Home-Network Implementation

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

By Mike Potts

1. Overview

This guide will attempt to show users how to setup 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 X (about $50 USD when this guide was written)
- Ubiquiti AP-AC-LR Wi-Fi Access Point (about $100 USD when this guide was written).

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

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

The Wired Home Network and Wi-Fi Home Network are actually the same Network. Your naming and use may / can be different. See Figure 1 - Overview Diagram.

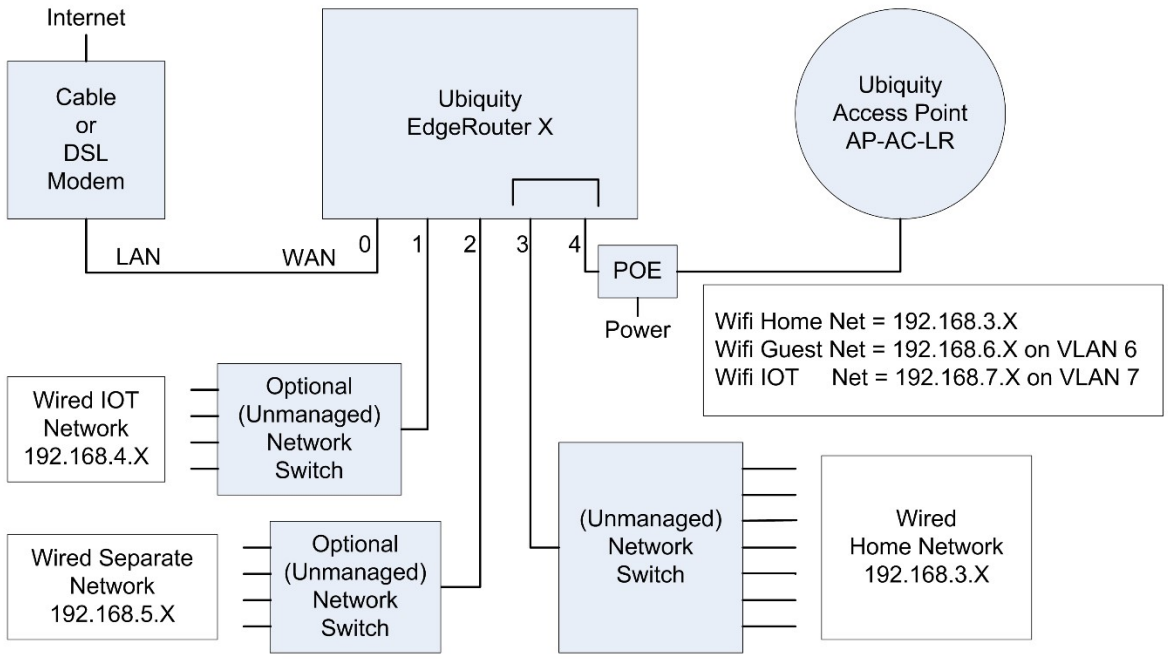

Figure 1 - Overview Diagram

With this setup, the Home Network (both Wired and Wi-Fi) is able to initiate connections / communicate with devices on both the Wired IOT Network and the Wi-Fi IOT Network. Devices on the IOT Networks are NOT able to initiate connections / independently communicate to the Home Network. No other Networks can communicate with the Wired Separate Network.

2. Disclaimer

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

3. EdgeRouter IP Address Use

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

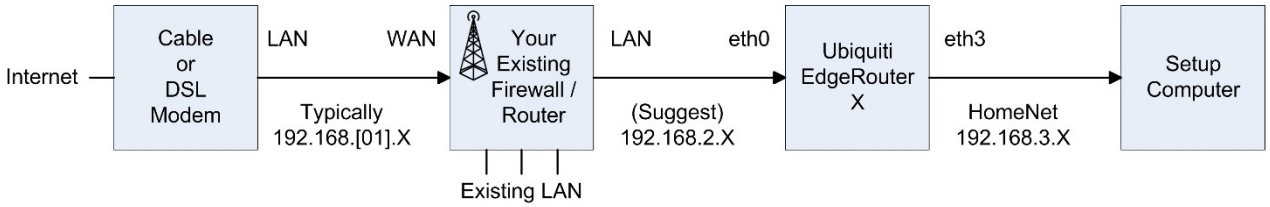

Figure 2 - EdgeRouter Configuration Setup

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

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

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

4. Acquire EdgeRouter Documentation

On your computer, which will be used to setup the EdgeRouter X, download the newest documentation from:
https://www.ubnt.com/download/edgemax/edgerouter-x/er-x
There are both a User's Guide and a Quick Start Guide.

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

5. Web Resources

EdgeMax	https://help.ubnt.com/hc/en-us/categories/200321064-EdgeMAX
EdgeMax FAQ	https://community.ubnt.com/t5/tkb/allarticlesprintpage/tkb-id/EdgeMAX_FAQ
Community	https://community.ubnt.com/t5/EdgeMAX/bd-p/EdgeMAX
Unofficial	https://www.reddit.com/r/Ubiquiti/

Here are some more references:
https://help.ubnt.com/hc/en-us/articles/115002531728-EdgeRouter-Beginners-Guide-to-EdgeRouter
http://www.guruadvisor.net/en/networking/321-edgerouter-x-tiny-but-full-of-resources

6. Initial EdgeRouter Hardware Setup

Configure the setup computer's Ethernet jack as having a fixed IP address of 192.168.1.X (where X is 2 to 254), and a netmask of 255.255.255.0. There are many tutorials available on the internet which shows how to configure a computer's Ethernet port to use a fixed IP address. One way for a Windows 10 computer is:

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

See Figure 3 – Windows 10 Ethernet Address Setup.

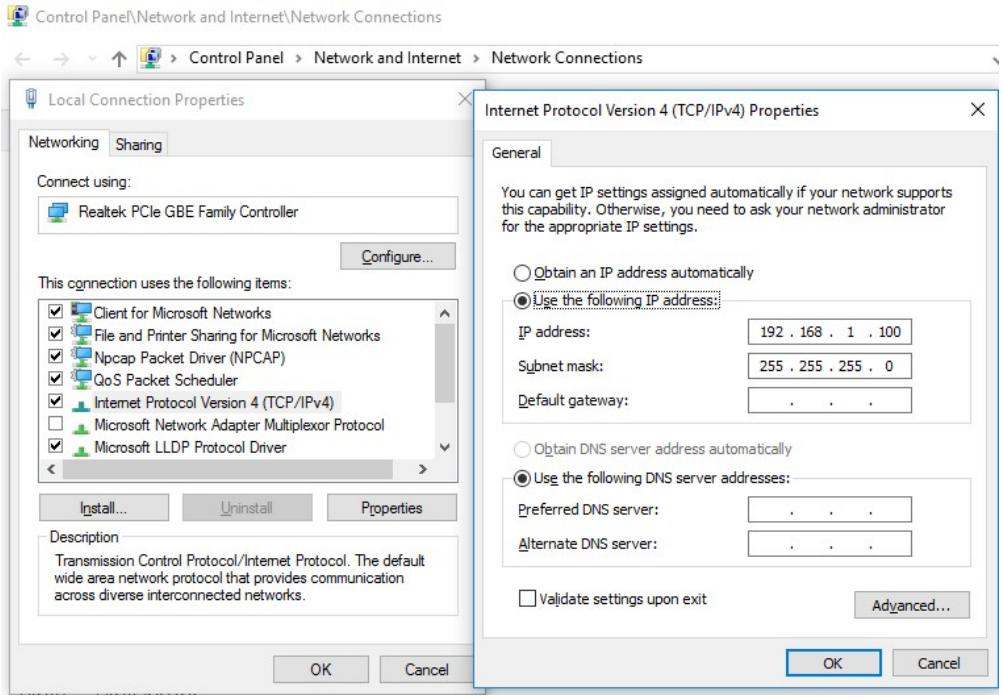

Figure 3 – Windows 10 Ethernet Address Setup

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

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

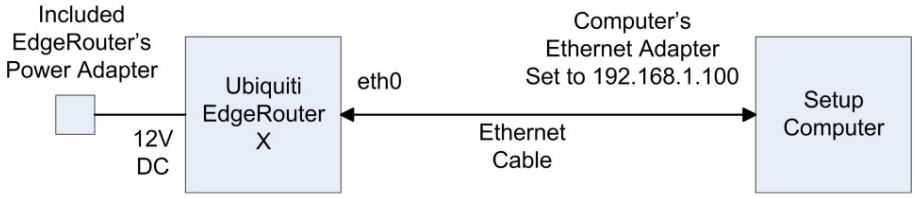

Figure 4 – Initial EdgeRouter Hardware Setup

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

7. Initial EdgeRouter Login

Wait about three minutes for the EdgeRouter to boot up, then open a web browser of your choice on your setup computer and enter https://192.168.1.1 into the address field. The browser may issue a security warning. You will need to "Continue to this web site" or equivalent. The exact prompts and responses vary by browser. See Figure 5 – IE Security Certificate Example.

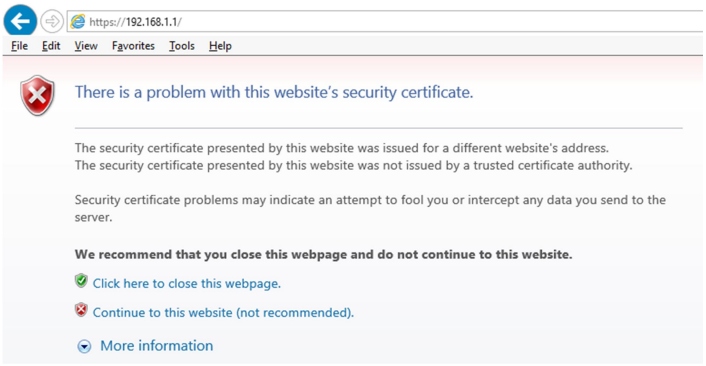

Figure 5 – IE Security Certificate Example

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

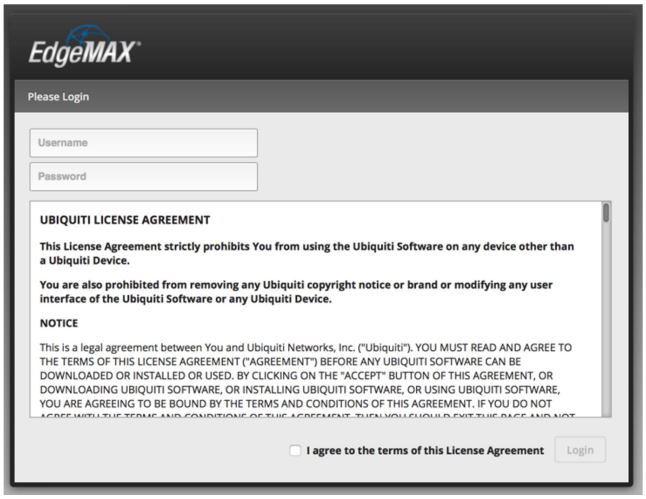

Figure 6 – Ubiquiti License Agreement Dialog

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

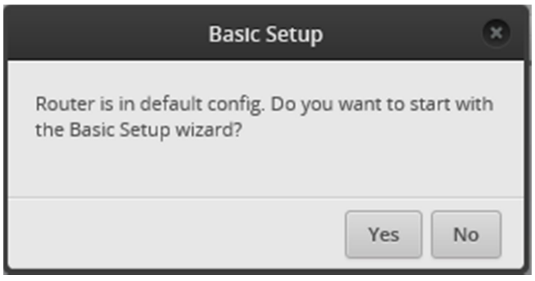

Figure 7 – Basic Setup Question

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

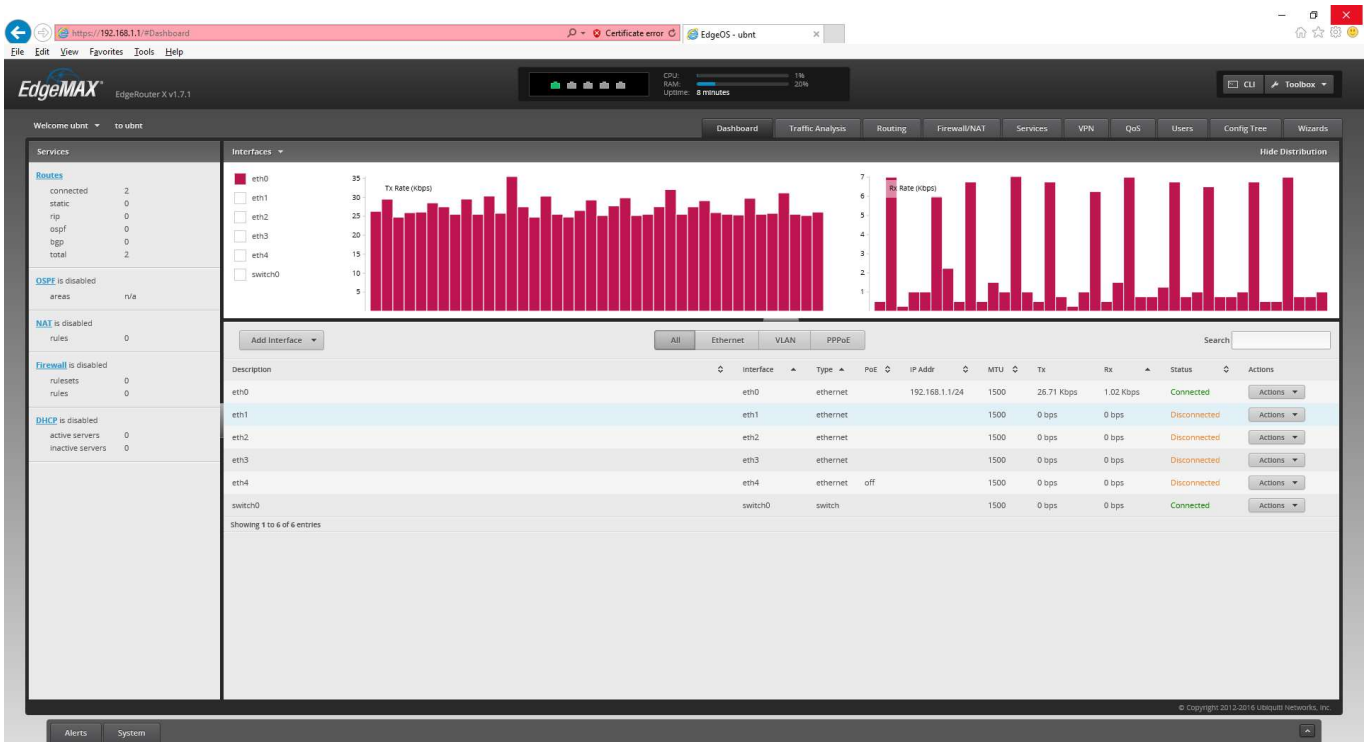

Figure 8 – Initial Dashboard Screen

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

8. Update EdgeRouter Firmware

On your setup computer, download the newest firmware from:
https://www.ubnt.com/download/edgemax/edgerouter-x/er-x

When this guide was initially written, the firmware version was at:
"EdgeRouter ER-X/ER-X-SFP/EP-R6: Firmware v1.9.0".
During the writing of this document, the firmware then moved to
"EdgeRouter ER-X/ER-X-SFP/EP-R6: Firmware v1.9.1".

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.

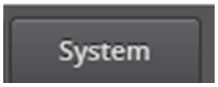

Figure 9 – System Button

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

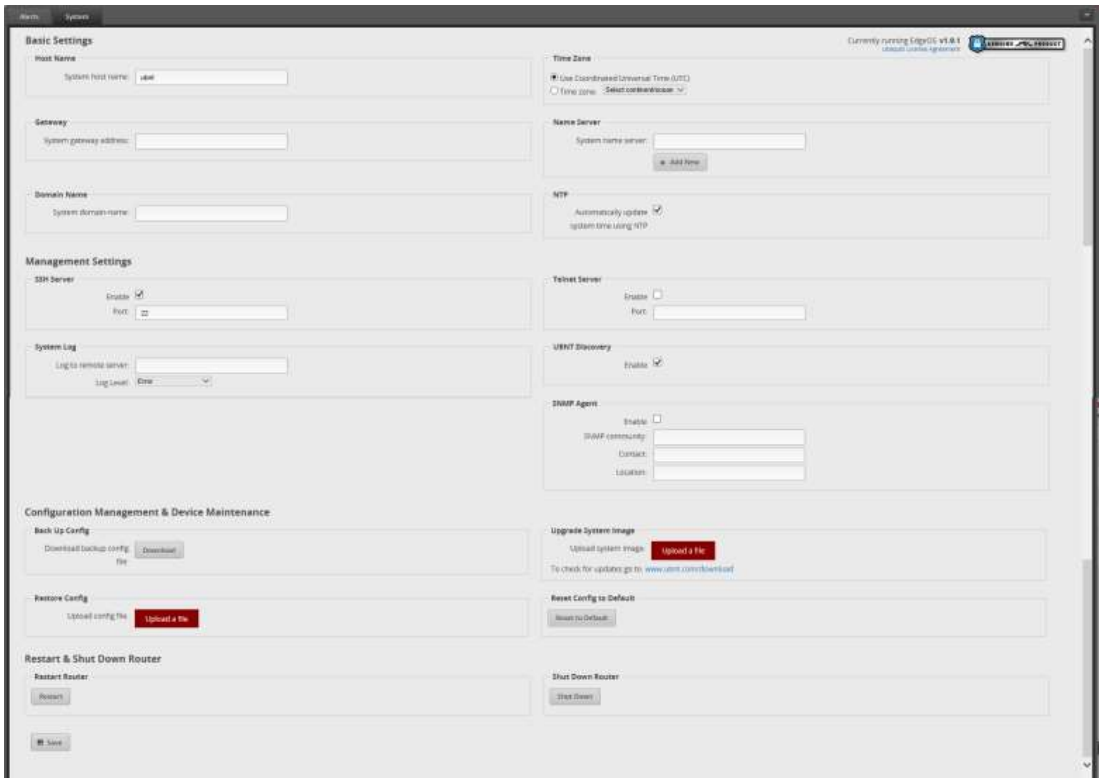

Figure 10 – System Pop-up Screen

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

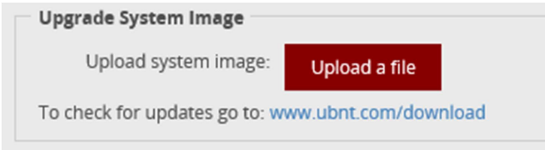

Figure 11 – Upgrade System Image

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

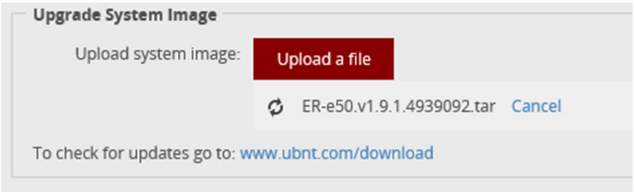

Figure 12 – Upload a file

You will eventually be asked if you want to re-boot the EdgeRouter. Press the “Reboot” button. You will then be asked to confirm the re-boot, click on the “Yes, I’m sure” button. See Figure 13 – Upgrade Complete Dialog.

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

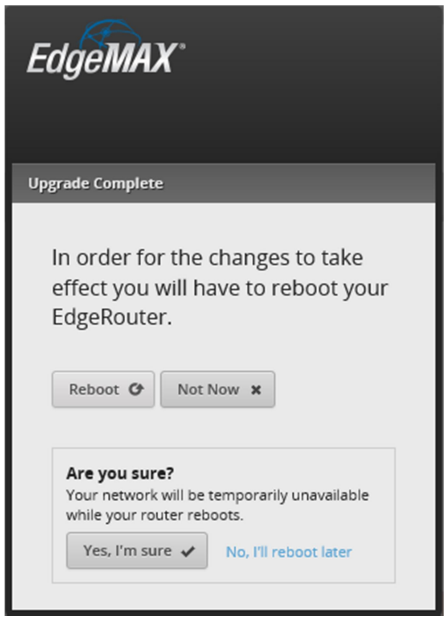

Figure 13 – Upgrade Complete Dialog

Figure 14 – Reboot Process

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

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

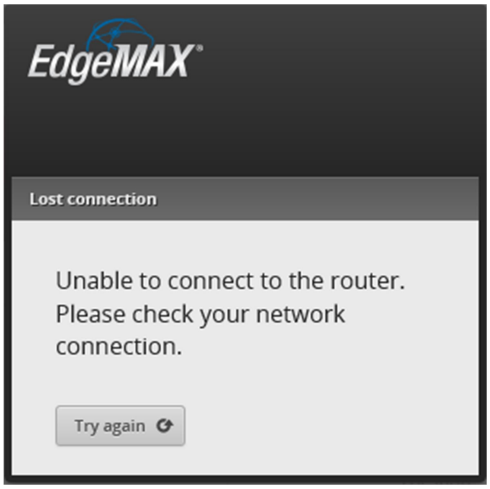

Figure 15 – Lost Connection Dialog

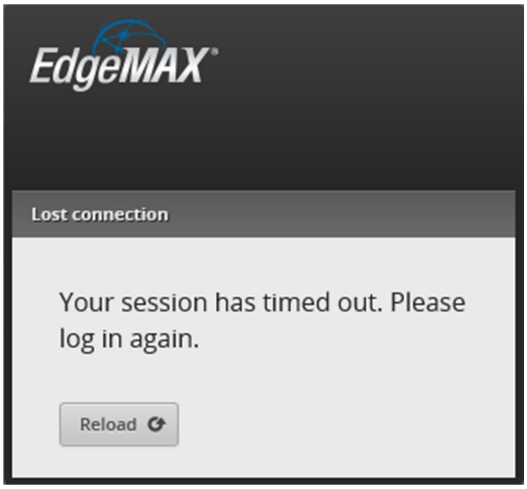

Figure 16 – Timed-Out Dialog

Press the Reload button.

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

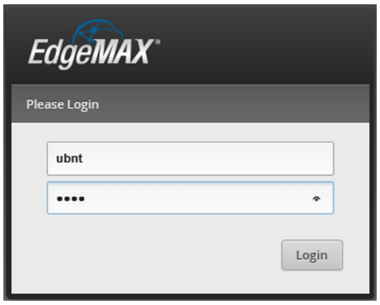

Figure 17 – Login Dialog

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

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

Figure 18 – Example EdgeRouter Version

9. EdgeRouter Wizard

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

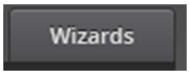

Figure 19 – Wizards Button

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

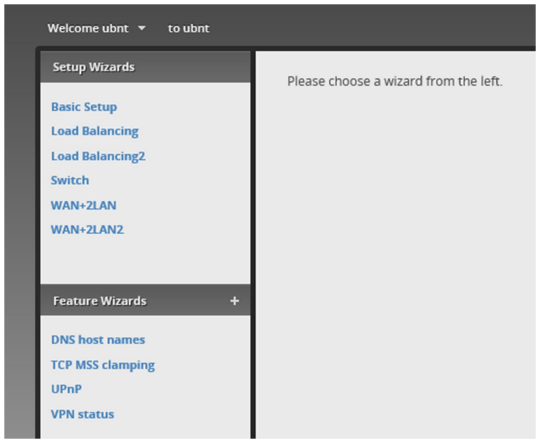

Figure 20 – Wizard Screen Portion

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

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

In the “Internet Port” section:

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

In the next (unlabeled) section:

One LAN:	UN-Checked	(Use only one LAN)

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

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

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

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

If your internet provider uses something other than DHCP (i.e. IP address provided from your cable / dsl modem), you will need to select “Static IP” or “PPPoE”, and then configure those settings accordingly.

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

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

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

Press “Apply” at the bottom of the screen.

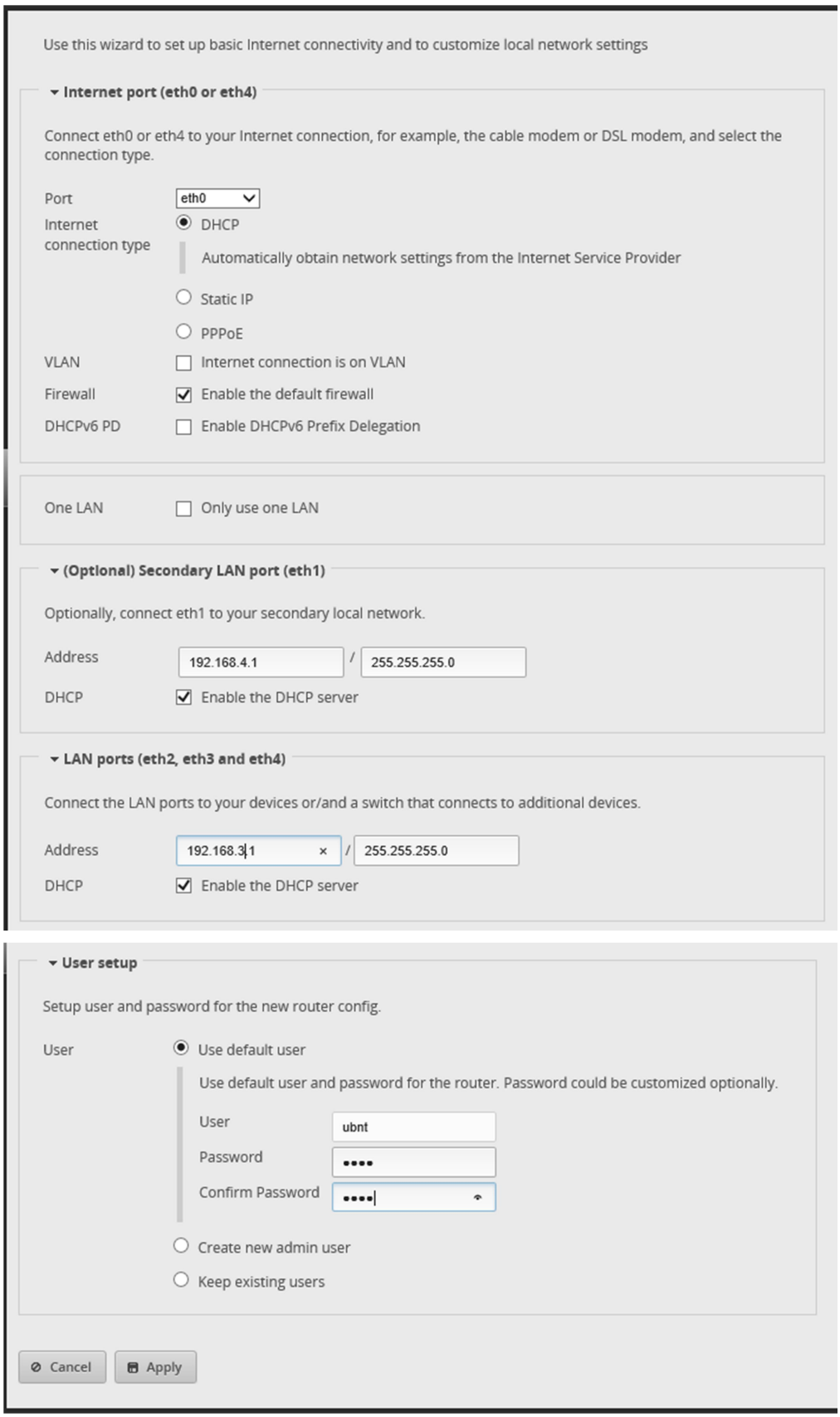

Figure 21 – Wan+2LAN2 Dialog

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

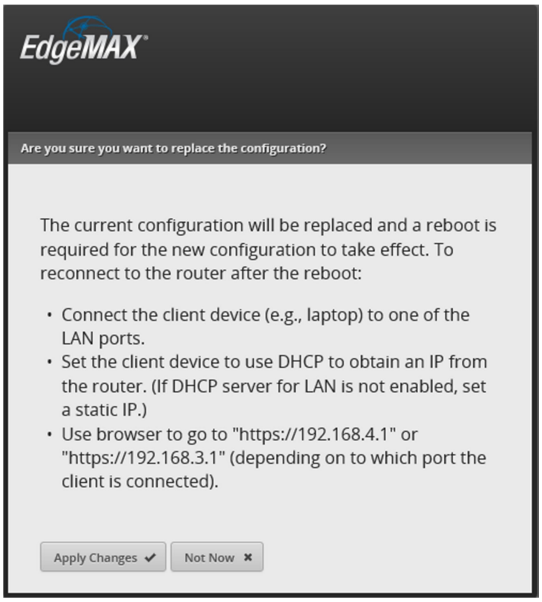

Figure 22 – Replace Configuration

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

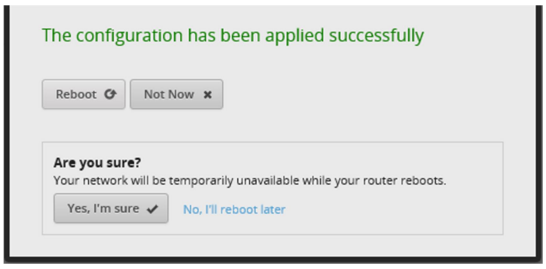

Figure 23 – Reboot into New Configuration

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

Disconnect your setup computer’s Ethernet jack from the EdgeRouter’s eth0 connection. Re-configure your setup computer’s Ethernet port back to using DHCP. Again, there are many tutorials available on the internet which shows how to configure a computer’s Ethernet jack to use DHCP. Reference section 6 - Initial EdgeRouter Hardware Setup, but instead choose “Obtain an IP address automatically”. Also reference Figure 3 – Windows 10 Ethernet Address Setup.

10. EdgeRouter Re-Connection

Ensure that your existing router's LAN ports are not using any of the addresses utilized by the EdgeRouter, i.e. not using 192.168.3.0 through 192.168.7.255. Reference section "3 - EdgeRouter IP Address Use". Connect the EdgeRouter's eth0 port into your existing router's LAN port with a standard Ethernet cable. Connect your setup computers Ethernet port (now re-configured for DHCP) into the EdgeRouter's eth3 port. See Figure 2 - EdgeRouter Configuration Setup.

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

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

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

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

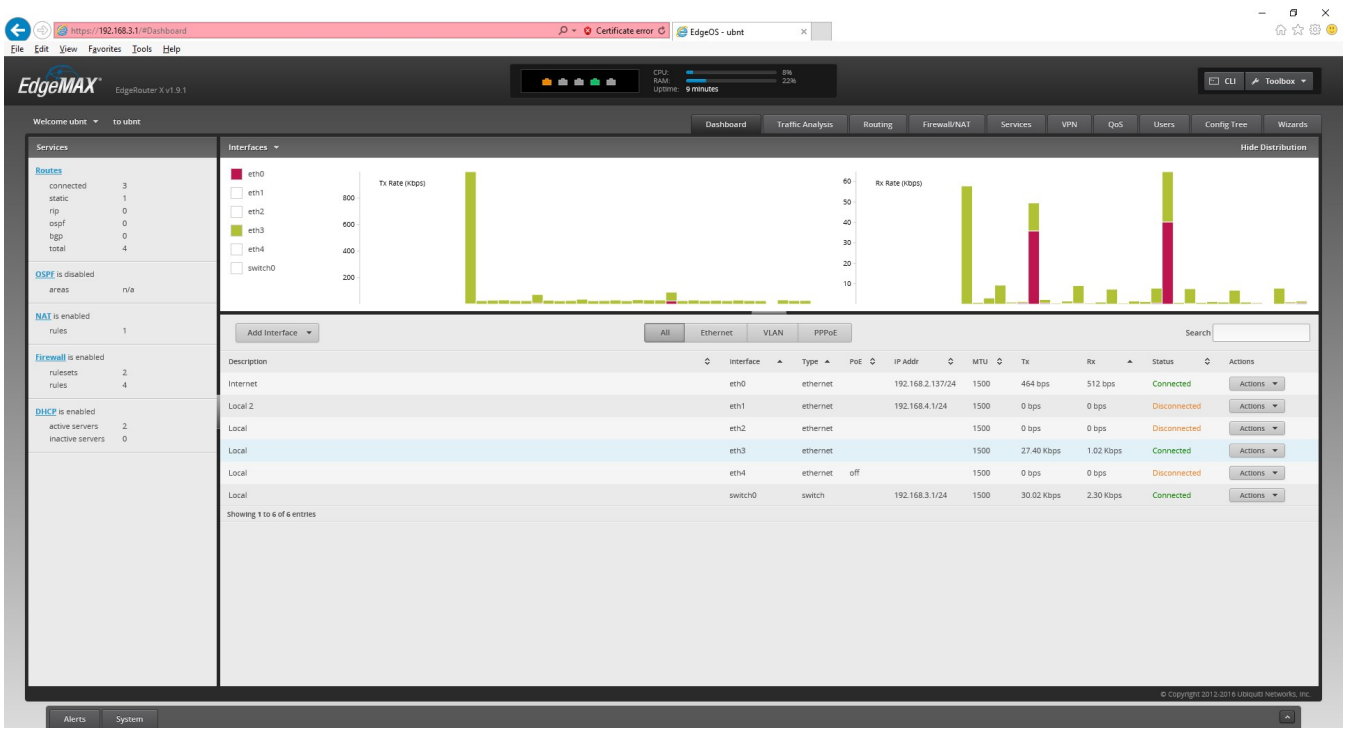

Figure 24 – Dashboard Screen

11. Network Naming

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

Network Name	IP Address Range	VLAN	Address Group Term
Home Network	192.168.3.X	No	HOME_GROUP
Wired IOT Network	192.168.4.X	No	WIRED_IOT_GROUP
Wired Separate Network	192.168.5.X	No	WIRED_SEPARATE_GROUP
Wi-Fi Guest Network	192.168.6.X	6	WIFI_GUEST_GROUP
Wi-Fi IOT Network	192.168.7.X	7	WIFI_IOT_GROUP

Table 1 - Table of Networks

Some of these Networks are on a Virtual LAN (VLAN). VLANs provide the ability for separate network data to be carried over shared Ethernet cables. Data “tagged” as belonging to a VLAN cannot interact with non-VLAN data (trunk data) or with other VLAN data.

When VLANs are used, all devices involved with this data needs to be VLAN aware. Any network switches carrying VLAN traffic will need to be managed Level 2 switches, i.e. adhering to IEEE 802.1Q.

Note that the only VLAN traffic shown in Table 1 - Table of Networks, is involved with the Wi-Fi Guest Network and the Wi-Fi IOT Network. The Ubiquiti AP-AC-LR access point is VLAN aware. Eventually the access point will be plugged-into the EdgeRouter’s eth4 interface, so VLAN data will be able to be carried between them. This Wi-Fi VLAN data does NOT need to flow to devices on the Wired Home Network. Therefore the network switch attached to the EdgeRouter’s eth3 interface can be (a cheaper) unmanaged switch. Reference Figure 1 - Overview Diagram. If they are needed, the network switches attached to the EdgeRouter’s eth1 and/or eth2 interfaces can also be (cheaper) unmanaged switches.

Each Network is also customizable as to provided 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

12. 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 much GUI screenshots are used, and they are typically posted only by novices.

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

Figure 25 – CLI Button

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

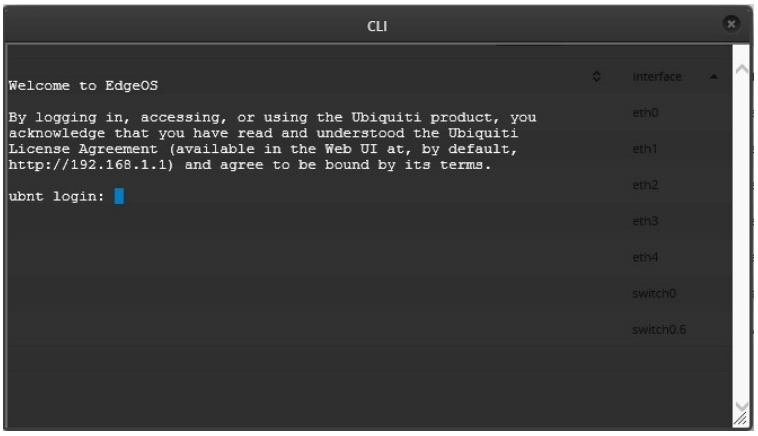

Figure 26 – Initial CLI Window

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

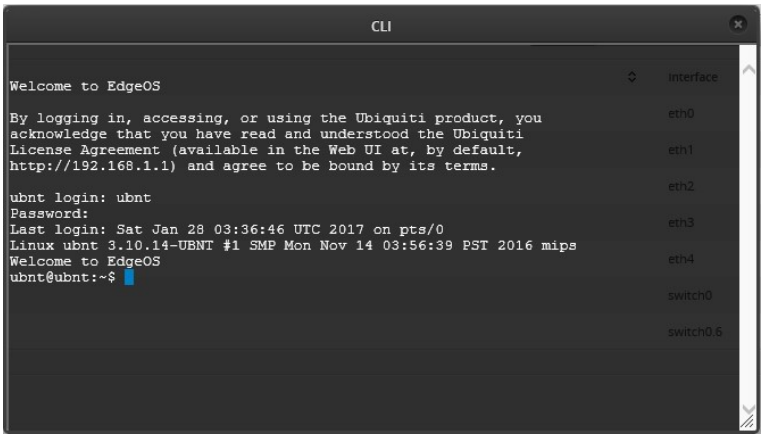

Figure 27 – Logged-In CLI Window

CLI commands are typically divided into "configuration" commands and non-configuration commands The CLI interface will only accept configuration commands when the "configuration" command has previously been entered. The "exit" command is used to leave configuration mode and return to normal mode.

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

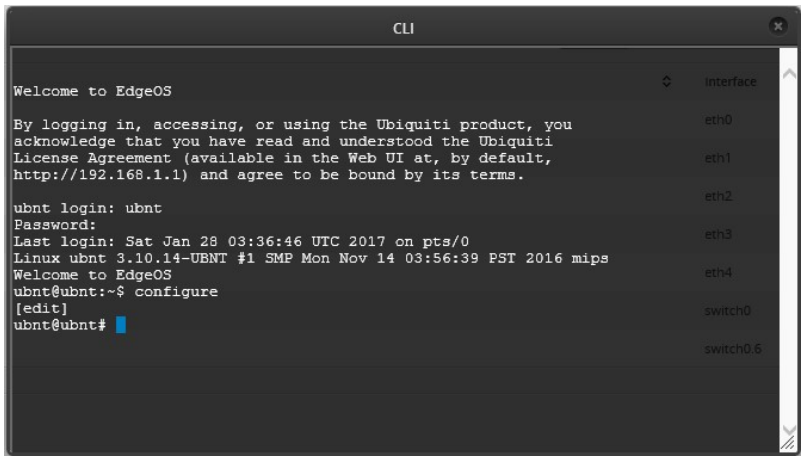

Figure 28 – Configure CLI Window

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

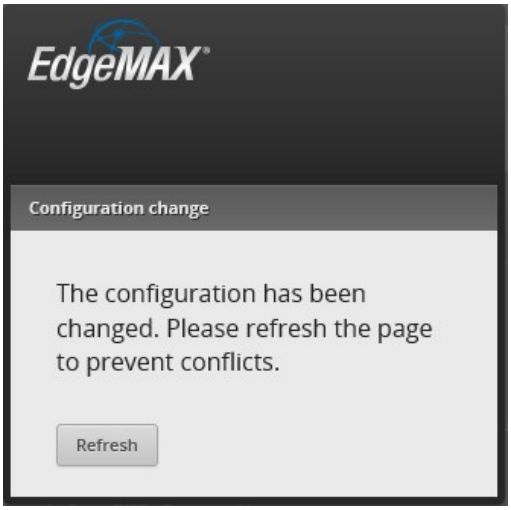

Figure 29 – Configuration Change

You can also use a popular Windows program, called putty.exe, to Secure Shell (SSH) into the EdgeRouter, and then issue CLI commands. Linux users should already be familiar with how to use SSH.

Here are some CLI references:

https://dl.ubnt.com/guides/edgemax/EdgeSwitch_CLI_Command_Reference_UG.pdf
https://community.ubnt.com/t5/EdgeMAX/EdgeOS-CLI-Primer-part-1/td-p/285388
https://community.ubnt.com/t5/EdgeMAX-CLI-Basics-Knowledge/tkb-p/CLI_Basics@tkb

13. EdgeRouter Config Tree

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

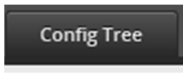

Figure 30 – Config Tree Button

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

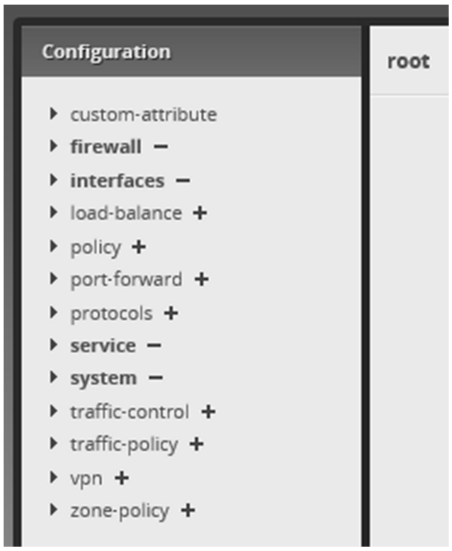

Figure 31 – Config Tree Initial Screen

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

14. 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, that multiple commands were issued.

See Figure 32 – Example of Multiple Config Tree Commands.

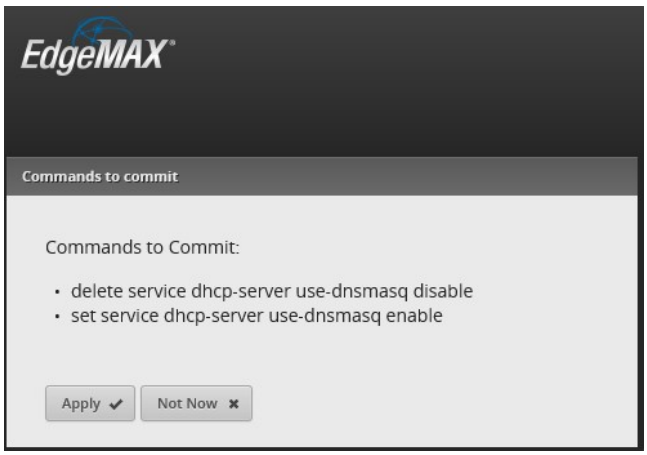

Figure 32 – Example of Multiple Config Tree Commands

Dnsmasq was incomplete as of firmware 1.9.0 and had an additional bug added in firmware 1.9.1. It sounds like dnsmasq would be worth it, but I am waiting until the next firmware release.

Here is a recent post of (some of the) EdgeMAX (EdgeRouter's firmware) Known Issues:
https://community.ubnt.com/t5/EdgeMAX/Known-Issues-of-EdgeMax-Series/td-p/1805816

15. EdgeRouter Backup / Configuration Files

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

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

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

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

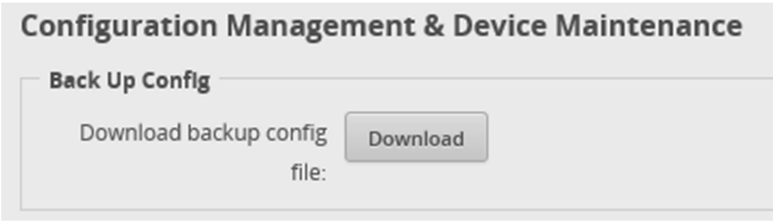

Figure 33 – Back Up Config Download Button

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

Another way to obtain a relevant portion of this file is to issue one of the following commands into the Command Line Interface (CLI) window. For information about the CLI, reference section “12 - EdgeRouter Command Line Interface (CLI)”.

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

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

I will try and show portions of this config data 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.

16. Remove eth2 from the EdgeRouter's Internal Switch

In this step, we will manually un-bundle the eth2 interface from the EdgeRouter's internal switch chip. This allows us to provide for an additional Network. The switch chip will remain enabled for eth3 and eth4 interfaces. The eth2 interface will be used as the Wired Separate Network. Later, we will setup firewall rules that will keep this Network isolated from the other Networks.

Press the Dashboard Button. See Figure 34 – Dashboard Button.

Figure 34 – Dashboard Button

On the right side of the Dashboard screen, select switch0's "Actions" button. See Figure 35 – switch0's Action Button.

Figure 35 – switch0's Action Button

A sub-menu will appear, Select "Config" from the menu items. See Figure 36 – switch0 Actions Config.

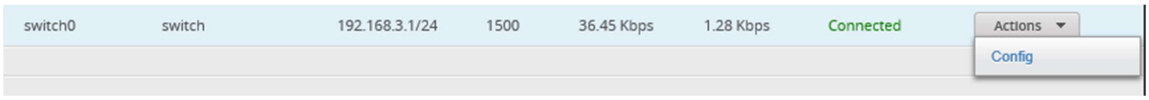

Figure 36 – switch0 Actions Config

You will be presented with the configuration dialog for switch0. See Figure 37 – switch0 Configuration.

Select the VLAN tab. Under the section labeled "Switch Ports", Un-check eth2. See Figure 38 – switch0 Switch Ports.

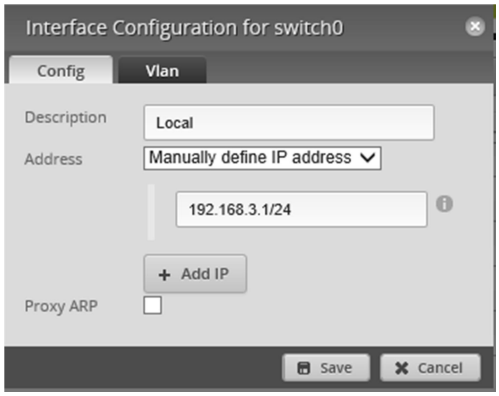

Figure 37 – switch0 Configuration

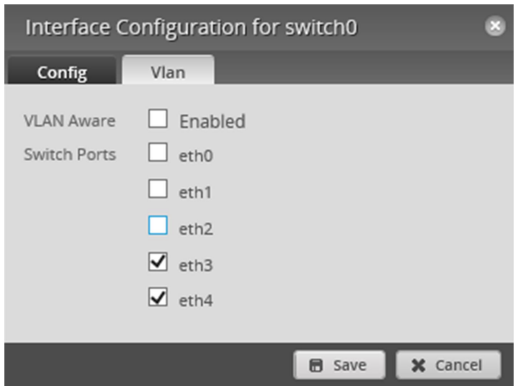

Figure 38 – switch0 Switch Ports

Press "Save". While the EdgeRouter is completing this task, a busy indicator will spin, in the upper right corner of the dialog. See Figure 39 – 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 40 – Finished Checkmark.

Figure 39 – Busy Indicator

Figure 40 – Finished Checkmark

17. Configure EdgeRouter's eth2 IP Addresses

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

On the right side of the Dashboard screen select eth2's "Actions" button. See Figure 41 – eth2's Actions Button.

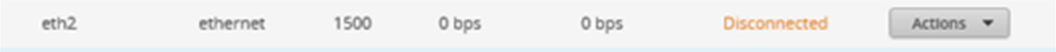

Figure 41 – eth2's Actions Button

A sub-menu will appear, See Figure 42 – Interface Actions.

Figure 42 – Interface Actions

Select "Config". You will be presented with Figure 43 – Configuration for eth2 Dialog.

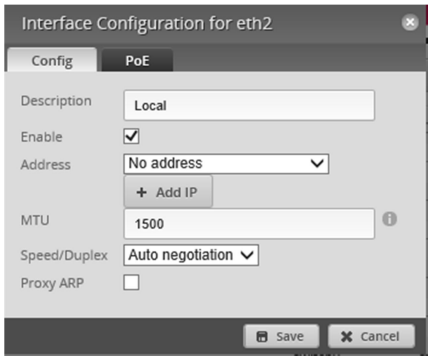

Figure 43 – Configuration for eth2 Dialog

Under the Address selection, choose "Manually define IP address", and enter "192.168.5.1/24" into the address field. See Figure 44 – eth2 Address Dialog.

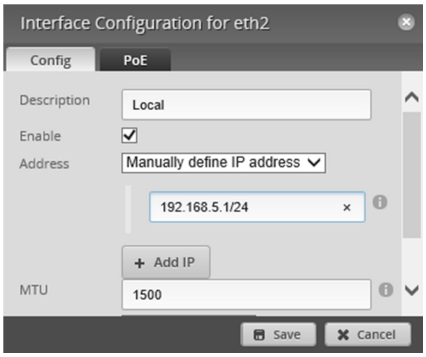

Figure 44 – eth2 Address Dialog

Click the Save button.

18. About DNS settings

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

There are two different DNS packages available within the EdgeRouter. They are ISC (default) and dnsmasq. As of firmware 1.9.0, dnsmasq worked, but would not populate the GUI / Traffic Analysis page. At least one dnsmasq bug was introduced into firmware 1.9.1.

Reference 1.9.0 Release Notes, section" [DHCP server]":
https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-software-release-v1-9-0/ba-p/1643332

New Bug
https://community.ubnt.com/t5/EdgeMAX/EdgeOS-1-9-1-dhcp-server-using-domain-search-rather-than-domain/m-p/1782188

For now, I'm staying with ISC.

Within this guide, I am using Level3 DNS addresses for the Home Network and Separate Network. I am also using / forcing OpenDNS DNS addresses for the IOT and Guest Networks. Change any or all of these addresses to whatever DNS provider / resolver addresses you desire.

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

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

Steve Gibson has another web page which tests the "spoofability" (security) of DNS resolvers. It is at:

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

Here are some alternate DNS resolvers, and additional DNS information pages:

https://en.wikipedia.org/wiki/List_of_managed_DNS_providers
https://dns.norton.com/configureRouter.html,
https://dns.norton.com/faq.html
https://support.opendns.com/hc/en-us/articles/228006047-Generalized-Router-Configuration-Instructions
https://use.opendns.com/#router
https://en.wikipedia.org/wiki/OpenDNS

EdgeRouter DNS References:

https://community.ubnt.com/t5/EdgeMAX/ERL-3-1-9-0-No-DHCP-leases-since-switching-to-DNSMasq/td-p/1644201
https://community.ubnt.com/t5/EdgeMAX/Traffic-Analysis-host-name-resolution/m-p/1774017#M141121
https://github.com/confirm/edgerouter-dnsmasq-updater
https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/

19. System DSN Settings

This step instructs the EdgeRouter to use specific DNS servers to resolve web URLs into IP addresses. These DNS servers are specified under the System widow. The Guest and IOT Networks setup via this guide use different DNS serves, as overridden by their specific DHCP servers.

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

On the system window, find the Name Server Box. See Figure 45 – Initial System Name Server.

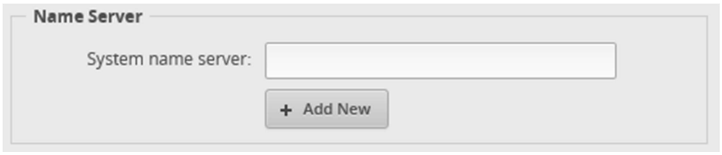

Figure 45 – Initial System Name Server

Fill in the System name server field with your primary DNS server address. I am using a Level3 address of:

209.244.0.3

Then press the “+ Add New” button and enter your secondary DNS server address. I am using a Level3 address of:

209.244.0.4

See Figure 46 – Example System DNS Entries.

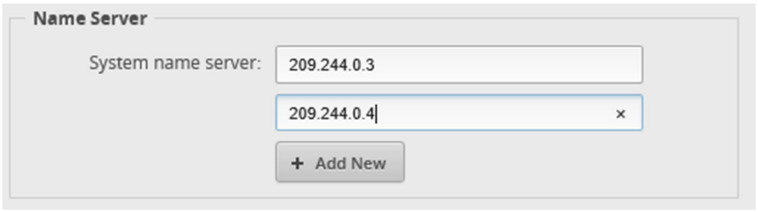

Figure 46 – Example System DNS Entries

Press the Save button near the bottom of the system page.

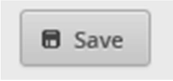

Figure 47 – System Save Button

20. Remove ISP Provided DNS Resolvers

I don't want to depend upon the DNS servers which are provided by my dsl / cable modem. The specific DNS resolver addresses are specified as part 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.

The site http://routersecurity.org/ is a big reason why I moved to this Ubiquiti equipment.

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

Since the DNS changer worm could attack an EdgeRouter, remember to change the EdgeRouter's password.

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 "12 - EdgeRouter Command Line Interface (CLI)")

The following text shows the two Level3 resolvers that were entered into the system page, and an ISP provided resolver, delivered via my existing router, which has an address of 192.168.2.1:

```
-----------------------------------------------
Nameservers configured for DNS forwarding
-----------------------------------------------
192.168.2.1 available via 'dhcp eth0'
209.244.0.3 available via 'system'
209.244.0.4 available via 'system'
```

To remove the ISP provided nameservers, 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
-----------------------------------------------
192.168.2.1 available via 'dhcp eth0'
```

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

QUESTION: Is this the best way to achieve this?

QUESTION: How you restore using the ISP's resolvers?

21. Configure EdgeRouter's eth2 DHCP Server

Now that eth2 has been un-bundled, and has a unique IP subnet assigned to it, we need to provide a DHCP server on this port. Near the top of the screen select the "Services" button. See Figure 48 – Services Button.

Figure 48 – Services Button

Ensure that the "DHCP Server" tab is selected. See Figure 49 – DHCP Server Screen.

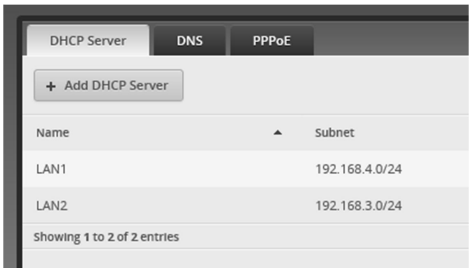

Figure 49 – DHCP Server Screen.

Note that I am using Level 3 DNS resolver addresses for DNS1 and DNS2 (below). You can change these to providers of your choice. If you change them here, you will also need to manually modify some firewall / NAT rules, presented later within this guide.

Click on the "+ Add DHCP Server" button. You will be presented with a Create DHCP Server dialog. See Figure 50 – Create eth2 DHCP Server Screen. Fill in the form as follows:

DHCP Name:	SecureNetDHCP
Subnet:	192.168.5.0/24
Range Start:	192.168.5.38
Range Stop:	192.168.5.243
Router:	192.168.5.1
DNS 1:	209.244.0.3
DNS 2:	209.244.0.4
Enable:	CHECKED

Click "Save".

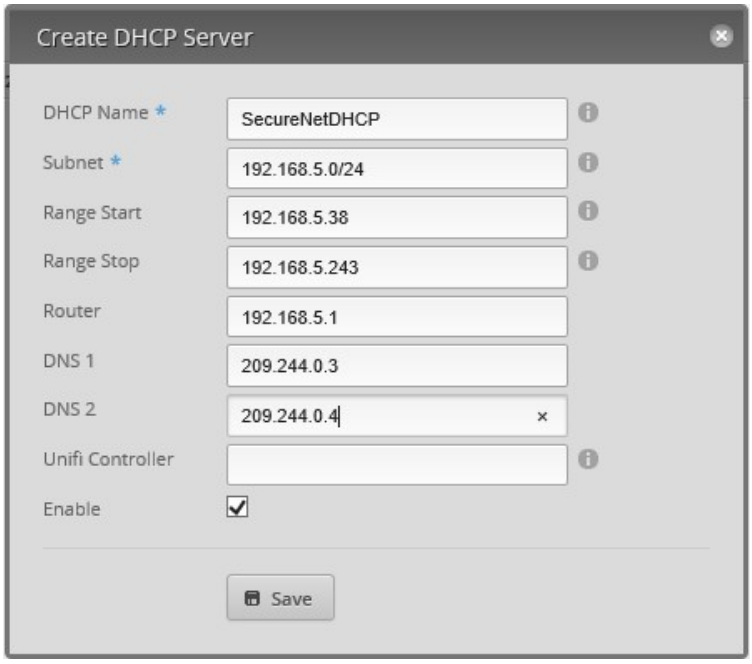

Figure 50 – Create eth2 DHCP Server Screen.

I used the same range start and range stop values (38 and 253) that the wan+2lan2 wizard used within the DHCP servers for LAN1 and LAN2.

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

22. Configure EdgeRouter's Time Zone

Near the top of the screen select the "Services" button. Reference Figure 48 – Services Button. Find the section titled Time Zone and configure the data in these fields according to the time zone you are in, unless you want your router to remain in UTC. See Figure 51 – Time Zone.

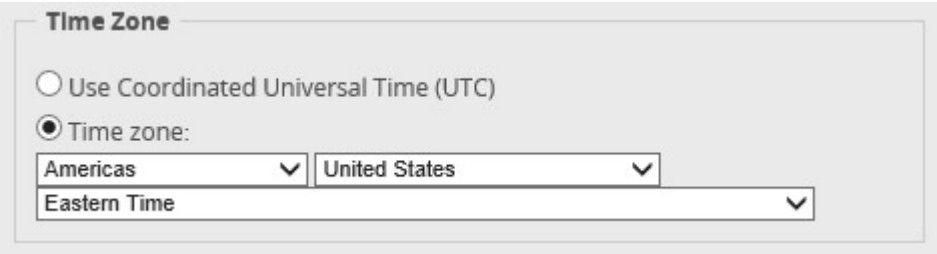

Figure 51 – Time Zone

23. Add eth2 to DNS Server

Press the “Services” button, near the top right of the window. Reference Figure 48 – Services Button. Ensure that the “DNS” Tab is selected. See Figure 52 – DNS Tab.

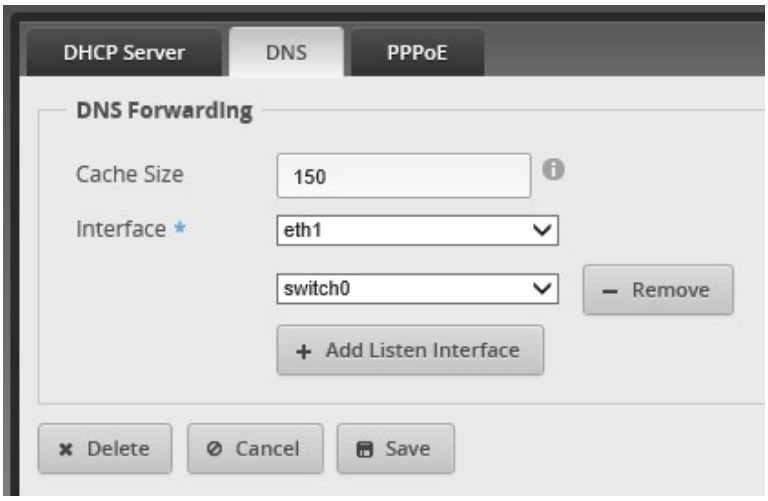

Figure 52 – DNS Tab.

Press the “+ Add Listen Interface” button, which is inside the DNS forwarding section, and select “eth2” from the selection box. See Figure 53 – Add eth2 to DNS. Press “Save”.

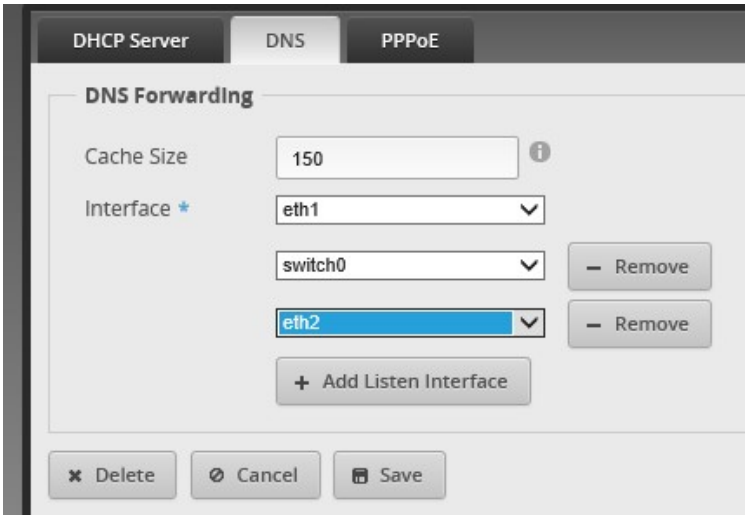

Figure 53 – Add eth2 to DNS.

24. Add VLAN Networks to the EdgeRouter

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

Press the Dashboard button near the top of the Screen. Reference Figure 34 – Dashboard Button. On the upper left side of the Dashboard screen select the Add Interface button. See Figure 54 – Add Interface Button

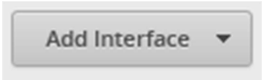

Figure 54 – Add Interface Button

The Add Interface menu will appear. Select "Add VLAN". See Figure 55 – Add Interface Menu

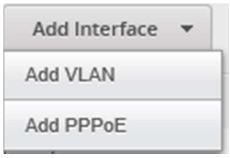

Figure 55 – Add Interface Menu

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

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

The AC-AP-LR access point will eventually be connected to the eth4 interface. The eth3 and eth4 interfaces are internally using the switch0 chip. Therefore, this VLAN needs to be attached to switch0, not to eth3 or to eth4. See Figure 56 – Create New VLAN Example. Press the Save button.

Figure 56 – Create New VLAN Example

Repeat these steps for adding a VLAN the Wi-Fi IOT Network. Fill in the information as follows:

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

There are the relevant sections from the backup file:

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

25. Add DHCP Servers to the VLANs

Following the directions which are in the section titled “21 - Configure EdgeRouter’s eth2 DHCP Server”, add DHCP servers for the two VLANs that were just created. Note that I am using Open DNS servers for these networks. If you change them here, you will also need to manually modify some firewall / NAT rules, presented later within this guide.

The information for VLAN 6, is as follows:

DHCP Name:	WifiGuestDHCP
Subnet:	192.168.6.0/24
Range Start:	192.168.6.38
Range Stop:	192.168.6.243
Router:	192.168.6.1
DNS 1:	208.67.222.222
DNS 2:	208.67.220.220
Enable:	CHECKED

The information for VLAN 7, is as follows:

DHCP Name:	WifiIotDHCP
Subnet:	192.168.7.0/24
Range Start:	192.168.7.38
Range Stop:	192.168.7.243
Router:	192.168.7.1
DNS 1:	208.67.222.222
DNS 2:	208.67.220.220
Enable:	CHECKED

You should now have five DHCP servers.

26. Set Domain Names for Networks

Near the top of the screen select the “Services” button. Reference Figure 48 – Services Button. Ensure that the “DHCP Server” tab is selected. Reference Figure 49 – DHCP Server Screen.

Find the LAN1 line, and follow it to the right side, to the line’s “Actions” button. Click the Actions button. You will be presented with a list of actions. See Figure 57 – DHCP Actions.

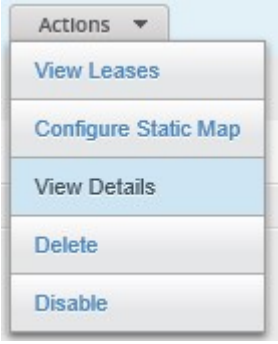

Figure 57 – DHCP Actions

Choose “View Details”. See Figure 58 – DHCP Server Details Dialog.

Figure 58 – DHCP Server Details Dialog

Fill-in the “Domain” field with:

WiredIotNet

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

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

DHCP Servers	Domain
LAN1	WiredIotNet
LAN2	HomeNet
SecureNetDHCP	SeparateNet
WiFiGuestDHCP	WifiGuestNet
WifiIOTDHCP	WifiIotNet

Table 2 - Table of Domain Names

27. Modify EdgeRouter's eth1 DHCP Server

Select the "Services" button. Reference Figure 48 – Services Button.

Ensure that the "DHCP Server" tab is selected. Reference Figure 49 – DHCP Server Screen.

Select the "Action" button to the right of the "LAN1" line. Reference Figure 57 – DHCP Actions.

Choose "View Details". Reference Figure 58 – DHCP Server Details Dialog.

Modify / enter the following information:

DNS 1: 208.67.222.222
DNS 2: 208.67.220.220

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

28. Make DHCP Servers “authorative”

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

Enter the Config Tree. Reference section “13 - EdgeRouter Config Tree”. Select and open up the following config tree sub-menu items from the configuration screen:

service
dhcp-server
shared-network-name

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

SecureNetDHCP

You should see some DHCP settings, including authorative. (Note, your screen will still show “disable”). See Figure 59 – Authorative Example.

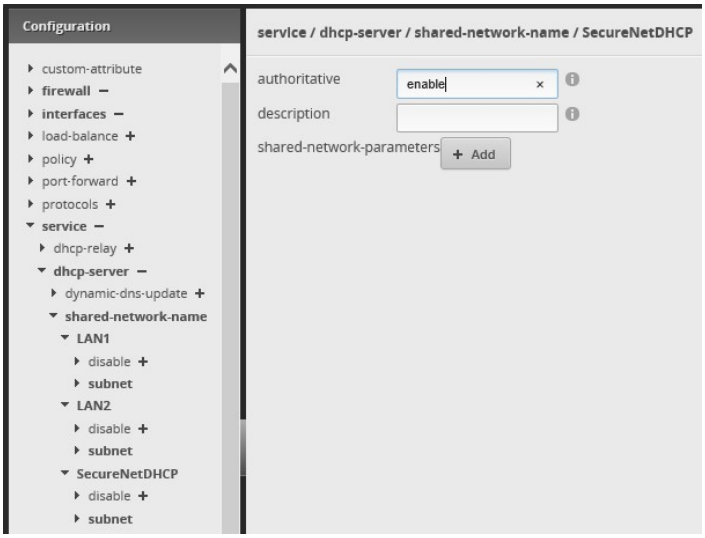

Figure 59 – Authorative Example

Type “enable” in the authorative box. Then press the “Preview” button. See Figure 60 – Authorative Commit.

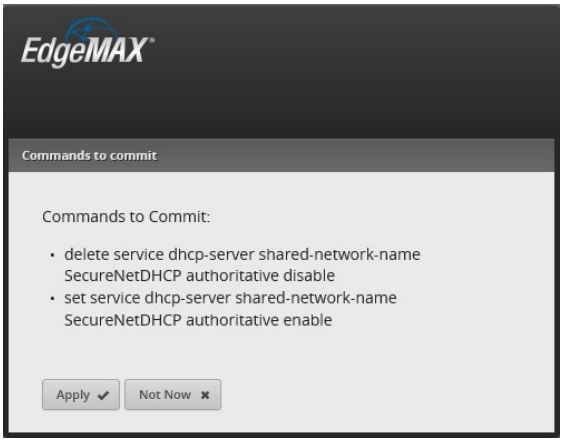

Figure 60 – Authorative Commit

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

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

Authorative DHCP Servers
SecureNetDHCP
WiFiGuestDHCP
WifiIotDHCP

Table 3 - Table of Authorative DHCP Servers

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

```
dhcp-server {
    disabled false
    hostfile-update disable
    shared-network-name LAN2 {
        authoritative enable
        subnet 192.168.3.0/24 {
            default-router 192.168.3.1
            dns-server 192.168.3.1
            domain-name HomeNet
            lease 86400
            start 192.168.3.38 {
                stop 192.168.3.243
            }
        }
    }
    shared-network-name SecureNetDHCP {
        authoritative enable
        subnet 192.168.5.0/24 {
            default-router 192.168.5.1
            dns-server 209.244.0.3
            dns-server 209.244.0.4
            domain-name SeparateNet
            lease 86400
            start 192.168.5.38 {
                stop 192.168.5.243
            }
        }
    }
    shared-network-name WifiGuestDHCP {
        authoritative enable
        subnet 192.168.6.0/24 {
            default-router 192.168.6.1
            dns-server 208.67.222.222
            dns-server 208.67.220.220
            domain-name WifiGuestNet
            lease 86400
            start 192.168.6.38 {
                stop 192.168.6.243
            }
        }
    }
    use-dnsmasq disable
}
```

29. EdgeRouter Enable HW NAT Assist

Enabling “hwnat”, turns-on some features of a hardware switching chip that 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.

Many people report 800 – 900Mbps.

Open up the Configuration Tree. Reference section 13 - EdgeRouter Config Tree.

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

system
offload

In the hwnat setting area, type

enable

See Figure 61 – System Offload Hwnat Selection.

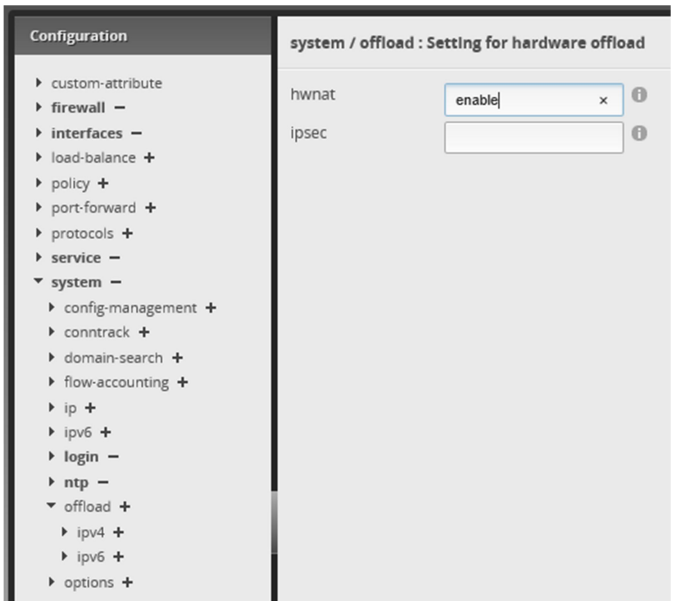

Figure 61 – System Offload Hwnat Selection

Select the “Preview” button. The Edgerouter will preview what command(s) it will issue. See Figure 62 – Preview hwnat Config.

Figure 62 – Preview hwnat Config

Press “Apply”. The system will inform you that “The configuration has been applied successfully”. See Figure 63 – hwnat Success

Figure 63 – hwnat Success

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

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

Compare the above command(s) with the command that the conifg-tree automatically issued in Figure 62 – Preview hwnat Config.

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

The following article is well worth reading:
http://kazoo.ga/re-visit-the-switch-in-edgerouter-x/

Performance references:
https://community.ubnt.com/t5/EdgeMAX/What-is-the-switch0-interface-re-EdgeRouter-X/td-p/1485842
https://community.ubnt.com/t5/EdgeMAX/Performance-of-EdgerouterX-vs-Edgerouter-Lite/td-p/1230924
https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-low-throughput-slow/td-p/1392229
https://community.ubnt.com/t5/EdgeMAX/ER-X-vs-ER-Lite-Head-to-Head-Speed-Results-on-Google-Fiber/td-p/1839844
https://www.stevejenkins.com/blog/2017/02/edgerouter-x-vs-edgerouter-lite-google-fiber-speed-tests/

30. EdgeRouter Quality of Service (QoS)

I haven’t done anything (yet) with Quality of Service.

The following article is well worth reading:
http://kazoo.ga/edgerouter-x-smart-queue/

QoS / Bufferboat:
https://www.reddit.com/r/Ubiquiti/comments/5otj22/edgerouter_x_qos_question/

31. EdgeRouter Enable Traffic Analysis

This step will enable the EdgeRouter to perform Deep Packet Inspection (DPI) / Traffic Analysis.

Press the “Traffic Analysis” button, near the top right of the screen. See Figure 64 – Traffic Analysis Button.

Figure 64 – Traffic Analysis Button

In the upper right area of the traffic analysis screen, is an “Operational Status” selection. Select “Enabled”. See Figure 65 – Enable Operational Status

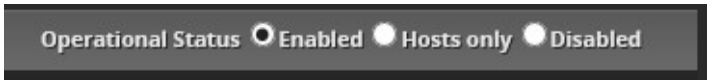

Figure 65 – Enable Operational Status

You will be presented with a confirmation dialog. See Figure 66 – Operational Status Confirmation.

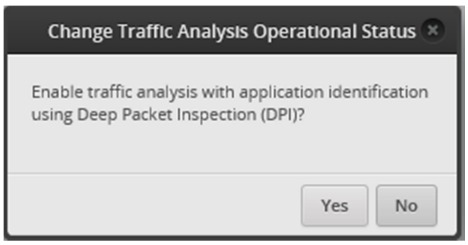

Figure 66 – Operational Status Confirmation

Select “Yes”. The software will (for some reason) present you with an Alert. This is seen in the lower left of the screen. See Figure 67 – Active Alert

Figure 67 – Active Alert

Click on the “Alerts” button. You will be presented with the Alert message(s). See Figure 68 – Active Traffic Analysis Message.

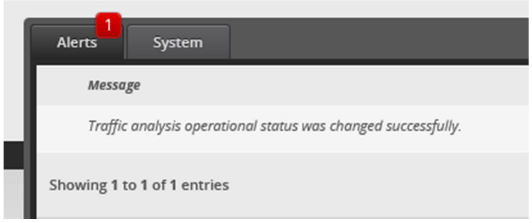

Figure 68 – Active Traffic Analysis Message

To remove this Alert message, press the “Remove” button, located on the right side of the screen. See Figure 69 – Remove Alert Button

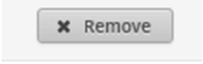

Figure 69 –Remove Alert Button

32. EdgeRouter Traffic Analysis

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

The only thing I had done, since I booted the "setup" computer, was to configure the EdgeRouter. I NEVER purposefully go to MSN.com, or to the Financial Times News (whatever that is). I only assume that those web lookups are from Microsoft's Internet Explorer / Microsoft performing their Windows 10 monetization of their users, sometimes referred to as "spying". See Figure 70 –Sample Traffic Analysis. This feature is pretty neat. In real use, there does seem to be a lot of uncharacterized traffic under "Other".

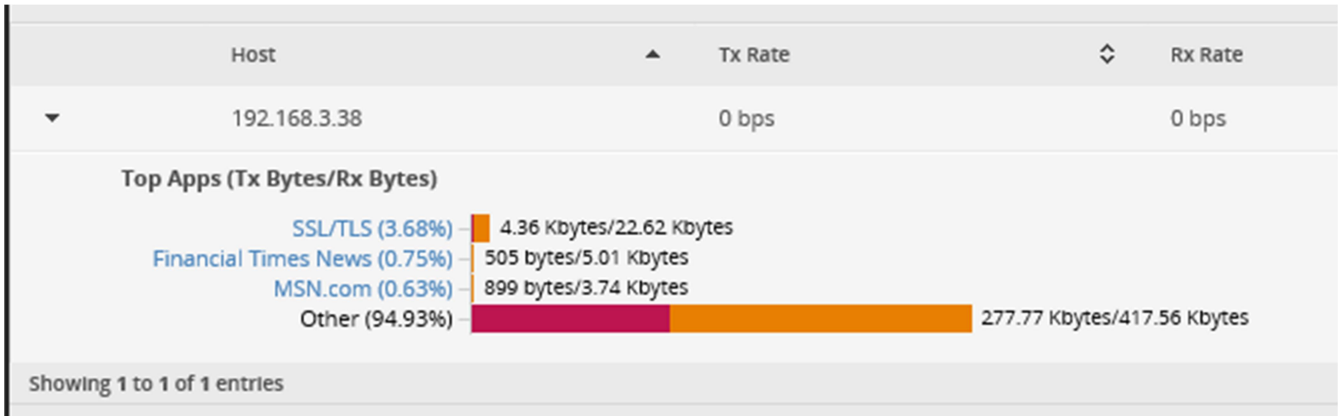

Figure 70 –Sample Traffic Analysis

Note that when HW NAT Assist is enabled, that 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 which is being handled internally by the switch chip is not visible to the CPU. 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).

33. EdgeRouter X/X-SFP bootloader bug

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

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

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

34. EdgeRouter X/X-SFP check bootloader version

Check the version of your bootloader per:

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

Add Clarifications / Hints.

35. EdgeMAX EdgeRouter X/X-SFP bootloader update

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

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

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

Add Clarifications / Hints.

36. EdgeRouter Power Cycle Warning

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

Reference TBD

37. EdgeRouter UPnP

Don't enable UPnP. 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.

Reference TBD

38. 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.

Reference TBD

39. 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 71 –Toolbox Items.

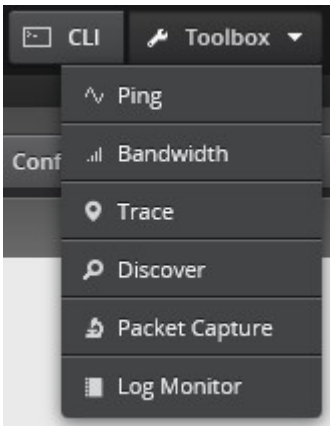

Figure 71 –Toolbox Items

40. Address Groups

The software in the EdgeRouter allows the user to define Address Groups. These groups are used for convenience. We will define several address groups, including one for each Network. Reference Table 1 - Table of Networks.

Select the “Firewall/NAT” Button from the top of the screen. See Figure 72 – Firewall/NAT Button.

Figure 72 – Firewall/NAT Button

From the tabs that are shown, select “Firewall/NAT Groups”. See Figure 73 – Firewall/NAT Groups Tab.

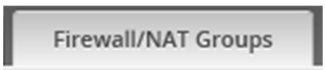

Figure 73 – Firewall/NAT Groups Tab

Find the “Add Group” button and click it. See Figure 74 – Add Group Button.

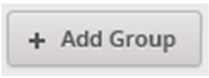

Figure 74 – Add Group Button

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

Name:	WIRED_IOT_GROUP
Description:	Wired Iot Group
Group Type:	Address Group.

See Figure 75 – Example New Address Group Dialog. Press Save.

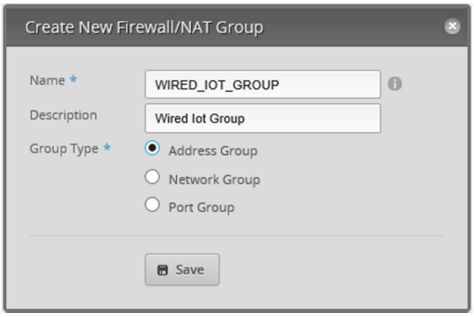

Figure 75 – Example New Address Group Dialog

An empty Address group will have been added. Notethat the “Number of group members” is 0. See Figure 76 – Added Address Group.

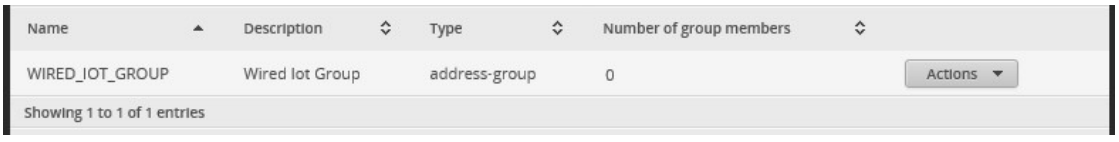

Figure 76 – Added Address Group

Press the WIRED_IOT_GROUP's Action button and select Config. See Figure 77 – Address Group Actions

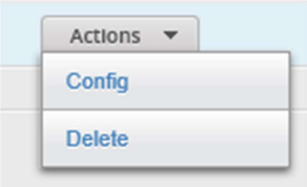

Figure 77 – Address Group Actions

Enter the address specifier of:

192.168.4.0/24

See Figure 78 – Example Edit Address Group. Press Save. When it is finished updating, close the dialog.

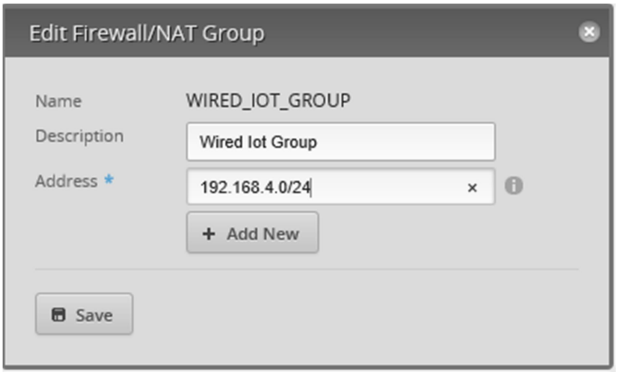

Figure 78 – Example Edit Address Group

Repeat the above steps for the following address groups. If there are 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 WIRED_IOT_GROUP.

```
group {
    address-group HOME_GROUP {
        address 192.168.3.0/24
        description "Home Group"
    }
    address-group MULTIPLE_GROUP {
        address 192.168.3.0/24
        address 192.168.4.0/24
        address 192.168.6.0/24
        address 192.168.7.0/24
        description "Multiple Groups"
    }
    address-group OPENDNS_SERVERS_GROUP {
        address 208.67.222.222
        address 208.67.220.220
        description "OpenDNS Servers"
    }
    address-group WIFI_GUEST_GROUP {
        address 192.168.6.0/24
        description "Wifi Guest Group"
    }
    address-group WIFI_IOT_GROUP {
        address 192.168.7.0/24
        description "Wifi Iot Group"
    }
    address-group WIRED_IOT_GROUP {
        address 192.168.4.0/24
        description "Wired Iot Group"
    }
    address-group WIRED_SEPARATE_GROUP {
        address 192.168.5.0/24
        description "Wired Separate Group"
    }
}
```

The above text section is from the backup file.

41. EdgeRouter Layman's Firewall Explanation

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

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

You REALLY should stop and read that (whole) posting right now.

I have re-produced the main diagram, from that article, as Figure 79 – Layman's Firewall Explanation Diagram. Note that this diagram is for an EdgeRouter Lite, which has its WAN port on eth1. The WAN interface is therefore shown in the middle of this diagram.

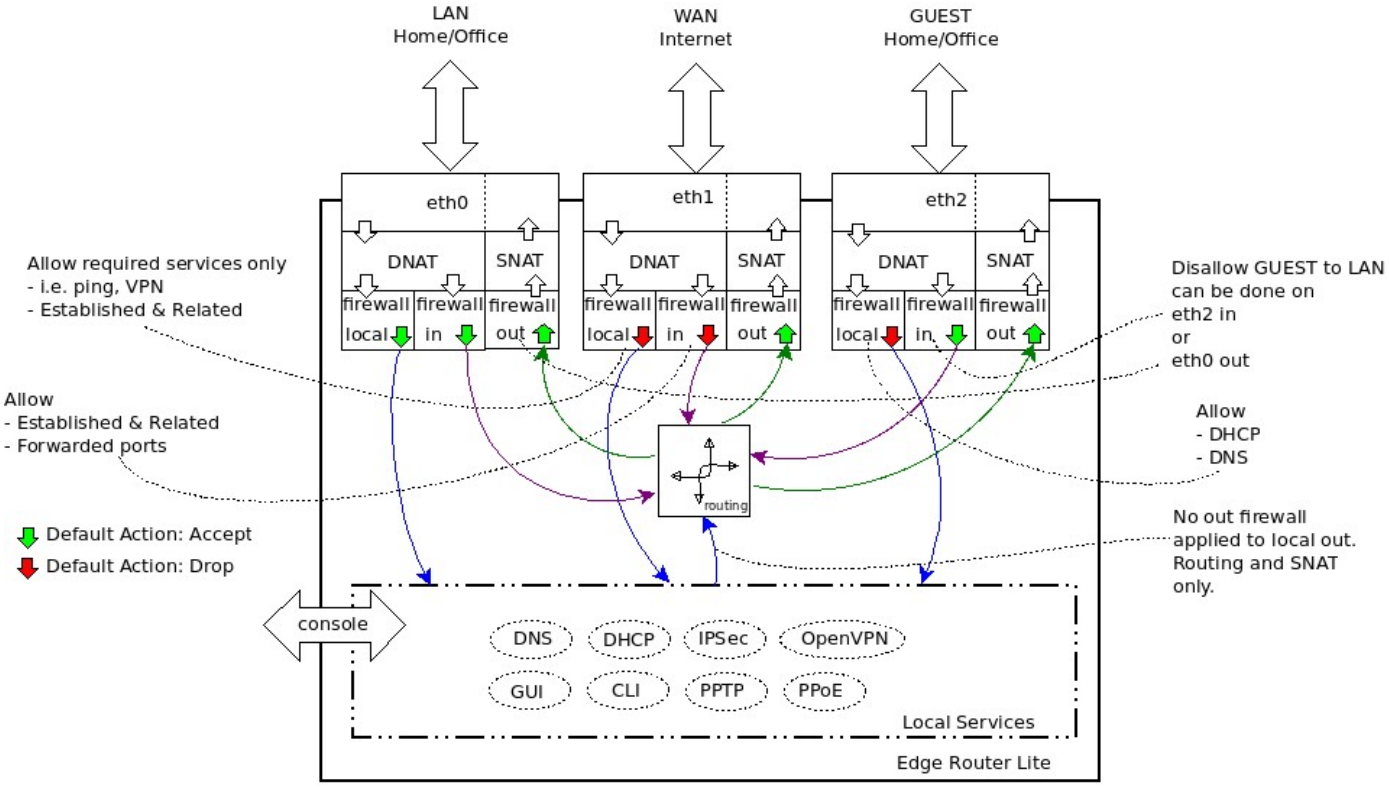

Figure 79 – Layman's Firewall Explanation Diagram

A firewall policy (ruleset) is a set of firewall rules along with a default action. The default action can be "accept", "reject", or "drop". A firewall ruleset is applied to a specific interface as well as applied to a specific "direction". For an EdgeRouter, the directions are "In", "Out", and "Local". The "In" direction is input IP packets from the internet as well as input into the EdgeRouter from devices on a Network (LAN). The "Out" direction consists of IP packets output from the EdgeRouter destined for the internet, as well as output to your Network devices from the EdgeRouter. Local refers to IP data coming into the EdgeRouter destined for (services on the) EdgeRouter itself. Reference Figure 79 – Layman's Firewall Explanation Diagram.

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 which 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 then taken for that packet. Once an IP packet matches an individual firewall rule, no other firewall processing is needed for that IP packet.

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

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

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

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

42. Firewall State

There are many conditions available which 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 which have invalid data in them.
Established – packets associated with an existing connection (conversation).
Related – packets related to an existing connection (conversation).

43. WAN Firewall Rules

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

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

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

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

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

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

QUESTION: I've often wondered why the invalid state rule (number 20) has not been placed before the established/related rule (10). For well-behaved web sites this order should not matter. With badly coded web servers, having the invalid rule first, might break some web usage. With the advent of malicious advertisements now being served up on legitimate web sites, it seems like it might make sense to place the invalid rule first, and risk some amount of web usage breakage.

44. EdgeRouter Detailed Firewall Setup

I have adapted Figure 79 – Layman's Firewall Explanation Diagram to my own diagram. See Figure 80 – Detailed Firewall Setup Diagram.

The FireWall Rules (FWR) that are described in this guide are numbered (as FWR*) in Figure 80 – Detailed Firewall Setup Diagram. Each is associated with a named firewall ruleset which will be described in the following sections. FWRs which are colored red means a ruleset terminates with a default of drop, while FWRs colored green mean a default of accept. The firewall rule sets are:

FWR1 = WAN_LOCAL.
FWR2 = WAN_IN.
FWR3 = WIRED_IOT_LOCAL.
FWR4 = WIRED_SEPARATE_LOCAL.
FWR5 = WIRED_SEPARATE_IN.
FWR6 = WIRED_SEPARATE_OUT.
FWR7 = HOME_OUT (same single set of rules, but shown in two places).
FWR8 = WIFI_GUEST_LOCAL.
FWR9 = WIFI_IOT_LOCAL.

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

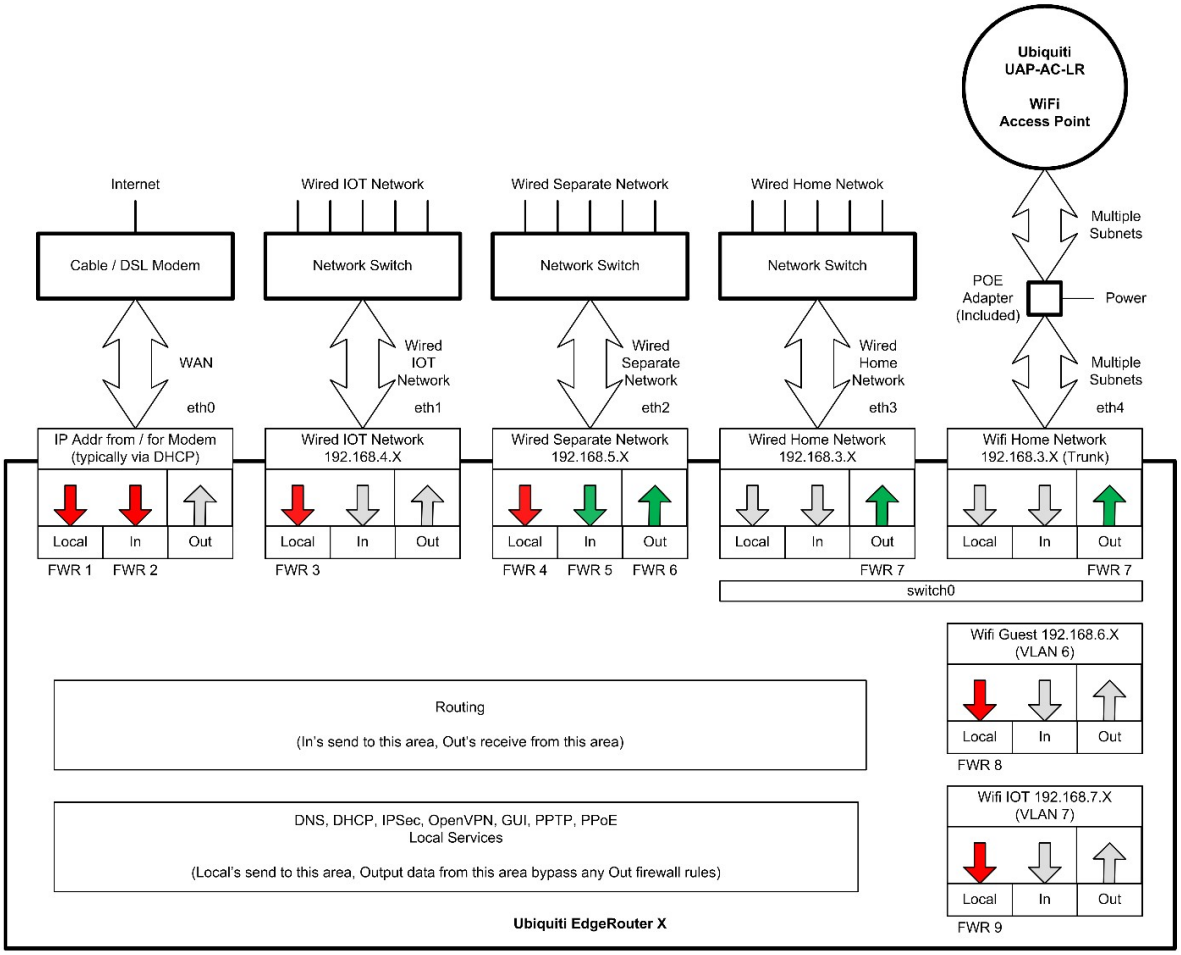

Figure 80 – Detailed Firewall Setup Diagram

45. WAN_LOCAL Firewall Rules

The basic operation of these firewall rules was described above, in the section titled “43 - WAN Firewall Rules”. These rules are FRW1 as shown in Figure 80 – Detailed Firewall Setup Diagram.

Add Optional VPN information, etc…

46. WAN_IN Firewall Rules

The basic operation of these firewall rules was described above, in the section titled “43 - WAN Firewall Rules”. These rules are FRW2 as shown in Figure 80 – Detailed Firewall Setup Diagram.

Add forwarded ports, etc…

Add information on double NAT.

47. HOME_OUT Firewall Rules

There are six firewall rules in this ruleset. These firewall rules inspect IP packets which are exiting the EdgeRouter towards devices on the Home Network. Reference “FWR7”, shown as two instances, in the upper right of Figure 80 – Detailed Firewall Setup Diagram.

These six rules are maintained as three sets of two rules per interface. I.e. These two-rule-sets are applied to three interfaces. Each interface is a separate Network. Except for naming, and the Network they are applied to, the sets of two rules are identical. Only one set of two rules are shown here. The three Networks, which these three sets are applied-to, are: Wired Iot Network, Wifi Iot Network, and Wifi Guest Network.

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

This is one set of two rules from the backup file:

```
name HOME_OUT {
    default-action accept
    description "Home Out"
    rule 1 {
        action accept
        description "Allow Wired Iot Replies"
        log disable
        protocol all
        source {
            group {
                address-group WIRED_IOT_GROUP
            }
        }
        state {
            established enable
            invalid disable
            new disable
            related enable
        }
    }
    rule 2 {
        action drop
        description "Drop Rest-Of Wired Iot Traffic"
        log disable
        protocol all
        source {
            group {
                address-group WIRED_IOT_GROUP
            }
        }
    }
…
```

Equation 1 – A Portion of the HOME_OUT Firewall Ruleset

The name of this ruleset is HOME_OUT. The rules in this ruleset are applied (not shown here) to the output side of both of the eth3 and eth4 interfaces, i.e. switch0. These interfaces are also known as the Home Network. IP packets which are exiting the EdgeRouter (on eth3/eth4) towards equipment on the Home Network are inspected and potentially dropped by these firewall rules. Remember that eth3 and eth4 are still bound together by the switch hardware within the EdgeRouter. In Figure 80 – Detailed Firewall Setup Diagram, this information is shown as duplicated in two blocks (in the upper right portion of the diagram) each labeled with FWR7.

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

The first rule (number 1) in this ruleset has an action of accept, and will allow IP packets which are "established" and "related" (i.e. associated) to an existing IP conversation, to exit the EdgeRouter to devices which are on the Home Network. Note that this rule has an additional qualifier that the source address must be in the address range of the WIRED_IOT_GROUP. I.e. This rule only apples to traffic which originates from the Wired IOT Network. The only way to have an existing connection between Wired IOT Network and the Home Network, is for the conversation to have been started from devices within the Home Network. The name associated with this rule is "Allow Wired Iot Replies".

The second rule (number 2) in this ruleset has an action of drop, and will drop all other IP packets which originate from the Wired IOT Network. Note that this rule also has the additional qualifier that the source address must be within the address range of the WIRED_IOT_GROUP. I.e. This rule only apples to traffic which originates from the Wired IOT Network. The name associated with this rule is "Drop Rest-Of Wired Iot Traffic ".

These two rules, treated together, describe the IP connections (conversations) that can occur between equipment on the Wired IOT Network and the Home Network.

If the conversation was started by devices in the Home Network and directed to devices residing on the Wired IOT Network, then replies to those conversations will be allowed back into the Home Network by firewall rule number 1. Internally, the firewall code keeps track of IP connections which are entering the EdgeRouter (the "In" side) and then allows traffic which is related to that data to exit the EdgeRouter towards the Hone Network devices.

If a conversation was instead started by devices within the Wired IOT Network and directed towards the Home Network, firewall rule 1 will have no prior knowledge about this conversation (because it is not "established"/"related"). Therefore firewall rule number 1 will not match, and firewall rule processing will then proceed to rule number 2. Rule number two drops all traffic from the Wired IOT Network.

There are two more sets of two rules (not shown here) within this ruleset, an identical set applied to the Wifi Guest Network (WIFI_GUEST_GROUP), and an identical set applied to the Wifi IOT Network (WIFI_IOT_GROUP).

Remember that the default action for this ruleset is "accept". You want the Home Network to be able to operate on its own, when it is not conversing with just these three networks.

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

QUESTION: Maybe a single firewall rule can be added, at the top of this ruleset, which allows internet traffic to be accepted. This would increase the efficiency of this ruleset, by not depending upon most of the traffic to reach the default "accept" rule before being accepted.

48. 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 81 – Firewall Conditions, Basic Tab.
Figure 82 – Firewall Conditions, Advanced Tab.
Figure 83 – Firewall Conditions, Source Tab.
Figure 84 – Firewall Conditions, Destination Tab.
Figure 85 – Firewall Conditions, Time Tab.

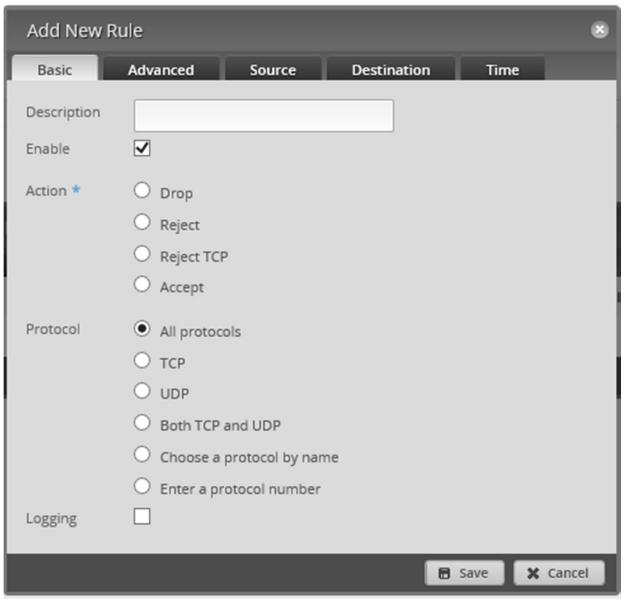

Figure 81 – Firewall Conditions, Basic Tab

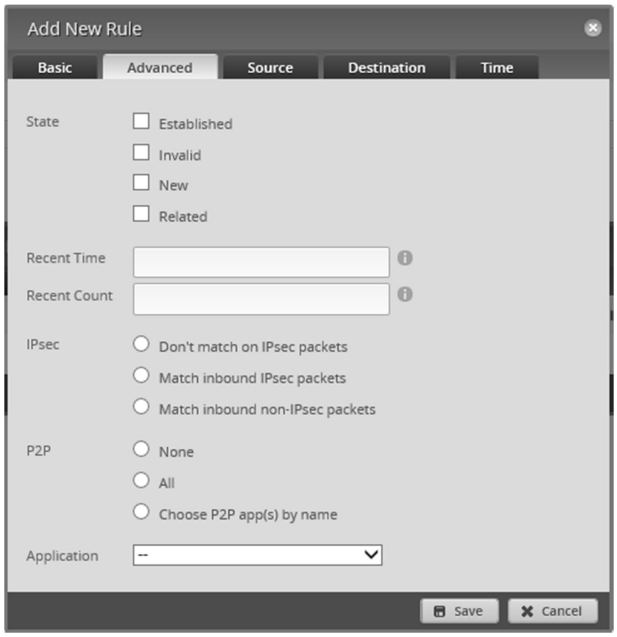

Figure 82 – Firewall Conditions, Advanced Tab

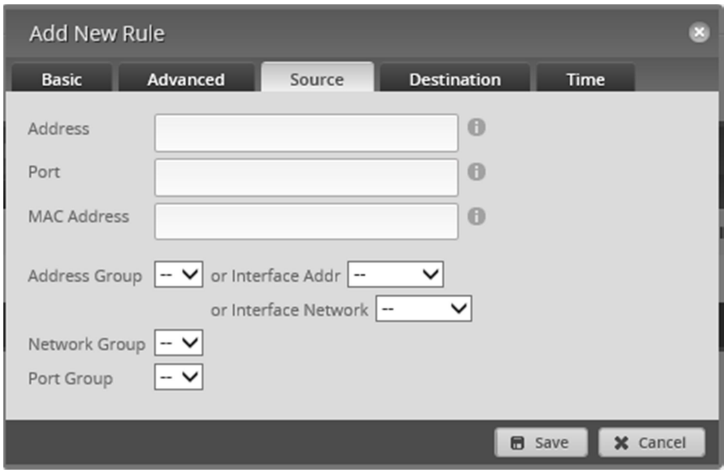

Figure 83 – Firewall Conditions, Source Tab

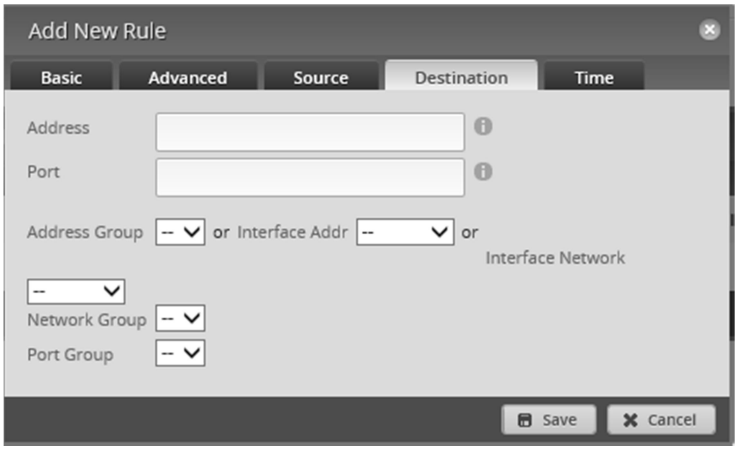

Figure 84 – Firewall Conditions, Destination Tab

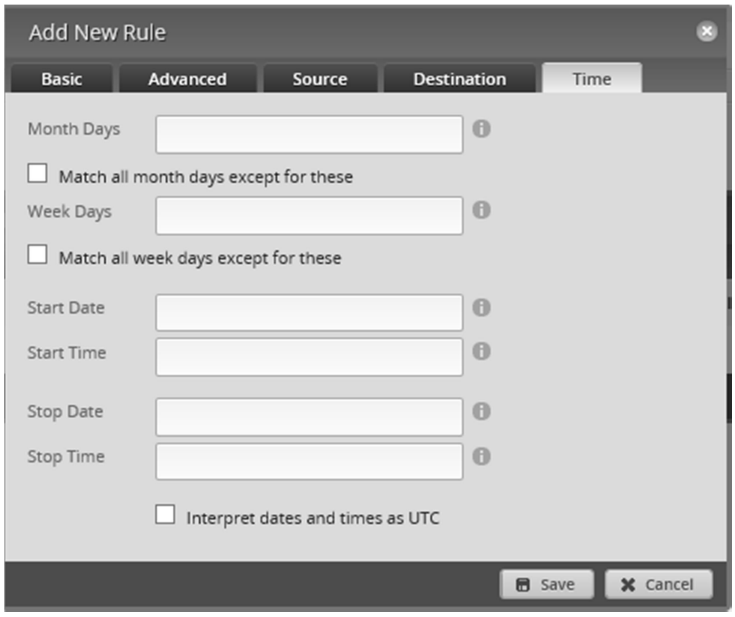

Figure 85 – Firewall Conditions, Time Tab

49. Adding Firewall Rules

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

While you are using the GUI to add these rules, please frequently reference the backup file segment labeled "Equation 1 – A Portion of the HOME_OUT Firewall Rules" which is in section "47 - HOME_OUT Firewall Rules". This should help you better relate between the two forms: that of the backup text description versus that of GUI entry.

Select the "Firewall/NAT" Button from the top of the screen. Reference Figure 72 – Firewall/NAT Button.

Ensure that the "Firewall Policies" Tab is selected. See Figure 86 – Firewall Policies Tab.

Figure 86 – Firewall Policies Tab

The two WAN rulesets, which were added by the Wizard, should be shown. Press the "+ Add Ruleset" button. See Figure 87 – Add Ruleset.

Figure 87 – Add Ruleset

You will be presented with a Create New firewall Ruleset. See Figure 88 – Blank Create New Firewall Ruleset.

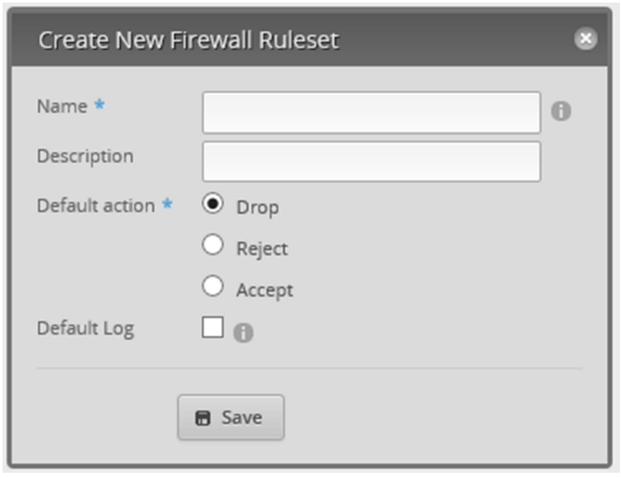

Figure 88 – Blank Create New Firewall Ruleset

Enter the following into the Create New Firewall Ruleset dialog:

Name	HOME_OUT
Description	Home Out
Default action	Accept

See Figure 89 – HOME_OUT Example New Ruleset.

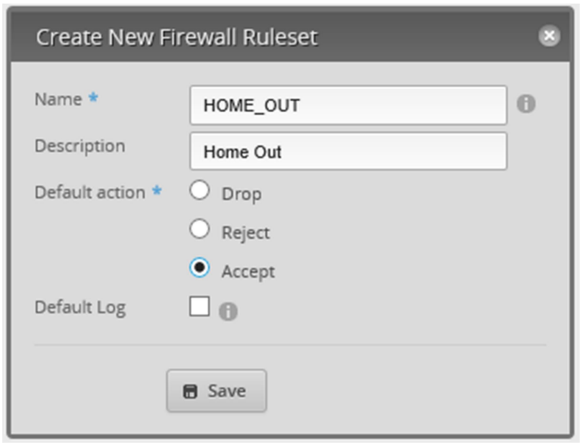

Figure 89 – HOME_OUT Example New Ruleset

Press "Save". A HOME_OUT ruleset will be created. Note that no interfaces have been selected, and the number of rules is 0. See Figure 90 – Empty HOME_OUT Ruleset.

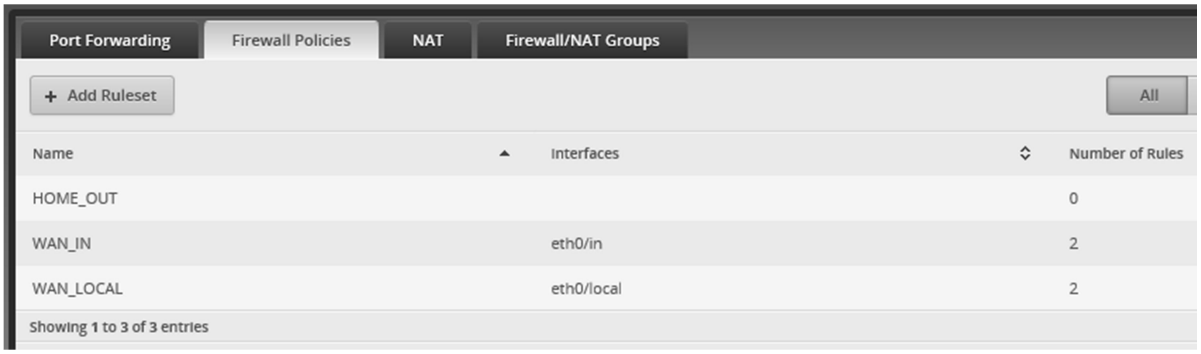

Figure 90 – Empty HOME_OUT Ruleset.

Find the "Actions" button at the right end of the HOME_OUT line (not shown) and press it. You will be presented with a Firewall Actions Menu. See Figure 91 – Firewall Actions Menu.

Figure 91 – Firewall Actions Menu

Choose “Edit Ruleset”. A dialog for editing firewall rules appears. The “Rules” Tab should already be selected. See Figure 92 – Edit Ruleset Dialog.

Note that this dialog also contains Tabs of “Configuration”, “Interfaces”, and “Stats”. These match the handy shortcuts that are also in the previously shown Actions menu, reference Figure 91 – Firewall Actions Menu.

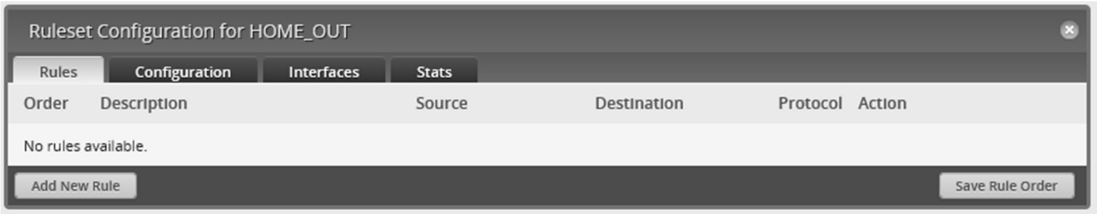

Figure 92 – Edit Ruleset Dialog

Choose the “Configuration” Tab. You should see the information that was entered earlier. See Figure 93 – Firewall Rule Configuration Tab.

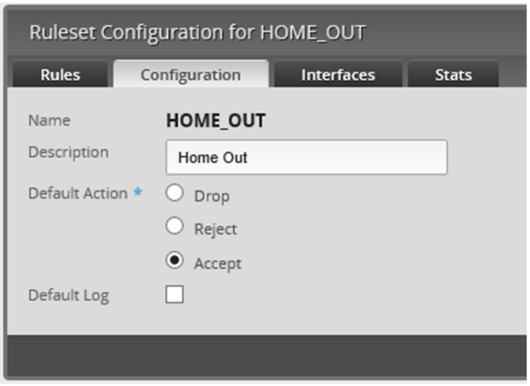

Figure 93 – Firewall Rule Configuration Tab

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

Interface	switch0
Direction	out

Then press the “Save Ruleset” button.

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

Since the Home Network is governed by switch0 (i.e.switch0 contains interfaces of eth3 and eth4), we need to choose “switch0” for the Interface, not the individual eth3 or eth4.If an interface is not part of switch0 (eth0, eth1, or eth2) then we would just select that individual interface. See Figure 94 – Firewall Rule Interface Tab.

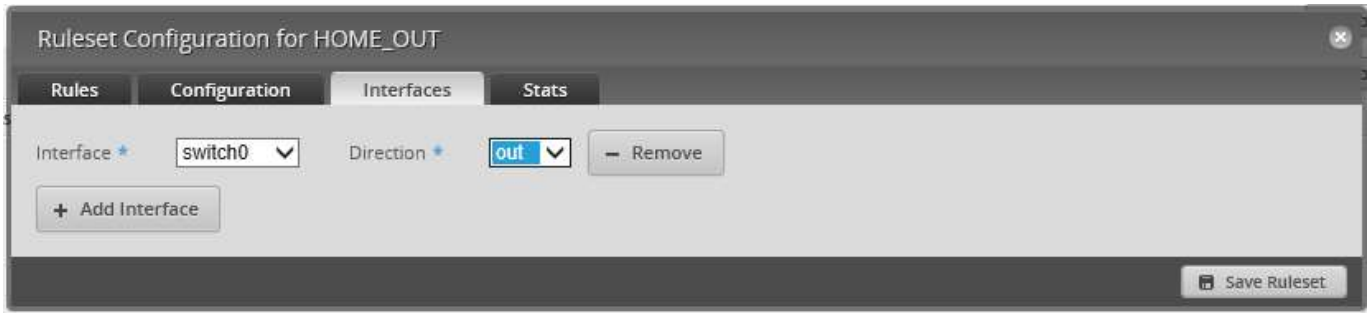

Figure 94 – Firewall Rule Interface Tab

Re-select the “Rules” Tab, and press the “Add New Rule” Button, that is shown in Figure 92 – Edit Ruleset Dialog. An “Add New Rule” dialog will be shown. See Figure 95 – HOME_OUT Firewall, Rule1, Basic. Enter the following into the Basic Tab:

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

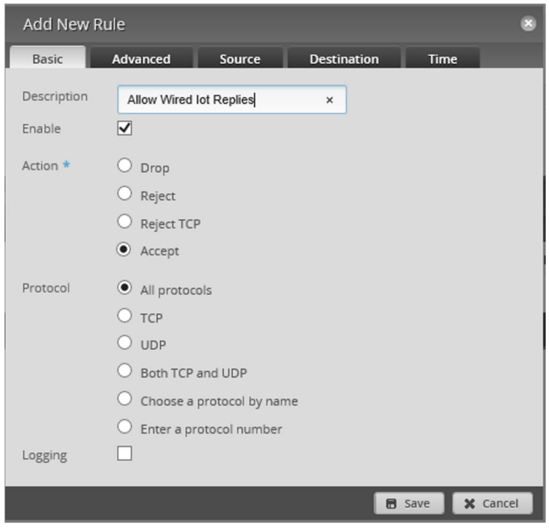

Figure 95 – HOME_OUT Firewall, Rule1, Basic

Click on the Advanced Tab. See Figure 96 – HOME_OUT Firewall, Rule1, Advanced. Enter the following information into the Advanced Tab:

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

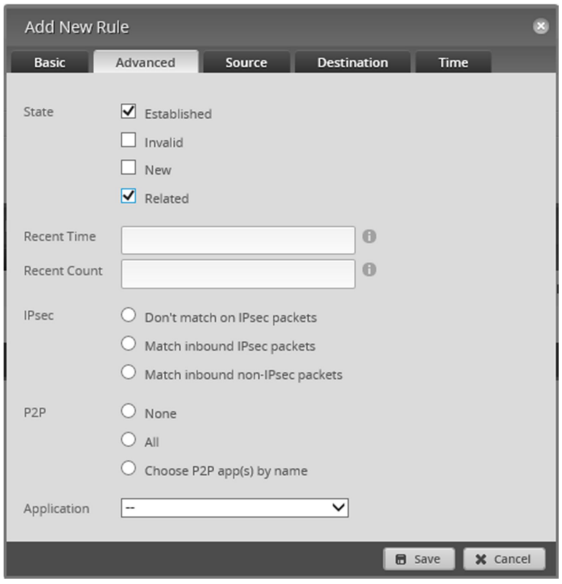

Figure 96 – HOME_OUT Firewall, Rule1, Advanced

Click on the Source Tab. See Figure 97 – HOME_OUT Firewall, Rule1, Source. Select the following information for the Source Tab:

Address Group Wired Iot Group.

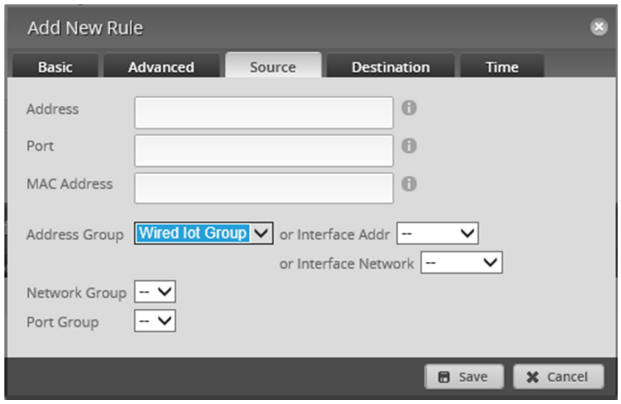

Figure 97 – HOME_OUT Firewall, Rule1, Source

Press the "Save" button. You now have a new rule in the HOME_OUT ruleset. See Figure 98 – HOME_OUT Firewall, Rule1.

Figure 98 – HOME_OUT Firewall, Rule1

It is time to add the second firewall rule of this ruleset. Press the "Add New Rule" button, as shown in Figure 98 – HOME_OUT Firewall, Rule1. You will be presented with the Basic dialog for adding firewall rules. See Figure 99 – HOME_OUT Firewall, Rule2, Basic. Enter the following information into the Basic Tab:

Description Drop Rest-Of Wired Iot Traffic
Enable CHECKED
Action Drop
Protocol All protocols

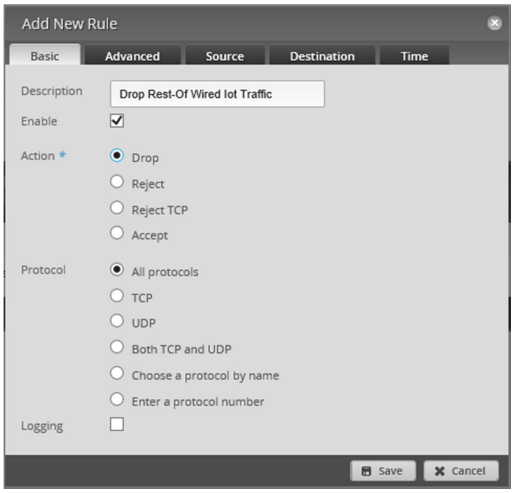

Figure 99 – HOME_OUT Firewall, Rule2, Basic

Click on the Source Tab. See Figure 100 – HOME_OUT Firewall, Rule2, Source. Select the following information for the Source Tab:

Address Group Wired Iot Group.

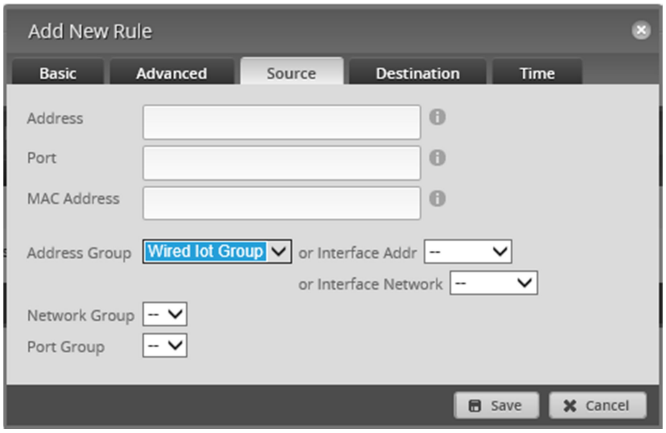

Figure 100 – HOME_OUT Firewall, Rule2, Source

Press the "Save" button. You now have two rules in the HOME_OUT ruleset, as shown in Figure 101 – HOME_OUT Firewall, Two Rules.

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

The second rules drops all traffic from the Wired IOT Network which was not matched by the first rule, i.e. Any non-requested traffic which was initiated by the Wired IOT Network.

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

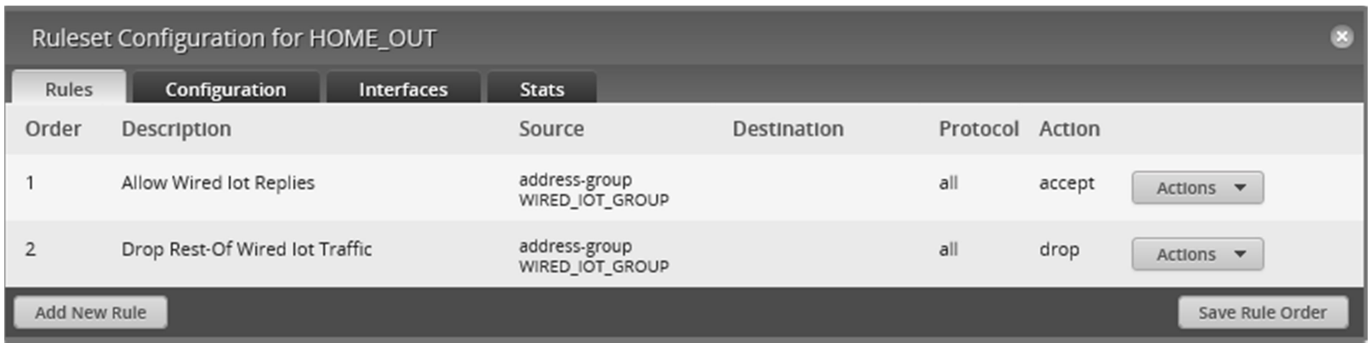

Figure 101 – HOME_OUT Firewall, Two Rules

50. Adding More HOME_OUT Firewall Rules

We now need to add four more rules to the HOME_OUT Ruleset. Using the steps which are shown in the above section “49 - Adding Firewall Rules”, add four more rules per the backup data which is shown below:

```
        rule 3 {
            action accept
            description "Allow Wifi Guest Reples"
            destination {
                group {
                }
            }
            log disable
            protocol all
            source {
                group {
                    address-group WIFI_GUEST_GROUP
                }
            }
            state {
                established enable
                invalid disable
                new disable
                related enable
            }
        }
        rule 4 {
            action drop
            description "Drop Rest-Of Wifi Guest Traffic"
            log disable
            protocol all
            source {
                group {
                    address-group WIFI_GUEST_GROUP
                }
            }
        }
        rule 5 {
            action accept
            description "Allow Wifi Iot Reples"
            log disable
            protocol all
            source {
                group {
                    address-group WIFI_IOT_GROUP
                }
            }
            state {
                established enable
                invalid disable
                new disable
                related enable
            }
        }
        rule 6 {
            action drop
            description "Drop Rest-Of Wifi Iot Traffic"
            log disable
            protocol all
            source {
                group {
                    address-group WIFI_IOT_GROUP
                }
            }
        }
```

51. WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules

These rules are FWR3 and FWR9 as shown in Figure 80 – Detailed Firewall Setup Diagram.

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

The DHCP protocol uses port 67 and port 68 of UDP.

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

The DNS firewall rules, presented below, for the Wired Iot and Wifi Iot Networks contain an additional destination-address restriction. These DNS firewall rules will only accept DNS requests, which are issued to the Open DNS resolver addresses. DNS requests to other providers will be dropped via the ruleset's default drop rule..

Note that the destination addresses specified here (via the OPENDNS_SERVERS_GROUP) must match the Wired Iot and Wifi Iot Networks DHCP entered DNS1 and DNS2 addresses. Reference section 25 - Add DHCP Servers to the VLANs and section 27 - Modify EdgeRouter's eth1 DHCP Server. It's not good to tell your Iot devices to use one set of DNS provider addresses (via DHCP) and then drop those requests when your firewall rules only accept addresses of a different DHCP provider.

We now need to add two more rulesets, with each ruleset containing two firewall rules. Using the steps which are shown in the above section "49 - Adding Firewall Rules", add the following two rulesets, each containing two firewall rules, per the backup data which is shown below:

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

Interface: eth1
Direction: local

```
name WIRED_IOT_LOCAL {
    default-action drop
    description "Wired IOP Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67-68
        }
        log disable
        protocol udp
        source {
        }
    }
    rule 2 {
        action accept
        description "Allow Only OpenDNS"
        destination {
            group {
                address-group OPENDNS_SERVERS_GROUP
            }
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

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

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

Interface: switch0.7

Direction: local

```
name WIFI_IOT_LOCAL {
    default-action drop
    description "Wired Iot Local"
    rule 1 {
        action accept
        description "Allow DHCP"
        destination {
            port 67-68
        }
        log disable
        protocol udp
    }
    rule 2 {
        action accept
        description "Allow Only OpenDNS"
        destination {
            group {
                address-group OPENDNS_SERVERS_GROUP
            }
            port 53
        }
        log disable
        protocol tcp_udp
    }
}
```

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

52. WIFI_GUEST_LOCAL Firewall Rules

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

To add the following ruleset and rules, follow what was done in the above section 51 - WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules.

Note that we are not dropping DNS requests based upon which DNS provider address(es) your guests may be using in their devices. Most people's devices are probably configured to just use the providers (provided via DHCP) DNS resolvers addresses. If a guest hardcoded the DNS resolver addresses within their device AND we only accepted DNS requests going to specific DNS resolvers, then we could have just denied our guests service on our network.

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

Interface: switch0.6
Direction: local

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

53. Optional DNS Forcing of the WIFI_GUEST_LOCAL Network

Performing the steps within this section is optional.

The destination Network Address Translation (NAT) rules, presented here, will force any guest's DNS request(s) to use (only) Open DNS resolvers. Nat rules are handled like firewall rules, the rules are traversed in order, when a NAT rules matches; NAT processing will stop for that packet.

I have seen several postings on the web about how to force a specific DNS provider, but have not seen any that will work when the primary DNS resolver is broken / out of service.

The two rules presented here work with each other. Rule #1 will translate a DNS request going to the primary OpenDNS resolver into a DNS request going to the (same) primary OpenDNS resolver. I.e. This request performs a translation into itself. Rules #2 will translate an address which is NOT the secondary OpenDNS resolver, and translate that address into the secondary OpenDNS resolver address. The "!"(bang) character which is in front of the destination address signifies "not".

This nat ruleset is not very efficient, but a separate destination NAT rule is needed for each of the primary and secondary DNS addresses, if you want to both force DNS providers and provide your guests with two resolver addresses. Hopefully your guests are not making 100s of DNS requests per second.

Press the Firewall/NAT button near the top of the screen. Reference Figure 72 – Firewall/NAT Button.

Ensure that the NAT tab is selected and then press the "+ Add Destination NAT Rule" button. See Figure 102 – NAT Tab.

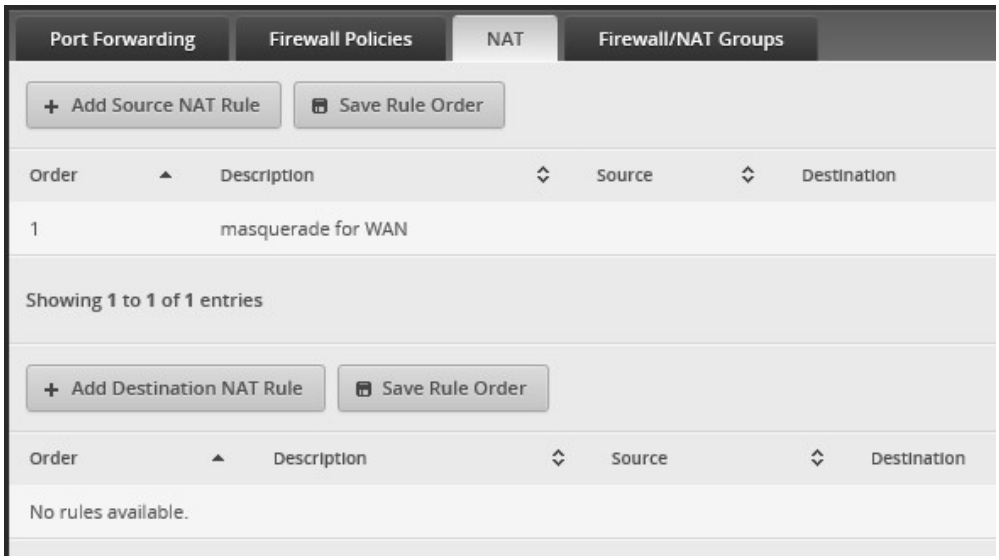

Figure 102 – NAT Tab

You will be presented with a “Destination NAT Rule Configuration” dialog. Enter the data for Rule #1, and Save it. See Figure 103 – NAT Rule #1. Then press the “+ Add Destination NAT Rule” button again andenter the data for Rule#2, and save it also. See Figure 104 – NAT Rule #2.

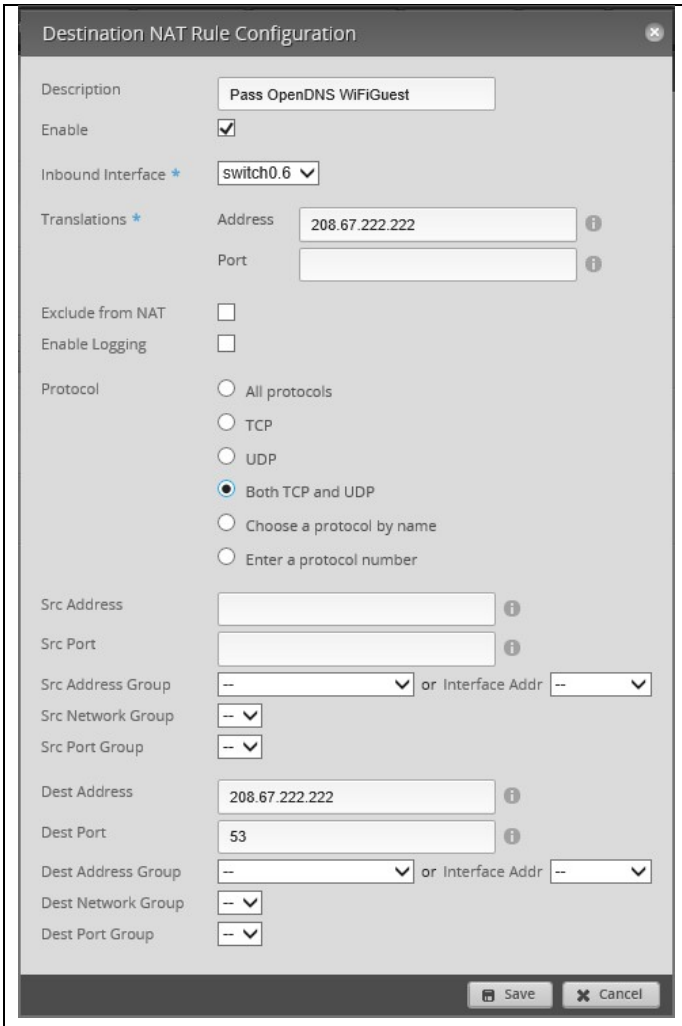

Figure 103 – NAT Rule #1

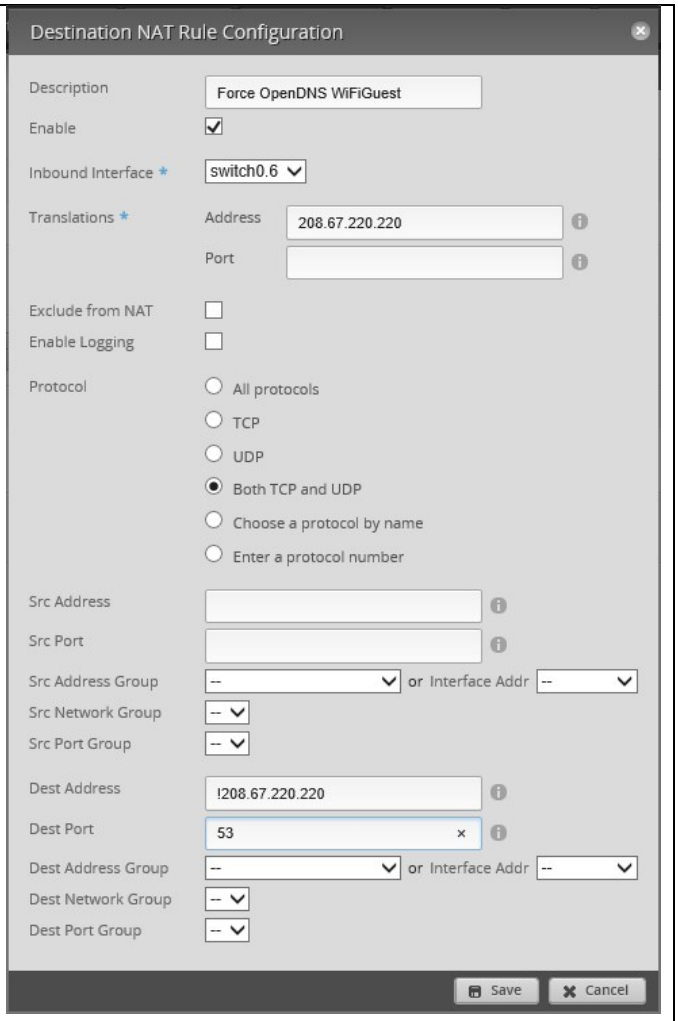

Figure 104 – NAT Rule #2

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 "Pass OpenDNS WiFiGuest"
            destination {
                address 208.67.222.222
                port 53
            }
            inbound-interface switch0.6
            inside-address {
                address 208.67.222.222
            }
            log disable
            protocol tcp_udp
            type destination
        }
        rule 2 {
            description "Force OpenDNS WiFiGuest"
            destination {
                address !208.67.220.220
                port 53
            }
            inbound-interface switch0.6
            inside-address {
                address 208.67.220.220
            }
            log disable
            protocol tcp_udp
            type destination
        }
        rule 5010 {
            description "masquerade for WAN"
            outbound-interface eth0
            type masquerade
        }
    }
```

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

http://welcome.opendns.com

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

To perform this test, first temporarily change the DNS resolvers associated with the Guest Network's DHCP server (switch0.6) to something else. I used addresses of 8.8.8.8 and 8.8.4.4 from Google. Reference section 25 - Add DHCP Servers to the VLANs. Then, using a device attached to the Guest Network, visit the OpenDNS test page. If you get their success page, then these two rules translated the Google DNS addresses into OpenDNS addresses. You may have to reboot the EdgeRouter and/or the Guest device to ensure that the changed DNS resolver addresses propogated to the Guest device. Remember to return the Guest Network's DNS resolver addresses (in the DHCP area) back to the OpenDNS addresses.

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

54. WIRED_SEPARATE Firewall Rules

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

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

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

Reference Figure 80 – Detailed Firewall Setup Diagram, for FWR numbers and Network routing / interactions.

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

To block instance number 1, we need to block traffic from exiting OUT the EdgeRouter and going to devices that are on the Separate Network. This ruleset will be labeled WIRED_SEPARATE_OUT and is denoted as FWR6. This ruleset will need to block addresses from the WIRED_IOT_GROUP and the HOME_GROUP.

Note that two of the Networks: "Wifi IOT Network" and "Wifi Guest Network" are using VLANs and originate from the Access Point. Within the Access Point, these Networks will be configured as Guest Networks, and will therefore be denied access to all of the EdgeRouter's addresses except for the Home Network, which is at 192.168.3.X. So no firewall rules are needed to block these two Networks from accessing the Wired Separate Network.

To add the following ruleset and rules, follow what was done in the above section 51 - WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules.

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

Interface: eth2
Direction: out

```
name WIRED_SEPARATE_OUT {
    default-action accept
    description "Wired Separate Out"
    rule 1 {
        action drop
        description "Drop Home Network"
        log disable
        protocol all
        source {
            group {
                address-group HOME_GROUP
            }
        }
    }
    rule 2 {
        action drop
        description "Drop Wired Iot Network"
        log disable
        protocol all
        source {
            group {
                address-group WIRED_IOT_GROUP
            }
        }
    }
}
```

To block instance number 2, we need to block traffic from entering IN the EdgeRouter and going to devices that are on the other networks. This ruleset will be labeled WIRED_SEPARATE_IN and is denoted as FWR5. Additionally, we need to block traffic from entering the EdgeRouter itself (LOCAL) except for DNS and DHCP requests. This ruleset will be labeled WIRED_SEPARATE_LOCAL and is denoted as FWR4.

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

Interface: eth2
Direction: in

```
name WIRED_SEPARATE_IN {
    default-action accept
    description "Wired Separate In"
    rule 1 {
        action drop
        description "Block Multiple Networks"
        destination {
            group {
                address-group MULTIPLE_GROUP
            }
        }
        log disable
        protocol all
    }
}
```

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

Interface: eth2
Direction: local

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

55. EdgeMax Change Interface Names

Press the Dashboard Button. Reference Figure 34 – Dashboard Button.

Find the line with an Interface of “switch0”. Click on the Action button to the right of this line. Select “Config” from the Actions Menu. You will see a dialog similar to Figure 37 – switch0 Configuration. Change the Description field to “Home Net”.

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

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

Table 4 - Table of Interface Names

56. AP-AC-LR Access Point Setup

Add Sections / Descriptions.

RFC 1918 Private Ranges.

Hookup, using two standard Ethernet cables:

```
                              POE Adapter
EdgeRouter_eth4   <------>    LAN_____POE      <----->    AP-AC-LR
```

Figure 105 – UniFi Base

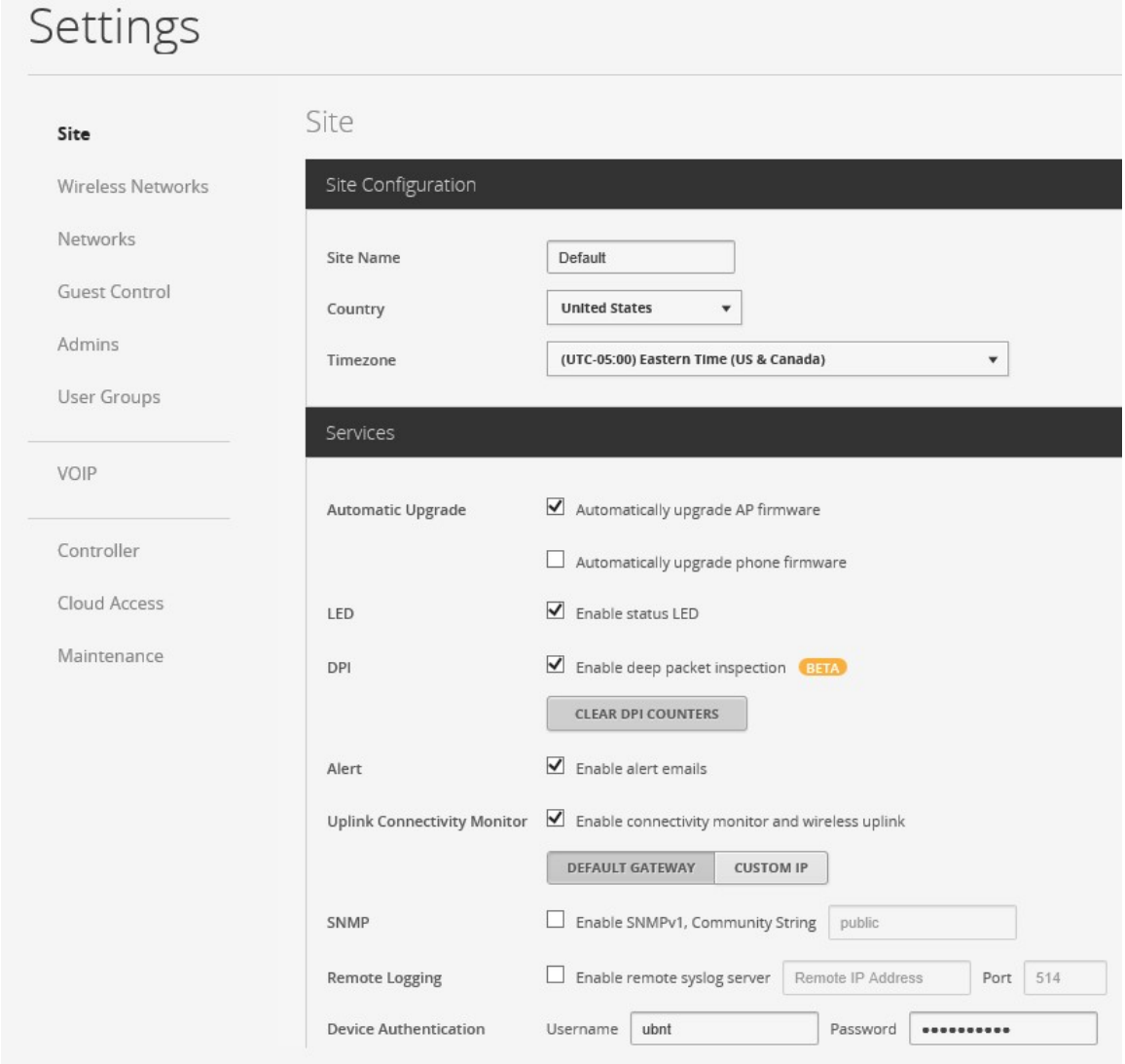

Figure 106 – UniFi Site

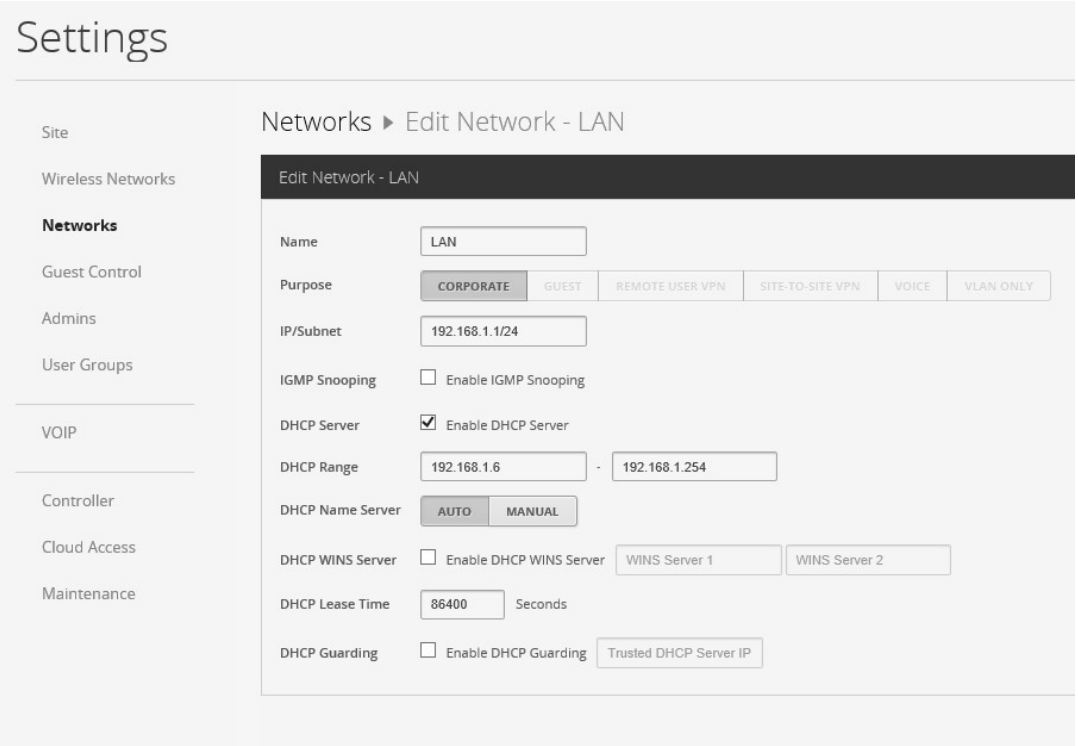

Figure 107 – UniFi Networks Edit LAN

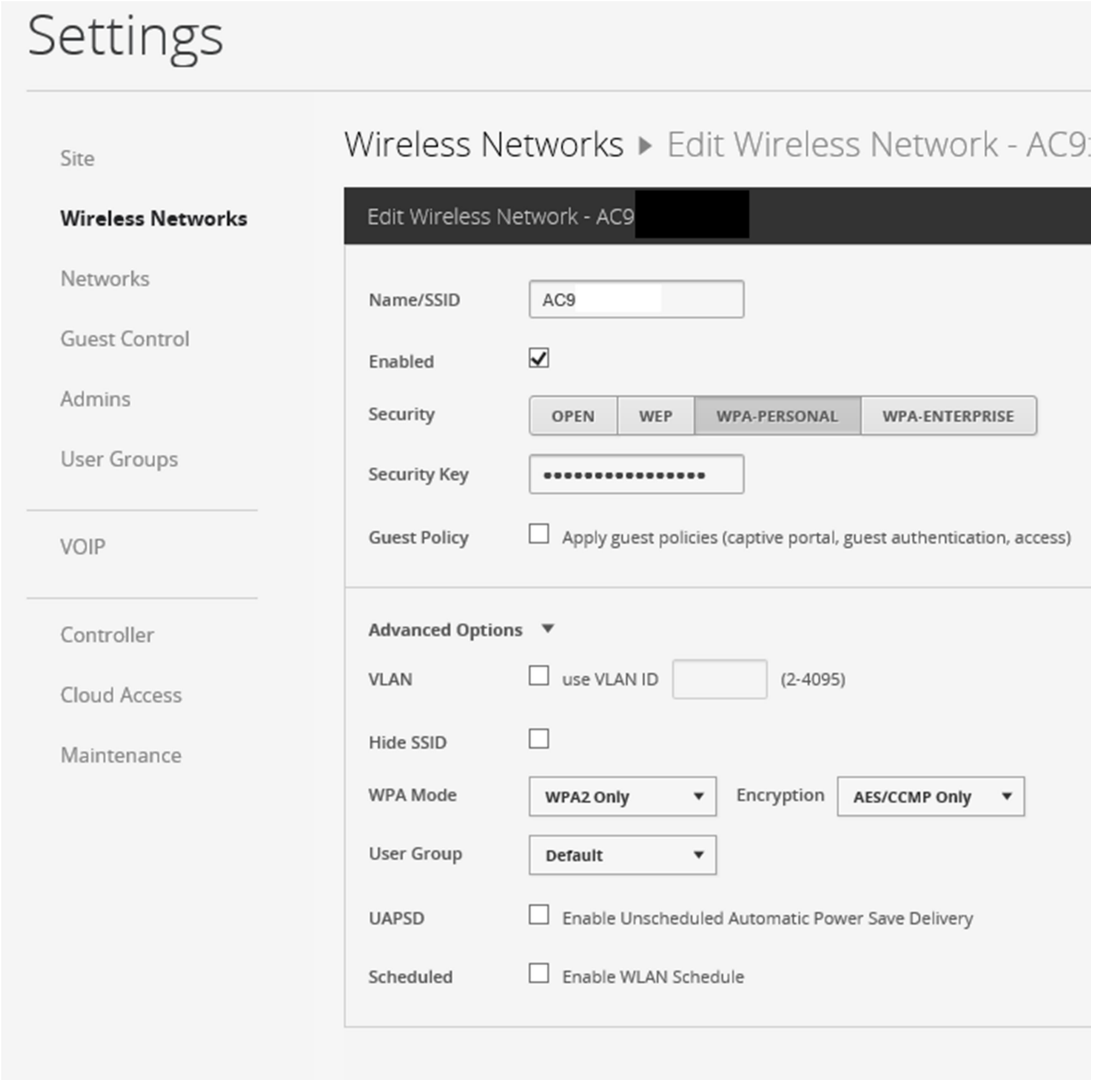

Figure 108 – UniFi Wireless Networks Edit Home Net

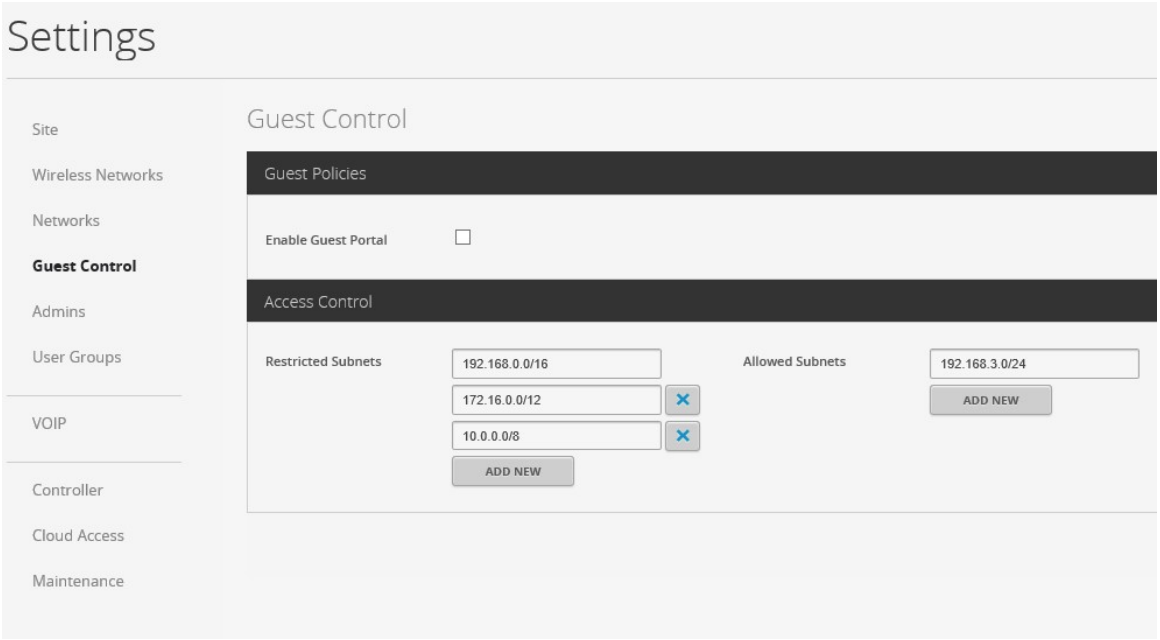

Figure 109 – UniFi Guest Control

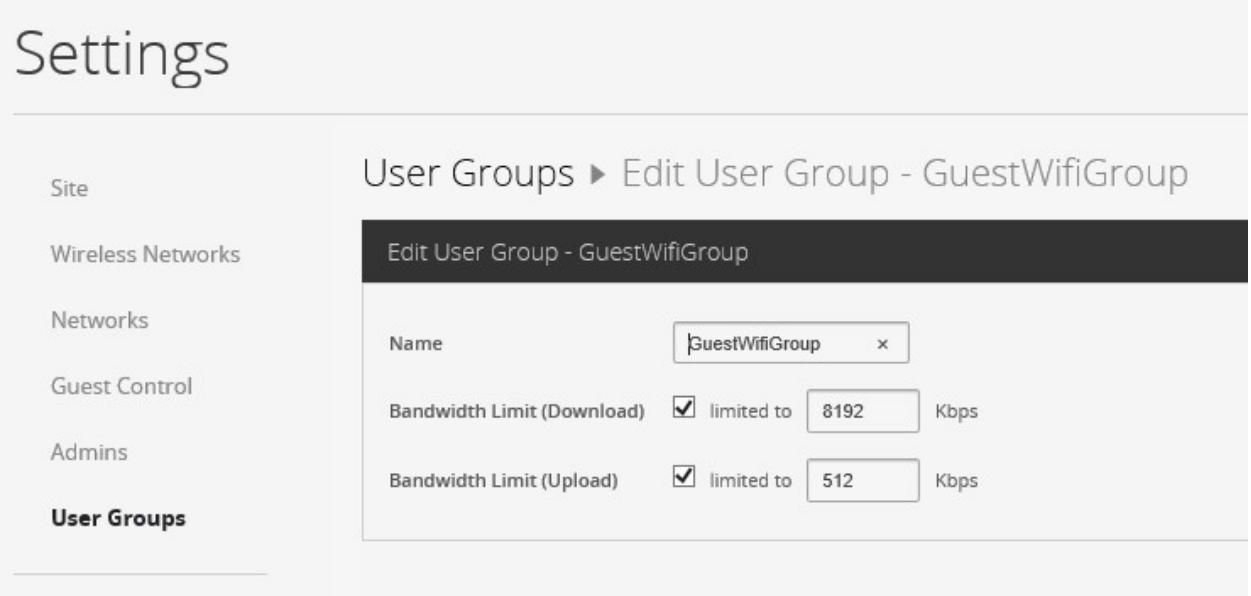

Figure 110 – UniFi Guest WiFi Group

I believe that the limits are per user, not per network, adjust limits as needed for your network bandwidth.

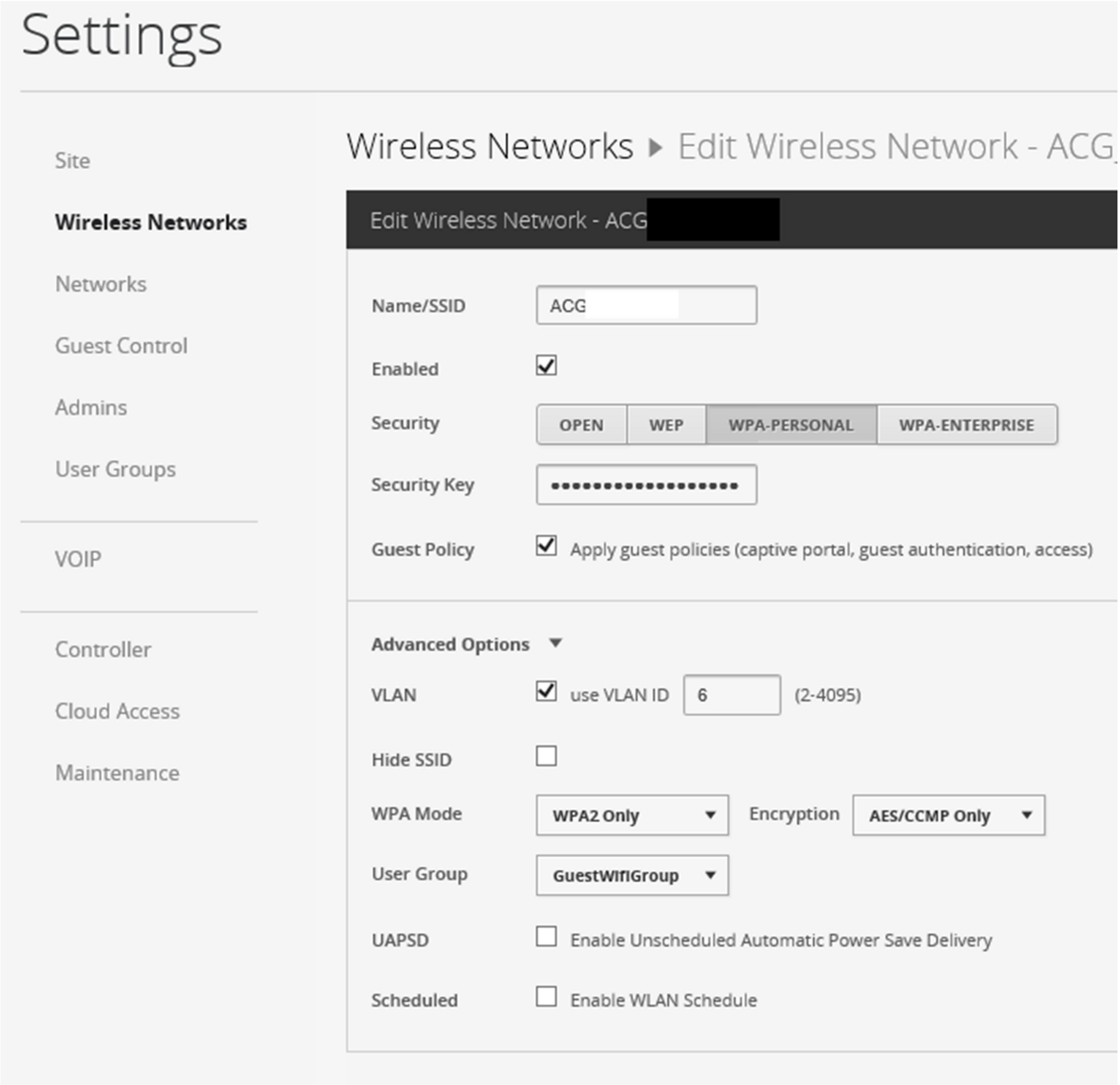

Figure 111 – UniFi Guest Wifi

Repeat Guest Wifi (above) for Vlan 7, Wifi Iot Net