FNGi
First Network Group Inc

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

FNGi
First Network Group Inc

FOCUS Newsletter

Summer is in full force. The sun is bright, the air is warm and the top is down on the car. Which isn't very private, but it’s much better than the latest privacy issues with used smart car.

We also look at the connected home and how the new EasyMesh standard will allow you to mix and match Wi-Fi routers.

FOCUS

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS July — September 2018

In This Issue

Update Your Heart

Mixing technology and our own bodies and health is becoming more prevalent. Thankfully while your own heart do not require software updates, a pacemaker and/or defibrillator just might!

In April, the US Food and Drug Administration (FDA) approved a firmware patch for pacemakers and implanted cardiac defibrillators made by Abbott (formerly St. Jude Medical).

If you or a loved one has one of these implantable devices, it’s extremely important to verify the manufacturer and if it was designed or crafted by Abbott (formerly St. Jude Medical). If so, the device may require this patch to continue to work correctly. Contact your cardiologist or family doctor and discuss your options and concerns.

The patch corrects a potential issue with the software that could allow the device to be altered incorrectly, accidentally or maliciously, via a radio frequency signal that could render the battery inoperable. It’s also important to note that there are no known cases of this happening, but the low level of encryption that is currently deployed on these devices still make it a high risk and very necessary update.

Thankfully, the software update process is very simple and has been thoroughly tested and confirmed by the FDA. It should only require a simple visit to your cardiologist or local hospital and take roughly 3 minutes to complete. The FDA is also reporting a very low rate of unsuccessful updates (0.62%), however work is being done to further improve this number.

Action items:

- Consult your physician(s) to determine when you should receive the firmware update and if you have any questions or concerns about the update. Your ongoing medical management should be based on your own medical history and clinical condition.

- If you receive the update and your device is affected by the Battery Advisory, contact your physician immediately if your vibratory alert is triggered to check that the alert is due to premature battery depletion. If it is, you will need to schedule a device removal and replacement procedure.

- Visit www.sjm.com/notices, or contact Abbott's hotline at 1-800-436-5056 for additional information, or if you have any questions or issues regarding your Abbott/ St. Jude Medical implantable cardiac defibrillator.
- Websites:

FDA: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm

From the Desk of Stephen Walter

Twenty years ago, the idea of the "connected home" was presented at Internet conferences across the country. Blacksburg, VA was being hailed as a leading edge connected community and the thoughts of how consumers and developers would use that connectivity - beyond email - ranged from modest proposals from the rise of home offices to a Jetson-like home where everything was connected.

Fast forward to 2018 and my own home has dozens of connected devices. Cell phones, tablets and computers for sure. On the audio/video front, our (smart) TVs, disk players and receivers and wireless speakers are all connected, as well as Roku video streamers and a home brew PLEX Media Server (built on a single board computer). Smart outlets online provide security and smart switches conserve electricity and control lighting. Our digital Wi-Fi thermostat runs on a schedule and can be reset or rescheduled by app from phone or tablet. Amazon's Echo (Alexa) integrates with many of those devices, and answers basic questions, plays music, news updates, and my local Public Radio station (via TuneIn). We also have multiple cameras with 2 way audio and 360 degree pan plus tilt, all that can be easily controlled from a phone or tablet - and sends pictures if the motion or sound detection is tripped while we are gone.

There are plenty of connected devices we don't have. I've seen ads for connected laundry equipment, refrigerators and all manner of connected appliances. One of the most ingenious applications for smart home technology may be Amazon's "dash button." Dash buttons are product specific (Tide, for example) Wi-Fi connected buttons that will reorder the product from Amazon at a simple press of the button. Stick one on your washing machine and press it when you are running low on soap. A convenience for the consumer and a great sales tool for the vendor.

In fact, the only member of our family who isn't connected is … our dog. There are plenty of devices to connect him! Pet specific IP cameras, remote controllable feeding stations, and at least one unit that combines the two. I've read about toys that can be remotely controlled over the net. Hmm, I wonder if that is another home-brew project I should put on my list.

The important part, I think, are the pieces that we take for granted. Our phones switch from cellular to Wi-Fi and we never think about it. Demand for streaming media may drive the hunger for more bandwidth but it is already clear that so much of so many households are connected that the availability and reliability of home Internet service are critical to modern the American home. The Jetsons? Maybe not yet, we still don't have Rosie (the robotic maid) in our home, maybe next year.

- Steve

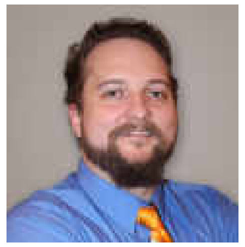
EasyMesh Wi-Fi Standard

In the last few years there have been many new routers on the market that create an at-home mesh network. If you are not familiar with the concept of mesh routers, think of them as a pack of mini routers that all seamlessly connect to each other and can be placed in multiple areas of your home. You can even add more later as the need arises. This greatly increases the quality of the wireless signal in your home and specifically where you need it the most.

Until now though, if you bought a mesh router setup from one manufacturer, you were stuck with that type of router from there on out. If you owned Google Wi-Fi mesh router and found a sale on individual Eero routers, you were out of luck.

To combat this issue and even the playing field, the Wi-Fi Alliance has announced the EasyMesh standards program. This will allow all EasyMesh compliant routers to talk to each other regardless of the manufacturer. They will all work together just as seamlessly as if they were both built by the same manufacturer. Look for the EasyMesh certification logo on networking gear coming later this year and early 2019.

Cory's 20th Anniversary



Over the summer, another one of our employees has celebrated their 20 year anniversary with the company!

Congratulations to Cory Lykins for reaching this milestone!

"It's been an amazing opportunity to work with everyone thru the years and see technology grow to where we are now. I want to thank every colleague I've ever had, every customer and every caller that I've ever helped over the years. My team is amazing and I wouldn't be who I am or where I am without their guidance, assistance, and friendship through the years. Thank you." - Cory Lykins

A Look at DHCPv6 Support

In the new version of the DHCPatriot software, 6.2.0, we have introduced DHCPv6 Authentication. As with IPv4, the DHCPatriot supports captive portal authentication via IPv6 as well. However, if you don't plan on using the captive portal login process user devices can still be logged and tracked without authentication in DHCPv6.

In DHCPv6 there are two options that could be used for identification purposes. First, there is option # 18 "Interface-Id" (RFC 3315 section-22.18). This option can contain an interface ID of some sort that can be used to identify a subscriber through plant records. This option will only exist if the relay agent added it to the packet. This is similar to option 82 sub-option 1 "Circuit-Id" from DHCPv4.

In DHCPv6, it is specified in RFC 3315 that the server may use the contents of option 18 to assign parameters which means in practice that the option will likely be plain text (even though it is considered an opaque value). This is a better situation than we had in DHCPv4 where the value of option 82 sub-option 1 could be plain text or binary. Second, we have option # 37 "remote ID" (RFC 4649).

This option is similar to option 18 in that it is added by the relay agent, it may be used by the DHCP server to assign parameters, and it should be considered an opaque value. There is one difference, however, which is the enterprise id portion. The option is vendor specific and thus will contain vendor specific data. The data may be binary or plain text.

As such, it would be hard to use this as an identifying key for a session. This option is similar to Option 82 sub-option 2 "Remote ID".

If either of these options are present, and plain text (ASCII), the DHCPatriot will record these options with the user device's session. When viewing these sessions in the DHCPatriot web GUI, clicking the 18/37 link will show a popup with the gathered 18 and 37 information if any. This information, in conjunction with some sort of plant records, should allow you to identify the subscriber in question.

Used Car Privacy

Our cars are becoming smarter every year, which has been both a blessing and a curse. Up until now the curse has only seemed to be all the extra buttons, features and options that could make driving a little more complicated than most people really need on their day-to-day use.

One feature that is hard to live without is Global Positioning Systems (GPS) as an option. In car navigation based on the car's own GPS position has become nearly indispensable for may of us. These systems can also be used to help track thieves or even find your car in a large parking lot. But this technology has also opened up a potential privacy hole in the entire experience.

Ashley Sehatti discovered this when she recently sold her 2015 Volkswagen Jetta back to a dealership in California. Her Jetta included features that would email her monthly health reminders, such as how long till her next oil change, current mileage, etc. The trouble is when Volkswagen Car-Net services continued to email her even after she sold the car.

She dismissed them as simple junk until she received one of these emails that displayed the current location of her old car. She realized she could fully access the car's features thru the software just like when she owned it. And while most of these systems are benign enough that only allow you to remotely honk the horn or flash the lights, she was able to know the car's exact location at any time.

She assumed, like most would, that selling your car would clear its smart data - especially if you sold it back to a dealer. This is not the case. According to Volkswagen (Car-Net) and GM (OnStar) it is up to the seller to disconnect themselves from these services. Volvo (On Call) operates on the notification they receive that the car has been sold and cancels their service for the seller. But that only works if you sell your car back to a dealer. Any automatic protections will only kick in if you sell your vehicle to a dealer. If you sell your car to a 3rd Party it's entirely up to you to make sure you are disconnected.

Something to keep in mind when purchasing a newer used car with smart features. The manufacturer should be able to confirm if there's an active account and service under someone else's name and if they are able to disable that. And if you plan on selling your car, just like your cell phone or computer, it's up to you to make sure it's clear of your data and accounts.