4-6 Perry Street
PO Box 1662
Wapakoneta, OH 45895

Located in historic downtown Wapakoneta, Ohio, FNGi has been instrumental in developing and supporting Internet Networks across the U.S. since 1993. The FNGi team can assist you with all phases of your Internet Network from initial planning through long-term support.

www.network1.net
800.578.6381

FOCUS Newsletter

Welcome to 2020. Beginning this year, we wanted to take a look at a few new changes, including USB 4.0, WIFI 6 and custom web certificates with the DHCPatriot. Our CEO, Stephen Walter also reminds us about the necessity of continued power thru backup solutions and on-site generation.

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS January — March 2020

In This Issue

USB 4.0, here we go again ...

Ever heard of the USB Implementers Forum (USB-IF)? Chances are you have lived your life up until this point and never realized such an entity even existed. Obvious by its name, they are the group that decides the fate, follow through and future of the USB tech standard. And they are set to make some changes, once again.

Odds are you probably, only now, have a few devices that utilizes the USB 3 type-C connection as its primary source of power and data. And while we've had USB 3 in various capacities and form factors, the type-C interface really helped cement the concept that version 3 is here and is now the future.

Funny how time flies, because the USB-IF have published their specification for USB4. Beginning in 1996, USB as we've come to know it has been the largish Type-A, only fits one way, connector. Now over 20 years we have USB 3 Type-C and everyone's dreams were fulfilled with the universal style connector that can be plugged in via any orientation. However, our dreams will not be dashed, nor will we have to buy all new cables, yet again!

USB4 will operate on all Type-A and Type-C style plugs and be backwards compatible with USB3.x and USB2.x devices. The real difference is now it is also compatible with Thunderbolt 3. The Thunderbolt technology was designed and licensed by Intel exclusively for many years. It has always been a faster way of transferring files than USB, thankfully, that's finally changing now as USB and Thunderbolt finally unite. The current USB3.2 spec caps out at 20 Gbits per second, while Thunderbolt 3 tops out at 40 Gbit per second! The only trouble is that any device that wants to announce its USB4 will work with Thunderbolt 3 will still need to be certified by Intel. A fact which makes Thunderbolt the less common standard in the industry as it allows Intel to exert certain control in the mix.

USB4 will also feature USB3 Power Delivery technology with a peak capacity of 100w of electricity over the cable. It will also feature intelligent and dynamic bandwidth sharing. This will allow it to automatically adjust data rates to what is demanding it more at that time. An example might be a large file transfer to an external drive would take precedence over video frames being pushed to your monitor. This will squeeze every last bit of efficiency out of its new 40 Gbit speed abilities.

When will you see your first USB4 devices? This year, 2020. But like with other versions of USB it will take awhile to fully catch on, so you have plenty of time. At least the baby can stay in with the bath water since each new standard supports the last. That means you can keep the gear you like, longer - and that's a good thing.

FNGi
First Network Group Inc

From the Desk of *"The Network Guy"*

As winter marches on and we have long since said goodbye to the wind and water of summer's storms, the potential for extreme cold, snow and ice have now been brought to bear. Few industries have spent their history with the care and attention to power that has been a hallmark of Telecommunications. You have often been the only industry in town with power during a crisis. Yet "stuff happens" and we can find ourselves without backup power when we need it the most.

Testing is a great idea but needs to be done with a thorough analysis of one's systems and points of failure. First Network Group manually tests its automatic backup generator on a regular basis, and has found failures that could have been catastrophic in an emergency. But a glitch that was not found was caused by a weak 9 volt battery needed by the automatic transfer switch to engage the generator during a failure. To think of it another way: a $2 component failure crashed a system that was a mid-five-figure investment.

Since servers and routers have been added to the Telecom mix, many have been specified with DC power to use the industrial batteries and generators providing backup power to more traditional communications gear. Others have been outfitted with dedicated battery backup that will continue to power equipment until generators can come online. One important factor in this scenario is the batteries themselves, they have a limited lifespan. Sometimes replacing the backup units is a better value than replacing the batteries, especially when the replacement has newer or better technology. As a cost conscious CEO, this was a difficult lesson for me to learn. And it is worth noting that powering servers (including routers) can be more than keeping them online for the duration of the outage. A power backup failure during a fifteen minute outage can require hours to repair a corrupted server that crashed when it lost all power.

I encourage you to reassess your backup power infrastructure. First Network Group IT Services will be happy to help you evaluate your current deployment and support you in testing. Confidence in your backup power should let you provide a superior service this winter and ease your mind during those long winter nights.

Sincerely,

Stephen C. Walter
The Network Guy
Founder and President, First Network Group, Inc.

Wi-Fi 6 is Here

Does your laptop support 802.11n, 802.11ac, or 802.11a10? If you don't know you're in luck and if you didn't realize one of those protocols was not real, your life is about to get better.

The Wi-Fi Alliance, the body that sets all the standards and protocols for each for of Wi-Fi technology, is finally going to drop the archaic numbering and lettering scheme. The next revision of Wi-Fi will be known as Wi-Fi 6 (technically 802.11ax).

"For nearly two decades, Wi-Fi users have had to sort through technical naming conventions to determine if their devices support the latest Wi-Fi," said Edgar Figueroa, president and CEO of Wi-Fi Alliance. "Wi-Fi Alliance is excited to introduce Wi-Fi 6, and present a new naming scheme to help industry and Wi-Fi users easily understand the Wi-Fi generation supported by their device or connection."

The naming scheme will go backwards as well.

- Wi-Fi 6 to identify devices that support 802.11ax technology
- Wi-Fi 5 to identify devices that support 802.11ac technology
- Wi-Fi 4 to identify devices that support 802.11n technology

The Wi-Fi alliance has approved the new logos and descriptions of the naming system to be used by anyone meeting the standard (basically everyone).

And even though we are now past the big holiday shopping season, we've only seen a few of these products enter the market and be branded as such. Look for all of that to change as consumer network manufacturers begin their push to the new labeling standard in earnest now.

DHCPatriot & Custom Web Certificates

By the time you read this, version 6.4.0 of the DHCPatriot software will have been released. It may even be installed on your DHCPatriot system already. This release is mostly focused on DHCPv6 and the continuing goal of reaching feature parity with DHCPv4. We still have a ways to go, but I'd like to use this quarter's newsletter to discuss how far 6.4.0 brings us.

There are three major new features in this version. All are related to DHCPv6. The first is IP/prefix delegation usage numbers for DHCPv6 subnets. Numbers and percentages as well as graphs are now available in DHCPv6 (IPv6) -> View Address Usage very similar to the same in the DHCPv4 version of View Address Usage. These numbers are also available via SNMP. The second new feature is Simultaneous Use Restrictions in DHCPv6. Like DHCPv4, you can now set restrictions for how many devices a user can have online simultaneously (authenticated DHCPv6 only).

There is a global setting to set the limit for all users. Each individual user can have their limit individually controlled by using the Port-Limit RADIUS attribute (as is already the case in DHCPv4). The final new feature is the inclusion of using per shared network RADIUS server and Captive portal groups in DHCPv6 authenticated networks. This is useful if multiple user-bases must be served from separate RADIUS servers and/or a different Captive Portal screen must be shown to a specific network.

These settings are now chosen in the shared network settings screen under DHCPv4 and DHCPv6. The Captive Portal and RADIUS settings screens have been moved to the System Configuration menu since they are now more of a global group of settings. The RADIUS and Captive Portal groupings are created in their respective setup screens and then chosen in the respective DHCPv4 and DHCPv6 shared network configuration screens. During install, the existing DHCPv4 entries are automatically configured properly. We are getting close to feature parity with DHCPv4 and DHCPv6 and will continue to work toward this goal in future releases.

In this version, there have also been several security enhancements aimed at preventing cross site scripting attacks as well as clickjacking mitigations. Not that anyone was targeting the DHCPatriot system for such attacks, but just to attempt to keep those things from happening in the future. There is more to do and we will be working on this more in the future. A side effect of the changes related to securing the login cookie causes Microsoft Edge to no longer work with the various popup windows unless a valid certificate is installed on the DHCPatriot system.

In other words, if there is an invalid (or the provided self-signed) web certificate, on the DHCPatriot system, then Microsoft Edge will lose the cookies in any popup windows and not be able to show the contents of the popup windows. Other browsers (such as Chrome and Firefox) will still show the popup windows correctly with an invalid web certificate. Microsoft Edge will properly show the popup windows if a valid web certificate is installed. A valid web certificate may be installed in System Configuration -> Custom Web Certificate.

— Darren Ankney
dankney@network1.net
1-800-578-6381 x8171