Home-Network Implementation Using the Ubiquiti EdgeRouter X and Ubiquiti AP-AC-LR Access Point By Mike Potts	=	Home-Network Implementation Using the Ubiquiti EdgeRouter X and Ubiquiti AP-AC-LR Access Point By Mike Potts
Project Home https://github.com/mjp66/Ubiquiti	<>	Check for updates at: https://github.com/mjp66/Ubiquiti
Table of Contents 	=	Table of Contents
	<>	

	=	
Table of Tables		Table of Tables
	<>	
	=	
	<>	
1. Overview This guide will attempt to show users how to set up two Ubiquiti pieces of » equipment, to provide for a secure and flexible firewall / router and a Wi-Fi Access Point. The two pieces of equipment » used in this guide are: - Ubiquiti EdgeRouter X (about $50 when this guide was » written) - Ubiquiti AP-AC-LR Wi-Fi Access Point (about $100 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	=	1. Overview This guide will attempt to show users how to set up two Ubiquiti pieces of » equipment, to provide for a secure and flexible firewall / router and a Wi-Fi Access Point. The two pieces of equipment » used in this guide are: - Ubiquiti EdgeRouter X (about $50 when this guide was » written) - Ubiquiti AP-AC-LR Wi-Fi Access Point (about $100 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 configuration 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 friends' tablets and smartphones - Wi-Fi IOT Network For Wi-Fi Internet-Of-Things devices The Wired Home Network and Wi-Fi Home Network is 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. None of » these Networks can communicate with the Wired Separate Network, and the Wired Separate Network cannot » communicate with them. This guide assumes that you will be using both an Ubiquiti EdgeRouter X (ER-X) and » some model of Ubiquiti Access		SSIDs. The networks provided by this equipment configuration 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 friends' tablets and smartphones - Wi-Fi IOT Network For Wi-Fi Internet-Of-Things devices The Wired Home Network and Wi-Fi Home Network is 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. None of » these Networks can communicate with the Wired Separate Network, and the Wired Separate Network cannot » communicate with them. This guide assumes that you will be using both an Ubiquiti EdgeRouter X (ER-X) and » some model of Ubiquiti Access
Point (UAP). I tend to use the terms ER-X and EdgeRouter somewhat interchangeable » within this quide.	<>	Point (UAP). I tend to use the terms ER-X and EdgeRouter somewhat interchangeable » within this guide.
	=	
Page 4 of 136 » 2/4/2019	<>	Page 4 of 157 » 5/18/2019
2. Disclaimer This is a guide, your results may vary. I am not a network engineer. Enough said. 3. Purpose	=	2. Disclaimer This is a guide, your results may vary. I am not a network engineer. Enough said. 3. Purpose
One purpose of this guide is to provide a stable and usable router / firewall / » access point configuration.	<>	One purpose of this guide is to provide a stable and usable router / firewall / » access point configuration. This specific implementation is aimed at the Home / SOHO user.
Another purpose is to provide background on what these configuration settings » accomplish, so that the reader can understand why these settings were chosen. I wrote this guide because I REALLY like this router. I was mostly motivated to switch routers by reading http://routersecurity.org/ and	=	Another purpose is to provide background on what these configuration settings » accomplish, so that the reader can understand why these settings were chosen. I wrote this guide because I REALLY like this router. I was mostly motivated to switch routers by reading http://routersecurity.org/ and

http://routersecurity.org/bugs.php. This website should scare just about anybody » that is currently using consumer / commercial routers. I'm so glad to be finished with that buggy » equipment. The only trouble with this router is that it is meant for professionals to use. » You have to scrounge around forums for postings on how to configure specific items. This doesn't mean that the » forum people are not friendly, just that the needed answers are not all in one place. Sometimes the answers are a » little bit terse for a new user. As stated, I am not a network engineer. This guide is the documentation, for the configuration that I setup for myself. » It took me a huge amount of time to put this document together. I've tried to write this guide in a teaching » manner, and cite references where I could. Note that I specifically call this a ‘guide’. When you go through this » document you should: experiment, modify, learn, tinker and play, extend, and learn some more. Mix and match the » sections as you see fit. Most of my source information came from reading postings at: https://community.ubnt.com/t5/EdgeMAX/bd-p/EdgeMAX		http://routersecurity.org/bugs.php. This website should scare just about anybody » that is currently using consumer / commercial routers. I'm so glad to be finished with that buggy » equipment. The only trouble with this router is that it is meant for professionals to use. » You have to scrounge around forums for postings on how to configure specific items. This doesn't mean that the » forum people are not friendly, just that the needed answers are not all in one place. Sometimes the answers are a » little bit terse for a new user. As stated, I am not a network engineer. This guide is the documentation, for the configuration that I setup for myself. » It took me a huge amount of time to put this document together. I've tried to write this guide in a teaching » manner, and cite references where I could. Note that I specifically call this a ‘guide’. When you go through this » document you should: experiment, modify, learn, tinker and play, extend, and learn some more. Mix and match the » sections as you see fit. Most of my source information came from reading postings at: https://community.ubnt.com/t5/EdgeMAX/bd-p/EdgeMAX
	-+	
When this document was ready, I joined the Ubiquiti community and announced it at: https://community.ubnt.com/t5/EdgeMAX/New-ERX-AC-AP-LR-setup-guide-for-beginners/t » d-p/1906477	=	When this document was ready, I joined the Ubiquiti community and announced it at: https://community.ubnt.com/t5/EdgeMAX/New-ERX-AC-AP-LR-setup-guide-for-beginners/t » d-p/1906477
	-+	
If you have specific questions about this configuration, your best bet is to » research postings at the above EdgeMax link, then try and experiment for yourself. If you get stuck, then join the » Ubiquiti community and ask. I’ve now purchased an additional ER-X router to continue experimenting and for use in » refining this guide. Note that the associated backup file(s) on github are not being actively » maintained or updated with later changes being made in this guide. It is there as a reference.	=	If you have specific questions about this configuration, your best bet is to » research postings at the above EdgeMax link, then try and experiment for yourself. If you get stuck, then join the » Ubiquiti community and ask. I’ve now purchased an additional ER-X router to continue experimenting and for use in » refining this guide. Note that the associated backup file(s) on github are not being actively » maintained or updated with later changes being made in this guide. It is there as a reference.
	<>	Page 5 of 157 » 5/18/2019 4. Alternate EdgeRouter Models There are now alternate “nicely priced” EdgeRouters available. I have no » experience with any of them.

		https://www.ui.com/edgemax/comparison/ https://store.ui.com/products/edgerouter-10x https://community.ubnt.com/t5/EdgeRouter/Anyone-want-to-share-their-experience-wit » h-ER-10X/m- p/2765723#M250254 https://store.ui.com/collections/routing-switching/products/edgerouter-12 https://community.ubnt.com/t5/EdgeRouter/New-ER-12-owner-ER-12-Questions/m-p/27686 » 23#M250484
Page 5 of 136 » 2/4/2019 4. EdgeRouter IP Address Use		Page 6 of 157 » 5/18/2019 5. EdgeRouter IP Address Use
For the purposes of this guide, I am assuming that you will put your 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 set up or re-configure your existing router to use IP addresses of 192.168.2.X on its LAN » ports. Existing router addresses of 192.168.0.X or 192.168.1.X will also work. Your existing equipment may have the » “Cable or DSL Modem” portion and “Your Existing Firewall / Router” portion combined into one single » unit. See Figure 2 - EdgeRouter Configuration Setup. You will also need a computer to setup the EdgeRouter. Figure 2 - EdgeRouter Configuration Setup Most cable / DSL modems seem to be pre-configured for DHCP, and for using » addresses of 192.168.0.X or 192.168.1.X on their LAN ports. Therefore, I configured the EdgeRouter Network » addresses not to include those ranges. I deliberately left the address range of 192.168.2.X unused within the » EdgeRouter, so those addresses could be used by an existing firewall / router’s LAN ports. If the EdgeRouter was using an address that was also used by your Cable / DSL » modem, it would mask / hide that equipment’s setup web page(s), and you would not be able to access those pages. The EdgeRouter will NOT work if the address presented via DHCP to its eth0 port	=	For the purposes of this guide, I am assuming that you will put your 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 set up or re-configure your existing router to use IP addresses of 192.168.2.X on its LAN » ports. Existing router addresses of 192.168.0.X or 192.168.1.X will also work. Your existing equipment may have the » “Cable or DSL Modem” portion and “Your Existing Firewall / Router” portion combined into one single » unit. See Figure 2 - EdgeRouter Configuration Setup. You will also need a computer to setup the EdgeRouter. Figure 2 - EdgeRouter Configuration Setup Most cable / DSL modems seem to be pre-configured for DHCP, and for using » addresses of 192.168.0.X or 192.168.1.X on their LAN ports. Therefore, I configured the EdgeRouter Network » addresses not to include those ranges. I deliberately left the address range of 192.168.2.X unused within the » EdgeRouter, so those addresses could be used by an existing firewall / router’s LAN ports. If the EdgeRouter was using an address that was also used by your Cable / DSL » modem, it would mask / hide that equipment’s setup web page(s), and you would not be able to access those pages. The EdgeRouter will NOT work if the address presented via DHCP to its eth0 port

» maps anywhere within one of the address ranges used internally by the EdgeRouter. If your Internet Service Provider’s (ISP) equipment does not provide an IP address » via DHCP, then you will need to adjust your WAN (eth0) settings after running the setup wizard. In particular, if » you need to use PPPoE, then you might want to read:		» maps anywhere within one of the address ranges used internally by the EdgeRouter. If your Internet Service Provider’s (ISP) equipment does not provide an IP address » via DHCP, then you will need to adjust your WAN (eth0) settings after running the setup wizard. In particular, if » you need to use PPPoE, then you might want to read:
	-+	
https://community.ubnt.com/t5/EdgeMAX/Can-t-open-some-webpages/m-p/1950743/highlig » ht/true#M163311	=	https://community.ubnt.com/t5/EdgeMAX/Can-t-open-some-webpages/m-p/1950743/highlig » ht/true#M163311
	-+	
https://samuel.kadolph.com/2015/02/mtu-and-tcp-mss-when-using-pppoe-2/	=	https://samuel.kadolph.com/2015/02/mtu-and-tcp-mss-when-using-pppoe-2/
Page 6 of 136 » 2/4/2019 5. Acquire EdgeRouter Documentation	<>	Page 7 of 157 » 5/18/2019 6. Acquire EdgeRouter Documentation
On the computer you use 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.	=	On the computer you use 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.
6. Web Resources	<>	7. 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-resourc » es These postings perform similar items as this guide does:	=	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-resourc » es These postings perform similar items as this guide does:

https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-segmentation/td-p/1767545 https://help.ubnt.com/hc/en-us/articles/218889067-EdgeMAX-How-to-Protect-a-Guest-N » etwork-on-EdgeRouter		https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-segmentation/td-p/1767545 https://help.ubnt.com/hc/en-us/articles/218889067-EdgeMAX-How-to-Protect-a-Guest-N » etwork-on-EdgeRouter
Page 7 of 136 » 2/4/2019 7. Initial EdgeRouter Hardware Setup	<>	Page 8 of 157 » 5/18/2019 8. Initial EdgeRouter Hardware Setup
Configure the setup computer’s Ethernet jack as having a fixed IP address of » 192.168.1.X (where X is 2 to 254), and a netmask of 255.255.255.0. There are many tutorials available on the internet » that shows how to configure a computer’s Ethernet port to use a fixed IP address. One way to configure a Windows » 10 computer is: Control Panel -> Network & Internet -> Ethernet -> Change Adapter Settings » -> Internet Protocol Version 4 -> Properties -> Use the following IP address. 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.	=	Configure the setup computer’s Ethernet jack as having a fixed IP address of » 192.168.1.X (where X is 2 to 254), and a netmask of 255.255.255.0. There are many tutorials available on the internet » that shows how to configure a computer’s Ethernet port to use a fixed IP address. One way to configure a Windows » 10 computer is: Control Panel -> Network & Internet -> Ethernet -> Change Adapter Settings » -> Internet Protocol Version 4 -> Properties -> Use the following IP address. 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.
Page 8 of 136 » 2/4/2019 8. Initial EdgeRouter Login	<>	Page 9 of 157 » 5/18/2019 9. 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	=	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.		» 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		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.		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		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.		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		Figure 7 – Basic Setup Question
Page 9 of 136 » 2/4/2019	<>	Page 10 of 157 » 5/18/2019
You will land on the Dashboard screen. See Figure 8 – Initial Dashboard Screen.	=	You will land on the Dashboard screen. See Figure 8 – Initial Dashboard Screen.
Figure 8 – Initial Dashboard Screen	<>	Figure 8 – Initial Dashboard Screen
	=	
Reference Quick Start Guide and the User’s Guide @Chapter 2:Using EdgeOS.		Reference Quick Start Guide and the User’s Guide @Chapter 2:Using EdgeOS.
9. Update EdgeRouter Firmware	<>	10. Update EdgeRouter Firmware
On your setup computer, download the NEWEST firmware from: https://www.ubnt.com/download/edgemax/edgerouter-x/er-x For reference, during the writing of this document, the firmware was at: “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.	=	On your setup computer, download the NEWEST firmware from: https://www.ubnt.com/download/edgemax/edgerouter-x/er-x For reference, during the writing of this document, the firmware was at: “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	<>	Figure 9 – System Button
	=	
Sometimes the System button and/or the Alerts button, which is right next to the » System button, don’t seem to work for me. I usually just click the other button twice, and then click the » button I want. You might want to join the Ubiquiti community and sign up for notifications about » new software / firmware updates. You could also just periodically poll the above link, looking for new		Sometimes the System button and/or the Alerts button, which is right next to the » System button, don’t seem to work for me. I usually just click the other button twice, and then click the » button I want. You might want to join the Ubiquiti community and sign up for notifications about » new software / firmware updates. You could also just periodically poll the above link, looking for new

» updates. It is probably a good idea to keep (somewhat) up to date firmware on your EdgeRouter, for security updates.		» updates. It is probably a good idea to keep (somewhat) up to date firmware on your EdgeRouter, for security updates.
Page 10 of 136 » 2/4/2019	<>	Page 11 of 157 » 5/18/2019
The System window will then pop-up an overlay that will cover most of your screen. » See Figure 10 – System Pop-up Screen.	=	The System window will then pop-up an overlay that will cover most of your screen. » See Figure 10 – System Pop-up Screen.
Figure 10 – System Pop-up Screen		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.		Find the “Upgrade System Image” section, and press the “Upload a file” button. See » Figure 11 – Upgrade System Image.
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.		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		Figure 12 – Upload a file
Page 11 of 136 » 2/4/2019	<>	Page 12 of 157 » 5/18/2019
You will eventually be asked if you want to reboot the EdgeRouter. Press the » “Reboot” button. You will then be asked to confirm the reboot, click on the “Yes, I’m sure” button. See Figure 13 – » Upgrade Complete Dialog. The router will inform you that it is rebooting. See Figure 14 – Reboot Process.	=	You will eventually be asked if you want to reboot the EdgeRouter. Press the » “Reboot” button. You will then be asked to confirm the reboot, click on the “Yes, I’m sure” button. See Figure 13 – » Upgrade Complete Dialog. The router will inform you that it is rebooting. See Figure 14 – Reboot Process.
Figure 14 – Reboot » Process		Figure 14 – Reboot » Process
Figure 13 – Upgrade Complete Dialog		Figure 13 – Upgrade Complete Dialog
While the EdgeRouter is rebooting, the web page will present you with a Lost » Connection Dialog. See Figure 15 – Lost Connection Dialog. Eventually, when the EdgeRouter has fully re-booted, the presented dialog will » change to Figure 16 – Timed-Out Dialog. This is a nice touch of web programming from Ubiquiti, so you can easily » know when re-booting has completed. Press the Reload button.		While the EdgeRouter is rebooting, the web page will present you with a Lost » Connection Dialog. See Figure 15 – Lost Connection Dialog. Eventually, when the EdgeRouter has fully re-booted, the presented dialog will » change to Figure 16 – Timed-Out Dialog. This is a nice touch of web programming from Ubiquiti, so you can easily » know when re-booting has completed. Press the Reload button.
Figure 15 – Lost Connection Dialog Figure 16 – » Timed-Out Dialog		Figure 15 – Lost Connection Dialog Figure 16 – » Timed-Out Dialog
Page 12 of 136 » 2/4/2019	<>	Page 13 of 157 » 5/18/2019
You will be asked to login; please enter the username and password into the	=	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		» dialog. The default username is “ubnt” and the default password is “ubnt”. See Figure 17 – Login Dialog. Figure 17 – Login Dialog You should be presented with a dialog box stating that the “Router is in default » config. Do you want to start with the Basic Setup wizard?” Answer “no.” Reference Figure 7 – Basic Setup Question. You will (again) land at the Dashboard screen. Reference Figure 8 – Initial » Dashboard Screen. Check the upper left of the screen and verify that you are presented with the version of code that you » just downloaded. See Figure 18 – Example EdgeRouter Version. Figure 18 – Example EdgeRouter Version
	-+	Additional Reference: https://help.ubnt.com/hc/en-us/articles/205146110-EdgeRouter-How-to-Upgrade-the-Ed » geOS-Firmware
If you get your EdgeRouter messed up, you might need to factory reset it. Here are » some link(s):	=	If you get your EdgeRouter messed up, you might need to factory reset it. Here are » some link(s):
	-+	
https://help.ubnt.com/hc/en-us/articles/205202620-EdgeRouter-Reset-to-Factory-Defa » ults	=	https://help.ubnt.com/hc/en-us/articles/205202620-EdgeRouter-Reset-to-Factory-Defa » ults
	-+	
https://help.ubnt.com/hc/en-us/articles/360002231073-EdgeRouter-How-to-Use-SSH-Rec » overy-	=	https://help.ubnt.com/hc/en-us/articles/360002231073-EdgeRouter-How-to-Use-SSH-Rec » overy-
	-+	
https://community.ubnt.com/t5/EdgeRouter/ERX-ERX-SFP-System-Recovery/td-p/2056921	=	https://community.ubnt.com/t5/EdgeRouter/ERX-ERX-SFP-System-Recovery/td-p/2056921
	<>	https://community.ubnt.com/t5/EdgeRouter/ERX-ERX-SFP-System-Recovery/m-p/2056921 If you really get your EdgeRouter into a non-booting mode, you could try new TFTP » recovery methods: https://help.ubnt.com/hc/en-us/articles/360018189493 https://community.ubnt.com/t5/EdgeRouter/TFTP-recovery-images-for-EdgeOS-request/m » -p/2676042#M240903 https://community.ubnt.com/t5/EdgeRouter/How-to-connect-ER-X-serial-console/m-p/26 » 07963#M233420 https://community.ubnt.com/t5/EdgeRouter/Updated-Edgerouter-X-to-EdgeMAX-EdgeRoute » r-software-release- v1/m-p/2711039/highlight/true#M244509
Page 13 of 136 » 2/4/2019 10. About Using Two or More Ubiquiti Access Points		Page 14 of 157 » 5/18/2019 11. About Using Two or More Ubiquiti Access Points
Some people have wanted to connect two (or more) Ubiquiti Access Points (UAPs) to	=	Some people have wanted to connect two (or more) Ubiquiti Access Points (UAPs) to

» their ER-X to provide more /		» their ER-X to provide more /
wider WiFi coverage. The following ideas should work, but I have only tested » Methods 1 and 4. Therefore, the	<>	wider WiFi coverage. The following ideas should work, but I have only tested » Methods 1 and 4. Therefore, the
following directions are approximate. Method 1: Connect an 802.1Q capable switch to eth4, and then connect your access » points to this switch. Some	=	following directions are approximate. Method 1: Connect an 802.1Q capable switch to eth4, and then connect your access » points to this switch. Some
switches will need to be specifically configured to pass VLAN 6 and VLAN 7 data. » The HomeNet / trunk / 192.168.3.X data will probably not need to be specifically configured.	<>	switches will need to be specifically configured to pass VLAN 6,7,8 data. The » HomeNet / trunk / 192.168.3.X data will probably not need to be specifically configured.
Netgear and TP-Link make some inexpensive switches which should work. Some models » are: Netgear: GS105Ev2 (5 port) and GS108Tv2 (8 port) TP-Link: TL-SG105E (5 port) and TL-SG108E (8 port) TP-Link: TL-SG105 Ver 2.1 (5 port) UN-managed switch	=	Netgear and TP-Link make some inexpensive switches which should work. Some models » are: Netgear: GS105Ev2 (5 port) and GS108Tv2 (8 port) TP-Link: TL-SG105E (5 port) and TL-SG108E (8 port) TP-Link: TL-SG105 Ver 2.1 (5 port) UN-managed switch
Note that these switches are typically configured via a Microsoft Windows (only) » program. Some of these switches now have an embedded web server in them for configuration. These web servers may » be incomplete in implementing the needed configuration commands. I have now tested Method 1 with a » TP-LINK TL-SG105EV2 managed switch and separately tested with a TL-SG105 Ver 2.1 Un-managed switch. I » believe you will need a hardware version of V2 or above to operate correctly. For configuration details, » reference Appendix A. I suggest that you don’t perform these operations until you are finished with the rest of » this document.	<>	Note that these managed switches are typically configured via a Microsoft Windows » (only) program. Some of these switches now have an embedded web server in them for configuration. These » web servers may be incomplete in implementing the needed configuration commands. I have now tested » Method 1 with a TP-LINK TL-SG105EV2 managed switch and separately tested with a TL-SG105 Ver 2.1 Un-managed » switch. I believe you will need a hardware version of V2 or above to operate correctly. For configuration » details, reference Appendix A. I suggest that you don’t perform these operations until you are finished with the » rest of this document.
Method 2: Plug your one or two additional UAP(s) directly into the ER-X router. » You will need to forego the Wired IOT Network and/or the Wired Separate Network. This would alternately configure » the HomeNet on ports 1,3,4 or 2,3,4 or 1,2,3,4. This saves the cost of needing to purchase an additional » 802.1Q capable switch, but delivers fewer features.	=	Method 2: Plug your one or two additional UAP(s) directly into the ER-X router. » You will need to forego the Wired IOT Network and/or the Wired Separate Network. This would alternately configure » the HomeNet on ports 1,3,4 or 2,3,4 or 1,2,3,4. This saves the cost of needing to purchase an additional » 802.1Q capable switch, but delivers fewer features.
To include port 1 in HomeNet, instead CHECK the "One LAN" box in section 11 / » Figure 21. You will need to figure	<>	To include port 1 in HomeNet, instead CHECK the "One LAN" box in section 12 / » Figure 21. You will need to figure
out the additional associated changes which are later in this document.	=	out the additional associated changes which are later in this document.
To include port 2 in HomeNet, DON'T follow sections 18, 19, 24. You will need to » figure out the additional	<>	To include port 2 in HomeNet, DON'T follow sections 19, 20, 25. You will need to » figure out the additional
associated changes which are later in this document. Method 3: Use an ER-X SFP instead of a “plain” ER-X. This model router has an	=	associated changes which are later in this document. Method 3: Use an ER-X SFP instead of a “plain” ER-X. This model router has an

» extra SFP port on it. You will also need an appropriate SFP adapter to use the extra port. Using this Method, just » about doubles the cost of this project. I hear that most ”copper” SFP modules do not auto-negotiate link speeds. Method 4: Configure the additional Ubiquiti access points to WiFi mesh / chain to » the original UAP. [Update: it appears that multi-hop support has been added in later versions of AP » firmware.] Reference the following:		» extra SFP port on it. You will also need an appropriate SFP adapter to use the extra port. Using this Method, just » about doubles the cost of this project. I hear that most ”copper” SFP modules do not auto-negotiate link speeds. Method 4: Configure the additional Ubiquiti access points to WiFi mesh / chain to » the original UAP. [Update: it appears that multi-hop support has been added in later versions of AP » firmware.] Reference the following:
https://help.ubnt.com/hc/en-us/articles/115002262328	<>	https://help.ubnt.com/hc/en-us/articles/115002262328-UniFi-UAP-Configuring-Wireles » s-Uplink
Ubiquiti also makes specific equipment for multi-hop deployments. Some of that » equipment is rated for outdoor use. Note that using mesh equipment / modes will likely decrease your wireless » bandwidth by at-least half. If you can, wire each Access Point back to your EdgeRouter.	=	Ubiquiti also makes specific equipment for multi-hop deployments. Some of that » equipment is rated for outdoor use. Note that using mesh equipment / modes will likely decrease your wireless » bandwidth by at-least half. If you can, wire each Access Point back to your EdgeRouter.
Page 14 of 136 » 2/4/2019	<>	Page 15 of 157 » 5/18/2019
General: Except for method 4, Each UAP should be Ethernet-wired and they should all be » configured the same, except that each UAP should be configured using different and non-overlapping WiFi channels. » For the U.S., the non- overlapping 2.4GHz channels are: 1, 6, 11. I would look at https://community.ubnt.com/t5/UniFi-Wireless/bd-p/UniFi for more » info on UAP setup. Remember that Ubiquiti Access Points (UAPs) are capable of supporting four SSIDs, » only three were used in the guide. You have another WiFi SSID available for use.	=	General: Except for method 4, Each UAP should be Ethernet-wired and they should all be » configured the same, except that each UAP should be configured using different and non-overlapping WiFi channels. » For the U.S., the non- overlapping 2.4GHz channels are: 1, 6, 11. I would look at https://community.ubnt.com/t5/UniFi-Wireless/bd-p/UniFi for more » info on UAP setup. Remember that Ubiquiti Access Points (UAPs) are capable of supporting four SSIDs, » only three were used in the guide. You have another WiFi SSID available for use.
See also section 13, the “VLAN References” portion of section 27, and more » information in Appendix A.	<>	See also section 14, the “VLAN References” portion of section 28, and more » information in Appendix A.
Ethernet data can be sent over cable TV coax by using “Multimedia over Coax » Alliance (MOCA)” adapters. These can be used for general purpose Ethernet drops or for wiring / placing UAPs within » a house. These are discussed in Appendix B.	=	Ethernet data can be sent over cable TV coax by using “Multimedia over Coax » Alliance (MOCA)” adapters. These can be used for general purpose Ethernet drops or for wiring / placing UAPs within » a house. These are discussed in Appendix B.
Page 15 of 136 » 2/4/2019 11. EdgeRouter Wizard	<>	Page 16 of 157 » 5/18/2019 12. EdgeRouter Wizard
Press the “Wizards” button, which is located in the upper-right portion of the	=	Press the “Wizards” button, which is located in the upper-right portion of the

» Dashboard screen. See Figure 19 – Wizards Button.		» Dashboard screen. See Figure 19 – Wizards Button.
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.		You will see the following (portion shown) of the Wizard Screen. See Figure 20 – » Wizard Screen Portion.
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”.		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”.
Page 16 of 136 » 2/4/2019	<>	Page 17 of 157 » 5/18/2019
Choose “WAN+2LAN2”. See Figure 21 – Wan+2LAN2 Dialog. You will need to expand / » open sections, and make the following selections:	=	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:		In the “Internet Port” section:
Port: eth0		Port: eth0
Internet CT: DHCP		Internet CT: DHCP
VLAN: UN-Checked (Internet Connection is on VLAN)		VLAN: UN-Checked (Internet Connection is on VLAN)
Firewall: CHECKED (Enable the default firewall)		Firewall: CHECKED (Enable the default firewall)
DHCv6 PD: UN-Checked (Enable DHCv6 Prefix Delegation)		DHCv6 PD: UN-Checked (Enable DHCv6 Prefix Delegation)
In the next (unlabeled) section:		In the next (unlabeled) section:
One LAN: UN-Checked (Only use one LAN)		One LAN: UN-Checked (Only use one LAN)
In the “(Optional) Secondary LAN port (eth1)” section:		In the “(Optional) Secondary LAN port (eth1)” section:
Address: 192.168.4.1 / 255.255.255.0		Address: 192.168.4.1 / 255.255.255.0
DHCP: CHECKED (Enable the DHCP server)		DHCP: CHECKED (Enable the DHCP server)
In the “LAN ports (eth2, eth3, eth4)” section:		In the “LAN ports (eth2, eth3, eth4)” section:
Address: 192.168.3.1 / 255.255.255.0		Address: 192.168.3.1 / 255.255.255.0
DHCP: CHECKED (Enable the DHCP server)		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.		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 “Only use one LAN” selection informs the Wizard to un-bundle eth1 » from eth2-4, allowing for the provision of a separate Network. I used this eth1 Network for Wired IOT devices.		Unchecking the “Only use one LAN” selection informs the Wizard to un-bundle eth1 » from eth2-4, allowing for the provision of a separate Network. I used this eth1 Network for Wired IOT devices.
It is important that “Enable the default firewall” is CHECKED. The entire security » of this router depends upon this setting.		It is important that “Enable the default firewall” is CHECKED. The entire security » of this router depends upon this setting.

Under the “User setup” section, either change the default password to something » secure / unique or “Create new admin user” with a secure / unique password. If you “Create new admin user”, you » will need to also return to this dialog and delete the default “ubnt” login. You will need to remember your login » credentials. [Note you REALLY should make a new and unique admin-user login-name and then » delete the default ‘ubnt’ login- name for security.] Press “Apply” at the bottom of the screen.		Under the “User setup” section, either change the default password to something » secure / unique or “Create new admin user” with a secure / unique password. If you “Create new admin user”, you » will need to also return to this dialog and delete the default “ubnt” login. You will need to remember your login » credentials. [Note you REALLY should make a new and unique admin-user login-name and then » delete the default ‘ubnt’ login- name for security.] Press “Apply” at the bottom of the screen.
Page 17 of 136 » 2/4/2019	<>	Page 18 of 157 » 5/18/2019
Figure 21 – Wan+2LAN2 Dialog	=	Figure 21 – Wan+2LAN2 Dialog
Page 18 of 136 » 2/4/2019	<>	Page 19 of 157 » 8/2019 5/1
After Applying, you will be presented with Figure 22 – Replace Configuration. » Please study what it says. Press “Apply Changes.”	=	After Applying, you will be presented with Figure 22 – Replace Configuration. » Please study what it says. Press “Apply Changes.”
Figure 22 – Replace Configuration		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.		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		Figure 23 – Reboot into New Configuration
The EdgeRouter will inform you that it is rebooting. Reference Figure 14 – Reboot » Process. The EdgeRouter takes several minutes to reboot. Disconnect your setup computer’s Ethernet jack from the EdgeRouter’s eth0 » connection. Re-configure your setup computer’s Ethernet port back to using DHCP. Again, there are many tutorials » available on the internet that show		The EdgeRouter will inform you that it is rebooting. Reference Figure 14 – Reboot » Process. The EdgeRouter takes several minutes to reboot. Disconnect your setup computer’s Ethernet jack from the EdgeRouter’s eth0 » connection. Re-configure your setup computer’s Ethernet port back to using DHCP. Again, there are many tutorials » available on the internet that show
how to configure a computer’s Ethernet jack to use DHCP. Reference section 7 - » Initial EdgeRouter Hardware	<>	how to configure a computer’s Ethernet jack to use DHCP. Reference section 8 - » Initial EdgeRouter Hardware
Setup, but instead choose “Obtain an IP address automatically.” Also reference » Figure 3 – Windows 10 Ethernet Address Setup.	=	Setup, but instead choose “Obtain an IP address automatically.” Also reference » Figure 3 – Windows 10 Ethernet Address Setup.
Page 19 of 136 » 2/4/2019 12. EdgeRouter Re-Connection	<>	Page 20 of 157 » 5/18/2019 13. 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	=	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 “4 - EdgeRouter IP » Address Use.” Connect the	<>	using 192.168.3.0 through 192.168.7.255. Reference section “5 - EdgeRouter IP » Address Use.” Connect the
EdgeRouter’s eth0 port into your existing router’s LAN port with a standard » Ethernet cable. Connect your setup computer’s Ethernet port (now re-configured for DHCP) into the EdgeRouter’s eth3 » port. See Figure 2 - EdgeRouter Configuration Setup. Open a web browser on your computer and enter https://192.168.3.1 into the address » field. Acknowledge the browser’s security warning, Reference Figure 5 – IE Security » Certificate Example. Login to your EdgeRouter, as shown in Figure 17 – Login Dialog. You will be presented with the Dashboard Screen. See Figure 24 – Dashboard Screen.	=	EdgeRouter’s eth0 port into your existing router’s LAN port with a standard » Ethernet cable. Connect your setup computer’s Ethernet port (now re-configured for DHCP) into the EdgeRouter’s eth3 » port. See Figure 2 - EdgeRouter Configuration Setup. Open a web browser on your computer and enter https://192.168.3.1 into the address » field. Acknowledge the browser’s security warning, Reference Figure 5 – IE Security » Certificate Example. Login to your EdgeRouter, as shown in Figure 17 – Login Dialog. You will be presented with the Dashboard Screen. See Figure 24 – Dashboard Screen.
Figure 24 – Dashboard Screen		Figure 24 – Dashboard Screen
Page 20 of 136 » 2/4/2019 13. Network Naming	<>	Page 21 of 157 » 5/18/2019 14. 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.	=	Setting up the EdgeRouter, per this guide, provides for several separate Networks. » In this guide, I try to use the word “Network” (capitalized) for these. Each Network has a unique IP address range » / subnet. See Table 1 - Table of Networks.
Network Name IP Address Range Interface » VLAN Address Group Term Internet DHCP eth0 » No - Home Network 192.168.3.X eth3, eth4 » No HOME_GROUP Wired IOT Network 192.168.4.X eth1 » No WIRED_IOT_GROUP Wired Separate Network 192.168.5.X eth2 » 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	=	Network Name IP Address Range Interface » VLAN Address Group Term Internet DHCP eth0 » No - Home Network 192.168.3.X eth3, eth4 » No HOME_GROUP Wired IOT Network 192.168.4.X eth1 » No WIRED_IOT_GROUP Wired Separate Network 192.168.5.X eth2 » 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
	-+	Wi-Fi Spare Network 192.168.8.X - 8 » WIFI_SPARE_GROUP
Table 1 - Table of Networks	=	Table 1 - Table of Networks
Some of these Networks are on a Virtual LAN (VLAN). VLANs provide the ability for		Some of these Networks are on a Virtual LAN (VLAN). VLANs provide the ability for

» separate network data to be carried over shared Ethernet cables. Data that is “tagged” as belonging to a » specific VLAN cannot interact with either non-VLAN data (trunk data) or with data from any different VLAN. When VLANs are used, all devices involved with this data need to be VLAN aware. » Any network switches carrying VLAN traffic will need to be IEEE 802.1Q capable, e.g. a Level 2 managed switch.		» separate network data to be carried over shared Ethernet cables. Data that is “tagged” as belonging to a » specific VLAN cannot interact with either non-VLAN data (trunk data) or with data from any different VLAN. When VLANs are used, all devices involved with this data need to be VLAN aware. » Any network switches carrying VLAN traffic will need to be IEEE 802.1Q capable, e.g. a Level 2 managed switch.
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	<>	Note that the only VLAN traffic shown in Table 1 - Table of Networks is involved » with the Wi-Fi Guest Wifi Iot, and Wifi Spare Networks. The Ubiquiti AP-AC-LR access point is VLAN aware. Eventually » the Access Point will be
plugged directly into the EdgeRouter’s eth4 interface, so VLAN data will be able » to be carried between them. If you are going to deploy multiple Access Points, then the network switch attaching » the Access Points to the EdgeRouter’s eth4 port MUST be IEEE 802.1Q capable. This Wi-Fi VLAN data does NOT need to flow to devices on the Wired Home Network, » therefore, the network	=	plugged directly into the EdgeRouter’s eth4 interface, so VLAN data will be able » to be carried between them. If you are going to deploy multiple Access Points, then the network switch attaching » the Access Points to the EdgeRouter’s eth4 port MUST be IEEE 802.1Q capable. 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 (inexpensive) » unmanaged switch.. Reference Figure 1	<>	switch attached to the EdgeRouter’s eth3 interface can be a (inexpensive) » unmanaged switch. Reference Figure 1
- Overview Diagram. If they are needed, the network switches attached to the » EdgeRouter’s eth1 and/or eth2 interfaces can also be (inexpensive) unmanaged switches. Each Network is also customizable to provide functionality and connectivity. The » rest of this guide will provide sufficient details on that. There are many VLAN references on the web. Here is one brief tutorial: http://www.microhowto.info/tutorials/802.1q.html More References: https://help.ubnt.com/hc/en-us/articles/204976664-EdgeRouter-Packets-Processing I was asked to add a reference for google config to this guide, so here it is: https://github.com/mjp66/Ubiquiti/issues/31	=	- Overview Diagram. If they are needed, the network switches attached to the » EdgeRouter’s eth1 and/or eth2 interfaces can also be (inexpensive) unmanaged switches. Each Network is also customizable to provide functionality and connectivity. The » rest of this guide will provide sufficient details on that. There are many VLAN references on the web. Here is one brief tutorial: http://www.microhowto.info/tutorials/802.1q.html More References: https://help.ubnt.com/hc/en-us/articles/204976664-EdgeRouter-Packets-Processing I was asked to add a reference for google config to this guide, so here it is: https://github.com/mjp66/Ubiquiti/issues/31
Page 21 of 136 » 2/4/2019 14. EdgeRouter Command Line Interface (CLI)	<>	Page 22 of 157 » 5/18/2019 15. EdgeRouter Command Line Interface (CLI)
In most of Ubiquiti’s Edgerouter forum posts, steps to (re-)configure items are » given as Command line Interface (CLI) commands. In fact, not very many GUI screenshots are used, and they are » typically posted only by novices. The following steps show how to open and use the built-in CLI interface. Click on	=	In most of Ubiquiti’s Edgerouter forum posts, steps to (re-)configure items are » given as Command line Interface (CLI) commands. In fact, not very many GUI screenshots are used, and they are » typically posted only by novices. The following steps show how to open and use the built-in CLI interface. Click on

» the “CLI” button, in the upper- right screen. See Figure 25 – CLI Button.		» the “CLI” button, in the upper- right screen. See Figure 25 – CLI Button.
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.		The initial CLI window will appear as a semi-transparent overlay. See Figure 26 – » Initial CLI Window.
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.		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		Figure 27 – Logged-In CLI Window
CLI commands are typically divided into configuration commands and » non-configuration commands. The CLI interface will accept only configuration commands when in configuration mode. Type » the “configuration” command to enter configuration mode. The “exit” command is used to leave » configuration mode and return to normal (non-configuration) mode.		CLI commands are typically divided into configuration commands and » non-configuration commands. The CLI interface will accept only configuration commands when in configuration mode. Type » the “configuration” command to enter configuration mode. The “exit” command is used to leave » configuration mode and return to normal (non-configuration) mode.
Page 22 of 136 » 2/4/2019	<>	Page 23 of 157 » 5/18/2019
If you enter the “configure” command, the CLI window’s prompt will now include » “[edit]”. See Figure 28 – Configure CLI Window.	=	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		Figure 28 – Configure CLI Window
Many times when doing a commit and/or a save command, the page will need to be » refreshed. A refresh dialog box will pop-up on the screen. See Figure 29 – Configuration Change. Press the » “Refresh” button.		Many times when doing a commit and/or a save command, the page will need to be » refreshed. A refresh dialog box will pop-up on the screen. See Figure 29 – Configuration Change. Press the » “Refresh” button.
Figure 29 – Configuration Change		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		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
Page 23 of 136 » 2/4/2019 15. EdgeRouter Config Tree	<>	Page 24 of 157 » 5/18/2019 16. 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.	=	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		Figure 30 – Config Tree Button
When you press it, the “Configuration” Tree window will appear. See Figure 31 – » Config Tree Initial Screen.		When you press it, the “Configuration” Tree window will appear. See Figure 31 – » Config Tree Initial Screen.
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).		Using the config tree is an alternate method (for some items) to using the Command » Line Interface (CLI).
Page 24 of 136	<>	Page 25 of 157
» 2/4/2019		» 5/18/2019
16. My Command Line Trouble		17. My Command Line Trouble
When I was experimenting with dnsmasq, many internet resources simply gave CLI » commands to enable this feature. When I tried some of these commands, my EdgeRouter had problems. I no » longer remember what the exact problem was, but I noticed that sometimes when using the Config Tree, » multiple commands were issued. See Figure 32 – Example of Multiple Config Tree Commands.	=	When I was experimenting with dnsmasq, many internet resources simply gave CLI » commands to enable this feature. When I tried some of these commands, my EdgeRouter had problems. I no » longer remember what the exact problem was, but I noticed that sometimes when using the Config Tree, » multiple commands were issued. See Figure 32 – Example of Multiple Config Tree Commands.
Figure 32 – Example of Multiple Config Tree Commands		Figure 32 – Example of Multiple Config Tree Commands
Page 25 of 136	<>	Page 26 of 157
» 2/4/2019		» 5/18/2019
17. EdgeRouter Backup / Configuration Files		18. 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 Tree or » the GUI. You can find this configuration data within the config.boot file that is inside of » the backup file generated from the system window. The file that is generated is typically named » edgeos_ubnt_<date>.tar.gz, with <date> replaced by numbers representing todays date. To generate a backup file, first press the System button, as shown in Figure 9 – » System Button. You will be presented with the System screen, as shown in Figure 10 – System Pop-up Screen. Find and press the “Download” button under the Configuration Management & Device » Management section. See Figure 33 – Back Up Config Download Button.	=	When EdgeRouters are described in most internet forums, their configuration » parameters are usually described (in text) by a standard file format. Eventually, you will need to be fluent in » reading these files and translating that data into actions taken in the Command Line Interface (CLI), the Config Tree or » the GUI. You can find this configuration data within the config.boot file that is inside of » the backup file generated from the system window. The file that is generated is typically named » edgeos_ubnt_<date>.tar.gz, with <date> replaced by numbers representing todays date. To generate a backup file, first press the System button, as shown in Figure 9 – » System Button. You will be presented with the System screen, as shown in Figure 10 – System Pop-up Screen. Find and press the “Download” button under the Configuration Management & Device » Management section. See Figure 33 – Back Up Config Download Button.

Figure 33 – Back Up Config Download Button		Figure 33 – Back Up Config Download Button
You will be presented with a dialog of where to (open or) save your backup file.		You will be presented with a dialog of where to (open or) save your backup file.
» This dialog is browser specific.		» This dialog is browser specific.
Save your file to a directory of your choice on your setup computer. This file		Save your file to a directory of your choice on your setup computer. This file
» will be needed if you ever need to		» will be needed if you ever need to
reload your EdgeRouter.You may want to do this frequently, when setting up this		reload your EdgeRouter.You may want to do this frequently, when setting up this
» device.		» device.
Another way to obtain a relevant portion of this file is to issue one of the		Another way to obtain a relevant portion of this file is to issue one of the
» following commands into the Command		» following commands into the Command
Line Interface (CLI) window. For information about the CLI, reference section “14	<>	Line Interface (CLI) window. For information about the CLI, reference section “15
» - EdgeRouter Command Line		» - EdgeRouter Command Line
Interface (CLI)”.	=	Interface (CLI)”.
Two different / similar normal-mode CLI command for acquiring the system		Two different / similar normal-mode CLI command for acquiring the system
» configuration are:		» configuration are:
cat /config/config.boot		cat /config/config.boot
show configuration | no-more		show configuration | no-more
	-+	show configuration | cat
	=	
I will show as many portions of this config data as possible throughout this		I will show as many portions of this config data as possible throughout this
» guide. One goal of this guide is to teach		» guide. One goal of this guide is to teach
users enough about this EdgeRouter that they are comfortable reading and		users enough about this EdgeRouter that they are comfortable reading and
» understanding the backup files.		» understanding the backup files.
You would do well to save / keep multiple backup files, while you are working		You would do well to save / keep multiple backup files, while you are working
» through this guide.		» through this guide.
	-+	An alternate method of generating backup data is to issue one of these commands:
		show configuration commands
		show configuration commands | cat
		which dumps a list of configuration commands which should re-generate your
		» installation. Internally generating
		this list has to be pretty crazy, since many commands will depend upon other
		» commands having already being
		entered.
Link(s):	=	Link(s):
https://help.ubnt.com/hc/en-us/articles/360002535514		https://help.ubnt.com/hc/en-us/articles/360002535514
	<>	https://community.ubnt.com/t5/EdgeRouter/Edgerouter-CLI-command/m-p/2728959
Page 26 of 136		Page 27 of 157
» 2/4/2019		» 5/18/2019
		Page 28 of 157 5/18/2019
18. Remove eth2 from the EdgeRouter’s Internal Switch		19. Remove eth2 from the EdgeRouter’s Internal Switch
In this optional step, we will manually un-bundle the eth2 interface from the	=	In this optional step, we will manually un-bundle the eth2 interface from the

» EdgeRouter’s internal switch chip to provide for the Wired Separate Network on the eth2 interface. Un-bundling this » interface from switch0 enables a separate physical network. An additional network could be achieved by adding a » logical VLAN, but we are choosing to implement an additional network on the physical eth2 port. The switch » chip will remain enabled for eth3 and eth4 interfaces. Later, we will assign an IP address range to this port, » setup DHCP to provide IP addresses to eth2 connected devices, and create firewall rules that will keep this Network » isolated from the other Networks. If you choose to not implement the Wired Separate Network, there are other » associated steps you will not perform. Press the Dashboard Button. See Figure 34 – Dashboard Button.		» EdgeRouter’s internal switch chip to provide for the Wired Separate Network on the eth2 interface. Un-bundling this » interface from switch0 enables a separate physical network. An additional network could be achieved by adding a » logical VLAN, but we are choosing to implement an additional network on the physical eth2 port. The switch » chip will remain enabled for eth3 and eth4 interfaces. Later, we will assign an IP address range to this port, » setup DHCP to provide IP addresses to eth2 connected devices, and create firewall rules that will keep this Network » isolated from the other Networks. If you choose to not implement the Wired Separate Network, there are other » associated steps you will not perform. Press the Dashboard Button. See Figure 34 – Dashboard Button.
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.		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		Figure 35 – switch0’s Action Button
A sub-menu will appear, Select “Config” from the menu items. See Figure 36 – » switch0 Actions Config.		A sub-menu will appear, Select “Config” from the menu items. See Figure 36 – » switch0 Actions Config.
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.		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		Figure 37 – switch0 Configuration Figure 38 – » switch0 Switch Ports
Page 27 of 136 » 2/4/2019	<>	Page 29 of 157 » 5/18/2019
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.	=	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		Figure 39 – Busy Indicator Figure 40 – » Finished Checkmark
Page 28 of 136	<>	Page 30 of 157

» 2/4/2019 19. Configure EdgeRouter's eth2 IP Addresses		» 5/18/2019 20. 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.	=	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.
Page 29 of 136 » 2/4/2019 20. About DNS settings	<>	Page 31 of 157 » 5/18/2019 21. About DNS settings
I seem to have spent more time investigating DNS settings for the EdgeRouter than » in learning firewall rules.	=	I seem to have spent more time investigating DNS settings for the EdgeRouter than » in learning firewall rules.
Within this guide, I am now using Quad9 DNS addresses for the Home Network and » Level3 DNS addresses for the Separate Network. I am also using / forcing OpenDNS DNS addresses for the IOT and » Guest Networks. Change any or all of these addresses to the DNS provider(s) / resolver(s) addresses of your » choice. Some people are reporting that Quad9 is slower, See Section 75 - Adblocking and » Blacklisting as a possible security alternative.	<>	Within my router, and within this guide, I tried using Quad9 DNS addresses, but » have now switched back to Level3 DNS addresses for the Home Network. For training / clarity purposes within this » guide, I am using Google DNS resolvers for the Separate Network and within the EdgeRouter Itself. I am also » using AND forcing OpenDNS DNS addresses for the IOT and Guest Networks. Some people have reported that Quad9 is » slower, See Section 75 - Adblocking and Blacklisting as a security alternative. Change any or all of the listed DNS providers to ones of your own choosing. These » are used within this guide: Level3 (CenturyLink) resolver addresses are 209.244.0.3 » 209.244.0.4 Google resolver addresses are 8.8.8.8 » 8.8.4.4 OpenDNS resolver addresses are 208.67.222.222 » 208.67.220.220
Steve Gibson has a web page that can help you characterize various DNS providers.	=	Steve Gibson has a web page that can help you characterize various DNS providers.

» Since it runs from your computer, the results are localized to your connection / ISP. Until the EdgeRouter » is fully setup, you might want to run this from a computer that is currently wired outside of the EdgeRouter. This » is shown as “Existing LAN” in Figure 2 - EdgeRouter Configuration Setup. The page is at: https://www.grc.com/dns/benchmark.htm Steve Gibson has another web page that tests the “spoofability” (security) of DNS » resolvers. It is at: https://www.grc.com/dns/dns.htm Here are some alternate DNS resolvers, and additional DNS information pages: https://en.wikipedia.org/wiki/List_of_managed_DNS_providers https://dns.norton.com/configureRouter.html, https://dns.norton.com/faq.html https://support.opendns.com/hc/en-us/articles/228006047-Generalized-Router-Configu » ration-Instructions https://use.opendns.com/#router https://en.wikipedia.org/wiki/OpenDNS https://www.quad9.net/ and https://www.quad9.net/faq https://www.globalcyberalliance.org/initiatives/quad9.html EdgeRouter DNS References: https://help.ubnt.com/hc/en-us/articles/115010913367-EdgeRouter-DNS-Forwarding-Set » up-Options https://community.ubnt.com/t5/EdgeMAX/ERL-3-1-9-0-No-DHCP-leases-since-switching-t » o-DNSMasq/td- p/1644201 https://community.ubnt.com/t5/EdgeMAX/Traffic-Analysis-host-name-resolution/m-p/17 » 74017#M141121 https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/ https://community.ubnt.com/t5/EdgeRouter/DNS-Forwarding-Name-Servers/td-p/1117142		» Since it runs from your computer, the results are localized to your connection / ISP. Until the EdgeRouter » is fully setup, you might want to run this from a computer that is currently wired outside of the EdgeRouter. This » is shown as “Existing LAN” in Figure 2 - EdgeRouter Configuration Setup. The page is at: https://www.grc.com/dns/benchmark.htm Steve Gibson has another web page that tests the “spoofability” (security) of DNS » resolvers. It is at: https://www.grc.com/dns/dns.htm Here are some alternate DNS resolvers, and additional DNS information pages: https://en.wikipedia.org/wiki/List_of_managed_DNS_providers https://dns.norton.com/configureRouter.html, https://dns.norton.com/faq.html https://support.opendns.com/hc/en-us/articles/228006047-Generalized-Router-Configu » ration-Instructions https://use.opendns.com/#router https://en.wikipedia.org/wiki/OpenDNS https://www.quad9.net/ and https://www.quad9.net/faq https://www.globalcyberalliance.org/initiatives/quad9.html EdgeRouter DNS References: https://help.ubnt.com/hc/en-us/articles/115010913367-EdgeRouter-DNS-Forwarding-Set » up-Options https://community.ubnt.com/t5/EdgeMAX/ERL-3-1-9-0-No-DHCP-leases-since-switching-t » o-DNSMasq/td- p/1644201 https://community.ubnt.com/t5/EdgeMAX/Traffic-Analysis-host-name-resolution/m-p/17 » 74017#M141121 https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/ https://community.ubnt.com/t5/EdgeRouter/DNS-Forwarding-Name-Servers/td-p/1117142
	-+	https://community.ubnt.com/t5/EdgeRouter/Setting-up-Local-DNS/td-p/449259 https://community.ubnt.com/t5/EdgeRouter/DNS-forwarding-listen-on-vs-dns-server-on » -DHCP-server/m- p/2613931
	=	
For more information on Quad9, see Security Now Podcast #638 at » https://www.grc.com/securitynow.htm	<>	For more information on Quad9, see: Security Now Podcast #638 at https://www.grc.com/securitynow.htm Reference: https://github.com/mjp66/Ubiquiti/issues/13 and » https://www.quad9.net/faq

	=	
Page 30 of 136 » 2/4/2019	<>	Page 32 of 157 » 5/18/2019
Dns Crash Note: I’ve experienced some infrequent router crashes. These crashes seem to involve dns » and last about five minutes. During this time your router is ineffective. I’ve posted about this issue on the » Ubiquiti forums and have not found a solution. Reference » https://community.ubnt.com/t5/EdgeRouter/ER-X-Dns-Forwarding-Not-Acting-Configur » ed- Correctly/td-p/2301019 You may not experience these crashes, or if you do, you may choose to just live » with these symptoms. One workaround seems to be not using the ER-X’s dnsmasq service as your Home Network » resolver. If you don’t use dnsmasq, you will lose the benefits of local caching and of being able to access » Network devices by their local name. The workaround involves changing “DNS 1” and “DNS 2” to alternate (external) » dns resolver IP addresses for LAN2 (the Home Network.) If you want to work around this issue, you should » probably perform these changes	=	Dns Crash Note: I’ve experienced some infrequent router crashes. These crashes seem to involve dns » and last about five minutes. During this time your router is ineffective. I’ve posted about this issue on the » Ubiquiti forums and have not found a solution. Reference » https://community.ubnt.com/t5/EdgeRouter/ER-X-Dns-Forwarding-Not-Acting-Configur » ed- Correctly/td-p/2301019 You may not experience these crashes, or if you do, you may choose to just live » with these symptoms. One workaround seems to be not using the ER-X’s dnsmasq service as your Home Network » resolver. If you don’t use dnsmasq, you will lose the benefits of local caching and of being able to access » Network devices by their local name. The workaround involves changing “DNS 1” and “DNS 2” to alternate (external) » dns resolver IP addresses for LAN2 (the Home Network.) If you want to work around this issue, you should » probably perform these changes
when performing the actions in section 29 - Set Domain Names for Networks, » remembering to additionally change	<>	when performing the actions in section 30 - Set Domain Names for Networks, » remembering to additionally change
LAN2.	=	LAN2.
[Update: I have not seen these in quite some time; I think newer ER-X firmware may » have fixed these.]	<>	[Update: I have not seen these in quite some time; I am using dnsmasq, and think » newer ER-X firmware may have fixed these.]
	=	
Page 31 of 136 2/4/ » 2019 21. dnsmasq	<>	Page 33 of 157 5/18/ » 2019 22. dnsmasq
There are two different DNS packages available within the EdgeRouter. They are ISC » (default) and dnsmasq. Dnsmasq was incomplete as of firmware 1.9.0 and had an additional bug added in » firmware 1.9.1, I think it was re-	=	There are two different DNS packages available within the EdgeRouter. They are ISC » (default) and dnsmasq. Dnsmasq was incomplete as of firmware 1.9.0 and had an additional bug added in » firmware 1.9.1, I think it was re-
broken and fixed during the hoxfixes of 1.9.7. Enabling dnsmasq is optional. To enable dnsmasq, enter the Config Tree. Reference section “15 - EdgeRouter » Config Tree.” Select and open up	<>	broken and fixed during the hoxfixes of 1.9.7. I now suggest that you use dnsmasq. To enable dnsmasq, enter the Config Tree. Reference section “16 - EdgeRouter » Config Tree.” Select and open up
the following config tree sub-menu items from the configuration screen:	=	the following config tree sub-menu items from the configuration screen:

service dhcp-server You should see some DHCP settings, including use-dnsmasq and hostfile-update. » (Note, your screen will still show “disable”). See Figure 45 – use-dnsmasq.		service dhcp-server You should see some DHCP settings, including use-dnsmasq and hostfile-update. » (Note, your screen will still show “disable”). See Figure 45 – use-dnsmasq.
	-+	Configure
Figure 45 – use-dnsmasq Type “enable” in the use-dnsmasq box and in the hostfile-update box. Then press » the “Preview” button. See Figure 46 – commit-dnsmasq.	=	Figure 45 – use-dnsmasq Type “enable” in the use-dnsmasq box and in the hostfile-update box. Then press » the “Preview” button. See Figure 46 – commit-dnsmasq.
Figure 46 – commit-dnsmasq Press “Apply.” You should see the message “The configuration has been applied » successfully”, in green, near the bottom of the screen.		Figure 46 – commit-dnsmasq Press “Apply.” You should see the message “The configuration has been applied » successfully”, in green, near the bottom of the screen.
Page 32 of 136 » 2/4/2019	<>	Page 34 of 157 » 5/18/2019
With local hostname resolution, you can lookup different devices / PCs on your » Network by just referencing the name of the device / PC. For instance, you can look up a second PC on your Home » Network from another PC on your Home Network by referencing its name, i.e. by typing (example) "ping » DifferentPcName" or by entering	=	With local hostname resolution, you can lookup different devices / PCs on your » Network by just referencing the name of the device / PC. For instance, you can look up a second PC on your Home » Network from another PC on your Home Network by referencing its name, i.e. by typing (example) "ping » DifferentPcName" or by entering
"http://DifferentPcName" (if it is a web server), etc....	<>	"http://DifferentPcName" (if it is a web server), etc.... You may need to add » “.local” to the end of the name.
	=	
To allow local hostname resolution, perform the following changes. Drop into the » Command Line Interface (CLI)	<>	To allow local hostname resolution, perform the following changes. Drop into the » Command Line Interface (CLI)
and issue the following commands: configure set system name-server 127.0.0.1	=	and issue the following commands: configure set system name-server 127.0.0.1
set service dns forwarding listen-on switch0	<>	set service dns forwarding listen-on switch0
set system domain-name home.local commit save exit	=	set system domain-name home.local commit save exit
You should see a yellow “The configuration has been changed and is in the process » of being committed” message. See Figure 47 – The Configuration has been changed message		You should see a yellow “The configuration has been changed and is in the process » of being committed” message. See Figure 47 – The Configuration has been changed message
Figure 47 – The Configuration has been changed message		Figure 47 – The Configuration has been changed message

References: https://help.ubnt.com/hc/en-us/articles/115002673188-EdgeRouter-Using-dnsmasq-for- » DHCP-Server		References: https://help.ubnt.com/hc/en-us/articles/115002673188-EdgeRouter-Using-dnsmasq-for- » DHCP-Server
https://help.ubnt.com/hc/en-us/articles/115010913367-EdgeRouter-DNS-Forwarding-Exp » lanation-Setup-Options	<>	https://community.ubnt.com/t5/EdgeRouter/vlan-can-not-connect-to-management-plane- » or-internet/m- p/2724332/highlight/true#M245769 https://community.ubnt.com/t5/EdgeRouter/Help-with-dnsmasq-on-ER-X/m-p/2477434
Additional:	=	Additional:
	-+	
https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/	=	https://loganmarchione.com/2016/08/edgerouter-lite-dnsmasq-setup/
Page 33 of 136 » 2/4/2019 22. System DNS 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 set up » via this guide use different DNS servers, as overridden by their specific DHCP servers.	<>	Page 35 of 157 » 5/18/2019 23. System DNS Settings This step instructs the EdgeRouter ITSELF to use specific DNS servers to resolve » web URLs into IP addresses. These DNS servers are specified under the System widow.
Press the “System” button. Reference Figure 9 – System Button. On the system window, find the Name Server Box. See Figure 48 – Initial System » Name Server.	=	Press the “System” button. Reference Figure 9 – System Button. On the system window, find the Name Server Box. See Figure 48 – Initial System » Name Server.
Figure 48 – Initial System Name Server	<>	Figure 48 – Initial System Name Server
	=	
Fill in the System name server field with your primary DNS server address. I » recently switched over to using a Quad9 resolver which has a primary address of: 9.9.9.9 Most DNS systems have multiple resolver addresses, in case of failure. The Quad9 » infrastructure recently added a secondary resolver address, so press the “+ Add New” button and enter your » secondary DNS server address. Quad9’s secondary address is 149.112.112.112 Reference: https://github.com/mjp66/Ubiquiti/issues/13 and » https://www.quad9.net/faq See Figure 49 – Example System DNS Entries.	<>	Your box should already be filled-in with 127.0.0.1, as this was set by CLI in the » previous section. You can leave it, or change it (as I did) to two DNS resolver addresses of your choice. I used » Google addresses for this guide. Most external DNS resolver systems have multiple resolver addresses, in case of failure » ; ensure that you add both the primary and secondary resolver addresses by (erasing what is already there and/or) » pressing the “+ Add New” button. See Figure 49 – Example Google DNS System DNS Entries.
	=	
Figure 49 – Example System DNS Entries	<>	Figure 49 – Example Google DNS System DNS Entries

Press the Save button near the bottom of the system page. See Figure 50 – System » Save Button.	<>	When you are done editing, press the Save button near the bottom of the system » page. See Figure 50 – System Save Button.
Figure 50 – System Save Button	=	Figure 50 – System Save Button
Page 34 of 136 » 2/4/2019 23. Remove ISP Provided DNS Resolvers	<>	Page 36 of 157 » 5/18/2019 24. Remove ISP Provided DNS Resolvers
I don’t want to depend upon the DNS servers that are provided by my dsl / cable » modem. The specific DNS	=	I don’t want to depend upon the DNS servers that are provided by my dsl / cable » modem. The specific DNS
resolver addresses are specified as part the DHCP data, which is given to the » EdgeRouter’s eth0 WAN port from	<>	resolver addresses are specified as part of the DHCP data, which is given to the » EdgeRouter’s eth0 WAN port from
the dsl / cable modem. Performing the commands in this section is optional / up to » you.	=	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		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		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,		backdoors in them. Commercial modems bulk produced by the lowest bidder and » externally controlled by large,
uncaring companies have got to be even worse.		uncaring companies have got to be even worse.
In particular, there are DNS changer worms, which attack consumer / commercial » routers and change their DNS		In particular, there are DNS changer worms, which attack consumer / commercial » routers and change their DNS
resolver settings. The way to help circumvent this problem is to instruct the » EdgeRouter to ignore the DHCP		resolver settings. The way to help circumvent this problem is to instruct the » EdgeRouter to ignore the DHCP
provided DNS resolver address from your commercial router / ISP.		provided DNS resolver address from your commercial router / ISP.
Since the DNS changer worm could attack an EdgeRouter, remember to change the » EdgeRouter’s default		Since the DNS changer worm could attack an EdgeRouter, remember to change the » EdgeRouter’s default
password to something strong. You don’t want to end up like these people:		password to something strong. You don’t want to end up like these people:
https://www.routersecurity.org/bugs.php,		https://www.routersecurity.org/bugs.php,
-> January 2018, -> MikroTik and Ubiquiti Routers defaced due to default » passwords		-> January 2018, -> MikroTik and Ubiquiti Routers defaced due to default » passwords
To see the DNS resolvers being used by the EdgeRouter, issue the CLI command:		To see the DNS resolvers being used by the EdgeRouter, issue the CLI command:
	<>	
show dns forwarding nameservers.		show dns forwarding nameservers.
(For information on the CLI, reference section “14 - EdgeRouter Command Line » Interface (CLI)”)		(For information on the CLI, reference section “15 - EdgeRouter Command Line » Interface (CLI)”)
	=	
The following text shows theQuad9 resolver that was entered into the system page,	<>	The following text shows the Google resolver addresses that were entered into the

» and an ISP-provided resolver, delivered via my existing / upstream router, which has an address of 192.168.2.1:		» system page, and an ISP- provided resolver, delivered via my existing / upstream router, which has an » address of 192.168.2.1:
	=	
----------		----------
Nameservers configured for DNS forwarding	<>	Nameservers configured for DNS forwarding
----------	=	----------
	-+	8.8.8.8 available via 'system' 8.8.4.4 available via 'system'
192.168.2.1 available via 'dhcp eth0'	=	192.168.2.1 available via 'dhcp eth0'
9.9.9.9 available via 'system' 149.112.112.112 available via 'system'	+-	
	=	
To remove the ISP-provided nameservers, drop into the Command Line Interface (CLI) » and issue the following	<>	To remove the ISP-provided nameserver, drop into the Command Line Interface (CLI) » and issue the following
commands: configure set service dns forwarding system commit save exit	=	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:	<>	Page 37 of 157 » 5/18/2019 To see if this worked, re-issue the CLI command “show dns forwarding » nameservers”. This is what I got:
	=	
----------		----------
Nameservers configured for DNS forwarding	<>	Nameservers configured for DNS forwarding
----------	=	----------
9.9.9.9 available via 'optionally configured'	<>	8.8.8.8 available via 'optionally configured' 8.8.4.4 available via 'optionally configured'
149.112.112.112 available via 'system'		
----------	=	----------
Nameservers NOT configured for DNS forwarding	<>	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		192.168.2.1 available via 'dhcp eth0' Reference https://community.ubnt.com/t5/EdgeMAX/Change-WAN-DNS-Server/td-p/977885
Page 35 of 136 » 2/4/2019	+-	

According to https://github.com/mjp66/Ubiquiti/issues/11, you would restore using » your ISP's resolvers with the following commands:	=	According to https://github.com/mjp66/Ubiquiti/issues/11, you would restore using » your ISP's resolvers with the following commands:
configure	=	configure
delete service dns forwarding system	<>	delete service dns forwarding system
set service dns forwarding listen-on eth0	<>	set service dns forwarding listen-on eth0
commit	=	commit
save	=	save
exit	=	exit
Page 36 of 136 » 2/4/2019	<>	Page 38 of 157 » 5/18/2019
24. Configure EdgeRouter's eth2 DHCP Server	<>	25. 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 » 51 – Services Button.	=	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 » 51 – Services Button.
Figure 51 – Services Button	<>	Figure 51 – Services Button
	=	
Ensure that the "DHCP Server" tab is selected. See Figure 52 – DHCP Server Screen.	=	Ensure that the "DHCP Server" tab is selected. See Figure 52 – DHCP Server Screen.
Figure 52 – DHCP Server Screen	<>	Figure 52 – 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.	<>	Note that I am using Google DNS resolver addresses for DNS1 and DNS2 (below). You » can change these to providers of your choice.
	=	
Click on the "+ Add DHCP Server" button. You will be presented with a Create » DHCP Server dialog. See Figure 53 –	<>	Click on the "+ Add DHCP Server" button. You will be presented with a Create DHCP » Server dialog. See Figure 53 –
Create eth2 DHCP Server Screen. Fill in the form as follows:	=	Create eth2 DHCP Server Screen. Fill in the form as follows:
DHCP Name: SecureNetDHCP	<>	DHCP Name: SecureNetDHCP
Subnet: 192.168.5.0/24	<>	Subnet: 192.168.5.0/24
Range Start: 192.168.5.38	<>	Range Start: 192.168.5.38
Range Stop: 192.168.5.243	<>	Range Stop: 192.168.5.243
Router: 192.168.5.1	<>	Router: 192.168.5.1
DNS 1: 209.244.0.3	<>	DNS 1: 8.8.8.8
DNS 2: 209.244.0.4	<>	DNS 2: 8.8.4.4
	<>	Unifi Controller: <Leave Blank>
Enable: CHECKED	<>	Enable: CHECKED
	=	

Click “Save.”		Click “Save.”
Page 37 of 136 » 2/4/2019	<>	Page 39 of 157 » 5/18/2019
Figure 53 – Create eth2 DHCP Server Screen	=	Figure 53 – Create eth2 DHCP Server Screen
I used the same range start and range stop values (38 and 243) that the wan+2lan2 » wizard used within the DHCP servers for LAN1 and LAN2. For some reason, the 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.		I used the same range start and range stop values (38 and 243) that the wan+2lan2 » wizard used within the DHCP servers for LAN1 and LAN2. For some reason, the 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.
25. Configure EdgeRouter’s Time Zone	<>	26. Configure EdgeRouter’s Time Zone
Near the bottom of the screen select the “System” button. Reference Figure 9 – » System Button. Find the section titled “Time Zone” and configure the data in these fields according to the time » zone you are in, unless you want your router to remain in UTC. See Figure 54 – Time Zone.	=	Near the bottom of the screen select the “System” button. Reference Figure 9 – » System Button. Find the section titled “Time Zone” and configure the data in these fields according to the time » zone you are in, unless you want your router to remain in UTC. See Figure 54 – Time Zone.
Figure 54 – Time Zone		Figure 54 – Time Zone
Press the Save button, Reference Figure 50 – System Save Button.		Press the Save button, Reference Figure 50 – System Save Button.
Page 38 of 136 » 2/4/2019 26. DNS Forwarding	<>	Page 40 of 157 » 5/18/2019 27. DNS Forwarding
Press the “Services” button, near the top right of the window. Reference Figure 51 » – Services Button. Ensure that the “DNS” Tab is selected. See Figure 55 – DNS Tab.	=	Press the “Services” button, near the top right of the window. Reference Figure 51 » – Services Button. Ensure that the “DNS” Tab is selected. See Figure 55 – DNS Tab.
Figure 55 – DNS Tab		Figure 55 – DNS Tab
I changed my cache size to 400. We want to remove eth1 from this list. Change the » first item (which can’t be removed) to “switch0”. Then press the “- Remove” button to the right of the second » item. The result should look like Figure 56 – Remove eth1 from DNS. Press “Save.”		I changed my cache size to 400. We want to remove eth1 from this list. Change the » first item (which can’t be removed) to “switch0”. Then press the “- Remove” button to the right of the second » item. The result should look like Figure 56 – Remove eth1 from DNS. Press “Save.”
Figure 56 – Remove eth1 from DNS Forwarding		Figure 56 – Remove eth1 from DNS Forwarding
Page 39 of 136 » 2/4/2019 27. Add VLAN Networks to the EdgeRouter	<>	Page 41 of 157 » 5/18/2019 28. 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	=	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.	<>	section will create three new Networks using VLANs.
Press the Dashboard button near the top of the Screen. Reference Figure 34 –	=	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 57 – » Add Interface Button Figure 57 – Add Interface Button The Add Interface menu will appear. Select “Add VLAN”. See Figure 58 – Add » Interface Menu Figure 58 – 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 59 – Create New VLAN Example. Press the “Save” button. Figure 59 – Create New VLAN Example		» Dashboard Button. On the upper left side of the Dashboard screen select the Add Interface button. See Figure 57 – » Add Interface Button Figure 57 – Add Interface Button The Add Interface menu will appear. Select “Add VLAN”. See Figure 58 – Add » Interface Menu Figure 58 – 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 59 – Create New VLAN Example. Press the “Save” button. Figure 59 – Create New VLAN Example
Page 40 of 136 » 2/4/2019 Repeat these steps for adding a VLAN the Wi-Fi IOT Network. Fill in the » information as follows:	<>	Page 42 of 157 » 5/18/2019 Repeat the above steps two more times, for adding two more VLANs. Fill in the » information as follows:
VLAN ID: 7 Interface: switch0 Description: “Wifi Iot Net” MTU: 1500 Address: Manually define IP address 192.168.7.1/24	=	VLAN ID: 7 Interface: switch0 Description: “Wifi Iot Net” MTU: 1500 Address: Manually define IP address 192.168.7.1/24
	-+	VLAN ID: 8 Interface: switch0 Description: “Wifi Spare Net” MTU: 1500 Address: Manually define IP address 192.168.8.1/24
There are the relevant sections from the backup file: vif 6 {	=	There are the relevant sections from the backup file: vif 6 {
address 192.168.6.1/24	<>	address 192.168.6.1/24

description "Wifi Guest Net"		description "Wifi Guest Net"
mtu 1500	=	mtu 1500
}		}
vif 7 {		vif 7 {
address 192.168.7.1/24	<>	address 192.168.7.1/24
description "Wifi Iot Net"		description "Wifi Iot Net"
mtu 1500	=	mtu 1500
}		}
	-+	vif 8 {
		address 192.168.8.1/24
		description "Wifi Spare Net"
		mtu 1500
		}
	=	
	-+	Page 43 of 157
		» 5/18/2019
Here is a link discussing using VLANs and managed switches to reduce the number of	=	Here is a link discussing using VLANs and managed switches to reduce the number of
» network cables in a home:		» network cables in a home:
https://community.ubnt.com/t5/EdgeMAX/Need-recommendation-on-tweaking-config-to-su		https://community.ubnt.com/t5/EdgeMAX/Need-recommendation-on-tweaking-config-to-su
» pport-some-		» pport-some-
VLAN/td-p/2155404		VLAN/td-p/2155404
When originally writing this guide, I was not able to figure out how to combine		When originally writing this guide, I was not able to figure out how to combine
» the Wired IOT Network (as		» the Wired IOT Network (as
192.168.4.X) and the Wi-Fi IOT Network (as 192.168.7.X) as a single Network /		192.168.4.X) and the Wi-Fi IOT Network (as 192.168.7.X) as a single Network /
» Subnet.		» Subnet.
I have now tried a method to coalesce the Wired IOT Network and the WiFi IOT	<>	I now use a method to coalesce the Wired IOT Network and the WiFi IOT Network.
» Network. Reference section 78 -		» Reference section 79 -
Coalescing the Wired Iot and Wifi Iot Networks. If you are going to perform those	=	Coalescing the Wired Iot and Wifi Iot Networks. If you are going to perform those
» optional steps, I'd wait until you		» optional steps, I'd wait until you
reach that section, and not perform those steps now.		reach that section, and not perform those steps now.
VLAN References:		VLAN References:
	-+	https://help.ubnt.com/hc/en-us/articles/222183968-Intro-to-Networking-Introduction
		» -to-Virtual-LANs-VLANs-
		and-Tagging
https://community.ubnt.com/t5/EdgeMAX-Stories/Do-people-use-VLANs-for-the-right-th	=	https://community.ubnt.com/t5/EdgeMAX-Stories/Do-people-use-VLANs-for-the-right-th
» ings-Pt-1/cns-p/1443246		» ings-Pt-1/cns-p/1443246
	-+	
https://community.ubnt.com/t5/EdgeMAX-Stories/Do-people-use-VLANs-for-the-right-th	=	https://community.ubnt.com/t5/EdgeMAX-Stories/Do-people-use-VLANs-for-the-right-th
» ings-Pt-2/cns-p/1443259		» ings-Pt-2/cns-p/1443259
https://community.ubnt.com/t5/EdgeMAX/Adding-a-new-subnet-to-an-Edge-Router-X/td-p		https://community.ubnt.com/t5/EdgeMAX/Adding-a-new-subnet-to-an-Edge-Router-X/td-p

» /2197809		» /2197809
https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch0		https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch0
» -with-Inter-VLAN-		» -with-Inter-VLAN-
Firewall-Limiting		Firewall-Limiting
https://help.ubnt.com/hc/en-us/articles/205197630-EdgeSwitch-VLANs-and-Tagged-Unta		https://help.ubnt.com/hc/en-us/articles/205197630-EdgeSwitch-VLANs-and-Tagged-Unta
» gged-Ports		» gged-Ports
https://help.ubnt.com/hc/en-us/articles/222183968-Intro-to-Networking-Introduction		https://help.ubnt.com/hc/en-us/articles/222183968-Intro-to-Networking-Introduction
» -to-Virtual-LANs-VLANs-		» -to-Virtual-LANs-VLANs-
and-Tagging		and-Tagging
Page 41 of 136	<>	Page 44 of 157
» 2/4/2019		» 5/18/2019
28. Add DHCP Servers to the VLANs		29. Add DHCP Servers to the VLANs
Following the directions that are in the section titled “24 - Configure		Following the directions that are in the section titled “25 - Configure
» EdgeRouter’s eth2 DHCP Server”, add DHCP		» 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 the three VLANs that were just created. Note that I am using Open DNS
» servers for these networks. If		» servers for these networks. If
you change them here, you will also need to manually modify some firewall / NAT	=	you change them here, you will also need to manually modify some firewall / NAT
» rules, presented later within		» rules, presented later within
this guide.		this guide.
The information for VLAN 6, is as follows:		The information for VLAN 6, is as follows:
DHCP Name: WifiGuestDHCP	<>	DHCP Name: WifiGuestDHCP
Subnet: 192.168.6.0/24		Subnet: 192.168.6.0/24
Range Start: 192.168.6.38		Range Start: 192.168.6.38
Range Stop: 192.168.6.243		Range Stop: 192.168.6.243
Router: 192.168.6.1		Router: 192.168.6.1
DNS 1: 208.67.222.222		DNS 1: 208.67.222.222
DNS 2: 208.67.220.220		DNS 2: 208.67.220.220
		Unifi Controller: <Leave Blank>
Enable: CHECKED		Enable: CHECKED
The information for VLAN 7, is as follows:	=	The information for VLAN 7, is as follows:
DHCP Name: WifiIotDHCP	<>	DHCP Name: WifiIotDHCP
Subnet: 192.168.7.0/24		Subnet: 192.168.7.0/24
Range Start: 192.168.7.38		Range Start: 192.168.7.38
Range Stop: 192.168.7.243		Range Stop: 192.168.7.243
Router: 192.168.7.1		Router: 192.168.7.1
DNS 1: 208.67.222.222		DNS 1: 208.67.222.222
DNS 2: 208.67.220.220		DNS 2: 208.67.220.220
		Unifi Controller: <Leave Blank>
Enable: CHECKED		Enable: CHECKED
		The information for VLAN 8, is as follows:

		DHCP Name: WifiSpareDHCP Subnet: 192.168.8.0/24 Range Start: 192.168.8.38 Range Stop: 192.168.8.243 Router: 192.168.8.1 DNS 1: 208.67.222.222 DNS 2: 208.67.220.220 Unifi Controller: <Leave Blank> Enable: CHECKED
You should now have five DHCP servers.		You should now have six DHCP servers.
	=	
Page 42 of 136 » 2/4/2019 29. Set Domain Names for Networks	<>	Page 45 of 157 » 5/18/2019 30. Set Domain Names for Networks
Near the top of the screen select the “Services” button. Reference Figure 51 – Services Button. Ensure that the “DHCP Server” tab is selected. Reference Figure 52 – DHCP Server Screen Find the LAN1 line, and follow it to the right side, to the line’s “Actions” button. Click the “Actions” button. You will be presented with a list of actions. Choose “View Details”. See Figure 60 – DHCP Actions. Figure 60 – DHCP Actions A dialog will open. See Figure 61 – DHCP Server Details Dialog. Figure 61 – DHCP Server Details Dialog Fill-in the “Domain” field with: WiredIotNet and then click “Save.” When it is done updating, close the dialog.	=	Near the top of the screen select the “Services” button. Reference Figure 51 – Services Button. Ensure that the “DHCP Server” tab is selected. Reference Figure 52 – DHCP Server Screen Find the LAN1 line, and follow it to the right side, to the line’s “Actions” button. Click the “Actions” button. You will be presented with a list of actions. Choose “View Details”. See Figure 60 – DHCP Actions. Figure 60 – DHCP Actions A dialog will open. See Figure 61 – DHCP Server Details Dialog. Figure 61 – DHCP Server Details Dialog Fill-in the “Domain” field with: WiredIotNet and then click “Save.” When it is done updating, close the dialog.
Page 43 of 136 » 2/4/2019	<>	Page 46 of 157 » 5/18/2019
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):	=	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		DHCP Servers / Domain LAN1 / WiredIotNet LAN2 / HomeNet SecureNetDHCP / SeparateNet WiFiGuestDHCP / WifiGuestNet WifiIOTDHCP / WifiIotNet
	-+	WifiSpareDHCP / WifiSpareNet
Table 2 - Table of Domain Names	=	Table 2 - Table of Domain Names

30. Modify EdgeRouter's eth1 DHCP Server	<>	31. Modify EdgeRouter's eth1 DHCP Server
Select the "Services" button. Reference Figure 51 – Services Button. Ensure that the "DHCP Server" tab is selected. Reference Figure 52 – DHCP Server » Screen Select the "Action" button to the right of the "LAN1" line. Reference Figure 60 – » DHCP Actions. Choose "View Details." Reference Figure 61 – DHCP Server Details Dialog. Modify / enter the following information: DNS 1: 208.67.222.222 DNS 2: 208.67.220.220 These DNS addresses have the equipment on the Wired Iot Network use Open DNS » resolvers. If different resolver addresses are used here, then some firewall rules (and probably group addresses) » will also need to be modified. Covered later in this guide.	=	Select the "Services" button. Reference Figure 51 – Services Button. Ensure that the "DHCP Server" tab is selected. Reference Figure 52 – DHCP Server » Screen Select the "Action" button to the right of the "LAN1" line. Reference Figure 60 – » DHCP Actions. Choose "View Details." Reference Figure 61 – DHCP Server Details Dialog. Modify / enter the following information: DNS 1: 208.67.222.222 DNS 2: 208.67.220.220 These DNS addresses have the equipment on the Wired Iot Network use Open DNS » resolvers. If different resolver addresses are used here, then some firewall rules (and probably group addresses) » will also need to be modified. Covered later in this guide.
Page 44 of 136 » 2/4/2019	<>	Page 47 of 157 » 5/18/2019 32. Rename DHCP Servers When the Wizard setup our EdgeRouter, it named the two original networks as LAN1 » and LAN2. To rename them, enter the CLI. Reference section 15 - EdgeRouter Command Line Interface (CLI).Type » the following commands into the CLI window: configure edit service dhcp-server rename shared-network-name LAN1 to shared-network-name » WiredIotDHCP rename shared-network-name LAN2 to shared-network-name » HomeNetDHCP commit save exit Exit the CLI interface. Page 48 of 157 » 5/18/2019
31. Make DHCP Servers "authoritative"		33. Make DHCP Servers "authoritative"
The EdgeRouter does not default any newly created DHCP servers to "authoritative." » This means that devices on the added Networks can take a long time to acquire an IP address. The Networks » that were added by the Wizard	=	The EdgeRouter does not default any newly created DHCP servers to "authoritative." » This means that devices on the added Networks can take a long time to acquire an IP address. The Networks » that were added by the Wizard

(LAN1 and LAN2) are made authoritative by default.		(LAN1 and LAN2) are made authoritative by default.
Enter the Config Tree. Reference section “15 - EdgeRouter Config Tree.” Select and » open up the following config	<>	Enter the Config Tree. Reference section “16 - EdgeRouter Config Tree.” Select and » open up the following config
tree sub-menu items from the configuration screen: service dhcp-server shared-network-name	=	tree sub-menu items from the configuration screen: service dhcp-server shared-network-name
	-+	
Click on the DHCP server you want to configure; in this case, it is: SecureNetDHCP You should see some DHCP settings, including authoritative. (Note, your screen » will still show “disable”). See Figure 62 – Authoritative Example. Figure 62 – Authoritative Example	=	Click on the DHCP server you want to configure; in this case, it is: SecureNetDHCP You should see some DHCP settings, including authoritative. (Note, your screen » will still show “disable”). See Figure 62 – Authoritative Example. Figure 62 – Authoritative Example
	-+	Page 49 of 157 » 5/18/2019
Type “enable” in the authoritative box. Then press the “Preview” button. See » Figure 63 – Authoritative Commit.	=	Type “enable” in the authoritative box. Then press the “Preview” button. See » Figure 63 – Authoritative Commit.
Figure 63 – Authoritative Commit	<>	Figure 63 – Authoritative Commit
	=	
Page 45 of 136 » 2/4/2019	+-	
Press “Apply.” You should see the message “The configuration has been applied » successfully”, in green, near the bottom of the screen. Repeat these steps for the following Authoritative DHCP Servers as shown in Table » 3 - Table of Authoritative DHCP Servers. (You have just done the first one of them):	=	Press “Apply.” You should see the message “The configuration has been applied » successfully”, in green, near the bottom of the screen. Repeat these steps for the following Authoritative DHCP Servers as shown in Table » 3 - Table of Authoritative DHCP Servers. (You have just done the first one of them):
Authoritative DHCP Servers	<>	Authoritative DHCP Servers
	=	
SecureNetDHCP	<>	SecureNetDHCP
	=	
WiFiGuestDHCP	<>	WiFiGuestDHCP
	=	
WifiIotDHCP	<>	WifiIotDHCP
	=	
	<>	WifiSpareDHCP
Table 3 - Table of Authoritative DHCP Servers		Table 3 - Table of Authoritative DHCP Servers
Shown below are excerpts of three of the five DHCP sections from the backup file:	=	Shown below are excerpts of three of the five DHCP sections from the backup file:

```
                                                                  <>
                                                                     Page 50 of 157
                                                                  » 5/18/2019
        dhcp-server    {                                             dhcp-server    {
             disabled    false                                           disabled    false
             hostfile-update    disable                               hostfile-update    disable
             shared-network-name     LAN2  {                        shared-network-name     HomeNetDHCP    {
                  authoritative    enable                                authoritative    enable
                  subnet  192.168.3.0/24     {                          subnet  192.168.3.0/24    {
                       default-router    192.168.3.1                         default-router    192.168.3.1
                       dns-server   192.168.3.1                           dns-server   192.168.3.1
                       domain-name   HomeNet                              domain-name   HomeNet
                       lease  86400                                       lease  86400
                       start  192.168.3.38    {                          start  192.168.3.38    {
                            stop  192.168.3.243                                 stop  192.168.3.243
                       }                                                   }
                  }                                                     }
             }                                                       }
             shared-network-name     SecureNetDHCP     {           shared-network-name     SecureNetDHCP    {
                  authoritative    enable                                authoritative    enable
                  subnet  192.168.5.0/24     {                          subnet  192.168.5.0/24    {
                       default-router    192.168.5.1                         default-router    192.168.5.1
                       dns-server   209.244.0.3                           dns-server   209.244.0.3
                       dns-server   209.244.0.4                           dns-server   209.244.0.4
                       domain-name   SeparateNet                          domain-name   SeparateNet
                       lease  86400                                       lease  86400
                       start  192.168.5.38    {                          start  192.168.5.38    {
                            stop  192.168.5.243                                 stop  192.168.5.243
                       }                                                   }
                  }                                                     }
             }                                                       }
             shared-network-name     WifiGuestDHCP     {           shared-network-name     WifiGuestDHCP    {
                  authoritative    enable                                authoritative    enable
                  subnet  192.168.6.0/24     {                          subnet  192.168.6.0/24    {
                       default-router    192.168.6.1                         default-router    192.168.6.1
                       dns-server   208.67.222.222                        dns-server   208.67.222.222
                       dns-server   208.67.220.220                        dns-server   208.67.220.220
                       domain-name   WifiGuestNet                         domain-name   WifiGuestNet
                       lease  86400                                       lease  86400
                       start  192.168.6.38    {                          start  192.168.6.38    {
```

stop 192.168.6.243 } } } use-dnsmasq enable }		stop 192.168.6.243 } } } use-dnsmasq enable }
	=	
Page 46 of 136 » 2/4/2019 32. EdgeRouter Enable HW NAT Assist	<>	Page 51 of 157 » 5/18/2019 34. EdgeRouter Enable HW NAT Assist
Enabling “hwnat” turns on some features of a hardware switching chip that is » within the EdgeRouter. This chip assists the EdgeRouter’s CPU with routing and NAT functionality, speeding up the » operation of the EdgeRouter X. Without this hardware assist, routing of packets is relatively slow. Be warned; if » Quality of Service (QoS) functionality is enabled, then this hwnat assist is internally / automatically » disabled. You also don’t want to enable bridging, since bridging is implemented via the CPU of the EdgeRouter X and » is also relatively slow. With hwnat enabled, many people report 800 – 900Mbps throughput.	=	Enabling “hwnat” turns on some features of a hardware switching chip that is » within the EdgeRouter. This chip assists the EdgeRouter’s CPU with routing and NAT functionality, speeding up the » operation of the EdgeRouter X. Without this hardware assist, routing of packets is relatively slow. Be warned; if » Quality of Service (QoS) functionality is enabled, then this hwnat assist is internally / automatically » disabled. You also don’t want to enable bridging, since bridging is implemented via the CPU of the EdgeRouter X and » is also relatively slow. With hwnat enabled, many people report 800 – 900Mbps throughput.
Open up the Configuration Tree. Reference section 15 - EdgeRouter Config Tree.	<>	Open up the Configuration Tree. Reference section 16 - EdgeRouter Config Tree.
Select and open up the following config tree sub-menu items from the configuration » screen: system offload In the hwnat setting area, type: enable then select the “Preview” button at the bottom of the page. See Figure 64 – System Offload Hwnat Selection (Partial). Figure 64 – System Offload Hwnat Selection (Partial)	=	Select and open up the following config tree sub-menu items from the configuration » screen: system offload In the hwnat setting area, type: enable then select the “Preview” button at the bottom of the page. See Figure 64 – System Offload Hwnat Selection (Partial). Figure 64 – System Offload Hwnat Selection (Partial)
Page 47 of 136 » 2/4/2019	+-	
The Edgerouter will preview what command(s) it will issue. See Figure 65 – Preview » hwnat Config.	=	The Edgerouter will preview what command(s) it will issue. See Figure 65 – Preview » hwnat Config.
Figure 65 – Preview hwnat Config	<>	Figure 65 – Preview hwnat Config
Press “Apply.” The system will inform you that, “The configuration has been » applied successfully”. See Figure 66 – hwnat Success	=	Press “Apply.” The system will inform you that, “The configuration has been » applied successfully”. See Figure 66 – hwnat Success

Figure 66 – hwnat Success	<>	Figure 66 – hwnat Success
	=	
	-+	Page 52 of 157 » 5/18/2019
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 65 – Preview hwnat Config. Remember that different models of EdgeRouters have different abilities / hardware » assisting chips within them. Their commands may be different. Reference: » https://help.ubnt.com/hc/en-us/articles/115006567467-EdgeRouter-Hardware-Offload » ing-Explained	=	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 65 – Preview hwnat Config. Remember that different models of EdgeRouters have different abilities / hardware » assisting chips within them. Their commands may be different. Reference: » https://help.ubnt.com/hc/en-us/articles/115006567467-EdgeRouter-Hardware-Offload » ing-Explained
33. EdgeRouter ER-X Speed	<>	35. EdgeRouter ER-X Speed
The ER-X router seems capable of routing about 1Gbit/second aggregate/total. The following article is well worth reading: http://kazoo.ga/re-visit-the-switch-in-edgerouter-x/ Other performance references: https://community.ubnt.com/t5/EdgeMAX/Performance-of-EdgerouterX-vs-Edgerouter-Lit » e/td-p/1230924 https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-low-throughput-slow/td-p/139222 » 9 https://community.ubnt.com/t5/EdgeMAX/ER-X-vs-ER-Lite-Head-to-Head-Speed-Results-o » n-Google-Fiber/td- p/1839844 https://www.stevejenkins.com/blog/2017/02/edgerouter-x-vs-edgerouter-lite-google-f » iber-speed-tests/ https://community.ubnt.com/t5/EdgeMAX/Edgerouter-X-Fios-Gigabit-Won-t-go-over-500- » Mbps/td-p/1910761	=	The ER-X router seems capable of routing about 1Gbit/second aggregate/total. The following article is well worth reading: http://kazoo.ga/re-visit-the-switch-in-edgerouter-x/ Other performance references: https://community.ubnt.com/t5/EdgeMAX/Performance-of-EdgerouterX-vs-Edgerouter-Lit » e/td-p/1230924 https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-low-throughput-slow/td-p/139222 » 9 https://community.ubnt.com/t5/EdgeMAX/ER-X-vs-ER-Lite-Head-to-Head-Speed-Results-o » n-Google-Fiber/td- p/1839844 https://www.stevejenkins.com/blog/2017/02/edgerouter-x-vs-edgerouter-lite-google-f » iber-speed-tests/ https://community.ubnt.com/t5/EdgeMAX/Edgerouter-X-Fios-Gigabit-Won-t-go-over-500- » Mbps/td-p/1910761
Page 48 of 136 » 2/4/2019 34. EdgeRouter Enable Traffic Analysis	<>	Page 53 of 157 » 5/18/2019 36. EdgeRouter Enable Traffic Analysis
This step will enable the EdgeRouter to perform Deep Packet Inspection (DPI) /	=	This step will enable the EdgeRouter to perform Deep Packet Inspection (DPI) /

» Traffic Analysis. If you have any speed issues with your ER-X, then this may need to stay off. Press the “Traffic Analysis” button, near the top right of the screen. See Figure » 67 – Traffic Analysis Button.		» Traffic Analysis. If you have any speed issues with your ER-X, then this may need to stay off. Press the “Traffic Analysis” button, near the top right of the screen. See Figure » 67 – Traffic Analysis Button.
Figure 67 – Traffic Analysis Button		Figure 67 – Traffic Analysis Button
In the upper-right area of the traffic analysis screen, is an “Operational Status” » selection. Select “Enabled.” See Figure 68 – Enable Operational Status		In the upper-right area of the traffic analysis screen, is an “Operational Status” » selection. Select “Enabled.” See Figure 68 – Enable Operational Status
Figure 68 – Enable Operational Status		Figure 68 – Enable Operational Status
You will be presented with a confirmation dialog. See Figure 69 – Operational » Status Confirmation.		You will be presented with a confirmation dialog. See Figure 69 – Operational » Status Confirmation.
Figure 69 – Operational Status Confirmation		Figure 69 – 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 70 – Active Alert.		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 70 – Active Alert.
Figure 70 – Active Alert		Figure 70 – Active Alert
Click on the “Alerts” button. You will be presented with the Alert message(s). See » Figure 71 – Active Traffic Analysis Message.		Click on the “Alerts” button. You will be presented with the Alert message(s). See » Figure 71 – Active Traffic Analysis Message.
Figure 71 – Active Traffic Analysis Message		Figure 71 – Active Traffic Analysis Message
To remove this Alert message, press the “Remove” button, located on the right side » of the screen. See Figure 72 – Remove Alert Button		To remove this Alert message, press the “Remove” button, located on the right side » of the screen. See Figure 72 – Remove Alert Button
Figure 72 –Remove Alert Button		Figure 72 –Remove Alert Button
Page 49 of 136 » 2/4/2019 35. 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.	<>	Page 54 of 157 » 5/18/2019 37. EdgeRouter Traffic Analysis The Traffic Analysis performed by the EdgeRouter X initially looks pretty neat. » The following screen shot was taken when the Edgerouter was at this configuration step in generating this » configuration document. The EdgeRouter had been booted for 41 minutes.
The only thing I had done, since I booted the “setup” computer, was to configure » the EdgeRouter. I NEVER purposefully go to MSN.com, or to the Financial Times News. I only assume that » those web lookups are from Microsoft’s Internet Explorer / Microsoft performing their Windows 10 monetization » of their users, sometimes	=	The only thing I had done, since I booted the “setup” computer, was to configure » the EdgeRouter. I NEVER purposefully go to MSN.com, or to the Financial Times News. I only assume that » those web lookups are from Microsoft’s Internet Explorer / Microsoft performing their Windows 10 monetization » of their users, sometimes
referred to as “spying.” See Figure 73 –Sample Traffic Analysis. This feature » seems pretty neat at first. In real use	<>	referred to as “spying.” See Figure 73 –Sample Traffic Analysis

there seems to be a lot of uncharacterized traffic under “Other.”		In real use, this feature there seems to puta lot of uncharacterized traffic under “Other.”
	=	
Figure 73 –Sample Traffic Analysis	<>	Figure 73 –Sample Traffic Analysis
Note that when HW NAT Assist is enabled, some traffic, which is handled by the internal switch chip, is not shown in traffic analysis. That is because Traffic Analysis is a CPU function, and the traffic that is being handled internally by the switch chip is not visible to the CPU. 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).	=	Note that when HW NAT Assist is enabled, some traffic, which is handled by the internal switch chip, is not shown in traffic analysis. That is because Traffic Analysis is a CPU function, and the traffic that is being handled internally by the switch chip is not visible to the CPU. 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).
Page 50 of 136 » 2/4/2019 36. EdgeRouter X/X-SFP bootloader bug	<>	Page 55 of 157 » 5/18/2019 38. EdgeMAX EdgeRouter X/X-SFP bootloader update ER-X’s, which have firmware versions of 1.10.7 or above, have a newer bootloader » available and/or newer method of bootloader update. You will want to update your bootloader. Reference: https://help.ubnt.com/hc/en-us/articles/360009932554-EdgeRouter-How-to-Update-Boot » loader Per the above link, I ran the following CLI / SSH / PuTTY command: show system boot-image and got the following text: The system currently has the following boot image » installed: Current boot version: UNKNOWN Current boot md5sum : 7580ebd7ce9303243292f586ab7c6daf New uboot version is available: boot_e50_001_1e49c.tar.gz New boot md5sum : 2146fb2e3b2cd543efaa0a687e2ad0ce Run "add system boot-image" to upgrade boot image. I updated my bootloader with add system boot-image (and yes) andthen » got the following text: Uboot version [UNKNOWN] is about to be replaced Warning: Don't turn off the power or reboot during » the upgrade! Are you sure you want to replace old version? (Yes/No) » [Yes]: yes Preparing to upgrade...Done Copying upgrade boot image...Done Checking boot version: Current is UNKNOWN; new is

		» e50_001_1e49c ...Done Checking upgrade image...Done Writing image...Done Upgrade boot completed I then re-ran the following command: show system boot-image and got the » following text: The system currently has the following boot image » installed: Current boot version: e50_001_1e49c Current boot md5sum : 2146fb2e3b2cd543efaa0a687e2ad0ce Next, issue the reboot command and when prompted with the prompt: Proceed with reboot? [confirm] Type a single y character to confirm the reboot. You will need to wait about3 to 5 minutes. After the re-boot, I re-ran the following command: show system boot-image » and got the following text: The system currently has the following boot image » installed: Current boot version: e50_001_1e49c Current boot md5sum : 2146fb2e3b2cd543efaa0a687e2ad0ce Page 56 of 157 » 5/18/2019 39. EdgeRouter X/X-SFP Legacy Bootloader Information Part 1
There is an initialization issue in the bootloader for the ER-X and ER-X-SFP » models that causes all ports to act as a "switch" during a brief period of time when the router is booting up.		Older bootloaders have an initialization issue in the bootloader for the ER-X and » ER-X-SFP models that causes all ports to act as a "switch" during a brief period of time when the router is » booting up.
When this guide was written, Ubiquiti had still not updated their production line » to incorporate the patched bootloader. Reference » https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-acts-as-switch-during-boot/td » -p/1393679	=	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
37. EdgeRouter X/X-SFP check bootloader version Check the version of your bootloader per:	<>	Part 2 For pre 1.10.6 firmware, check the version of your bootloader per:
https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-X-SFP-check-bootloader-version/ » td-p/1617287 Some postings may be missing the “s” in “firmwares”.	=	https://community.ubnt.com/t5/EdgeMAX/EdgeRouter-X-X-SFP-check-bootloader-version/ » td-p/1617287 Some postings may be missing the “s” in “firmwares”.
38. EdgeMAX EdgeRouter X/X-SFP bootloader update	<>	

Note: Newer ER-X's supposedly have a newer bootloader and/or newer method of » bootloader update. My EdgeRouters are older, so I have not tried this: https://help.ubnt.com/hc/en-us/articles/360009932554-EdgeRouter-How-to-Update-Boot » loader Older bootloader updating text follows:		Part 3 Older bootloader (pre 1.10.6) updating is follows:
If your bootloader is not the newest, update your bootloader per: http://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-X-X-SFP-bootl » oader-update/ba-p/1472216 https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/DEPRECATED-EdgeMAX-EdgeRouter-X » -X-SFP-bootloader-update/ba-p/1472216 It is much easier to update the EdgeRouter's bootloader when the EdgeRouter is » connected to the internet. You may need to prepend "sudo" to one for more of the following commands, to get » this to work: https://community.ubnt.com/t5/EdgeMAX/ERX-bootloader-update/td-p/1892923 https://community.ubnt.com/t5/EdgeRouter/ER-X-bootloader-update-versions/td-p/2134 » 544	=	If your bootloader is not the newest, update your bootloader per: http://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-X-X-SFP-bootl » oader-update/ba-p/1472216 https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/DEPRECATED-EdgeMAX-EdgeRouter-X » -X-SFP-bootloader-update/ba-p/1472216 It is much easier to update the EdgeRouter's bootloader when the EdgeRouter is » connected to the internet. You may need to prepend "sudo" to one for more of the following commands, to get » this to work: https://community.ubnt.com/t5/EdgeMAX/ERX-bootloader-update/td-p/1892923 https://community.ubnt.com/t5/EdgeRouter/ER-X-bootloader-update-versions/td-p/2134 » 544
 39. EdgeRouter Power Cycle Warning	<>	40. EdgeOS file system layout and firmware images @BranoB made the following interesting posting: https://community.ubnt.com/t5/EdgeRouter/EdgeOS-file-system-layout-and-firmware-im » ages/m-p/2377075 41. EdgeRouter Power Cycle Warning
Generally, you should use the reboot button that is located on the system screen » to restart the EdgeRouter; don't simply remove power to the EdgeRouter, if you can help it. Reference TBD	=	Generally, you should use the reboot button that is located on the system screen » to restart the EdgeRouter; don't simply remove power to the EdgeRouter, if you can help it. Reference TBD
40. EdgeRouter UPnP	<>	42. 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	=	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

41. Extended GUI Access / Use May Crash the EdgeRouter	<>	43. 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.	=	Leaving the EdgeRouter's GUI interface up for extended periods of time (maybe like » a day or so) may crash the Edgerouter.
I can't find my original reference, so here is a related one: One specific example is leaving the GUI open which can cause an unexpected » reboot. We are currently working on a fix for this. It's not convenient, but saying out of the GUI may prevent these reboots assuming it is the same » cause.	=	I can't find my original reference, so here is a related one: One specific example is leaving the GUI open which can cause an unexpected » reboot. We are currently working on a fix for this. It's not convenient, but saying out of the GUI may prevent these reboots assuming it is the same » cause.
	-+	
https://community.ubnt.com/t5/EdgeMAX/ER-PRO-8-random-reboots-1-9-7-hotfix-1/td-p/ » 2033684	=	https://community.ubnt.com/t5/EdgeMAX/ER-PRO-8-random-reboots-1-9-7-hotfix-1/td-p/ » 2033684
	<>	Page 58 of 157 » 5/18/2019
42. EdgeRouter Toolbox		44. 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 74 –Toolbox Items.	=	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 74 –Toolbox Items.
Figure 74 –Toolbox Items	<>	Figure 74 –Toolbox Items
	=	
	<>	There is a handy log monitor here: https://community.ubnt.com/t5/EdgeRouter/Viewing-Firewall-Logs-in-GUI/m-p/2686126/highlight/true#M241809
Page 52 of 136 » 2/4/2019		Page 59 of 157 » 5/18/2019
43. Address Groups		45. Address Groups
The software in the EdgeRouter allows the user to define Address Groups. These » groups are used for convenience.	=	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.	<>	We will define several address groups.
Select the "Firewall/NAT" Button from the top of the screen. See Figure 75 – » Firewall/NAT Button.	=	Select the "Firewall/NAT" Button from the top of the screen. See Figure 75 – » Firewall/NAT Button.
Figure 75 – Firewall/NAT Button	<>	Figure 75 – Firewall/NAT Button
From the tabs that are shown, select "Firewall/NAT Groups". See Figure 76 – » Firewall/NAT Groups Tab.	=	From the tabs that are shown, select "Firewall/NAT Groups". See Figure 76 – » Firewall/NAT Groups Tab.
Figure 76 – Firewall/NAT Groups Tab	<>	Figure 76 – Firewall/NAT Groups Tab
Find the "+ Add Group" button and click it. See Figure 77 – Add Group Button.	=	Find the "+ Add Group" button and click it. See Figure 77 – Add Group Button.

Figure 77 – Add Group Button	<>	Figure 77 – Add Group Button
You will see the “Create New Firewall/NAT Group” dialog. Fill in this form as » follows:	=	You will see the “Create New Firewall/NAT Group” dialog. Fill in this form as » follows:
Name: WIRED_IOT_GROUP Description: Wired Iot Group	<>	Name: OPENDNS_SERVERS_GROUP Description: OpenDNS Servers
Group Type: Address Group. See Figure 78 – Example New Address Group Dialog. Press “Save.”	=	Group Type: Address Group. See Figure 78 – Example New Address Group Dialog. Press “Save.”
Figure 78 – Example New Address Group Dialog An empty Address group will have been added. Note that the “Number of group » members” is 0. See Figure 79 – Added Address Group.		Figure 78 – Example New Address Group Dialog An empty Address group will have been added. Note that the “Number of group » members” is 0. See Figure 79 – Added Address Group.
Figure 79 – Added Address Group	<>	Figure 79 – Added Address Group
	=	
Page 53 of 136 » 2/4/2019 Press the WIRED_IOT_GROUP‘s Action button and select Config. See Figure 80 – » Address Group Actions	<>	Page 60 of 157 » 5/18/2019 Press the OPENDNS_SERVERS_GROUP ‘s Action button and select Config. See Figure 80 » – Address Group Actions
Figure 80 – Address Group Actions Enter the address specifier of:	=	Figure 80 – Address Group Actions Enter the address specifier of:
192.168.4.0/24	<>	208.67.222.222 Press the “+ Add New” button and then add 208.67.220.220
See Figure 81 – Example Edit Address Group. Press “Save.” When it is finished » updating, close the dialog.	=	See Figure 81 – Example Edit Address Group. Press “Save.” When it is finished » updating, close the dialog.
Figure 81 – Example Edit Address Group		Figure 81 – Example Edit Address Group
Page 54 of 136 » 2/4/2019	+-	
Repeat the above steps for the following address groups. If there is more than one » address listed in a group, then you will need to use the “+ Add New” button to add additional address(es) to the » group. You have just done the	=	Repeat the above steps for the following address groups. If there is more than one » address listed in a group, then you will need to use the “+ Add New” button to add additional address(es) to the » group. You have just done the
WIRED_IOT_GROUP.	<>	OPENDNS_SERVERS_GROUP.
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"
}
}
		address-group OPENDNS_SERVERS_GROUP {
		address 208.67.222.222
		address 208.67.220.220
		description "OpenDNS Servers"
		}
		address-group RFC-1918_GROUP {
		address 192.168.0.0/16
		
		address 172.16.0.0/12
		
		address 10.0.0.0/8
		description "RFC-1918 Group"
		}
		
		}

The above text section is from the backup file.	=	The above text section is from the backup file.
Page 55 of 136 » 2/4/2019 44. EdgeRouter Layman’s Firewall Explanation	<>	Page 61 of 157 » 5/18/2019 46. EdgeRouter Layman’s Firewall Explanation
I initially had trouble understanding the EdgeRouter’s firewall rules. The » firewall rules that I saw on the internet appeared backwards (in direction) to me. I also didn’t understand what “local” » rules meant or applied to. Then I found the article “Layman's firewall explanation”. Reference: » https://community.ubnt.com/t5/EdgeMAX/Layman-s-firewall-explanation/td-p/1436103	=	I initially had trouble understanding the EdgeRouter’s firewall rules. The » firewall rules that I saw on the internet appeared backwards (in direction) to me. I also didn’t understand what “local” » rules meant or applied to. Then I found the article “Layman's firewall explanation”. Reference: » https://community.ubnt.com/t5/EdgeMAX/Layman-s-firewall-explanation/td-p/1436103

I highly recommend that you stop and read that entire posting now. I have re-produced the main diagram, from that article, as Figure 82 – 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.		I highly recommend that you stop and read that entire posting now. I have re-produced the main diagram, from that article, as Figure 82 – 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 82 – Layman's Firewall Explanation Diagram	<>	Figure 82 – 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		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 82 – Layman's Firewall Explanation Diagram.	<>	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 82 – Layman's Firewall Explanation Diagram. The In and » Out directions are referenced as viewed from the EdgeRouter.
	=	
Each firewall rule, within a ruleset, also has an action of "accept," "reject," or » "drop." Each IP packet attempting to traverse an interface that has firewall rules will be tested by the individual » firewall rules, in the ruleset order, until a firewall rules matches the rule's condition criteria. The individual firewall » rules contain conditions that need to all be matched for that firewall rule to perform its action. If no firewall rules » match an IP packet, then the ruleset's default action is taken for that packet. Once an IP packet matches an individual » firewall rule, no other firewall processing is needed for that IP packet.		Each firewall rule, within a ruleset, also has an action of "accept," "reject," or » "drop." Each IP packet attempting to traverse an interface that has firewall rules will be tested by the individual » firewall rules, in the ruleset order, until a firewall rules matches the rule's condition criteria. The individual firewall » rules contain conditions that need to all be matched for that firewall rule to perform its action. If no firewall rules » match an IP packet, then the ruleset's default action is taken for that packet. Once an IP packet matches an individual » firewall rule, no other firewall processing is needed for that IP packet.
	<>	
Page 56 of 136 » 2/4/2019		Page 62 of 157 » 5/18/2019
Firewall rules within the ruleset are applied (tested) in the specific order that » they were arranged. Therefore, it is	=	Firewall rules within the ruleset are applied (tested) in the specific order that » they were arranged. Therefore, it is

important to order the firewall rules so that the most frequently used rules are » arranged at or near the top of the set of rules, allowing for efficiency within the EdgeRouter.		important to order the firewall rules so that the most frequently used rules are » arranged at or near the top of the set of rules, allowing for efficiency within the EdgeRouter.
	-+	Sometimes the firewall rule numbers seem to increment by one and sometimes they » increment by ten. I think that different versions of EdgeRouter firmware have implemented numbering » differently, so don’t worry if your firewall rule’s absolute numbers don’t match this guide, only the rules ordering » matters. Firewall processing is ordered by lowest number to highest number.
Firewall policies are applied before SNAT (Source Network Address Translation) and » after DNAT (Destination Network Address Translation). The descriptions above are by no means exact regarding what is happening » internally. These descriptions are just meant to convey enough information to help understand these firewall rules, their » design, and their operation. Additional References: https://help.ubnt.com/hc/en-us/articles/204976664-EdgeMAX-How-are-packets-processe » d-by-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 regarding what is happening » internally. These descriptions are just meant to convey enough information to help understand these firewall rules, their » design, and their operation. Additional References: https://help.ubnt.com/hc/en-us/articles/204976664-EdgeMAX-How-are-packets-processe » d-by-EdgeRouter
	<>	You can issue a CLI command to view the firewall’s connection table with: sudo conntrack -L
Page 57 of 136 » 2/4/2019 45. Firewall State		Page 63 of 157 » 5/18/2019 47. Firewall State
There are many conditions available that can constitute a firewall rule. One of » the most important conditions is “State.” States are maintained internally by the underlying firewall code that is » within the EdgeRouter, and are: New – a packet starting a new connection Invalid – packets that have invalid data in them Established – packets associated with an existing connection (conversation) Related – packets related to an existing connection (conversation)	=	There are many conditions available that can constitute a firewall rule. One of » the most important conditions is “State.” States are maintained internally by the underlying firewall code that is » within the EdgeRouter, and are: New – a packet starting a new connection Invalid – packets that have invalid data in them Established – packets associated with an existing connection (conversation) Related – packets related to an existing connection (conversation)
46. WAN Firewall Rules	<>	48. WAN Firewall Rules
The most important firewall rules in an EdgeRouter, from a security standpoint, » are the default WAN_IN and WAN_LOCAL rulesets. These rulesets were generated by the WLAN+2LAN2 Wizard. The » firewall rules with these rulesets provide the “firewall” protection associated with (consumer) Network » Address Translation (NAT) routers.	=	The most important firewall rules in an EdgeRouter, from a security standpoint, » are the default WAN_IN and WAN_LOCAL rulesets. These rulesets were generated by the WLAN+2LAN2 Wizard. The » firewall rules with these rulesets provide the “firewall” protection associated with (consumer) Network » Address Translation (NAT) routers.

```
The WAN_IN and WAN_LOCAL rulesets are identical, except for naming, and for the
» interface that they are
applied to. This is the WAN_IN ruleset, from the backup file:
        name   WAN_IN  {
             default-action    drop
             description    "WAN  to internal"
             rule  10  {
                  action  accept
                  description   "Allow   established/related"
                  state  {
                       established   enable
                       related  enable
                  }
             }
             rule  20  {
                  action  drop
                  description   "Drop   invalid  state"
                  state  {
                       invalid  enable
                  }
             }
        }
The name of this ruleset is WAN_IN. The rules in this ruleset are applied (not
» shown here) to the input side of the
eth0 interface, i.e., to IP packets that are entering the EdgeRouter from the
» internet.
This ruleset has a default action of drop. If a packet destined for this interface
» doesn’t match any firewall rule,
then the packet will be dropped.
The first rule (rule 10) in the ruleset has an action of “accept,” and will allow
» packets that are “established” and
“related” (i.e. associated) to an existing IP conversation to enter eth0. The only
» way to have an existing
connection on eth0 is for the connection to have been started from within the
» EdgeRouter’s system, i.e., from the
EdgeRouter itself, or from a device on one of the EdgeRouter Networks. Note that
» there are no other / additional
qualifiers on this rule(s), so it is applied to every IP packet entering from the
» internet.
The second rule (rule 20) has an action of “drop.” Any packet matching this rule:
```

```
The WAN_IN and WAN_LOCAL rulesets are identical, except for naming, and for the
» interface that they are
applied to. This is the WAN_IN ruleset, from the backup file:
        name   WAN_IN  {
             default-action    drop
             description    "WAN  to internal"
             rule  10  {
                  action  accept
                  description   "Allow   established/related"
                  state  {
                       established   enable
                       related  enable
                  }
             }
             rule  20  {
                  action  drop
                  description   "Drop   invalid  state"
                  state  {
                       invalid  enable
                  }
             }
        }
The name of this ruleset is WAN_IN. The rules in this ruleset are applied (not
» shown here) to the input side of the
eth0 interface, i.e., to IP packets that are entering the EdgeRouter from the
» internet.
This ruleset has a default action of drop. If a packet destined for this interface
» doesn’t match any firewall rule,
then the packet will be dropped.
The first rule (rule 10) in the ruleset has an action of “accept,” and will allow
» packets that are “established” and
“related” (i.e. associated) to an existing IP conversation to enter eth0. The only
» way to have an existing
connection on eth0 is for the connection to have been started from within the
» EdgeRouter’s system, i.e., from the
EdgeRouter itself, or from a device on one of the EdgeRouter Networks. Note that
» there are no other / additional
qualifiers on this rule(s), so it is applied to every IP packet entering from the
» internet.
The second rule (rule 20) has an action of “drop.” Any packet matching this rule:
```

» “invalid state” will be dropped. 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.		» “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.
Page 58 of 136 » 2/4/2019 47. EdgeRouter Detailed Firewall Setup	<>	Page 64 of 157 » 5/18/2019 49. EdgeRouter Detailed Firewall Setup
I have adapted Figure 82 – Layman’s Firewall Explanation Diagram to my own » diagram. See Figure 83 – Detailed Firewall Setup Diagram. The FireWall Rules (FWR) that are described in this guide are numbered (as FWR*) » in Figure 83 – Detailed Firewall Setup Diagram. Each is associated with a named firewall ruleset that will be » described in the following sections. FWRs that are colored red means a ruleset terminates with a default of drop, while » FWRs colored green mean a default of accept. The firewall rule sets are: FWR1 = WAN_LOCAL. FWR2 = WAN_IN. FWR3 = WIRED_IOT_LOCAL. FWR4 = WIRED_SEPARATE_LOCAL. FWR5 = WIRED_SEPARATE_IN. FWR6 = WIRED_SEPARATE_OUT. FWR7 = HOME_OUT (same single set of rules, but shown in two » places). FWR8 = WIFI_GUEST_LOCAL. FWR9 = WIFI_IOT_LOCAL.	=	I have adapted Figure 82 – Layman’s Firewall Explanation Diagram to my own » diagram. See Figure 83 – Detailed Firewall Setup Diagram. The FireWall Rules (FWR) that are described in this guide are numbered (as FWR*) » in Figure 83 – Detailed Firewall Setup Diagram. Each is associated with a named firewall ruleset that will be » described in the following sections. FWRs that are colored red means a ruleset terminates with a default of drop, while » FWRs colored green mean a default of accept. The firewall rule sets are: FWR1 = WAN_LOCAL. FWR2 = WAN_IN. FWR3 = WIRED_IOT_LOCAL. FWR4 = WIRED_SEPARATE_LOCAL. FWR5 = WIRED_SEPARATE_IN. FWR6 = WIRED_SEPARATE_OUT. FWR7 = HOME_OUT (same single set of rules, but shown in two » places). FWR8 = WIFI_GUEST_LOCAL. FWR9 = WIFI_IOT_LOCAL.
	-+	FWR10 = WIFI_SPARE_LOCAL (identical to FWR8, but not shown).
The descriptions below are by no means exact regarding what is happening » internally. These descriptions are just meant to convey enough information to help understand these firewall rules, their » design and their operation. Figure 83 – Detailed Firewall Setup Diagram	=	The descriptions below are by no means exact regarding what is happening » internally. These descriptions are just meant to convey enough information to help understand these firewall rules, their » design and their operation. Figure 83 – Detailed Firewall Setup Diagram
Page 59 of 136	<>	Page 65 of 157

» 2/4/2019 48. WAN_LOCAL Firewall Rules The basic operation of these firewall rules is described above, in the section » titled “46 - WAN Firewall Rules”.		» 5/18/2019 50. WAN_LOCAL Firewall Rules The basic operation of these firewall rules is described above, in the section » titled “48 - WAN Firewall Rules”.
These rules are FRW1 as shown in Figure 83 – Detailed Firewall Setup Diagram.	=	These rules are FRW1 as shown in Figure 83 – Detailed Firewall Setup Diagram.
Add Optional VPN information, etc… A VPN link: https://help.ubnt.com/hc/en-us/articles/115015971688-EdgeRouter-OpenVPN-Server	+-	
	=	
49. WAN_IN Firewall Rules The basic operation of these firewall rules is described above, in the section » titled “46 - WAN Firewall Rules”.	<>	51. WAN_IN Firewall Rules The basic operation of these firewall rules is described above, in the section » titled “48 - WAN Firewall Rules”.
These rules are FRW2 as shown in Figure 83 – Detailed Firewall Setup Diagram. Add forwarded ports, etc…	=	These rules are FRW2 as shown in Figure 83 – Detailed Firewall Setup Diagram. Add forwarded ports, etc…
Page 60 of 136 » 2/4/2019 50. HOME_OUT Firewall Rules There are six firewall rules in this ruleset. These firewall rules inspect IP » packets that are exiting the EdgeRouter	<>	Page 66 of 157 » 5/18/2019 52. HOME_OUT Firewall Rules There are five firewall rules in this ruleset. These firewall rules inspect IP » packets that are exiting the EdgeRouter
towards devices on the Home Network. Reference “FWR7,” shown as two instances, in » the upper-right of Figure 83 – Detailed Firewall Setup Diagram.	=	towards devices on the Home Network. Reference “FWR7,” shown as two instances, in » the upper-right of Figure 83 – 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 that 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 Gues » t Network.	<>	These five rules are maintained as four accept rules (one rule per interface), » followed by one general-purpose drop rule. Each interface is a separate Network. Except for naming and the Network » that they are applied to, the accept rules are identical. The four Networks, which these are applied-to, are: » Wired Iot Network, Wifi Iot Network, Wifi Guest Network, and Wifi Spare Network.
The following section of backup file will be referenced later, so it was given a » reference tag of Equation 1 – A Portion of the HOME_OUT Firewall Ruleset.	=	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:	<>	This is a portion from the backup file:
name HOME_OUT {		name HOME_OUT {
default-action accept description "Home Out"	=	default-action accept description "Home Out"
rule 1 {	<>	rule 10 {
action accept	=	action accept
description "Allow Wired Iot Replies"	<>	description "Allow Wired Iot Established Replies"

log disable	=	log disable
protocol all		protocol all
source {		source {
group {		group {
address-group WIRED_IOT_GROUP	<>	address-group NETv4_eth1
}	=	}
}		}
state {		state {
established enable		established enable
invalid disable		invalid disable
new disable		new disable
related enable		related enable
}		}
}		}
	<>	...
rule 2 {		rule 50 {
action drop	=	action drop
description "Drop Rest-Of Wired Iot Traffic"	<>	description "Drop RFC-1918 Traffic"
log disable	=	log disable
protocol all		protocol all
source {		source {
group {		group {
address-group WIRED_IOT_GROUP	<>	address-group RFC-1918_GROUP
}	=	}
}		}
}		}
	<>	}
…		
Equation 1 – A Portion of the HOME_OUT Firewall » Ruleset	=	Equation 1 – A Portion of the HOME_OUT Firewall » Ruleset
Page 61 of 136 » 2/4/2019	<>	Page 67 of 157 » 5/18/2019
The name of this ruleset is HOME_OUT. The rules in this ruleset are applied (not » shown here) to the output side of	=	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	<>	both of the eth3 and eth4 interfaces, i.e., switch0. These interfaces are also » known as the Home Network. IP
packets that are exiting the EdgeRouter (on eth3/eth4) towards equipment on the » Home Network are inspected and potentially dropped by these firewall rules. Remember that eth3 and eth4 are » still bound together by the	=	packets that are exiting the EdgeRouter (on eth3/eth4) towards equipment on the » Home Network are inspected and potentially dropped by these firewall rules. Remember that eth3 and eth4 are » still bound together by the

switch hardware within the EdgeRouter. In Figure 83 – 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.		switch hardware within the EdgeRouter. In Figure 83 – Detailed Firewall Setup » Diagram, this information is shown as duplicated in two blocks (in the upper-right portion of the diagram), each » labeled with FWR7. This ruleset has a default action of “accept.” If a packet destined for this » interface doesn’t match any individual firewall rule, then the packet will be accepted, i.e., passed along to devices » attached to the Home Network.
The first rule (rule 1) in this ruleset has an action of “accept,” and will allow » IP packets that are “established” and	<>	The first rule (rule 10) in this ruleset has an action of “accept,” and will allow » IP packets that are “established” and
“related” (i.e. associated) to an existing IP conversation, to exit the EdgeRouter » to devices that are on the Home Network. Note that this rule has an additional qualifier that the source address » must be in the address range of the WIRED_IOT_GROUP, i.e., this rule only apples to traffic that originates from » the Wired IOT Network. The only way to have an existing connection between Wired IOT Network and the Home Network » is for the conversation to have been started from devices within the Home Network. The name associated with » this rule is "Allow Wired Iot Replies."	=	“related” (i.e. associated) to an existing IP conversation, to exit the EdgeRouter » to devices that are on the Home Network. Note that this rule has an additional qualifier that the source address » must be in the address range of the WIRED_IOT_GROUP, i.e., this rule only apples to traffic that originates from » the Wired IOT Network. The only way to have an existing connection between Wired IOT Network and the Home Network » is for the conversation to have been started from devices within the Home Network. The name associated with » this rule is "Allow Wired Iot Replies."
The second rule (rule 2) in this ruleset has an action of “drop,” and will drop al » l other IP packets that 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 tr » affic that 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.	<>	Rules 20, 30, and 40 are also “accept”, “established / related”, operate identical » to Rule 10, but are applied to different Networks. Rule 50 in this ruleset has an action of “drop,” and will drop all other IP » packets that originate from any RFC-1918 address. This address set include all of the Networks used in this project. This » is a change from earlier versions of this guide, as there was separate “drop” rule for each Network. Reference section » 84 - Simple Service Discovery Protocol (SSDP) / igmp-proxy for what I found that slipped around the previous » rules. The two rules, number 10 and number 50, treated as a set, describe the IP » connections (conversations) that can occur between equipment on the Wired IOT Network and the Home Network.
If the conversation was started by devices in the Home Network and directed to » devices residing on the Wired IOT Network, then replies to those conversations will be allowed back into the Home » Network by firewall rule number	=	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	<>	10. Internally, the firewall code keeps track of IP connections, which are

» the EdgeRouter (the “In” side)		» entering the EdgeRouter (the “In” side)
and then allows traffic that is related to that data to exit the EdgeRouter	=	and then allows traffic that is related to that data to exit the EdgeRouter
» towards the Home Network devices.		» towards the Home Network devices.
If a conversation was instead started by devices within the Wired IOT Network and		If a conversation was instead started by devices within the Wired IOT Network and
» directed towards the Home		» directed towards the Home
Network, firewall rule 1 will have no prior knowledge about this conversation	<>	Network, firewall rule 10 will have no prior knowledge about this conversation
» (because it is not		» (because it is not
“established”/”related”). Therefore, firewall rule number 1 will not match, and		“established”/”related”). Therefore, firewall rule number 10 will not match, and
» firewall rule processing will then		» firewall rule processing will then
proceed to rule number 2. Rule number two drops all traffic from the Wired IOT		proceed to rule number 20. Rules number 20, 30, and 40 do not apply to traffic
» Network.		» from the Wired IOT Network, so
There are two more sets of two rules (not shown here) within this ruleset, an iden		those rules do not apply, and no action is taken for them. When this traffic is in
» tical set applied to the Wifi		» spected by rule number 50, this
Guest Network (WIFI_GUEST_GROUP), and an identical set applied to the Wifi IOT		rules condition will match, and the “drop” action will be taken. This data will be
» Network (WIFI_IOT_GROUP).		» discarded by the EdgeRouter, and
		will therefore NOT reach any device on the Home Network.
Remember that the default action for this ruleset is “accept.” You want the Home	=	Remember that the default action for this ruleset is “accept.” You want the Home
» Network to be able to operate		» Network to be able to operate
on its own, when it is not conversing with just these three networks.	<>	on its own, i.e. over the Internet, when it is not conversing with just these
		» internal Networks.
Note that every IP packet attempting to exit the EdgeRouter towards devices on the	=	Note that every IP packet attempting to exit the EdgeRouter towards devices on the
» Home Network will need to		» Home Network will need to
be inspected by these six firewall rules. Most of the traffic destined for the		be inspected by these six firewall rules. Most of the traffic destined for the
» Home Network will not be from one of		» Home Network will not be from one of
the IOT or Guest Networks.		the IOT or Guest Networks.
QUESTION: Maybe a single firewall rule can be added, at the top of this ruleset,		QUESTION: Maybe a single firewall rule can be added, at the top of this ruleset,
» which allows internet traffic to be		» which allows internet traffic to be
accepted. This would increase the efficiency of this ruleset, by not depending		accepted. This would increase the efficiency of this ruleset, by not depending
» upon most of the traffic to reach the		» upon most of the traffic to reach the
default “accept” rule before being accepted.		default “accept” rule before being accepted.
Page 62 of 136	<>	Page 68 of 157
» 2/4/2019		» 5/18/2019
51. Firewall Conditions		53. Firewall Conditions
The following figures are from the “Add New Rule” firewall dialog. We will explain	=	The following figures are from the “Add New Rule” firewall dialog. We will explain
» how to get to these in the next		» how to get to these in the next
section. There are several Tabs in this dialog for entering firewall conditions.		section. There are several Tabs in this dialog for entering firewall conditions.
» You might want to study the		» You might want to study the
following figures, and familiarize yourself with what firewall conditions are		following figures, and familiarize yourself with what firewall conditions are
» available. See the following figures:		» available. See the following figures:
Figure 84 – Firewall Conditions, Basic Tab.		Figure 84 – Firewall Conditions, Basic Tab.

Figure 85 – Firewall Conditions, Advanced Tab. Figure 86 – Firewall Conditions, Source Tab. Figure 87 – Firewall Conditions, Destination Tab. Figure 88 – Firewall Conditions, Time Tab. Figure 84 – Firewall Conditions, Basic Tab Figure 85 – Firewall Conditions, Advanced Tab		Figure 85 – Firewall Conditions, Advanced Tab. Figure 86 – Firewall Conditions, Source Tab. Figure 87 – Firewall Conditions, Destination Tab. Figure 88 – Firewall Conditions, Time Tab. Figure 84 – Firewall Conditions, Basic Tab Figure 85 – Firewall Conditions, Advanced Tab
Page 63 of 136 » 2/4/2019	<>	Page 69 of 157 » 5/18/2019
Figure 86 – Firewall Conditions, Source Tab Figure 87 – Firewall Conditions, Destination Tab Figure 88 – Firewall Conditions, Time Tab	=	Figure 86 – Firewall Conditions, Source Tab Figure 87 – Firewall Conditions, Destination Tab Figure 88 – Firewall Conditions, Time Tab
Page 64 of 136 » 2/4/2019 52. Adding Firewall Rules	<>	Page 70 of 157 » 5/18/2019 54. Adding Firewall Rules
Hopefully, you now understand the design of the HOME_OUT firewall rules. Now it is » time to actually add these	=	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	<>	rules. This section will use a portion of HOME_OUT rules as an example of how to » add firewall rules using the GUI
interface. While you are using the GUI to add these rules, please frequently reference the » backup file segment labeled	=	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 “50 - » HOME_OUT Firewall Rules.”	<>	“Equation 1 – A Portion of the HOME_OUT Firewall Rules”, which is in section “52 - » 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 75 – » Firewall/NAT Button. Ensure that the “Firewall Policies” tab is selected. See Figure 89 – Firewall » Policies Tab. Figure 89 – Firewall Policies Tab The two WAN rulesets, which were added by the Wizard, should be shown. Press the » “+ Add Ruleset” button. See Figure 90 – Add Ruleset. Figure 90 – Add Ruleset You will be presented with a “Create New firewall Ruleset.” See Figure 91 – Blank » Create New Firewall Ruleset. Figure 91 – Blank Create New Firewall Ruleset	=	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 75 – » Firewall/NAT Button. Ensure that the “Firewall Policies” tab is selected. See Figure 89 – Firewall » Policies Tab. Figure 89 – Firewall Policies Tab The two WAN rulesets, which were added by the Wizard, should be shown. Press the » “+ Add Ruleset” button. See Figure 90 – Add Ruleset. Figure 90 – Add Ruleset You will be presented with a “Create New firewall Ruleset.” See Figure 91 – Blank » Create New Firewall Ruleset. Figure 91 – Blank Create New Firewall Ruleset
Page 65 of 136 » 2/4/2019	<>	Page 71 of 157 » 5/18/2019

Enter the following into the Create New Firewall Ruleset dialog: Name HOME_OUT Description Home Out Default action Accept See Figure 92 – HOME_OUT Example New Ruleset. Figure 92 – 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 93 – Empty HOME_OUT Ruleset. Figure 93 – 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 94 – Firewall Actions Menu. Figure 94 – Firewall Actions Menu	=	Enter the following into the Create New Firewall Ruleset dialog: Name HOME_OUT Description Home Out Default action Accept See Figure 92 – HOME_OUT Example New Ruleset. Figure 92 – 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 93 – Empty HOME_OUT Ruleset. Figure 93 – 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 94 – Firewall Actions Menu. Figure 94 – Firewall Actions Menu
Page 66 of 136 » 2/4/2019	<>	Page 72 of 157 » 5/18/2019
Choose “Edit Ruleset.” A dialog for editing firewall rules appears. The “Rules” » Tab should already be selected. See Figure 95 – 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 94 » – Firewall Actions Menu. Figure 95 – Edit Ruleset Dialog Choose the “Configuration” Tab. You should see the information that was entered » earlier. See Figure 96 – Firewall Rule Configuration Tab. Figure 96 – 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 97 » – Firewall Rule Interface Tab.	=	Choose “Edit Ruleset.” A dialog for editing firewall rules appears. The “Rules” » Tab should already be selected. See Figure 95 – 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 94 » – Firewall Actions Menu. Figure 95 – Edit Ruleset Dialog Choose the “Configuration” Tab. You should see the information that was entered » earlier. See Figure 96 – Firewall Rule Configuration Tab. Figure 96 – 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 97 » – Firewall Rule Interface Tab.

Figure 97 – Firewall Rule Interface Tab		Figure 97 – Firewall Rule Interface Tab
Page 67 of 136 » 2/4/2019	<>	Page 73 of 157 » 5/18/2019
Re-select the “Rules” Tab, and press the “Add New Rule” Button, that is shown in » Figure 95 – Edit Ruleset Dialog. An “Add New Rule” dialog will be shown. See Figure 98 – 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 98 – HOME_OUT Firewall, Rule1, Basic Click on the Advanced Tab. See Figure 99 – 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 99 – HOME_OUT Firewall, Rule1, Advanced	=	Re-select the “Rules” Tab, and press the “Add New Rule” Button, that is shown in » Figure 95 – Edit Ruleset Dialog. An “Add New Rule” dialog will be shown. See Figure 98 – 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 98 – HOME_OUT Firewall, Rule1, Basic Click on the Advanced Tab. See Figure 99 – 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 99 – HOME_OUT Firewall, Rule1, Advanced
Page 68 of 136 » 2/4/2019	<>	Page 74 of 157 » 5/18/2019
Click on the Source Tab. See Figure 100 – HOME_OUT Firewall, Rule 1, Source. » Select the following information for the Source Tab:	=	Click on the Source Tab. See Figure 100 – HOME_OUT Firewall, Rule 1, Source. » Select the following information for the Source Tab:
Address Group Wired Iot Group.	<>	Interface Network eth1
	=	
Figure 100 – HOME_OUT Firewall, Rule 1, Source	<>	Figure 100 – HOME_OUT Firewall, Rule 1, Source
	=	
Press the “Save” button. You now have a new rule in the HOME_OUT ruleset. See Figu » re 101 – HOME_OUT Firewall, Rule 1.	<>	Press the “Save” button. Earlier versions of this guide used an “Address Group” » instead of “Interface Network”. These two methods are equivalent, but there was more setup involved in using an » “Address Group”. Reference https://community.ubnt.com/t5/EdgeRouter/Firewall-Interface-Addr-vs-Interface-Netw » ork/td-p/2238960 You now have a new rule in the HOME_OUT ruleset. See Figure 101 – HOME_OUT » Firewall, Rule 1.
	=	

Figure 101 – HOME_OUT Firewall, Rule 1	<>	Figure 101 – HOME_OUT Firewall, Rule 1
	=	
It is time to add the second firewall rule of this ruleset. Press the “Add New » Rule” button, as shown in Figure 101 – HOME_OUT Firewall, Rule 1. You will be presented with the Basic dialog for adding » firewall rules. See Figure 102 – HOME_OUT Firewall, Rule 2, Basic. Enter the following information into the Basic » Tab:	<>	
Description Drop Rest-Of Wired Iot Traffic Enable CHECKED Action Drop Protocol All protocols		
Figure 102 – HOME_OUT Firewall, Rule 2, Basic		
Click on the Source Tab. See Figure 103 – HOME_OUT Firewall, Rule 2, Source. » Select the following information for the Source Tab:		
Address Group Wired Iot Group.		
Figure 103 – HOME_OUT Firewall, Rule 2, Source		55. Adding More HOME_OUT Firewall Rules
Press the “Save” button. You now have two rules in the HOME_OUT ruleset, as shown » in Figure 104 – HOME_OUT Firewall, Two Rules. The first rule allow traffic that is “established” and “related” (i.e. associated) » to go out FROM the EdgeRouter, towards devices on the Home Network that have a SOURCE address that matches » (originated from) the Wired IOT Network. The association would be to traffic that previously went IN (towards the » EdgeRouter) destined for the Wired IOT Network. This would typically be a request to a device on the Wired IOT » Network from a device on the Home Network. The second rule drops all traffic from the Wired IOT Network that was not matched » by the first rule, i.e., any non-requested traffic that 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.		We now need to add three more rules to the HOME_OUT Ruleset. These rules have iden » tical composition to the rule that was already added,, only the names and sources are different. Using the » steps that are shown in the

Figure 104 – HOME_OUT Firewall, Two Rules		
Page 70 of 136		
» 2/4/2019		
53. Adding More HOME_OUT Firewall Rules		
We now need to add four more rules to the HOME_OUT Ruleset. Using the steps that		
» are shown in the above		
section “52 - Adding Firewall Rules”, add four more rules per the backup data that		above section “54 - Adding Firewall Rules”, add three more rules per the backup
» is shown below:		» data that is shown below:
rule 3 {		rule 20 {
action accept	=	action accept
description "Allow Wifi Guest Replies"	<>	description "Allow Wifi Guest Established Replies"
log disable	=	log disable
protocol all		protocol all
source {		source {
group {		group {
address-group WIFI_GUEST_GROUP	<>	address-group NETv4_switch0.6
}	=	}
}		}
state {		state {
established enable		established enable
invalid disable		invalid disable
new disable		new disable
related enable		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 {		rule 30 {
action accept	=	action accept
description "Allow Wifi Iot Replies"	<>	description "Allow Wifi Iot Established Replies"
log disable	=	log disable

protocol all		protocol all
source {		source {
group {		group {
address-group WIFI_IOT_GROUP	<>	address-group NETv4_switch0.7
}	=	}
}		}
state {		state {
established enable		established enable
invalid disable		invalid disable
new disable		new disable
related enable		related enable
}		}
}		}
	<>	
rule 6 {		rule 40 {
		action accept
		description "Allow Wifi Spare Established Replies"
		log disable
		protocol all
		source {
		group {
		address-group NETv4_switch0.8
		}
		}
		state {
		established enable
		invalid disable
		new disable
		related enable
		}
		}
		Page 76 of 157
		» 5/18/2019
		We now need to add the final “drop” rule to the HOME_OUT Ruleset. This rule
		» consists of:
		Basic Tab has an Action of “drop”.
		Advanced Tab has nothing selected (i.e. no state).
		Source Tab uses an Address Group of “RFC-1918 Group”.
		Using the steps that are shown in the above section “54 - Adding Firewall Rules”,
		» add the last rule per the

		following backup data that is shown below (which matches the above settings):
		rule 50 {
action drop	=	action drop
description "Drop Rest-Of Wifi Iot Traffic"	<>	description "Drop RFC-1918 Traffic"
log disable	=	log disable
protocol all		protocol all
source {		source {
group {	<>	group {
address-group WIFI_IOT_GROUP		address-group RFC-1918_GROUP
}	=	}
}		}
}		}
	<>	Here is a recap of how the HOME_OUT ruleset works.
		The first rule allows traffic that is “established” and “related” (i.e.
		» associated) to go out FROM the EdgeRouter,
		towards devices on the Home Network that have a SOURCE address that matches
		» (originated from) the Wired IOT
		Network. The association would be to traffic that previously went IN (towards the
		» EdgeRouter) destined for the
		Wired IOT Network. This would typically be a request to a device on the Wired IOT
		» Network from a device on the
		Home Network.
		The last rule (which we just configured) drops all traffic from all the local
		» Networks that was not matched by any
		of the established / related rules, i.e., any non-requested traffic that was
		» initiated by a device on one of the non-
		home Networks.
		The default action for the HOME_OUT ruleset is “accept,” allowing traffic that is
		» not SOURCED from the Wired IOT
		Network to pass OUT to devices on the Home Network. This would be traffic coming
		» from the internet, or from
		the EdgeRouter itself.
Page 71 of 136		Page 77 of 157
» 2/4/2019		» 5/18/2019
		Remember that the order of firewall rules really matters in what happens to
		» traffic. The current HOME_OUT rules
		are shown in Figure 102 – Firewall Ruleset Ordering
		Figure 102 – Firewall Ruleset Ordering
		To change the order of firewall rules, you simply drag a row up or down and let
		» go. The numbers will change to

		show you what the order will be when you press the “Save Rule Order” button, which » is in the lower right. To cancel a move, select the “X” in the upper right. Drag the row "Allow Wifi Iot Established Replies" to the top of the entries, » and let go of the mouse button. Your screen should look like Figure 103 – Firewall Ruleset New Order. » Press “Save Rule Order” button. I am doing this, as I expect there will be more replies from Iot equipment than » replies from equipment on any other Network. This processing order should be more efficient. Figure 103 – Firewall Ruleset New Order Page 78 of 157 » 5/18/2019
54. WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules		56. WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules
These rules are FWR3 and FWR9 as shown in Figure 83 – 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 for the Wired Iot and Wifi Iot Networks, presented below, » 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	=	These rules are FWR3 and FWR9 as shown in Figure 83 – 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 for the Wired Iot and Wifi Iot Networks, presented below, » 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 Network’s DHCP entered DNS1 and DNS2 addresses. Reference section » 28 - Add DHCP Servers to the VLANs and section 30 - Modify EdgeRouter’s eth1 DHCP Server. It’s not good to » tell your Iot devices to use one	<>	Iot and Wifi Iot Network’s DHCP entered DNS1 and DNS2 addresses. Reference section » 29 - Add DHCP Servers to the VLANs and section 31 - 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 that are	=	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 that are
shown in the above section “52 - Adding Firewall Rules”, add the following two » rulesets, each containing two	<>	shown in the above section “54 - Adding Firewall Rules”, add the following two » rulesets, each containing two

firewall rules, per the backup data that is shown below:	=	firewall rules, per the backup data that is shown below:
When adding the following WIRED_IOT_LOCAL ruleset, remember to also set and SAVE		When adding the following WIRED_IOT_LOCAL ruleset, remember to also set and SAVE
» the following:		» the following:
Interface: eth1		Interface: eth1
Direction: local		Direction: local
name WIRED_IOT_LOCAL {		name WIRED_IOT_LOCAL {
default-action drop		default-action drop
description "Wired IOT Local"	<>	description "Wired Iot Local"
rule 1 {	=	rule 1 {
action accept		action accept
description "Allow DHCP"		description "Allow DHCP"
destination {		destination {
port 67-68		port 67-68
}		}
log disable		log disable
protocol udp		protocol udp
source {		source {
}		}
}		}
rule 2 {		rule 2 {
action accept		action accept
description "Allow Only OpenDNS"		description "Allow Only OpenDNS"
destination {		destination {
group {		group {
address-group OPENDNS_SERVERS_GROUP		address-group OPENDNS_SERVERS_GROUP
}		}
port 53		port 53
}		}
log disable		log disable
protocol tcp_udp		protocol tcp_udp
}		}
}		}
When adding the DNS rule, the above “tcp_ucp” description is shown in the GUI as		When adding the DNS rule, the above “tcp_ucp” description is shown in the GUI as
» “Both TCP and UDP.”		» “Both TCP and UDP.”
Page 72 of 136	<>	Page 79 of 157
» 2/4/2019		» 5/18/2019
		Note that there is an “Actions” / “Copy Ruleset” available, that can be used to
		» clone an existing ruleset.
When adding the following WIFI_IOT_LOCAL ruleset, remember to also set and SAVE	=	When adding the following WIFI_IOT_LOCAL ruleset, remember to also set and SAVE
» the following:		» the following:

Interface: switch0.7
Direction: local
name WIFI_IOT_LOCAL {
default-action drop
description "WiFi Iot Local"
rule 1 {
action accept
description "Allow DHCP"
destination {
port 67-68
}
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
}
}
		Interface: switch0.7
		Direction: local
		name WIFI_IOT_LOCAL {
		default-action drop
		description "WiFi Iot Local"
		rule 1 {
		action accept
		description "Allow DHCP"
		destination {
		port 67-68
		}
		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.”		When adding the DNS rule, the above “tcp_ucp” description is shown in the GUI as » “Both TCP and UDP.”
Page 73 of 136 » 2/4/2019 55. WIFI_GUEST_LOCAL Firewall Rules	<>	Page 80 of 157 » 5/18/2019 57. WIFI_GUEST_LOCAL Firewall Rules These rules are FWR8 as shown in Figure 83 – Detailed Firewall Setup Diagram.
The purpose of these rules is to block the use of EdgeRouter local services from » the Wi-Fi Guest Network, except for the use of DNS and the operation of DHCP.	=	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 » 54 - WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules.	<>	To add the following ruleset and rules, follow what was done in the above section » “54 - Adding Firewall Rules”.
Note that we are not dropping DNS requests based upon which DNS provider	=	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 just to 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
             }
        }
```

<>

```
    Page 81 of 157
» 5/18/2019
58.  WIFI_SPARE_LOCAL Firewall Rules
These rules are designated as FWR10 but are not shown in Figure 83 – Detailed
» Firewall Setup Diagram. You can
instead look at the similar FWR8.
```

```
                                                    The purpose of these rules is to block the use of EdgeRouter local services from
                                                    » the Wi-Fi Spare Network, except
                                                    for the use of DNS and the operation of DHCP.
                                                    To add the following ruleset and rules, follow what was done in the above section
                                                    » “54 - Adding Firewall Rules”.
                                                    When adding the following WIFI_SPARE_LOCAL ruleset, remember to also set and SAVE
                                                    » the following:
                                                          Interface:         switch0.8
                                                          Direction:         local
                                                            name   WIFI_SPARE_LOCAL     {
                                                                 default-action     drop
                                                                 description    "WiFi   Spare  Local"
                                                                 rule  1 {
                                                                      action  accept
                                                                      description    "Allow   DHCP"
                                                                      destination    {
                                                                           port  67-68
                                                                      }
                                                                      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
                                                                 }
                                                            }
    Page 74 of 136                                      Page 82 of 157
» 2/4/2019                                          » 5/18/2019
56.   Optional DNS Forcing of the WIFI_GUEST_LOCAL Network  59.   Optional DNS Forcing of the WIFI_GUEST_LOCAL Network
Performing the steps within this section is optional.  = Performing the steps within this section is optional.
The destination Network Address Translation (NAT) rules, presented here, will  The destination Network Address Translation (NAT) rules, presented here, will
» force any devices on the guest                    » force any devices on the guest
```

Network to only be able to use Open DNS resolvers. This is regardless of if the » devices specify their own DNS resolver addresses and ignore the DNS resolver addresses suggested by the » EdgeRouter's guest DHCP server.		Network to only be able to use Open DNS resolvers. This is regardless of if the » devices specify their own DNS resolver addresses and ignore the DNS resolver addresses suggested by the » EdgeRouter's guest DHCP server.
The two rules presented here work with each other. Rule #1 will exclude NAT from » being performed on either of the OpenDNS resolver addresses. These two addresses are in an address group. This » allows both the primary and secondary resolver addresses to pass-through the EdgeRouter from the Guest » Network. Rule #2 will act upon any port 53 (DNS) request from the Guest network, and translate the associated IP » address into the address of the primary OpenDNS resolver.	<>	The two rules presented here work with each other. Rule #1 will exclude NAT from » being performed DNS requests directed towards either of the OpenDNS resolver addresses. These two addresses are » in an address group. This allows both the primary and secondary resolver addresses to pass-through the » EdgeRouter from the Guest Network. Rule #2 will act upon any remaining port 53 (DNS) requests (that did not » match Rule #1) from the Guest network, and translate the associated IP address into the address of the primary » OpenDNS resolver.
Press the Firewall/NAT button near the top of the screen. Reference Figure 75 – » Firewall/NAT Button.	=	Press the Firewall/NAT button near the top of the screen. Reference Figure 75 – » Firewall/NAT Button.
Ensure that the NAT tab is selected and then press the "+ Add Destination NAT » Rule" button. See Figure 105 – NAT	<>	Ensure that the NAT tab is selected and then press the "+ Add Destination NAT » Rule" button. See Figure 104 – NAT
Tab.	=	Tab.
Figure 105 – NAT Tab	<>	Figure 104 – NAT Tab
	=	
Page 75 of 136 » 2/4/2019	<>	Page 83 of 157 » 5/18/2019
You will be presented with a "Destination NAT Rule Configuration" dialog. Enter the data for NAT rule #1, as follows: Description Exclude OpenDNS Wifi Guest Enable CHECKED Inbound Interface switch0.6 Translations, Port 53 Exclude From NAT CHECKED Protocol Both TCP and UDP Dest Port 53 Dest Address Group OpenDNS Servers	=	You will be presented with a "Destination NAT Rule Configuration" dialog. Enter the data for NAT rule #1, as follows: Description Exclude OpenDNS Wifi Guest Enable CHECKED Inbound Interface switch0.6 Translations, Port 53 Exclude From NAT CHECKED Protocol Both TCP and UDP Dest Port 53 Dest Address Group OpenDNS Servers
and save it. See Figure 106 – NAT Rule Number 1.	<>	and save it. See Figure 105 – NAT Rule Number 1.
	=	
Figure 106 – NAT Rule Number 1	<>	Figure 105 – NAT Rule Number 1
	=	
Page 76 of 136 » 2/4/2019	<>	Page 84 of 157 » 5/18/2019

Press the “+ Add Destination NAT Rule” button and enter the data for NAT rule #2, as follows:	=	Press the “+ Add Destination NAT Rule” button and enter the data for NAT rule #2, as follows:
Description Force OpenDNS Wifi Guest		Description Force OpenDNS Wifi Guest
Enable CHECKED		Enable CHECKED
Inbound Interface switch0.6		Inbound Interface switch0.6
Translations, Address 208.67.220.220	<>	Translations, Address 208.67.222.222
Exclude From NAT Un-Checked	=	Exclude From NAT Un-Checked
Protocol Both TCP and UDP		Protocol Both TCP and UDP
Dest Port 53		Dest Port 53
and save it. See Figure 107 – NAT Rule Number 2.	<>	and save it. See Figure 106 – NAT Rule Number 2.
	=	
Figure 107 – NAT Rule Number 2	<>	Figure 106 – NAT Rule Number 2
	=	
Page 77 of 136	<>	Page 85 of 157
» 2/4/2019		» 5/18/2019
This is the relevant portion from the backup file. Rule 5010 is an existing Source NAT rule for handling the WAN port (eth0).	=	This is the relevant portion from the backup file. Rule 5010 is an existing Source NAT rule for handling the WAN port (eth0).
nat {		nat {
rule 1 {		rule 1 {
description "Exclude OpenDNS Wifi Guest"	<>	description "Exclude OpenDNS WiFi Guest"
destination {	=	destination {
group {		group {
address-group OPENDNS_SERVERS_GROUP		address-group OPENDNS_SERVERS_GROUP
}		}
port 53		port 53
}		}
exclude		exclude
inbound-interface switch0.6		inbound-interface switch0.6
inside-address {		inside-address {
port 53		port 53
}		}
log disable		log disable
protocol tcp_udp		protocol tcp_udp
type destination		type destination
}		}
rule 2 {		rule 2 {
description "Force OpenDNS WiFi Guest"		description "Force OpenDNS WiFi Guest"
destination {		destination {
port 53		port 53

}		}
inbound-interface switch0.6		inbound-interface switch0.6
inside-address {		inside-address {
address 208.67.220.220	<>	address 208.67.222.222
}	=	}
log disable		log disable
protocol tcp_udp		protocol tcp_udp
type destination		type destination
}		}
rule 5010 {		rule 5010 {
description "masquerade for WAN"		description "masquerade for WAN"
outbound-interface eth0		outbound-interface eth0
type masquerade		type masquerade
}		}
}		}
These rules can be tested, if you are implementing this DNS forcing using actual		These rules can be tested, if you are implementing this DNS forcing using actual
» OpenDNS resolvers. This is		» OpenDNS resolvers. This is
because OpenDNS has a test page:		because OpenDNS has a test page:
http://welcome.opendns.com		http://welcome.opendns.com
that can show if you are using OpenDNS as a resolver.		that can show if you are using OpenDNS as a resolver.
To perform this test, first temporarily change the DNS resolvers associated with		To perform this test, first temporarily change the DNS resolvers associated with
» the Guest Network’s DHCP server		» 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	<>	(switch0.6) to something else. I used addresses of 8.8.8.8 and 8.8.4.4 from
» Google. Reference section 28 - Add		» Google. Reference section 29 - Add
DHCP Servers to the VLANs. Then, using a device attached to the Guest Network,	=	DHCP Servers to the VLANs. Then, using a device attached to the Guest Network,
» visit the OpenDNS test page. If		» visit the OpenDNS test page. If
you get their success page, then these two rules translated the Google DNS		you get their success page, then these two rules translated the Google DNS
» addresses into OpenDNS addresses.		» addresses into OpenDNS addresses.
You may have to reboot the EdgeRouter and/or the Guest device to ensure that the		You may have to reboot the EdgeRouter and/or the Guest device to ensure that the
» changed DNS resolver		» changed DNS resolver
addresses propagated to the Guest device. Remember to return the Guest Network’s		addresses propagated to the Guest device. Remember to return the Guest Network’s
» DNS resolver addresses (in		» DNS resolver addresses (in
the DHCP area) back to the OpenDNS addresses.		the DHCP area) back to the OpenDNS addresses.
Reference this OpenDNS page about testing:		Reference this OpenDNS page about testing:
https://support.opendns.com/hc/en-us/articles/227986567-How-to-Test-for-Successful		https://support.opendns.com/hc/en-us/articles/227986567-How-to-Test-for-Successful
» -OpenDNS-Configuration-		» -OpenDNS-Configuration-
Page 78 of 136	<>	Page 86 of 157
» 2/4/2019		» 5/18/2019
57. WIRED_SEPARATE Firewall Rules		60. WIRED_SEPARATE Firewall Rules
The Wired Separate Network is meant to be kept separate from the other Networks,	=	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.		» 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 your basement. In this instance, you don’t want any people or devices on the Separate » Network to be able to access any of your Networks, or be able to access internals of the EdgeRouter.	<>	In this instance, people and devices on the other Networks cannot get to » your banking computer. 2. You might want to provide internet access to the friend’s kid » (i.e.tenant) who lives in your basement. In this instance, you don’t want any people or devices on the Separate » Network to be able to access any of your other Networks, OR be able to access » the internals of the EdgeRouter. I’m thinking that eth2 needs to be removed from the ER-X’s switch to ensure that » tagged VLAN data does not leak out the eth2 port from the switch usage.
Reference Figure 83 – Detailed Firewall Setup Diagram, for FWR numbers and Network » routing / interactions Reference Table 1 - Table of Networks, for Network subnet addresses	=	Reference Figure 83 – Detailed Firewall Setup Diagram, for FWR numbers and Network » routing / interactions Reference Table 1 - Table of Networks, for Network subnet addresses
To block instance number 1, we need to block traffic from exiting OUT of the » EdgeRouter 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, unless you have disabled configuring these as Guest Networks. To add the following ruleset and rules, follow what was done in the above section » 54 - WIRED_IOT_LOCAL, WIFI_IOT_LOCAL Firewall Rules.	<>	To block instance number 1, we need to block traffic from exiting OUT of the » EdgeRouter that was initiated from another Network / subnet, and then allow other traffic (from the Internet.) To add the following ruleset and rules, follow what was done in the above section » “54 - Adding Firewall Rules”.
When adding the following WIRED_SEPARATE_OUT ruleset, remember to also set and » SAVE the following: Interface: eth2 Direction: out	=	When adding the following WIRED_SEPARATE_OUT ruleset, remember to also set and » SAVE the following: Interface: eth2 Direction: out

name WIRED_SEPARATE_OUT {		name WIRED_SEPARATE_OUT {
default-action accept		default-action accept
description "Wired Separate Out"		description "Wired Separate Out"
rule 1 {		rule 1 {
action drop		action drop
description "Drop Home Network"	<>	description "Drop Non-Separate Traffic"
log disable	=	log disable
protocol all		protocol all
source {		source {
group {		group {
address-group HOME_GROUP	<>	address-group RFC-1918_GROUP
}	=	}
}		}
}		}
rule 2 {	+-	
action drop		
description "Drop Wired Iot Network"		
log disable		
protocol all		
source {		
group {		
address-group WIRED_IOT_GROUP		
}		
}		
}		
}	=	}
Page 79 of 136	<>	Page 87 of 157
» 2/4/2019		» 5/18/2019
To block instance number 2, we need to block traffic from entering IN the		To block the first part of instance number 2, we need to block traffic from
» EdgeRouter and going to devices that		» entering IN the EdgeRouter and going
are on the other networks. This ruleset will be labeled WIRED_SEPARATE_IN and is		to devices that are on any of the other Networks. This ruleset will be labeled
» denoted as FWR5.		» WIRED_SEPARATE_IN and is denoted
Additionally, we need to block traffic from entering the EdgeRouter itself (LOCAL)		as FWR5.
» 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	=	When adding the following WIRED_SEPARATE_IN ruleset, remember to also set and SAVE
» the following:		» the following:
Interface: eth2		Interface: eth2
Direction: in		Direction: in

name WIRED_SEPARATE_IN {		name WIRED_SEPARATE_IN {
default-action accept		default-action accept
description "Wired Separate In"		description "Wired Separate In"
rule 1 {		rule 1 {
action drop		action drop
description "Block Multiple Networks"	<>	description "Block RFC-1918 Traffic"
destination {	=	destination {
group {		group {
address-group MULTIPLE_GROUP	<>	address-group RFC-1918_GROUP
}	=	}
}		}
log disable		log disable
protocol all		protocol all
}		}
}		}
	-+	To block the second part of instance number 2, we need to block traffic from » entering the EdgeRouter itself (LOCAL) except for DNS and DHCP requests. This ruleset will be labeled » WIRED_SEPARATE_LOCAL and is denoted as FWR4.
When adding the following WIRED_SEPARATE_LOCAL ruleset, remember to also set and » SAVE the following:	=	When adding the following WIRED_SEPARATE_LOCAL ruleset, remember to also set and » SAVE the following:
Interface: eth2		Interface: eth2
Direction: local		Direction: local
name WIRED_SEPARATE_LOCAL {		name WIRED_SEPARATE_LOCAL {
default-action drop		default-action drop
description "Wired Separate Local"		description "Wired Separate Local"
rule 1 {		rule 1 {
action accept		action accept
description "Allow DHCP"		description "Allow DHCP"
destination {		destination {
port 67-68		port 67-68
}		}
log disable		log disable
protocol udp		protocol udp
}		}
rule 2 {		rule 2 {
action accept		action accept
description "Allow DNS"		description "Allow DNS"
destination {		destination {

```
                    port    53
                }
                log  disable
                protocol    tcp_udp
            }
        }
```

```
                    port    53
                }
                log  disable
                protocol    tcp_udp
            }
        }
```

Page 80 of 136 » 2/4/2019 58. EdgeMax Change Interface Names	<>	Page 88 of 157 » 5/18/2019 61. 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 the last one)	=	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 the last one)
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		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
Page 81 of 136 » 2/4/2019 59. SmartQueue Setup	<>	Page 89 of 157 » 5/18/2019 62. SmartQueue Setup
This section is optional. Turning on SmartQueue (on your WAN port) can help solve » the issue of “bufferbloat”. Reference the internet for “bufferbloat” if you are unfamiliar with it. Smart » Queue is a variety of Quality of Service	=	This section is optional. Turning on SmartQueue (on your WAN port) can help solve » the issue of “bufferbloat”. Reference the internet for “bufferbloat” if you are unfamiliar with it. Smart » Queue is a variety of Quality of Service
(QoS.) Enabling QoS may disable the hardware acceleration that was enabled in » section 32 - EdgeRouter Enable	<>	(QoS.) Enabling QoS may disable the hardware acceleration that was enabled in » section 34 - EdgeRouter Enable
HW NAT Assist. I think that if you only enable this on the WAN port, that HW » acceleration will stay enabled.	=	HW NAT Assist. I think that if you only enable this on the WAN port, that HW » acceleration will stay enabled.
	<>	One place to test connection speeds (and bufferbloat), to see if you should setup » QoS, is: http://www.dslreports.com/speedtest
To enable SmartQueue, press the QoS button, located near the top of the page. See		To enable SmartQueue, press the QoS button, located near the top of the page. See

» Figure 108 – QoS button.		» Figure 107 – QoS button.
	=	
Figure 108 – QoS button	<>	Figure 107 – QoS button
Ensure that the Smart Queue tab is selected, then press the “+ Add Smart Queue” » button.	=	Ensure that the Smart Queue tab is selected, then press the “+ Add Smart Queue” » button.
From what I understand, you should enter about 95% of you connection speeds into » the form. My connection speeds are 26 down and about 5 up. Adjust the values for your own connection speed » (s). There are also posting / indications that you should only implement SmartQueue in the Upload direction. One place to test connection speeds (and bufferbloat) is: http://www.dslreports.com/speedtest See Figure 109 – Example SmartQueue Settings	<>	From what I understand, you should enter about 90% to 95% of your real connection » speed(s) into the form. If you make a number too high, then QoS will not take effect, and you lose the benefi » t of having QOS. There are also posting / indications that you should only implement SmartQueue in the Upload » direction. My (example) connection speeds are 26 down and about 5 up, therefore I entered 4.5 Mbits/sec » for Upload. Choose a Policy name, like “Internet QoS”. Choose WAN Interface of eth0. Enter a 90%-adjusted-value for your own upload-connection-speed into the Upload » Rate box. Uncheck “Apply to download traffic”. Press Apply. See Figure 108 – Example SmartQueue Settings
	=	
Figure 109 – Example SmartQueue Settings	<>	Figure 108 – Example SmartQueue Settings
	=	
	-+	Page 90 of 157 » 5/18/2019
References: https://www.youtube.com/watch?v=3hvmzEv8iNQ http://kazoo.ga/edgerouter-x-smart-queue/ https://www.reddit.com/r/Ubiquiti/comments/5otj22/edgerouter_x_qos_question/ This is the end of the ER-X BASIC setup.	=	References: https://www.youtube.com/watch?v=3hvmzEv8iNQ http://kazoo.ga/edgerouter-x-smart-queue/ https://www.reddit.com/r/Ubiquiti/comments/5otj22/edgerouter_x_qos_question/ This is the end of the ER-X BASIC setup.
Page 82 of 136 » 2/4/2019 60. Ubiquiti AP-AC-LR Access Point Setup	<>	Page 91 of 157 » 5/18/2019 63. Ubiquiti AP-AC-LR Access Point Setup
This guide will utilize Access Point software installed on a Windows PC. This » software ONLY needs to be running WHEN you are adopting or making configuration changes to your Access Point(s). The » software does NOT need to be running all the time. Other Ubiquiti Access points should work; the Ubiquiti AP-AC-LR model is just the	=	This guide will utilize Access Point software installed on a Windows PC. This » software ONLY needs to be running WHEN you are adopting or making configuration changes to your Access Point(s). The » software does NOT need to be running all the time. Other Ubiquiti Access points should work; the Ubiquiti AP-AC-LR model is just the

» one that I purchased. There are also clients available for Linux, Macs, Android phones and Apple phones. There are optional guest portal / data-collection features that require this » software to be running all the time. These features might be found in a Motel/Hotel WiFi system. Some people choose to » therefore install and then continuously run this software on a Raspberry Pi. Ubiquiti has a Cloud Key device » that is recommended, if you are going to be running this software all the time. I have now purchased a Cloud-Key and played with it. Having this device saves the » hassle of installing the UniFi		» one that I purchased. There are also clients available for Linux, Macs, Android phones and Apple phones. There are optional guest portal / data-collection features that require this » software to be running all the time. These features might be found in a Motel/Hotel WiFi system. Some people choose to » therefore install and then continuously run this software on a Raspberry Pi. Ubiquiti has a Cloud Key device » that is recommended, if you are going to be running this software all the time. I have now purchased a Cloud-Key and played with it. Having this device saves the » hassle of installing the UniFi
(and Java) software on a PC. The configuration steps look the same / similar. » Pricing seems about $80. Reference: https://www.ubnt.com/unifi/unifi-cloud-key/	<>	(and insecure Java) software on a PC. The configuration steps look the same / » similar. Pricing seems about $80. If you can afford it, this is well worth the hassle of loading Java on your PC. » Running on a Raspberry Pi should be better than loading Java on a PC. Reference: » https://www.ubnt.com/unifi/unifi-cloud-key/
If you are going to re-purpose a consumer router as an access point, instead of » using an Ubiquiti Access Point, remember that some of the Network security is achieved via VLANS and Guest options » within the Access Point. Firewall rules within the EdgeRouter may need to be adjusted, probably additional » Guest Control Post-	=	If you are going to re-purpose a consumer router as an access point, instead of » using an Ubiquiti Access Point, remember that some of the Network security is achieved via VLANS and Guest options » within the Access Point. Firewall rules within the EdgeRouter may need to be adjusted, probably additional » Guest Control Post-
Authorization Restrictions. See near Figure 143 –Unifi Guest Control.	<>	Authorization Restrictions. See near Figure 142 –Unifi Guest Control.
	=	
61. Hookup the Ubiquiti AP-AC-LR Access Point	<>	64. Hookup the Ubiquiti AP-AC-LR Access Point
Using two standard Ethernet cables: Wire the EdgeRouter’s eth4 port to the LAN port of the included Power Over » Ethernet (POE) Adapter. Wire the POE port of the POE adapter to the Ethernet port on the Ubiquiti » AP-AC-LR Access Point.	=	Using two standard Ethernet cables: Wire the EdgeRouter’s eth4 port to the LAN port of the included Power Over » Ethernet (POE) Adapter. Wire the POE port of the POE adapter to the Ethernet port on the Ubiquiti » AP-AC-LR Access Point.
See Figure 110 – Access Point Wiring.	<>	See Figure 109 – Access Point Wiring.
Plug the POE adapter into your main electrical power. Note: Connecting the POE port of the POE adapter to any other device will probably » burn-up that other device. There are also internet posts that have the POE adapter powering both the ER-X and » the AP-AC-LR Access point. I am not powering my devices that way. Ubiquiti seems to be changing its Access » Point voltages / powering options.	=	Plug the POE adapter into your main electrical power. Note: Connecting the POE port of the POE adapter to any other device will probably » burn-up that other device. There are also internet posts that have the POE adapter powering both the ER-X and » the AP-AC-LR Access point. I am not powering my devices that way. Ubiquiti seems to be changing its Access » Point voltages / powering options.

Figure 110 – Access Point Wiring	<>	Figure 109 – Access Point Wiring
	=	
Page 83 of 136	<>	Page 92 of 157
» 2/4/2019		» 5/18/2019
62. Download and Install the Access Point Software		65. Download and Install the Access Point Software
For Windows users, you will need to be an Administrator, or the installation will	=	For Windows users, you will need to be an Administrator, or the installation will
» install (somewhere else) in the		» install (somewhere else) in the
area belonging to the admin’s account that was used.		area belonging to the admin’s account that was used.
Browse to:		Browse to:
https://www.ubnt.com/download/unifi/		https://www.ubnt.com/download/unifi/
Under the SOFTWARE section, download the NEWEST “Unifi Controller for Windows”		Under the SOFTWARE section, download the NEWEST “Unifi Controller for Windows”
» software (Unifi-		» software (Unifi-
installer.exe). When this guide was written, it was version 5.4.11.		installer.exe). When this guide was written, it was version 5.4.11.
Under the DOCUMENTATION section, you might also want to download:		Under the DOCUMENTATION section, you might also want to download:
UniFi Controller v5 Users Guide (or later version)		UniFi Controller v5 Users Guide (or later version)
UniFi AC-LR-AP Quick Start Guide.		UniFi AC-LR-AP Quick Start Guide.
The following install items may be slightly out of order between your installation		The following install items may be slightly out of order between your installation
» and that of this guide. I had to		» and that of this guide. I had to
re-start my UniFi Setup. You might also reference		re-start my UniFi Setup. You might also reference
» https://github.com/mjp66/Ubiquiti/issues/7		» https://github.com/mjp66/Ubiquiti/issues/7
Run the Unifi-installer.exe. Acknowledge any Windows admin prompts. See Figure 111	<>	Run the Unifi-installer.exe. Acknowledge any Windows admin prompts. See Figure 110
» – UniFi Setup Welcome		» – UniFi Setup Welcome
Screen.	=	Screen.
Figure 111 – UniFi Setup Welcome Screen	<>	Figure 110 – UniFi Setup Welcome Screen
	=	
If Java is not installed on your your PC, you will be prompted to install Java.	<>	If Java is not installed on your your PC, you will be prompted to install Java.
» See Figure 112 – UniFi Java Required.		» See Figure 111 – UniFi Java Required.
Click “OK”.	=	Click “OK”.
Figure 112 – UniFi Java Required	<>	Figure 111 – UniFi Java Required
	=	
Page 84 of 136	<>	Page 93 of 157
» 2/4/2019		» 5/18/2019
You will be taken to an Oracle site to download Java. Click on the “Free Java		You will be taken to an Oracle site to download Java. Click on the “Free Java
» Download” button. See Figure 113 –		» Download” button. See Figure 112 –
Unifi Download Oracle Java. Note that Oracle asks “Why download Java?” My only	=	Unifi Download Oracle Java. Note that Oracle asks “Why download Java?” My only
» answer is “Because I have to”.		» answer is “Because I have to”.
Figure 113 – Unifi Download Oracle Java	<>	Figure 112 – Unifi Download Oracle Java
	=	
While downloading, Oracle will inform you that their security holes are found		While downloading, Oracle will inform you that their security holes are found
» everywhere, and that you can		» everywhere, and that you can

experience that also. See Figure 114 – UniFi Downloading Oracle Java.	<>	experience that also. See Figure 113 – UniFi Downloading Oracle Java.
	=	
Figure 114 – UniFi Downloading Oracle Java	<>	Figure 113 – UniFi Downloading Oracle Java
	=	
Page 85 of 136 » 2/4/2019	<>	Page 94 of 157 » 5/18/2019
When done downloading, they will try and monetize you by setting up crapware. » Select “Do not update browser	=	When done downloading, they will try and monetize you by setting up crapware. » Select “Do not update browser
settings”, unless you like this type of stuff. See Figure 115 – UniFi Oracle » Crapware.	<>	settings”, unless you like this type of stuff. See Figure 114 – UniFi Oracle » Crapware.
	=	
Figure 115 – UniFi Oracle Crapware	<>	Figure 114 – UniFi Oracle Crapware
Run the downloaded JavaSetup*.exe executable. Java will install. Oracle will again » inform you that they are probably responsible for hundreds of billions of accumulated security holes, with » billions of them in internet	=	Run the downloaded JavaSetup*.exe executable. Java will install. Oracle will again » inform you that they are probably responsible for hundreds of billions of accumulated security holes, with » billions of them in internet
connected devices that will never be patched. See Figure 116 –UniFi Java » Installing. When Java is done installing you will see the dialog of See Figure 117 – UniFi » Java Done. Press “Close”. When the	<>	connected devices that will never be patched. See Figure 115 –UniFi Java » Installing. When Java is done installing you will see the dialog of See Figure 116 – UniFi » Java Done. Press “Close”. When the
next browser window opened (to verify Java is working), I closed that browser » verify page.	=	next browser window opened (to verify Java is working), I closed that browser » verify page.
Figure 116 –UniFi Java Installing Figure 117 – » UniFi Java Done	<>	Figure 115 –UniFi Java Installing Figure 116 – » UniFi Java Done
	=	
Page 86 of 136 » 2/4/2019	<>	Page 95 of 157 » 5/18/2019
Press the Windows Start button; Go to the list of programs, select Java, then » select “Configure Java”. Press the	=	Press the Windows Start button; Go to the list of programs, select Java, then » select “Configure Java”. Press the
“Security” tab, and UNCHECK the”Enable Java content in the browser” checkbox. See » Figure 118 – UniFi Java	<>	“Security” tab, and UNCHECK the”Enable Java content in the browser” checkbox. See » Figure 117 – UniFi Java
Control Panel. Without this you will be live-bait for any drive-by browsing » malware.	=	Control Panel. Without this you will be live-bait for any drive-by browsing » malware.
Figure 118 – UniFi Java Control Panel	<>	Figure 117 – UniFi Java Control Panel
	=	
Page 87 of 136 » 2/4/2019 I had to restart the UniFi installer. See Figure 119 – UniFi Installing.	<>	Page 96 of 157 » 5/18/2019 I had to restart the UniFi installer. See Figure 118 – UniFi Installing.
	=	

Figure 119 – UniFi Installing	<>	Figure 118 – UniFi Installing
	=	
The UniFi software will finish installing. See Figure 120 – UniFi Done Installing	<>	The UniFi software will finish installing. See Figure 119 – UniFi Done Installing
	=	
Figure 120 – UniFi Done Installing	<>	Figure 119 – UniFi Done Installing
	=	
Page 88 of 136 » 2/4/2019 63. Running the UniFi Software Double click the Unifi icon on your desktop. See Figure 121 – UniFi Icon	<>	Page 97 of 157 » 5/18/2019 66. Running the UniFi Software Double click the Unifi icon on your desktop. See Figure 120 – UniFi Icon
	=	
Figure 121 – UniFi Icon	<>	Figure 120 – UniFi Icon
	=	
The UniFi controlling software will start to initialize. See Figure 122 – UniFi » Controller Software Initializing.	<>	The UniFi controlling software will start to initialize. See Figure 121 – UniFi » Controller Software Initializing.
	=	
Figure 122 – UniFi Controller Software Initializing	<>	Figure 121 – UniFi Controller Software Initializing
	=	
When it has fully started, it will look like Figure 123 – UniFi Controller » Software Running.	<>	When it has fully started, it will look like Figure 122 – UniFi Controller » Software Running.
	=	
Figure 123 – UniFi Controller Software Running	<>	Figure 122 – UniFi Controller Software Running
	=	
Page 89 of 136 » 2/4/2019 When the UniFi Software started for the first time, a Windows Firewall dialog » popped up. See Figure 124 –	<>	Page 98 of 157 » 5/18/2019 When the UniFi Software started for the first time, a Windows Firewall dialog » popped up. See Figure 123 –
Windows Initial Firewall - UniFi.	=	Windows Initial Firewall - UniFi.
Figure 124 – Windows Initial Firewall - UniFi	<>	Figure 123 – Windows Initial Firewall - UniFi
The wording and default selections seem backwards to me. I reversed the selections » and pressed “Allow access”.	=	The wording and default selections seem backwards to me. I reversed the selections » and pressed “Allow access”.
See Figure 125 – Windows My Firewall Settings - UniFi.	<>	See Figure 124 – Windows My Firewall Settings - UniFi.
	=	
Figure 125 – Windows My Firewall Settings - » UniFi	<>	Figure 124 – Windows My Firewall Settings - » UniFi
QUESTION: Which settings are correct for keeping Java to only my local / private » network?	=	QUESTION: Which settings are correct for keeping Java to only my local / private » network?
Page 90 of 136	<>	Page 99 of 157

» 2/4/2019 64. Initial Setup of the UniFi Software		» 5/18/2019 67. Initial Setup of the UniFi Software
Either press the “Launch a Browser to Manage the Network” button or enter: https://localhost:8443/manage into your browser. Most of the following screenshots are portions of the full browser screen.	=	Either press the “Launch a Browser to Manage the Network” button or enter: https://localhost:8443/manage into your browser. Most of the following screenshots are portions of the full browser screen.
Select your country, time zone, and enable Auto Backup”, then press Next. See » Figure 126 – UniFi Setup Wizard.	<>	Select your country, time zone, and enable Auto Backup”, then press Next. See » Figure 125 – UniFi Setup Wizard.
	=	
Figure 126 – UniFi Setup Wizard	<>	Figure 125 – UniFi Setup Wizard
	=	
Your Ubiquiti Access Point should show up in the list. Check it and then press » Next. See Figure 127 – UniFi	<>	Your Ubiquiti Access Point should show up in the list. Check it and then press » Next. See Figure 126 – UniFi
Configure Devices.	=	Configure Devices.
Figure 127 – UniFi Configure Devices	<>	Figure 126 – UniFi Configure Devices
	=	
Page 91 of 136 » 2/4/2019 You will see the initial configure WiFi screen. See Figure 128 – UniFi Initial » Configure WiFi.	<>	Page 100 of 157 » 5/18/2019 You will see the initial configure WiFi screen. See Figure 127 – UniFi Initial » Configure WiFi.
	=	
Figure 128 – UniFi Initial Configure WiFi	<>	Figure 127 – UniFi Initial Configure WiFi
Fill in your main network’s SSID and your WiFi password. I used the name “HomeNet » “for this guide. This is the WiFi network that most of your computers, tablets, and cell phones will connect » to. Leave the Enable Guest	=	Fill in your main network’s SSID and your WiFi password. I used the name “HomeNet » “for this guide. This is the WiFi network that most of your computers, tablets, and cell phones will connect » to. Leave the Enable Guest
Network as UNCHECKED, and then press Next. See Figure 129 – UniFi Configure Wifi » SSID.	<>	Network as UNCHECKED, and then press Next. See Figure 128 – UniFi Configure Wifi » SSID.
	=	
Figure 129 – UniFi Configure Wifi SSID	<>	Figure 128 – UniFi Configure Wifi SSID
	=	
Page 92 of 136 » 2/4/2019	<>	Page 101 of 157 » 5/18/2019
To access this UniFi software later on, fill in the following information: Admin Name Admin Email Password You will want to write these down and/or put them in your password safe. The email » address is used for password	=	To access this UniFi software later on, fill in the following information: Admin Name Admin Email Password You will want to write these down and/or put them in your password safe. The email » address is used for password

recovery. When finished, press Next. See Figure 130 – UniFi Controller Access.	<>	recovery. When finished, press Next. See Figure 129 – UniFi Controller Access.
	=	
Figure 130 – UniFi Controller Access	<>	Figure 129 – UniFi Controller Access
	=	
Since I am not using Cloud Access, I pressed Skip. See Figure 131 – UniFi Cloud » Access.	<>	Since I am not using Cloud Access, I pressed Skip. See Figure 130 – UniFi Cloud » Access.
	=	
Figure 131 – UniFi Cloud Access	<>	Figure 130 – UniFi Cloud Access
	=	
Page 93 of 136 » 2/4/2019 You are then asked to confirm the above information. If it is correct, press » Finish. See Figure 132 – UniFi Confirm	<>	Page 102 of 157 » 5/18/2019 You are then asked to confirm the above information. If it is correct, press » Finish. See Figure 131 – UniFi Confirm
Setup.	=	Setup.
Figure 132 – UniFi Confirm Setup	<>	Figure 131 – UniFi Confirm Setup
	=	
65. Login to the UniFi Software You will be asked to login to the UniFi Software. See Figure 133 – UniFi Login. » Use your newly created credentials that were entered at Figure 130 – UniFi Controller Access.	<>	68. Login to the UniFi Software You will be asked to login to the UniFi Software. See Figure 132 – UniFi Login. » Use your newly created credentials that were entered at Figure 129 – UniFi Controller Access.
	=	
Figure 133 – UniFi Login	<>	Figure 132 – UniFi Login
	=	
Page 94 of 136 » 2/4/2019 You will land on the Dashboard page. See Figure 134 – Initial UniFi Dashboard Page	<>	Page 103 of 157 » 5/18/2019 You will land on the Dashboard page. See Figure 133 – Initial UniFi Dashboard Page
	=	
Figure 134 – Initial UniFi Dashboard Page	<>	Figure 133 – Initial UniFi Dashboard Page
	=	
From the upper left hand side choose Devices. See Figure 135 – UniFi Devices » Button.	<>	From the upper left hand side choose Devices. See Figure 134 – UniFi Devices » Button.
	=	
Figure 135 – UniFi Devices Button	<>	Figure 134 – UniFi Devices Button
	=	
Page 95 of 136 » 2/4/2019 66. UniFi Devices You will see the devices page, and the Access Point should be Pending Adoption. » See Figure 136 – Initial UniFi	<>	Page 104 of 157 » 5/18/2019 69. UniFi Devices You will see the devices page, and the Access Point should be Pending Adoption. » See Figure 135 – Initial UniFi
Device Screen. Note that this screenshot / figure was cut into two pieces and	=	Device Screen. Note that this screenshot / figure was cut into two pieces and

» folded into one image.		» folded into one image.
Figure 136 – Initial UniFi Device Screen	<>	Figure 135 – Initial UniFi Device Screen
	=	
Press the Upgrade button on the right side of the device line. Reference Figure 13	<>	Press the Upgrade button on the right side of the device line. Reference Figure 13
» 6 – Initial UniFi Device Screen.		» 5 – Initial UniFi Device Screen.
You will be presented with an upgrade confirmation dialog. Press Confirm. See		You will be presented with an upgrade confirmation dialog. Press Confirm. See
» Figure 137 – UniFi - Upgrade		» Figure 136 – UniFi - Upgrade
Access Point	=	Access Point
Figure 137 – UniFi - Upgrade Access Point	<>	Figure 136 – UniFi - Upgrade Access Point
	=	
You should see acknowledgement of the upgrade. See Figure 138 – UniFi – Upgrading.	<>	You should see acknowledgement of the upgrade. See Figure 137 – UniFi – Upgrading.
	=	
Figure 138 – UniFi – Upgrading Access Point	<>	Figure 137 – UniFi – Upgrading Access Point
	=	
When the upgrade is finished, press the Adopt button on the right side of the	<>	When the upgrade is finished, press the Adopt button on the right side of the
» device line. Reference Figure 136 –		» device line. Reference Figure 135 –
Initial UniFi Device Screen. You should see acknowledgement of the Adoption.		Initial UniFi Device Screen. You should see acknowledgement of the Adoption.
» SeeFigure 139 – UniFi – Adopting.		» SeeFigure 138 – UniFi – Adopting.
	=	
Figure 139 – UniFi – Adopting Access Point	<>	Figure 138 – UniFi – Adopting Access Point
	=	
Page 96 of 136	<>	Page 105 of 157
» 2/4/2019		» 5/18/2019
Your device should now say Connected. The buttons on the right now allow you to	=	Your device should now say Connected. The buttons on the right now allow you to
» locate, restart, and upgrade		» locate, restart, and upgrade
the Access Point. See Figure 140 – UniFi Access Point Connected. Note that this	<>	the Access Point. See Figure 139 – UniFi Access Point Connected. Note that this
» screenshot / figure was cut into		» screenshot / figure was cut into
two pieces and folded into one image.	=	two pieces and folded into one image.
Figure 140 – UniFi Access Point Connected	<>	Figure 139 – UniFi Access Point Connected
	=	
Find the Settings button, near the lower left side of the screen, and press it.	<>	Find the Settings button, near the lower left side of the screen, and press it.
» See Figure 141 – Settings Button		» See Figure 140 – Settings Button
	=	
Figure 141 – Settings Button	<>	Figure 140 – Settings Button
	=	
Page 97 of 136	<>	Page 106 of 157
» 2/4/2019		» 5/18/2019
67. UniFi Settings		70. UniFi Settings
You should see the Site Tab of the Settings page. Check Automatically Upgrade	=	You should see the Site Tab of the Settings page. Check Automatically Upgrade
» firmware, and then press Apply		» firmware, and then press Apply

Changes. See Figure 142 – UniFi Site Configuration.	<>	Changes. See Figure 141 – UniFi Site Configuration.
	=	
Figure 142 – UniFi Site Configuration	<>	Figure 141 – UniFi Site Configuration
	=	
Page 98 of 136 » 2/4/2019	<>	Page 107 of 157 » 5/18/2019
Click on the Guest Control tab. Under the Access Control section, add: 192.168.3.0/24	=	Click on the Guest Control tab. Under the Access Control section, add: 192.168.3.0/24
to Pre-Authorization Access, then press Apply Changes. See Figure 143 –Unifi Guest » Control. This will allow devices on the Wifi Guest Network to (respond to) communications » from the Home Network. Remember that the EdgeRouter has firewall rules prohibiting Guest network devices » from initiating communications with the Home Network. This allows Guest devices to RESPOND to Home » Network initiated conversations.	<>	to Pre-Authorization Access, then press Apply Changes. See Figure 142 –Unifi Guest » Control. This will allow devices on a Wifi Network designated as using “Guest Policy to » (respond to) communications from the Home Network. Remember that the EdgeRouter has firewall rules prohibiting » Guest network devices from directly initiating communications with the Home Network. This allows Guest » devices to RESPOND to Home Network initiated conversations.
	=	
Figure 143 –Unifi Guest Control	<>	Figure 142 –Unifi Guest Control
	=	
Click on the User Groups tab, and then press Create New User Group. See Figure 144 » – UniFi Initial User Groups.	<>	Click on the User Groups tab, and then press Create New User Group. See Figure 143 » – UniFi Initial User Groups.
	=	
Figure 144 – UniFi Initial User Groups	<>	Figure 143 – UniFi Initial User Groups
	=	
Page 99 of 136 » 2/4/2019	<>	Page 108 of 157 » 5/18/2019
The following settings allow the Access Point to limit the bandwidth used by users » within the guest networks. You may choose to enter different limit values and/or leave either or both of the » settings as unchecked. Unchecked is unlimited. The values used here are: download speed is limited to 10 Mbps upload speed is limited to 2 Mbps. I believe that the limits are per user, not per network. Reference: https://community.ubnt.com/t5/UniFi-Wireless/User-Group-Bandwidth-limit-group-or-u » ser/td-p/1828127 To use the values that are in this guide, complete the form as follows: Name GuestGroup Bandwidth Limit (Download) Checked 10000	=	The following settings allow the Access Point to limit the bandwidth used by users » within the guest networks. You may choose to enter different limit values and/or leave either or both of the » settings as unchecked. Unchecked is unlimited. The values used here are: download speed is limited to 10 Mbps upload speed is limited to 2 Mbps. I believe that the limits are per user, not per network. Reference: https://community.ubnt.com/t5/UniFi-Wireless/User-Group-Bandwidth-limit-group-or-u » ser/td-p/1828127 To use the values that are in this guide, complete the form as follows: Name GuestGroup Bandwidth Limit (Download) Checked 10000

Bandwidth Limit (Upload) Checked 2000		Bandwidth Limit (Upload) Checked 2000
then press Save. See Figure 145 – UniFi Guest Group	<>	then press Save. See Figure 144 – UniFi Guest Group
	=	
Figure 145 – UniFi Guest Group	<>	Figure 144 – UniFi Guest Group
	=	
You should now see the newly created group. See Figure 146 – UniFi New User » Groups.	<>	You should now see the newly created group. See Figure 145 – UniFi New User » Groups.
	=	
Figure 146 – UniFi New User Groups	<>	Figure 145 – UniFi New User Groups
	=	
Page 100 of 136 » 2/4/2019 Click on the Wireless Networks tab, you should see the Home Network that was setup » earlier. See Figure 147 –	<>	Page 109 of 157 » 5/18/2019 Click on the Wireless Networks tab, you should see the Home Network that was setup » earlier. See Figure 146 –
UniFi Wireless Network Setup. Click on Create New Wireless Network button	=	UniFi Wireless Network Setup. Click on Create New Wireless Network button
Figure 147 – UniFi Wireless Network Setup	<>	Figure 146 – UniFi Wireless Network Setup
	=	
Click on Create New Wireless Network button. You will be presented with the Create » New Wireless Network dialog. See Figure 148 – UniFi Create New Wireless Network.	<>	Click on Create New Wireless Network button. You may need to open up “Advanced » Options”. You will be presented with the Create New Wireless Network dialog. See Figure 147 – UniFi » Create New Wireless Network.
	=	
Figure 148 – UniFi Create New Wireless Network	<>	Figure 147 – UniFi Create New Wireless Network
	=	
Page 101 of 136 » 2/4/2019	<>	Page 110 of 157 » 5/18/2019
		Note that any wireless network which has checked the “Guest Policy” checkbox will » isolate ALL devices from every other device on that wireless network.
Note that some people do not apply the guest policies on the GuestWifi and/or IotW » ifi Networks, as they want individual WiFi devices on the Guest / IOT Networks to be able to access other » Guest / IOT WiFi devices, respectively. Newer versions of the UniFi software have an additional checkbox » “Multicast and Broadcast Filtering” (not shown), which also needs to be unchecked to enable the WiFi » clients to communicate with each		Many people do have (groups of) IOT devices which need to communicate with each ot » her to function. Examples are multiple Amazon devices, video cameras and their (storage) servers, etc… Newer » versions of the UniFi software have an additional checkbox “Multicast and Broadcast Filtering” (not » shown), which also needs to be unchecked to enable the WiFi clients to communicate with each other. See also » related sections: 83 - Multicast DNS and 81 - What devices should be placed on which Network?. Maybe a good compromise for security vs convenience is to:
other. If Guest Policy is not checked, you might need to add more firewall rules		Enable “Guest Policy” and Enable Broadcast Filtering for the Wi-Fi Guest Net

» to the ER-X, to maintain Network		» work and Disable “Guest Policy” and Disable Broadcast Filtering for the Wi-Fi IOT
		» Network.
security, probably equivalent to Guest Control Post-Authorization Restrictions. Se		You will need to choose these settings for yourself, based upon your own installed
» e Figure 143 –Unifi Guest		» IOT devices.
		In the following WiFi setups, I don’t know what to do with the “Multicast
		» Enhancement” checkbox. Mine is Un-
Control.		Checked, maybe because it was setup so long ago. Here are some References:
		https://help.ubnt.com/hc/en-us/articles/115001529267-UniFi-Managing-Broadcast-Traf
See also section 73 - Multicast DNS.		» fic
		https://community.ubnt.com/t5/airOS-Software-Configuration/quot-Multicast-Enhancem
		» ent-quot-checkbox/td-
You can change the Name/SSID, Security Key (i.e. password) and WPA Modes as suites		p/550452
» you.		
		https://community.ui.com/t5/UniFi-Wireless/Enable-multicast-enhancement-IGMPv3-fea
		» ture/td-p/2249142
Change / Enter the following information:		Page 111 of 157
		» 5/18/2019
		You can change the following settings as suites you. Change / Enter the following
		» information:
Name/SSID GuestWifi		Name/SSID GuestWifi
Security WPA Personal		Security WPA Personal
Security Key <Enter your own password for the guest wifi network >		Security Key <Enter your own password for the guest wifi network
		» >
Guest Policy CHECKED Apply guest policies		Guest Policy CHECKED Apply guest policies
		Multicast … Filtering CHECKED Block LAN to WLAN Multicast … Data
VLAN CHECKED VlanId 6		VLAN CHECKED Use VLAN 6
WPA Mode WPA2 Only Encryption AES/CCMP Only		WPA Mode WPA2 Only Encryption AES/CCMP Only
User Group GuestGroup		User Group GuestGroup
Press Save. See Figure 149 – UniFi Guest Wif.		Press Save. See Figure 148 – UniFi Guest Wif.
	=	
Figure 149 – UniFi Guest Wif	<>	Figure 148 – UniFi Guest Wif
	=	
Page 102 of 136	<>	Page 112 of 157
» 2/4/2019		» 5/18/2019
Click on Create New Wireless Network button.	=	Click on Create New Wireless Network button.

You can change the Name/SSID, Security Key (i.e. password) and WPA Modes as suites you.	<>	
Change / Enter the following information:		You can change the following settings as suites you. Change / Enter the following information:
Name/SSID IotWifi		Name/SSID IotWifi
Security WPA Personal		Security WPA Personal
Security Key <Enter your own password for the iot wifi network >		Security Key <Enter your own password for the iot wifi network >
Guest Policy CHECKED Apply guest policies		Guest Policy Un-Checked Apply guest policies
		Multicast … Filtering Un-Checked Block LAN to WLAN Multicast … Data
VLAN CHECKED VlanId 7		VLAN CHECKED Use VLAN 7
WPA Mode WPA2 Only Encryption AES/CCMP Only		WPA Mode WPA2 Only Encryption AES/CCMP Only
User Group GuestGroup		User Group Default
Press Save. SeeFigure 150 – UniFi Iot WiFi.		Press Save. SeeFigure 149 – UniFi Iot WiFi.
	=	
Figure 150 – UniFi Iot WiFi	<>	Figure 149 – UniFi Iot WiFi
	=	
Page 103 of 136	<>	Page 113 of 157
2/4/2019		5/18/2019
You should now have the following networks. Note that:	=	You should now have the following networks. Note that:
GuestWifi Checked as Guest Vlan 6	<>	GuestWifi Checked as Guest VLAN 6
HomeNet (Unchecked Guest) (no Vlan)		HomeNet (Unchecked Guest) (no VLAN)
IotWifi Checked as Guest Vlan 7		IotWifi (Unchecked Guest) VLAN 7
See Figure 151 – UniFi Three WiFi Networks.		See Figure 150 – UniFi Three WiFi Networks.
	=	
Figure 151 – UniFi Three WiFi Networks	<>	Figure 150 – UniFi Three WiFi Networks
	=	
	-+	If you want to implement another “Spare” WiFi network, you would do that now, following the above steps, but instead specifying: VLAN CHECKED Use VLAN 8.
Click on the DPI tab, and set:	=	Click on the DPI tab, and set:
Enable Deep Packet Inspection (DPI) On		Enable Deep Packet Inspection (DPI) On
Press Apply Changes. See Figure 152 – UniFi Deep Packet Inspection	<>	Press Apply Changes. See Figure 151 – UniFi Deep Packet Inspection
	=	
Figure 152 – UniFi Deep Packet Inspection	<>	Figure 151 – UniFi Deep Packet Inspection
	=	
Page 104 of 136	<>	Page 114 of 157
2/4/2019		5/18/2019
Return to the Dashboard screen by pressing the Dashboard button. See Figure 153 – UniFi Dashboard Button.		Return to the Dashboard screen by pressing the Dashboard button. See Figure 152 – UniFi Dashboard Button.

	=	
Figure 153 – UniFi Dashboard Button	<>	Figure 152 – UniFi Dashboard Button
	=	
In the upper right part of the dashboard screen is the Open Properties button.	<>	In the upper right part of the dashboard screen is the Open Properties button.
» Press the button. See Figure 154 –		» Press the button. See Figure 153 –
UniFi Open Properties Button	=	UniFi Open Properties Button
Figure 154 – UniFi Open Properties Button	<>	Figure 153 – UniFi Open Properties Button
	=	
These are the Properties of the access point. There are some nice settings in	<>	These are the Properties of the access point. There are some nice settings in
» here. See Figure 155 – UniFi Access		» here. See Figure 154 – UniFi Access
Point Properties.	=	Point Properties.
Figure 155 – UniFi Access Point Properties.	<>	Figure 154 – UniFi Access Point Properties.
	=	
Page 105 of 136	<>	Page 115 of 157
» 2/4/2019		» 5/18/2019
68. UniFi Configuration Backup		71. UniFi Configuration Backup
Find the Settings button, near the lower left side of the screen, and press it.		Find the Settings button, near the lower left side of the screen, and press it.
» See Figure 141 – Settings Button.		» See Figure 140 – Settings Button.
You should see the Maintenance Tab of the Settings page. Press it. Reference		You should see the Maintenance Tab of the Settings page. Press it. Reference
» Figure 156 – UniFi Maintenance		» Figure 155 – UniFi Maintenance
Screen.	=	Screen.
Figure 156 – UniFi Maintenance Screen	<>	Figure 155 – UniFi Maintenance Screen
	=	
In the middle of this screen is a BACKUP section. I have changed my backup setting		In the middle of this screen is a BACKUP section. I have changed my backup setting
» to be ‘Settings only’.		» to be ‘Settings only’.
Press the ‘DOWNLOAD BACKUP’ button and store the resultant file. This is your		Press the ‘DOWNLOAD BACKUP’ button and store the resultant file. This is your
» access point configuration		» access point configuration
backup.		backup.
You can now exit the UniFi browser and close the UniFi Controller Software by		You can now exit the UniFi browser and close the UniFi Controller Software by
» pressing the X in the upper-right		» pressing the X in the upper-right
corner, as shown in Figure 123 – UniFi Controller Software Running.	<>	corner, as shown in Figure 122 – UniFi Controller Software Running.
		Page 116 of 157
		» 5/18/2019
		Links:
		UniFi - Methods for Capturing Useful Debug Information
		https://help.ubnt.com/hc/en-us/articles/227129127
This is the end of the Access Point / UniFi setup.	=	This is the end of the Access Point / UniFi setup.
The following sections are additional EdgeRouter configuration steps.		The following sections are additional EdgeRouter configuration steps.
Page 106 of 136	<>	Page 117 of 157
» 2/4/2019		» 5/18/2019

69. Timed Based Firewall Rules		72. Timed Based Firewall Rules
Several people have wanted to restrict their children's Internet usage based upon » time. Here are some sample links: https://community.ubnt.com/t5/EdgeMAX/Restrict-WAN-Access-to-from-LAN-Clients-by-S » pecific-IP-By-Time/td-p/2083140 https://community.ubnt.com/t5/UniFi-Wireless/User-based-time-control-of-wifi-acces » s/td-p/1490803 https://community.ubnt.com/t5/EdgeMAX/Time-control-parental-controll/td-p/1035259 https://community.ubnt.com/t5/EdgeMAX/Set-up-time-limits-for-kids-internet-access/ » td-p/1824135 https://community.ubnt.com/t5/EdgeMAX/Parental-controls-time-of-day-routing-conten » t-filtering/td-p/1268520	=	Several people have wanted to restrict their children's Internet usage based upon » time. Here are some sample links: https://community.ubnt.com/t5/EdgeMAX/Restrict-WAN-Access-to-from-LAN-Clients-by-S » pecific-IP-By-Time/td-p/2083140 https://community.ubnt.com/t5/UniFi-Wireless/User-based-time-control-of-wifi-acces » s/td-p/1490803 https://community.ubnt.com/t5/EdgeMAX/Time-control-parental-controll/td-p/1035259 https://community.ubnt.com/t5/EdgeMAX/Set-up-time-limits-for-kids-internet-access/ » td-p/1824135 https://community.ubnt.com/t5/EdgeMAX/Parental-controls-time-of-day-routing-conten » t-filtering/td-p/1268520
70. Double-NAT	<>	73. Double-NAT
When one firewall/router is behind another firewall/router, that combination is » called double-NAT. Each router	=	When one firewall/router is behind another firewall/router, that combination is » called double-NAT. Each router
performs Network-Address-Translation (NAT.) Each router will introduce a small » time delay as it processes IP	<>	performs Network-Address-Translation (NAT.) Each router will introduce a small » time delay as it processes IP
packets. If you are running a server behind your (inner) router, then Double NAT » can be particularly difficult to configure. Most people in the Ubiquiti forums hate Double-NAT.	=	packets. If you are running a server behind your (inner) router, then Double NAT » can be particularly difficult to configure. Most people in the Ubiquiti forums hate Double-NAT.
Once the EdgeRouter 's firewall has been enabled / configured, the EdgeRouter CAN » (but does not have to) be	<>	Once the EdgeRouter 's firewall has been enabled / configured, the EdgeRouter can » (but does not have to) be
your main and only router. Remember to replace and then remove the default 'ubnt' » login before using the ER-X as your internet facing router.	=	your main and only router. Remember to replace and then remove the default 'ubnt' » login before using the ER-X as your internet facing router.
71. Configuring a Second / Testing ER-X	<>	74. Configuring a Second / Testing ER-X
It is handy to have a second, already-configured, ER-X on hand as a cold spare. If » you are considering using	=	It is handy to have a second, already-configured, ER-X on hand as a cold spare. If » you are considering using
"Adblocking and Blacklisting" from section 75, you could configure one ER-X with a » nd one ER-X without Adblocking. Testing that feature is now as easy as the five minutes it takes to » swap routers.	<>	"Adblocking and Blacklisting" from section 77, you could configure one ER-X with A » dblocking and one ER-X without Adblocking. Testing that feature is now as easy as the five minutes it » takes to swap routers.
To configure a Second/ Testing ER-X, it is important that the IP address presented » to the WAN port NOT be within	=	To configure a Second/ Testing ER-X, it is important that the IP address presented » to the WAN port NOT be within
one of our internal IP address ranges. Reference section 4 - EdgeRouter IP Address » Use and Table 1 - Table of	<>	one of our internal IP address ranges. Reference section 5 - EdgeRouter IP Address » Use and Table 1 - Table of
Networks for that data.	=	Networks for that data.
	<>	Normally your Setup/Testing PC would be wired directly (or through a switch) to

		» your “Master” ER-X. See Figure 156 – Typical Testing PC Setup.
		Figure 156 – Typical Testing PC Setup
		Page 118 of 157
		» 5/18/2019
One way of presenting a different IP address to the Second / Testing ER-X, is to		One way of presenting a different IP address to the Second/Testing ER-X, is to
» insert your leftover consumer		» insert your leftover consumer
router (with its LAN configured for 192.168.[0,1,2].X) before your Second /		router (with its LAN configured for 192.168.[0,1,2].X) before your Second /
» Testing ER-X router.		» Testing ER-X router. The Testing ER-X
See Figure 157 – Second / Testing ER-X Wiring.		then connects to you Setup/Testing PC. See Figure 157 – Second / Testing ER-X
		» Wiring.
	=	
Figure 157 – Second / Testing ER-X Wiring	<>	Figure 157 – Second / Testing ER-X Wiring
	=	
Page 107 of 136	<>	
» 2/4/2019		
72. Another link		
This seems like a wealth of information:		
http://wiki.indie-it.com/wiki/Ubiquiti		
		75. Ubnt Discovery
Page 108 of 136		
» 2/4/2019		
73. Multicast DNS		
The use of MDNS between Networks, was suggested in		
» https://github.com/mjp66/Ubiquiti/issues/29 with a link		
of: https://www.youtube.com/watch?v=1mjdkki2pIY		
I believe MDNS allows device discovery between two or more Networks by merging the		
» Networks’ broadcast		
traffic. I don’t know what security implications this merging might have. I have		
» tried enabling MDNS within the ER-		
X, but have not fully investigated it. MDNS can be enabled via the CLI or via the		
» Config Tree. To enable via the		
Config Tree, open up the service -> mdns -> repeater sub-menus. Enter in your inte		Recently,the Ubnt Discovery service has shown up in an EdgeRouter Community postin
» rfaces, and then click Preview.		» g:
See Figure 158 – MDNS Setup Example.		https://community.ubnt.com/t5/EdgeRouter/EdgeOS-responds-to-udp-10001-probes-even-
		» if-service-ubnt/td-
		p/1886105
Figure 158 – MDNS Setup Example.		
		“The default WAN firewall policies added by the Basic Setup wizard will block all
		» probes to UDP/TCP port 10001

While trying to determine the impact of mdns, I had trouble disabling this feature » via the Config Tree, so I used the following commands via the command line interface to disable this service. configure delete service mdns repeater commit save exit It appears that enabling Multicast DNS is also available within the UniFi (Access » Point) system. Reference the following link: https://community.ubnt.com/t5/UniFi-Routing-Switching/USG-and-Chromecast-across-su » bnets-VLANs-Multicast-or-mDNS/td-p/1782140 Within that article is the following post: https://community.ubnt.com/t5/UniFi-Routing-Switching/USG-and-Chromecast-across-su » bnets-VLANs-Multicast-or-mDNS/m-p/2016844/highlight/true#M53023 More investigation is needed. Page 109 of 136 » 2/4/2019 See also the following posts: https://community.ubnt.com/t5/EdgeRouter/mDNS-bonjour-forwarding/td-p/414093/ https://community.ubnt.com/t5/EdgeRouter/mDNS-forwarding-so-that-iPhone-can-commun » icate-with-iTunes-on-a/m-p/1752138/ https://community.ubnt.com/t5/EdgeRouter/Multicast-Sonos-Phorus-amp-Play-Fi-Broadc » ast-255-255-255-255-lt/td-p/1259616		and will prevent the EdgeRouter from being discoverable on the WAN.” Per https://help.ubnt.com/hc/en-us/articles/204976244 If you still want to disable this service, the following may help you: [UBNT-discover] - Add CLI command to disable "ubnt-discovery" daemon, thus ER will » stop responding to discovery messages on 10001 UDP port. (set service ubnt-discover-server disable). Reference https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-so » ftware-release-v1-10-0/ba-p/2233263 [Discovery] - UBNT discovery daemon can be configured to listen to TCP discovery » requests (by default it listens to UDP only). This feature can be enbled with "set service ubnt-discover-server » protocol tcp_udp" CLI command. https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-software-rel » ease-v1-10-7/ba-p/2513718
	=	
Page 110 of 136 » 2/4/2019 74. Reserving Device Addresses via DHCP	<>	Page 119 of 157 » 5/18/2019 76. Reserving Device Addresses via DHCP

When you have the ER-X reserve a DHCP address for a device, that device will » always be presented with the same IP address. This is useful for devices like servers. This is different than » “fixing” a device’s IP. Fixing usually involves configuring the device itself, to use a certain IP address. Reserving addresses » has the added benefit that the rest of the DHCP settings continue to be presented to the device. Static mapping is » another term for reserving. Ensure your device is powered on and connected to the Network you wish. To reserve an IP address, select the “Services” button. Reference Figure 51 – » Services Button. Ensure that the “DHCP Server” tab is selected. Reference Figure 52 – DHCP Server Screen. Find the » correct DHCP line for your Network, follow it to the right side, to the line’s “Actions” button. Click the » “Actions” button. You will be	=	When you have the ER-X reserve a DHCP address for a device, that device will » always be presented with the same IP address. This is useful for devices like servers. This is different than » “fixing” a device’s IP. Fixing usually involves configuring the device itself, to use a certain IP address. Reserving addresses » has the added benefit that the rest of the DHCP settings continue to be presented to the device. Static mapping is » another term for reserving. Ensure your device is powered on and connected to the Network you wish. To reserve an IP address, select the “Services” button. Reference Figure 51 – » Services Button. Ensure that the “DHCP Server” tab is selected. Reference Figure 52 – DHCP Server Screen. Find the » correct DHCP line for your Network, follow it to the right side, to the line’s “Actions” button. Click the » “Actions” button. You will be
presented with a list of actions. Choose “View Leases”, See Figure 159 – View » Leases Button.	<>	presented with a list of actions. Choose “View Leases”, See Figure 158 – View » Leases Button.
	=	
Figure 159 – View Leases Button.	<>	Figure 158 – View Leases Button.
You will be presented with a DHCP Server Dialog. This dialog will contain a list » of your devices which have acquired	=	You will be presented with a DHCP Server Dialog. This dialog will contain a list » of your devices which have acquired
a dynamic DHCP lease. See Figure 160 – DHCP Server Leases Dialog.	<>	a dynamic DHCP lease. See Figure 159 – DHCP Server Leases Dialog.
	=	
Figure 160 – DHCP Server Leases Dialog.	<>	Figure 159 – DHCP Server Leases Dialog.
	=	
Page 111 of 136 » 2/4/2019	<>	Page 120 of 157 » 5/18/2019
To reserve an IP address for that device, Press the “Map Static IP” button near » the right side of the screen, for the	=	To reserve an IP address for that device, Press the “Map Static IP” button near » the right side of the screen, for the
correct device. You will be presented Figure 161 – Static IP Mapping Dialog.	<>	correct device. You will be presented Figure 160 – Static IP Mapping Dialog.
	=	
Figure 161 – Static IP Mapping Dialog.	<>	Figure 160 – Static IP Mapping Dialog.
You can modify the IP address to a different one or just leave it. If you modify » it, only change the last octet (the last number.) Press “Save”, then close the DHCP Server Leases dialog. If you » modified the presented IP address, you will need to “release” and “renew” the devices IP address and/or reboot that » device now. To view static IP	=	You can modify the IP address to a different one or just leave it. If you modify » it, only change the last octet (the last number.) Press “Save”, then close the DHCP Server Leases dialog. If you » modified the presented IP address, you will need to “release” and “renew” the devices IP address and/or reboot that » device now. To view static IP

reservations, find the Actions button, and click the “Configure Static Map” » button. See Figure 162 – Configure	<>	reservations, find the Actions button, and click the “Configure Static Map” » button. See Figure 161 – Configure
Static Map Button.	=	Static Map Button.
Figure 162 – Configure Static Map Button.	<>	Figure 161 – Configure Static Map Button.
	=	
You will be presented with a list of reserved IP addresses for the chosen DHCP » server. See Figure 163 – Static IP	<>	You will be presented with a list of reserved IP addresses for the chosen DHCP » server. See Figure 162 – Static IP
Mapping Dialog.	=	Mapping Dialog.
Figure 163 – Static IP Mapping Dialog.	<>	Figure 162 – Static IP Mapping Dialog.
	=	
Page 112 of 136 » 2/4/2019 75. Adblocking and Blacklisting This is optional. This seems to work flawlessly.	<>	Page 121 of 157 » 5/18/2019 77. Adblocking and Blacklisting This is optional. This seems to work flawlessly. Also reference section 78 - » Pi-Hole Network-wide Ad Blocking.
You should note before implementing this section that some web sites / web pages » you may wish to visit will be blocked by this code. In some cases you may not be able to determine which URLs in » the blocking lists are blocking which sites / page you want to visit, as some website links ‘redirect’ » through advertisers’ sites. These advertisers’ sites will now be blocked. There are a number of similar posts with different version numbers. I had to use » an SSH package (e.g. putty for Windows) to paste the following commands into the EdgeRouter, as the CLI doesn’t » seem to support copy / paste. Reference: » https://community.ubnt.com/t5/EdgeMAX/DNS-Adblocking-amp-Blacklisting-dnsmasq-Configuration/td-p/2215008	=	You should note before implementing this section that some web sites / web pages » you may wish to visit will be blocked by this code. In some cases you may not be able to determine which URLs in » the blocking lists are blocking which sites / page you want to visit, as some website links ‘redirect’ » through advertisers’ sites. These advertisers’ sites will now be blocked. There are a number of similar posts with different version numbers. I had to use » an SSH package (e.g. putty for Windows) to paste the following commands into the EdgeRouter, as the CLI doesn’t » seem to support copy / paste. Reference: » https://community.ubnt.com/t5/EdgeMAX/DNS-Adblocking-amp-Blacklisting-dnsmasq-Configuration/td-p/2215008
	<>	See also: https://github.com/britannic/blacklist
The following text is cached from the above URL when the code was at V1.1.6.3 (you » should check for updated information and use the newest code and any newer directions :)	<>	The following text is cached from the above URL when the stated version was at » V1.1.7.4. You should check for updated information and use the newest code and any newer » directions.
First ensure the router has enough space (2 lines):	=	First ensure the router has enough space (2 lines):
sudo apt-get clean cache delete system image	<>	sudo apt-get clean cache delete system image
Installation (2 lines):	=	Installation (2 lines):
	<>	curl -L -O https://raw.githubusercontent.com/britannic/blacklist/master/edgeos-
curl -L -O		

» https://raw.githubusercontent.com/britannic/blacklist/master/edgeos-dnsmasq-blacklist_1.1.6.3_mipsel.deb sudo dpkg -i edgeos-dnsmasq-blacklist_1.1.6.3_mipsel.deb Removal (1 line): sudo apt-get remove --purge edgeos-dnsmasq-blacklist		dnsmasq-blacklist_1.1.7.4_mipsel.deb sudo dpkg -i edgeos-dnsmasq-blacklist_1.1.7.4_mipsel.deb Removal, if ever wanted (1 line): sudo apt-get remove --purge edgeos-dnsmasq-blacklist
Upgrade: Since dpkg cannot upgrade packages, follow the instructions under » Installation and the previous package version will be automatically removed before the new package version is » installed There is much more listed at this post.	=	Upgrade: Since dpkg cannot upgrade packages, follow the instructions under » Installation and the previous package version will be automatically removed before the new package version is » installed There is much more listed at this post.
When I installed this, I saw the following line: Total entries extracted 98158. An associated (similar) posting is at: https://github.com/britannic/blacklist	<>	When I installed this, I saw the following lines: Total entries found: 99770 Total entries extracted 81838 Total entries dropped 17932 Some more links: https://britannic.github.io/blacklist/#frequently-asked-questions https://github.com/britannic/blacklist/blob/master/CHANGELOG.md https://britannic.github.io/blacklist/#frequently-asked-questions
There is also an associated project located at: » https://github.com/britannic/pixelserv (which I have not tried.)	=	There is also an associated project located at: » https://github.com/britannic/pixelserv (which I have not tried.)
Page 113 of 136 » 2/4/2019	<>	Page 122 of 157 » 5/18/2019
Reference the following from his post: dnsmasq may need to be configured to ensure blacklisting works correctly Here is an example using the EdgeOS configuration shell configure set service dns forwarding cache-size 2048 set service dns forwarding except-interface [Your WAN i/f] set service dns forwarding name-server [Your choice of IPv4 » Internet Name- Server] set service dns forwarding name-server [Your choice of IPv4 » Internet Name- Server] set service dns forwarding name-server [Your choice of IPv6 » Internet Name- Server] set service dns forwarding name-server [Your choice of IPv6 » Internet Name-	=	Reference the following from his post: dnsmasq may need to be configured to ensure blacklisting works correctly Here is an example using the EdgeOS configuration shell configure set service dns forwarding cache-size 2048 set service dns forwarding except-interface [Your WAN i/f] set service dns forwarding name-server [Your choice of IPv4 » Internet Name- Server] set service dns forwarding name-server [Your choice of IPv4 » Internet Name- Server] set service dns forwarding name-server [Your choice of IPv6 » Internet Name- Server] set service dns forwarding name-server [Your choice of IPv6 » Internet Name-

```
      Server]
      set  service  dns  forwarding       options   bogus-priv
      set  service  dns  forwarding       options   domain-needed
      set  service  dns  forwarding       options   domain=mydomain.local
      set  service  dns  forwarding       options   enable-ra
      set  service  dns  forwarding       options   expand-hosts
      set  service  dns  forwarding       options   localise-queries
      set  service  dns  forwarding       options   strict-order
      set  service  dns  forwarding       system
      set  system  name-server        127.0.0.1
      set  system  name-server        '::1'
      commit;  save;   exit
For testing, I picked a well-known advertisement site owned by Google. I tried and
» couldn’t get there.
Thanks to @britannic for this.
Also reference https://github.com/britannic/blacklist#frequently-asked-questions
» especially the section titled
“EdgeOS dnsmasq Configuration”. This appears to be the same text as above.
```


<>


```
78.  Pi-Hole Network-wide Ad Blocking
I have not tried this. Looks interesting. Also Reference section 77 - Adblocking
» and Blacklisting.
Reference:
      https://pi-hole.net/
Ubiquiti Links (see also the entire threads, if needed):
https://community.ubnt.com/t5/EdgeRouter/Intercepting-and-Re-Directing-DNS-Queries
» /td-p/1554378/page/2
https://community.ubnt.com/t5/EdgeRouter/Redirect-Hard-Coded-DNS-w-EdgeRouter/m-p/
» 2354331#M208753
Above links are from:
» https://community.ubnt.com/t5/EdgeRouter/Redirect-DNS-to-Pi-hole/m-
p/2389150/highlight/true#M212068
Other Links:
https://community.ubnt.com/t5/EdgeRouter/Redirect-DNS-to-Pi-hole/m-p/2718992
https://community.ubnt.com/t5/EdgeRouter/Please-help-me-work-out-how-to-set-up-DNS
» -details-inside/m-
p/2745497
https://community.ubnt.com/t5/EdgeRouter/config-for-an-internal-DNS-server-pihole-
» works-but-client/m-
```

p/2669894
https://community.ubnt.com/t5/EdgeRouter/ER-X-Pi-Hole-and-cross-interface-communic
» ation/m-p/2517626\
https://community.ubnt.com/t5/EdgeRouter/Forcing-DNS-to-PiHole-w-DNAT-Allowing-for
» -Backup-DNS-server/td-
p/2458039

79. Coalescing the Wired Iot and Wifi Iot Networks
This optional section allows the coalescence of the Wired Iot and Wifi Iot
» Networks. This involves enabling switch0
to be VLAN Aware. When configuring switch0 to be VLAN Aware, it is important to
» NOT be connected to an
EdgeRouter port which is using switch0. I used the Wired Separate Network (which
» is not in switch0, if you
followed previous sections) for these re-configuration steps. I locked myself out
» of my ER-X EdgeRouter (and had
to factory reset / reload the base configuration) about 4 times while researching
» and writing this section. You
should generate a backup, right now, if you are going to implement this.
I have now converted my ER-X to being VLAN Aware.
Login to EdgeRouter
The following (temporarily) allows the Wired Separate Network to access the
» EdgeRouter itself.
Firewall/NAT
Firewall Policies
WIRED_SEPARATE_LOCAL -> Actions -> Configuration
Default Action: Accept
Save Ruleset
Disconnect your computer's Ethernet cable from eth3 / Home Network. Wait 5 to
» 10 seconds. Re-connect your
computer's Ethernet cable to eth2 / Wired Separate Network.
Open a new Browser window/tab and enter a URL of 192.168.5.1 and Login to the
» EdgeRouter
Now we are connected to the EdgeRouter without using switch0.
Move the Home Network Address setup from switch0 to vid 1.
Dashboard
Home Net switch0 -> Actions -> Config
Config Tab
Address: No address

```
                    Save
    Dashboard
         Add  Interface
              Add     VLAN
                      VLANID:           1
                      Interface:        switch0
                      Description:      Home     Net
                      MTU:              1500
                      Address:          Manually      define    IP       Address
                                        192.168.3.1/24
                      Save
Remove the address range from Wired Iot Network.
    Dashboard
         Wired      Iot Net  / eth1  ->  Actions      ->    Config
              Address:             No  address
              Save
    Page 125 of 157
» 5/18/2019
Remove firewall rules from Wired Iot Network.
    Firewall/NAT
         Firewall    Policies
                   WIRED_IOT_LOCAL          ->  Actions  ->  Edit   Ruleset
                        Rules      Tab
                                Rule   2->  Action    -> Delete    Rule,    Yes
                                Rule   1->  Action    -> Delete    Rule,    Yes
                        Interfaces        Tab
                                Set  Interface     --
                                Set  Direction     -
                                -Remove
                                Save   Ruleset
                   WIRED_IOT_LOCAL          ->  Actions  ->  Delete   Ruleset,
» Yes
Delete the Wired Iot Network DHCP server.
    Services
         DHCP  Server
              WiredIotDHCP
                   Actions       Delete
                   Yes
Move Home Network firewall rules from switch0 to vid 1
    Firewall/NAT
```

```
        Firewall    Policies
             HOME_OUT    Actions        ->   Interfaces
                  Interfaces:       switch0.1
                  Save  Ruleset
Enable switch0 to be Vlan Aware.
Note: If the dialog gets stuck, click the Config Tab, then click the Vlan tab to
» refresh the dialog / size.
Note that you could optionally add “eth3  vid  6,7” if you have multiple Access
» Points AND will be wiring them
through a smart Ethernet switch connected to eth3.
    Dashboard
         Switch0    Config
              Vlan
                   Vlan  Aware      Enabled      checked
                   eth0  UNCHECKED
                   eth1  checked
                   eth1  pvid      7
                   eth2  UNCHECKED
                   eth3  checked
                   eth3  pvid      1
                   eth4  checked
                   eth4  pvid      1
                   eth4  vid      6,7
                   Save
Disconnect your computer's Ethernet cable from eth2 / Wired Separate Network. Wait
» 5 to 10 seconds.
Re-connect your computer's Ethernet cable to eth3 / Home Network. Open a new
» Browser window/tab and enter
a URL of 192.168.3.1 and Login to the EdgeRouter
   Page 126 of 157
» 5/18/2019
The following restores the Wired Separate Network firewall restrictions.
    Firewall/NAT
            Firewall  Policies
                WIRED_SEPARATE_LOCAL         ->  Actions   -> Configuration
                     Default    Action:     Drop
                     Save   Ruleset
You may want to rename the “Wifi Iot” / “Wired Iot” items to simply be “Iot”
» items.
At this point, I suggest that you backup your new config. Maybe rename it with
```

» _VlanAware in the name.
References:
https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch
https://github.com/mjp66/Ubiquiti/issues/5
https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-Inter-VLAN-routing-issues-Ho
» w-I-solved-it/td-
p/1813187
https://help.ubnt.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRout
» er-as-a-Layer-2-Switch
https://community.ubnt.com/t5/EdgeRouter/Setting-VLAN-s-with-ERX-broke-it-complete
» ly/td-p/1917708
https://community.ubnt.com/t5/EdgeRouter/Edge-Router-X-as-Switch-with-VLAN-Need-He
» lp/td-p/1992908
https://community.ubnt.com/t5/EdgeRouter/How-to-configure-EdgeRouter-X-as-switch-r
» eposted-at-differnt/m-
p/2635039/highlight/true
https://community.ubnt.com/t5/EdgeRouter/Edge-router-X-SFP-VLAN-s/td-p/1971128
https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch
https://community.ubnt.com/t5/EdgeRouter/riddle-me-this-ER-X-how-do-I-set-a-native
» -VLAN-on-the-switch/m-
p/2667164/highlight/true
https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-VLAN-config-for-switch0-with
» -LAN-and-VLAN-on-
same/m-p/2666616/highlight/true
https://community.ubnt.com/t5/EdgeRouter/locked-out-of-edgerouter-after-vlan-confi
» g/m-p/2557366
Page 127 of 157
» 5/18/2019
Differences between being VLAN Aware and NOT being VLAN Aware:
https://community.ubnt.com/t5/EdgeRouter/riddle-me-this-ER-X-how-do-I-set-a-native
» -VLAN-on-the-switch/m-
p/2667164/highlight/true#M240023
https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-VLAN-config-for-switch0-with
» -LAN-and-VLAN-on-
same/m-p/2666758/highlight/true#M239994
There are additional interesting links within the second URL by @BuckeyeNet.
https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-VLAN-config-for-switch0-with
» -LAN-and-VLAN-on-
same/m-p/2666758/highlight/true
There is also a discussion at https://github.com/mjp66/Ubiquiti/issues/35

		This posting performs similar actions, but all from the CLI interface: https://community.ubnt.com/t5/EdgeRouter/ERX-Unifi-VLAN-Guest-Portal/m-p/2755024/highlight/true#M249244 Page 128 of 157 » 5/18/2019 80. Simple Network Management Protocol (SNMP) To enable the ER-X to be a source of SNMP data, first press the “System” button. » Reference Figure 9 – System Button. Find the SNMP Agent section, fill-in the three fields, and check Enable. » Press “Save”. See Figure 163 – Sample SNMP configuration. The ER-X appears to support both version 1 and version2(c). Version 2 supports 64 » bit counters. The only security available is to change the SNMP community string to something hard to guess. Most » installations assume “public”. Figure 163 – Sample SNMP configuration. There is a huge list of SNMP programs which could monitor you router. Some I have » seen referenced are: Snmpwalk (Referenced in Appendix C) Cacti NetworX / LibreNMS / PRTG Nagips / Zabbix / Dude OpenNMS MRTG Grafana / InfluxDB / Telegraf (See Appendix C) Page 129 of 157 » 5/18/2019
76. What devices should be placed on which Network?		81. What devices should be placed on which Network?
Some devices could go either on the Home Network or on the Iot Network. I'll use an Amazon Echo as the first example. The echo can execute just fine from » the Iot Network. The echo typically uses a smart phone app to control it. Since Amazon's phone app doesn't » have a place to enter the echo's IP address, then both the phone and the echo need to be on the same Network. If » you want the echo to live on the Iot network, then you will need to temporarily connect your phone / switch » your phone to the Iot network to control the echo. Note this method won’t work for Wired Iot devices.	=	Some devices could go either on the Home Network or on the Iot Network. I'll use an Amazon Echo as the first example. The echo can execute just fine from » the Iot Network. The echo typically uses a smart phone app to control it. Since Amazon's phone app doesn't » have a place to enter the echo's IP address, then both the phone and the echo need to be on the same Network. If » you want the echo to live on the Iot network, then you will need to temporarily connect your phone / switch » your phone to the Iot network to control the echo. Note this method won’t work for Wired Iot devices.
The echo could also be placed on the Home Network. Since the echo gets regular » updates from Amazon, and	<>	The echo could also be placed on the Home Network. Since the echo gets regular » updates from Amazon, and

Amazon is, presumably, smart enough to keep their device secure, I don't see » having this device on the Home Network as a real problem.	=	Amazon is, presumably, smart enough to keep their device secure, I don't see » having this device on the Home Network as a real problem.
Then there are devices I would NOT let on my Home Network. These are devices which » don’t receive firmware updates, devices which likely connect to some web service, or devices which » ultimately come from Chinese manufacturers. My examples of these devices would be Baby Monitors / Security » Cameras / the proverbial “Light Bulb” / etc... Who knows what is happening inside these devices firmware? Are » there hard coded logins-passwords / open telnet ports / etc...? Hackers may be able to easily penetrate » these devices, and then they are inside the Network these devices are connected to.		Then there are devices I would NOT let on my Home Network. These are devices which » don’t receive firmware updates, devices which likely connect to some web service, or devices which » ultimately come from Chinese manufacturers. My examples of these devices would be Baby Monitors / Security » Cameras / the proverbial “Light Bulb” / etc... Who knows what is happening inside these devices firmware? Are » there hard coded logins-passwords / open telnet ports / etc...? Hackers may be able to easily penetrate » these devices, and then they are inside the Network these devices are connected to.
If you can’t tell or test the security of a device, if it is not being actively » updated, or if it is from some unknown manufacturer, I’d put that device on the Iot Network. To me, these types of » devices are not worth the risk of having them on my Home Network, right alongside my household personal computers.		If you can’t tell or test the security of a device, if it is not being actively » updated, or if it is from some unknown manufacturer, I’d put that device on the Iot Network. To me, these types of » devices are not worth the risk of having them on my Home Network, right alongside my household personal computers.
This is ultimately a convenience vs security trade off. Choose carefully. By even » having an Iot network, you can now choose which Network to put your stuff onto.		This is ultimately a convenience vs security trade off. Choose carefully. By even » having an Iot network, you can now choose which Network to put your stuff onto.
This is from a discussion at https://github.com/mjp66/Ubiquiti/issues/18		This is from a discussion at https://github.com/mjp66/Ubiquiti/issues/18
Page 115 of 136 » 2/4/2019	<>	Page 130 of 157 » 5/18/2019
		82. Device Discovery Across Networks / Subnets
		This subject is complicated. This section and the next couple of sections are all » related. Your mileage will vary, as everybody has a different set of equipment, which relies on different discovery » methods. The Networks involved will typically be the Home Network and one or more of the Iot Network(s).
		Related Links:
		https://community.ubnt.com/t5/EdgeRouter/IOT-VLAN-multicast-still-not-working/m-p/ » 2739880
		https://community.ubnt.com/t5/EdgeRouter/Chromecast-Discovery-Across-VLANs/m-p/271 » 1173
		https://community.ubnt.com/t5/EdgeRouter/Chromecast-traffic-between-VLANs/m-p/2381 » 712
		https://help.ubnt.com/hc/en-us/articles/115001529267
77. Simple Network Management Protocol (SNMP)		

To enable the ER-X to be a source of SNMP data, first press the “System” button.
» Reference Figure 9 – System
Button. Find the SNMP Agent section, fill-in the three fields, and check Enable.
» Press “Save”. See Figure 164 –
Sample SNMP configuration.

The ER-X appears to support both version 1 and version2(c). Version 2 supports 64
» bit counters. The only security

available is to change the SNMP community string to something hard to guess. Most
» installations assume “public”.

Figure 164 – Sample SNMP configuration.

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

Snmpwalk (Referenced in Appendix C)
Cacti
NetworX / LibreNMS / PRTG
Nagips / Zabbix / Dude
OpenNMS
MRTG
Grafana / InfluxDB / Telegraf (See Appendix C)

83. Multicast DNS
The use of MDNS between Networks, was suggested in
» https://github.com/mjp66/Ubiquiti/issues/29 with a link
of: https://www.youtube.com/watch?v=1mjdkki2pIY
I believe MDNS allows clients to resolve host names within a subnet / Network. By
» adding multiple interfaces, this
extends the service across multiple Networks. I don’t know what security
» implications this extending might have.

I have tried enabling MDNS within my ER-X,didn’t seem to help my particular
» installation.
The following interfaces may be different for you, depending upon what Networks
» you are trying to repeat /
connect and if you choose to implement being VLAN Aware. Reference section 79.
» This example connects Home
Net and Iot Net on a VLAN Aware system.
MDNS can be enabled via the CLI or via the Config Tree. To enable via the Config
» Tree, open up the service ->
mdns -> repeater sub-menus. Enter in your interfaces, and then click Preview. See
» Figure 164 – MDNS Setup
Example.

Figure 164 – MDNS Setup Example.

While trying to determine the impact of mdns, I had trouble disabling this feature
» via the Config Tree, so I used
the following commands via the command line interface to disable this service.

```
configure
delete    service       mdns  repeater
commit

save
exit
```

It appears that enabling Multicast DNS is also available within the UniFi (Access
» Point) system.

		Reference the following link: https://community.ubnt.com/t5/UniFi-Routing-Switching/USG-and-Chromecast-across-su » bnets-VLANs-Multicast- or-mDNS/td-p/1782140 Within that article is the following post: https://community.ubnt.com/t5/UniFi-Routing-Switching/USG-and-Chromecast-across-su » bnets-VLANs-Multicast- or-mDNS/m-p/2016844/highlight/true#M53023
	=	
Page 116 of 136 » 2/4/2019	<>	Page 132 of 157 » 5/18/2019 See also the following posts: https://community.ubnt.com/t5/EdgeRouter/mDNS-bonjour-forwarding/td-p/414093/ https://community.ubnt.com/t5/EdgeRouter/mDNS-forwarding-so-that-iPhone-can-commun » icate-with-iTunes- on-a/m-p/1752138/ https://community.ubnt.com/t5/EdgeRouter/Multicast-Sonos-Phorus-amp-Play-Fi-Broadc » ast-255-255-255-255- lt/td-p/1259616
78. Coalescing the Wired Iot and Wifi Iot Networks		Page 133 of 157 » 5/18/2019 84. Simple Service Discovery Protocol (SSDP) / igmp-proxy
This optional section allows the coalescence of the Wired Iot and Wifi Iot Network » s. This involves enabling switch0 to be VLAN Aware. When configuring switch0 to be VLAN Aware, it is important to » NOT be connected to an Edgerouter port which is using switch0. I used the Wired Separate Network (which i » s not in switch0) for these re- configuration steps. I locked myself out of my ER-X EdgeRouter (and had to factory » reset / reload the base configuration) about 4 times while researching and writing this section. Remember that the Wifi Iot Network is setup as a Guest Network, isolating the WiFi » clients from each other. If you would like the WiFi clients to be able to communicate with each other, then you wi » ll need to uncheck ‘Guest Policy” for the WiFi Iot Network. Reference the section near Figure 150 – UniFi Io		SSDP is a discovery protocol used by Universal Plug and Play (UPnP.) Note that » this protocol (SSDP) does not need to open holes in your WAN firewall to operate. This protocol uses UDP packets sent » to a fixed IP address / port for discovering devices. I don’t think this protocol was ever expected to work across » two subnets i.e. two Networks. I have been able to get the SSDP discovery packets to be transferred / copied from » the Home Network to the Iot Network by using an igmp-proxy service. In order to get the SSDP replies back, I h » ad to open up holes in the firewall from the Iot Network back into the Home Network. Not great, but what is » needed if you want to discover devices on the Iot Network from a device on the Home Network. If I were opening up » firewall holes, I would reserve IP address for the Iot device(s), and then only open UDP holes in the Home

» t WiFi. Newer versions of the

UniFi software have an additional checkbox “Multicast and Broadcast Filtering” (on
» the same dialog), which needs
to be unchecked to enable the WiFi clients to communicate with each other.

If you disable guest control, you may need to add additional ER-X firewall rules
» to maintain security, probably
equivalent to Guest Control Post-Authorization Restrictions. See Figure 143 –Unifi
» Guest Control.
I have done limited testing with this configuration, so I still consider this to
» be experimental for Home Usage.

Login to EdgeRouter
The following allows the Wired Separate Network to access the EdgeRouter itself.

    Firewall/NAT
        Firewall   Policies
            WIRED_SEPARATE_LOCAL   -> Actions   -> Configuration
                    Default Action: Accept
                    Save Ruleset

Disconnect your computer's Ethernet cable from eth3 / Home Network.   Wait 5 to
» 10 seconds. Re-connect your
computer's Ethernet cable to eth2 / Wired Separate Network.
Open a new Browser window/tab and enter a URL of 192.168.5.1 and   Login to the
» EdgeRouter
Now we are connected to the EdgeRouter without using switch0.

Move the Home Network Address setup from switch0 to vid 1.

    Dashboard

» Out firewall for those specific
device replies. Reference section 52 - HOME_OUT Firewall Rules and section 76 -
» Reserving Device Addresses via
DHCP.
The following interfaces may be different for you, depending upon what Network you
» are trying to discover from
which other Network, and if you choose to implement being VLAN Aware. Reference
» section 79. This example

allows devices on the Iot Net to be discovered from the Home Net, on a VLAN Aware
» system.
To enable igmp-proxy, use the CLI / putty / SSH to issue the following commands:
      configure
      set protocols   igmp-proxy   interface   switch0.1   role   u
» pstream

      set protocols   igmp-proxy   interface   switch0.7   role
» downstream

      set protocols   igmp-proxy   interface   switch0.1   threshold
» 1
      set protocols   igmp-proxy   interface   switch0.1
» alt-subnet   0.0.0.0/0
      set protocols   igmp-proxy   interface   switch0.7   threshold
» 1
      set protocols   igmp-proxy   interface   switch0.7
» alt-subnet   0.0.0.0/0
      commit   ;   save
To check the igmp-proxy, issue the following commands (you may need to wait

```
                                                                    » several seconds):
                                                                          show  ip  multicast     mfc
                                                                          show  ip  multicast     interfaces

        Home     Net  switch0  ->  Actions   ->  Config
             Vlan     Tab
                    Address:           No address

                                                                    To remove the igmp-proxy services, issue the following commands
    Dashboard
        Add  Interface                                                    configure
             Add     VLAN
                    VLANID:            1
                    Interface:         switch0
                    Description:       Home  Net                        delete   protocols     igmp-proxy
                    MTU:               1500                             commit   ;    save
                    Address:           Manually           define  IP    Address  My ER-X's igmp-proxy seems to restart, with no problems, after a controlled shutdo
                                                                    » wn / restart.
                                      192.168.3.1/24                This following link may or may not be relevant:
                                                                    https://community.ubnt.com/t5/EdgeRouter/IGMP-proxy-not-starting-automatically-aft
                                                                    » er-reboot/td-p/2095339
                                                                    Reference these specifications (see Discovery sections):
                                                                          http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf
                                                                          http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v2.0.pdf
                                                                =
    Page 117 of 136                                                 <>    Page 134 of 157
» 2/4/2019                                                                » 5/18/2019
Remove the address range from Wired Iot Network.                          This is a weird protocol. The device doing the discovery sends out a UDP packet,
                                                                          » somewhat formatted as HTTP-
    Dashboard                                                             data, to a non-existing IP address of 239.255.255.250 with a destination port of
                                                                          » 1900. SSDP listeners (somehow)
                                                                          receive this packet even though they are actually on a different (for us:
                                                                          » 192.168.X.X) Network and (should)
                                                                          respond back to the sender's real (originating) IP address / port number with
                                                                          » their "discoverable" information.

        Wired  Iot    Net /      eth1  ->    Actions   -> Config          Now this gets even weirder.  I have a Roku device on my Iot Network. It responded
                                                                          » back TWICE, saying it was from
             Address:               No   address                         address / port:
                                                                                192.168.7.95 / 60000 (Correct)
Remove firewall rules from Wired Iot Network.
    Firewall/NAT
        Firewall    Policies
```

WIRED_IOT_LOCAL -> Actions -> Edit Ruleset Rules Tab Rule 2-> Action -> Delete Rule Rule 1-> Action -> Delete Rule Interfaces Tab		and from 192.168.49.1 / 60000 (Incorrect) The contents of the reply packets from the Roku both contained the correct IP » address / port of the Roku: “LOCATION: http://192.168.7.95:60000/upnp/dev/...”. for the discoverer to be able to contact the Roku device. The second packet (which » was addressed to 192.168.49.1) broke through my original Home Out firewall rules. Reference updated » rules within section 52 - HOME_OUT Firewall Rules. This is why I have switched over to using the full set of » RFC-1918 addresses. Here are some related links: https://help.ubnt.com/hc/en-us/articles/360001004034-UniFi-Best-Practices-for-Mana » ging-Chromecast-Google- Home-on-UniFi-Network https://help.ubnt.com/hc/en-us/articles/204961854-EdgeRouter-Set-up-IGMP-proxy-and » -statistics https://community.ubnt.com/t5/UniFi-Routing-Switching/Configure-Sonos-across-subne » ts-on-USG/td-p/1979899
Set Interface --		
Set Direction -- WIRED_IOT_LOCAL -> Actions -> Delete Rules » et Delete the Wired Iot Network DHCP server. Services DHCP Server WiredIotDHCP Actions Delete		
	=	
Move Home Network firewall rules from switch0 to vid 1 Firewall/NAT Firewall Policies HOME_OUT Actions -> Interfaces Interfaces: switch0.1 Enable switch0 to be Vlan Aware. Note that I connect my Access Point to eth4, so I could have, but didn’t add “vid » 6, 7” to eth3.	<>	Here is a command to see what is going through the firewall on port 1900: sudo tcpdump -i switch0.1 port 1900 -vv Page 135 of 157 » 5/18/2019 85. socat - Multipurpose relay (SOcket CAT) I have not tried this, but this is another tool for discovery across Networks / » subnets.

Dashboard
Switch0 Config
Vlan
Vlan Aware Enable checked
eth1 checked
(Click Config Tab, then Click Vlan tab to refresh the dialog » / size)
eth1 pvid 7
eth3 checked

eth3 pvid 1
eth4 checked
eth4 pvid 1

eth4 vid 6, 7

The following restores the Wired Separate Network firewall restrictions.

Firewall/NAT

Reference links:
http://www.dest-unreach.org/socat/
https://linux.die.net/man/1/socat

Ubiquiti Links:
https://community.ubnt.com/t5/EdgeRouter/Howto-HDHomerun-discovery-on-different-LA » N-segment/m-
p/2750080
http://www.cron.dk/edgerouter-and-chromecast/

86. Insecurity versus Convenience
Otherwise known as “Punching holes in your firewall”.

This example will involve allowing an SSDP rely from a specific IOT device to » reach a specific HomeNet device.
Reference section 52 - HOME_OUT Firewall Rules. The HOME_OUT firewall has a bunch » of Allow “Established /
Related” rules, with one for each Network, followed by a drop of RFC-1918 » addresses.
Reference section 84 - Simple Service Discovery Protocol (SSDP) / igmp-proxy. In » SSDP, the querying equipment
opens a (high) UDP port, sends out a UDP query to a destination port of 1900, and » listens / receives replies which
are sent back to the original (high) UDP port. The SSDP query data contains the » originators IP address and the
originators (high) UDP port number, so the responders know where to respond. This » (high) port number may-not-
be / is-probably-not at a fixed port number.
For the following rule to work, ensure that both devices have had their IP address » es reserved. Reference section
76 - Reserving Device Addresses via DHCP.
The following rule (inserted in HOME_OUT) would allow the 192.168.7.154 IOT device » to reply back to the
192.168.3.81 HomeNet device with any UDP data to any UDP port:

Firewall Policies
WIRED_SEPARATE_LOCAL -> Actions -> Configuration
 	
Default Action: Drop
Save Ruleset
		rule 40 {
		action accept
		description "Allow Example IOT Reply"
		destination {
		address 192.168.3.81
		}
		log disable
		protocol udp
		source {
		address 192.168.7.154
		}
		}
		
		Related Links:
		Secure IoT Network Configuration - YouTube -Crosstalk Solutions
		https://m.youtube.com/watch?v=6ElI8QeYbZQ

	=	
Page 118 of 136 » 2/4/2019 You may want to rename the “Wifi Iot” / “Wired Iot” items to simply be “Iot” » items. References: https://github.com/mjp66/Ubiquiti/issues/5 https://community.ubnt.com/t5/EdgeRouter/EdgeRouter-X-Inter-VLAN-routing-issues-Ho » w-I-solved-it/td- p/1813187 https://help.ubnt.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRout » er-as-a-Layer-2-Switch	<>	Page 137 of 157 » 5/18/2019 87. Virtual Private Networks (VPN) I have not played with or implemented a VPN. There seem to be several types. Here » are some VPN links. EdgeRouter - OpenVPN Server: https://help.ubnt.com/hc/en-us/articles/115015971688 EdgeRouter - L2TP IPsec VPN Server: » https://help.ubnt.com/hc/en-us/articles/204950294-EdgeRouter-L2TP-IPsec-VPN-Serv » er EdgeRouter - Site-to-Site VPN Behind NAT https://help.ubnt.com/hc/en-us/articles/115013382567-EdgeRouter-Site-to-Site » -VPN-Behind-NAT EdgeRouter - EoGRE Layer 2 Tunnel » https://help.ubnt.com/hc/en-us/articles/204961754-EdgeRouter-EoGRE-Layer-2-Tunne » l GUIDE: How to configure Local PPTP VPN: https://community.ubnt.com/t5/EdgeRouter/GUIDE-How-to-configure-Local-PPTP-V » PN-on-1-5-0-

		Firmware-works-on/m-p/971155
		Private Internet Access Open VPN - Step by Step Configuration:
		» https://community.ubnt.com/t5/EdgeRouter/Private-Internet-Access-Open-VPN-Step-b
		» y-Step-
		Configuration/m-p/1711643
		Troubleshooting-Site-To-Site-on-ER-Xs:
https://community.ubnt.com/t5/EdgeRouter/Setting-VLAN-s-with-ERX-broke-it-complete		https://community.ubnt.com/t5/EdgeRouter/Troubleshooting-Site-To-Site-on-ER-
» ly/td-p/1917708		» Xs/m-p/2749611
		ubiquiti-edgerouter-ipsec-performance:
		https://www.simonmott.co.uk/2018/08/ubiquiti-edgerouter-ipsec-performance/
		OpenVPN vs L2TP:
		https://community.ubnt.com/t5/EdgeRouter/OpenVPN-vs-L2TP/m-p/2659909
		Secure OpenVPN server setup with multi-factor authentication (Google
		» Authenticator): step-by-step:
https://community.ubnt.com/t5/EdgeRouter/Edge-Router-X-as-Switch-with-VLAN-Need-He		https://community.ubnt.com/t5/EdgeRouter/Secure-OpenVPN-server-setup-with-mu
» lp/td-p/1992908		» lti-factor-
		authentication/m-p/1240405
		OpenVPN configurator for EdgeMax
https://community.ubnt.com/t5/EdgeRouter/Edge-router-X-SFP-VLAN-s/td-p/1971128		https://community.ubnt.com/t5/EdgeRouter/Helpful-Tool-OpenVPN-configurator-f
		» or-EdgeMax/m-
		p/2779412#M251490
		Wireguard [New]:
https://help.ubnt.com/hc/en-us/articles/115012700967-EdgeRouter-VLAN-Aware-Switch		https://community.ubnt.com/t5/EdgeRouter/Release-WireGuard-for-EdgeRouter/td-p/190
		» 4764
		https://github.com/Lochnair/vyatta-wireguard
		https://www.wireguard.com/
		https://andrew.dunn.dev/posts/wireguard-from-your-isp/
		https://www.erianna.com/wireguard-ubiquity-edgeos/
	=	
Page 119 of 136	<>	Page 138 of 157
» 2/4/2019		» 5/18/2019
		88. UNMS - Ubiquiti Network Management System
		Barely played with this:
		https://help.ubnt.com/hc/en-us/sections/115003321288-UNMS-Ubiquiti-Network-Managem
		» ent-System
		https://help.ubnt.com/hc/en-us/articles/360008732414-UNMS-NetFlow
79. Intrusion Detection Systems		89. Intrusion Detection Systems
QUESTION: Which one to pick? How to configure it / connect it to the EdgeRouter?	=	QUESTION: Which one to pick? How to configure it / connect it to the EdgeRouter?
@BuckeyeNet suggests Security Onion. Security Onion is at	<>	@BuckeyeNet suggests Security Onion. Security Onion is at

» https://securityonion.net/ and		» https://securityonion.net/ and
https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecu » rityOnion Seems to be rather involved. I have not tried Security Onion yet.	=	https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecu » rityOnion Seems to be rather involved. I have not tried Security Onion yet.
	<>	Page 139 of 157 » 5/18/2019 90. Miscellaneous Links This seems like a wealth of information: http://wiki.indie-it.com/wiki/Ubiquiti Run script which disable/enables a firewall policy: » https://community.ubnt.com/t5/EdgeRouter/Run-script-which-disable-enables-a-fire » wall-policy/m- p/2724337 Forward port to PC on IoT Network: » https://community.ubnt.com/t5/EdgeRouter/Forward-port-to-PC-on-IoT-Network/m-p/2 » 709401 UBRSS_Training_Guide_V1.2: https://dl.ubnt.com/guides/training/courses/UBRSS_Training_Guide_V1.2.pdf How to set up MTU properly: » https://community.ubnt.com/t5/EdgeRouter/How-to-set-up-MTU-properly/m-p/2337184 EdgeRouter - Configure an EdgeRouter as a Layer 2 Switch (Handy for a remote » POE-powered Ethernet switch): » https://help.ubnt.com/hc/en-us/articles/217990978-EdgeRouter-Configure-an-EdgeRo » uter-as-a-Layer-2- Switch Measure instantaneous bandwidth usage over time: » https://community.ubnt.com/t5/EdgeRouter/Measure-instantaneous-bandwidth-usage-o » ver-time/m- p/2554597 Help setting up NetFlow : » https://community.ubnt.com/t5/EdgeRouter/Help-setting-up-NetFlow/m-p/464367/high » light/true Add Debian Packages to EdgeOS:

		» https://help.ubnt.com/hc/en-us/articles/205202560-EdgeRouter-Add-Debian-Packages » -to-EdgeOS Page 140 of 157 » 5/18/2019
80. Conclusions		91. Conclusions
I hope that this guide helped you set up your Ubiquiti equipment, and that you » have learned a lot. Enjoy your new network. -Mike	=	I hope that this guide helped you set up your Ubiquiti equipment, and that you » have learned a lot. Enjoy your new network. -Mike
Page 120 of 136 » 2/4/2019	<>	Page 141 of 157 » 5/18/2019
Appendix A. TP-Link TL-SG105EV2 Switch Setup	=	Appendix A. TP-Link TL-SG105EV2 Switch Setup
This section has nothing to do with the ER-X setup. This section is related to » Method 1 of section 10, for using	<>	This section has nothing to do with the ER-X setup. This section is related to » Method 1 of section 11, for using
multiple UAPs. [Note I also tried a TP-Link TL-SG105 (Ver 2.1) UN-managed Gigabit switch, and it » also worked. I am amazed. Maybe Gigabit switch chips are now designed to pass (the larger) VLAN frame data » automatically, I don’t know. This makes the rest of this section pretty much academic.] The inexpensive Netgear switches should also work, I just happened to have Tp-Link » models available for use. I believe these switches will need a hardware version of V2 or above to operate » correctly. These directions are approximate.	=	multiple UAPs. [Note I also tried a TP-Link TL-SG105 (Ver 2.1) UN-managed Gigabit switch, and it » also worked. I am amazed. Maybe Gigabit switch chips are now designed to pass (the larger) VLAN frame data » automatically, I don’t know. This makes the rest of this section pretty much academic.] The inexpensive Netgear switches should also work, I just happened to have Tp-Link » models available for use. I believe these switches will need a hardware version of V2 or above to operate » correctly. These directions are approximate.
I configured an additional AP-AC-LR Ubiquiti Access Point by referencing the » “General” portion of section 10, and then following sections 62 through 67 for this additional UAP.	<>	I configured an additional AP-AC-LR Ubiquiti Access Point by referencing the » “General” portion of section 11, and then following sections 65 through 70 for this additional UAP.
	=	
I connected the Tp-Link switch to my computer which was configured with a fixed » address of 192.168.1.10.		I connected the Tp-Link switch to my computer which was configured with a fixed » address of 192.168.1.10.
Reference section 7 for how to configure a computer’s Ethernet port. Using the » Tp-Link software, I then	<>	Reference section 8 for how to configure a computer’s Ethernet port. Using the » Tp-Link software, I then
configured this switch to have a specific 192.168.3.X address. After saving the » configuration, I re-configured my computer back to DHCP, and re-connected the computer to the Home Network. I also » connected the new switch to the Home Network. I then made a static reservation within the ER-X for this » switch. For this example, I will use and connect two UAPs to this switch. I choose port 4	=	configured this switch to have a specific 192.168.3.X address. After saving the » configuration, I re-configured my computer back to DHCP, and re-connected the computer to the Home Network. I also » connected the new switch to the Home Network. I then made a static reservation within the ER-X for this » switch. For this example, I will use and connect two UAPs to this switch. I choose port 4

» and port 5 for those UAP connections. I also choose port 1 of this switch to connect to the ER-X's eth4 » port. Using the Tp-Link software, I selected the VLAN / 802.1Q VLAN page. See Figure » 165 – Tp-Link Initial 802.1Q Dialog. Figure 165 – Tp-Link Initial 802.1Q Dialog.		» and port 5 for those UAP connections. I also choose port 1 of this switch to connect to the ER-X's eth4 » port. Using the Tp-Link software, I selected the VLAN / 802.1Q VLAN page. See Figure » 165 – Tp-Link Initial 802.1Q Dialog. Figure 165 – Tp-Link Initial 802.1Q Dialog.
Page 121 of 136 » 2/4/2019	<>	Page 142 of 157 » 5/18/2019
On the VLAN page, enable the Global Config. Reference Table 1 - Table of Networks for the VLAN Networks used for this project. » Enter the following information into the VLAN Page: VLAN: 6 VLAN Name: WiFiGuest Tag the ports: 1, 4, 5 See Figure 166 – Tp-Link VLAN 6 Configuration. Press Apply Figure 166 – Tp-Link VLAN 6 Configuration.	=	On the VLAN page, enable the Global Config. Reference Table 1 - Table of Networks for the VLAN Networks used for this project. » Enter the following information into the VLAN Page: VLAN: 6 VLAN Name: WiFiGuest Tag the ports: 1, 4, 5 See Figure 166 – Tp-Link VLAN 6 Configuration. Press Apply Figure 166 – Tp-Link VLAN 6 Configuration.
Page 122 of 136 » 2/4/2019	<>	Page 143 of 157 » 5/18/2019
Enter the following information into the VLAN Page: VLAN: 7 VLAN Name: WiFiIot Tag the ports: 1, 4, 5 See Figure 167 – Tp-Link VLAN 7 Configuration. Press Apply. Figure 167 – Tp-Link VLAN 7 Configuration.	=	Enter the following information into the VLAN Page: VLAN: 7 VLAN Name: WiFiIot Tag the ports: 1, 4, 5 See Figure 167 – Tp-Link VLAN 7 Configuration. Press Apply. Figure 167 – Tp-Link VLAN 7 Configuration.
Page 123 of 136 » 2/4/2019	<>	Page 144 of 157 » 5/18/2019
When you are finished, your screen should look like Figure 168 – Tp-Link VLAN » Final Configuration. Press Save in the upper right. Figure 168 – Tp-Link VLAN Final Configuration. After this configuration, I disconnected this switch from the Home Network. I » disconnected the original UAP from the ER-X eth4 port.	=	When you are finished, your screen should look like Figure 168 – Tp-Link VLAN » Final Configuration. Press Save in the upper right. Figure 168 – Tp-Link VLAN Final Configuration. After this configuration, I disconnected this switch from the Home Network. I » disconnected the original UAP from the ER-X eth4 port.
Page 124 of 136 » 2/4/2019	<>	Page 145 of 157 » 5/18/2019
I then connected port 1 of the Tp-Link switch to the ER-X's eth4 port. I connected	=	I then connected port 1 of the Tp-Link switch to the ER-X's eth4 port. I connected

» one UAP (via its Power Over		» one UAP (via its Power Over
Ethernet (POE) adapter) to the Tp-Link switch port 4 and the other UAP, via its		Ethernet (POE) adapter) to the Tp-Link switch port 4 and the other UAP, via its
» POE, to the Tp-Link switch port 5.		» POE, to the Tp-Link switch port 5.
See Figure 169 – Multiple Access Point Wiring. Also reference section 61 and	<>	See Figure 169 – Multiple Access Point Wiring. Also reference section 64 and
» Figure 110 – Access Point Wiring. I		» Figure 109 – Access Point Wiring. I
did nothing with the Tp-Link switch ports 2 and 3.	=	did nothing with the Tp-Link switch ports 2 and 3.
Figure 169 – Multiple Access Point Wiring.		Figure 169 – Multiple Access Point Wiring.
For testing purposes, I configured each of my two UAPs with differently-named-sets		For testing purposes, I configured each of my two UAPs with differently-named-sets
» of SSIDs. This way I could		» of SSIDs. This way I could
control and test which UAP I was actually connecting to.		control and test which UAP I was actually connecting to.
Page 125 of 136	<>	Page 146 of 157
» 2/4/2019		» 5/18/2019
Appendix B. Multimedia over Coax Alliance (MOCA)	=	Appendix B. Multimedia over Coax Alliance (MOCA)
This section has nothing to do with the ER-X setup; this is just general		This section has nothing to do with the ER-X setup; this is just general
» networking information.		» networking information.
If you house is wired for television coax i.e. “Cable TV” and you do not have		If you house is wired for television coax i.e. “Cable TV” and you do not have
» satellite TV, you might be able to use		» satellite TV, you might be able to use
Multimedia over Coax Alliance (MOCA) adapters as an alternative to direct Ethernet		Multimedia over Coax Alliance (MOCA) adapters as an alternative to direct Ethernet
» cabling. This could be useful if		» cabling. This could be useful if
you want to place your UAP in the center of your house, and don’t have / can’t		you want to place your UAP in the center of your house, and don’t have / can’t
» wire direct Ethernet cabling to that		» wire direct Ethernet cabling to that
location from your router. These could also be used to positon a second UAP at		location from your router. These could also be used to positon a second UAP at
» that far end of a house, where		» that far end of a house, where
you can’t run any Ethernet wires.		you can’t run any Ethernet wires.
A MOCA adapter will re-broadcast Ethernet traffic over Cable TV wires to another		A MOCA adapter will re-broadcast Ethernet traffic over Cable TV wires to another
» MOCA adapter. You need at		» MOCA adapter. You need at
least two MOCA adapters to network together. These adapters can concurrently		least two MOCA adapters to network together. These adapters can concurrently
» operate over coax wires which		» operate over coax wires which
are carrying Cable TV signals. If you use these adapters, you will also want to		are carrying Cable TV signals. If you use these adapters, you will also want to
» install a Point of Entry (POE) filter, so		» install a Point of Entry (POE) filter, so
that your MOCA signals don’t contaminate the Cable TV provider’s network, i.e.		that your MOCA signals don’t contaminate the Cable TV provider’s network, i.e.
» your neighborhood.		» your neighborhood.
A friend of mine had trouble streaming WiFi data to his television set, which was		A friend of mine had trouble streaming WiFi data to his television set, which was
» at the far end of his house from		» at the far end of his house from
his router. He purchased two MOCA adapters to Ethernet connect his Television to		his router. He purchased two MOCA adapters to Ethernet connect his Television to
» his router. He has had no		» his router. He has had no
problems and has since purchased two more adapters to provide more Ethernet drops		problems and has since purchased two more adapters to provide more Ethernet drops
» in his house.		» in his house.
You will want at least version 2.0 adapters. You will need MOCA adapters which		You will want at least version 2.0 adapters. You will need MOCA adapters which
» support 802.1Q if you will be		» support 802.1Q if you will be

using them to connect UAPs to your ER-X. A pair of these adapters seems to be » about U.S. $170. That's pretty expensive, but might be worth it, if your only other alternative is (typically » unreliable) Power-line Ethernet adapters. References: http://www.mocalliance.org/ https://en.wikipedia.org/wiki/Multimedia_over_Coax_Alliance		using them to connect UAPs to your ER-X. A pair of these adapters seems to be » about U.S. $170. That's pretty expensive, but might be worth it, if your only other alternative is (typically » unreliable) Power-line Ethernet adapters. References: http://www.mocalliance.org/ https://en.wikipedia.org/wiki/Multimedia_over_Coax_Alliance
Page 126 of 136 » 2/4/2019	<>	Page 147 of 157 » 5/18/2019
Appendix C. Monitoring an EdgeRouter via SNMP with Grafana running on a Raspberry Pi This section has nothing to do with the ER-X setup. ========== Appendix C - Part 1 The following directions will show how to install and configure Grafana, InfluxDB, » and Telegraf on a Raspberry Pi, for monitoring EdgeRouter statistics. Preview pictures are available in one of the » below links. The heavy lifting on this project was done by @waterside. Here are the major » references: https://github.com/WaterByWind/grafana-dashboards » https://github.com/WaterByWind/grafana-dashboards/tree/master/UBNT-EdgeRouter https://grafana.com/dashboards/1756 (with pictures) » https://community.ubnt.com/t5/UniFi-Wireless/Grafana-dashboard-for-UniFi-APs-now » -available/td- p/1833532 Most of the following items will be performed in a command terminal, so you will » need to be generally familiar	=	Appendix C. Monitoring an EdgeRouter via SNMP with Grafana running on a Raspberry Pi This section has nothing to do with the ER-X setup. ========== Appendix C - Part 1 The following directions will show how to install and configure Grafana, InfluxDB, » and Telegraf on a Raspberry Pi, for monitoring EdgeRouter statistics. Preview pictures are available in one of the » below links. The heavy lifting on this project was done by @waterside. Here are the major » references: https://github.com/WaterByWind/grafana-dashboards » https://github.com/WaterByWind/grafana-dashboards/tree/master/UBNT-EdgeRouter https://grafana.com/dashboards/1756 (with pictures) » https://community.ubnt.com/t5/UniFi-Wireless/Grafana-dashboard-for-UniFi-APs-now » -available/td- p/1833532 Most of the following items will be performed in a command terminal, so you will » need to be generally familiar
with RaspberryPi / Linux / Rasbian to continue. You will need to enable SNMP on » the ER-X, Reference section 77 -	<>	with RaspberryPi / Linux / Rasbian to continue. You will need to enable SNMP on » the ER-X, Reference section 80 -
Simple Network Management Protocol (SNMP). To enable the Grafana web page to be remotely accessed by computers other than the » Pi (i.e. accessed via PCs on the HomeNetwork), the Pi running these tools will need to be assigned a reserved » IP address. Reference section	=	Simple Network Management Protocol (SNMP). To enable the Grafana web page to be remotely accessed by computers other than the » Pi (i.e. accessed via PCs on the HomeNetwork), the Pi running these tools will need to be assigned a reserved » IP address. Reference section
74 - Reserving Device Addresses via DHCP, for how to do this. Since the Pi is » relatively slow, I suggest not	<>	76 - Reserving Device Addresses via DHCP, for how to do this. Since the Pi is » relatively slow, I suggest not

browsing directly on the Pi, after the initial setup. Start with Rasbian Stretch. I used a 32Gig micro SD card, as I expect to collect a » lot of data over time. Configure Pi Menu -> Preferences -> Raspberry Pi Configuration Localization Tab Set Locale Set Timezone Set Keyboard Set WiFi Country (You may also want to enable the following) Interfaces Tab SSH: Enable VNC: Enable Update PI Operating System sudo apt-get update sudo apt-get upgrade Install SNMP and associated tools sudo apt-get install snmp sudo apt-get install snmpd sudo apt-get install dnsutils	=	browsing directly on the Pi, after the initial setup. Start with Rasbian Stretch. I used a 32Gig micro SD card, as I expect to collect a » lot of data over time. Configure Pi Menu -> Preferences -> Raspberry Pi Configuration Localization Tab Set Locale Set Timezone Set Keyboard Set WiFi Country (You may also want to enable the following) Interfaces Tab SSH: Enable VNC: Enable Update PI Operating System sudo apt-get update sudo apt-get upgrade Install SNMP and associated tools sudo apt-get install snmp sudo apt-get install snmpd sudo apt-get install dnsutils
Page 127 of 136 » 2/4/2019	<>	Page 148 of 157 » 5/18/2019
Test ER-X's SNMP setup by issuing: snmpwalk -v2c -c public 192.168.3.1 You should see a lot of data, most of it starting with “iso”. Download binaries Go to https://www.influxdata.com/ (The depiction below is what I saw and the commands which I copied from the » website and then ran.) (You will want to check for and use updated instructions / versions / » commands.) (The wget commands are one long line, which is wrapped within this » document.) Select Download tab Select Telegraf (v1.5.2) button Find Linux Binaries (ARM) section wget https://dl.influxdata.com/telegraf/releases/telegraf- 1.5.2_linux_armhf.tar.gz tar xvfz telegraf-1.5.2_linux_armhf.tar.gz	=	Test ER-X's SNMP setup by issuing: snmpwalk -v2c -c public 192.168.3.1 You should see a lot of data, most of it starting with “iso”. Download binaries Go to https://www.influxdata.com/ (The depiction below is what I saw and the commands which I copied from the » website and then ran.) (You will want to check for and use updated instructions / versions / » commands.) (The wget commands are one long line, which is wrapped within this » document.) Select Download tab Select Telegraf (v1.5.2) button Find Linux Binaries (ARM) section wget https://dl.influxdata.com/telegraf/releases/telegraf- 1.5.2_linux_armhf.tar.gz tar xvfz telegraf-1.5.2_linux_armhf.tar.gz

```
      Select InflluxDB (v1.4.3) button
      Find Linux Binaries (ARM) section
            wget    https://dl.influxdata.com/influxdb/releases/influxdb-
1.4.3_linux_armhf.tar.gz
            tar    xvfz      influxdb-1.4.3_linux_armhf.tar.gz
      Select Chronograf (v1.4.2.1) button
      Find Linux Binaries (ARM) section
            wget    https://dl.influxdata.com/chronograf/releases/chronograf-
1.4.2.1_linux_armhf.tar.gz
            tar    xvfz      chronograf-1.4.2.1_linux_armhf.tar.gz
Install (copy) binaries per
https://community.influxdata.com/t/installing-on-a-raspberry-pi/2159
(You will want to adjust directory names for your specific versions.)
      cd  telegraf
      sudo  cp    -rp       usr/*  /usr
      sudo  cp    -rp       etc/*  /etc
      sudo  cp    -rp       var/*  /var
      cd  ..
      cd  influxdb-1.4.3-1
      sudo  cp    -rp       usr/*  /usr
      sudo  cp    -rp       etc/*  /etc
      sudo  cp    -rp       var/*  /var
      cd  ..
      cd  cronograf-1.4.2.1-1
      sudo  cp    -rp       usr/*  /usr
      sudo  cp    -rp       etc/*  /etc
      sudo  cp    -rp       var/*  /var
      cd  ..
```



```
      Select InflluxDB (v1.4.3) button
      Find Linux Binaries (ARM) section
            wget    https://dl.influxdata.com/influxdb/releases/influxdb-
1.4.3_linux_armhf.tar.gz
            tar    xvfz      influxdb-1.4.3_linux_armhf.tar.gz
      Select Chronograf (v1.4.2.1) button
      Find Linux Binaries (ARM) section
            wget    https://dl.influxdata.com/chronograf/releases/chronograf-
1.4.2.1_linux_armhf.tar.gz
            tar    xvfz      chronograf-1.4.2.1_linux_armhf.tar.gz
Install (copy) binaries per
https://community.influxdata.com/t/installing-on-a-raspberry-pi/2159
(You will want to adjust directory names for your specific versions.)
      cd  telegraf
      sudo  cp    -rp       usr/*  /usr
      sudo  cp    -rp       etc/*  /etc
      sudo  cp    -rp       var/*  /var
      cd  ..
      cd  influxdb-1.4.3-1
      sudo  cp    -rp       usr/*  /usr
      sudo  cp    -rp       etc/*  /etc
      sudo  cp    -rp       var/*  /var
      cd  ..
      cd  cronograf-1.4.2.1-1
      sudo  cp    -rp       usr/*  /usr
      sudo  cp    -rp       etc/*  /etc
      sudo  cp    -rp       var/*  /var
      cd  ..
```

```
      Put the following text into:
            /etc/systemd/system/influxdb.service
            [Unit]
            Description=InfluxDB            service
            After=network.target
            [Service]
            ExecStart=/usr/bin/influxd
            Restart=always
            [Install]
            WantedBy=multi-user.target
```

```
      Put the following text into:
            /etc/systemd/system/influxdb.service
            [Unit]
            Description=InfluxDB            service
            After=network.target
            [Service]
            ExecStart=/usr/bin/influxd
            Restart=always
            [Install]
            WantedBy=multi-user.target
```

Start the service (now) with the following command:		Start the service (now) with the following command:
sudo systemctl start influxdb.service		sudo systemctl start influxdb.service
Check that the service is running with:		Check that the service is running with:
systemctl | grep influx		systemctl | grep influx
Auto start the service (after re-boots) with the following command:		Auto start the service (after re-boots) with the following command:
sudo systemctl enable influxdb.service		sudo systemctl enable influxdb.service
Put the following text into:		Put the following text into:
/etc/systemd/system/telegraf.service		/etc/systemd/system/telegraf.service
[Unit]		[Unit]
Description=Telegraf service		Description=Telegraf service
After=network.target		After=network.target
[Service]		[Service]
ExecStart=/usr/bin/telegraf -config		ExecStart=/usr/bin/telegraf -config
» /etc/telegraf/telegraf.conf		» /etc/telegraf/telegraf.conf
Restart=always		Restart=always
[Install]		[Install]
WantedBy=multi-user.target		WantedBy=multi-user.target
Note that the ExecStart is really one long line, upto the Restart line. It		Note that the ExecStart is really one long line, upto the Restart line. It
» may be wrapped within this		» may be wrapped within this
document.		document.
Start the service (now) with the following command:		Start the service (now) with the following command:
sudo systemctl start telegraf.service		sudo systemctl start telegraf.service
Check that the service is running with:		Check that the service is running with:
systemctl | grep telegraf		systemctl | grep telegraf
Auto start the service (after re-boots) with the following command:		Auto start the service (after re-boots) with the following command:
sudo systemctl enable telegraf.service		sudo systemctl enable telegraf.service
Download and install grafana		Download and install grafana
Go to https://github.com/fg2it/grafana-on-raspberry		Go to https://github.com/fg2it/grafana-on-raspberry
(You will want to check for and use updated instructions / versions /		(You will want to check for and use updated instructions / versions /
» commands.)		» commands.)
(Some instructions / commands will be presented, after you issue the dpkg		(Some instructions / commands will be presented, after you issue the dpkg
» command.)		» command.)
Press the raspberry pi 2 and 3 (armv7) Download button in the middle of		Press the raspberry pi 2 and 3 (armv7) Download button in the middle of
» screen		» screen
Save file grafana_5.0.0_armhf.deb whose link is near the bottom of the page		Save file grafana_5.0.0_armhf.deb whose link is near the bottom of the page
Issue the following command:		Issue the following command:
sudo dpkg -i Downloads/grafana_5.0.0_armhf.deb		sudo dpkg -i Downloads/grafana_5.0.0_armhf.deb
Page 129 of 136	<>	Page 150 of 157
» 2/4/2019		» 5/18/2019
Follow presented instructions, which for my version, included:	=	Follow presented instructions, which for my version, included:

```
                sudo  /bin/systemctl         daemon-reload
                sudo  /bin/systemctl         enable  grafana-server
                sudo  /bin/systemctl         start  grafana-server
Acquire needed mib files, by issuing the following command:
      sudo      apt-get   install       snmp-mibs-downloader
Download zip from:
      https://github.com/WaterByWind/grafana-dashboards
      (Use the green “Clone or download” button, then “Download ZIP” button)
Unzip the file:
      unzip      Downloads/grafana-dashboards-master.zip
Configure telegraf
      cd  /etc/telegraf
      cp  telegraf.conf           telegraf.conf.orig
      Edit telegraf.conf
                Change the line:        interval   =  "10s"
                To:                     interval   =  "60s"
                Change the line:        collection_jitter       = "0s"
                To:                     collection_jitter       = "10s"
                Change the line:        # username    = "telegraf"
                To:                     username   =  "username"
                Change the line:        # password    =
» "metricsmetricsmetricsmetrics"
                To:                     password   =  "password"
                Uncomment:              # user_agent    =   "telegraf"
                Append the contents of
» grafana-dashboards-master/UBNT-EdgeRouter/telegraf-inputs.conf
                to telegraf.conf. You may want to add separator comment line(s)
» between the sections.
                Change the line:        agents   = [  "edgerouter1",
» "edgerouter2"    ]
                To:                     agents   = [  "192.168.3.1"      ]
      sudo      systemctl    restart       telegraf.service
      cd  /home/pi
Check that the service is running with:
      systemctl        | grep     telegraf
Test telegraf (this is one long command line)
      telegraf        --config     /etc/telegraf/telegraf.conf
» --config-directory
/etc/telegraf/telegraf.d             --input-filter      snmp   --test
You should see a huge block of data, with no error messages.
```

```
                sudo  /bin/systemctl         daemon-reload
                sudo  /bin/systemctl         enable  grafana-server
                sudo  /bin/systemctl         start  grafana-server
Acquire needed mib files, by issuing the following command:
      sudo      apt-get   install       snmp-mibs-downloader
Download zip from:
      https://github.com/WaterByWind/grafana-dashboards
      (Use the green “Clone or download” button, then “Download ZIP” button)
Unzip the file:
      unzip      Downloads/grafana-dashboards-master.zip
Configure telegraf
      cd  /etc/telegraf
      cp  telegraf.conf           telegraf.conf.orig
      Edit telegraf.conf
                Change the line:        interval   =  "10s"
                To:                     interval   =  "60s"
                Change the line:        collection_jitter       = "0s"
                To:                     collection_jitter       = "10s"
                Change the line:        # username    = "telegraf"
                To:                     username   =  "username"
                Change the line:        # password    =
» "metricsmetricsmetricsmetrics"
                To:                     password   =  "password"
                Uncomment:              # user_agent    =   "telegraf"
                Append the contents of
» grafana-dashboards-master/UBNT-EdgeRouter/telegraf-inputs.conf
                to telegraf.conf. You may want to add separator comment line(s)
» between the sections.
                Change the line:        agents   = [  "edgerouter1",
» "edgerouter2"    ]
                To:                     agents   = [  "192.168.3.1"      ]
      sudo      systemctl    restart       telegraf.service
      cd  /home/pi
Check that the service is running with:
      systemctl        | grep     telegraf
Test telegraf (this is one long command line)
      telegraf        --config     /etc/telegraf/telegraf.conf
» --config-directory
/etc/telegraf/telegraf.d             --input-filter      snmp   --test
You should see a huge block of data, with no error messages.
```

Page 130 of 136 » 2/4/2019	<>	Page 151 of 157 » 5/18/2019
Only if you see error messages, will you need to acquire additional mib files from » your ER-X's /usr/share/mibs directory. (I used WinSCP, which allows files to be copied to/from a Windows PC against » another system.) (You may instead be able to acquire the mib files by other means or over the » internet.) (See also https://github.com/WaterByWind/grafana-dashboards/issues/3) (See also https://github.com/WaterByWind/grafana-dashboards/issues/1) mkdir /usr/share/mibs/ mkdir /usr/share/mibs/site chmod ugo+w /usr/share/mibs/site cp <mib_files> /usr/share/mibs/site cd /home/pi	=	Only if you see error messages, will you need to acquire additional mib files from » your ER-X's /usr/share/mibs directory. (I used WinSCP, which allows files to be copied to/from a Windows PC against » another system.) (You may instead be able to acquire the mib files by other means or over the » internet.) (See also https://github.com/WaterByWind/grafana-dashboards/issues/3) (See also https://github.com/WaterByWind/grafana-dashboards/issues/1) mkdir /usr/share/mibs/ mkdir /usr/share/mibs/site chmod ugo+w /usr/share/mibs/site cp <mib_files> /usr/share/mibs/site cd /home/pi
Locally login to grafana, by browsing to http://localhost:3000 admin admin Login button		Locally login to grafana, by browsing to http://localhost:3000 admin admin Login button
Reference: https://github.com/WaterByWind/grafana-dashboards/tree/master/Extra (To enable the Grafana web page to be remotely accessed by computers other than » the Pi (i.e. accessed via PCs on the HomeNetwork), substitute the Pi's IP address for the » above "localhost".)		Reference: https://github.com/WaterByWind/grafana-dashboards/tree/master/Extra (To enable the Grafana web page to be remotely accessed by computers other than » the Pi (i.e. accessed via PCs on the HomeNetwork), substitute the Pi's IP address for the » above "localhost".)
Choose Add data source Enter the following information: Name Telegraf Type InfluxDB URL http://localhost:8086 Access direct Database telegraf User username Password password Press the Save&Test button		Choose Add data source Enter the following information: Name Telegraf Type InfluxDB URL http://localhost:8086 Access direct Database telegraf User username Password password Press the Save&Test button
Add a dashboard 1. Hover over the upper-left + button 2. Choose Import from the Create section 3. Enter 1756 into the Grafana.com Dashboard box 4. Press the Load Button		Add a dashboard 1. Hover over the upper-left + button 2. Choose Import from the Create section 3. Enter 1756 into the Grafana.com Dashboard box 4. Press the Load Button

5. Under “Options Name”, Enter: UBNT EdgeRouter Dashboard 6. Under “Options Telegraf”, Select: Telegraf 7. Press the Import button The new dashboard should then be selected for you Under Choose Router, select: 192.168.3.1 If the dashboard is not selected, hover over the “4 squares” upper-left icon, and » then select Dashboard <dashboard name>. You should now be viewing your ER-X’s SNMP data graphs. You can change the time scale of the graphs by clicking on the upper-right clock » icon.		5. Under “Options Name”, Enter: UBNT EdgeRouter Dashboard 6. Under “Options Telegraf”, Select: Telegraf 7. Press the Import button The new dashboard should then be selected for you Under Choose Router, select: 192.168.3.1 If the dashboard is not selected, hover over the “4 squares” upper-left icon, and » then select Dashboard <dashboard name>. You should now be viewing your ER-X’s SNMP data graphs. You can change the time scale of the graphs by clicking on the upper-right clock » icon.
Page 131 of 136 » 2/4/2019	<>	Page 152 of 157 » 5/18/2019
==========	=	==========
Appendix C - Part 2 At some point, I was having occasional network problems and suspected dns as the » root problem. Here are some additions to the above grafana setup. This portion will graph pinging times to web servers, which will test internet » access. Per https://grafana.com/dashboards/2690 Append the following to your telegraf.conf: (You may want to add separator comment line(s) between the sections.) [[inputs.ping]] interval = "60s" urls = ["amazon.com", "github.com", "google.com" »] count = 4 ping_interval = 1.0 timeout = 2.0 Restart telegraf sudo systemctl restart telegraf.service Test new telegraf entry (this is one long command line) telegraf --config /etc/telegraf/telegraf.conf » --config-directory /etc/telegraf/telegraf.d --input-filter ping --test After a few seconds, you should see 3 "> ping" lines. Add a dashboard 1. Hover over the upper-left + button 2. Choose Import from the Create section		Appendix C - Part 2 At some point, I was having occasional network problems and suspected dns as the » root problem. Here are some additions to the above grafana setup. This portion will graph pinging times to web servers, which will test internet » access. Per https://grafana.com/dashboards/2690 Append the following to your telegraf.conf: (You may want to add separator comment line(s) between the sections.) [[inputs.ping]] interval = "60s" urls = ["amazon.com", "github.com", "google.com" »] count = 4 ping_interval = 1.0 timeout = 2.0 Restart telegraf sudo systemctl restart telegraf.service Test new telegraf entry (this is one long command line) telegraf --config /etc/telegraf/telegraf.conf » --config-directory /etc/telegraf/telegraf.d --input-filter ping --test After a few seconds, you should see 3 "> ping" lines. Add a dashboard 1. Hover over the upper-left + button 2. Choose Import from the Create section

3. Enter 2690 into the Grafana.com Dashboard box 4. Press the Load Button 5. Under “Options Name”, Enter: Ping Monitor 6. Under “Options Telegraf”, Select: Telegraf 7. Press the Import button As written, this dashboard seems to have trouble displaying the data sometimes. The following edits seem to help: 1. Select the Ping Monitor dashboard. 2. Hover over the “Ping Average Response Time” title, and then click on the » down caret which appears. 3. Choose Edit 4. Ensure you have the Metrics Tab selected (in the middle of the screen) 5. Go to the line GROUP BY time($_interval) tag(url) fill(null) and click on the word ‘null’, select ‘none’ from the list, as in: GROUP BY time($_interval) tag(url) fill(none) Click on the X, which is to the right of all of the graph tabs, to exit » editing. Press the Save Dashboard button, which looks like a floppy icon, at the top » of screen.		3. Enter 2690 into the Grafana.com Dashboard box 4. Press the Load Button 5. Under “Options Name”, Enter: Ping Monitor 6. Under “Options Telegraf”, Select: Telegraf 7. Press the Import button As written, this dashboard seems to have trouble displaying the data sometimes. The following edits seem to help: 1. Select the Ping Monitor dashboard. 2. Hover over the “Ping Average Response Time” title, and then click on the » down caret which appears. 3. Choose Edit 4. Ensure you have the Metrics Tab selected (in the middle of the screen) 5. Go to the line GROUP BY time($_interval) tag(url) fill(null) and click on the word ‘null’, select ‘none’ from the list, as in: GROUP BY time($_interval) tag(url) fill(none) Click on the X, which is to the right of all of the graph tabs, to exit » editing. Press the Save Dashboard button, which looks like a floppy icon, at the top » of screen.
Page 132 of 136 » 2/4/2019	<>	Page 153 of 157 » 5/18/2019
Perform the same change as above i.e. “fill(null)” -> fill(none)”, for the “Packet » Loss Percentage” graph. You should start collecting data. A portion of the screen should eventually look » like Figure 170 – Example Grafana Ping Monitor Portion. Figure 170 – Example Grafana Ping Monitor Portion	=	Perform the same change as above i.e. “fill(null)” -> fill(none)”, for the “Packet » Loss Percentage” graph. You should start collecting data. A portion of the screen should eventually look » like Figure 170 – Example Grafana Ping Monitor Portion. Figure 170 – Example Grafana Ping Monitor Portion
Page 133 of 136 » 2/4/2019	<>	Page 154 of 157 » 5/18/2019
========== Appendix C - Part 3 This portion will graph dns queries made to multiple dns resolvers. Per https://github.com/influxdata/telegraf/tree/master/plugins/inputs/dns_query Append the following to your telegraf.conf: (You may want to add separator comment line(s) between the sections.) # Dns Query Config: [[inputs.dns_query]] ## servers to query servers = ["192.168.3.1", "209.244.0.3", "8.8.8.8",	=	========== Appendix C - Part 3 This portion will graph dns queries made to multiple dns resolvers. Per https://github.com/influxdata/telegraf/tree/master/plugins/inputs/dns_query Append the following to your telegraf.conf: (You may want to add separator comment line(s) between the sections.) # Dns Query Config: [[inputs.dns_query]] ## servers to query servers = ["192.168.3.1", "209.244.0.3", "8.8.8.8",

```
» "9.9.9.9"           ]
       ##  Network      is  the    network     protocol       name.
       network       = "udp"
       ##  Domains      or  subdomains        to  query.
       domains       = [  "amazon.com",        "github.com",         "google.com"
» ]
       ##  Query      record     type.
       ##  Posible      values:       A,   AAAA,  CNAME,      MX,   NS, PTR,
» TXT,  SOA,          SPF,  SRV.
       record_type        = "A"
       ##  Dns      server  port.
       port      =  53
       ##  Query      timeout     in  seconds.
       timeout       = 2
Restart telegraf
      sudo  systemctl       restart      telegraf.service
Test new entry (this is one long command line)
      telegraf       --config     /etc/telegraf/telegraf.conf
» --config-directory
/etc/telegraf/telegraf.d            --input-filter          dns_query     --test
You should see 12 "> dns_query" lines.
Create a new Dashboard
      1. Hover over / click on the “4 squares” upper-left icon, then select
» Dashboards / Home.
      2. Hover over the upper-left + button, choose Create Dashboard
      3. Choose Graph
      4. Hover over the “Panel Title” title, and then click on the down caret
» which appears.
      5. Choose Edit
      6. Select General Tab under Graph
      7.In the Title box, enter:               ER-X Dns
      8. Select Metrics Tab under Graph
      9. Under Data Source, select:            Telegraf
      10: You should see a line which looks like:
                  “FROM default select measurement WHERE +”
                  Click on “select measurement” and choose “dns_query”
                  Click on the + sign and select “server”
                  Click on “select tag value” and select “192.168.3.1”, leave the
» “=” sign alone.
                  The line should now look like: “FROM default dns_query WHERE
```

```
» "9.9.9.9"           ]
       ##  Network      is  the    network     protocol       name.
       network       = "udp"
       ##  Domains      or  subdomains        to  query.
       domains       = [  "amazon.com",        "github.com",         "google.com"
» ]
       ##  Query      record     type.
       ##  Posible      values:       A,   AAAA,  CNAME,      MX,   NS, PTR,
» TXT,  SOA,          SPF,  SRV.
       record_type        = "A"
       ##  Dns      server  port.
       port      =  53
       ##  Query      timeout     in  seconds.
       timeout       = 2
Restart telegraf
      sudo  systemctl       restart      telegraf.service
Test new entry (this is one long command line)
      telegraf       --config     /etc/telegraf/telegraf.conf
» --config-directory
/etc/telegraf/telegraf.d            --input-filter          dns_query     --test
You should see 12 "> dns_query" lines.
Create a new Dashboard
      1. Hover over / click on the “4 squares” upper-left icon, then select
» Dashboards / Home.
      2. Hover over the upper-left + button, choose Create Dashboard
      3. Choose Graph
      4. Hover over the “Panel Title” title, and then click on the down caret
» which appears.
      5. Choose Edit
      6. Select General Tab under Graph
      7.In the Title box, enter:               ER-X Dns
      8. Select Metrics Tab under Graph
      9. Under Data Source, select:            Telegraf
      10: You should see a line which looks like:
                  “FROM default select measurement WHERE +”
                  Click on “select measurement” and choose “dns_query”
                  Click on the + sign and select “server”
                  Click on “select tag value” and select “192.168.3.1”, leave the
» “=” sign alone.
                  The line should now look like: “FROM default dns_query WHERE
```

» server = 192.168.3.1”		» server = 192.168.3.1”
Page 134 of 136	<>	Page 155 of 157
» 2/4/2019		» 5/18/2019
11. You should see a line which looks like:	=	11. You should see a line which looks like:
“SELECT field(value) mean() +”		“SELECT field(value) mean() +”
Click on “value” and select “query_time_ms”		Click on “value” and select “query_time_ms”
Click on “mean() and select Remove, click on the new + sign and		Click on “mean() and select Remove, click on the new + sign and
» choose max() under Selectors.		» choose max() under Selectors.
The line should now look like: “SELECT field(query_time_ms) max()”		The line should now look like: “SELECT field(query_time_ms) max()”
12. You should see a line which looks like:		12. You should see a line which looks like:
GROUP BY time($_interval) fill(null) +		GROUP BY time($_interval) fill(null) +
Click on the + sign, and select “tag(domain)”.		Click on the + sign, and select “tag(domain)”.
Select “null” and change into “none”		Select “null” and change into “none”
The line should now look like: “GROUP BY time($_interval)		The line should now look like: “GROUP BY time($_interval)
» tag(domain) fill(none)”		» tag(domain) fill(none)”
13. Leave the “FORMAT AS Time series line alone.		13. Leave the “FORMAT AS Time series line alone.
14. In the ALIAS BY box, enter: $tag_domain		14. In the ALIAS BY box, enter: $tag_domain
15. Select the Graph Axes Tab.		15. Select the Graph Axes Tab.
Under the Left Y group change the following:		Under the Left Y group change the following:
Y-Min auto to 0		Y-Min auto to 0
Y-Max auto to 100		Y-Max auto to 100
16 Click on the X, which is to the right of all of the graph tabs, to exit		16 Click on the X, which is to the right of all of the graph tabs, to exit
» editing.		» editing.
17. Press the Save Dashboard button, which looks like a floppy icon, at the		17. Press the Save Dashboard button, which looks like a floppy icon, at the
» top of screen.		» top of screen.
DNS data should start accumulating. We need a total of four panels, so we will		DNS data should start accumulating. We need a total of four panels, so we will
» duplicate this panel three times,		» duplicate this panel three times,
slightly editing each one.		slightly editing each one.
Duplicate Panel		Duplicate Panel
1. Hover over the “ER-X Dns” title, and then click on the down caret which		1. Hover over the “ER-X Dns” title, and then click on the down caret which
» appears.		» appears.
2. Select More, then select Duplicate.		2. Select More, then select Duplicate.
Modify New Panel		Modify New Panel
1. Hover over the NEW “ER-X Dns” title, and then click on the down caret		1. Hover over the NEW “ER-X Dns” title, and then click on the down caret
» which appears.		» which appears.
2. Select Edit.		2. Select Edit.
3. Select General Tab under Graph		3. Select General Tab under Graph
4.In the Title box, change: ER-X Dns to Level3 Dns		4.In the Title box, change: ER-X Dns to Level3 Dns
5. Select Graph Metrics Tab under Graph		5. Select Graph Metrics Tab under Graph
6. In the FROM line, select 192.168.3.1 and then select (change to)		6. In the FROM line, select 192.168.3.1 and then select (change to)

» 209.244.0.3 7. Click on the X, which is to the right of all of the graph tabs, to exit » editing. 8. Press the Save Dashboard button, which looks like a floppy icon, at the » top of screen. Repeat the above “Duplicate Panel” and “Modify New Panel” steps with the following » data: Title Google Dns server equals 8.8.8.8 Repeat the above “Duplicate Panel” and “Modify New Panel” steps with the following » data: Title Quad9 Dns server equals 9.9.9.9		» 209.244.0.3 7. Click on the X, which is to the right of all of the graph tabs, to exit » editing. 8. Press the Save Dashboard button, which looks like a floppy icon, at the » top of screen. Repeat the above “Duplicate Panel” and “Modify New Panel” steps with the following » data: Title Google Dns server equals 8.8.8.8 Repeat the above “Duplicate Panel” and “Modify New Panel” steps with the following » data: Title Quad9 Dns server equals 9.9.9.9
Page 135 of 136 » 2/4/2019	<>	Page 156 of 157 » 5/18/2019
My graphs eventually looked like Figure 171 – Example Grafana DNS Queries. How interesting!	=	My graphs eventually looked like Figure 171 – Example Grafana DNS Queries. How interesting!
I believe that I will need to investigate and adjust dnsmasq settings in the75 - » Adblocking and Blacklisting section.	<>	I believe that I will need to investigate and adjust dnsmasq settings in the77 - » Adblocking and Blacklisting section.
What I have seems to work, but is definitely non-optimal. Figure 171 – Example Grafana DNS Queries ========== Appendix C - Part 4 This portion may someday graph UniFi Access Point information, per the URLs given » in Part 1.	=	What I have seems to work, but is definitely non-optimal. Figure 171 – Example Grafana DNS Queries ========== Appendix C - Part 4 This portion may someday graph UniFi Access Point information, per the URLs given » in Part 1.
Page 136 of 136 » 2/4/2019	<>	Page 157 of 157 » 5/18/2019