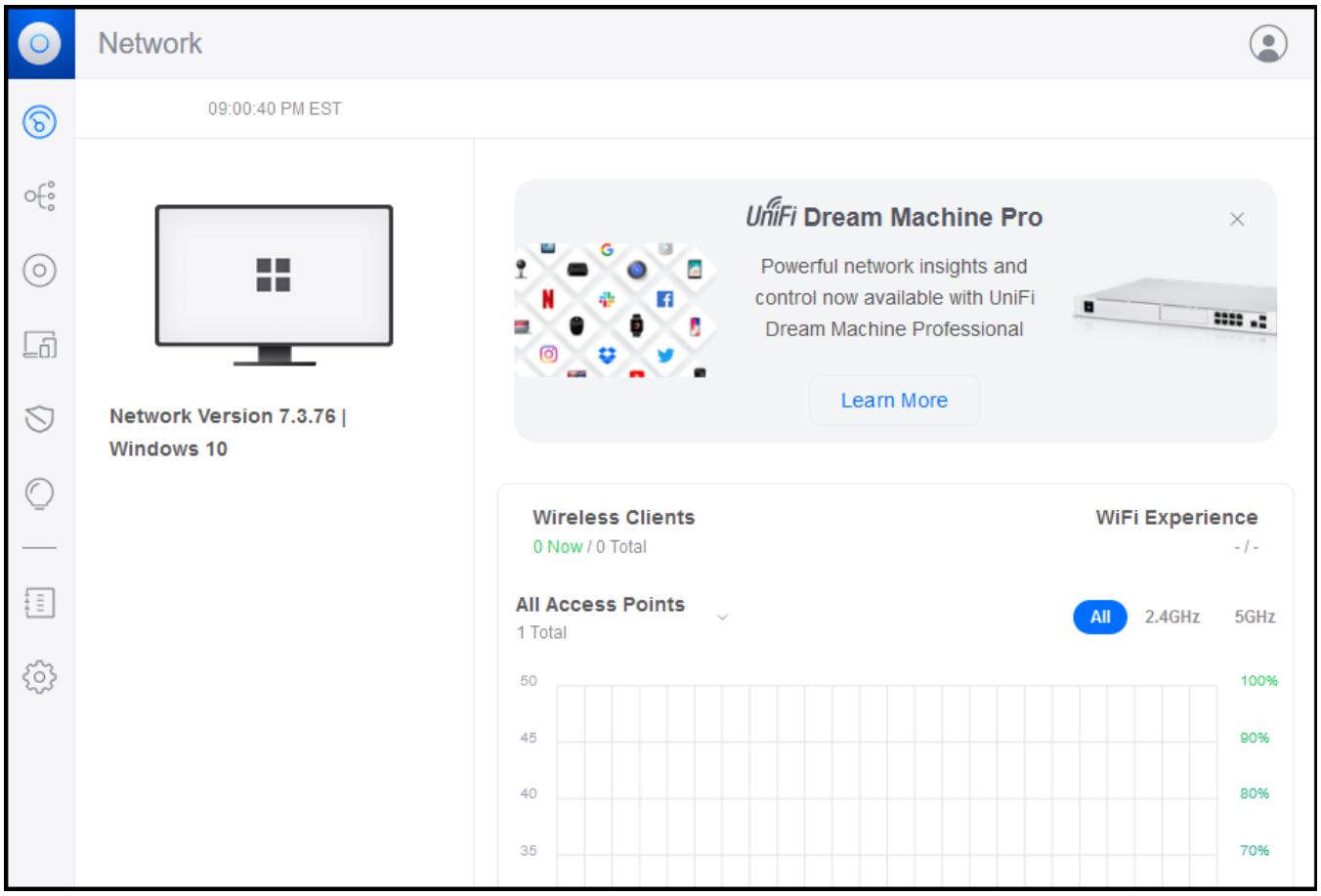


Figure 168 – UniFi Dashboard Page – New Interface

Before you get too invested in this installation, I suggest you click on the person icon in the upper right, and then select Sign Out. See Figure 169 – UniFi Sign Out. This will ensure you can actually log back in.

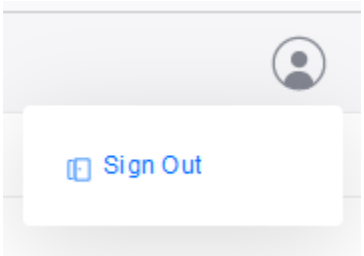


Figure 169 – UniFi Sign Out

86. UniFi Software

86.1 Login to Unifi

From your Setup Computer, open a new window / tab on your browser.
Enter the address https://192.168.3.4:8443 and Login to the UniFi Software. See Figure 170 – UniFi Login Screen.
Use your newly created credentials that were entered at Figure 162 – UniFi Step 2 of 6 - Advanced Setup.

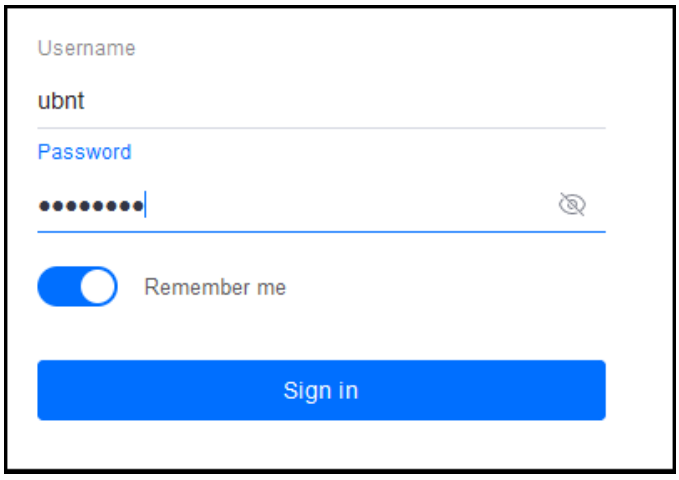


Figure 170 – UniFi Login Screen

86.2 UniFi Navigation Bar

Across the left side of the screen are icon / buttons which form the Navigation Bar. See Figure 171 – UniFi Navigation Bar. Click on "Settings", you should see Figure 172 – Setting's Sub-Menu - New.

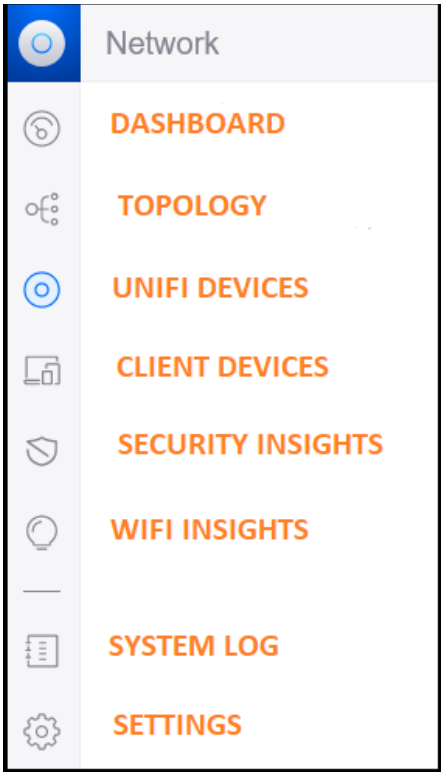


Figure 171 – UniFi Navigation Bar

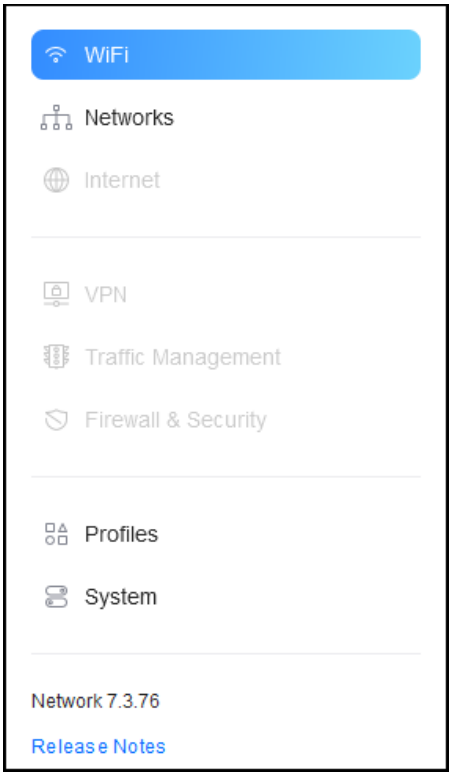


Figure 172 – Setting's Sub-Menu - New

86.3 UniFi System Page – New Interface.

To configure UniFi to work with an external / foreign-to-unifi-product-line router (our ER-X) we need to switch to a Legacy UniFi interface. To do that, click System. You will see the new interface's system page as shown in Figure 173 – UniFi System Page – New Interface. On the bottom half of the page are expandable (Show More) menu items.

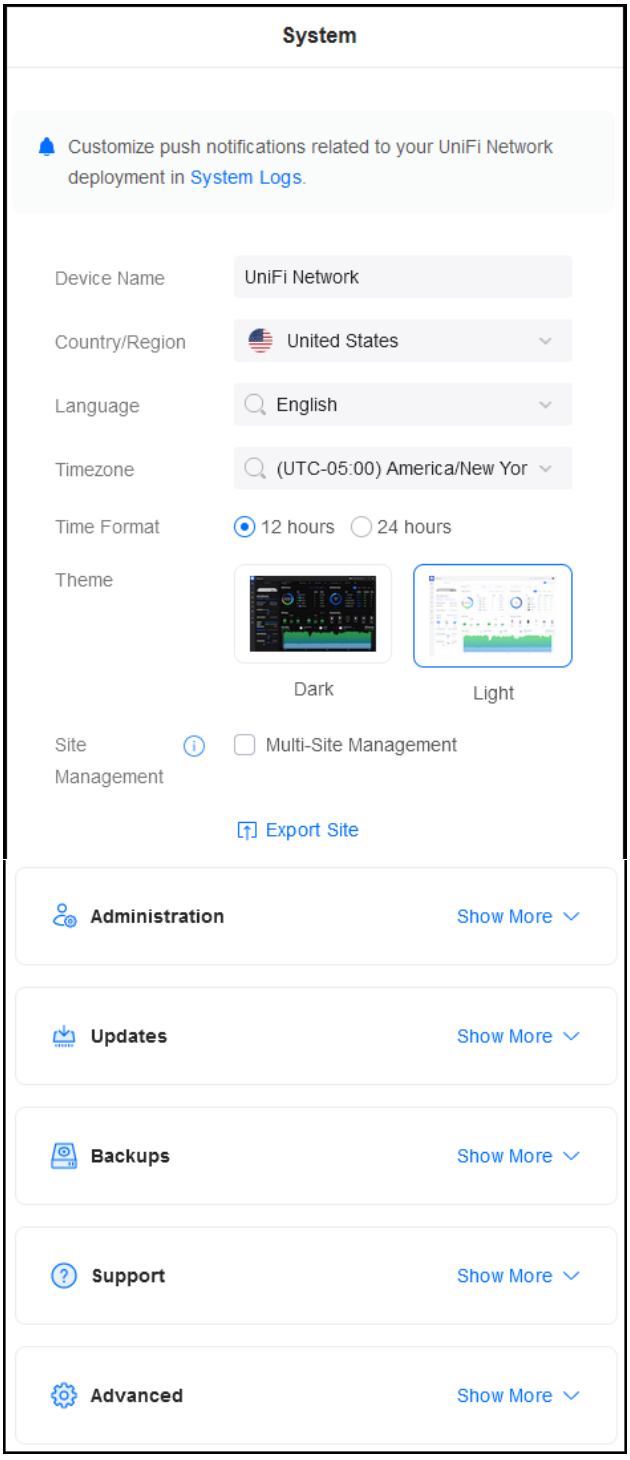


Figure 173 – UniFi System Page – New Interface

86.4 Switch to Legacy Interface

Click “Show More” on the right side of “Advanced” and find the Interface setting. See Figure 174 – UniFi Interface Setting - New.

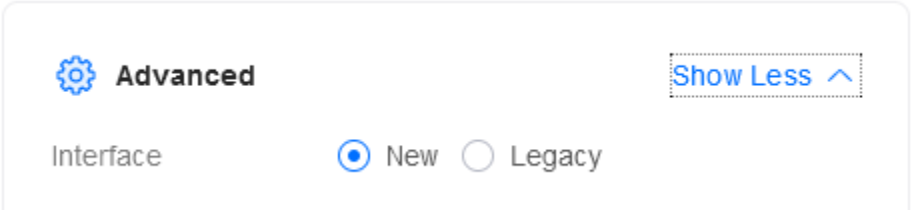


Figure 174 – UniFi Interface Setting - New

Click on “Legacy”. You will be presented with a warning dialog. See Figure 175 – UniFi Interface Setting - Warning Click “Deactivate”.

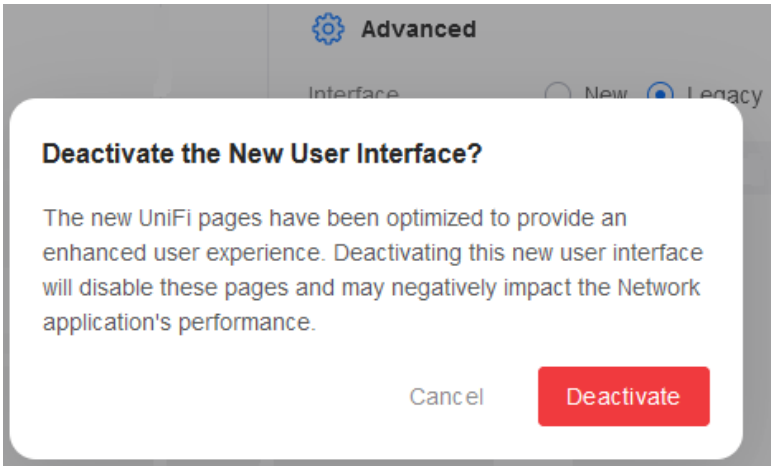


Figure 175 – UniFi Interface Setting - Warning

When switching interfaces, I sometimes saw Figure 176 – UniFi Data Collection Screen, and sometimes I did not see it. Click as you see fit. I clicked Don’t Send.

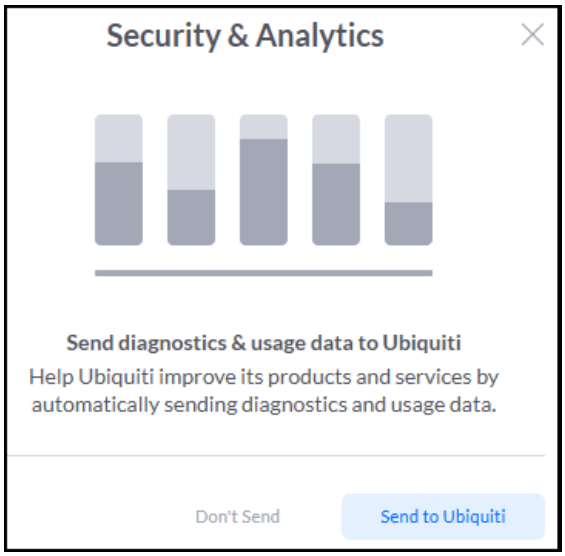


Figure 176 – UniFi Data Collection Screen

86.5 Dashboard Page - Legacy

You should land on a page as shown in Figure 177 – UniFi Dashboard Page - Legacy. This page is completely different than the New Dashboard page; reference Figure 168 – UniFi Dashboard Page – New Interface on page 186. By the way, your Unifi UAPs could be broken or actually on fire, and this interface will still say "Everything is Great!".

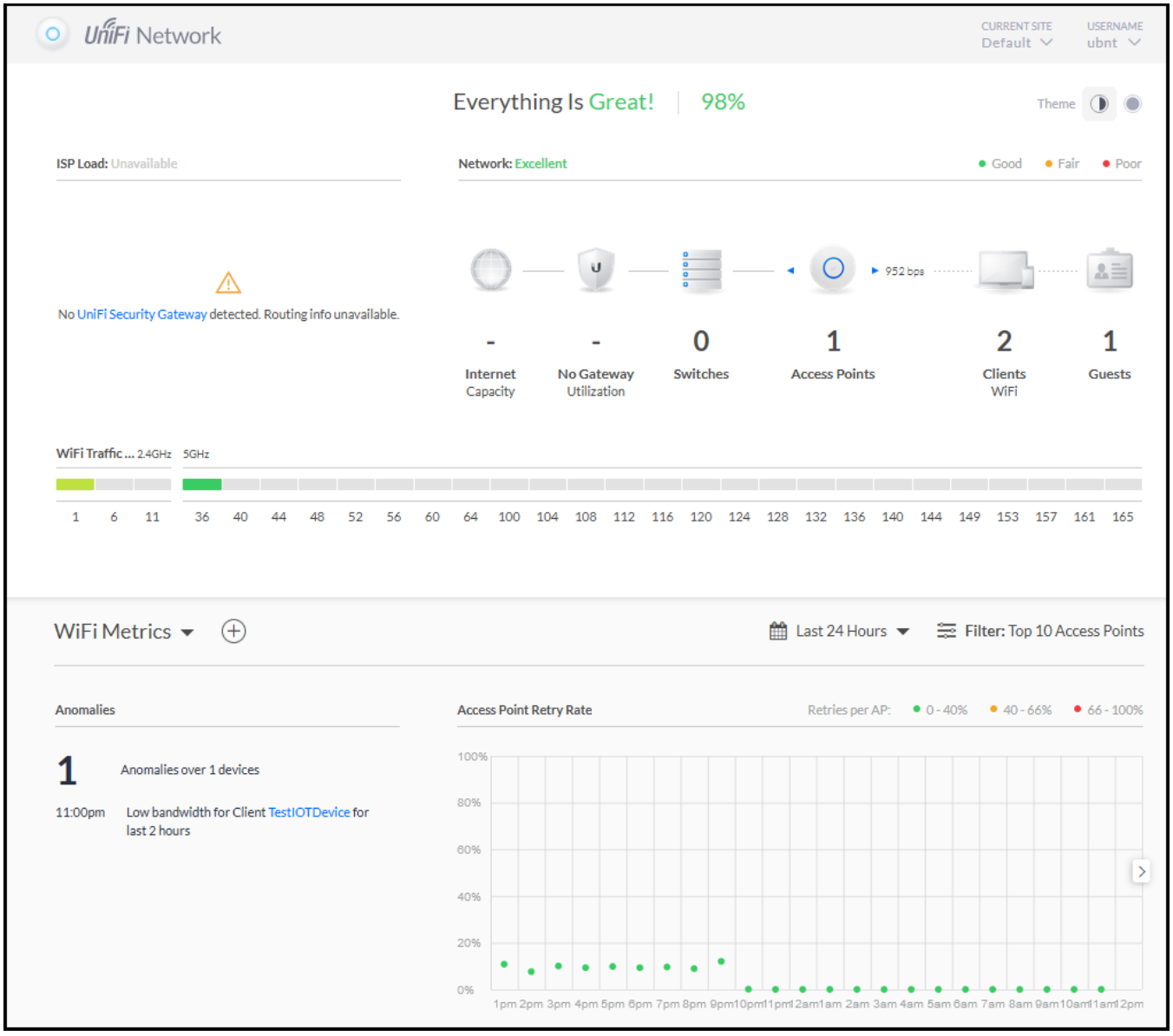


Figure 177 – UniFi Dashboard Page - Legacy

86.6 Settings Sub-Menu

Click on the Navigation Bar's "Settings" button. Reference Figure 171 – UniFi Navigation Bar on page 187.

The Legacy Settings page has a sub-menu as shown in Figure 178 – UniFi Settings –Legacy SubMenu.

Note that changing some of the settings described in the sub-menus within these tabs, will re-provision your UAP(s). Re-provisioning means that your UAP(s) will re-configure their internal settings and therefore not-be-broadcasting-WiFi-signals while this re-configuration occurs. This change usually takes about a minute or two. The word "Operational" will change to "Provisioning" on the Devices page during this. See Figure 195 – UniFi Device Page – Legacy on page 211. Maybe do your adjustments during non-critical WiFi times.

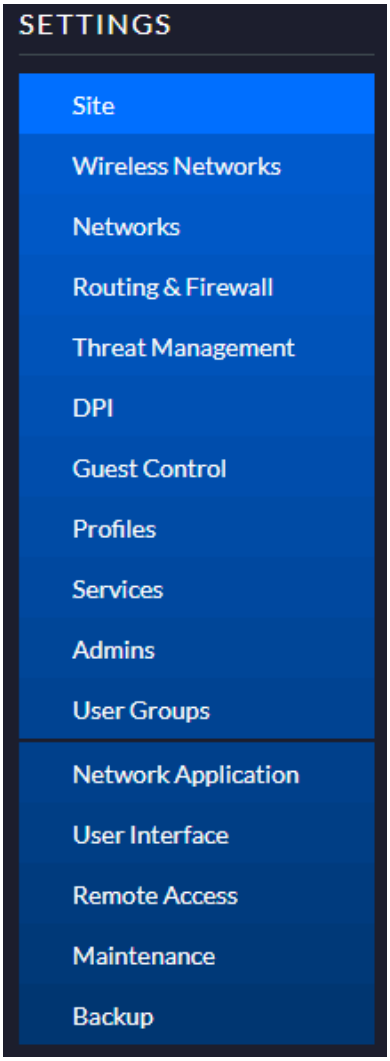


Figure 178 – UniFi Settings –Legacy SubMenu

87. Site Settings

Within the “Settings” menu, click on the “Site” tab as shown in Figure 178 – UniFi Settings –Legacy SubMenu on page 191. The following is Figure 179 – UniFi Site Page.

Figure 179 – UniFi Site Page

87.1 Site LED and Screen Settings

Within my home, I prefer to (globally) disable the UAP's LED. After a couple of years with the LED on, the LED is barely visible, even during nighttime. Turning LEDs off is, of course, to your preference.

Change / Edit the following settings within the "Led and Screen Settings" section
(Reference See Figure 179 – UniFi Site Page on page 192.):

LED / Screen	UN-`Checked`	Enable status LED / screen Authentication

Press "Apply Changes" at the bottom of the page.

87.2 Site Services

If some of you UAPs are not-Ethernet-wired (Reference section 8.3 - Mesh vs Roaming on page 16) you will need to instead `Check` "Uplink Connectivity Monitor". If all of your UAPs are Ethernet wired, leaving this enabled can create problems with your installation.

Change / Edit the following settings within the "Services" section
(Reference See Figure 179 – UniFi Site Page on page 192.):

Automatic Upgrades	UN-`Checked`	Automatically upgrade device firmware
Uplink Connectivity Monitor	UN-`Checked`	Enable wireless uplink

Press "Apply Changes" at the bottom of the page.

87.3 Site Device Authentication

If your UAP's ever get into a weird state, and won't connect to the UniFi Controller, you will want to be able to login directly into the UAP to be able to re-acquire it.

Change / Edit the following settings within the "Device Authentication" section
(Reference See Figure 179 – UniFi Site Page.):

SSH Authentication	`Checked`	Enable SSH Authentication
Username	`<Your UAP Recovery Username>`	
Password	`<Your UAP Recovery Password>`	

Press "Apply Changes" at the bottom of the page.

88. Guest Control

These settings control how the guest network operates. See Figure 180 – UniFi Guest Control - Original.

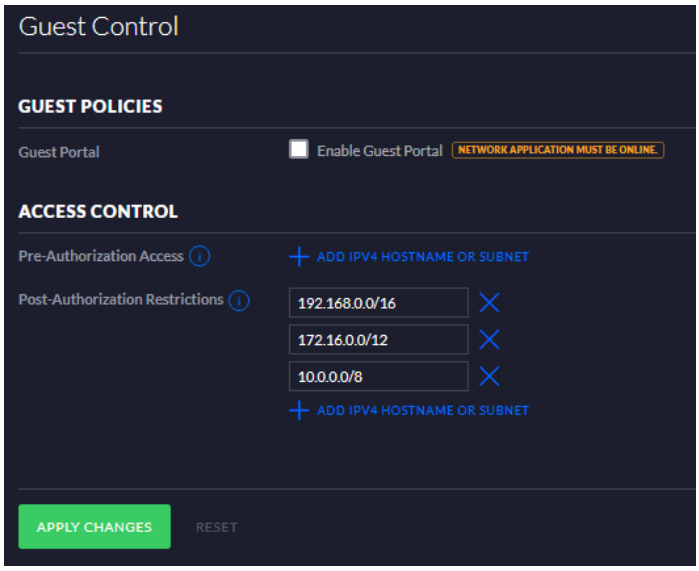


Figure 180 – UniFi Guest Control - Original

If you want to generate vouchers for guest control (like a Hotel / Motel) then you can check the "Enable Guest Portal" checkbox. If you check this, you will *need to continuously run* this UniFi Controller. I have never tried this.

For our installation, we want the GuestNet to be able to reply to traffic generated by the HomeNet. To allow these replies, click on the Pre-Authentication Access' "+ Add IPV4 Hostname for Subnet" button. In the entry field which appears, enter the text: `192.168.3.0/24`

Press "Apply Changes" at the bottom of the page. The Pre-Authentication Access line should now allow (and show) the above address range. See Figure 181 – UniFi Guest Control – Modified.

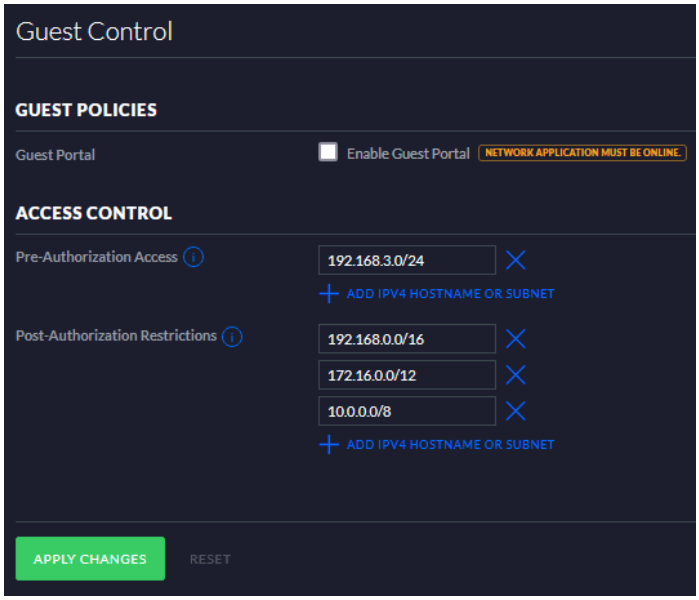


Figure 181 – UniFi Guest Control – Modified

89. Networks Settings

Data for this section is detailed within Table 2 – Network Details on page 42.

Within the “Settings” menu, click on the “Networks” tab. See Figure 182 – UniFi Networks – Initial.

The Networks section is where we inform UniFi about the details of the data being sent over the UAP’s Ethernet cable.

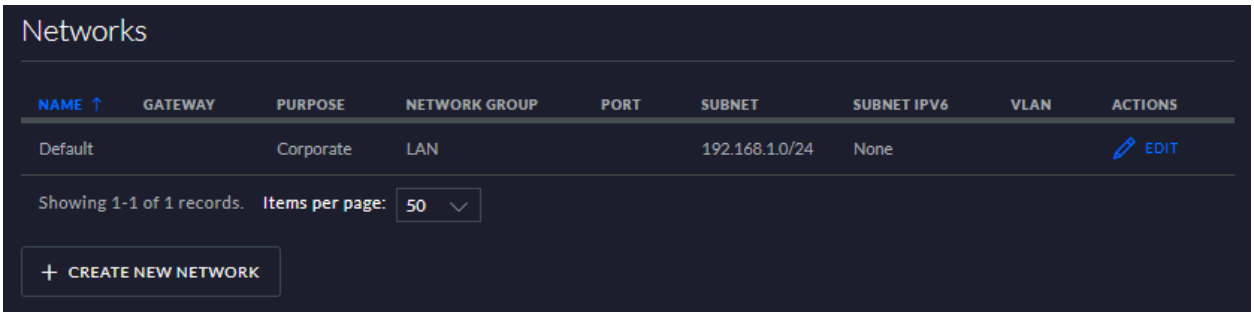


Figure 182 – UniFi Networks – Initial

89.1 Network Edit

Click on the “Edit” button, located at the right side of the “Default” line. See Figure 183 – UniFi Network Edit.

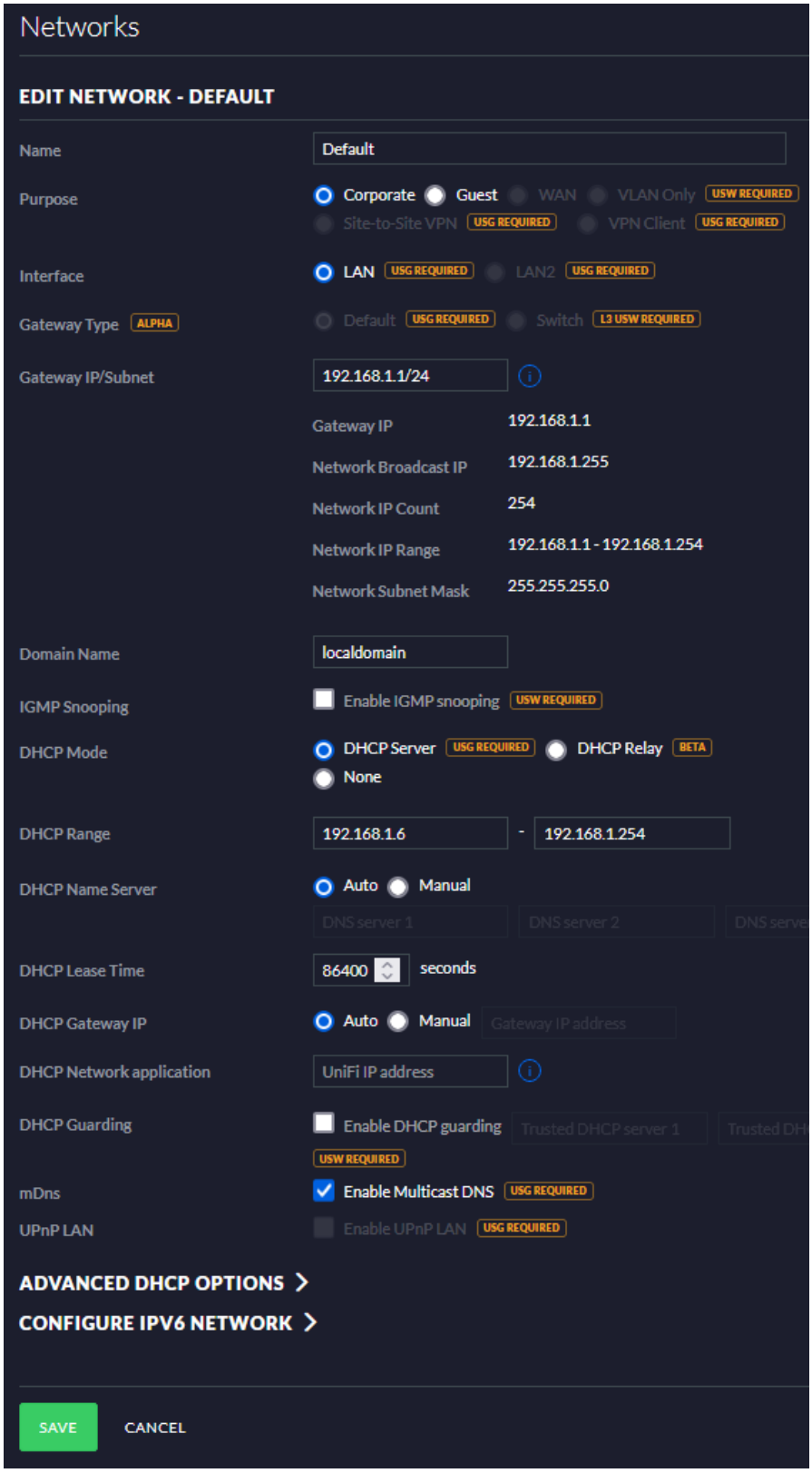


Figure 183 – UniFi Network Edit

Change / Edit the following settings on this page:

Name	`HomeNetwork`
Gateway IP/Subnet	`192.168.3.1/24`
Domain Name	`HomeNet`
DHCP Range	`192.168.3.38  192.168.3.243`

You can press the “UPDATE DHCP RANGE” button after updating the Gateway IP/Subnet, but press it before editing the DHCP range values. The above DHCP values were generated by the WAN+2LAN2 Wizard in section 15 - EdgeRouter Wizard on page36.

Press “Save” at the bottom of the page.

89.2 Create New Network

On the Networks page, press “+Create New Network”. You should see a page like Figure 184 – UniFi Network Create.

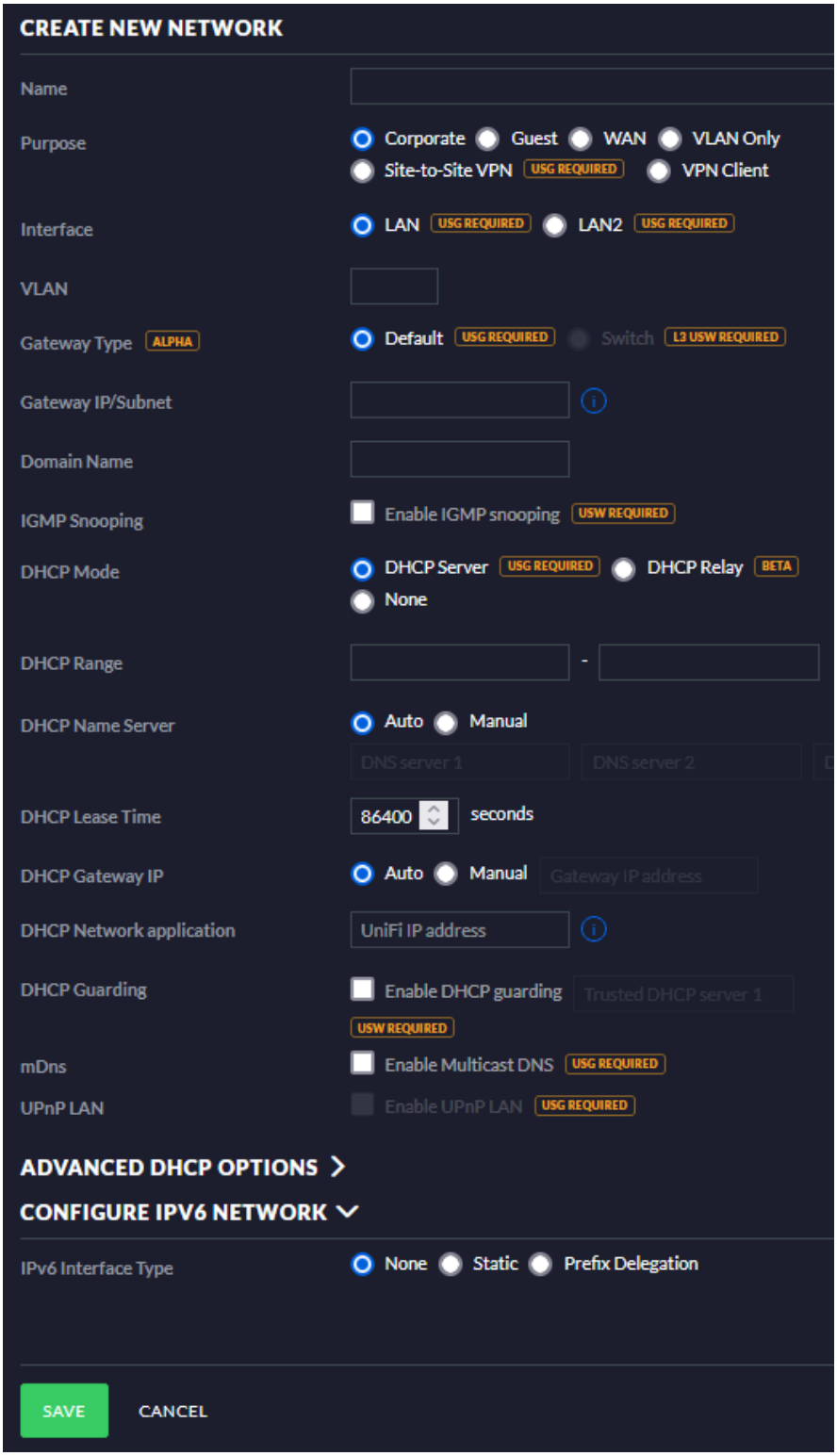


Figure 184 – UniFi Network Create

Change / Edit the following settings on this page for the Guest Network:

Name	GuestNetwork
Purpose	Guest (See section 90.3 - Create New Wifi on page 204)
VLAN	6
Gateway IP/Subnet	192.168.6.1/24
Domain Name	GuestNet
DHCP Range	192.168.6.38 192.168.6.243

You can press the “UPDATE DHCP RANGE” button after entering the Gateway IP/Subnet, but press it before editing the DHCP range values. The above DHCP values are from section 34 - Setup Remaining DHCP Servers on page 70.

Press “Save” at the bottom of the page.

On the Networks page, press “+Create New Network”.
Change / Edit the following settings on this page for the Iot Network:

Name	IotNetwork
VLAN	7
Gateway IP/Subnet	192.168.7.1/24
Domain Name	IotNet
DHCP Range	192.168.7.38 192.168.7.243

You can press the “UPDATE DHCP RANGE” button after updating the Gateway IP/Subnet, but press it before editing the DHCP range values. The above DHCP values were originally generated by the WAN+2LAN2 Wizard in section 15 - EdgeRouter Wizard on page36, and then re-entered near Figure 68 – eth2 DHCP Details on page 64.

Press “Save” at the bottom of the page.

On the Networks page, press “+Create New Network”.
Change / Edit the following settings on this page for the Spare Network:

Name	SpareNetwork
VLAN	8
Gateway IP/Subnet	192.168.8.1/24
Domain Name	SpareNet
DHCP Range	192.168.8.38 192.168.8.243

You can press the “UPDATE DHCP RANGE” button after updating the Gateway IP/Subnet, but press it before editing the DHCP range values. The above DHCP values are from section 34 - Setup Remaining DHCP Servers on page 70.

Press “Save” at the bottom of the page.

90. Wireless Networks

With Ubiquiti, Never set anything on "Auto". Note that the preceding was bolded so you would notice it.

Click on "Wireless Networks. See Figure 185 – UniFi Wireless Networks.

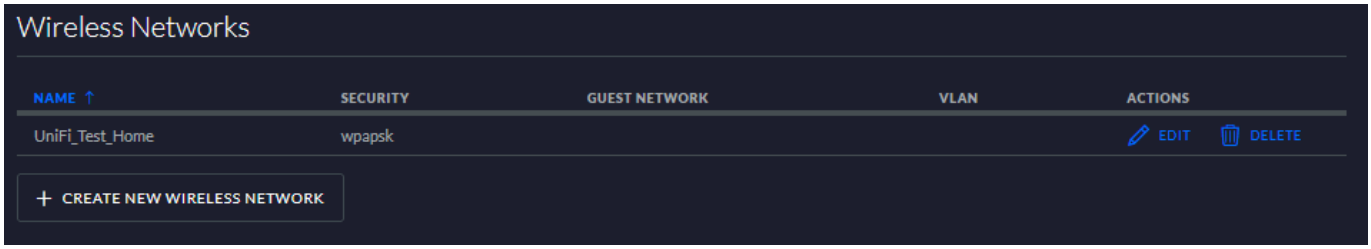


Figure 185 – UniFi Wireless Networks

90.1 Wireless Networks - Edit

Click “Edit” on the right side of the “UniFi_Test_Home” line. The resulting dialog is too large for display as one screenshot. See Figure 186 – UniFi Edit Wireless Network – Top and Figure 187 – UniFi Edit Wireless Network - Bottom

Figure 186 – UniFi Edit Wireless Network – Top

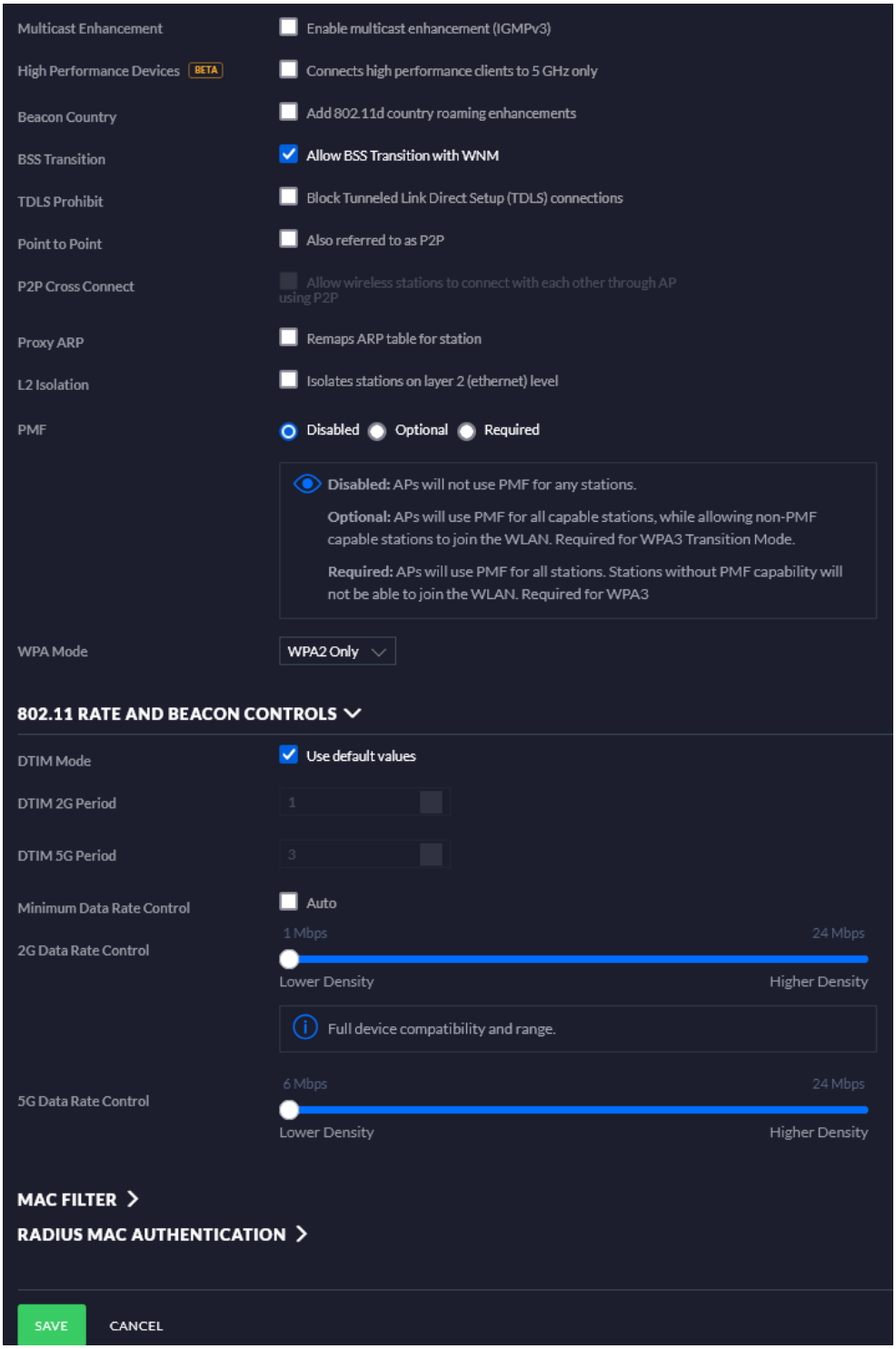


Figure 187 – UniFi Edit Wireless Network - Bottom

90.2 802.11 Rate and Beacon Controls

See section 102.8 - Enable minimum data rate controls. on page 228 for a more information about these values.

Find the following settings by clicking on the Navigation Bar's Setting's button. Select the "Wireless Networks" tab. Find the desired WiFi Network line, and then click on the Edit button, at the right side of that WiFi Network.

Change / Edit the following settings on this page for (the UniFi-Test_Home) Wireless Network:

DTIM Mode	`Checked`	Use default values
Minimum Data Rate Control	`UN-Checked`	Auto
2G Data Rate Control	`6 Mbps`	(Drag)
5G Data Rate Control	`12 Mbps`	(Drag)

Press "Save" at the bottom of the page.

See Figure 188 – UniFi 802.11 Rate and Beacon Controls.

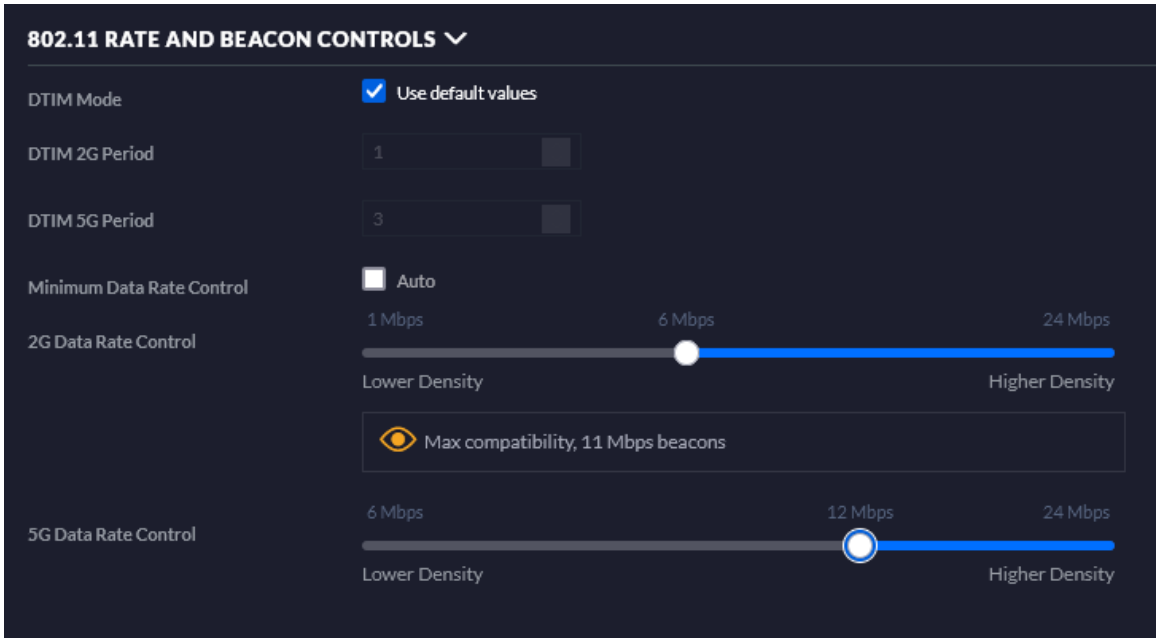


Figure 188 – UniFi 802.11 Rate and Beacon Controls

90.3 Create New Wifi

Note that any wireless network which has checked the "`Guest Policy`" checkbox will isolate *all* WiFi devices from every other WiFi device on that wireless network. Additionally the "`Multicast and Broadcast Filtering`" checkbox also needs to be unchecked to enable the Wi-Fi clients to communicate with each other. These settings are in Figure 190 – UniFi New Wireless Network – Advanced - Top on page 206.

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. See also related sections: 74.1 - Multicast DNS and 78.1 - 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. Before disabling the filtering, read the Information by clicking on the "I" inside of the circle.

Some impact of this setting is described in section 62 - Firewall Testing on page 124 and in Table 3 – Firewall Test Results on page 126. Remember there is another (marked) associated setting in section 89.2 - Create New Network on or after page 198.

Find the following settings by clicking on the Navigation Bar's Setting's button. Select the "Wireless Networks" tab. Press the "+ Create New Wireless Network" button. See Figure 189 – UniFi New Wireless Network - Basic.

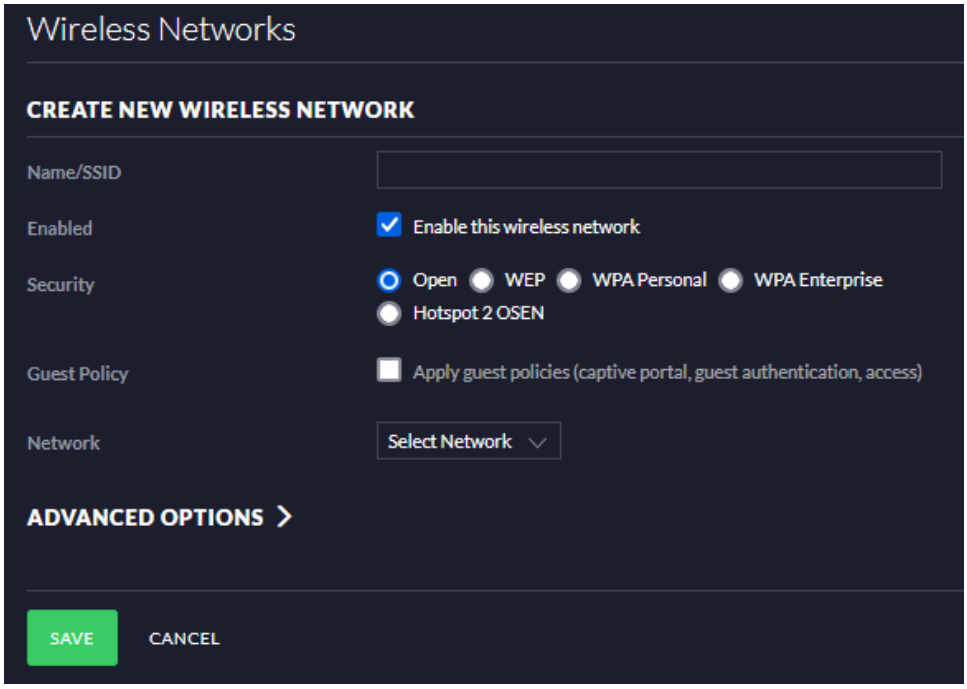


Figure 189 – UniFi New Wireless Network - Basic

See Figure 190 – UniFi New Wireless Network – Advanced - Top and Figure 191 – UniFi New Wireless Network – Advanced – Bottom.

Change / Edit the following settings on this page for the Guest Network:

Name/SSID	`<Your GuestNet WiFi SSID>`	
Security	`WPA Personal`	
Security Key	`<Your GuestNet WiFi Password>`	
Guest Policy	`Checked`	Apply guest policies
Network	`GuestNetwork`	

Open the “Advanced Options” section, Change / Edit the following settings on this page:

Multicast and Broadcast Filtering	`Checked`	Block LAN to WAN Multicast …

Open the “802.11 Rate and Beacon Controls” section, Change / Edit the following settings on this page:

Minimum Data Rate Control	`UN-Checked`	Auto
2G Data Rate Control	`6 Mbps`	(Drag)
5G Data Rate Control	`12 Mbps`	(Drag)

Press “Save” at the bottom of the page.

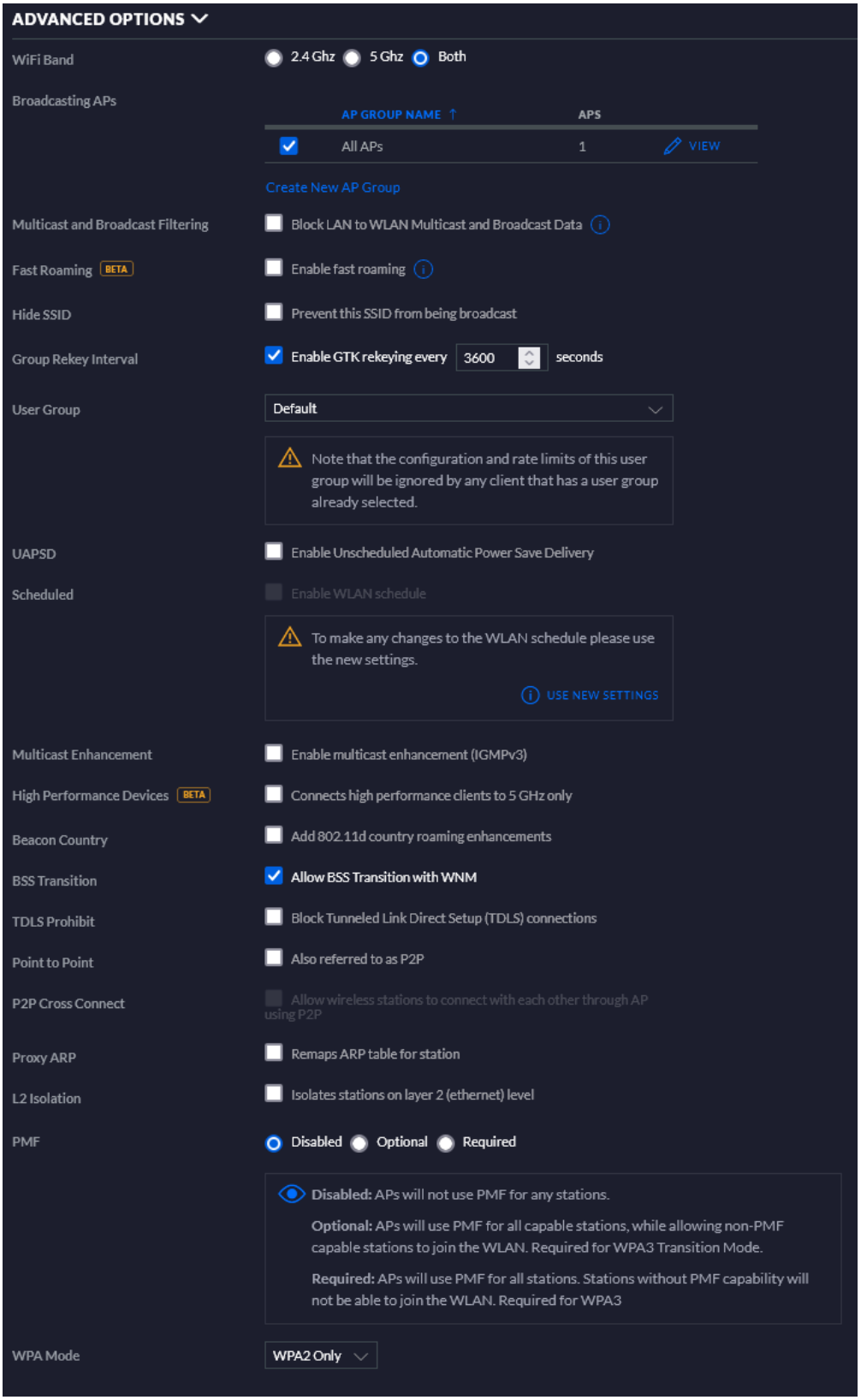


Figure 190 – UniFi New Wireless Network – Advanced - Top

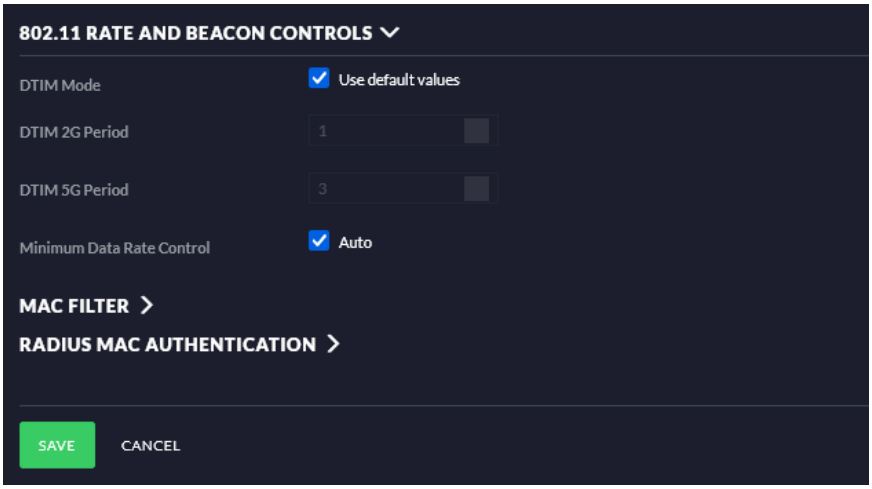


Figure 191 – UniFi New Wireless Network – Advanced – Bottom

Press the "+ Create New Wireless Network" button. Change / Edit the following settings on this page for the Iot Network:

Name/SSID	<Your IotNet WiFi SSID>	
Security	WPA Personal	
Security Key	<Your IotNet WiFi Password>	
Guest Policy	UN-Checked	Apply guest policies
Network	IotNetwork	

Open the "Advanced Options" section, Change / Edit the following settings on this page:

Multicast and Broadcast Filtering	UN-Checked	Block LAN to WAN Multicast …

Open the "802.11 Rate and Beacon Controls" section, Change / Edit the following settings on this page:

Minimum Data Rate Control	UN-Checked	Auto
2G Data Rate Control	6 Mbps	(Drag)
5G Data Rate Control	12 Mbps	(Drag)

Press "Save" at the bottom of the page.

Press the "+ Create New Wireless Network" button. Change / Edit the following settings on this page for the Spare Network:

Name/SSID	<Your SpareNet WiFi SSID>	
Security	WPA Personal	
Security Key	<Your SpareNet WiFi Password>	
Guest Policy	UN-Checked	Apply guest policies
Network	SpareNetwork	

Open the "Advanced Options" section, Change / Edit the following settings on this page:

Multicast and Broadcast Filtering	Checked	Block LAN to WAN Multicast …

Open the "Advanced Options" section, Change / Edit the following settings on this page:

Minimum Data Rate Control	UN-Checked	Auto
2G Data Rate Control	6 Mbps	(Drag)
5G Data Rate Control	12 Mbps	(Drag)

Press "Save" at the bottom of the page.

90.4 Re-provisioning UAP(s)

I temporarily changed my Guest Network settings while testing the ER-X firewall. Reference section 62 - Firewall Testing on page 124. After I disabled two UniFi "Guest network" settings, the Guest network was still blocked by my UAP. I forced the UAP to re-provision, and then the settings changed to what I expected.

To force a UAP to re-provision, select the UAP, and then go to the configuration tab. Reference Figure 198 – UniFi U6Lite – Config on page 213. Open up "Manage Device" and then press the "Provision", button within the "Force Provision" section. This causes the UAP to (temporarily) go offline, while it re-applies all of its configuration settings. The particular settings I changed are described in section 90.3 - Create New Wifi on page 204

90.5 Switching to New User Interface

If you are in Legacy mode, you can return to the New User Interface by Clicking on "Settings" in the Navigation Bar. See Figure 171 – UniFi Navigation Bar. Once in Settings, click on the "User Interface" tab. Reference Figure 178 – UniFi Settings –Legacy SubMenu. For the specific setting, see Figure 192 – UniFi Interface Setting - Legacy.

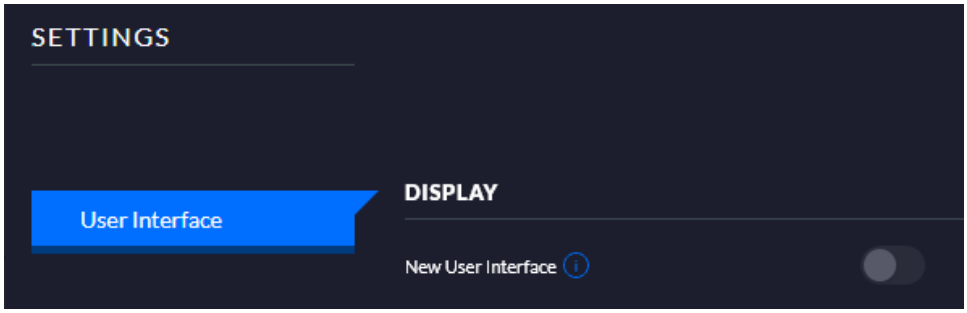


Figure 192 – UniFi Interface Setting - Legacy

In the "Display" section, enable the "New User Interface" slider.

Press "Apply Changes" at the bottom of the page.

90.6 Global AP Settings

You will need to be in the New User Interface, See section 86.3 - UniFi System Page – New Interface.on page 188.

Click on the Navigation Bar's "Setting" icon; reference Figure 171 – UniFi Navigation Bar on page 187. From the Setting Sub-Menu (shown in Figure 172 – Setting's Sub-Menu - New. on page 187) click on "WiFi". See Figure 185 – UniFi Wireless Networks on page 200.

Set the "Global AP Settings" as follows:

2.4 GHz Radio:

Channel Width (MHz)	20		(Never set to 40)
Transmit Power	Custom	13 dBm	(Scroll Down for Custom)

5 GHz Radio:

Channel Width (MHz)	40		
Transmit Power	Custom	20 dBm	(Scroll Down for Custom)

Press "Apply Changes" at the bottom of the page.

90.7 AP Site Settings

You will need to be in the New User Interface, See section 86.3 - UniFi System Page – New Interface.on page 188.

Reference section 8.4 - Ethernet Wiring your UAPs on page 17, and section 8.6 - UAP Wireless Uplinking on page 19 for information pertaining to the "Wireless Connectivity" / "Wireless Meshing" setting.

Click on the Navigation Bar's "Setting" icon; reference Figure 171 – UniFi Navigation Bar on page 187. From the Setting Sub-Menu (shown in Figure 172 – Setting's Sub-Menu - New. on page 187) click on "WiFi". See Figure 185 – UniFi Wireless Networks on page 200.

Change the "AP Site Settings" as follows:

Wireless Connectivity	Un-check	Wireless Meshing

"Confirm" the Disable.

Press "Apply Changes" at the bottom of the page.

90.8 Nightly Channel Optimization

You will need to be in the New User Interface, See section 86.3 - UniFi System Page – New Interface.on page 188.

Click on the Navigation Bar's "Setting" icon; reference Figure 171 – UniFi Navigation Bar on page 187. From the Setting Sub-Menu (shown in Figure 172 – Setting's Sub-Menu - New. on page 187) click on "WiFi". See Figure 185 – UniFi Wireless Networks on page 200.

Change the "Nightly Channel Optimization" as follows:

Channel Optimization `Un-check`

"Confirm" the Disable.

Press "Apply Changes" at the bottom of the page.

While monitoring my system, I noticed that my U6-Lite seemed to *still* be switching channels. So I also choose "AP Exclusions" and selected my AP in the menu. You might want to add all of your UAPs to the exclusion list.
Press "Apply Changes" at the bottom of the page.

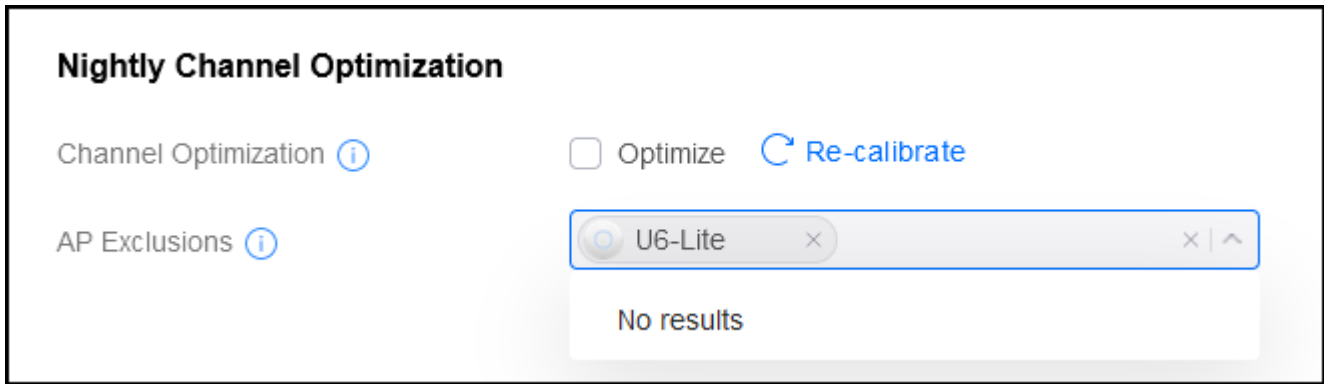


Figure 193 – UniFi Nightly Channel Optimization

Switch back to the Legacy Interface as shown in section 86.4 - Switch to Legacy Interface on page 189

91. UniFi Devices Page

You can be in either the New Interface or Legacy Interface. The columns / data shown will change between the two interfaces. I will be in the Legacy Interface. The columns are customizable as to show or hide.

Each device is clickable, which will bring up device configuration / status pages.

Click on the Navigation Bar's "UniFi Devices" icon; see Figure 171 – UniFi Navigation Bar on page 187.

The device pages look like Figure 194 – UniFi Device Page – New and Figure 195 – UniFi Device Page – Legacy.

Figure 194 – UniFi Device Page – New

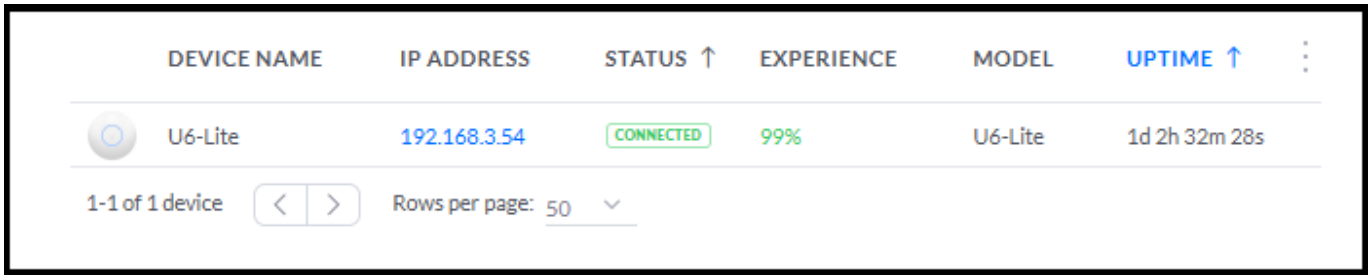


Figure 195 – UniFi Device Page – Legacy

92. Unifi Device Screens

Once you are on the Devices page, Reference section 91 - UniFi Devices Page on page 211, then you can click on an Access Point to investigate its status and/or configure it. My test installation has a single U6-Lite. Click on one of your UAPs. I see five screens / tabs across the top. See the following figures, which are named for its tab:

Figure 196 – UniFi U6Lite - Details

Figure 197 – UniFi U6Lite - Clients

Figure 198 – UniFi U6Lite – Config

Figure 199 – UniFi U6Lite – Tools

Figure 200 – UniFi U6Lite – Stats

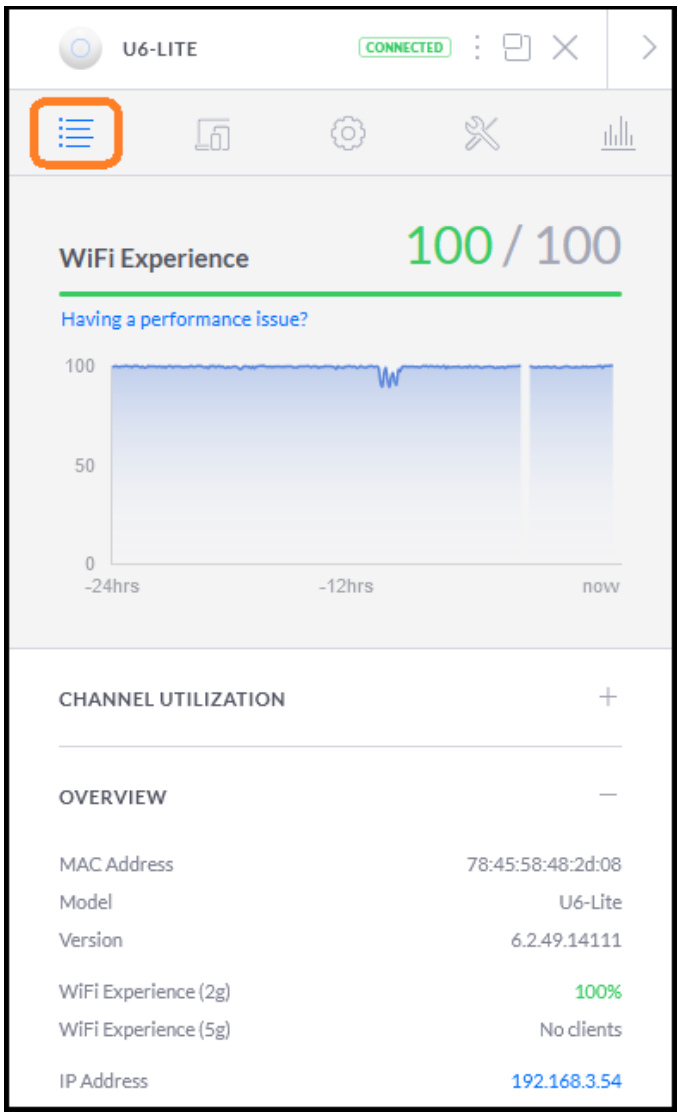


Figure 196 – UniFi U6Lite - Details

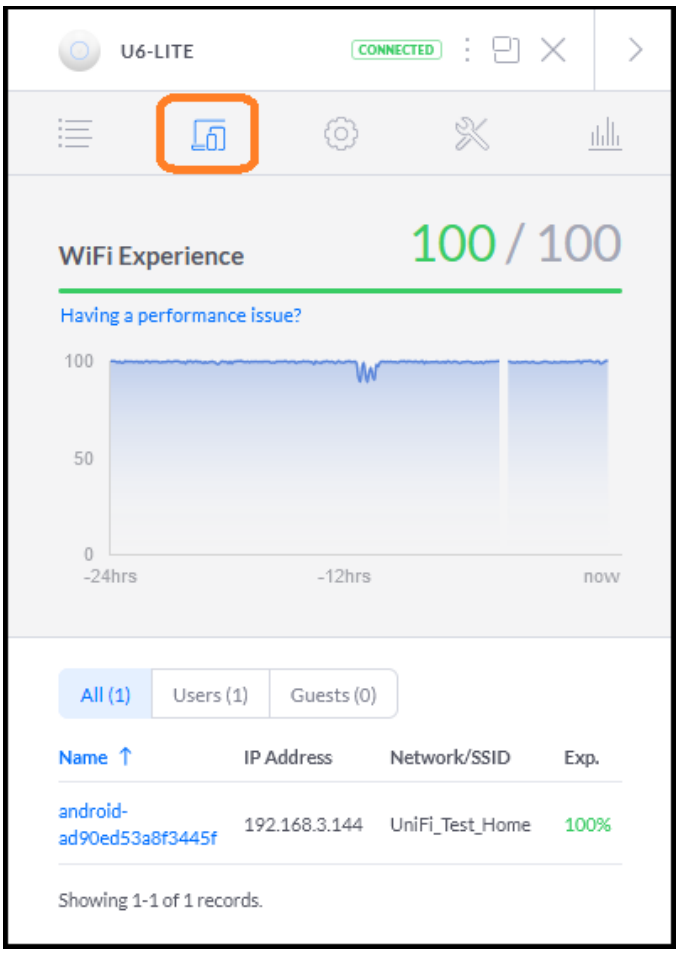


Figure 197 – UniFi U6Lite - Clients

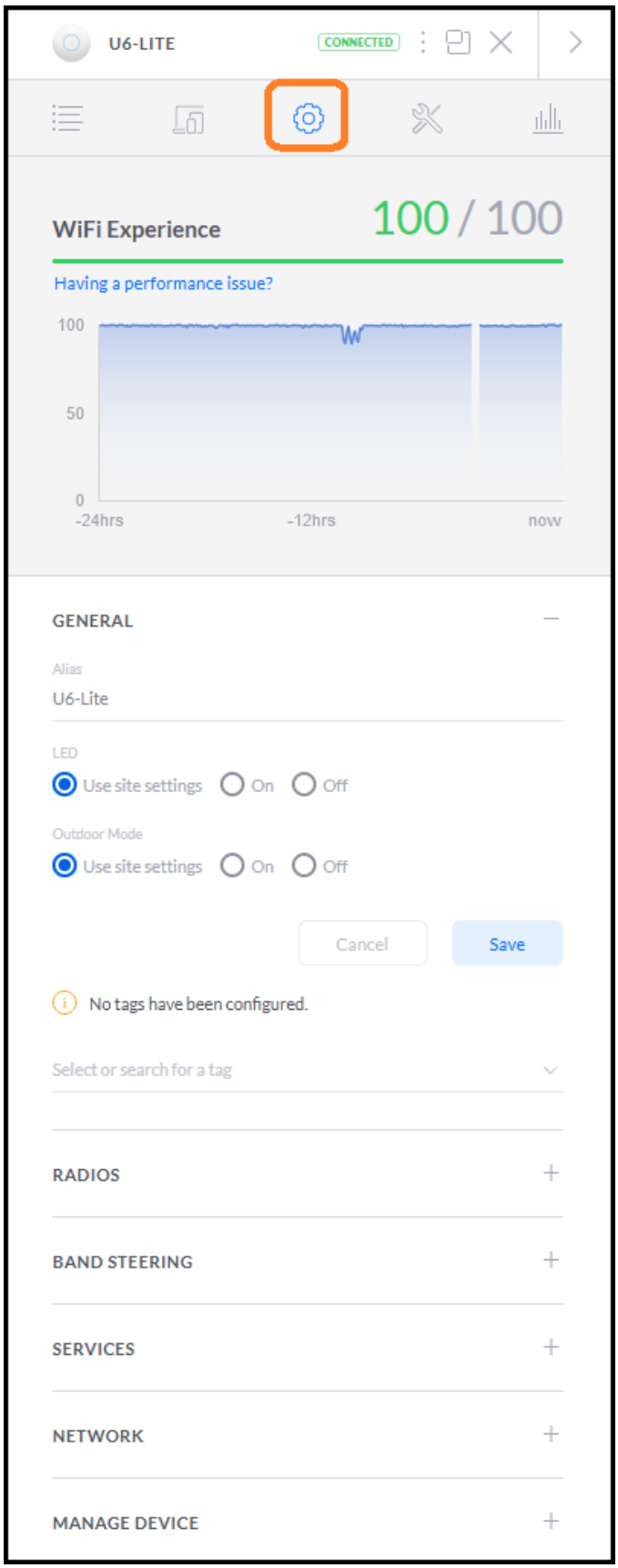


Figure 198 – UniFi U6Lite – Config

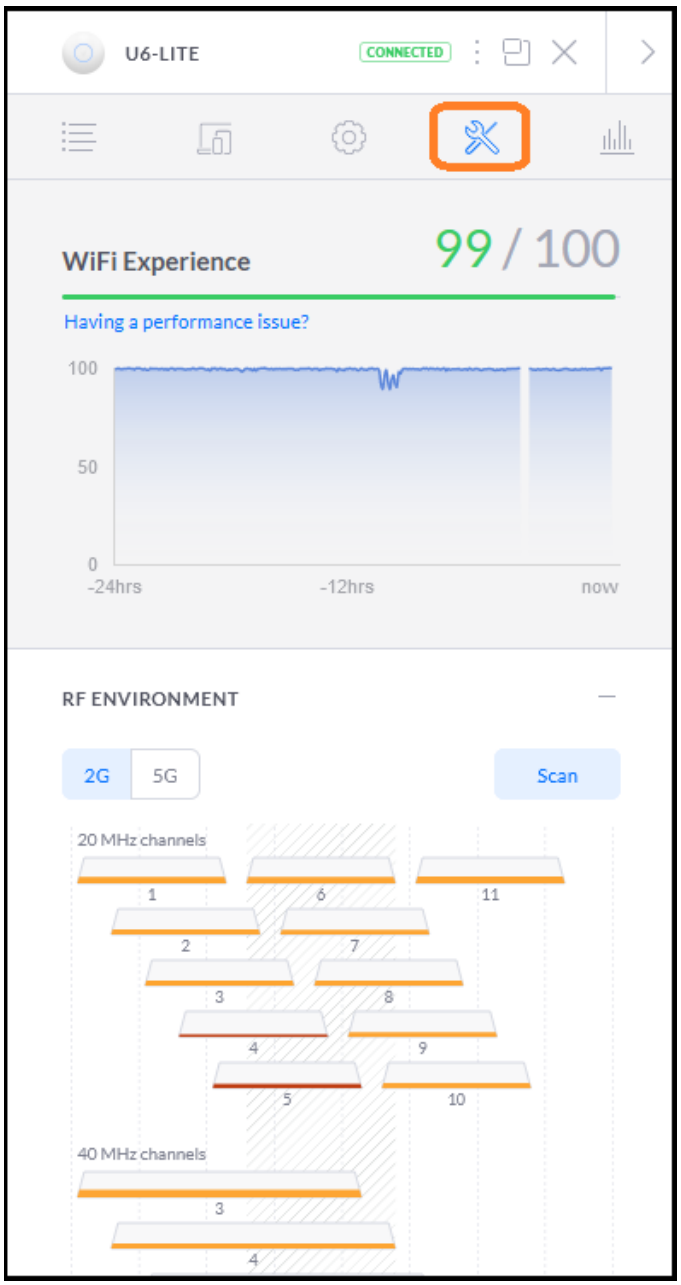


Figure 199 – UniFi U6Lite – Tools

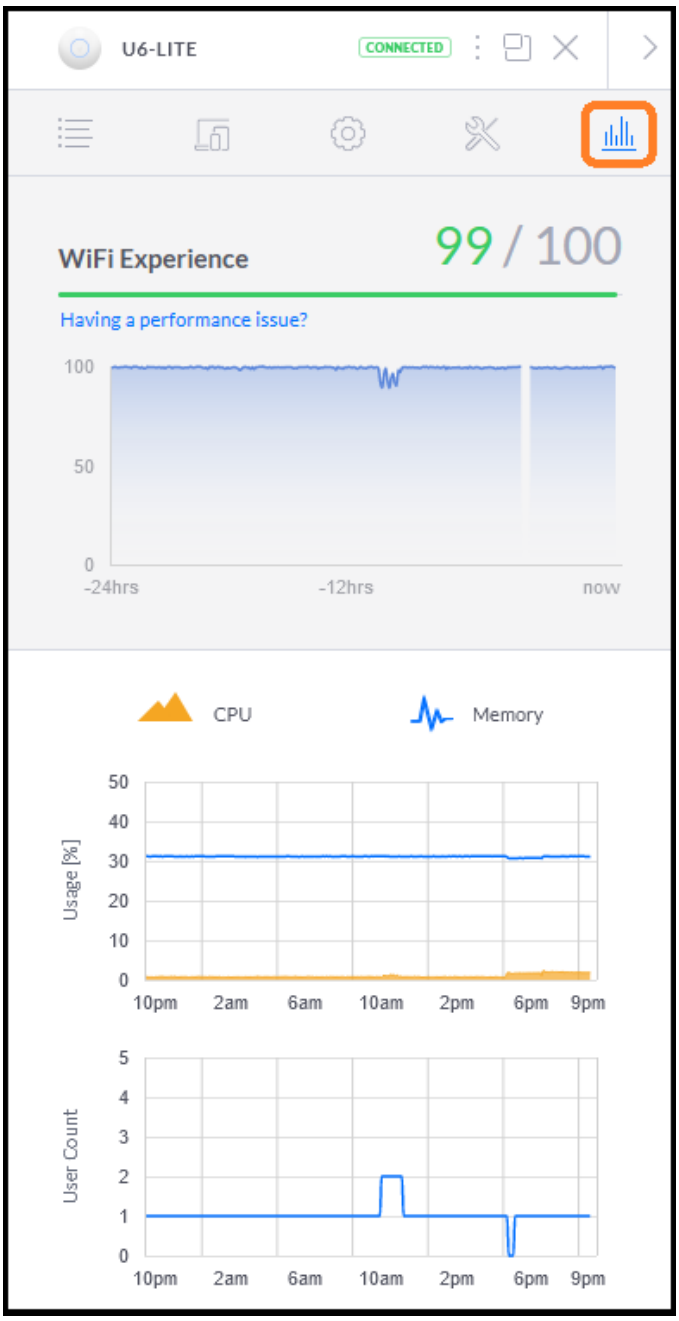


Figure 200 – UniFi U6Lite – Stats

92.1 UAP Channel Scan

A UAP channel scan can be performed via the page shown on Figure 199 – UniFi U6Lite – Tools on page 214. Reference item #7 of @AlexWilsonsBlog's comment on page 230.

If your channel scan does not work, reference section 105 - UniFi STUN / Channel Scanning on page 243.

93. Configure UAP Channel / Power Levels

Click on the Navigation Bar's "UniFi Devices" icon; reference Figure 171 – UniFi Navigation Bar on page 187, then click on an Access Point you want to modify, and then click on the Config tag. Reference Figure 198 – UniFi U6Lite – Config on page 213.

You will need to repeat this step for each of your UAPs.

Within the General area:

You can provide an Alias (name) for your Access Point.

You can control if the LED should follow the UniFi Controller's global LED setting, or is On, or is Off.

See the following sections for information pertaining to the specific values to enter in the following example:

102.3 - Channel assignment for the 2.4GHz band. on page 220

102.4 - Channel assignment for the 5GHz band. on page 221

102.5 - Power Levels. on page 224

102.6 - Band Steering. on page 227

Within the Radios area, change the following,

Use Global AP Settings		Off	
Nightly Channel Optimization		Off	
2.4GHz	Channel Width	HT20	
2.4GHz	Channel	<Your Channel>	(Use only 1, 6, 11)
2.4GHz	Transmit Power	Custom 13dBm	
2.4GHz	Enable Minimum RSSI	Off	
5GHz	Channel Width	HE40	(Suggest 40)
5GHz	Channel	<Your Channel>	(Typically 36 / 44 / 149 / 157)
5GHz	Transmit Power	Custom 20dBm	
5GHz	Enable Minimum RSSI	Off	

Press "Queue Change"

Within the Band Steering area, ensure the following,

Band Steering Off

Press "Queue Change" if needed.

Press "Apply Changes"

Your Access Point(s) should now be running.

94. UniFi Client Page

Click on the Navigation Bar's "Clients" icon; see Figure 201 – UniFi Clients Page – Legacy.

You can show / hide the columns displayed, by first clicking on the three bars (underlined in orange), followed by clicking on the three dots (also underlined in orange). This brings up a clickable list of column header-names which can be selected or de-selected.

You can also sort the column data, I like selecting "Signal" (outlined in green) so the weakest / problem devices are displayed at the bottom of the list and can then be easily monitored See Figure 201 – UniFi Clients Page – Legacy. I have already modified the columns shown and the order (signal) to my liking.

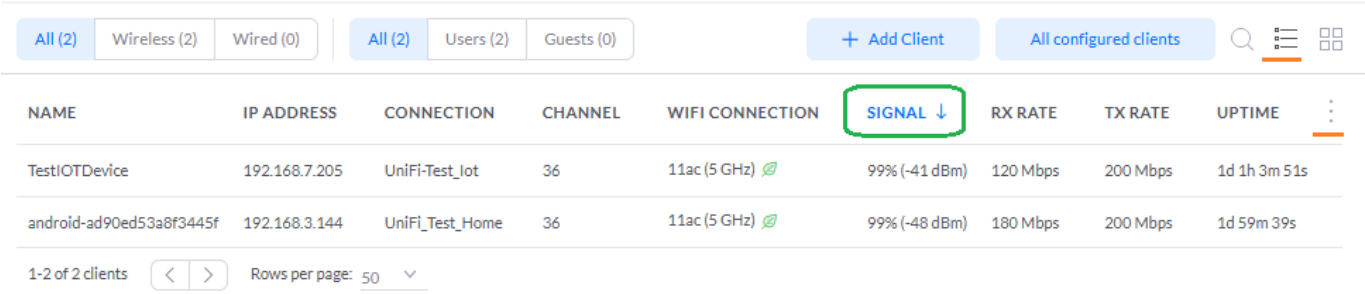


Figure 201 – UniFi Clients Page – Legacy

95. UniFi Map Page

Click on the Navigation Bar's "Map" icon; see Figure 201 – UniFi Clients Page – Legacy.

I have never used use this.

96. UniFi Statistics Page

Click on the Navigation Bar's "Statistics" icon; see Figure 201 – UniFi Clients Page – Legacy.

Interesting items in the sub-menu are:

System Stats

Performance

Debugging Metrics

97. UniFi Insights Page

Click on the Navigation Bar's "Insights" icon; see Figure 201 – UniFi Clients Page – Legacy.

Interesting items in the sub-menu are:

Client History

Neighboring Access Points

98. UniFi Events Page

Click on the Navigation Bar's "Events" icon; see Figure 201 – UniFi Clients Page – Legacy.

This page shows what activities have occurred within the UniFi system.

99. UnFi Alerts Page

Click on the Navigation Bar's "Alerts" icon; see Figure 201 – UniFi Clients Page – Legacy.

This page shows what alert items have occurred within the UniFi system.
Alerts are usually of high importance, e.g. "U6-Lite-TestUAP was disconnected".

To dismiss alert notifications, press the "ARCHIVE ALL" button.

100. UniFi Updates

Updates to Unifi software and UAP firmware are typically shown in the upper right. See Figure 202 – UniFi Update Notification(s). Reference section 82.2 - System Stability on page 175.

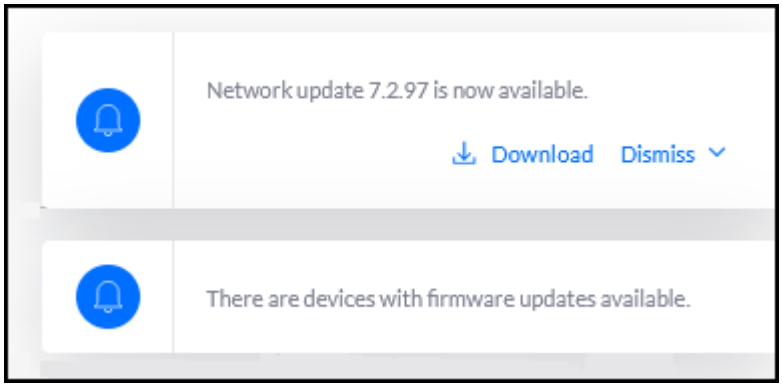


Figure 202 – UniFi Update Notification(s)

101. UniFi Configuration Backup

Click on the Navigation Bar's "Settings" button. Reference Figure 171 – UniFi Navigation Bar.
The Legacy Settings page has a sub-menu as shown in Figure 178 – UniFi Settings –Legacy SubMenu.
Click on "Backup". See Figure 203 – UniFi Backup Screen.

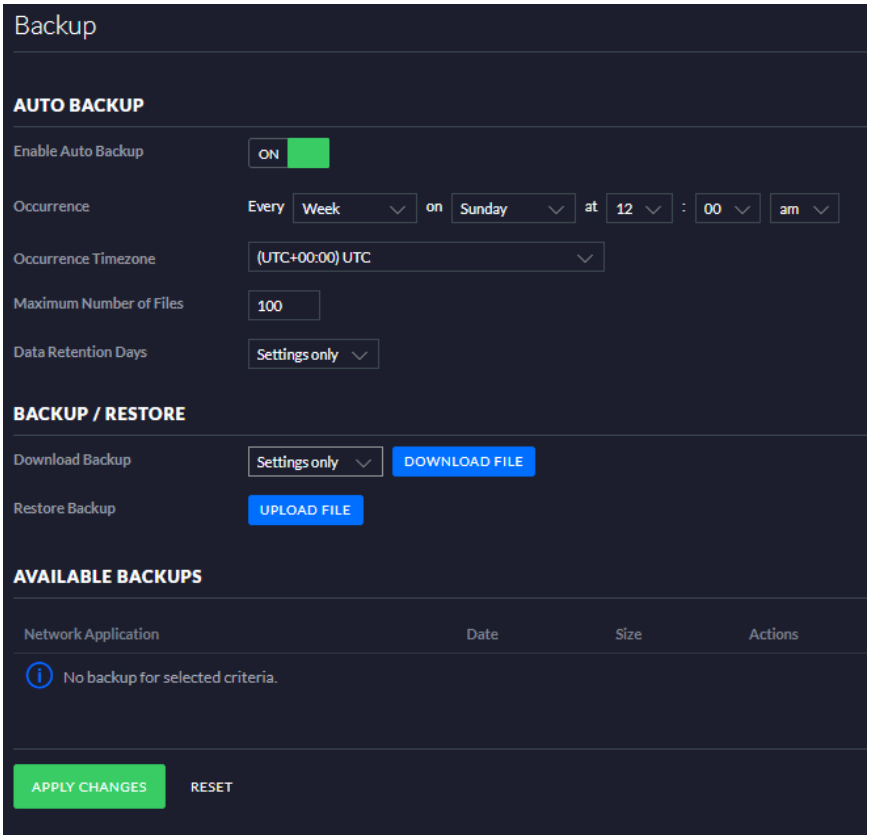


Figure 203 – UniFi Backup Screen

Near the top of this screen is an "Auto Backup" section. I set mine to "On", and to back up every Week with "Data Retention Days" set to "Setting only". Haha Ubiquiti. Since I don't know where the backup files are being stored, I am not relying upon this feature. Note that at the bottom of my backup page is a section titled "Available backups". Even though I have been running this UniFi Controller for several weeks, its list is empty.

In the middle of the page is a section titled "Backup / Restore". To (attempt) to generate a backup file, I set the Download Backup (type) to "Settings only" and then pressed the "Download File" button. All I got was Figure 204 – UniFi Backup Failed. Ah, Snap.

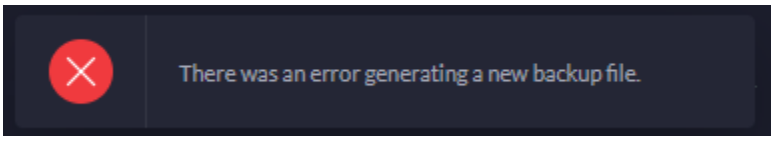


Figure 204 – UniFi Backup Failed

So I rebooted my Unifi Controller, Tried again, and this time I got a successful backup file. See Figure 205 – UniFi Backup Passed.

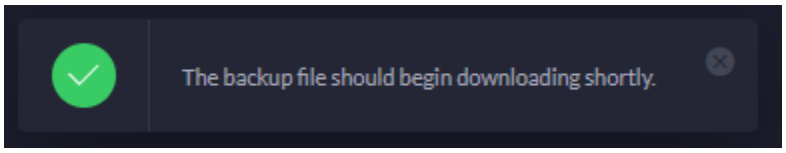


Figure 205 – UniFi Backup Passed

My backup file was named "7.3.76-20230210-1931.unf". These backup files can only be used on the stated version of Unifi, or loaded into a newer UniFi version. They will not work with an earlier version.

An hour or so later, when I tried to generate a new backup file, I got another failure as shown in Figure 204 – UniFi Backup Failed. So another reboot was required. So much for stable software. Please generate a backup file every time you make a configuration change.

If you do decide to upgrade to a newer UniFi version, don't destroy your existing backup file. There are many postings of users whom upgrade to a newer / unstable / bad UniFi Controller version, and then could not get back, to the current one, because they didn't keep their old backup files.

Ubiquiti help article:

https://help.ui.com/hc/en-us/articles/360008976393-UniFi-Backups-and-Migration

https://help.ui.com/hc/en-us/articles/205202580

102. Channels, Power Levels, and Minimum Data Rates

This information in this section (and sub-sections) should apply to just about any single or multi access-point installation. The following is only what I have read and/or done for my installation. Specifics may apply to U.S.A only, other countries will likely vary.

How to set channel assignments (2.4 GHz and 5 GHz) and how to set power levels are described in section 93 - Configure UAP Channel / Power Levels on page 215.

102.1 The best link on Wi-Fi details.

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

102.2 SSIDs.

Everything that I have read, says that **all** Access Point(s) 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 the installation area.

102.3 Channel assignment for the 2.4GHz band.

Each Access Point should use a separate, non-overlapping channel (as much as possible for 2.4GHz.).

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 206 – 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.

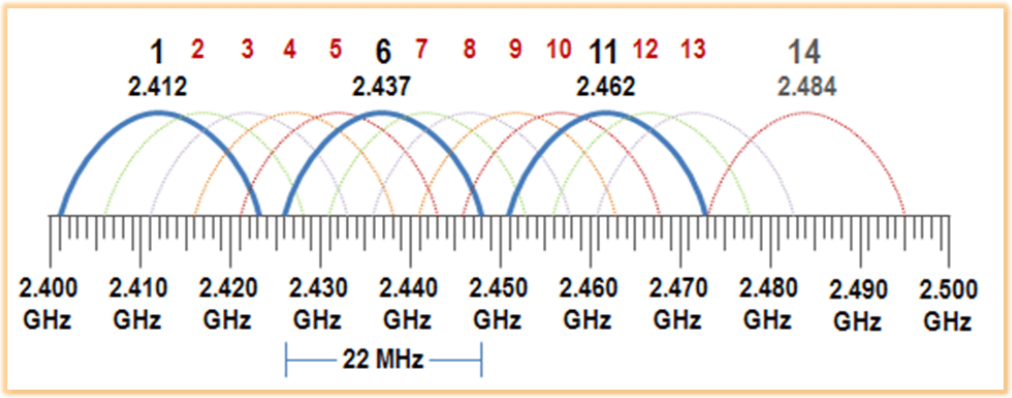


Figure 206 – 2.4 GHz Channel Frequencies

102.4 Channel assignment for the 5GHz band.

Each Access Point should use a separate, non-overlapping channel.

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 207 – 5 GHz Channel Frequencies – One.

Also see (borrowed from the Internet) Figure 208 – 5 GHz Channel Frequencies - Two on page 222.

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 (52 base = 58 center) or to (149 base = 155 center). Using VHT80 achieves a higher 5G data rate, at the 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.

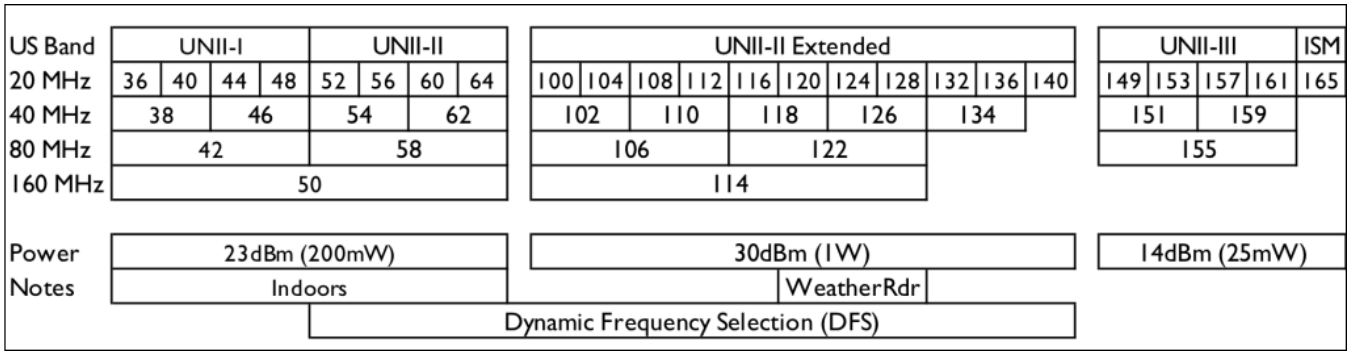


Figure 207 – 5 GHz Channel Frequencies – One

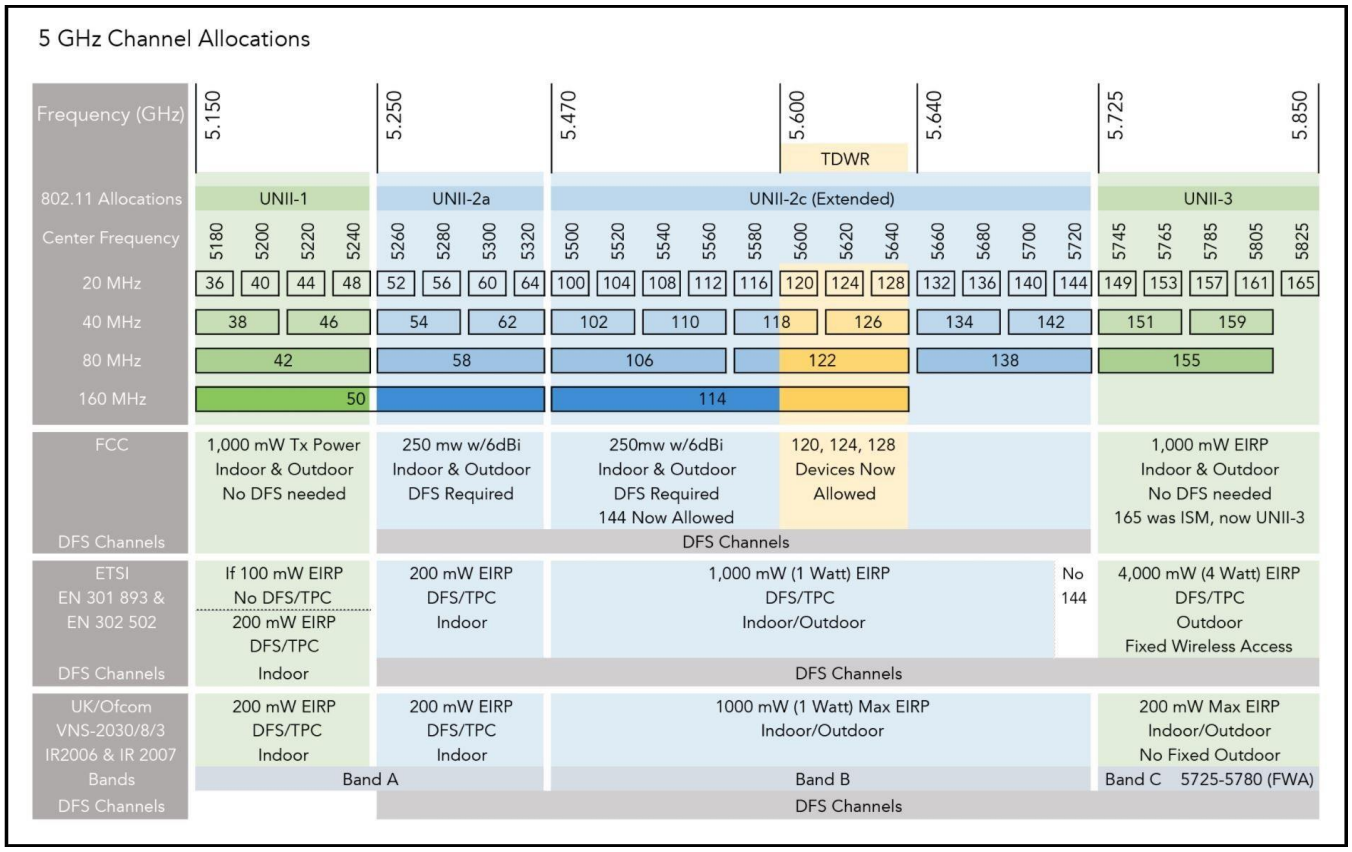


Figure 208 – 5 GHz Channel Frequencies - Two

@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
[Editorial note: loosing 3dBm of signal strength equates to loosing *half* of your signal strength.]

102.5 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

@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

102.6 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.

102.7 DTIM Settings.

I believe the values should be:

DTIM 2G period	1
DTIM 5G period	3

With the Unifi installation, that was current when this was re-written, the above values were the default.

The way to set these is shown in section 90.2 - 802.11 Rate and Beacon Controls on page 203.

102.8 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 102.11 - 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

To set these values, reference section 90.2 - 802.11 Rate and Beacon Controls on page 203.

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

102.9 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

102.10 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

102.11 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

102.12Wi-Fi Modulation Coding Scheme (MCS).

Figure 209 – 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 209 – Wi-Fi Modulation Coding Scheme (MCS) Table

I believe that (borrowed from the internet) Figure 210 – 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 209 – 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.

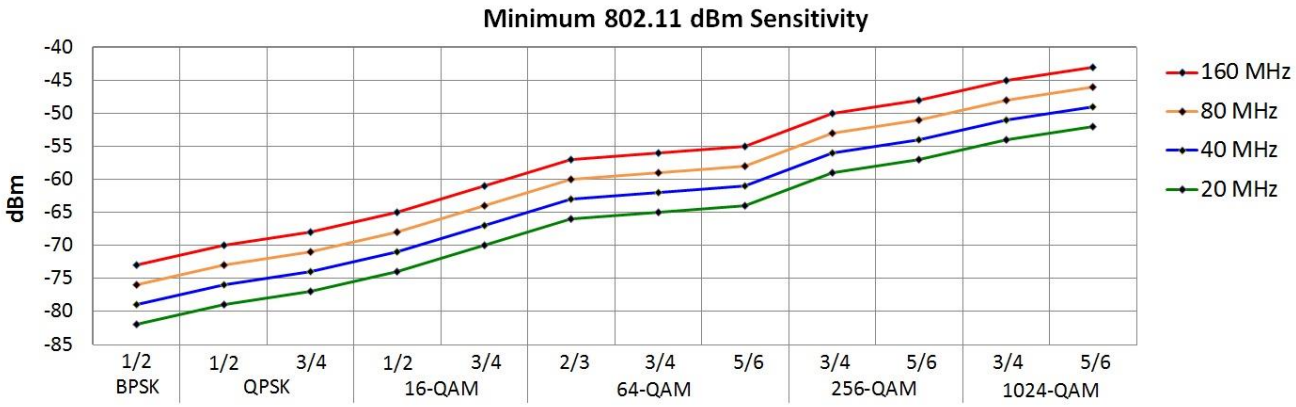


Figure 210 – Wi-Fi Minimum 802.11 dBm Sensitivity Table

102.13 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 211 – 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 211 – 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 212 – 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 213.

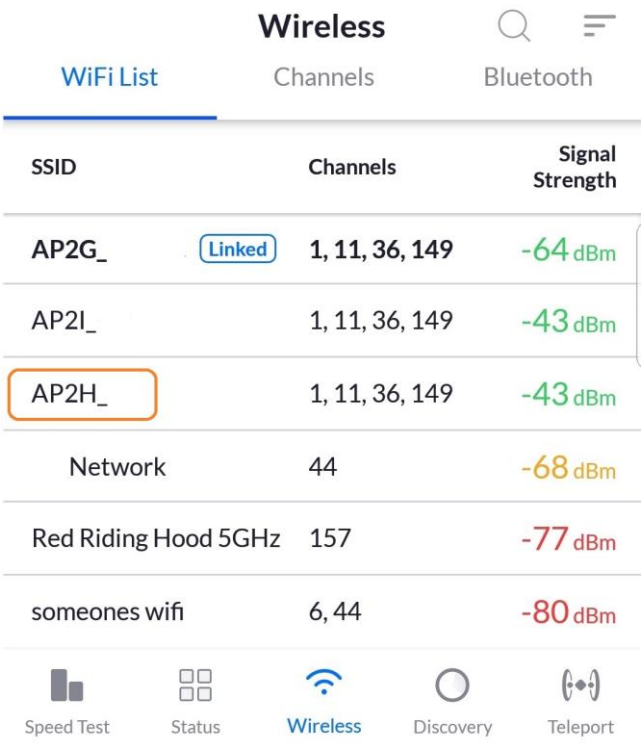


Figure 212 – WiFiMan WiFi-List Screenshot

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 230.

At each location, I measured and recorded what dBm signal strength was received by a device, from each UAP. Examples of this will be shown in Figure 213 – 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 214 – 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 213 – 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!]

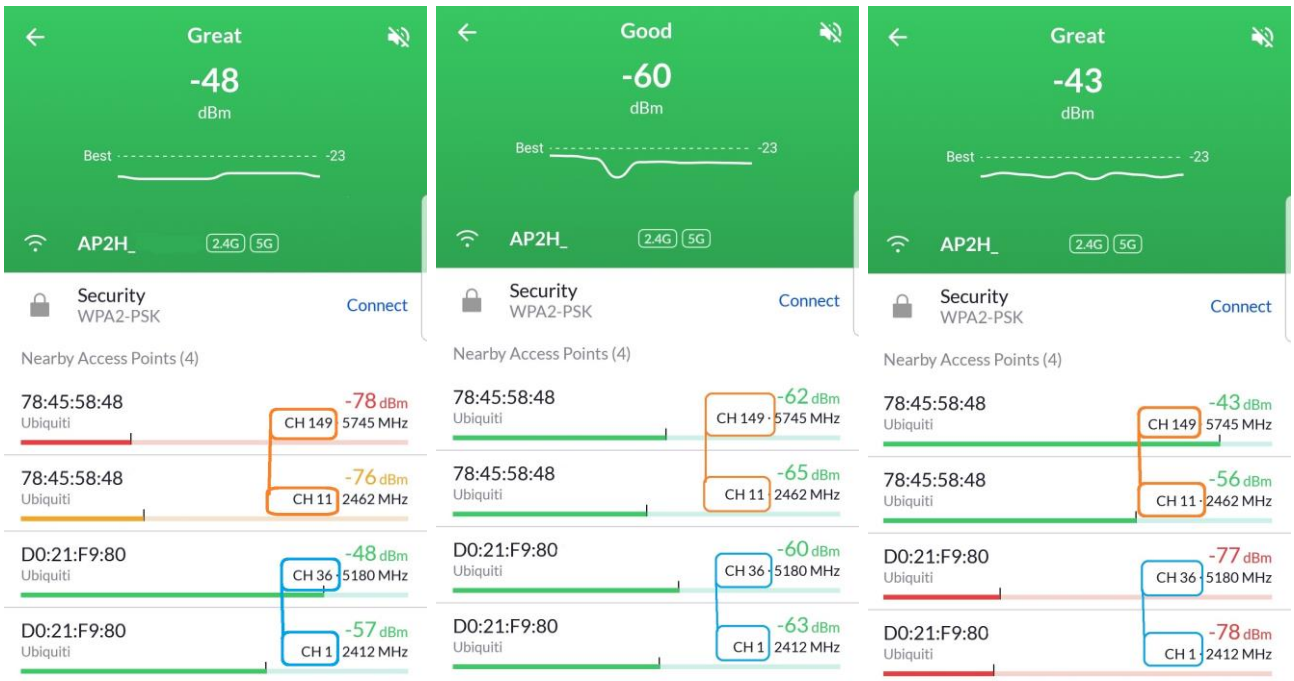


Figure 213 – WiFiMan dBm Screenshots

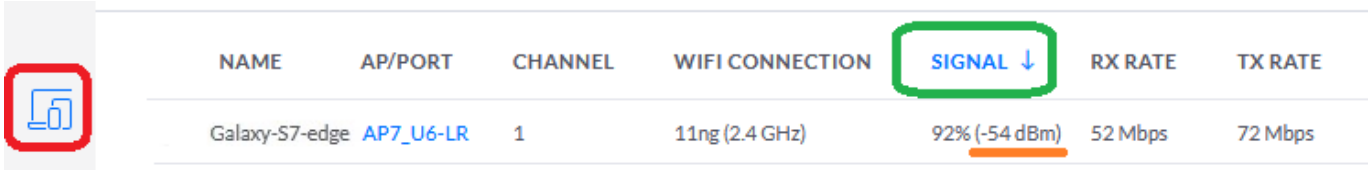


Figure 214 – UniFi's Received Signal Value

103. Troubleshooting UniFi / Wi-Fi Performance

Apple:

About wireless roaming for enterprise <Apple>

https://support.apple.com/en-us/HT203068

UniFi Help References:

UniFi Network - Wireless Client Connectivity

https://help.ui.com/hc/en-us/articles/221029967

UniFi - Troubleshooting Slow Wi-Fi Speeds

https://help.ui.com/hc/en-us/articles/360012947634-UniFi-Troubleshooting-Slow-Wi-Fi-Speeds

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

104. Some Other Wi-Fi References.

Wikipedia
https://en.wikipedia.org/wiki/List_of_WLAN_channels

WiFi 5GHz band and wide channels
https://metis.fi/en/2018/02/5ghz-channels/

2.4 GHz Channel Planning
https://www.extremenetworks.com/extreme-networks-blog/2-4-ghz-channel-planning/

IEEE 802.11ac Gigabit Wi-Fi
https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ac.php

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

Best WiFi Coverage for Medical Office
https://community.ui.com/questions/Best-WiFi-Coverage-for-Medical-Office/2be1dc1b-6c1d-4e41-9385-5c54bd5be0ed

105. UniFi STUN / Channel Scanning

Note: this section was needed for earlier installations, and it does not appear to be needed now, but I'm leaving this section here for now. This section was not re-written. Reference section 92.1 - UAP Channel Scan on page 214.

Reference item #7 of @AlexWilsonsBlog's comment on page 230 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 4 - Reserved Address. Reserve the addresses for your "UniFi Controller" and all of your Access Point(s) by following section 68 - 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 64 - Optional DNS Forcing of the IOT Network, but enter the information from Figure 215 – STUN DNAT Rule Data

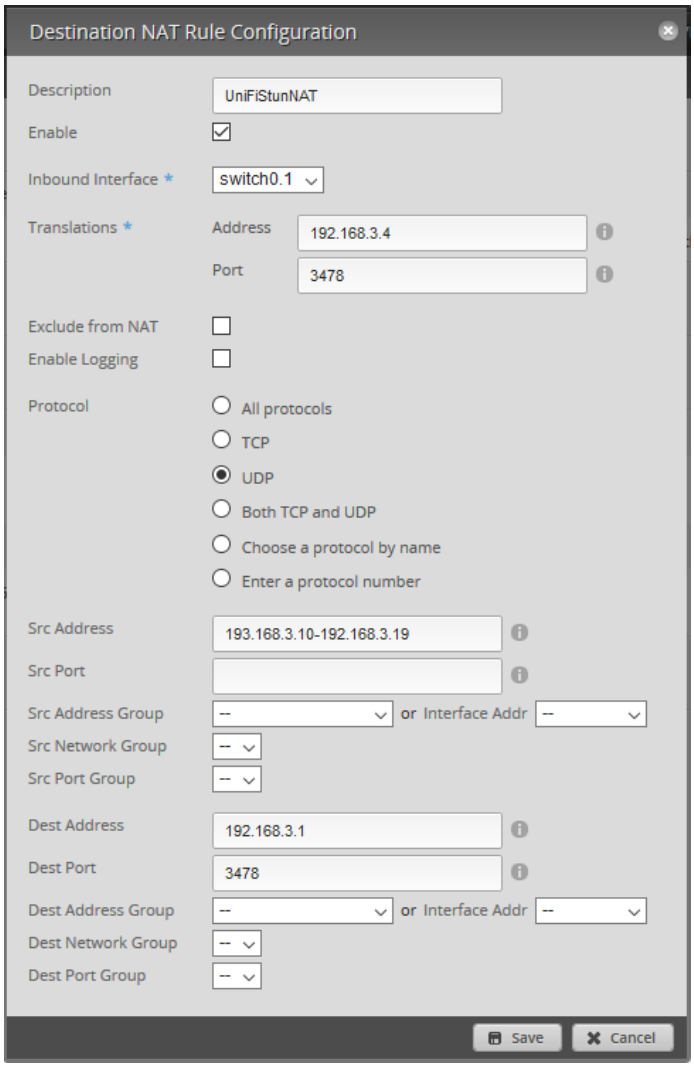


Figure 215 – STUN DNAT Rule Data

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 199 – UniFi U6Lite – Tools on page 214.

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 216 – Channel Scanning Context

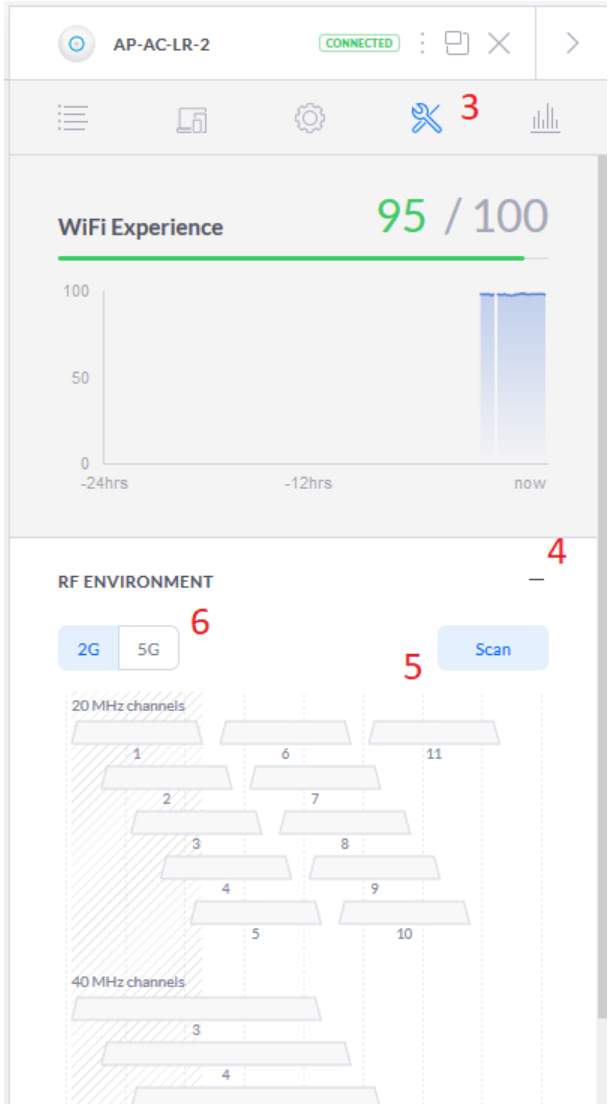


Figure 216 – Channel Scanning Context

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

106. 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

107. End of UniFi / Access Point Setup

This is the end of the Access Point / UniFi Software / UniFi Controller setup.

108. 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.ui.com/questions/Run-script-which-disable-enables-a-firewall-policy/008bcb4f-2699-4b2c-aaf3-5cc0af8bec3d#answer/3747b450-29c8-4cab-b74d-1a2a5a6a7c22

Forward port to PC on IoT Network:
https://community.ui.com/questions/Forward-port-to-PC-on-IoT-Network/4c5b662c-13d9-4a52-9d38-584b15957e10

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.ui.com/questions/How-to-set-up-MTU-properly/dbb28fa7-0873-418b-bae5-0ed471b84a88

EdgeRouter - Configure an EdgeRouter as a Layer 2 Switch (Handy for a remote POE-powered Ethernet switch):
https://help.ui.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRouter-as-a-Layer-2-Switch

Measure instantaneous bandwidth usage over time:
https://community.ui.com/questions/Measure-instantaneous-bandwidth-usage-over-time/797a40f2-b170-4b5d-8c13-637028cc375f

Help setting up NetFlow :
https://community.ui.com/questions/Help-setting-up-NetFlow/76f3a152-3f01-4e68-aa32-58c988c2b77e

Add Debian Packages to EdgeOS:
https://help.ui.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

@BranoB made the following interesting posting about the file system:
https://community.ui.com/questions/EdgeOS-file-system-layout-and-firmware-images/b5e5f4c8-20b1-4fae-8689-638ab48cb595

@16gain Port Mirroring on an ER-X configured as a network switch:
https://community.ui.com/questions/Edgerouter-X-Port-Mirroring-Issue/fdc37e51-0d3f-4b38-bf15-d92d57f5c84b#answer/4f64288a-2ef8-4310-ae26-37b32a143578

Configure an EdgeRouter as a Layer-2 Switch:
https://help.ui.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRouter-as-a-Layer-2-Switch

Port Forwarding with a local address:
https://community.ui.com/questions/Is-there-a-way-to-setup-port-forwarding-so-that-the-receiving-system-on-the-local-network-sees-a-lo/66b9b667-b6f2-474a-a350-23259e3edc40

109. 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. Multimedia over Coax Alliance (MOCA)

This section 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(s). You need at least two MOCA adapters to network together. Multiple MOCA adapters just form a larger network. 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 so he could 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 $180 US. That’s pretty expensive, but still better than using UAP Wireless Uplinking, discussed in section 8.6 on page 19.

One method of testing the MOCA link-speed is to run an internet “speed test” from a suitable device (e.g laptop) plugged into the far-adapter, with the near-adapter plugged-into your ER-X router. Your ISP up / down internet rate may be a limiting factor for this result, since the far end of this test, is actually the internet.

More tech-savvy people might instead run iperf3 from two PC(s) / laptop(s) with the desired MOCA link in-between them. Iperf3 is the internal protocol which used within internet speed tests. Do not attempt to run iper3 *on* the ER-X, as it is not designed for this task.

References:
http://www.mocalliance.org/
https://en.wikipedia.org/wiki/Multimedia_over_Coax_Alliance

Appendix B. Ethernet Over Power Adapters

This section is just general networking information. The electrical information may only apply to the U.S.A.

If you need to get an Ethernet cable run between two points and cannot physically run a cable, you might be able to use a pair of Ethernet-Over-Power (EOP) adapters. 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 each plug into a standard wall power-outlet. Each device has at-least one Ethernet port; some also have the equivalent of a Wi-Fi Access Point in them. These adapters use a HomePlug AV2 protocol to communicate between each other. Each device converts Ethernet data into AV2 data, and injects that (high frequency) AV2 data onto the power lines of your house. Each device also converts (that) AV2 powerline data back into Ethernet data. Multiple EOP adapters just form a larger network.

I have only played around with these devices, and have not used them for permanent data runs. Earlier EOP models / adapters, appear to have been largely unreliable. You should only plug these directly into wall outlets, extension cords and especially power strips attenuate the high frequencies these adapters depend-upon for operation.

I have read that these devices do not work well when an EOP adapter is connected to a power circuit on the "A" side of your circuit breaker panel, and another EOP adapter is connected to a power circuit on the "B" side of your circuit breaker panel. See Figure 217 – Typical U.S.A Home Circuit Breaker Panel.

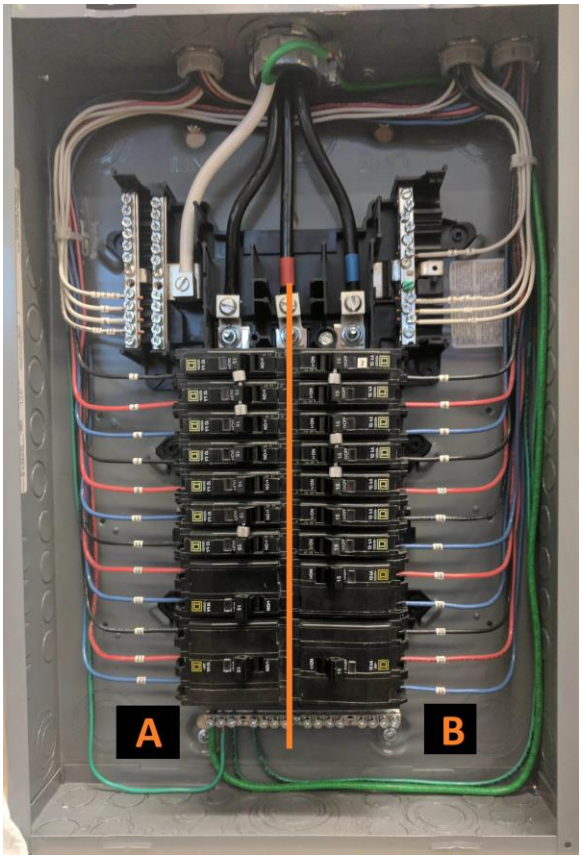


Figure 217 – Typical U.S.A Home Circuit Breaker Panel

I believe in this case, that there is no easy way for the high frequency AV2 data to get from one (A) side of the panel to the other (B) side. The only thing connecting both sides of your electrical box is your (far away) power transformer, which does not pass-through high frequencies.

Every house's wiring is different. You may be able to inspect your electrical panel and determine if the particular outlets / endpoints you desire-to-connect-together are both on the same side of the panel. About the only (practical) thing you can do, is to purchase a pair of EOP units and actually try them out. A popular series of EOP units are manufactured by Tp-Link and are the AV600 series. These appear to be under $100 US a set. You will need EOP adapters which support 802.1Q, if you will be using them to connect Access Points to your ER-X.

I have heard of people swapping an electrical-panel circuit/wire on the "A" side with a circuit/wire on the "B" side, to achieve a suitable link. If you envision this, you should use a certified electrician to swap those circuits/wires.

One method of testing the EOP link-speed is to run an internet "speed test" from a suitable device (e.g laptop) plugged into the far-adapter, with the near-adapter plugged-into your ER-X router. Your ISP up / down internet rate may be a limiting factor for this result, since the far end of this test, is actually the internet.

More tech-savvy people might instead run iperf3 from two PC(s) / laptop(s) with the desired EOP link in-between them. Iperf3 is the internal protocol which used within internet speed tests. Do not attempt to run iper3 *on* the ER-X, as it is not designed for this task.

Appendix C. Original Unifi Installation Script for Raspberry Pi

This is the community posting that I (originally) referenced to install the UniFi software onto a Raspberry Pi:

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

> @SmokingCrop (the Author) has provided an update to the above posting / URL, made about 5/27/2023:
>
> THIS APPEARS TO NO LONGER WORK ON A RASPBERRY PI 4 WITH THE LATEST UPDATES.
> PLEASE TRY THIS SCRIPT INSTEAD IF YOU ARE ON A RASPBERRY PI:
> 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
> I WILL NOT UPDATE ~~THIS~~ [MY] SCRIPT ANYMORE, IF IT STOPS WORKING, [THEN] IT STOPS WORKING.
> You can use the posting information as a reference as it still has useful information to learn about setting it up.

I booted my Raspberry-Pi-based Unifi test-installation, which was used during the writing of the Second Edition, i.e. version UniFi 7.3.76. I issued Raspberry Pi commands of `cat /etc/os-release` and `cat /etc/rpi-issue` and determined that Raspbian 11 (bullseye) of 2022-09-22 was used.

To re-create this installation, I found and downloaded the raspios_armhf-2022-09-26 OS release from:
https://downloads.raspberrypi.org/raspios_armhf/images/
Using the Raspberry Pi Imager tool, I selected "`CHOOSE OS`" then "`Use custom`" to burn a micro-SC card with the above downloaded (now-earlier) OS release. I booted the OS and then localized it to my location. Running the below script, successfully re-created the 7.3.76 installation.

This posting has two install scripts; one for UniFi, the second installs UniFi and Pi-hole. I have not gotten to the Pi-Hole portion, yet.

Here is the main command (captured from the above link) to install UniFi Software onto a Raspberry Pi, 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
```

Cache of script(s), captured on 2023_01_30, when UniFi was version 7.3.76 from https://github.com/SmokingCrop/UniFi

install-unifi-pihole-English.sh

```
#! /bin/bash

Colour='\033[1;31m'
less='\033[0m'
requiredver='7.3.76'

echo -e "${Colour}By using this script, you'll update the system, install the stable UniFi controller
of your choice and install Pi-hole.\nUse CTRL+C to cancel the script\n\n${less}"
read -p "Please enter a STABLE version of your choice (e.g: 7.2.95) or press enter for the latest
stable version 7.3.76: " version

if [[ -z "$version" ]]; then
    version='7.3.76'
fi

echo -e "${Colour}\n\nAdding the Raspbian Stretch sources.list for MongoDB compatability.\n\n${less}"
echo 'deb http://archive.raspbian.org/raspbian stretch main contrib non-free rpi' | sudo tee
/etc/apt/sources.list.d/raspbian_stretch_for_mongodb.list

echo -e "${Colour}\n\nThe system will now upgrade all the software and firmware, as well as clean up
old/unused packages.\n\n${less}"
sudo apt update && sudo apt full-upgrade -y && sudo apt autoremove -y && sudo apt-get autoclean -y

echo -e "${Colour}\n\nThe UniFi controller with version $version is downloading now.\n\n${less}"
wget https://dl.ui.com/unifi/$version/unifi_sysvinit_all.deb -O unifi_$version\_sysvinit_all.deb

echo -e "${Colour}\n\nChecking if Java 11 is required for this version...\n\n${less}"
if [ "$(printf '%s\n' "$requiredver" "$version" | sort -V | head -n1)" = "$requiredver" ];
 then
    echo -e "${Colour}\n\nJava 11 is required. Checking if Java 11 is installed...\n\n${less}"
    if [ $(dpkg-query -W -f='${Status}' openjdk-11-jre-headless 2>/dev/null | grep -c "ok installed")
-eq 0 ];
    then
        echo -e "${Colour}\n\nJava 11 wasn't found, installing now...\n\n${less}"
        sudo apt install openjdk-11-jre-headless -y
    fi
 else
     echo -e "${Colour}\n\nJava 8 is required for the chosen version. Installing now.\n\n${less}"
     sudo apt install openjdk-8-jre-headless jsvc libcommons-daemon-java -y
 fi

echo -e "${Colour}\n\nMongoDB will now be installed as it's a dependency of UniFi.\n\n${less}"
sudo apt install mongodb-server mongodb-clients -y

echo -e "${Colour}\n\nThe UniFi controller will be installed now.\n\n${less}"
sudo dpkg -i unifi_$version\_sysvinit_all.deb; sudo apt install -f -y

if [[ -z "$1" ]] ; then
    echo -e "${Colour}\n\nPi-hole will be installed now.\nThe initial configuration is
interactive.\n\n${less}"
    curl -sSL https://install.pi-hole.net | bash

    echo -e "${Colour}\n\nOne more step is changing the password for the web interface of the Pi-
hole.\n\n${less}"
    pihole -a -p
fi

echo -e "${Colour}\n\nTo finish the installation, a reboot is required. Starting a reboot in 3
seconds.\n\n${less}"
sleep 3
echo -e "${Colour}\nRestarting the Raspberry Pi now.\n${less}"
sudo reboot now
```

update-unifi-pihole-English.sh

```
#! /bin/bash

Colour='\033[1;31m'
less='\033[0m'
requiredver='7.3.76'

echo -e "${Colour}By using this script you will UPGRADE your system, the UniFi Controller and Pi-
hole.\n${less}"
read -p "Please enter a STABLE version of your choice (e.g: 7.2.95) or press enter for the latest
stable version 7.3.76: " version

if [[ -z "$version" ]]; then
    version='7.3.76'
fi
echo -e "${Colour}\n\nThe system will now upgrade all the software and firmware, as well as clean
up old/unused packages.\n\n${less}"
sudo apt update && sudo apt full-upgrade -y && sudo apt autoremove -y && sudo apt-get autoclean -y

echo -e "${Colour}\n\nStopping the UniFi service...\n\n${less}"
sudo service unifi stop

echo -e "${Colour}\n\nChecking if Java 11 is required for this version...\n\n${less}"
if [ "$(printf '%s\n' "$requiredver" "$version" | sort -V | head -n1)" = "$requiredver" ];
 then
       echo -e "${Colour}\n\nJava 11 is required. Checking if Java 8 is still
installed...\n\n${less}"
    if [ $(dpkg-query -W -f='${Status}' openjdk-8-jre-headless 2>/dev/null | grep -c "ok
installed") -eq 1 ];
    then
      echo -e "${Colour}\n\nRemoving Java 8...\n\n${less}"
      sudo apt purge openjdk-8-jre-headless -y && sudo apt autoremove -y
    fi

       echo -e "${Colour}\n\nChecking if Java 11 automatically got installed after deleting Java
8...\n\n${less}"
    if [ $(dpkg-query -W -f='${Status}' openjdk-11-jre-headless 2>/dev/null | grep -c "ok
installed") -eq 0 ];
    then
       echo -e "${Colour}\n\nJava 11 wasn't found, installing now...\n\n${less}"
      sudo apt install openjdk-11-jre-headless -y
    fi
 else
     echo -e "${Colour}\n\nJava 11 isn't required yet for the chosen version.\n\n${less}"
 fi

echo -e "${Colour}\n\nThe UniFi controller (version $version) will now be downloaded.\n\n${less}"
wget https://dl.ui.com/unifi/$version/unifi_sysvinit_all.deb -O unifi_$version\_sysvinit_all.deb
echo -e "${Colour}\n\nThe UniFi controller will now be upgraded.\n\n${less}"
sudo dpkg -i unifi_$version\_sysvinit_all.deb

if hash pihole 2>/dev/null; then
    echo -e "${Colour}\n\nPi-hole will now be upgraded.\n\n${less}"
        pihole -up
fi
```