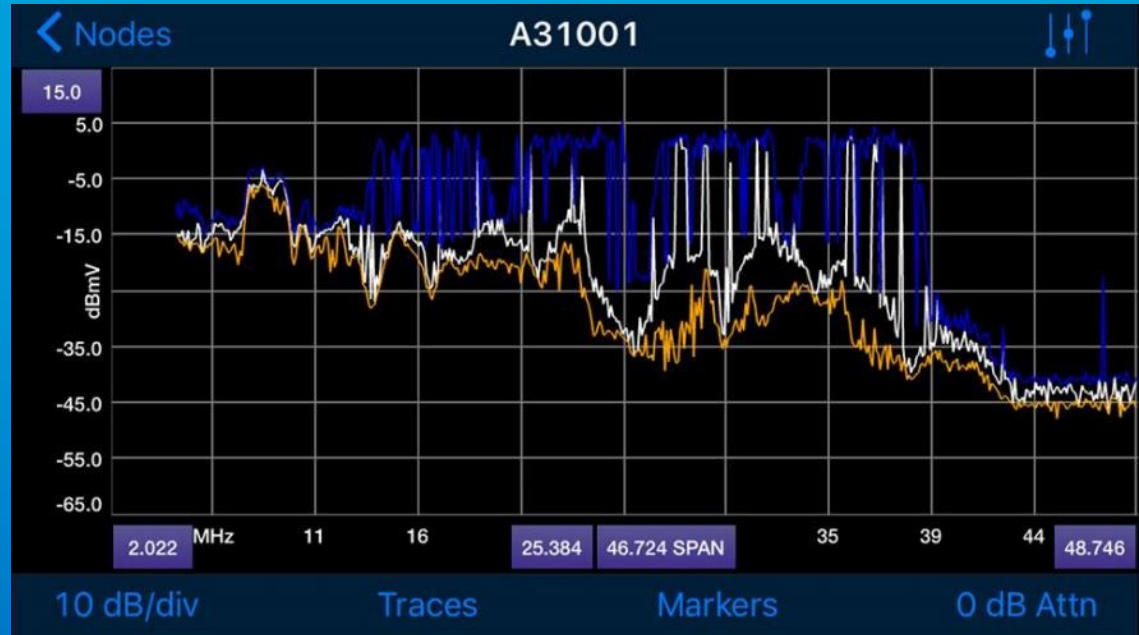


Signal leakage, ingress, and direct pickup (Part 1):

A Closer Look

Ron Hranac

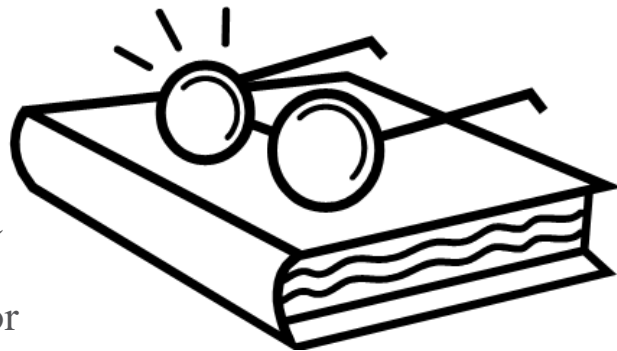


Terminology

Ingress – in·gress (in' gres) *n.* [< L. *in-*, into + *gradi*, to go]

The unwanted entrance of over-the-air signals into a cable network, caused by degraded shielding effectiveness of the network's coaxial cables and/or other components.¹ Opposite of signal leakage.

Signal leakage – sig·nal (sig' n'l) leak·age (lek' ij) The unwanted emission of radio frequency signals from inside of a cable network into the over-the-air environment, caused by degraded shielding effectiveness of the network's cables and/or other components. Also called egress.



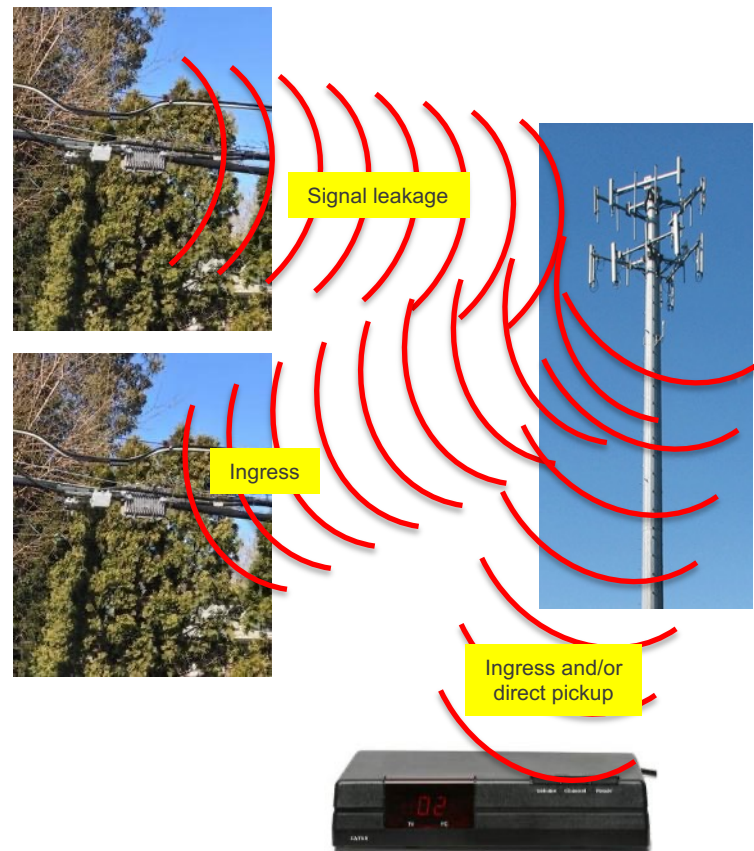
1. Note: **Direct pickup** is similar to ingress, except that the over-the-air signal(s) enters a susceptible set-top, cable modem, TV set, test instrument, or other device directly, often without any cables or other external devices physically connected. If the susceptible device's outer case or cover is inadequately shielded, then the internal wiring, printed circuit board traces, and/or components can directly receive interfering over-the-air signals.

What causes ingress and leakage?

- Coaxial cables and other components used in the distribution and subscriber drop portions of a cable TV network provide a **shielded transmission medium** that is independent of the over-the-air environment.
- Over-the-air radio frequencies are allocated to various services by government agencies, while cable operators largely enjoy the ability to use frequencies within their closed networks as they see fit.
- A cable TV network is theoretically a **closed transmission medium**, allowing the use of frequencies or channels inside of the coaxial cable and components that may be used for something else altogether in the over-the-air environment. What is called **frequency reuse** allows cable operators to provide a wide variety of services via their broadband networks.

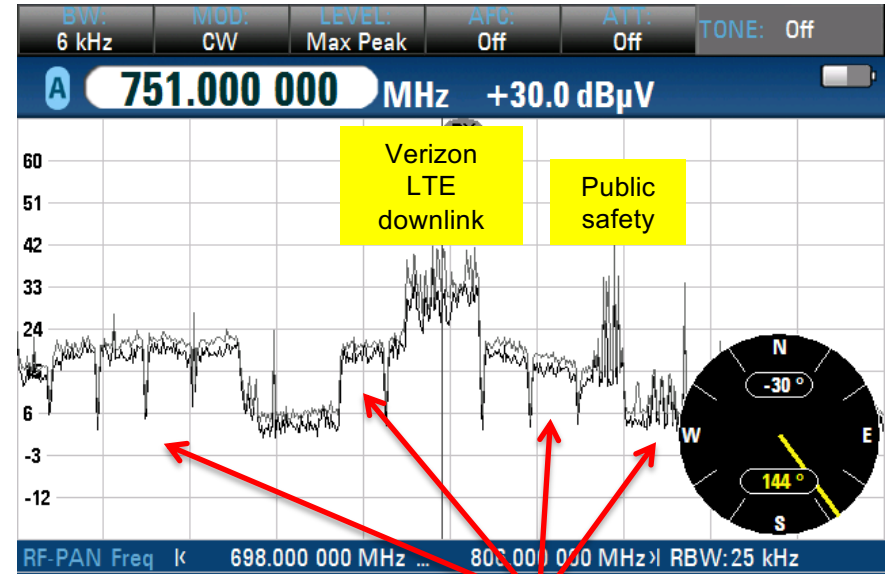
What causes ingress and leakage?

- If the **shielding integrity** of the cable network is compromised for any reason, then signals inside of the network can leak out and potentially interfere with licensed over-the-air services.
- Going the other direction, over-the-air signals can leak into the cable network, and potentially interfere with signals inside of the cable network.



Signal leakage interference

- **What:** Signals inside of the cables leak out, causing interference to over-the-air services such as long term evolution (LTE)
- **How:** Shielding effectiveness of the cables and components degraded for some reason
- **Why is this important?** Harmful interference can occur to over-the-air users, resulting in government penalties (\$\$) or worse!



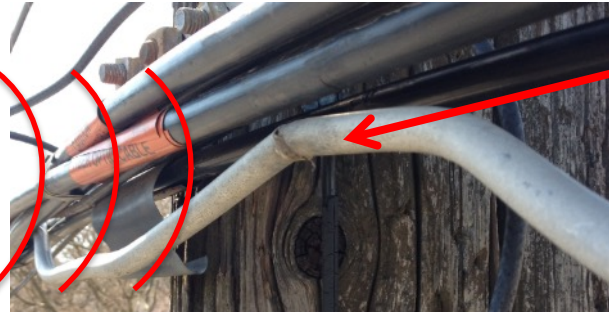
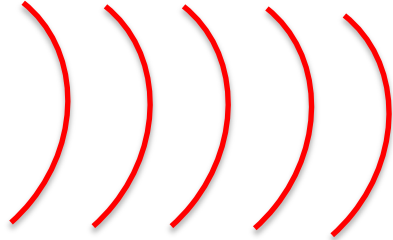
Leaking SC-QAM and other signals present in over-the-air spectrum

Ingress interference

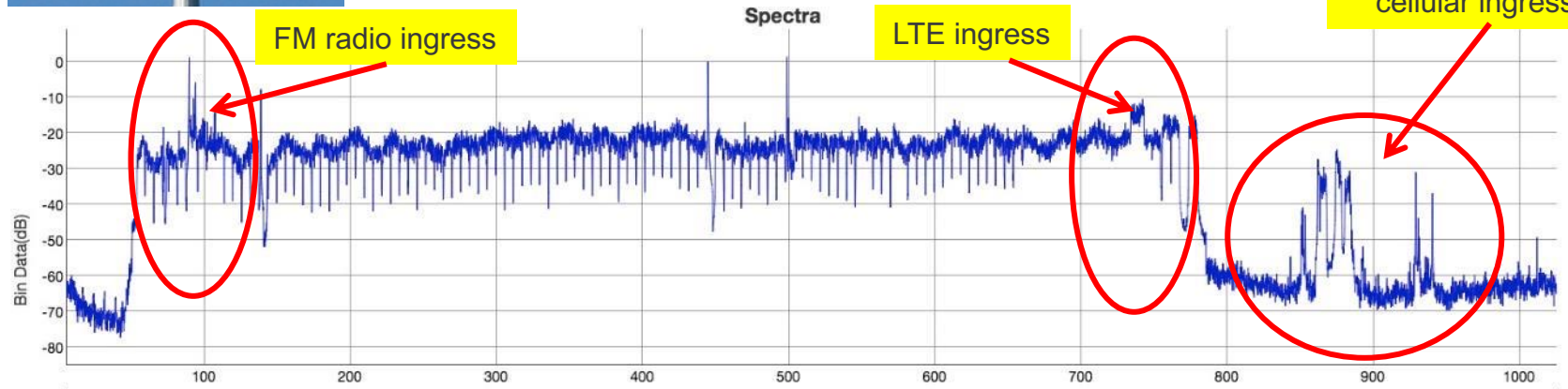
- **What:** Over-the-air signals leak into the cable network
- **How:** Shielding effectiveness of the cables and components degraded for some reason
- **Why is this important?**
Interference can occur to cable network's signals and services



Ingress interference in the outside plant

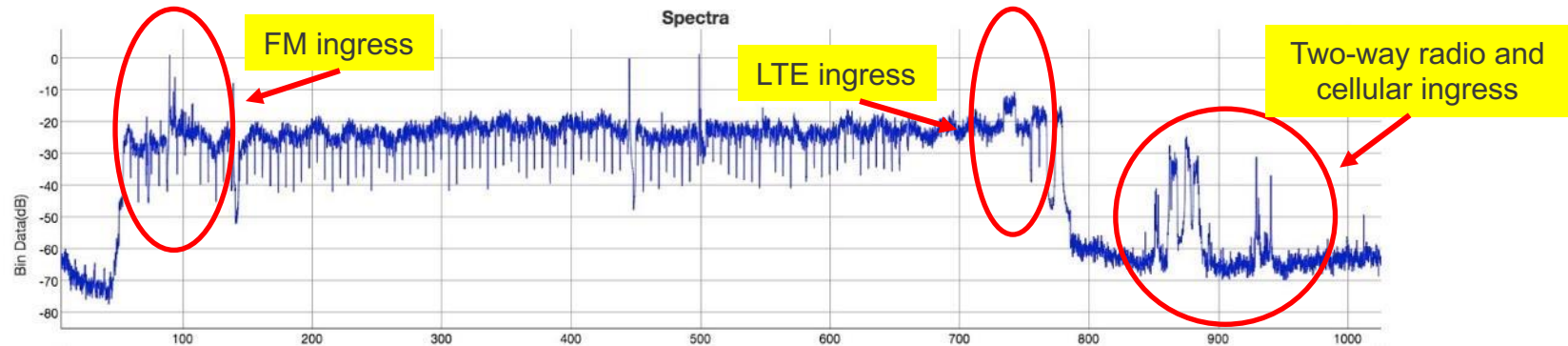


Ingress enters through crack in cable (or some other shielding defect)



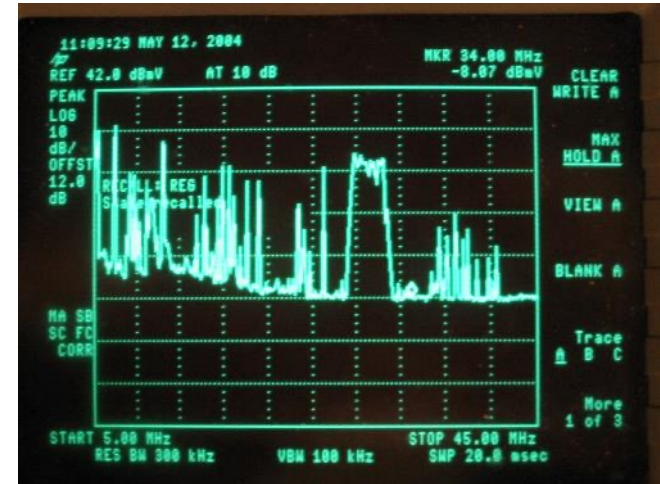
Cable network ingress

Downstream ingress usually manifests itself as in-channel interference to analog TV channels and digitally modulated signals. Common sources include two-way radios (commercial, government, amateur or “ham”), local TV and FM radio broadcast signals, LTE downlink signals (tower to user equipment), and LTE uplink signals (UE to tower).

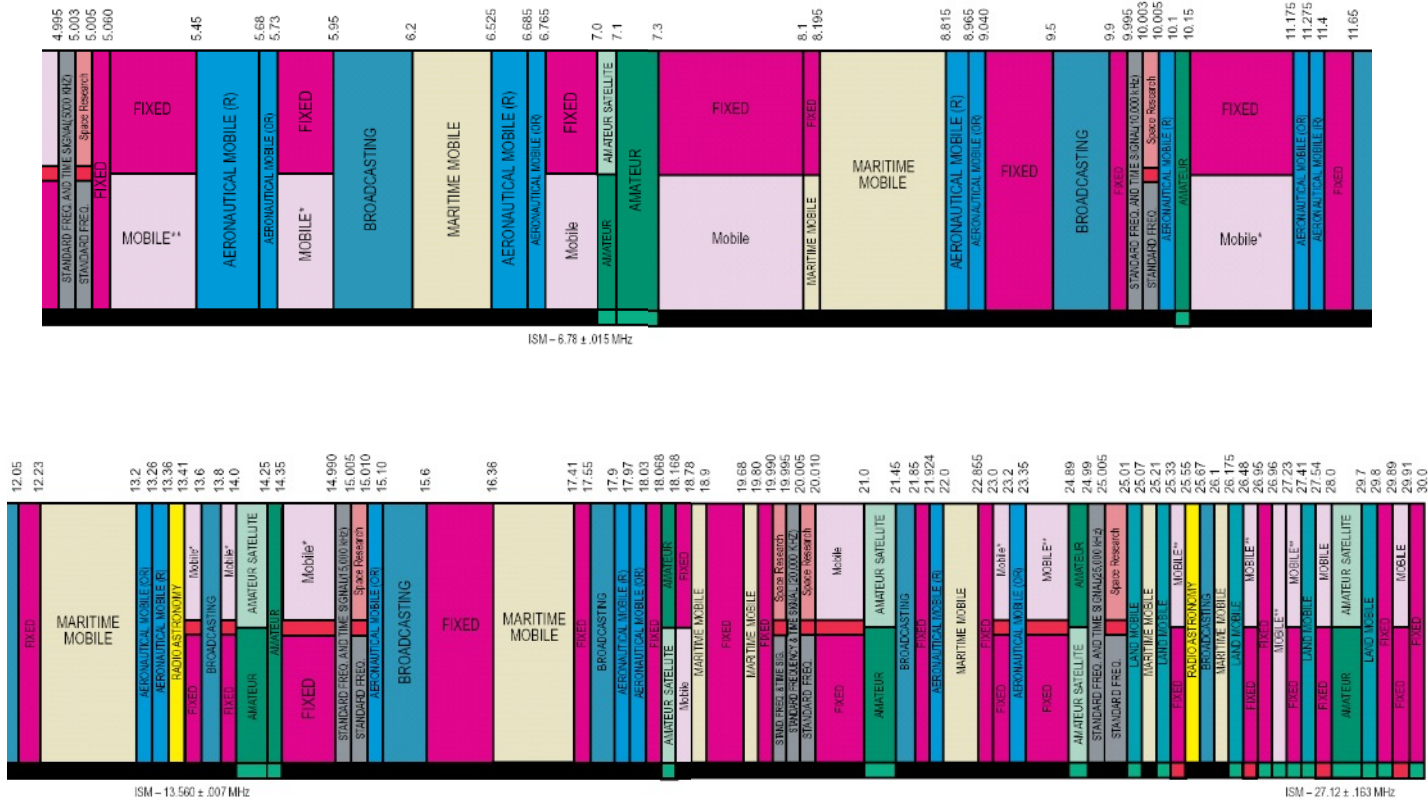


Cable network ingress

- **Upstream ingress** includes shortwave broadcast signals; aeronautical, maritime, government and military communications; amateur radio; CB; and all sorts of impulse and burst noise (vehicle ignitions, neon signs, static from lightning, power line switching transients, power line gap noise, electric motors, electronic switches, household appliances, switch mode power supplies, grow lights/ballasts, Part 15 devices).
- Upstream ingress can be in-channel, but ingress at other frequencies – especially below about 15 MHz to 20 MHz – can cause upstream laser clipping. One often overlooked interference source that can cause laser clipping is AM broadcast radio ingress below 5 MHz (530 kHz to 1700 kHz). Laser clipping affects ALL upstream frequencies.



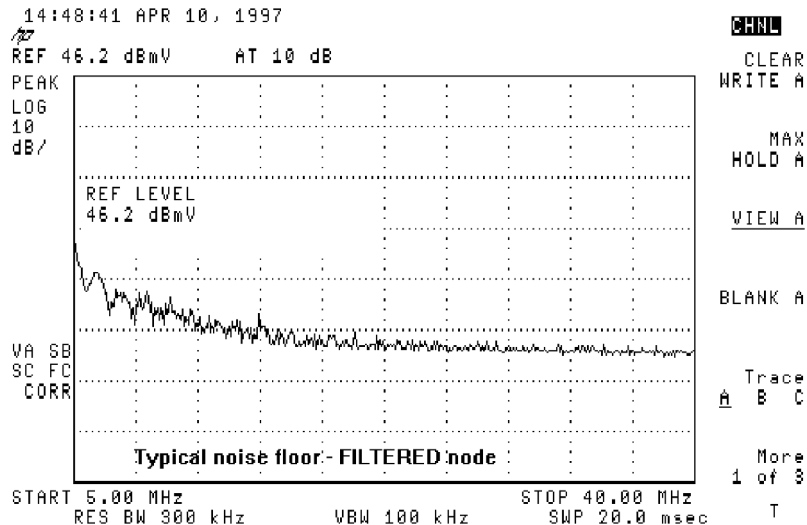
Over-the-air spectrum, 5 MHz to 30 MHz



Source: NTIA (<http://www.ntia.doc.gov/osmhome/allochrt.pdf>)

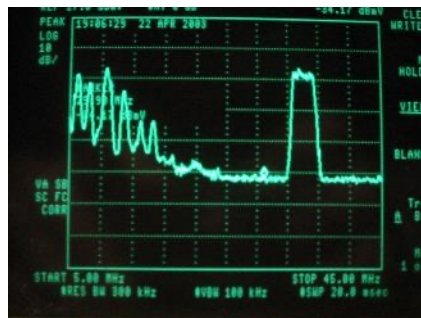
Upstream ingress

Anecdotally, the cable industry has found that on average, as much as 95% of upstream ingress comes from the subscriber drop: 25% in the portion between the tap and side of the house, the remaining 70% or so from inside the home. (The actual percentages vary somewhat from system to system).

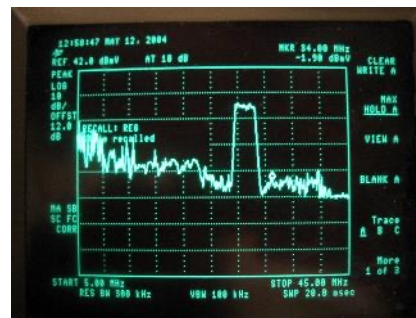


What about cable system upstreams?

Fairly typical example



Marginal-to-poor



In need of
immediate
attention



Where ingress gets in*

- Poorly shielded customer premises equipment connected directly to the subscriber drop
- Inadequately shielded cable and equipment (can be a problem near high-power transmitters)
- Loose, damaged or improperly installed connectors, adapters, and splices
- Damaged cable shielding: abrasion, burns, bullet (and pellet) holes, corrosion, cracks, cuts, rodent chews, staple through drop cable
- Damaged RF gaskets on passive and active device housings and faceplates
- Loose passive device faceplates
- Loose or warped amplifier housing lids
- Retail-grade cables, connectors, passives (typically purchased and installed by subscriber)
- Theft of service

*Note: All of these are also sources of signal leakage.

Examples of ingress sources



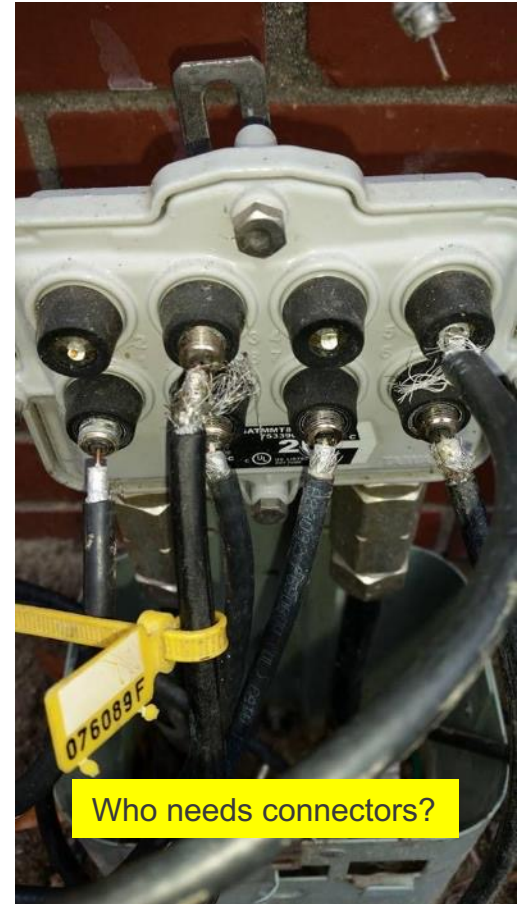
Rodent damage



Cracked shield

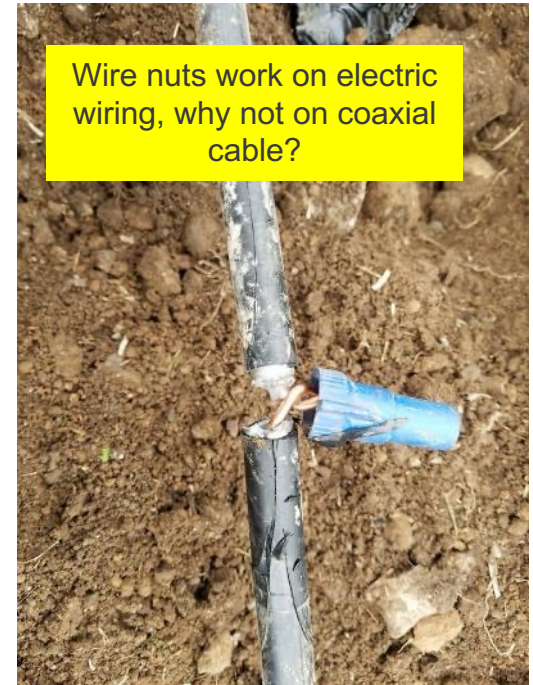
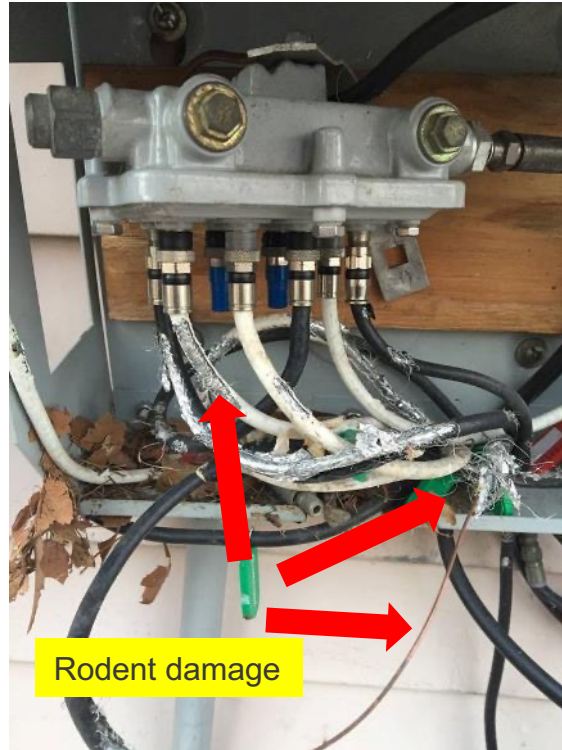


Cracked shield

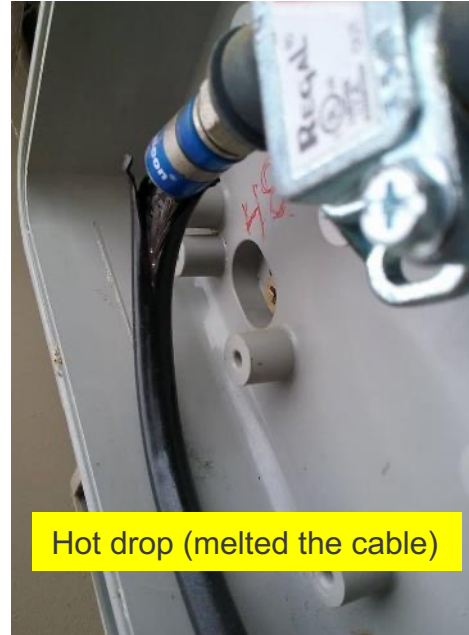
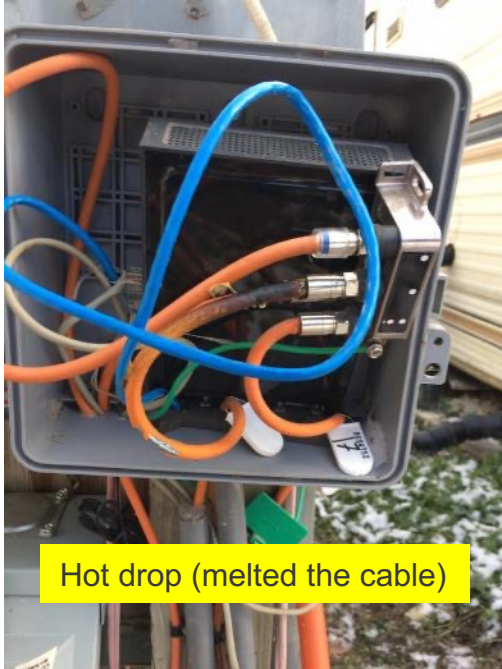


Who needs connectors?

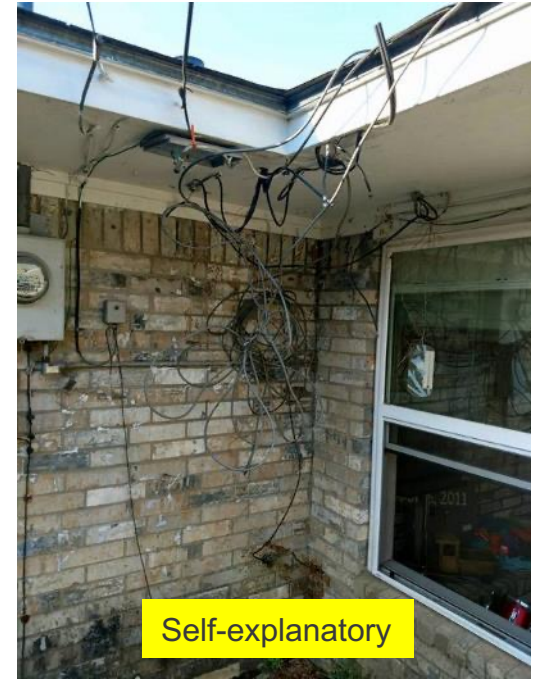
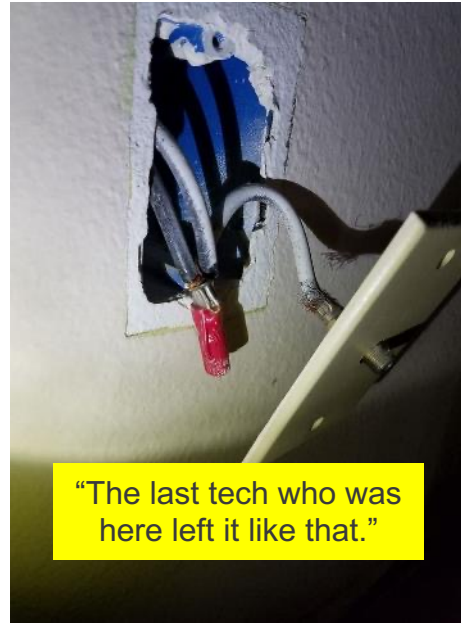
Examples of ingress sources



Examples of ingress sources



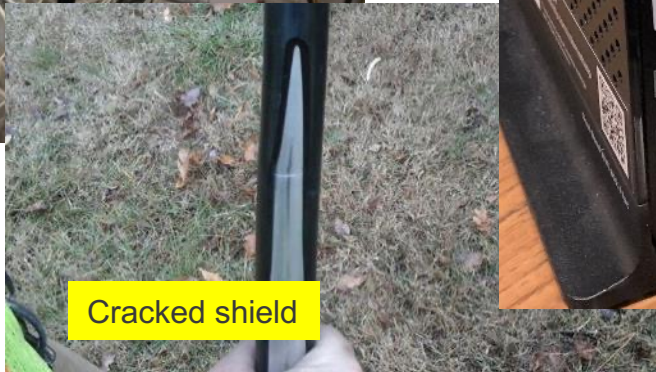
Examples of ingress sources



Examples of ingress sources



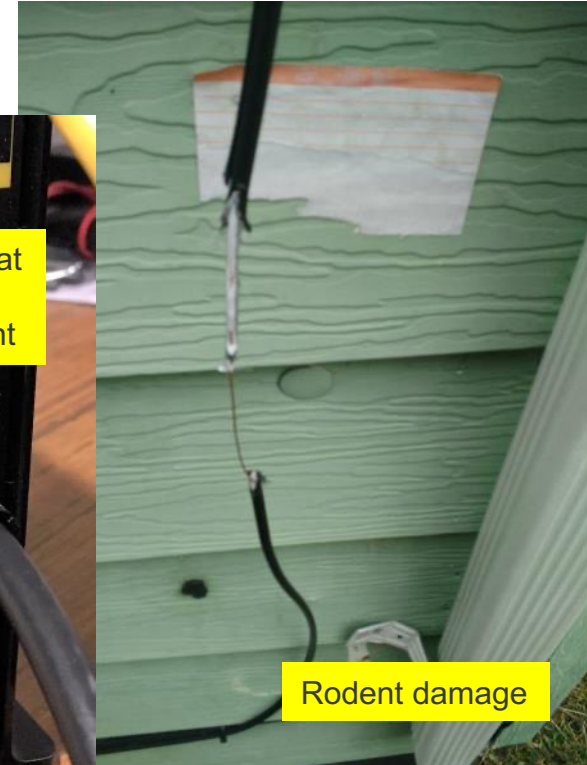
Self-explanatory



Cracked shield

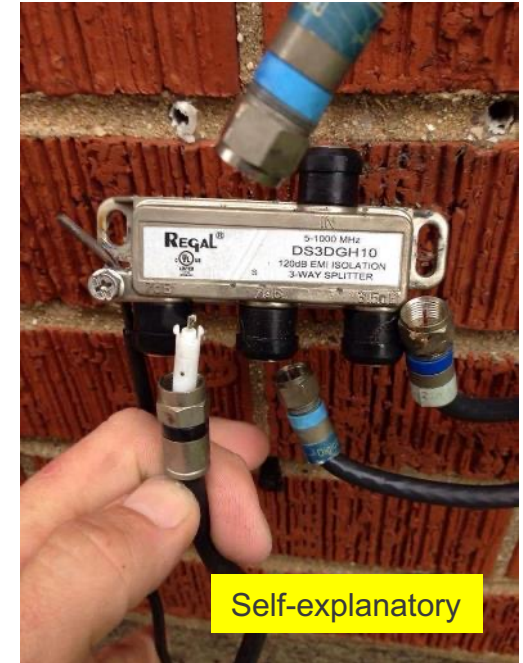
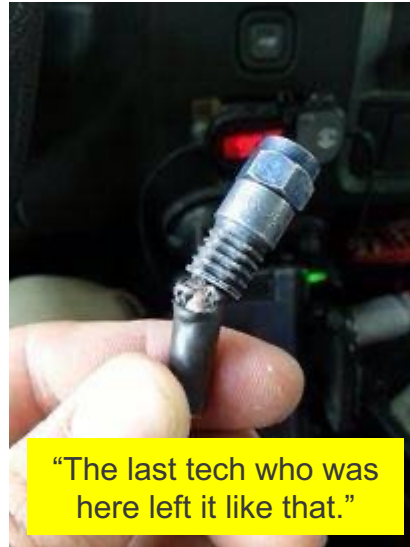


Loose F connector at input to customer premises equipment

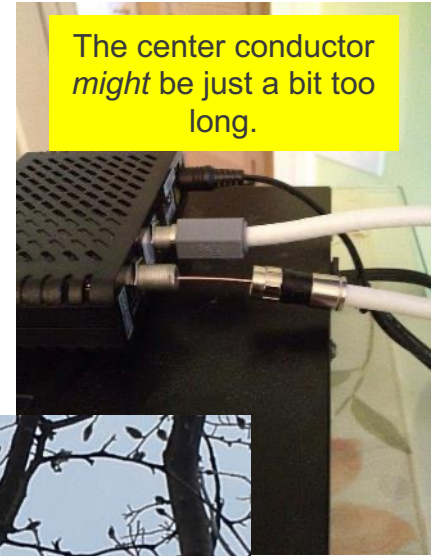


Rodent damage

Examples of ingress sources



Examples of ingress sources

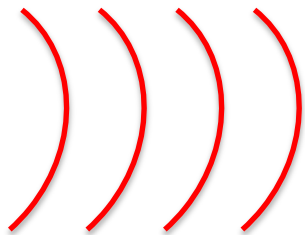


Examples of ingress sources

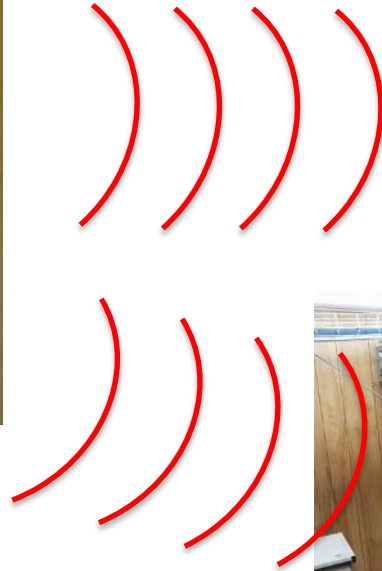


Direct pickup interference

- **What:** Over-the-air signals “leak” directly into an affected device, sometimes without any physical connection to that device
- **How:** Shielding of the affected device is inadequate; signal coupled to internal circuits via ventilation slots, case seams, common-mode current on cables
- **Why is this important?** Direct pickup can interfere with the performance of the device and/or the cable service!



Direct pickup interference to CPE, headend equipment and test equipment



Older CPE usually more susceptible; newer CPE has better shielding. Poorly shielded retail-grade cables, splitters, etc., can offset the benefits of good CPE shielding.



Some headend and test equipment is susceptible to direct pickup interference because of inadequate shielding

Join us next time for Part 2

**Signal leakage,
ingress, and
direct pickup
(Part 2):
Managing Ingress**

