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 FOCUS Newsletter

In this edition we are well into summer and celebrating our 25 years in business and serving more and more customers across the country from our small Ohio town of Wapakoneta. We're going to talk about securing Smart TV's, keeping your data and network up 99.999% of the time, the future of the DHCPatriot with more IPv6 news.

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS July — Sept 2020

In This Issue

25th ANNIVERSARY

FNGi 2020, 25 Years and Beyond

Greetings to all of our valued friends, customers, clients, and compatriots. Given that I write this during the ongoing coronavirus pandemic, I start with our highest hope that you and yours are well and continue to be!

July 2020 will mark the 25th anniversary for First Network Group, Inc. It has been an honor and privilege to serve you and we look forward to serving your needs for the next 25 years. From our changes among Ohio and Wisconsin Telcos who have been with us since the early days, to turning up a DHCPatriot in Iraq as part of U.S. efforts in that region, to COVID-19, it has been an interesting year so far, to say the least. I could not be more proud of our staff who has demonstrated the agility with which we were founded as they successfully migrated to a work from home model, implementing that section of our "crash plan" ensuring our operational continuity and yours.

I founded FNGi on the premise that commercially available Internet Service needed support services that were professional, responsive and agile, something that was not common in the Internet that was based in Higher Ed. and Community Non-profits back in the day. Since then, we have extended our services - especially our Call Center - to serve your other and growing needs. Be that processing Customer Service calls for your Telephone and CATV, or other service offerings, even processing your customer's payments when needed, or handling your Lawful Intercept calls. You added Cellular Service. We added support for it. You moved from dialup to broadband and we added support for it. You will soon offer something currently and completely unknown and yes, we will support it.

The most important thing to us is that we were here then, we are here now and we will be here tomorrow. Yes, our employees are currently working from home, something we trust has been seamless for you and your customers. Working from home safeguards our employees from unnecessary health risk that could make them unavailable to serve you. As always, we do what it takes when it is required, to provide you with the highest quality service. We are operating with a "business as usual" mindset, which for us means expecting the unusual. If you find yourself in need of additional services, please do not hesitate to ask. If you have a need, we may already be providing that service for one or more of your peers. If you need us to provide extra depth for you, we are here. If you need to expand coverage, we are here. If you need support for a new product rollout, we are here.

It has been our deepest honor to serve you for the last 25 years, and God willing, 25 more. Wishing you health, success and prosperity.

Sincerely,

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

Securing Smart TV's

Printed with attribution.

Yes, I said your TV. Specifically your smart TV...the one that is sitting in your living room right now. Or, the one that you plan to buy on super sale on Black Friday.

Smart TV's are called that because they connect to the Internet. They allow you to use popular streaming services and apps. Many also have microphones for those of us who are too lazy to actually to pick up the remote. Just shout at your set that you want to change the channel or turn up the volume and you are good to go.

A number of the newer TV's also have built-in cameras. In some cases, the cameras are used for facial recognition so the TV knows who is watching and can suggest programming appropriately. There are also devices coming to market that allow you to video chat with grandma in 42" glory.

Beyond the risk that your TV manufacturer and app developers may be listening and watching you, that television can also be a gateway for hackers to come into your home. A bad cyber actor may not be able to access your locked-down computer directly, but it is possible that your unsecured TV can give him or her an easy way in the backdoor through your router.

Hackers can also take control of your unsecured TV. At the low end of the risk spectrum, they can change channels, play with the volume, and show your kids inappropriate videos. In a worst-case scenario, they can turn on your bedroom TV's camera and microphone and silently cyberstalk you.

TV's and technology are a big part of our lives, and they aren't going away. So how can you protect your family?

- Know exactly what features your TV has and how to control those features. Do a basic Internet search with your model number and the words "microphone," "camera," and "privacy."
- Don't depend on the default security settings. Change passwords if you can – and know how to turn off the microphones, cameras, and collection of personal information if possible. If you can't turn them off, consider whether you are willing to take the risk of buying that model or using that service.
- If you can't turn off a camera but want to, a simple piece of black tape over the camera eye is a back-to-basics option.
- Check the manufacturer's ability to update your device with security patches. Can they do this? Have they done it in the past?
- Check the privacy policy for the TV manufacturer and the streaming services you use. Confirm what data they collect, how they store that data, and what they do with it.

As always, if you have been victimized by a cyber fraud, be sure to report it to the FBI's Internet Crime Complaint Center at www.IC3.gov or call your local FBI office.

Beth Anne Steele
Public Affairs Specialist / Media Coordinator
Portland Oregon FBI

Uninterruptible Operation

The past few months have shown us that unexpected events can prove challenging to continuous business operation, particularly for ISPs, telcos, and other critical infrastructure providers. Many companies are now reevaluating their procedures and infrastructure setup to ensure their operations continue no matter what circumstances arise.

One of the major focuses recently has been on working from home as much as possible. The main component that allows that to operate smoothly and securely is a Virtual Private Network (VPN) connection. A centrally-managed VPN solution can be critical in securing your systems and data, while providing the flexibility for users to connect from wherever they are. Advanced features like Active Directory integration, security policy enforcement, and configurable network permissions and routing are just a few of the powerful tools available with more advanced systems.

We can work with you to implement the appropriate VPN hardware and software to achieve the required level of connectivity for remote workers without the headache of setting it all up yourselves dealing with substandard, unstable, and difficult to configure alternatives.

In addition to new challenges with regard to where employees are working, we have also noticed an increased demand in making sure networks, servers, and other infrastructure are as fault-tolerant as possible. This includes redundant networking, secondary sites for disaster recovery, and much more. Remote management, out-of-band access, multi-tiered backup systems, and secondary cloud hosting are further examples of items that we deal with every day. First Network Group is your source for rock solid, carrier-grade equipment and software to achieve the resiliency required.

By reducing the need for site visits to deal with IT issues, we can make it easier for your local employees to work without being interrupted and having to travel around as much. That is a great thing for everyday operations in addition to unique situations that call for quarantine or isolation.

As you may know, we also operate a fully-staffed 24/7/365 call center that can field calls from customers for a wide range of issues from customer service, triage, and technical support for internet, phone, TV, and pretty much anything else. Free up your employees to do more critical duties while providing your customers with even better service.

Let First Network Group assist you with all of that! Together, we can work to provide the best possible service to your customers.

Randy Carpenter
VP of IT Services
1-800-578-6381, option 1.

DHCPatriot in 2020

It is 2020 and we are seeing more of our customers start to add IPv6/DHCPv6 to their DHCPatriot systems. Even more should be starting to migrate. With that in mind, we thought it was worth sharing some information about the basics of DHCPv6 that was first published in 2012. Our hope is that this will help even more of our customers begin to migrate to DHCPv6 on their DHCPatriot systems.

IPv6 offers many ways of assigning addresses to network connected equipment. These methods consist of statically entering address information on the interface, Stateless Automatic Address Configuration (SLAAC), Point to Point Protocol over Ethernet (PPPoE), and Dynamic Host Configuration Protocol version 6 (DHCPv6). The focus of this article will be an overview of DHCPv6.

Most current clients that support IPv6 will have at least two modes of operation that can be set: manual and automatic. When a client is set to automatic, it uses information received from the router via a Router Announcement (RA) to determine which method should be used to configure an IP address on the client's connected interface.

At this point, the client has already established communication with the link local network. The link local network is a special network that each host becomes a part of just by having IPv6 enabled. Addresses are created based on the MAC address on the connected interface of machinery connected to the network. Machinery on the local network can communicate with each other via these addresses. The gateway for the client will be set to the router's link local address.

The router, if configured as such, will tell the client to get its address via DHCPv6. The client will then ask the DHCP server for an address via a special local multi-cast address (To simplify we will assume a local DHCP server). The DHCP server will give the client an address to use for a specified time range.

The client, if it needs to provide addresses to equipment connected to it on another interface (example: a customer's home router), may also ask for a prefix delegation. Prefix delegation refers to assigning a subnet to be used by a router on their local inside LAN network for connected devices on that network. This is necessary as one-to-many NAT is no longer available in IPv6 and all equipment that needs Internet access must have a globally routable (in IPv4 language a "public") address.

The DHCPatriot can provide the above services. In addition, it can track sessions for both the allocated IPv6 address, as well as a prefix delegation, thus tying the address or prefix to a specific subscriber. It can do this either via circuit id (option 18 in DHCPv6 was option 82 sub option 1 in DHCPv4) or via captive portal authentication. We continue to improve the DHCPv6 support in the DHCPatriot system with each software release.

Darren Ankney
VP of Product Development
1-800-578-6381, option 3.

Top 20 Products with the Most Technical Vulnerabilities Over Time

1999 to 2019		2019	
Debian Linux	3,067	Android	414
Android	2,563	Debian Linux	360
Linux kernel	2,357	Windows Server 2016	357
Mac OS X (Mac OS)	2,212	Windows 10	357
Ubuntu	2,007	Windows Server 2019	351
Mozilla Firefox	1,873	Adobe Acrobat Reader DC	342
Google Chrome	1,858	Adobe Acrobat	342
iPhone iOS	1,655	cPanel	321
Windows Server 2008	1,421	Windows 7	250
Windows 7	1,283	Windows Server 2008	248

Source: National Institute of Standards and Technology's National Vulnerability Database