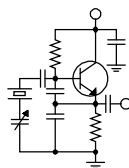


The Local Oscillator



The Newsletter of Crawford Broadcasting Company Corporate Engineering

OCTOBER 2026 • VOLUME 36 • ISSUE 10 • W.C. ALEXANDER, CPBE, AMD, DRB EDITOR

Well Done!

As you are reading this, the FCC's new cybersecurity rules are in effect, and I am pleased to say that we are fully compliant across the company. Those new rules are contained in just a few sentences and offer very little in the way of detail, but the intent is clear: protect EAS and protect other parts of the broadcast infrastructure from cyber-mischief. How we achieve that is largely up to us, but good engineering practice mostly dictates the methods.

We've talked a lot about this subject in recent issues of these pages, and I won't revisit the issue in any substantial way this month, but I do want to say one thing: I am proud of our engineering team across the company for figuring all this out and making it happen.

Birmingham chief engineer Todd Dixon served as team leader on the project, figuring out how to create VPN tunnels from our studio firewalls to our transmitter site firewall/routers. Amanda Hopp worked closely with Todd, implementing the changes not only at the five Denver-area transmitter sites but also at our California studios and transmitter sites. Rick Sewell and his crew figured things out in Chicago and Rockford. Mike Kernan, who is partial to Ubiquiti UniFi hardware, worked with Todd to figure things out with that gear in Detroit. Bill Stachowiak and Josh Myers had no issues getting tunnels set up at all the New York sites, and of course Todd Dixon and Jack Bonds led the way with their own network in Alabama.

None of this process was "plug and play;" every site required considerable work to change the local network to a unique scheme, every site required

some experimentation and tweaking to get things working properly, and frustration came in abundance at no additional charge with the new routers. I am proud of every one of you for not giving up and working through the issues.

So now we move on in this brave new (and for the moment, anyway,) cybersecure world. I am certain that maintaining compliance will be a moving target going forward, one that will challenge our people at every turn, but I am equally confident that our team is up to the task. Well done, guys (and gal)!



Legislative Stuff

There was some good news last month out of Washington with the passage of the AM Radio for Every Vehicle Act in the house of representatives. Moving that bill across the finish line in the house was a huge step and a big victory for broadcasters. Now it needs passage in the senate, and as I understand it, it has enough bipartisan support to be filibuster proof in that body, so it would seem it's down to scheduling and procedure at this point. President Trump has indicated he will sign the bill if it is passed.

There are lots of good reasons to keep AM reception available in automobiles, not the least of which is the wide-area coverage and AM's role in the nation's emergency information dissemination. Historically and continuing into recent years and events, it has been the big-gun AM stations that have been the go-to source for information during emergencies in our big cities. In smaller and rural communities, often AM stations are the only outlets, and if people can't receive those stations, they will

miss out on a primary information source. FM translators paired with the AM parent station only go so far, but the AM stations cover a much wider area.

The passage of the act in the house did come with a compromise, namely an eight-year sunset rather than the ten years in the original bill. I think that's reasonable, and the reality is that with the high cost of new cars these days, people are keeping them longer anyway, so eight years represents a longer period than is apparent. Some sources indicate that the average age of passenger vehicles is 12 years.

As I understand it, the bill would give DOT one year after enactment to issue its AM rule. The AM radio requirement would generally become effective no more than two years after that rule is issued, although smaller manufacturers that produced less than 40,000 passenger vehicles for U.S. sale in 2022 would receive at least four years. For now and up until the mandate takes effect, vehicles sold without AM would need to carry a clear disclosure indicating that there is no AM reception, and dealers and manufacturers could not charge an additional fee for AM access.

So now we wait for senate passage, and the clock starts ticking.

One other legislative item that got a lot of press a few months ago and will no doubt again rise to the surface in the coming weeks is the Sunshine Protection Act, which proposes to make daylight time permanent year-round. This is one of those things that initially sounds really good but upon closer examination has some problems. For the moment, the bill is stalled in the senate, and it's my hope that it will die there.

The big impetus for this bill is the inconvenience of changing our clocks twice a year. That is a PITA for sure, but in my experience it is less so than in years past. In my homes, most of the clocks are WWVB synchronized, so they update automatically. Even clocks that are not WWVB synchronized somehow have tables in their firmware that makes the DST adjustments automatic. So it's down to my wristwatch, stove and microwave oven.

What works against it is that in winter months the sun would not rise until after 8:00 AM in many locations. Here in Colorado where I live, in December and January, local sunrise would not occur until 8:15 AM! That means that school kids would be going to school in the dark, which is definitely a problem for those who walk or bike to school and would also impact those who wait for a bus to pick them up. Not good.

For many AM broadcasters, staying on DST year-round would likely be fatal. Daytime stations

would not be able to go on the air or power up until morning drive was for all intents and purposes over, and even many of those that operate 24 hours would have to stay on reduced nighttime power/patterns until that time.

Proponents argue that those AM stations would be compensated with an extra hour of operation or on day power/pattern in the evenings, but that's no compensation at all. Morning drive is where it's at; afternoon drive is secondary at best.

It's my belief that should the Sunshine Protection Act become law, there would be a lot of "civil disobedience" on the part of affected AM broadcasters. It would be a matter of survival for them, so they really wouldn't have a choice. It would be my hope that the FCC would make allowances for affected stations to keep to their old schedules during the short-day months, but since international treaties are involved, the agency's hands may be tied. My guess is that they would simply look the other way while affected stations did what they had to in order to survive.

Where this legislation will go is anyone's guess at this point. The president is very much in favor of it, and it has strong support in the house. We will be watching it closely.

Invisible Engineers

I recently read a really excellent article in *Radio World* by Rojith Thomas, the technology coordinator for KUT Public Media in Austin, Texas. The gist of the article was that the technical team – the broadcast engineers – behind what listeners hear on the air, on the stream or in the podcast, is invisible under normal circumstances, and rightly so. A few key points from the article:

- "Radio engineering used to mean transmitters, antennas and studio gear. That work hasn't gone away, but now it's maybe a third of the job." *Can I get a witness?*
- "A [radio] station isn't really an RF operation anymore. It's a technology company that happens to broadcast." *Precisely.*
- "The best engineering work is the kind no one ever hears about." *Spot-on!*
- "An engineer can take on more infrastructure, lead bigger projects and become indispensable to station operations, and still have no defined path to the next title." *Sad but true in most cases.*

The article dealt with the thin pipeline of up-and-coming engineers, and that's a real thing that the SBE and the industry as a whole has recognized but has yet to address in any meaningful way (but not for lack of trying). It's certainly a concern that I have.

I love the concluding paragraph: "Most listeners will never know an engineer's name. Most

will never see the systems keeping their favorite station on air. But the reliability they take for granted, the app that loads instantly, the stream that never buffers, the signal that comes in clean in a moving car, has someone's fingerprints all over it." Couldn't have said it better myself!

The New York Minutes
by
Bill Stachowiak
Chief Engineer, CBC – Western New York

Greetings from Buffalo!

We installed a replacement transmitter at the WLGH transmitter site. We knew this was supposed to happen this summer, but we weren't sure if it really would.

We had some serious problems with the 30-year-old Continental transmitter, which brought this project more into the foreground. Josh and I were excited to hear that a brand new Nautel NV10^{LT} had been ordered for the station.

This project had many hurdles that required careful planning to make sure the project would precede with no obstacles. Josh and I sat down to do some brainstorming to come up with what we thought was a viable plan.

We decided it would be best to have the transmitter delivered to Buffalo so that it would be in our possession and we could deliver it ourselves to the Rochester FM transmitter site when we could accommodate it.

The second hurdle was getting the Continental out of the building. Fortunately, WDCX has a tractor and trailer that we could use to move both transmitters. The tractor is equipped with a forklift that we could use to pick up the Continental.

We couldn't move the Continental until we removed a wall-mounted rack that housed the WDCX translator and some other ancillary equipment. We moved all this equipment to a different rack that was already installed but not utilized.

There was a patch panel mounted to the top of the Continental that we had to support from the ceiling. There was a work bench that had to be

moved as well. Our plan evolved to accomplish all these tasks.

A few weeks before the big day, we started preparing for the install. Josh and I went to the transmitter site, disconnected the Continental and used a hydraulic jack to move the transmitter into the walkway so that we could move it out of the building.

The next day we met Brett Larson at the WDCZ site to load the new transmitter onto the trailer for transport.

We were able to get the Continental out of the Rochester transmitter building and the new transmitter in place as planned without any problems.

Josh and I went back the next day and got everything connected. We put it on the air the following day without any problems.

Any time I am involved in a project that requires a lot of planning, I try and imagine myself at the project site doing the project. I will try and figure out exactly what I will need to see the project through completion. The last thing you want to happen is to run into some unexpected problems the day you are trying to get the project done.

In the case of this project, everything went according to plan because all of us involved had several meetings and eventually came up with a plan that we knew would work. We created a checklist to make sure we had all the materials available on site when we needed them.

I hope you enjoy the project photos on the following pages.

That's all for now. See you next time.



The Local Oscillator
October 2026



Taking delivery...



Removing the old Continental



The tractor sure helped!



The translator wall rack.



The new translator rack.



Old transmitter-mounted patch panel.



New suspended patch panel.



NV10^{LT} installed!



RF plumbing.

The Motown Update
by
Mike Kernan, CPBE
Chief Engineer, CBC–Detroit

Wanna get some Pi?

The Raspberry Pi and its clone and knock-off devices have made more than a few inroads in the Crawford engineering environment. I've written about Stephen Poole's latest exploit of this technology before, and I'll let him tell you about his update to it (should we call it version 1.1?) which adds some features to better get operator's attention.

Having the new Stephen Poole designed "Nauga" event monitor up on the wall for about a month was just enough for the Python program's host Raspberry Pi 4 to roll over and die. Cris quickly sent me a replacement, which is working as intended, but we began to suspect that the unit fried from too much heat. I applied the kit's two included heatsinks to the chips, but the GPIO breakout connector prevents the case from being completely assembled, and therefore the case fan is negated.

Cris and Amanda discovered their Pi's CPU was running at 60C and while that's below the specifications maximum of 85C, it still seems way too hot. CPUs can malfunction or fail from too much heat and of course no one wants to buy a new Pi 4 every month or two.

I had Cris order a larger case, which will allow me to use the GPIO connector breakout AND it has a fan.



Hyper-V and U, U, and You

Detroit's network has been slowly converted over the last 6 years to Ubiquiti's UniFi platform. It's slick, unified (as the name suggests) and very much the backbone and in some cases the "frontbone" of our networks.

UniFi works with an HTML front-end that allows the user to manage every manner of their UniFi network and its devices. It's incredible and it's important.

As vendors often do, the big brains at Ubiquiti decided that their tiny little app that runs on any computer connected to the network was no longer up to the task of providing a proper management gateway for admins and had to be replaced. It had been warning me for a while, but I was never able to get its replacement, UniFi OS, to install on the PC I'd been using for the old Java application. Even with the help of Ubiquiti's support team, it would throw an error after timing out after one of its processes failed to start.

When support can't figure it out, it's time for a new approach. I decided to "spin-up" a VM



ElectroCookie Pi-4 Case. The header is brought out the side, it has a good-sized fan and lots of pretty blinkies (with adjustable brightness)!

(Virtual Machine) on our Hyper-V server for this one task, and rather than buying another Microsoft Windows 11 license, I picked a distribution of Linux called Ubuntu, which is free and very, very stable for my operating system. Ubiquiti supplies a build of UniFi OS designed for Linux, and I knew Todd Dixon uses Linux for his UniFi Wi-Fi management, so I determined this was the way to go.

Once I learned how to install the UniFi OS package onto Linux, it's been easy going and working perfectly. I can access it anywhere on the network simply by navigating to the VM's IP address using the UniFi OS port on any web browser.

Miscellaneous Ramblings and Goings On

Often, I think of broadcast engineering as a job requiring a person to be a "Jack of all trades and a master of none." I've always been comfortable with this trope and have worn it like a badge of honor. We jump into whatever and as long as there's some hot coffee, we press on!

A thought also occurs to me that broadcast engineering has become much more of an IT profession. While taking the compulsory "Typing 101" in high school, I mused that beyond churning

out an occasional resumé, I'd practically never need that skill. These days a QWERTY keyboard never leaves my pocket. This's not to say that there are no other components; certainly still you cannot do this job without at least a cursory understanding of many disciplines. I started my career as an electrician, honest work and I was good at it, but I really didn't enjoy crawling under mobile homes in the winter!

As usual, lots of other things have been going on here in the Detroit market.

One of the tiny dishes we use to bridge our network up to our microwave backhaul has been going offline every few weeks.

Accessing the wireless bridge's GUI, I

can see the unit's CPU load is nearly 100%. I have a new one on the bench just to test until the tower crew arrives.

Another contributor to this month's workload has been routine system backup. It's important to keep config files from every piece of equipment that will let you download them. These are saved on a network drive on our NAS and a backup of these backups are then replicated on a portable hard drive. Once, I had to rebuild a complicated Burk Jet flowchart for our pre-sunrise daytime transmitter power levels. It was hard enough just to remember what I'd done the first time around, and figuring it all out again is not my idea of fun!

Time to go assemble my lime green ElectroCookie case for my Raspberry Pi. Tata for now!



Ubiquiti PowerBeam "tiny dish"

News from the South
by
Todd Dixon, CBRE
Chief Engineer, CBC–Alabama

Adding to VPN Madness

Once the craziness of complying with the new FCC rules on EAS network-connected equipment is in the rear-view mirror, let me encourage you to take the next step in your journey. Here in our company, most of you have, in one way or another, had to implement Wireguard VPN tunnels between your studio firewalls and the routers at your transmitter sites in order to protect STL backup links that use the public internet with an encrypted data stream.

Although I keep reminding folks that the Wireguard VPN technology itself is not considered a server-client relationship but is instead a peer-to-peer relationship, our TP-Link Omada routers use the terminology of server and client. In fact, most of our connections were identified as having the “server” on the PfSense firewall and setting up a “client” on the TP-Link routers.

It might surprise you that having that one encrypted connection we have set up between the studio and the router is not really consuming that much extra in terms of the router’s resource capabilities. The router was already handling the ISP data. We’ve just added a little more processing with the introduction of the encryption.

So now that you are wondering what to do next, perhaps I can challenge you onto your next Wireguard journey, and have you create a Wireguard “server” (really a peer), on your TP-Link Omada router at the transmitter site. This will be a VPN network separate and set apart from the Wireguard client that you have already created that connects to the studio. The process is not that difficult in the Omada interface, as you will be able to quickly set up a Wireguard server and create several users with their own “.conf” files that will give you direct, encrypted access to the tower site’s network via your backup (or in a couple of cases, primary) ISP STL path.

The mere mention of this likely blew a neuron in your brain, but when you think about it, you are really not adding a lot of complexity to the router at all. In fact, this extra Wireguard path will only be used when you actually have the need to use

it, and as such adds no additional heaviness to what the router is already doing.

I guess the question forming in your head is, “Why would I entertain this foolishness?” I would suggest that it is direct access to the site – maybe your ISP connection to the station is down. Quite possibly, there is nothing wrong with your point-to-point microwave links, but that isn’t helping you if your internet connection at the studio is out and you have to check on your tower site. So take my advice, add the Wireguard server to your router, create the users and download the configuration file and add it to the rest of your Wireguard configurations. You just may owe me a lunch some day!

If this has whetted your appetite for all things Wireguard, next month, I’ll introduce creating a Wireguard connection to your toaster oven...

Is there a real problem here to fix?

If you’ve been reading what I write for any length of time with regard to computer security, this FCC requirement of a 15-character password is probably at least five years late in my estimation. Several years ago, I came across some research that showed that even a 10-character password dropped the probability of getting hacked by 93 percent!!! Only recently, I wrote about how quantum computing is going to make almost every modern password obsolete anyway. Folks, that is all coming to computer near you.

Forgive me if I was a little astounded when I was thumbing through the Broadcast Engineers Facebook group and a post began to discuss the 15-character non-dictionary constraints that the FCC was placing on EAS and related STL and remotely managed equipment (that includes our radio playout software) and saw a comment that asked, “Is there a real problem to fix here? Is this just FCC overreach?”

I don’t even want to dignify those questions with a response. My take on it, in general, is that it is not that difficult an ask to update 40 or 50 passwords and strengthen our overall cybersecurity position in the process. Is it going to be inconvenient for everybody involved? The answer clearly is yes.



Greater security is always the enemy of the user's convenience, but certainly everyone is capable of remembering a 15-character password, even if it is random one. I can also hum along to or sing 5,000 songs from every genre of music if I were really pushed, and some of those were created before I was born. The way my mind pigeonholes memories pulled a quote from the classic 1984 movie, *16 Candles*, where Molly Ringwald's character, when asked by her sister if she can remember to turn off the oven in 20 minutes, responds, "Yes, I can remember lots of things," as the rest of her family has completely forgotten it's her 16th birthday.

As I pondered other answers to those questions, I began to think about the very real struggle that the radio industry is in for advertising dollars and audiences, and my thought became, "Fella, do you really want to be the station that

advertisers (or listeners) lose faith in because you couldn't make your network at least minimally secure with little to no effort?" The corollary is similar: "Are you willing to be the cautionary tale of the station that had to pay the FCC fine (which I'm sure would be the textbook example of a punitive fine) because you didn't do it?" Overreach might be the least of your concerns.

Don't get me wrong. I mean, I live in Alabama, where famously, AM tower sites apparently can up and vanish without a trace with, "We didn't know it was gone," as the excuse. I don't want to be that person, I'm sure you don't, either, and I know we'll come out the other side of this with more secure platforms and better ways to manage all of the chaos that we often find ourselves in.

Until next time, may God bless the work of your hands.

Tales From Cousin IT
by
Stephen Poole
CBC Corporate IT Specialist

With the world behaving more and more like "the inmates are running the asylum and are gnawing the curtains," let's start with something light-hearted. The genus *Leopardus* contains a number of small wildcats, all from South America. Figure 1 shows the newest member, the Tilcayo. Don't think about having one as a pet, though, unless you want to spend time at the local Doc-In-A-Box getting stitched up. The late Salvador Dali had a famous Ocelot named "Babou," but he was already crazy. Stick with a nice adoption from the local shelter.

The horrible heat and humidity in Alabama have finally started to subside. Daytime temps are in the 80s and we are even dipping into the upper 50's at night. My poor overworked heat pump is finally catching a break. Believe me, that musty, dusty "first heater turn-on" smell was quite welcome the other day.

A quick Kia update: I prepaid for regular oil changes and checkups with my dealer, but their service department stays backed up. After a couple of cancel-and-reschedule episodes, I just took it to a reputable quick lube place. I got the required synthetic oil and filter, but noticed that they'd recorded that it was done with four miles on my odometer. I'll have to run by and ask them to reprint

it with the correct mileage (over 4,400 miles). I want to protect that 10-year warranty.



The AI Wars

At least twice a week now, I have had to install updates on every corporate server (17 times for each one in September alone). This takes many hours, and as I've mentioned here before, you can't be sure that the update won't break something. The other day, I updated our email server and Zimbra refused to restart. After a good bit of detective work, I saw that Zimbra needs admin-level access to its nginx proxy. The update had reset that, so I had to re-enable it.

Frequent updates have become routine now that AI is being used to find vulnerabilities. As a result, there's a real battle between the good guys and the bad guys. The good guys will warn the software vendors and assist with fixes. The bad guys use AI, not just to find cracks, but to create very realistic-looking emails and text messages to "phish" people into providing credentials.

Some of these vulnerabilities are true show stoppers, including Remote Command Execution, Multi-Factor Identification capture and you name it. I get daily headlines for the latest problems. One recent example involved the Elementor plugin for

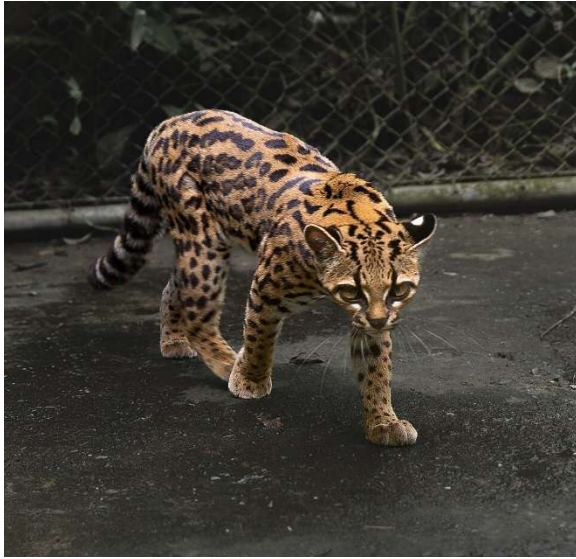


Figure 1 - Spooky eyes ... the Tilcayo!

WordPress that we use for some Websites. Hardly a day goes by without a "critical warning" for kernel (i.e., operating system) vulnerabilities, too.

Cris sent out a missive a few days ago warning everyone in our company to use strong (at least 15 characters), unique passwords. For anything exposed to the Internet, the days of using the same, easy-to-remember password for multiple logins need to end ASAP. I'll be the first to admit that I'm an offender. What's really scary is that I know that there are long-forgotten sites that I used years ago with a common password.

The bad guys aren't actively targeting second and third-tier systems like ours at present, but that could change anytime. Even the Middle East is involved: Iranians (and others) are trying to attack infrastructure targets like power distribution, water and sewer systems.

Additional Steps

There are some other steps that you should take. Remember that you're not just protecting your personal information; you could expose our company if you're compromised. Start with a reliable anti-malware app on all devices. We require ESET Security for protection with our stuff. A VPN has also become essential, especially when traveling. Our company uses Wireguard; for my personal devices, I have a subscription with NordVPN.

Remember, your hotel doesn't want people calling the front desk with network problems, so they make their access criminally easy to use. You should browse to their "We ain't responsible for nuthin"

disclaimer page normally; activate your VPN before doing anything else.

Google, Facebook, Amazon and other large corporations have plenty of IT staff and take security seriously. But be careful about using that "login with Facebook (or whatever)" with third party sites. Hackers are targeting these smaller, less-capable vendors because they're easier targets. This isn't just worrywart theory, either; in September alone, the e-commerce platform BigCommerce and healthcare support provider Veradigm were reportedly accessed via third parties.



Figure 2 - A search for 'ecommerce' gave me this. Of course.

This bears repeating: don't connect to a wireless network that doesn't support strong encryption, preferably WPA3. NEVER use WiFi with no password, or with the access info displayed for customers (ex., airports or a doctor's office). Some of our company email accounts have been taken over this way. There's a real temptation to quickly do some email on public WiFi, but a hacker could be sitting in that coffee shop a few tables over. With kits that can be downloaded online, they can sniff and examine what you send or receive on an unencrypted connection.

From time to time, check your mobile devices to confirm that unwanted services haven't been turned on without your knowledge. This is one of those "ask me how I know" things: Android Auto in my new Kia will re-enable Bluetooth even after I've disabled it. I prefer to only enable it when I actually need it. I've also turned off the "automatically connect to any available WiFi" toggle.

If you are computer literate and get a long list of update notices, you'll be tempted to go through

it to decide which ones to accept. Unless you're willing to spend the time to research which items are vulnerable, just let your device's update manager handle it. I've learned that researching each item often ends up taking longer than just letting a full update run, anyway.

That'll do for now. It's a never-ending battle, but the cost can be significant if you get hacked. While you can't possibly anticipate every possible threat, you need to reduce the odds to make yourself a less attractive target. Remember, you're not just protecting your bank account and personal email, you're protecting our company as well.

Odds and Ends

While taking breaks, I used to browse through short videos (called "Reels") on Facebook. They've become almost worthless lately. Most of them are teasers that urge you to click a link to get more. Even ignoring the possibility that it could lead to a Bad Guy site, you'll discover that most of them want you to subscribe or watch ads for each 1-minute snippet. Waste of time. On YouTube, if a particular Short series becomes popular, you'll start seeing clones and incomplete copies. Double waste of time.

As for the shorts themselves, most use AI heavily nowadays. It's hilarious to see the same faces and voices in different videos. In some cases, the originals were obviously done with foreign characters (often Chinese) that were "AI-shopped" for the United States. Any text in the screen will still be in unreadable foreign characters.

The plots are also rehashed and reused over and over. One common trope is the guy or gal who's really important, but likes to maintain a low profile (cab driving seems to be especially popular). He will be threatened with dire consequences unless he admits that he's an ordinary guy. People end up hollering at each other. Then a newcomer will arrive and say, "Yes, he's the real deal!" only to have another join in to say, "No, he can't be! I've known him since Moby Dick was a minnow!" Finally, the Big Reveal will come and the horrified doubters whisper, "No ... impossible!" Rinse, repeat.

The images came from Wikimedia Commons; Figure 1 is from user Alessandro Verniani and Figure 2, user Babewyn. The trademarks used here are the properties of their respective owners. Until next time, keep the inmates away from the drapes and never stop praying for this nation!

The Chicago Chronicles by

Rick Sewell, CSRE, CBNT, AMD
Engineering Manager, CBC–Chicago

I am quite sure I am not the only one busy with getting either last-minute changes or checks on the equipment logs for compliance with the new FCC mandate on cybersecurity. At the time of this writing, the deadline is barely over 24 hours away.

From the beginning of the rules being put in place, there seemed to be a lot of variances in interpretation of what you needed to do to be compliant. I heard some broadcasters say that if you have the passwords policy and you are behind a firewall, that is good enough.

Our company's brain trust, the Crawford engineering crew, interpreted that passwords and a firewall were not enough. You need to have your over the open Internet STL audio streams run through a VPN.

I really have always thought this was a good idea but now having a deadline to do it means actually getting it done. As they say, "deadlines spur action."



For our setup in Chicago, we use the Tieline codecs with SmartStream technology, so the data is sent over two separate but redundant data streams/paths. Three of the sites have the main data stream going through our own private Cambium Ethernet microwave network, so that part was already in compliance since they are not going over the open Internet and they're already behind our firewall. One of those three has its redundant data stream through a 5.8 GHz Ubiquiti Ethernet radio, so that whole site was already compliant.

However, three of the sites have over-the-open-Internet data streams for their secondary, redundant streams, and this is where the compliance issues showed up. In fact, our one site is about 100-mile drive away from the studios and has two separate Internet pathways for the Tieline codec.

This meant that we needed four VPN tunnels created, with the one site needing two. We only needed to create one VPN tunnel from our main

studio network, and that would be the main data path for that site. The main obstacle I faced with this was the fact that all the equipment at the transmitter site was still on the same subnet scheme as one of our studio networks. This was due to the fact that the site used to be linked by T1 lines that essentially acted like a 100-mile Ethernet cable.

All of that needed to be changed in order to get a VPN link working because the routers and firewalls would be confused about which direction to forward data. Once that was changed, the VPN worked flawlessly.

I then had to install another router at the transmitter site and create a VPN tunnel back to a secondary router at the studio. This secondary router at the studio was in actuality a different network that was really only used for the NIC2 ports of the Tieline units at the studio, and it has a different ISP.

I needed to set up three VPN tunnels from this router to three different sites. Previously, these

connections were made through old routers via port forwarding, and that, in my opinion, is not really secure.

In total, we purchased five new TP Link Omada ER707 routers to complete the project, moving all the port forwarding to the VPN tunnels.

Keep in mind that we have just one Tieline Gateway 8 at the studio making all these calls to four sites with redundant data streams, some over the Cambium private network links and four of the data streams going out through the Internet. All at the same time. It's a very complicated calling program on that Tieline codec, and it took a few adjustments along the way to make sure these data streams weren't bumping into each with the same control and audio ports.

It's good to say that is all working and the deadline spurred the necessary action and we're better for it.

Rocky Mountain Ramblings
The Denver Report
by
Amanda Hopp, CBRE
Chief Engineer, CBC - Denver

Happy Fall! It's finally here! Here in Colorado, the aspen leaves are turning a beautiful gold with some red mixed in. I think everyone in Colorado is praying for a very wet, snowy fall and winter. We need it in the worst way. I am looking forward to slowing down a bit and being home on the weekends.

Odd Network Issue

As many of you know, we've changed our networks around at each transmitter site to help make them more secure. For the most part, it was fairly painless. We did have some issues here and there, but once we got things working, we were able to just leave it alone.

The KLDC site in Englewood was the exception. We ran for a couple weeks with no issues. Keep in mind, during this transition, we also had tower work done to replace the shielded UV-rated CAT-6 cable going up to the Cambium microwave radio on the tower. This was to correct another issue that would cause the Cambium to lose its Ethernet connection, causing the station to constantly be switching to our Barix internet backup for audio. This tower work corrected that problem. However, within



a few days, I noticed the disconnect happening again. The difference was, the microwave showed it was still connected and the station would go completely silent. This pointed to the router at the site. Once things came back up, I was able to see in the system logs both WANs disconnecting then reconnecting.

I put in another TP-Link Omada ER707 router with the same result. I factory reset the one I took out and set it up manually, once again with the same result. I did some research and didn't find anything helpful.

I finally took a network switch I had to the site and basically connected the Cambium microwave radio to that, moved our BridgeIT XTRA codec directly to it, and then connected another port to the WAN2 port on the router to allow the other equipment to work properly. This put the codec directly on the Cambium ahead of the router. I let it run like that for a week with no issues.

On another trip to the site for an unrelated issue, I put things back the way they should be. It ran fine for several hours, but then the disconnects started happening. I immediately went to the site and put that

network switch back in.

We really aren't sure what is going on. The setup is identical to our other four sites. Todd Dixon has some thoughts for us to try that include the routing of the BridgeIT XTRA audio between the two LANs at the studio. I am unsure if we are going to try that or not. Truth is, it's working the way we have it set up. It doesn't hurt anything to have it set up this way either, it's just one more piece of equipment. And if it ain't broke...

Nautel J1000

KLDC was the trouble child for us in September. In August, we had a power failure at the site that was bad. There were several times the power came back on momentarily and then immediately went back off. It ended up tripping the panel breaker for the Nautel J1000. We had to reset that as well as do a transmitter reset to get the transmitter working again.



A pile of damaged parts that we replaced in the KLDC J1000.

We didn't think much about it then, but one subsequent weekend I got a silent alarm for the station and immediately began digging into it. The

transmitter was not producing power. I could not get it to come up at all, so I put it on the backup transmitter.

On the following Monday, we went to the site and found both modules were in alarm and showing failures. We pulled one, opened it and saw many burned-up components in the modulator. We pulled the other and found the same. We took them, and the spare parts box back to the studio with us where we could more easily troubleshoot and do repairs.

Once the repairs were done, we took the modules back and plugged them in. Module A was good, but B was still in alarm. We pulled it back out and took it back to the shop to troubleshoot further. We couldn't find anything wrong with the modulator or RF power amplifier that we had repaired.

We went back to the site and did some more testing. Swapped modules, swapped the modulators

between modules, swapped PA assemblies, and found that the problem was staying with the module and not moving with the assemblies. That left just the passive PA interface board and the Forward Converter board, which is essentially the variable B+ power supply for the module. The first rectifier we checked on the Forward Converter module was shorted. We replaced it and checked everything else we could, finding no other issues. We once again took the module to the site and installed it, and saw the transmitter was happy again. Clearly this problem came in on the power line.

Cybersecurity

I don't think it's a secret about the new password rules the FCC has implemented. Nothing bugs me more than when people who have no clue about something tell me how to do my job. I understand wanting to protect what's going out on the airwaves. But you can only do so much. At some point you must allow the broadcaster to do what they can and if something happens, deal with it then.

Trying to figure out what all we have to do to be compliant has been a chore. Some equipment doesn't allow us to log in remotely and change the password. Instead, we have to take time to drive to a site and change the password from the front panel.

Some equipment may not even take a 15-character password. Plus having to have a different password for everything is difficult. I can see, in the future, having to deal with an off-air situation and time being wasted having to look up passwords.

We really need more time to get things done, and we need better clarification. Not some broad thing that can be interpreted in many different ways.

We did our best to get everything done by the deadline, and were successful. But oh what a pain...

Coming Up

Growing season is over, which is great. We will be able to make less frequent trips to the transmitter sites. We need to do a good cleaning everywhere and clear out any growth that's still left.

I hope to get some cleanup done at the studios too. The consoles are dusty and could use a really good cleaning. The equipment in the racks could use a good wipe down as well.

I think that about covers it for this month. I pray you all have a safe and wonderful month!

The Local Oscillator
October 2026

KBRT • Costa Mesa - Los Angeles, CA
740 kHz/100.7 MHz, 50 kW-D/0.2 kW-N, DA-1

KNSN • San Diego, CA
1240 kHz/103.3 MHz, 550W-U

KCBC • Manteca - San Francisco, CA
770 kHz/94.7 MHz, 50 kW-D/4.3 kW-N, DA-2

KLZ • Denver, CO
560 kHz/100.7 MHz, 5 kW-U, DA-1

KLDC • Denver, CO
1220 kHz, 1 kW-D/11 W-N, ND

KLTT • Commerce City - Denver, CO
670 kHz/95.1 MHz, 50 kW-D/1.4 kW-N, DA-2

KLVZ • Brighton-Denver, CO
810 kHz/94.3 MHz/95.3 MHz, 2.2 kW-D/430 W-N, DA-2

WDCX • Rochester, NY
990 kHz/107.1 MHz, 5 kW-D/2.5 kW-N, DA-2

WDCX-FM • Buffalo, NY
99.5 MHz, 110 kW/195m AAT

WDCZ • Buffalo, NY
950 kHz/94.1 MHz, 5 kW-U, DA-1

WDJC-FM • Birmingham, AL
93.7 MHz, 100 kW/307m AAT

WCHB • Royal Oak - Detroit, MI
1340 kHz/96.7 MHz, 1 kW-U, DA-D

WRDT • Monroe - Detroit, MI
560 kHz/107.1 MHz, 500 W-D/14 W-N, DA-D

WMUZ-FM • Detroit, MI
103.5 MHz, 50 kW/150m AAT

WMUZ • Taylor - Detroit, MI
1200 kHz, 50 kW-D/15 kW-N, DA-2

WPWX • Hammond - Chicago, IL
92.3 MHz, 50 kW/150m AAT

WSRB • Lansing - Chicago, IL
106.3 MHz, 4.1 kW/120m AAT

WYRB • Genoa - Rockford, IL
106.3 MHz, 3.8 kW/126m AAT

WYCA • Crete - Chicago, IL
102.3 MHz, 1.05 kW/150m AAT

WYDE • Birmingham, AL
1260 kHz/95.3 MHz, 5 kW-D/41W-N, ND

WYDE-FM • Cordova-Birmingham, AL
92.5 MHz, 2.2 kW/167m AAT

WXJC-FM • Cullman - Birmingham, AL
101.1 MHz, 100 kW/410m AAT



Corporate Engineering
2821 S. Parker Road • Suite 1205
Aurora, CO 80014

email address: calexander@crawfordmediagroup.net