The Local Oscillator

The Newsletter of Crawford Broadcasting Company Corporate Engineering

AUGUST 2026 • VOLUME 36 • ISSUE 8 • W.C. ALEXANDER, CPBE, AMD, DRB EDITOR

Zombies Ahead!

For what it's worth, I hate dealing with cybersecurity stuff. It's a major PITA, and without exception it makes my life harder. That said, it's a necessary evil, and I've got no choice but to embrace it.

When I was growing up in Mayberry in the 1960s (okay, it was Amarillo, Texas, but it was a lot like Mayberry), we had locks on our doors, but everyone knew we kept a spare key in the awning over the front porch. We didn't lock our car doors, and crime was rare. I can't ever remember a house being burglarized in our neighborhood, and I didn't know of anyone who had been burglarized in our circle of friends and acquaintances.

That world is gone and has been for a long time. If you value your belongings, you'd better secure your home with a good deadbolt, and you should really have an alarm system as well. The same goes for your automobile. You'd better lock it up, and if it has a security system, use it! If you don't, you may not have a car when you come out of the store or whatever.

The public internet started out pretty much that same way. Security wasn't much needed, and where it existed, it was a simple password. Over time, however, as the internet grew and our use of it grew to include banking, e-commerce and other financial interests, criminals found easy pickings, stealing credit card numbers, banking information and identity info. The various industries had to ramp up internet security to protect the information being transmitter over the internet. Those security measures have become increasingly complex over the years, and yet cybercriminals still manage to punch their way through them from time to time.

Cybermischief, for want of a better word, has expanded through the years, and we have had to guard against it in its many forms – viruses, malware, phishing, etc. Some of it is relatively harmless and somewhat humorous (such as "Zombies Ahead!" on roadside electronic signs), but quite often it causes real damage and pain. Numerous ransomware attacks have hit our industry in recent years, including once in one of our own markets.

I remember a movie from the 1970s, "Network." Some miscreants used a "microwave truck" to hijack a television station's STL and put their own programming directly on the air. It was pretty funny, but working in broadcasting at the time, it occurred to me how easy that would be to pull off. I'm sure it's happened to radio and TV stations in real life back when we used unencrypted over-the-air analog STLs, and there wasn't a whole lot that could be done to protect against it.

Could the same thing happen today to IP codecs used in STL applications over the public internet? I'm thinking that it could, and it wouldn't be that hard. Figure out the IP address and port and a miscreant with some hacking skills probably wouldn't find it that difficult.

The FCC has, in recent rulemaking, recognized this vulnerability and is requiring stations to implement cybersecurity measures to protect codecs providing feeds to transmitter sites over the public internet. We have sixty days from the date of publication of the new rule in the Federal Register to implement these changes. That publication will likely take place this month, so the clock is ticking.

Thankfully, we have some resources within our existing network infrastructures to make this

happen. Our primary firewalls at the studio have integral VPN servers, and many of our transmitter sites have VPN peers in their routers. Todd Dixon has figured out how to use these resources to create a secure VPN tunnel over the internet to connect studio codec to transmitter site codec, and we're working on getting those tunnels set up everywhere we have a codec using a public internet connection to pass traffic.

We have just a few sites that use the internet as primary transport, but many of our sites that use Part 101 microwave or satellite transport as primary use the public internet as a secondary, backup path. We've got to protect those paths, and we should have that done companywide in the coming weeks.

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

Greetings from Buffalo!

We had a few issues with our A/C units at the WDCX transmitter and the WDCZ AM transmitter over the past month. We had to have the units serviced. Since then, the units have been running without problems.

We had a power outage at the WDCX studio while Josh and I were in Rochester. We had to manually turn on a few computers that weren't on the UPS. We have since put those computers on the UPS so this won't happen again.

In Rochester Josh and I are getting ready for the installation of the new WLGZ transmitter. We have to move the WDCX 107.1 translator equipment to a different rack so that we can remove a wall mounted rack that will be in the way when we remove the old Continental 816R.

Also, there is a patch panel mounted on the top of the Continental that we'll have to secure since the transmitter is moving out. We plan to use Unistrut and secure it with threaded rod coming down from the ceiling. We will be moving the old transmitter to Buffalo for storage. We still have a Continental transmitter serving as the AUX for WDCX-FM, so we can grab parts off it as we need them.

The Nexgen computer in the WLGZ studio failed last month. Fortunately, we were able to get a replacement power supply to get the computer back online quickly.

From my past experiences…

I once had a situation where a station had its C-band satellite antenna and receiver located out at the transmitter site, but we needed to control it from the studio. They had an old Mosely TRC15 remote control, which only had control and metering available.

This posed a big problem. How could we know what channel the receiver was selected to back at the studio? In some cases, you would be able to tell by listening to what was on the channel, but this wouldn't always be possible.

Many of you may remember the old Scientific Atlanta receivers. There were two rack mounted units. One of them contained the downconverter and power supplies. The second unit contained all of the demod cards. There were two varieties: 7.5 kHz and 15 kHz demods.

I sat down with Dave Halik, one of my employees at the time, to figure out how we were going to accomplish this. The first thing we had to do was figure out the very poorly documented control interface of the receiver.

To step the channel up and down, you had to load a BCD word and then pulse a strobe. This meant we had to build a decade counter that we could step up or down.

We designed that using a bunch of TTL chips and tested it in the shop. We didn't have a receiver we could test it on, so we had to hope it would work when we connected it to the receiver.

We had to read BCD data from the receiver and convert it to a voltage that would change linearly, depending on the channel data read from the receiver. We accomplished this with an analog-to-digital converter and more TTL chips. Eventually we got it all working.

We were able to test it out on a receiver that we had access to locally. When we eventually connected it to the remote control, we were amazed as to how accurate the reading reflected the channel number!

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

That Confounded Bridge

Regular readers of *The Local Oscillator* will remember approximately one year ago when at our WRDT AM transmitter site a farmer had an accident, bringing tower 4 to the ground. I'll stop short of retelling the entire story here again. The super condensed version is that the farmer snagged the northeast guy anchor with his disc harrow. This snapped four of the eight turnbuckles and the tower collapsed.

While we were in the process of installing a replacement tower, the immediate area was cleared of all significant vegetation, revealing a badly rotted bridge.

This tower sits adjacent to a canal, the Davis Swale, that drains into Lake Erie less than three miles to the east. The swale passes below the south guys and between the tower and the transmitter building, necessitating a bridge so that the antenna transmission line, electrical, and control wiring didn't hang in the water.

Figure 1 - What was left of the old bridge.

The old bridge was made from pressure treated lumber resembling the construction of a residential deck. Two concrete footings on either side of the swale bank and additional concrete piers poured in the water formed the supports. Planks lined the joists, and evidence of railings long rotted away, could be seen on either side.

Below the bridge the wires and transmission lines were still supported, although some of the brackets were long gone.

As the tower installation progressed, the tower contractor and I talked about how we could redo this bridge. I had no interest in making it for foot traffic (as was apparently one of its original purposes), so he suggested using a horizontal section of a tower they had decommissioned and had lying around at their shop. It turned out to be the perfect length and more than heavy-duty enough to support the wire and cabling over the swale.

Two vertical fence posts were installed on either side of the swale with horizontal Uni-strut between them forming a cradle for the tower section. The tower was laid on its side and the wires attached to the bottom side. A perfect professional-looking installation that should last a very long time.

Figure 2 - The new bridge under construction.

Alert Monitors Refresh

Our very own Stephen Poole has done custom coding for several Crawford undertakings. His most recent is a modern take on the old Enberg BA-6. It displays alerts on a computer monitor rather than lighting a bulb as on the BA-6.

Cris had Amanda install one in each of the four Denver control rooms and proposed the idea of putting one or more up in Detroit. I jumped on the idea because the old Enbergs, while still operational, were quite long-in-the-tooth and as the model number suggests, only good for six different alert conditions.

Figure 3 - The new alert monitor under test.

The new system runs Python code on a Raspberry Pi. The Raspberry Pi can be fitted with a breakout terminal block. This allows the user to easily wire the "Pi" onboard GPIO to the eight different alerts that the system will monitor. We decided to wire each of them to our Wheatnet logic ports and use Wheatnet's convenient network to expand and route each of the alert conditions we planned to monitor.

Since we have four radio stations, the first four indicated conditions were silence alerts on each of the four stations. After that, I decided to add an alert for the front door and one for when the building was being supplied by generator power.

Since every alert on the system should be able to be seen by any staff person, I decided I could use the additional Raspberry Pi devices to drive monitors wherever needed and simply use VNC protocol to plop in an alert monitor anywhere I'd like.

Miscellaneous Ramblings and Goings On

Many other things have been competing for my time over the last month. The FCC's pending regulatory move forcing broadcasters to secure their public internet STL pathways is the big one. For years, several of our studio-to-transmitter links have traversed the public internet without issue. Sadly, a few stations out there left their IP audio transports with their factory default passwords in place, inviting nefarious actors to either bring down these links or worse, introduce unwanted program material onto the affected radio station. Those of us who've used even moderately secure passwords have had nary a problem, but the rule is coming, so we may as well figure out how to comply.

Compliance isn't complicated in the sense that an encrypted VPN can be nailed up between the studio and each transmitter site with associated STL traffic forced onto it. I have been working to that end for each of my sites, but there's much to learn about the VPN setup and how to get the far-end networks routed correctly. That's been a bit complicated, so thanks much to my friend and colleague Todd Dixon, Chief Engineer in our Birmingham, AL market, for his patience and knowledge transfer!

LXE OLED Display

Following up from last month, the Verizon 4G LTE service that I installed at WCHB has run completely error free, so I hope to continue migrating to these as our secondary internet connection at all transmitter sites. They're significantly less expensive than satellite delivered internet, with very significantly lower latency, too.

Coming soon, I will be changing out all 39 OLED displays on the WCHB Wheatstone LXE console. They've all dimmed to a point where they can barely be seen.

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

Grubby hacker paws…

In the middle of June, Cris notified all of us about the FCC's rulemaking about enhanced cybersecurity for EAS hardware and transmissions. Every part of our networks had to be evaluated in an effort to protect EAS output from malicious hacking intent. We were already doing several of the things or could get them done quickly. Updated minimum passwords of 15 characters in length were an easy target and could be done quickly. We were also already using a fairly robust firewall in PfSense, so our local studio networks are not easy targets for hacking access.

A number of our markets use licensed point-to-point STL paths. We consider these pretty secure since they are already behind our firewalls and any hacking would require expensive specialized radio equipment that somehow was able to be configured in the exact path of the signal.

The one requirement that created a problem for most of our markets was protecting STL paths that go over the internet. Here in Birmingham, we use the internet for all of our secondary STLs. Other markets have towers that are beyond the maximum distance that P2P would be effective, so they rely on the internet for both primary and secondary audio.

Even though almost all of our markets use Tieline audio codecs and gateways with their SmartStream Plus technology, which provides a bit for bit audio comparison of two streams to make sure audio doesn't drop out, theoretically, hackers could insert fake EAS or program audio into the air chain and create a false EAS alert. The solution for us, in general, is to use Wireguard VPN to encrypt the streams that traverse the internet so that it would not even be an option for them to attempt.

Fortunately, not only have we standardized on PfSense firewalls that can have a Wireguard VPN package added to them, but we have been using Wireguard VPN for all of remote access to our sites for some time for both engineering and talent work. Most of our markets have also been using TP Link dual WAN routers (ER7206s and ER707-M2s) that can not only serve our point to point wireless connections, but also our internet connections with ease. Their firmware over the course of the last few years has also been upgraded to provide a fairly robust Wireguard VPN experience for us to use as well.

How it actually works…

Officially, Wireguard doesn't operate on a server/client model – each unit is simply a peer. The tunnel between two peers is actually completed when each peer receives the other's "public" key and internally verifies a trust between the two using a modern encryption algorithm called "Curve25519" based on an elliptical curve.

Once that handshake is complete, the tunnel is established and any traffic that passes between the two can only be unencrypted when it passes through the other end. In fact, anybody can get a hold of the public part of the peer's identity, but until it is used with its paired private key, no connection takes place. You'll notice that all of the Wireguard .conf files include a private key and a public key.

When Cris handed me the project, the most difficult part was creating a network picture that showed what was really going on. In the end, it became clear to me when I thought about each internet stream as a single Wireguard "peer" connecting back to a "peer" at the studio. We've been doing this for several years now.

A peer at the studio facilitates encrypted connections to all of the Wireguard "peers" out in the field. They are dialing back to a fixed IP address that has a Wireguard client behind a firewall. That is what our tower sites will be doing. See Figure 1.

The same thing is essentially happening between the TP-Link routers and PfSense.

A cavaet before you start: it also requires thinking through your tower site network naming schemes. Each of the networks cannot can have the same default subnet, like 192.168.1.1 that a TP-link router might have shipped with. They need to be separate networks. As an example, a network that I have to use Wireguard to get into regularly for the company has a subnet scheme of 192.168.1.1; my home also gets presented a subnet by my ATT ISP router of 192.168.1.1. When I have to remote into

that network from home, the Wireguard peers at both ends look like they are watching a tennis match. Both are asking, I wonder if he wants the router on the far side or the one in his home and it creates a real network nightmare.

Not that I am a fount of creativity, but our 93.7 site has an IP range that has a "93" in the 3rd octet of the IP address, 850 has an "85" in its 3rd octet, and 101.1 has a "101" in its address. Those are taken, so come up with your own, but it may require you thinking through what you already have established.

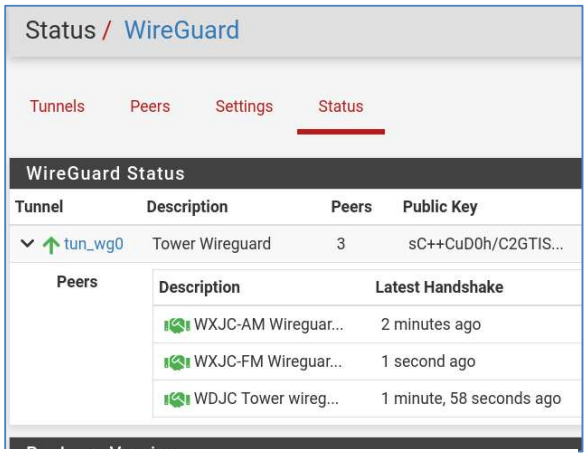


Figure 1 - One Wireguard peer at the studio and three peers representing a connection from each tower, the image is obviously cropped to not reveal any sensitive data.

I asked Cris to send me an ER707-M2 that he had, which most of the company uses, and after updating its firmware to the latest package, I was ready to start working my way through the connections.

The critical part was establishing the Wireguard handshake between the two units. This involves some PfSense work setting up a tunnel, a Wireguard interface that you can define on PfSense so that you can route traffic to and through it, and some basic firewall rules to allow the data to pass.

On the TP-Link end, it involves creating a public/private key pair for it (and putting its public key in PfSense as a peer) and placing PfSense's public key in the TP-Link router as a peer at the tower site. Once that was done, the Wireguard handshake happened nearly instantaneously. For our purposes, an encrypted link was established.

I wish that this were all that needed to be done. If it were, it would have hardly been considered a project.

Another part of the Wireguard .conf file is a section called "Allowed IPs." VPN means virtual private network, so not only do you have this secret network IP that has been given to each peer in a particular network segment, but you also have to tell Wireguard what IP ranges can cross through the tunnel. In our current use of Wireguard for remote access this was normally "any IP address" (designated as 0.0.0.0/24), but in this case we want to narrow the scope of the IP addresses considerably.

So a peer on the PfSense side would generally have the IP address given of the peer on the other side and any networks at the tower site. As an example, let's say the TP-Link router has a LAN at the tower of 192.168.97.xxx and a WG peer of 10.5.0.2, the allowed IPs would be 10.5.0.2 and 192.168.97.0/24 (all of the IPs on the tower LAN subnet). On the tower side of the tunnel, the Allowed IPs would be 10.5.0.1 (the PfSense WG IP) and the LAN on PfSense where the Tieline hardware sits-lets say it is 10.10.10.0/24. Effectively, the use of "Allowed IPs" narrows the path considerably.

Of course, anybody that works with Tieline products realizes that there are two critical network ports that are used to make the audio connections happen between units. One is a TCP port that contains session data and the other is a UDP port that the audio uses. These have to be addressed on both sides of the tunnel with static routing so that the network traffic knows where to be directed.

I created a document for all of our engineers that goes through setting up the entire system on the ER707-M2 routers with PFSense. While each individual tunnel is one internet route, don't forget that you may be sending HD2 and other audio signals to the tower that have to traverse that tunnel. Even if you only need to create one tunnel, you still may have to do the backend work on PfSense and TP-Link for each Tieline signal that you are sending to the site.

The end goal was to make sure that any EAS audio that goes to our tower sites could not be tampered with by a hacker, but a side benefit is that you now have an encrypted tunnel for any other work that you need to accomplish-even if your point to point wireless signal is down. Once you have remoted into your PfSense system with Wireguard (as before), it now knows how to route you out to any of the LAN networks at your tower site via another encrypted Wireguard network so that you can safely access any hardware at the site.

I hope this helps everyone to make sense of what is happening within Wireguard VPN and how we are planning to use it to protect our internet STLs and their EAS components.

Tales From Cousin IT
by
Stephen Poole
CBC Corporate IT Specialist

Y'all can rest easy: I'm not going to talk about "explosive" gastrointestinal problems. We have more to worry about than whether fruits and vegetables have been contaminated by the Pathogen of the Month™. You can thank me later.

I also won't devote a lot of time to the weather. Typical Alabama: lots of storms, trees down in roads, flooding, all sorts of happiness. And when it's not storming, we have pea soup humidity (Figure 1). That picture was taken over my kitchen sink, looking into my back yard. That's not rain; it's condensation. As always, water pours from the drain on our AC units here, too.

The black and green mold that we constantly battle as a result is almost as bad as "explosive" gastrointestinal stuff. Almost. In the past, the only things that I've found to work on that gunk is bleach or hydrogen peroxide. Chlorine gives me a pounding headache; I've never liked it. Peroxide kills the mold but creates an annoying vinegar odor.

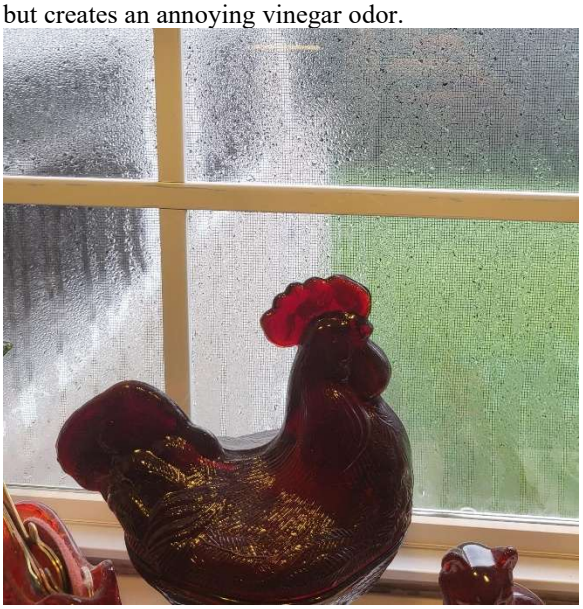


Figure 1 - Alabama, the home of heroic humidity.

I've found something new: citric acid. Those of you with mold and mildew at your transmitter sites might give it a try. The only thing is that if the mist gets up your nose, you might sneeze a bit, but it works!

Bartz vs. Anthropic

I mentioned this lawsuit almost a year ago. Anthropic has worked up a 1.5 billion dollar class action settlement with those who brought copyright claims against them. Anthropic admitted that they were using copyrighted materials, but argued that Fair Use should permit it. Without getting into the weeds here, the judge overseeing the trial, William Alsup, ruled that the use of purchased books was OK, but the use of copyrighted stuff without paying was not.

Anthropic had used "The Pile," almost 1 petabyte of texts that were created by a non-profit, EleutherAI, specifically for training Artificial Intelligence. This blob of data was specifically created for that purpose. The problem was, it contained some pirated copies of certain books (which have since been removed). Oops.

Copyright law is a complex, headache-inducing mess. For the record, I only use (a) pictures that I've taken myself, (b) images with Creative Commons licensing or (c) stuff from the public domain. You need to be mindful of this as well.

Software Updates

Here's a bit of an inside look at what it's like to be Cousin IT. Most people never see what I work on, and that's as it should be. I remember the first full-time engineering job that I took as a teenager. The station owner told me that if an engineer is doing his or her job, you won't call them very often. The same is true in IT.

Most folks run Windows and are only too familiar with broken updates. Linux and BSD are an order of magnitude better, but still have trouble sometimes. That's when I have to consult my Inner Wild Geek and pull out my software gadgets – usually working remotely, in a terminal – to fix the problem. If I can't get in remotely, I have to holler for Todd or Jack here in Alabama or Cris and Amanda in Denver.

To be fair, a modern OS is huge and complicated. The software is expected to work with any common hardware and things change. In the past, Microsoft had it especially bad; they had to support old 16-bit programs from when Windows was a Thing running atop DOS, Win32 software when the 386 became popular and now the current generation of 64-bit software. All at the same time(!).

I won't bore you with geeky details of the x86 processor family, but programming it at the hardware level can be downright Byzantine. The original 16-bit 8088 and 8086 "segmented" memory into 64K-byte blocks. Better yet, these segments could overlap. Later iterations, from the 286 through the current generation (called "686" by the geeks) now offer protected memory; if you try to access it from an ordinary program, you get the dreaded Blue Screen of Death.

When you add in the fact that AI is now being used by the Bad Guys to find ways into our systems, it's a never-ending battle. There's a tendency to become complacent and assume that because everything has been working well for years, it'll probably continue to function into the future. Case in point:

The LibSSL Vulnerability

This one was published with a "high severity" rating a few weeks ago. Once again avoiding the weeds, the OpenSSL library handles the encryption that is used on secure connections. A serious bug could allow a Bad Guy to gain root (adminstrator!) access on a Linux system. While I waited for a patch, I eliminated public access to our Web servers and required that anyone who wanted to poke around in would have to do so over a Virtual Private Network.

As I write this, the latest version of the OpenSSL kit has finally been patched. I installed the updates today. This is always nerve-wracking with either our web server (which hosts our all-important POR system) and the email server. It doesn't happen often, thank the Lord, but once in a while, an update will break something, even with a Red Hat-compatible Linux.

Figure 2 - KQMT is in Denver!

For example, Zimbra wants us to use a particular system for local DNS lookups (this is called "DNS spoofing"). Red Hat and compatible clones default to an older, different system. For quite a while a couple of years ago, every time the system was updated, the older DNS system would be restarted. Hilarity would ensue and the mail server wouldn't work. I'd have to run some geek commands in a terminal to slaughter the legacy system and give full control back to the one I needed.

Finally: A KIA Update

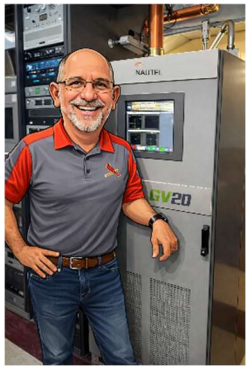
The late Lavert Agee, a brother who worked with us some years ago, would call us when he was having problems. He'd always start with, "Brother, this thing is acting crazy!" Well, my KIA continues to do things that I can't explain. Figure 2, taken from my dash, shows a preset for 99.5 FM, WZRR, a local FM station. The KIA insists that it's KQMT in Denver, CO, and I can't change it. What's really spooky is that KQMT's transmitter is on Lookout Mountain, where we have some stuff. Go figure.

That's it for this time. All trademarks are the properties of their respective owners. Until next month, keep praying for this nation!

The Chicago Chronicles
by
Rick Sewell, CSRE, CBNT, AMD
Engineering Manager, CBC–Chicago

We're just getting through the summer vacation time, but it doesn't mean we haven't had a lot of projects still developing.

With the recent FCC mandate to protect EAS and internet STL pathways, we, like the rest of the broadcast engineering community, have been having to examine these setups. I can't say we didn't see it coming. No one is beyond being a target for hackers.



In my 12 years heading the Crawford Chicago engineering operations, I can count on one hand the number of times we have been successfully hacked. But each time, it was a reminder that our whole world could be wrecked rather quickly. I think the mandate is good, and it will cause us to be better prepared.

Beyond the protection of the EAS equipment, with the exception of one site, we use the public internet for not only backup operations but also for redundant stream data. We do have one site that is entirely public internet connected to the studios. This will need to be converted from numerous port forwards to a dual VPN approach. In the long run, this will make us less vulnerable.

Once again, we are also looking at doing ad replacement on our streams. We have done this in the past with varying success.

One of the downfalls of ad replacement in our past has been that we had our spot blocks for the most part on the terrestrial station being covered with a lot of PSA material on the streams. This can really be a tune out with the monotony of those messages.

The other issue in the PPM world in which we live is that we encode the PPM watermark in the audio before sending it to our streaming provider. With ad replacement covering up the spot blocks, we lose PPM encoding during the breaks. I believe we are little more comfortable with that because the streaming provider tracks how many listeners we have on the streams, so we still have data that supports sales.

This switchover is still developing at the time of this writing. We should have a better idea of how this is working in the next month.

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

As I write this, I am so happy that July is almost over! It was quite a hectic month.

Early in the month I was doing something… I honestly can't remember off the top of my head what it was… but in the process I noticed our Gateway 8 wasn't connecting to our Lookout Mountain site on either station. I don't recall getting any alarms about this, so I began investigating, and it didn't take long for me to figure out the Gateway 4 up at the site was toast. I went up there and it was dead-dead. It was a paper weight. Thankfully the backup links, which use Barix Exstreamer 1000s, were working and keeping both stations on the air.

I had taken a Bridge-IT XTRA up to the site to get the music station onto it but forgot that the Omnia One and Gateway both use RJ connections for AES audio, and this shared mountaintop site is not a place where we can keep extra stuff. I left it alone and the next day brought the Bridge-IT XTRA back along with an audio cable we made with an RJ on one end and XLR-female on the other. We were able to get Legends 95.3 set up on it and left 100.7 on the Barix.

Before sending it in to Tieline for repair, we popped the lid on the Gateway 4 and found part of the circuit board pretty much incinerated. No idea why. There was nothing else damaged at that site, so it's doubtful it was lightning.

Tieline repaired the Gateway for us and sent it back. We have since installed it and got it working easily. I did end up having to create an answering program so both stations would connect and route properly. It is definitely a load off knowing that the two stations are back on air on the main codec and microwave link before I leave for vacation.

Is HVAC a New Four-Letter Word?

July has been a month of HVAC issues. On the weekend of the Fourth, I had just gotten out of town when I got my first alert from the KLTT transmitter site. It was 80 degrees at the thermostat in the building's back room. I tried switching to the main HVAC unit with no luck. You might remember that the main unit, which is the newer one, has one entire stage down so it cannot keep up with cooling on the hot days. Because of the cost of the repair, we are running the backup HVAC unit for cooling and the main for heating.

Because of how the system is set up, it would not switch to the main unit as it was too hot in the building, which triggered a thermostat that forced a switch to the backup HVAC (which was apparently not working). I reduced power on the transmitter to 10 kW and remotely turned the HVAC unit off for a while and when I turned it on, I noticed it was cooling some. I sent Daniel out there to change the filters, thinking that maybe reduced airflow had caused a freeze-up.

Stephen got to work on the Pi that controls switching between the two systems, including 480V power for the RTUs and the positions of several dampers in the shared ductwork. He was able to get it to ignore the override thermostat and manually switch to the main HVAC unit, so we had some cooling at that point. We left it like this for several days until we could get someone out to look at the unit.

Wern Air, our HVAC service contractor, came out that next week and found one of the refrigerant lines in the backup HVAC had a leak. They worked to repair it. We also had them do a good cleaning of the unit. While out there they verified what was wrong with the main unit (failed compressor) so we could get a quote to get it repaired. We will do that work next year.

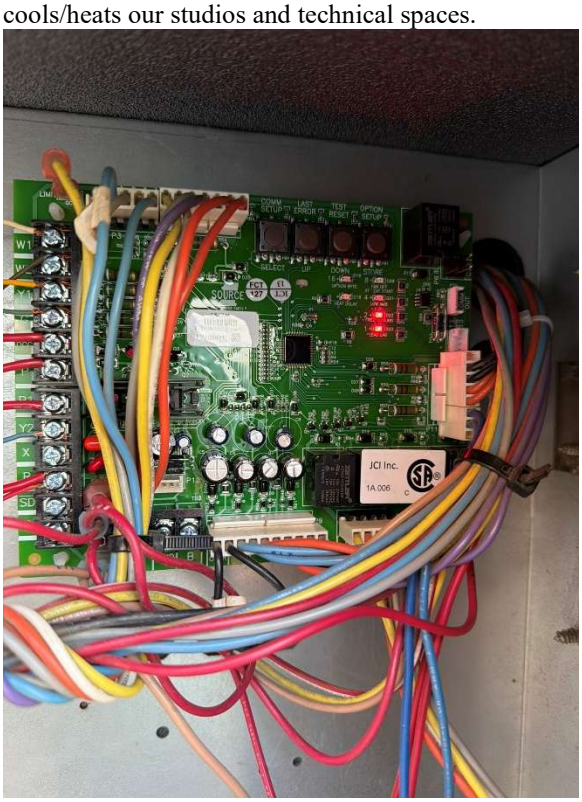
The Burk also gave me some alarms about the temperature in the building at the KLVZ transmitter site. Much like KLTT, I have an app on my phone to control the two units. I checked and sure enough, they were showing it was hot. I swapped units to allow it to cool down and went to the site.

I have found that pulling the service disconnect outside is the way to fix most issues/errors the units get. A breaker reset just doesn't seem to clear anything. So, I reset the units using the disconnect outside and tested each one. Both began blowing cold air. I went ahead and left both units on to cool down the inside of the building quickly. I have since turned one unit off.

I have since received a couple of high temp

alarms for the site from Burk, but when I check both HVAC units, they show the temperature is normal at 72. My guess is the sun is shining on the building heating up the wall where the thermostat the Burk uses is mounted.

Finally, the big issue and the most annoying was our studio HVAC RTU. We're in a high-rise building on the top regular floor (below the penthouse, which is mostly mechanical stuff), and the building HVAC either shuts down or scales back after hours and on weekends, so we have a two-stage 10-ton RTU feeding a separate zoned system that cools/heats our studios and technical spaces.



The studio RTU control board – blinky lights were telling us what the problem was.

It was very sporadic at first. It would be warm and humid in the studios. I would check and see that things weren't cooling, so, I would do a power cycle of the RTU with the circuit breaker. We have found this is a good way to clear up issues and get the unit going again, and it did this time as well. It would start cooling off well. For a few weeks, it would work for several days, sometimes over a week, before needing the reset. There was no point in calling Wern Air because by the time they would arrive, it would be working again.

I did not want to leave it not working for obvious reasons. Once again, after the holiday weekend, it began not working consistently, so I called Wern Air and they came out. They changed the filters for us and saw the control board had a bunch of red blinky lights. They were able to get the system to cool down, but assumed the issue was a faulty control board. We were able to find one and had it overnighted in.

Daniel and I changed it out. Once again, the unit began to cool. However, the next day I noticed it was warm again. I went up to the roof and saw the red lights on the board. The new board came with some documentation to explain the flashing lights. I found the issue was a second stage high pressure lockout. I called Wern Air and talked to the tech, who told me to clean the coils, so we did. Once again, the unit began cooling a bit better.

While cleaning, I noticed with the power off to the unit that one of the two condenser fans was not spinning freely – definitely something mechanically binding in there. One fan would spin if you looked at it, and kept getting in the way of my sprayer. The other fan would sit still. I was able to move it manually, but it was just not as free. This clued me in that the issue had to do with that.

After the cleaning, we turned the unit on and hung out on the roof for a good half hour. One fan would come on but that other fan would not. I thought maybe it just needed time, so the next morning I checked and found it still not running. My dad came up to the roof with me to confirm my thinking. With a nudge from a screwdriver, we got the fan moving again – sort of… it would only turn at a fraction of the normal speed, and it was humming and vibrating.

I notified Wern Air of our findings and they ordered a condenser fan motor and brought it out to install. This seems to have done the trick, as I can say it's been good and cold in our TOC since.

Now someone needs to explain to me why I had to do all the heavy lifting in troubleshooting that RTU. Why didn't the tech pick up on the code the control board was flashing out and then correlate that with the binding condenser fan? Why did we have to purchase and install a new control board when there was nothing wrong with the old one? Maybe it's time for a change…

Storms

After a very dry winter and spring, monsoon season is finally here. On Wednesday the 22nd, we had some storms roll through. That evening, I was checking the sites to see how they did after the storms and found the KLZ site was not responding in

AutoPilot. I immediately got on the computer at the site by using our backup internet service and quickly determined the issue was the Cambium microwave link. I had no access to the radio at the site, but from the office could get on the studio end and then from the transmitter side I was able to see the Ubiquiti PowerBeam on the tower. I tried a few remote power cycles – we have a 2-pole 30A contactor in series with the power feed to the tower that we can control with the Burk – but the Cambium radio would not come back to life.

The next day, the plan was to fly the tower with the drone to see if we had lights on the radio. My dad and I were able to find a tower crew to come out that morning. We confirmed no lights, so we sent up a power supply with them but also had our spare radio ready to go just in case. Thankfully, the issue was the power supply, and by mid-afternoon, the crew got the new power supply installed and us back on the microwave.

A new Omron 48-volt DIN-rail power supply in place in the NEMA box at the 400-foot level of the KLZ west tower got the link back up and running.

I must say, I love how we have things set up now. Having the Barix as our backup audio plus at KLZ, having the Gateway 4 set up with two different networks has saved us numerous times at all our sites. That main link drops and that backup internet takes care of the rest for us, and no one notices we are on backup audio, no airtime lost.

Before heading to KLZ to fly the tower and meet the tower crew, we stopped by the KLTT site. We had a couple things we needed to do. First was to put the HVAC control system Pi on a UPS. My dad worked on that while I worked on our other project, which was updating at TP Link ER707 router.

The FCC is putting rules into place for keeping the transport links secure, so, we need to find a way to secure the link that comes over the public internet. Long story short, to do this we needed to upgrade the firmware of the units as well as change the network some. The plan was to just update the unit for now. The network changes could wait. However, I clearly had a brain fart that day and decided to just do it all and do it all at once. I changed all the IP addresses for the port forwards, changed the IPs on the equipment and finally changed the main IP of the unit.

Things did not work as expected. It should have worked flawlessly, but it didn't. I worked on it for a while and would see some equipment was working but other equipment was not.

After we got the tower crew going at KLZ, I went back to KLTT, and one thing caught my eye. The NVR's camera system was on the same IP address scheme as we set up for the site. The company that sold us the system always told me that it didn't matter what the "switch" IP addresses were as they don't see the LAN, so I didn't think much of it. Clearly, they were wrong, and the NVR functions to some degree as a router.

I was able to change the switch IP address range with much difficulty. I could still get to some stuff but not others. I had to go back to KLZ to pick my dad up as the tower crew was done. I had the KLTT Bridge-IT XTRA plugged directly into the studio network via the microwave link, so we were okay. I left it for the day.

That evening, from home, I tried accessing everything on the local computer at the site by VNC. I could get to it all. Then I tried getting on everything remotely and all was right in the world.

The next morning, I went out and put the Bridge-IT XTRA back on the local network and waited for it to connect. I monitored it for a bit and found it was holding solid. At this, I figured that the NVR switch does have some effect on the network. Since it had the same IP address as the ER-707, it was causing packet collisions, making things not work. Clearly it does function as a router.

Going forward, as we move through the

various sites, I will need to remember to change our NVR first because each one is on the network IP scheme I want for the site on the ER-707.

Windows Updates

Microsoft knows best. Or at least that's their thinking. I have made it a habit to try and do Windows updates on all Zetta machines at least a couple times a year. I have been told multiple times by RCS Support that even if we have them disabled, if we ever have to reboot a computer, Microsoft may force the updates anyway which could keep a computer down for hours. I had already experienced this with NexGen. An audio server would quit responding, and the only solution was a power down reboot, then Windows update would start despite being turned off, and we'd be off air for a few hours while we could only wait.

With Zetta, the updates on the sequencers are so easy. I love how seamless "hot sparing" is. I was able to get updates done on all four sequencers with no issues.

Once I finished those, I moved on to the file server. I have only done this twice, so I called RCS Support to refresh my memory on what exactly I needed to do because the last thing I wanted to do was take any station off air. I wasn't doing this overnight, but late evening when we had paid shows on one station only. I followed their instructions and it did not go well.

The first issue was we had an employee show up late to do weekend work. I did not know he worked Friday nights. After doing one of the updates, I was able to stop the other and did a reboot of the file server. I could not get the sequencers to see the file server, though. Support looked at it and could not figure it out. I was told by the person on the phone that they had no clue.

They were going to try a WinSocket reset when that triggered a thought. Public vs Private. I asked them to wait and suggested we look at the NIC to see if it got switched to Public. Sure enough, it did. Microsoft knows best I guess and thought that would be a good idea to do when updating. We switched it to Private and things started talking.

I worked with RCS to get each station back looking at the file server. This was fine, but then the issue was that playback went back in time to when we took the database down. We would get it synced back up to the correct time, but on two of the stations, I noticed after we had done this, it still jumped back. Unfortunately, I interrupted one paid program on KLTT. Thankfully, I think that was the only paid program that was affected.

I have learned my lesson. I hate to say it, but any future updates will be done overnight. Most likely early morning (1-2AM). I was unable to get the updates finished but I did go in to the file server and sequencers and turned them off. My hope is that they stay off, especially while I am on vacation.

SBE 48 Picnic

On the 17th, our local SBE chapter hosted our annual picnic up at Lookout Mountain Park in Golden, CO. It is a beautiful site. I am unsure when we first started using the space for the summer gathering, but it's been a lot of years. It is always a fun time.

I was able to get our usual Famous Dave's BBQ for catering. Their food is good and we really like the guy they send up, Jonah. He does such a good job, and I don't have to walk him through setup. He knows where to go and what to do.

We had some nice Aircans headphones that BSW provided for us to give away. We had 28 people show up. It was really a lot of fun.

Our next big event will be our holiday party in November. I will start working on that once we return from vacation. I also have a couple meetings between now and then to prepare for.

If any of you would like to join us for our meetings online, you are always welcome. You do not need to be a member of the SBE or of this particular chapter. For the most part, we do hybrid meetings and have people from all over join. Feel free to go to our website for updates on meetings, www.sbe48.org. Our next meeting will be Wednesday August 19 at 11:30am MT. Kirk Harnack will join us over Zoom, so it will no doubt be a good time

Coming Up

With that, as I write this, I am getting ready for vacation! It is that time of year again when my parents, husband and I all head down to southwest Colorado to Lake City. This year will be a little different. They have a wildfire burning just a few miles away from town in some pretty rough terrain that can't be easily reached. We were unsure if we'd be able to go because the town was in a pre-evacuation status for a couple weeks. They also closed many of the trails that we enjoy exploring. Thankfully, as mentioned earlier, monsoon season is here and they have been getting a lot of rain. As of this writing, the town is safe. Fire crews worked hard to create some good fire lines around town. There are no pre-evacuation warnings and beginning on the 31st, they will open the trails/roads they had closed.

We pray the afternoon rain showers continue and help put the fire out.

I still have some stuff I'm trying to get done before leaving. It's always stressful because I don't have someone super experienced to watch things. Even the guys who are available to help Daniel don't know our system that well as it's all fairly new. I'm still learning it all. But the hope is that together, if something goes wrong, they can figure it out.

Thankfully the house we stay at has good Starlink internet. My husband will also bring his mobile Starlink he uses for work. He's bringing that mainly for safety reasons. We don't want to be in the woods, out of cell service, and not know if the fire has shifted or maybe there is a new fire and we need to evacuate. We figure this will be a good way to keep up to date on things. I have no plans on taking a laptop off-roading with me, but if something happens back in Denver, and I'm needed, the hope is I can do it on my phone.

August will no doubt fly by with me being gone for a full week. I honestly have nothing in the calendar for things to do at the office. I'm sure things will pop up to keep me busy once I return.

I think that about covers it for this edition. I pray you all stay safe and well!

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 • Birmingham, AL
850 kHz/96.9 MHz, 50 kW-D/1 kW-N, DA-2
WXJC-FM • Cullman - Birmingham, AL
101.1 MHz, 100 kW/410m AAT

Crawford

Corporate Engineering

2821 S. Parker Road • Suite 1205

Aurora, CO 80014