Jeff Welton

Sales Manager, USA East

Nautel

Shane Toven

Chief Engineer

Cumulus Media - San Francisco

David D. Oxenford

Partner

Wilkinson, Barker, Knauer LLP

TRANSMISSION TALK TUESDAY

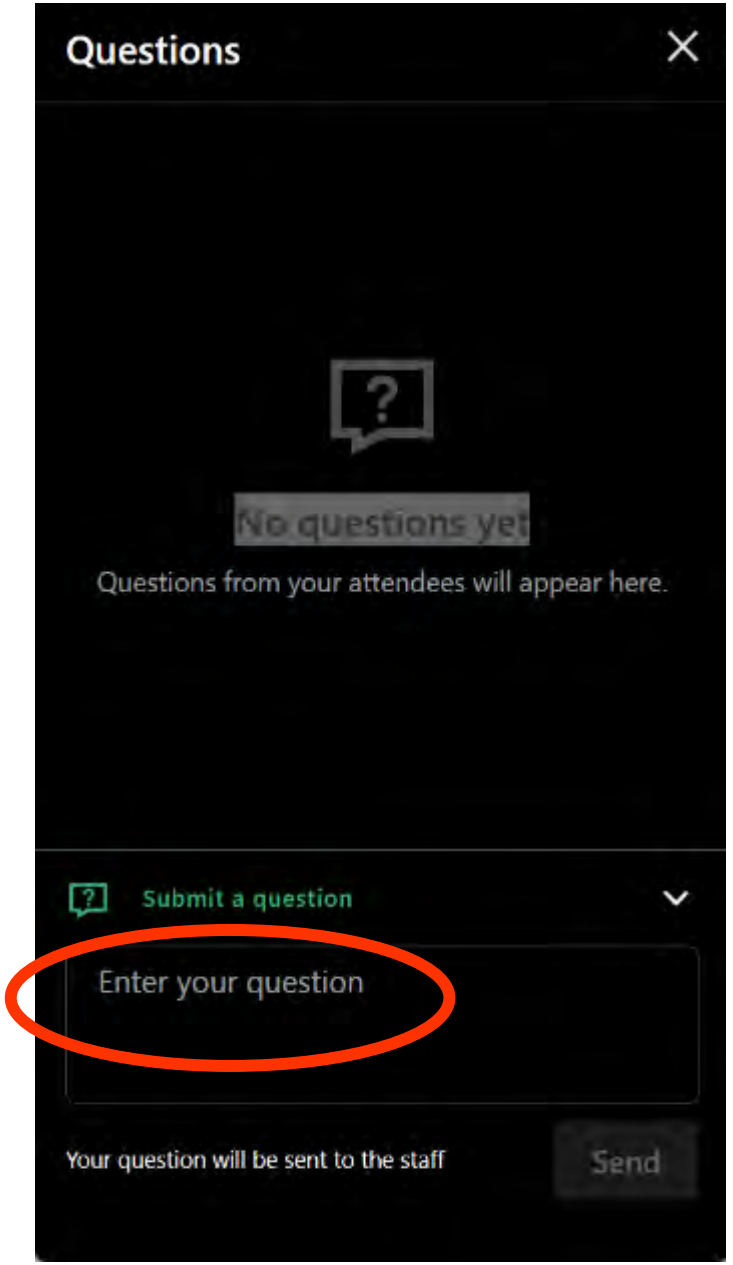
Episode #102

IT Security Implications of the FCC Report and Order/Notice

nautel

Your questions please?

1. Find Questions symbol on the webinar control menu.
2. Please enter your questions in the text box of the webinar control panel window. (remember to press send)



Remember: The completion of a Nautel webinar qualifies for ½ SBE re-certification credit, identified under Category I of the Re-certification Schedule for SBE Certifications.

Lawrence	What are the specific steps to obtain and install a sufficient firewall?
Mark	How does one prove they've implemented this three-point plan?
jason	Will the FED start testing your passwords or pen testing your firewalls?
Roger	Why are we spending money for a system that the FCC never utilizes in true emergencies...?? OK...you don't have to answer that
Shawn	Any penalty that we know of if some equipment can’t handle 15 character passwords?
David	How do you think the Commission will handle the issue of analogue S.T.L.s and their vulnerability?
Troy	Can you also address what the ramificatoins would be about software defined EAS vs hardware from a vendor and the implications?
Paul	I need some practical lessons in spectrum monitoring.
Jeff	Please address password requirements if all remote access is behind a VPN and not directly exposed to the internet.
Dale	How do you think the guidance in the report and order be verified by the FCC? Can we assume penetration testing?
Ted	We hear WHAT people should do to protect networked infrastructure. We don't often see HOW to. Esp. for LPFM, small ops. No staff
Jerry	What, if any, password allowance for being behind a firewall?
Kpasiaka	What affects transmission
SEAN	How many of you use a commercial firewall product that has a yearly subscription for support and category-blocking updates?
Nabaraj	We stared formal education for women in primary level.
Maurice	Does this rule apply to all IP (internal and external) access devices or only to publicly accessible IP devices?
Dave	Isn't it enough that all airchain devices and transmitters are on a private LAN behind a firewall with excellent security?
Eshima	As ministries and nonprofit organizations increasingly use internet-connected broadcast and digital media systems to serve commu
Kevin	What is implied by Network segmentation/separation for something that needs public internet to get to the cap messages
Matt	Looking down the road, do you expect the EAS daisy-chain to exist long-term, or is this the opening salvo in a move to WEA etc.?
Vic	I'm going to try to make this , but if not , will this be recorded ? Thank You

The 2013 and 2017 "Zombie Apocalypse" Hacks

The most famous EAS cyberattacks occurred on February 11, 2013, affecting multiple television stations, including KRTV in Great Falls, Montana, and WBUP and WNMU in Marquette, Michigan. [1, 2]

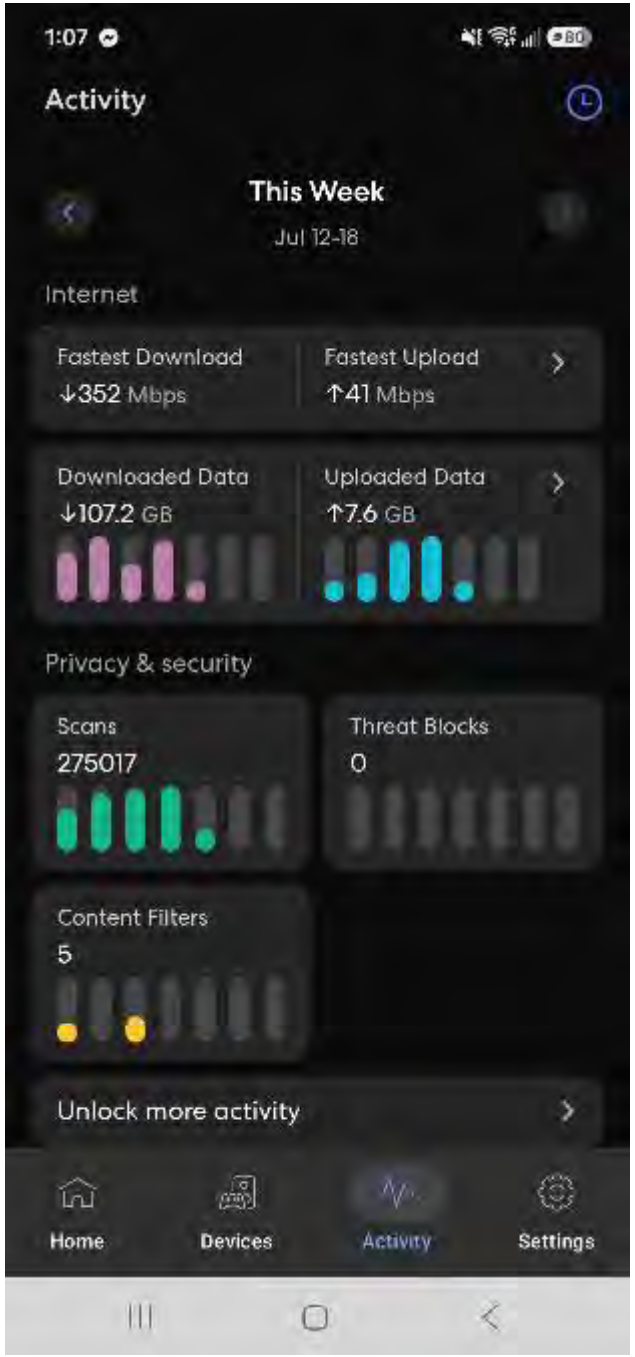
- The Incident: Attackers overrode the stations' regular programming to broadcast a crawl and audio warning stating that "the bodies of the dead are rising from their graves and attacking the living." [1, 2]
- The Vulnerability: Security researchers at IOActive discovered that the Monroe Electronics DASDEC encoder/decoder appliances shipped with root-privileged SSH keys hardcoded directly into the firmware. This allowed remote attackers to log into internet-exposed devices with administrative control. [1]
- The Follow-up: In February 2017, radio station WZZY in Winchester, Indiana, was targeted with the exact same "zombie" audio because the station was running unpatched Sage ENDEC equipment using default credentials. [1, 2]

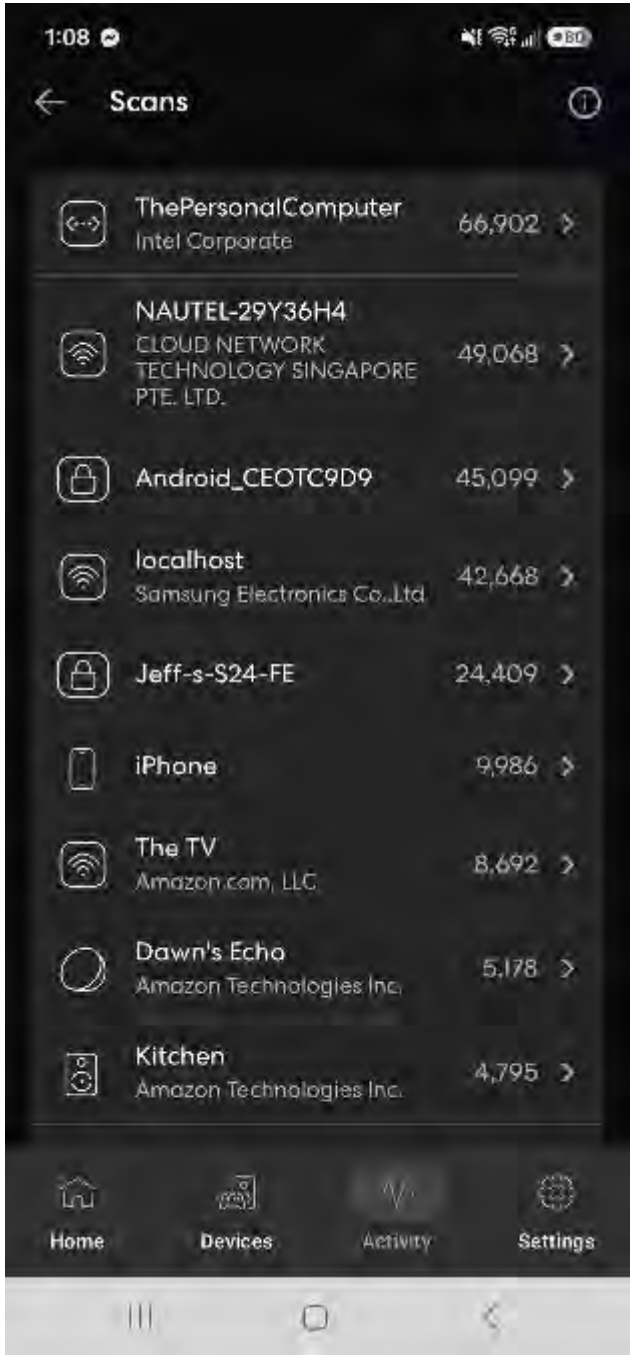
Recent Studio-Transmitter Link (STL) Hijacks

In late 2025, a new string of cyber intrusions hit regional U.S. radio broadcasters, including Houston's ESPN 97.5 and local NPR affiliates. [1, 2]

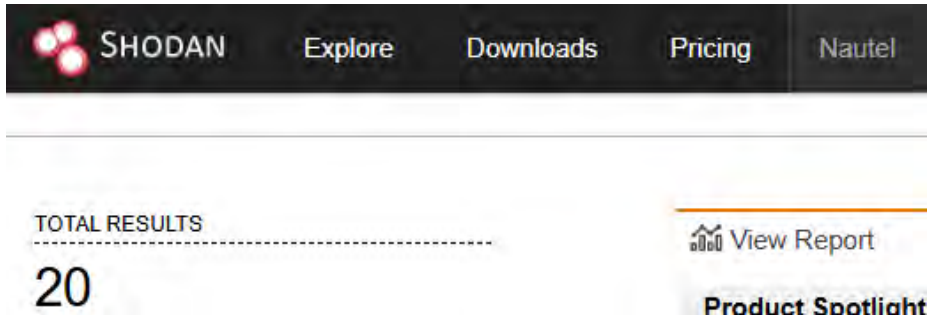
- The Incident: Hackers interrupted live programming (including a Dallas Cowboys broadcast) to inject simulated EAS attention signals, offensive/racist music, and social media promos. [1]
- The Vulnerability: The Federal Communications Commission (FCC) issued an official warning revealing that threat actors did not breach the core EAS boxes directly. Instead, they targeted insecure Studio-Transmitter Links (STLs)—specifically exposed Barix audio-over-IP equipment. Hackers used these open paths to reconfigure the audio feed sent to remote transmitters. [1, 2, 3]

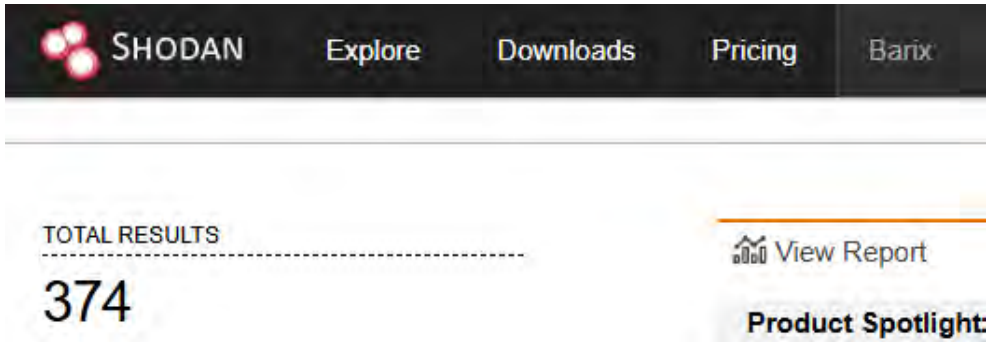
Google search term: “station EAS hack”

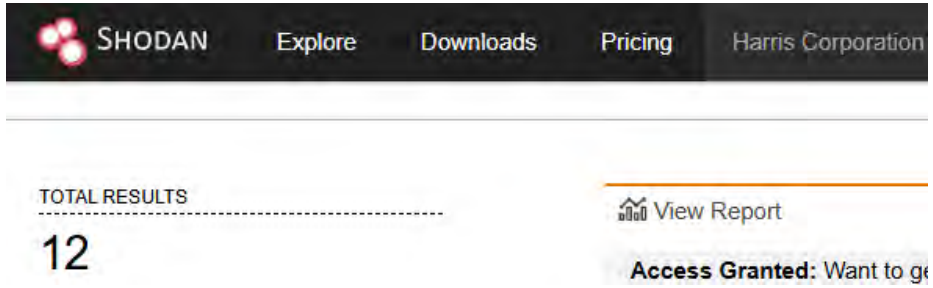


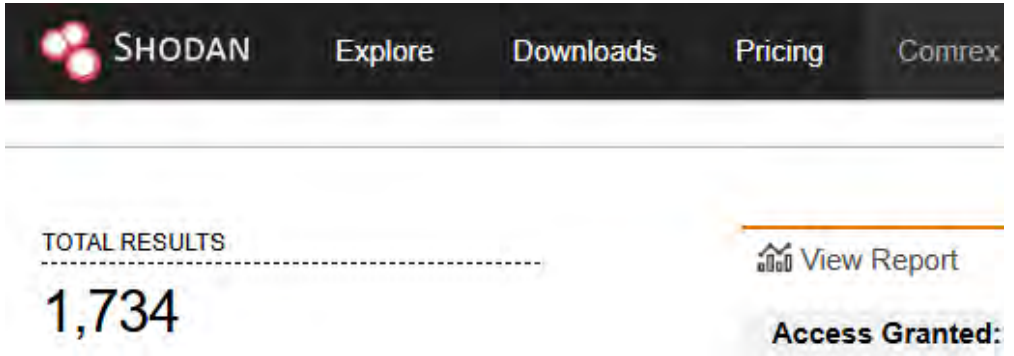


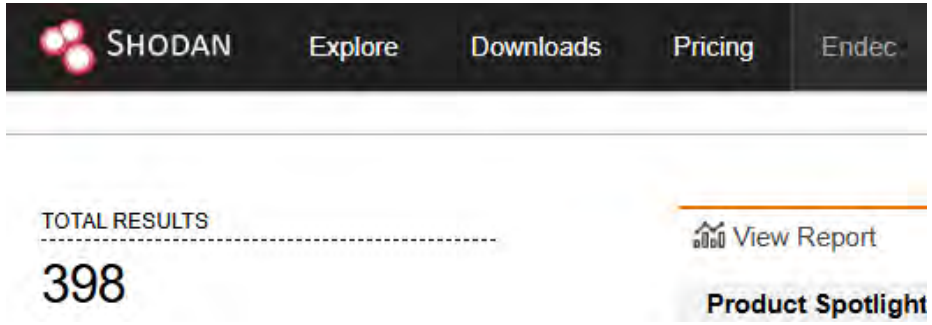
TRANSMISSION TALK TUESDAY











Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Modernization of the Nation's Alerting Systems	)	PS Docket No. 25-224
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	)	PS Docket No. 22-329
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System	)	PS Docket No. 15-94

REPORT AND ORDER IN PS DOCKETS 25-224 AND 22-329, AND FURTHER NOTICE OF PROPOSED RULEMAKING IN PS DOCKETS 25-224, 15-94, AND 15-91

https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf

Published in the Federal Register on July 31, so deadline for compliance is September 29, 2026!

Open **Ports**

22 80 161 443

nautel

Active Preset: [redacted]

[redacted] FM 102.30 FM - 402 W

07 Sep 2024 - 08:18:28

Remote Local | 402 W | 17.0 W | 87.3 °F | 96.7 % | RF On RF Off | 1

nautel

Active Preset: Normal 1

[redacted] 100.70 FM - 314 W

07 Sep 2024 - 09:31:46

Remote Local | 313 W | 0.57 W | 70.2 °F | 99.7 % | RF On RF Off

nautel

Active Preset: Preset 1

93.30 FM - 341 W

07 Sep 2024 - 09:36:21

Remote Local | 341 W | 3.58 W | 64.9 °F | 52.2 % | RF On RF Off

nautel

Active Preset: Preset 1

[redacted] 88.70 FM - 500 W

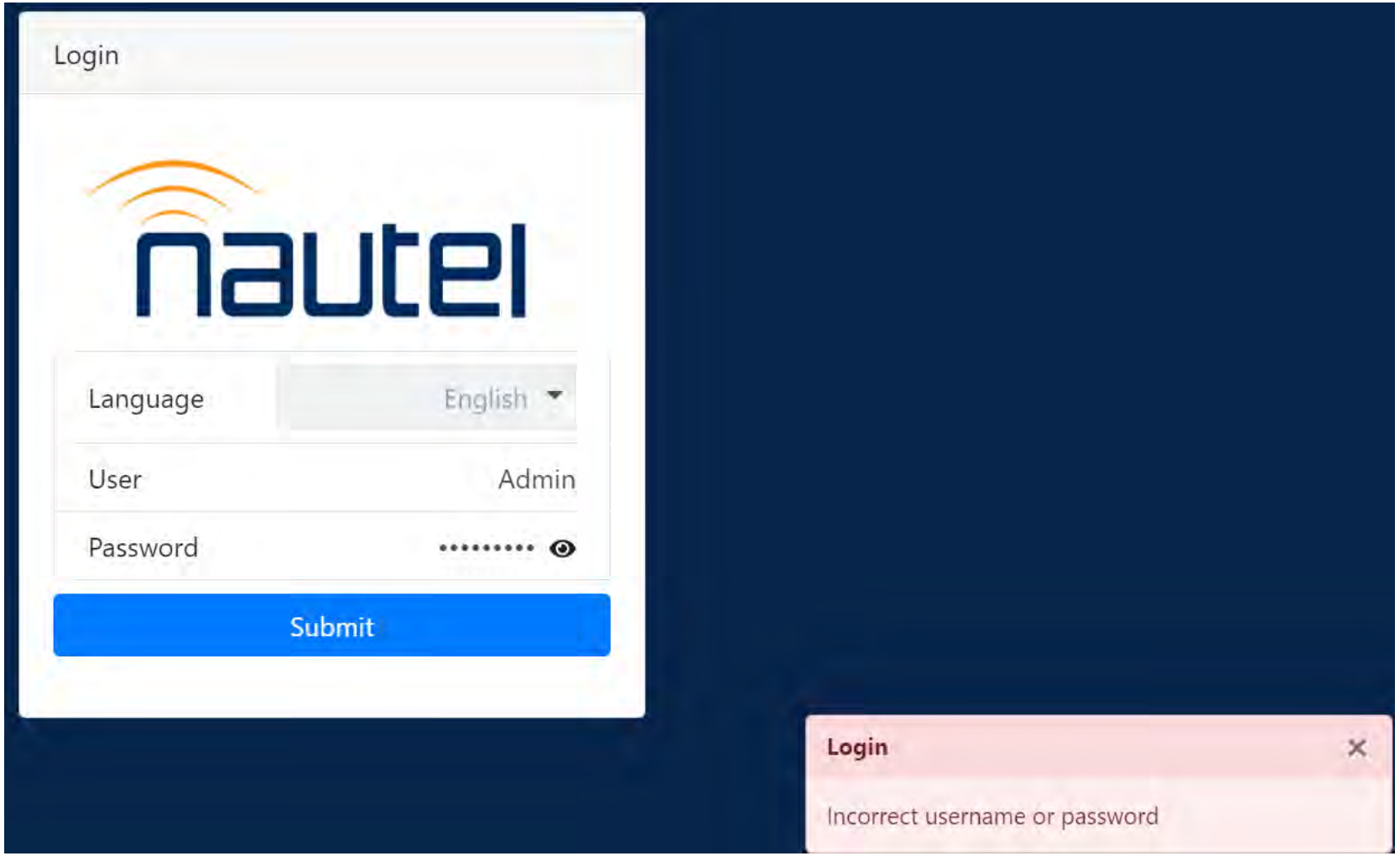
07 Sep 2024 - 07:45:35

Remote Local | 499 W | 0.08 W | 63.5 °F | 97.2 % | RF On RF Off

TRANSMISSION TALK TUESDAY

18. *Password requirements*. Strong password security is essential to protecting EAS equipment, studio-transmitter link equipment, and remotely accessible equipment from unauthorized access that exploits weak or default credentials. Digital Alert Systems, Inc. (DAS) and former broadcaster, Jonah Kibin, caution against using default passwords and recommend changing required credentials upon setup as default passwords, particularly on encoders, "are widely available on the internet and have led to high-profile intrusions of the EAS in the last couple of decades."[68] We require that default passwords for EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream be changed prior to any use to broadcast to the public. Passwords used for this equipment must employ a minimum of 15 characters, not use dictionary words (because they can be cracked through brute force), and not be reused for other accounts, equipment, applications, and services that the EAS Participant uses.

https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf



TRANSMISSION TALK TUESDAY

IT Administration

A Free Tool To Comply With The New FCC EAS Password Rule – And More!

Written By Ken Fine Posted In IT Administration.

The FCC has issued the Public Notice and Order requiring EAS units to be held to a much tighter security standard

BDR Password Generator

By Ken Fine and Claude AI

Date of generation: **Jul 13, 2026**

Password for

EAS

New password Copy

Password for **EAS**

`8IYd3n9bEtyaz6ei`

19. As an alternative to a strong password, we permit EAS Participants to use alternative authentication measures that are reasonably sufficient to mitigate the risk of unauthorized access. We believe that there are numerous authentication methods available to EAS Participants that would be reasonably sufficient, including methods that have been highlighted by the National Institute of Standards and Technology (NIST) as meeting one of three authentication assurance levels.[69] For example, NIST's guidance provides that authentication properly implemented at Authentication Assurance Level 1 can include, in addition to passwords, look-up secrets, which are "[a] secret determined by the claimant by looking up a prompted value in a list held by the subscriber"; out-of-band devices, consisting of "[a] secret sent or received through a separate communication channel with the subscriber"; single- or multi-factor one-time password devices, in which a one-time secret is obtained from a device or application held by the subscriber, which may or may not require activation by a second authentication factor; and single- or multi-factor cryptographic authentication, which entails "[p]roof of possession and control via an authentication protocol of a cryptographic key held by the subscriber," which may or may not require activation by a second authentication factor.[70] We recognize that, were we to simply require use of specifically structured passwords, our rule could preclude the use of other authentication methods offering

https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf

Step 3: Introducing … GV²

Studio

IP STL

Transmitter

JUST ADD AUDIO

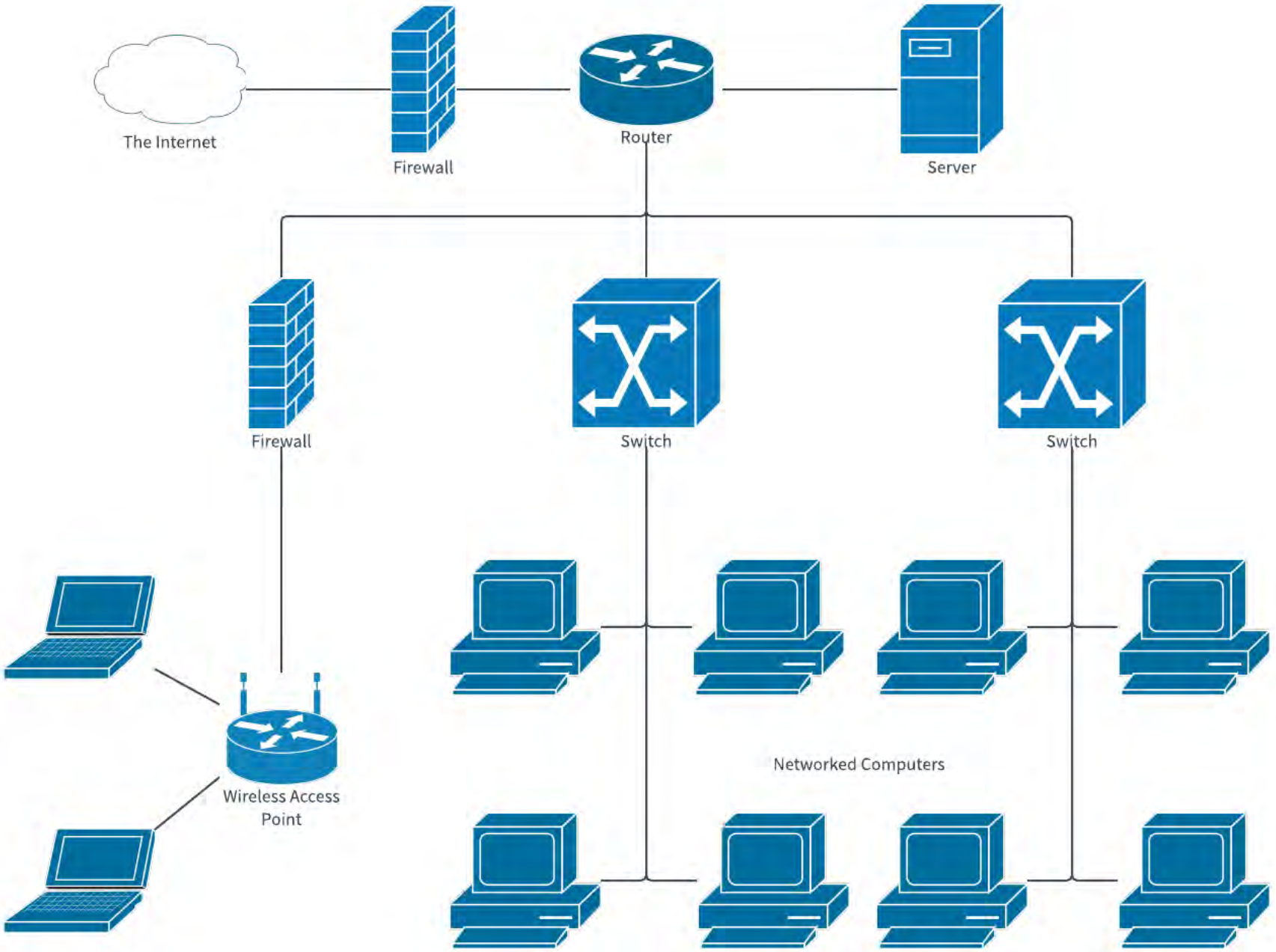
Livewire

Integrated HD
Audio Processing
STL solution

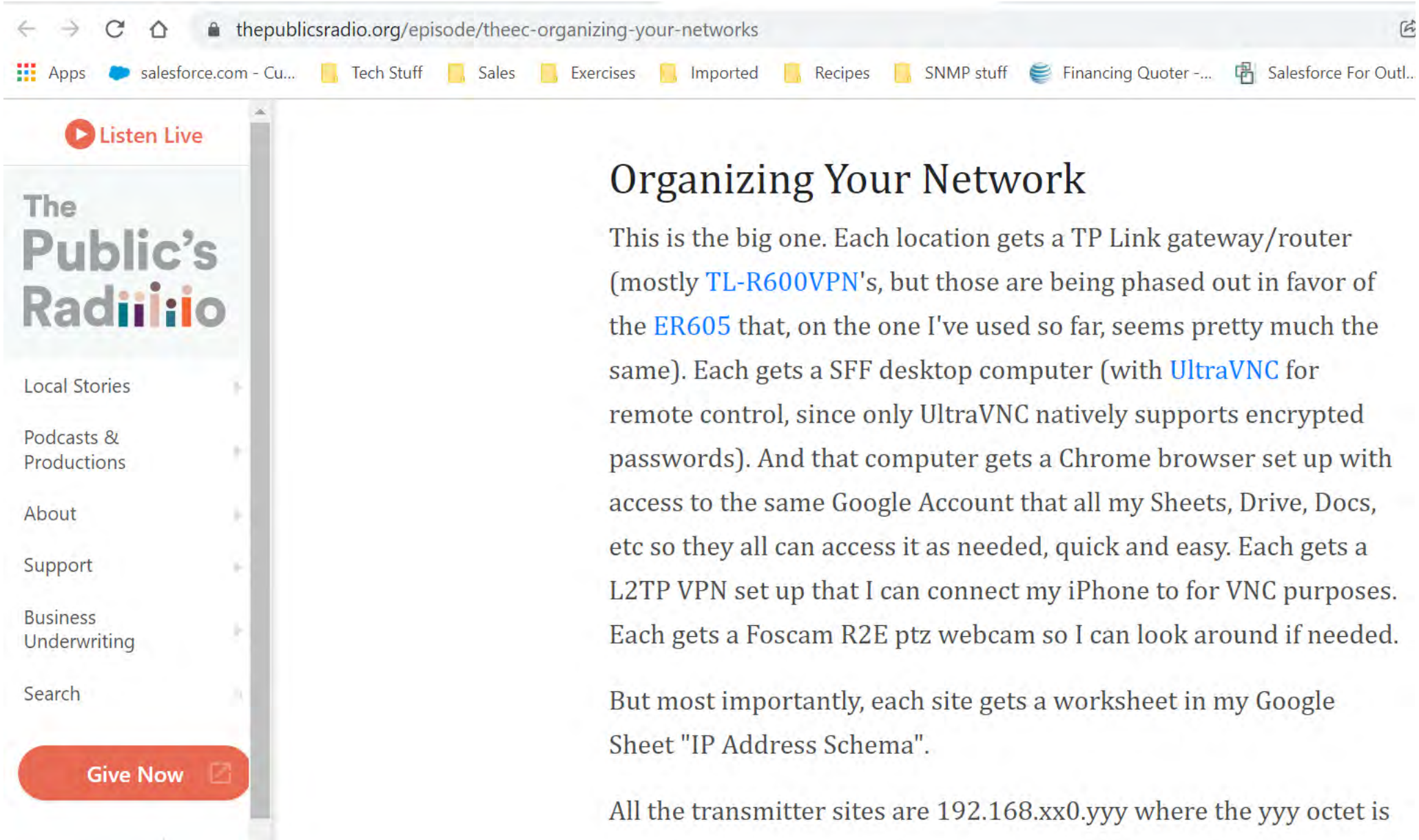
TRANSMISSION TALK TUESDAY

21. Firmware and Software Patching. Prompt firmware and software patching are key to reducing the risk that bad actors will exploit known vulnerabilities to infiltrate broadcast and cable systems to insert false EAS tones or alerts. The record includes support for requiring EAS Participants to promptly install security patches and firmware and software updates. DAS also points to the failure to apply software updates as a “systemic risk[]” to EAS.82 One comment submitted by a radio broadcast engineer recommends that the Commission require EAS equipment to automatically query a centralized database to confirm EAS codec firmware and certificate updates.83 APCO opines that “[t]he Commission should consider rules requiring EAS and WEA participants to maintain current software and replace outdated equipment in a timely manner,” citing findings from the Commission’s 2023 Nationwide Emergency Alert Test showing that “approximately 23 percent of the EAS equipment units were either using outdated software or operating equipment that was no longer supported with regular software updates.”84 The fact that nearly a quarter of EAS devices may potentially be exposed to known, readily addressed vulnerabilities because they are operating obsolete or out-of-date equipment represents a significant gap in the security of the nation’s alerting capacity that poses national security risks.

https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf



https://www.edrawmax.com/network-diagram/how-to-draw-a-network-diagram/


thepublicsradio.org/episode/theec-organizing-your-networks
Apps
salesforce.com - Cu...
Tech Stuff
Sales
Exercises
Imported
Recipes
SNMP stuff
Financing Quoter -...
Salesforce For Outl..
Listen Live
The Public's Radiiiio
Local Stories
Podcasts & Productions
About
Support
Business Underwriting
Search
Give Now
Organizing Your Network
This is the big one. Each location gets a TP Link gateway/router (mostly TL-R600VPN's, but those are being phased out in favor of the ER605 that, on the one I've used so far, seems pretty much the same). Each gets a SFF desktop computer (with UltraVNC for remote control, since only UltraVNC natively supports encrypted passwords). And that computer gets a Chrome browser set up with access to the same Google Account that all my Sheets, Drive, Docs, etc so they all can access it as needed, quick and easy. Each gets a L2TP VPN set up that I can connect my iPhone to for VNC purposes. Each gets a Foscam R2E ptz webcam so I can look around if needed.
But most importantly, each site gets a worksheet in my Google Sheet "IP Address Schema".
All the transmitter sites are 192.168.xx0.yyy where the yyy octet is

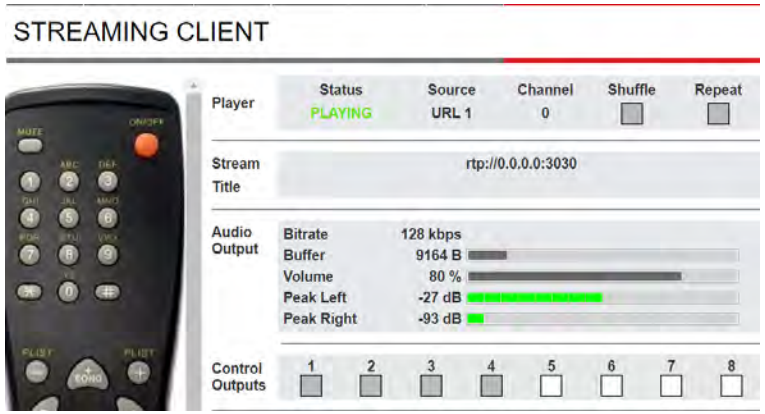
22. Use of a Firewall or Comparable Network Segmentation. We require EAS Participants to use a network firewall or comparable network segmentation practices to limit remote management access to authorized devices and authorized users, which will secure EAS and other vulnerable equipment on a private network inaccessible to the public Internet. This requirement addresses a widespread EAS vulnerability. In response to the Alerting Security NPRM, REC Networks identified 730 EAS Participant servers through which the password screen for Sage Alerting Systems' ENDEC EAS device was directly exposed.87 Of those servers, 288 operated on port 80, which is the default port for HTTP web services.88

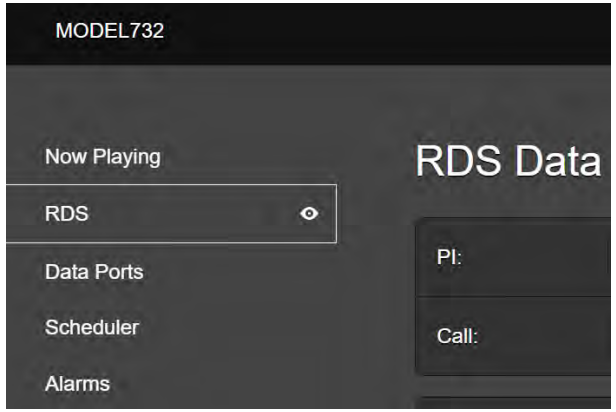
https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf


Login
nautel
Connected to
Please enter


Open Ports
8080
8081
8082
8086
10001


N750 Wireless Dual Band Gigabit Router
Model No. TL-WDR4300

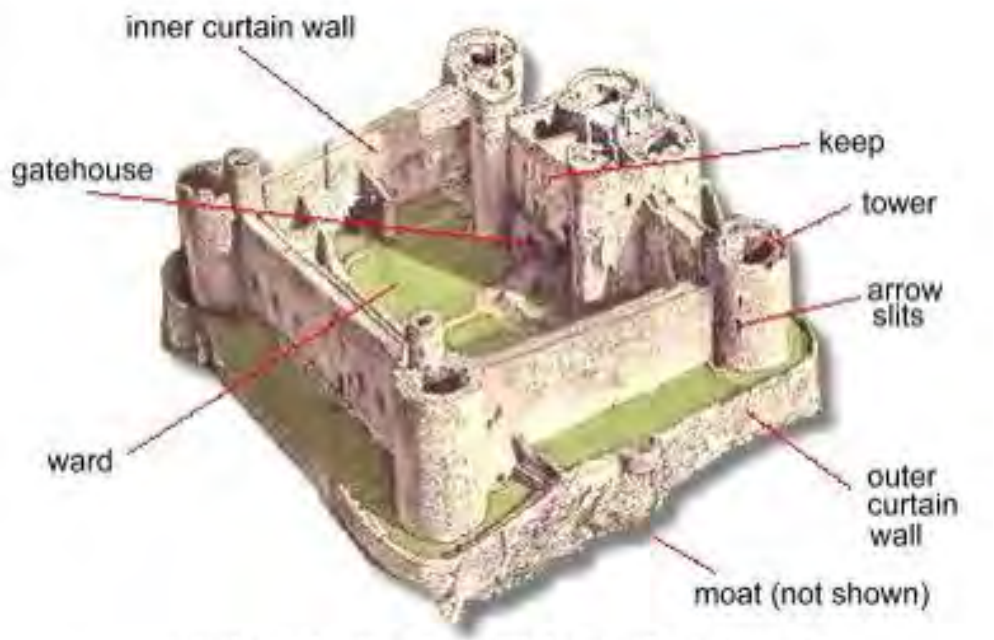

STREAMING CLIENT
Player
Status
PLAYING
Source
URL 1
Channel
0
Shuffle
Repeat
Stream Title
rtp://0.0.0.0:3030
Audio Output
Bitrate
128 kbps
Buffer
9164 B
Volume
80 %
Peak Left
-27 dB
Peak Right
-93 dB
Control Outputs
1
2
3
4
5
6
7
8


MODEL732
Now Playing
RDS
Data Ports
Scheduler
Alarms
RDS Data
PI:
Call:

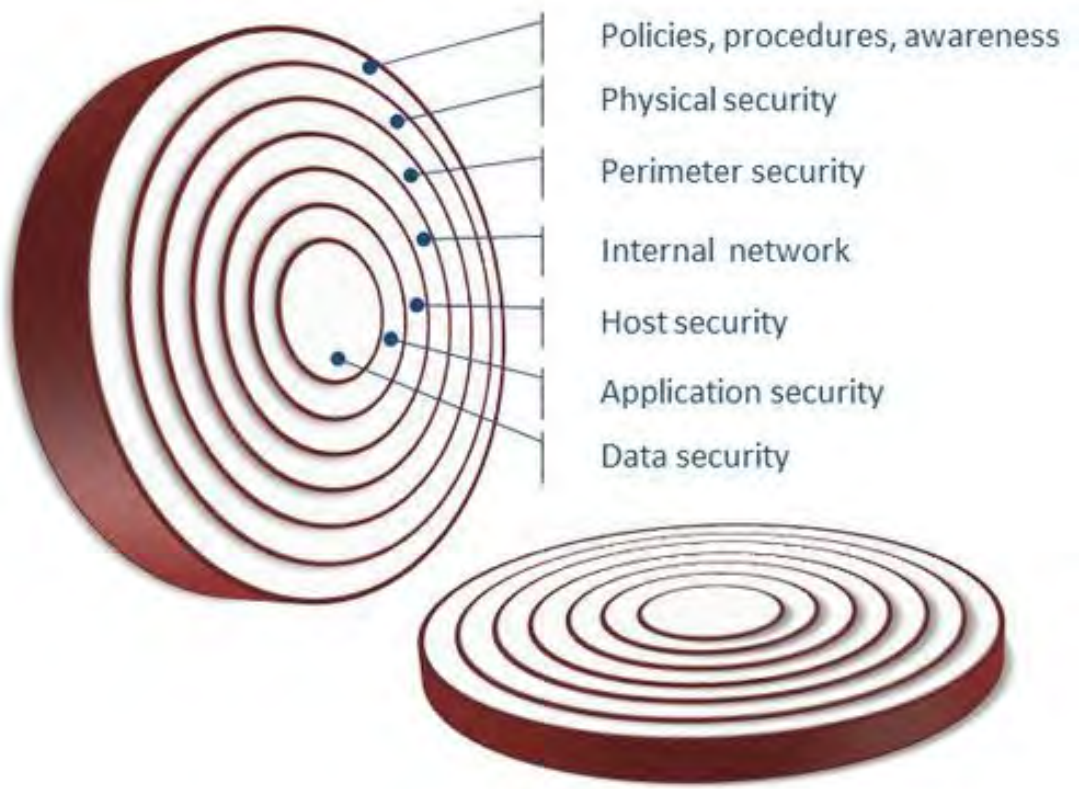

TRANSMISSION
TALK
TUESDAY

Security Zones

Segmented Network Architecture



Harlech Castle, North Wales, built in 1283 AD



The “Onion Approach”

Do These 10 Things

Essential

- Change default logins
- Use strong passwords (paraphrases)
- Separate Admin & User accounts on hosts (WIN)
- Segment your network (VLAN) – create multi-layer security zones
- Use packet filtering to control host access (ACL and/or firewall)
- Disable un-used services – close ports not used
- Monitor your network – know what is normal
- Use secure access (SSH not telnet)
- Use VPN for off-site access
- Don’t be a social engineering victim – educate users

Centrally managed security

"Your device is temporarily blocked from synchronizing using Exchange ActiveSync until your administrator grants it access."

Zero Trust vs. BYOD

Hardware

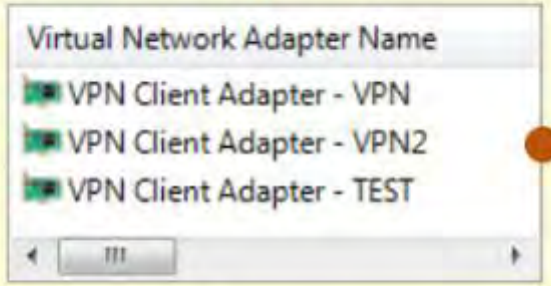
Ethernet Adapter

Ethernet Cable

Ethernet Switch

Virtualization with SoftEther VPN

Software



VPN Tunnel

Virtual Hub Name	Status	Sessions	MAC Tables	IP Tables
BEIJING_SEGMENT	Online	0	0	0
CHINATEST	Online	2	0	0
moosta	Online	3	3	5
Okkota	Online	0	0	0
SoftEther Network	Online	20	474	430
TEST1	Online	0	0	0
UT	Online	0	0	0
VLAN	Online	3	514	2

Virtual Ethernet Adapter

VPN Session over TCP / UDP

Virtual Ethernet Switch (Virtual Hub)

TRANSMISSION TALK TUESDAY

Pros of HW

- Appliance based - Usually can have some kind of support contract
- Dedicated hardware
- Multiprotocol support

Cons of HW

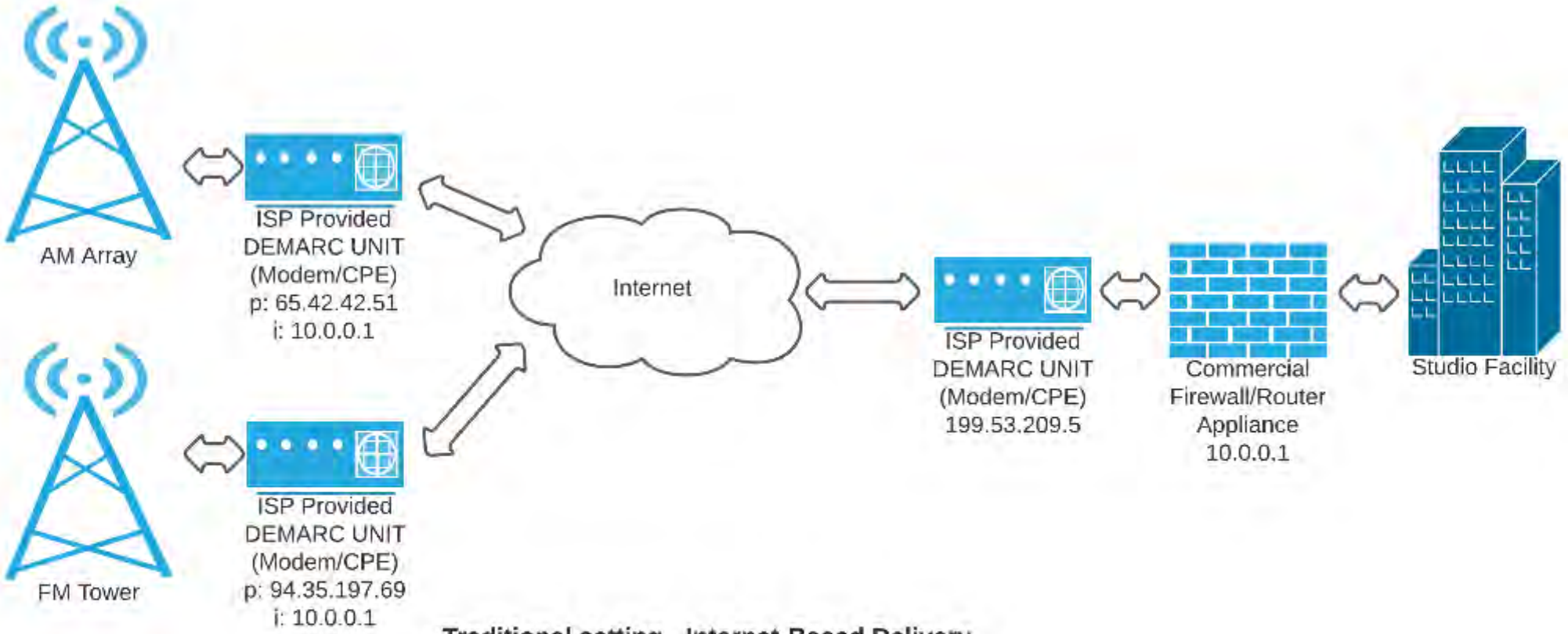
- Can be limiting in advanced network topologies
- Cheaper units cannot support lots of remote sites/users
- Can sometimes require a separate authentication system to maintain

Pros of SW:

- Configurable, multiprotocol support
- Installation can be quite simple
- Easy to rollback using snapshots (if enabled, different webinar)
- Can be locked down to single hosts

Cons of SW:

- Gets a little tricky when trying to share with other devices on your networks
- Can be limiting depending on topology
- Requires a little under the hood work at times to implement
- At the mercy of the PC if running critical infrastructure



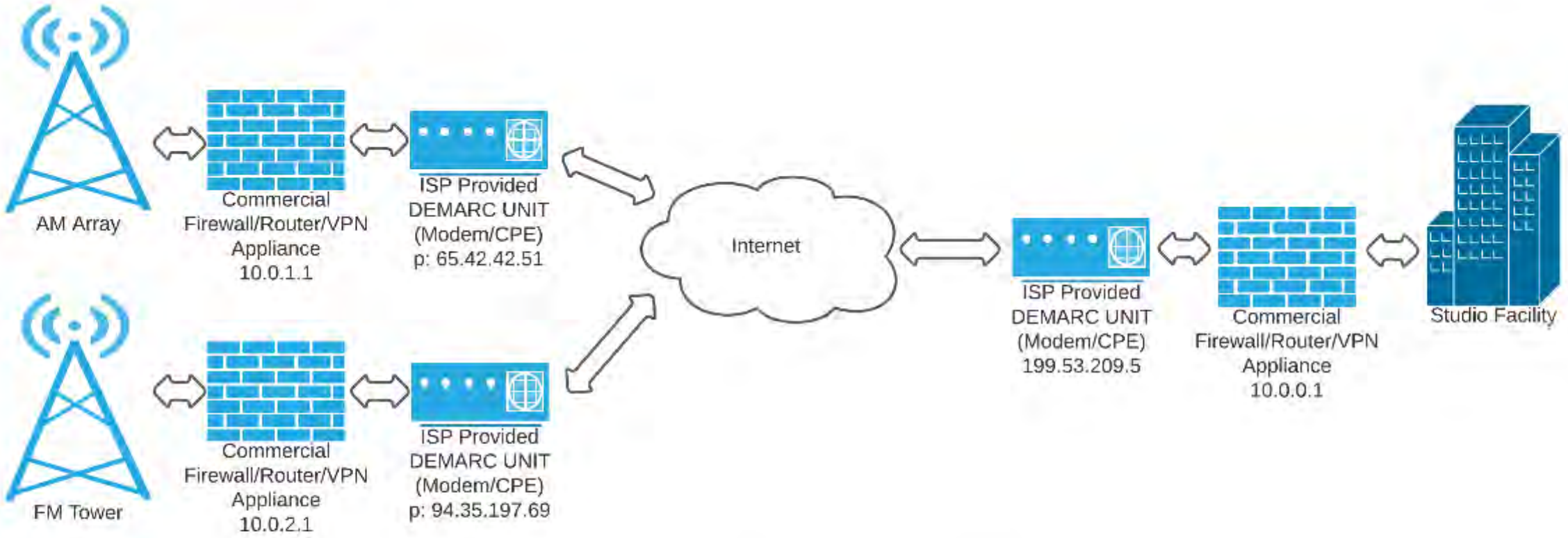
Traditional setting - Internet-Based Delivery

Punch holes through firewalls to deliver audio
Punch holes through firewall to get telemetry
Punch holes through firewall for remote access

DON'T DO THIS!

https://www.lucidchart.com/pages/

TRANSMISSION TALK TUESDAY



Site-to-SiteVPN Topology - Commercial Appliances

All Internet Traffic through VPN tunnels
No externally visible ports
All traffic is inspected by the home firewall if internet access is required (No "Split-tunnel")
All sites authenticated

I try to keep track of all the vulnerabilities, but it's getting harder and harder as time passes. RedHat alone sends out as many as a dozen reports a day; most are for minor bug fixes, but a few are true show-stoppers. As I write this, I just installed a newly-patched Linux kernel on our web server. All of those RedHat advisories made me suspect that it was time to upgrade. Indeed it was.

Stephen Poole, from Crawford Media Group's January engineering newsletter

Resources/Useful Links

Broadcast Law Blog (Discussion of FCC, copyright, advertising and other legal issues from David Oxenford):
https://www.broadcastlawblog.com/2026/07/articles/

KnowBe4 (User cybersecurity training and testing):
https://www.knowbe4.com

1Password (Password management):
https://1password.com/

Lucidchart (Network diagramming):
https://lucid.co/lucidchart

Angry IP Scanner (Scans a network for live systems and specified network ports):
https://angryip.org/

NMAP (Far more advanced tool, includes some "preset" scan modes, can do network mapping with Zenmap GUI):
https://nmap.org/

Wireshark (Analyze traffic on a network):
https://www.wireshark.org/

VPN Basics:
https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html

Tailscale+WireGuard (a software-based VPN solution):
https://tailscale.com/wireguard-vpn

VLAN Basics:
https://www.firewall.cx/networking/vlan-networks/vlan-concept.html

Ubiquiti UniFi (networking hardware and software defined networking):
https://www.ui.com/

CBT Nuggets (IT Training site that has helpful blogs on various IT related topics)
https://www.cbtnuggets.com/blog

Shodan (IoT search engine with various free and paid options, including the ability to search IP addresses or ranges):
https://www.shodan.io/dashboard

Online Information

Webinars
https://www.nautel.com/resources/webinars/

Nautel Waves Newsletter
https://www.nautel.com/newsletters/

YouTube
http://www.youtube.com/user/NautelLtd

Online Info, such as the Broadcasters' Desktop Resource
https://www.thebdr.net/

THANK YOU!