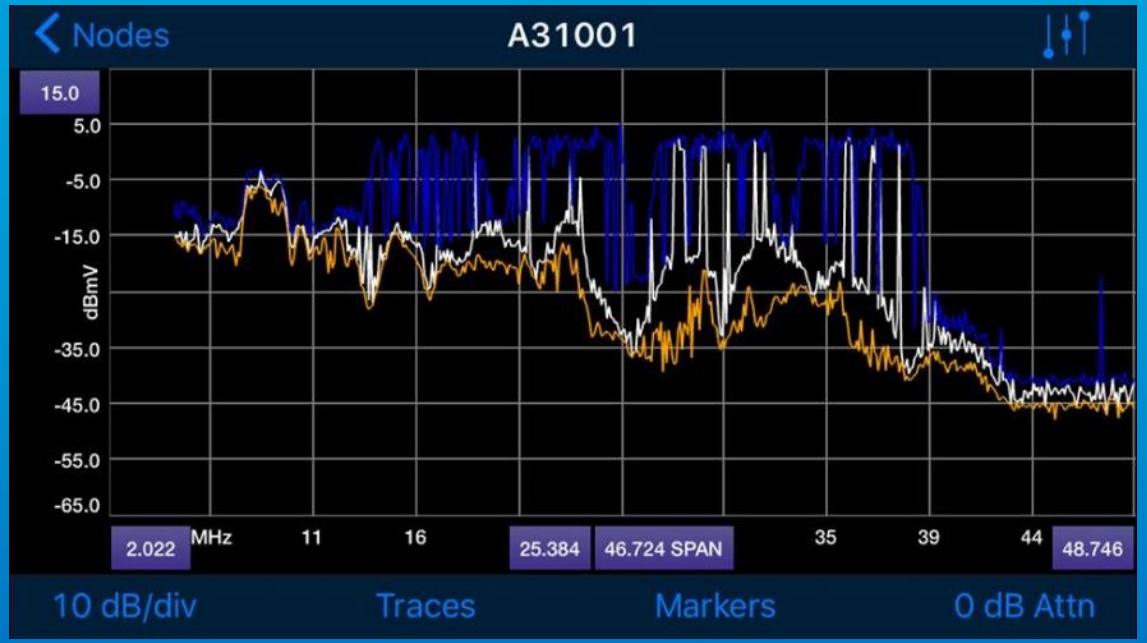
Signal leakage, ingress, and direct pickup (Part 1):

A Closer Look

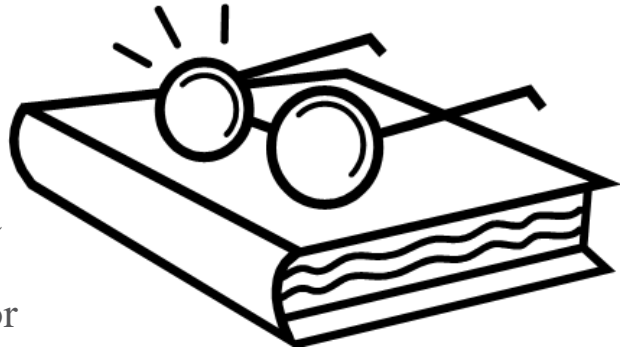
Ron Hranac



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.



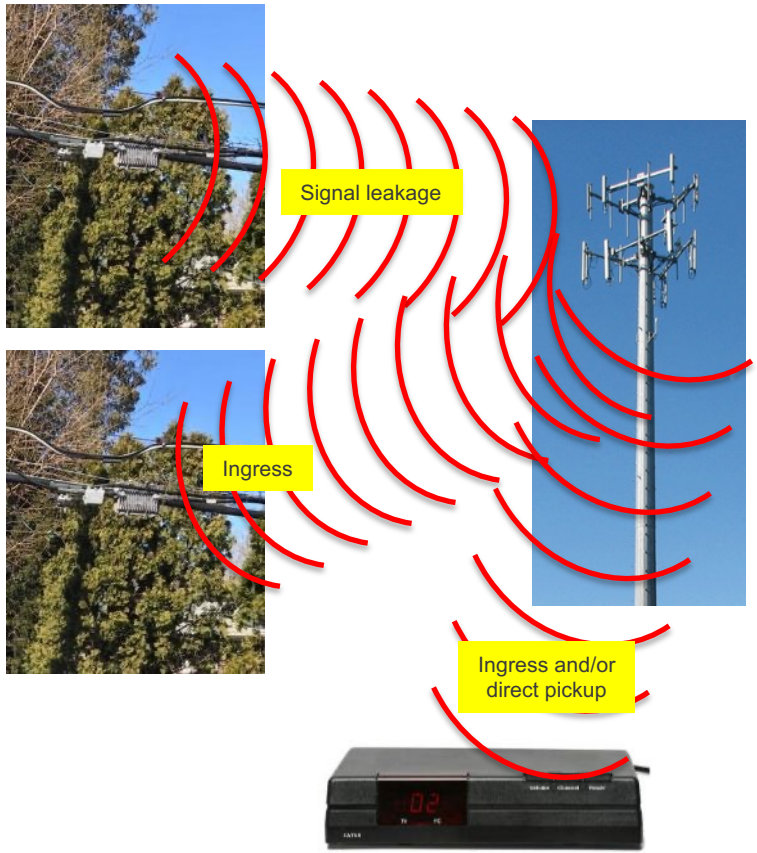
1. Note: Direct pickup is similar to ingress, except that the over-the-air signal(s) enters a susceptible set-top, cable modem, TV set, test instrument, or other device directly, often without any cables or other external devices physically connected. If the susceptible device's outer case or cover is 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.

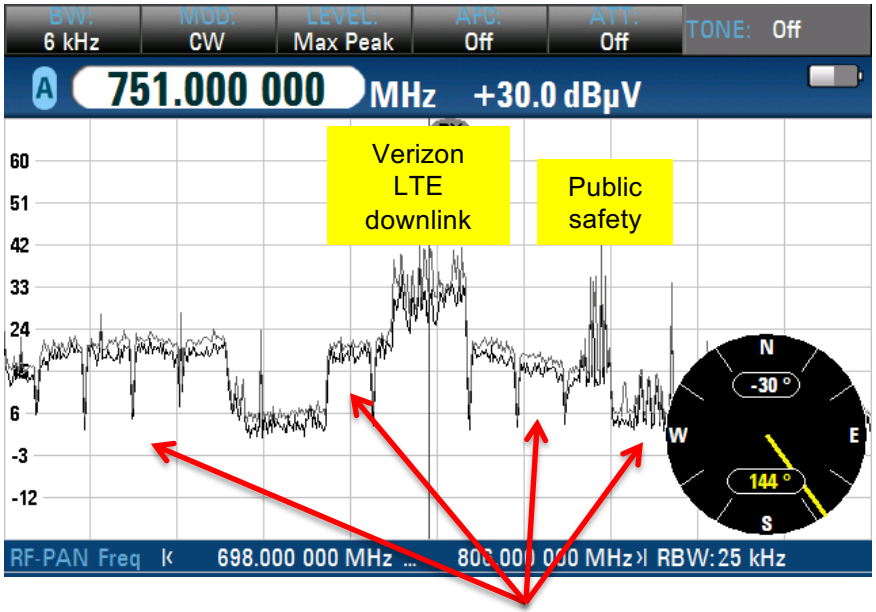
What causes ingress and leakage?

- 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

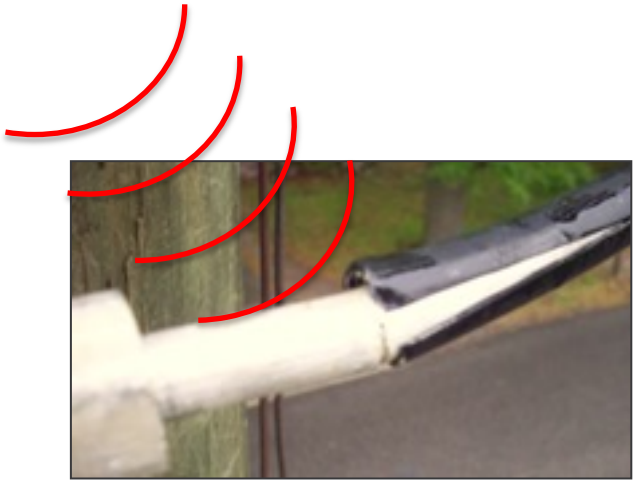
- **What:** Signals inside of the cables leak out, causing interference to over-the-air services such as long term evolution (LTE)
- **How:** Shielding effectiveness of the cables and components degraded for some reason
- **Why is this important?** Harmful interference can occur to over-the-air users,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



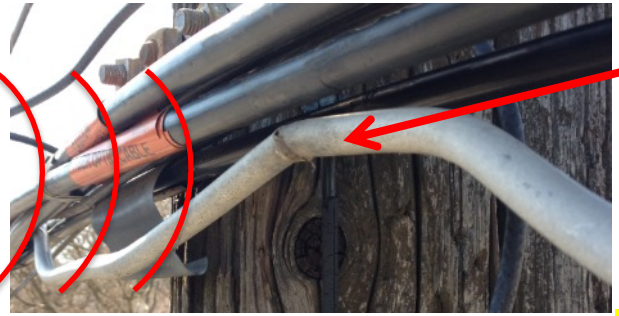
Leaking SC-QAM and other signals present in over-the-air spectrum

Ingress interference

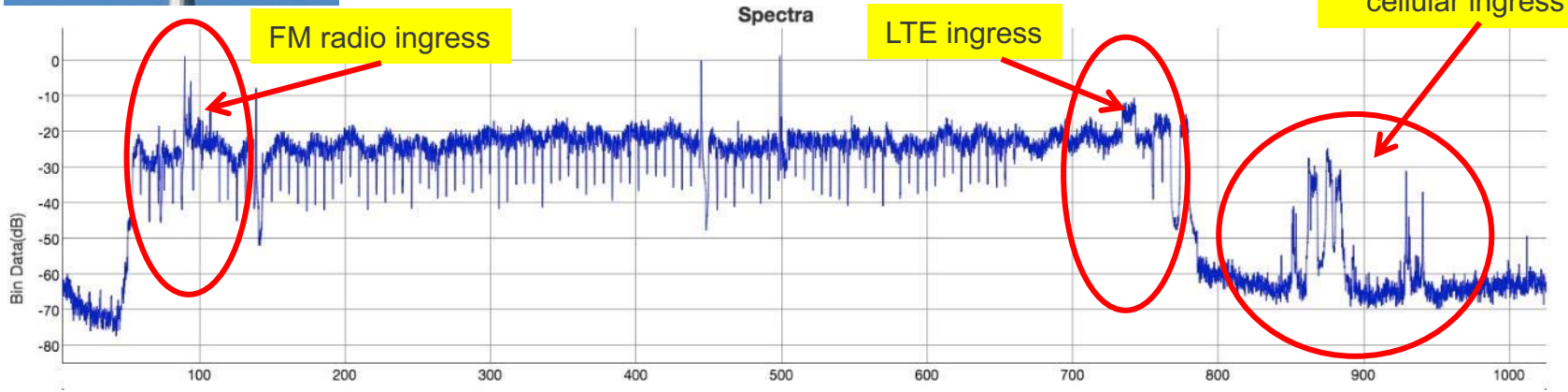
- **What:** Over-the-air signals leak into the cable network
- **How:** Shielding effectiveness of the cables and components degraded for some reason
- **Why is this important?** Interference can occur to cable network's signals and services



Ingress interference in the outside plant



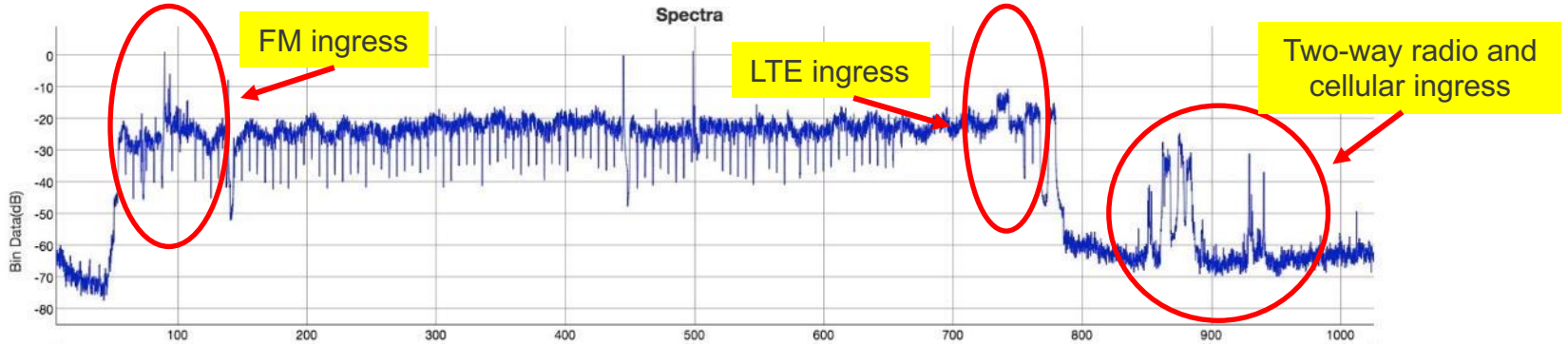
Ingress enters through crack in cable (or some other shielding defect)



Full band capture graphic courtesy of Comcast

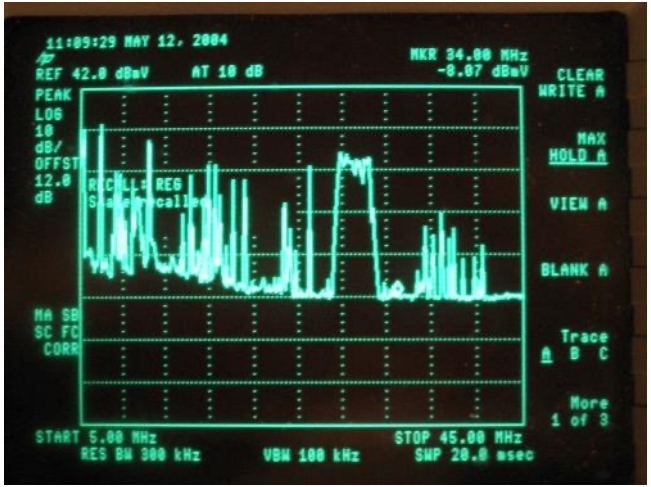
Cable network ingress

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).

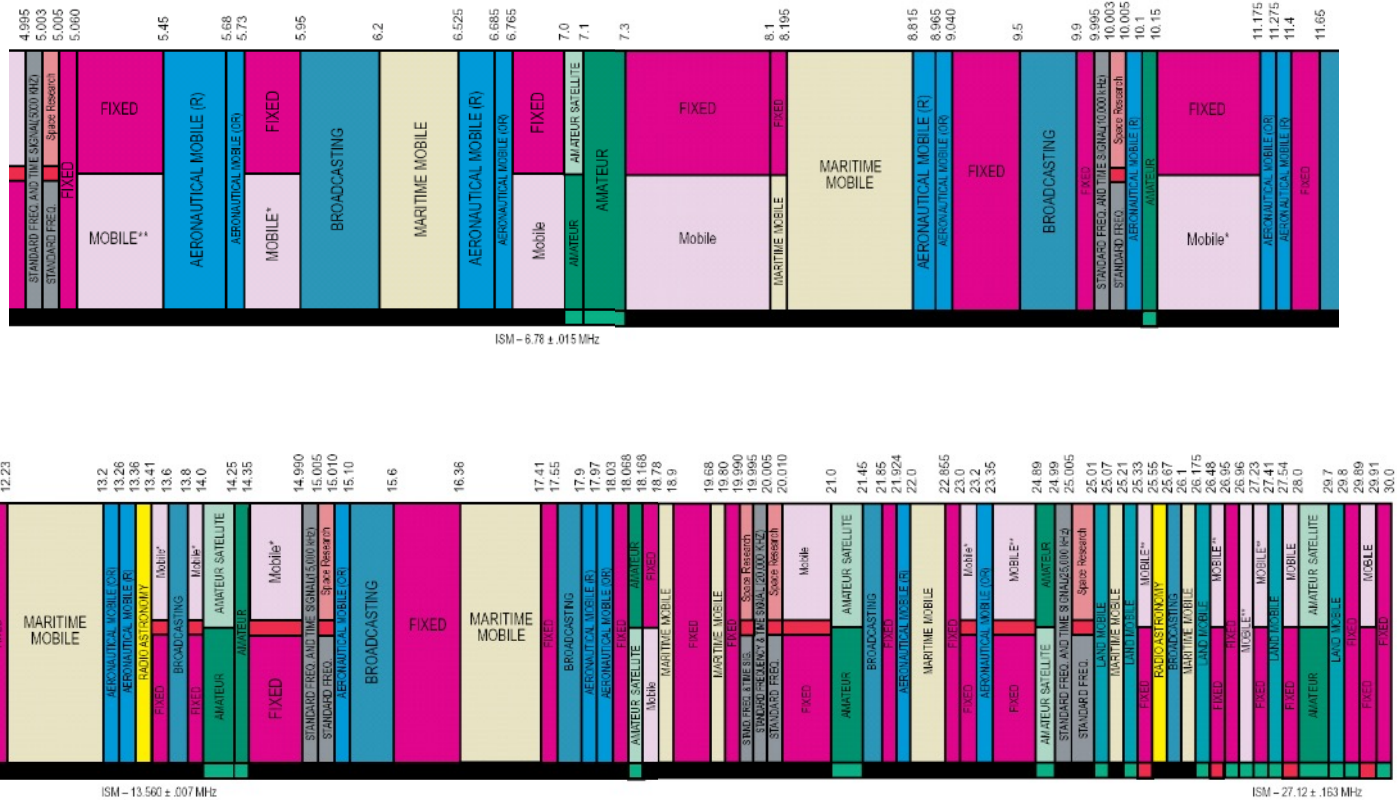


Cable network ingress

- 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.



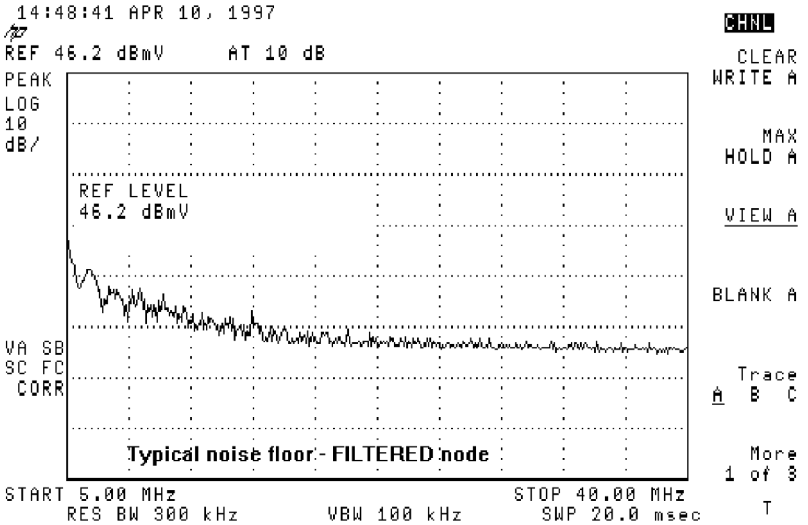
Over-the-air spectrum, 5 MHz to 30 MHz



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

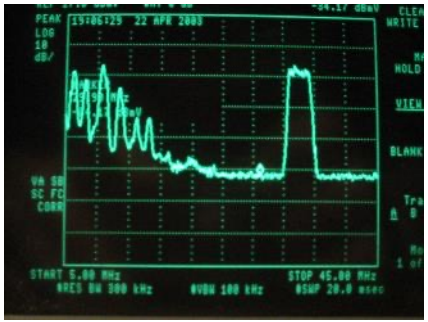
Upstream ingress

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).



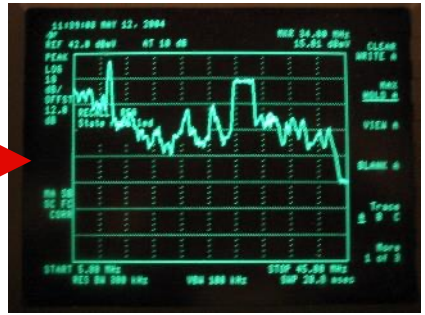
What about cable system upstreams?

Fairly typical example



Marginal-to-poor

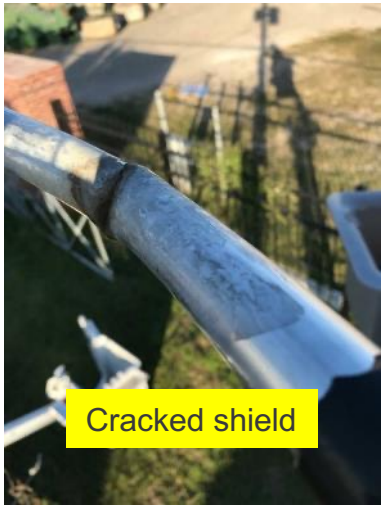
In need of immediate attention



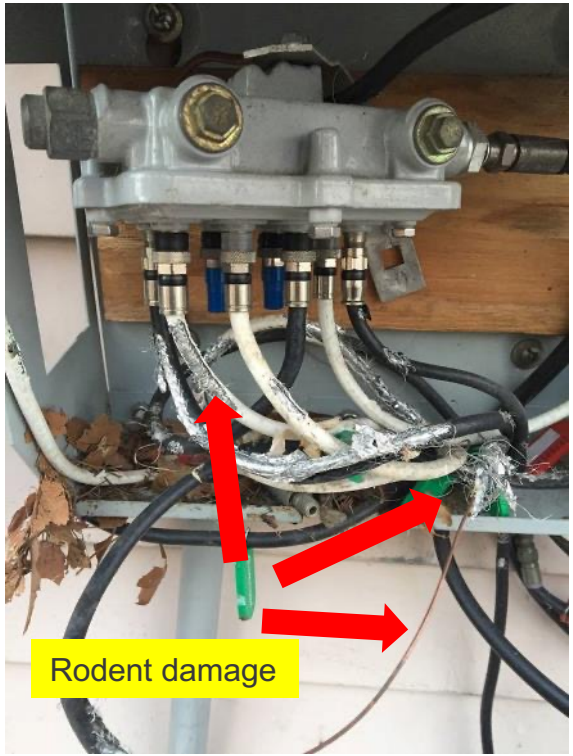
Where ingress gets in and leakage gets out

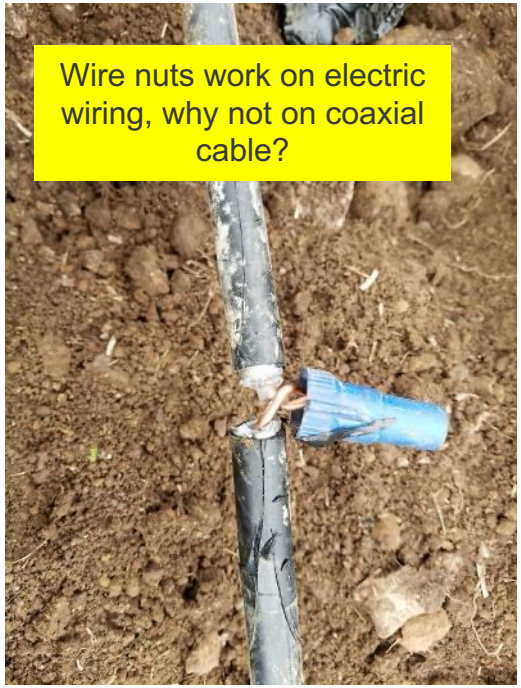
- Poorly shielded customer premises equipment connected directly to the subscriber drop
- Inadequately shielded cable and equipment (can be a problem near high-power transmitters)
- Loose, damaged or improperly installed connectors, adapters, and splices
- Damaged cable shielding: abrasion, burns, bullet (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

Examples of shielding defects

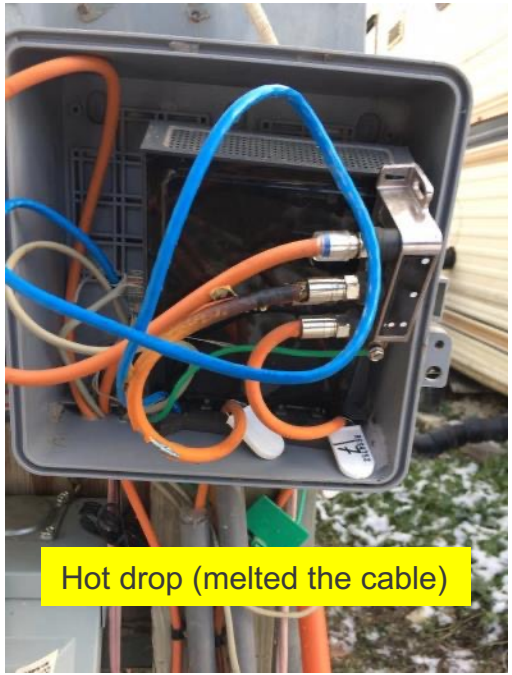


Examples of shielding defects

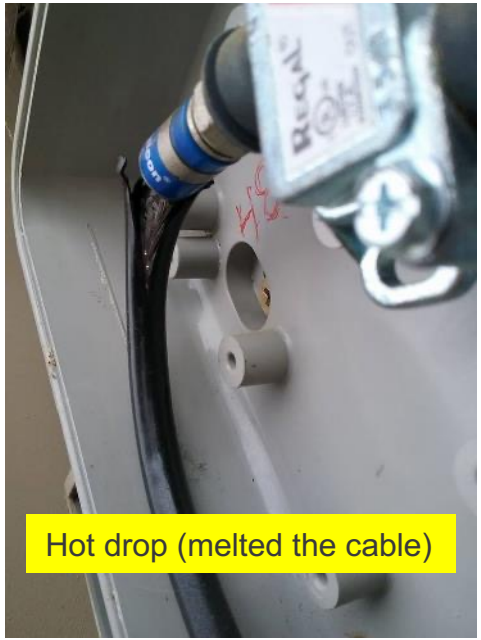




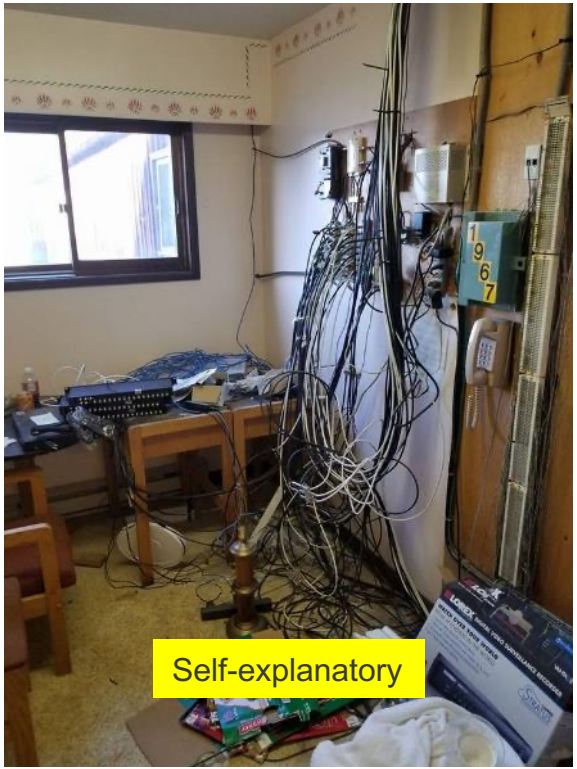
Examples of shielding defects



Hot drop (melted the cable)

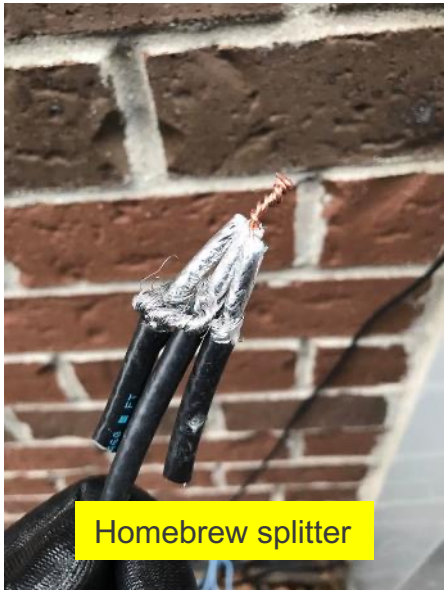


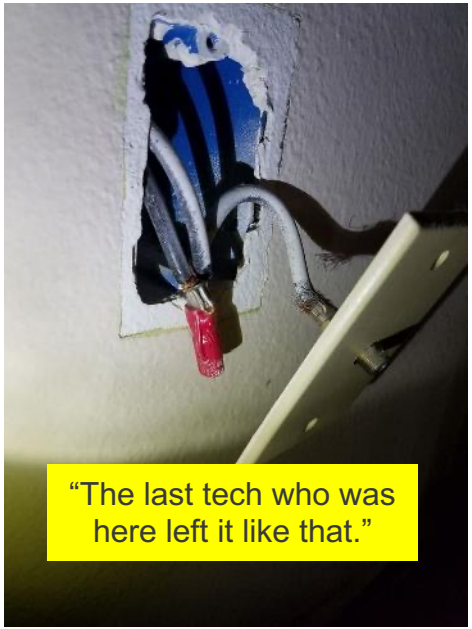
Hot drop (melted the cable)

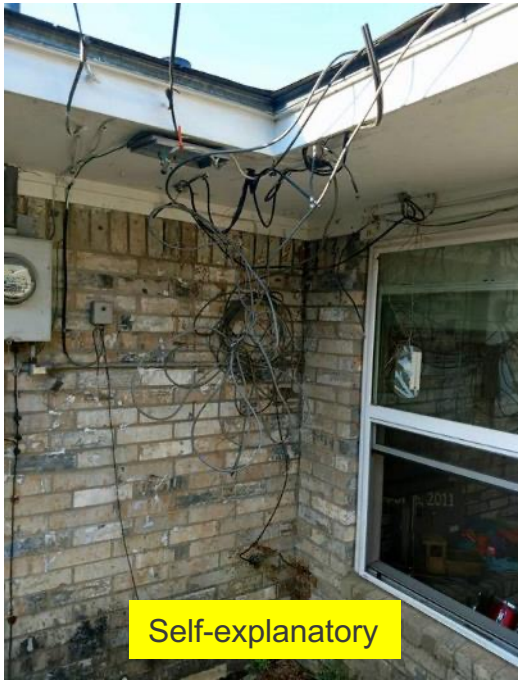


Self-explanatory

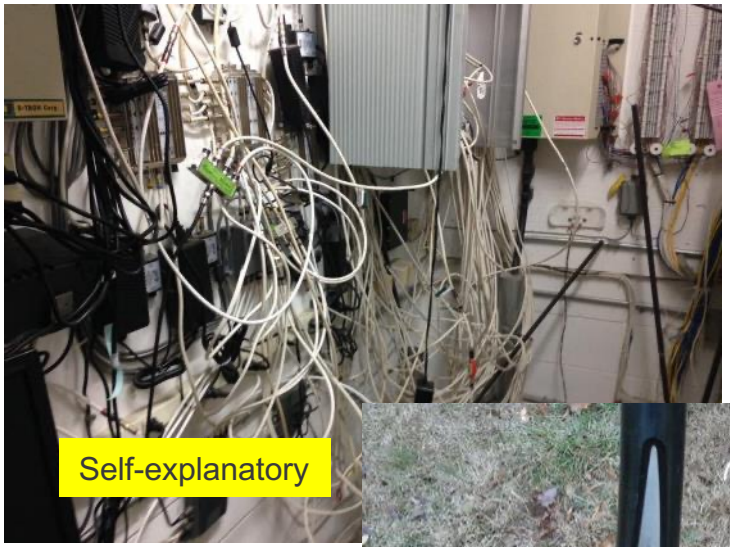
Examples of shielding defects



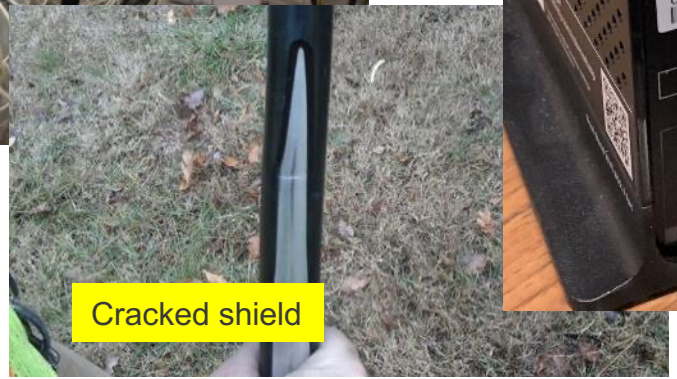




Examples of shielding defects

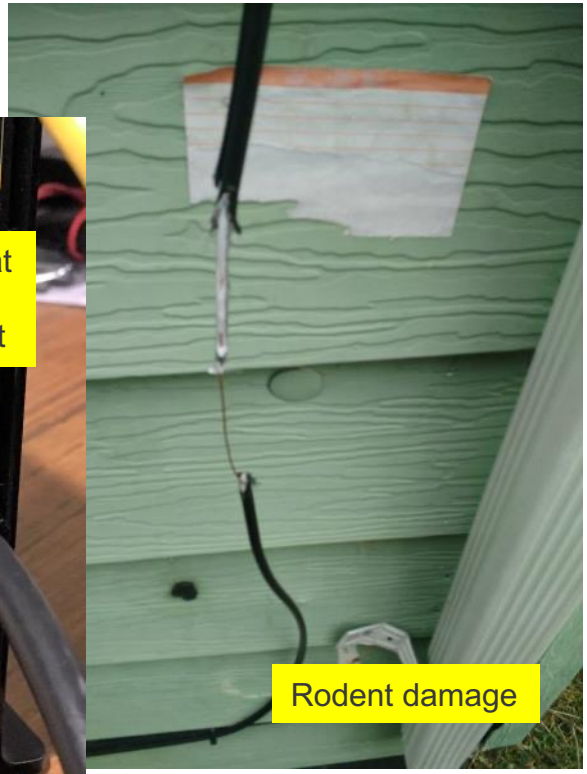


Self-explanatory



Cracked shield

Loose F connector at input to customer premises equipment



Rodent damage

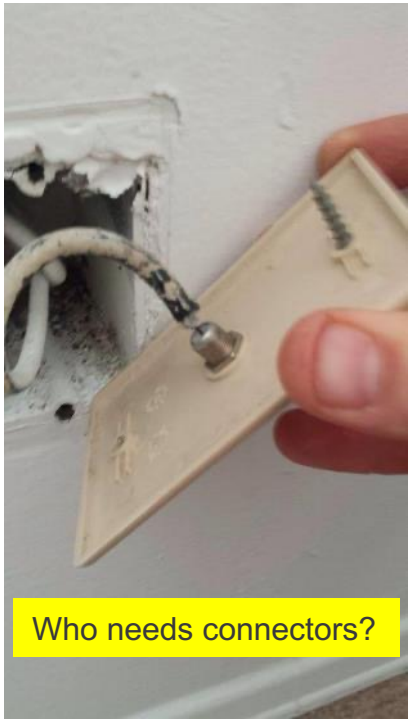
Examples of shielding defects

Warped amplifier housing? No problem, some aluminum foil will fix that!

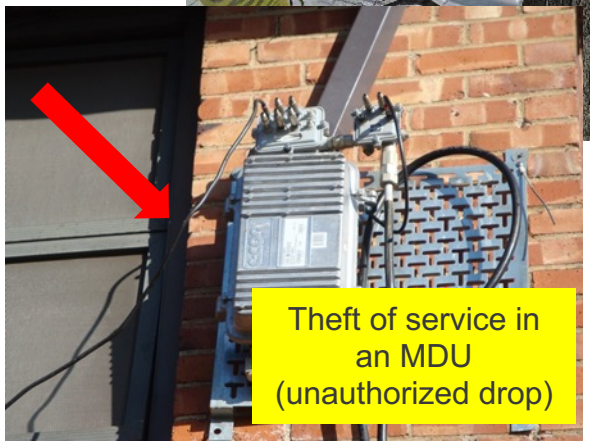
"The last tech who was here left it like that."

Self-explanatory

Examples of shielding defects



Examples of shielding defects



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

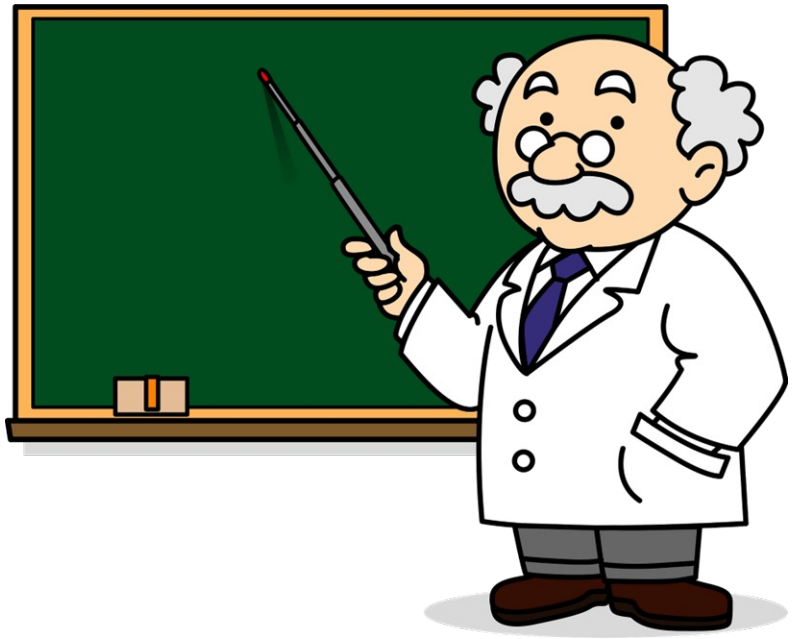
Older CPE usually more susceptible; newer CPE has better shielding. Poorly shielded retail-grade cables, splitters, etc., can offset the benefits of good CPE shielding.

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):

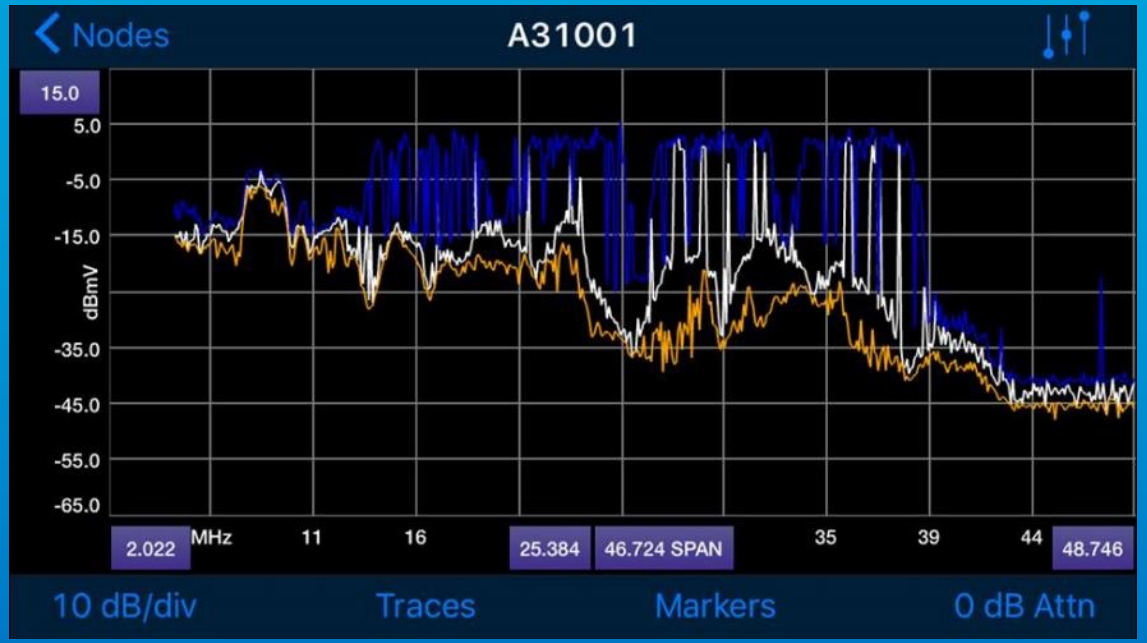
Managing Ingress



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

Managing Ingress

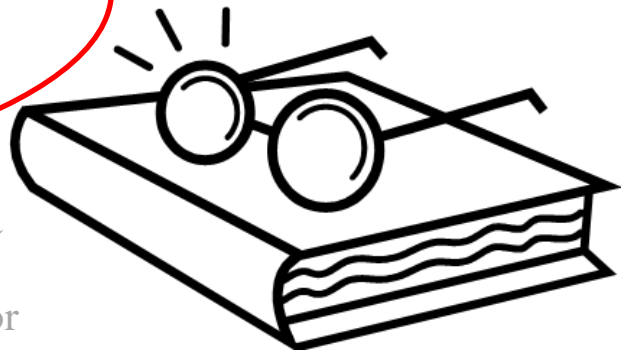
Ron Hranac



Recap from Part 1: 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.

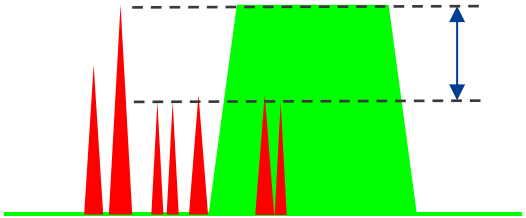
Recap from Part 1: Where ingress gets in (and leakage gets out)

- 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

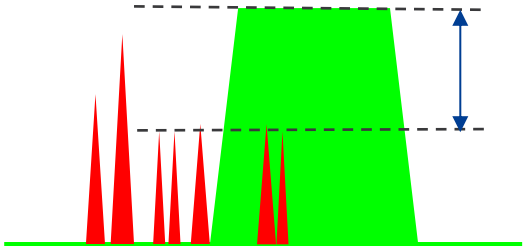
Managing ingress: A look at current techniques

Upstream RF signal levels

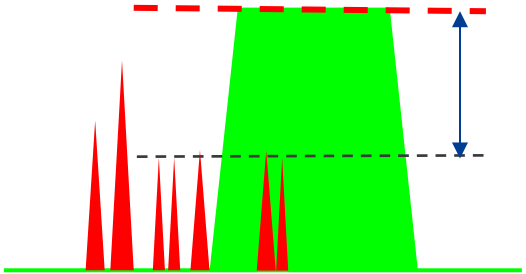
- It is not possible to make the upstream spectrum *completely* impervious to ingress interference by simply increasing modem transmit power to improve the “signal-to-junk” ratio. That said, higher modem transmit power can help *somewhat*.



Poor signal-to-interference ratio



Improved signal-to-interference ratio

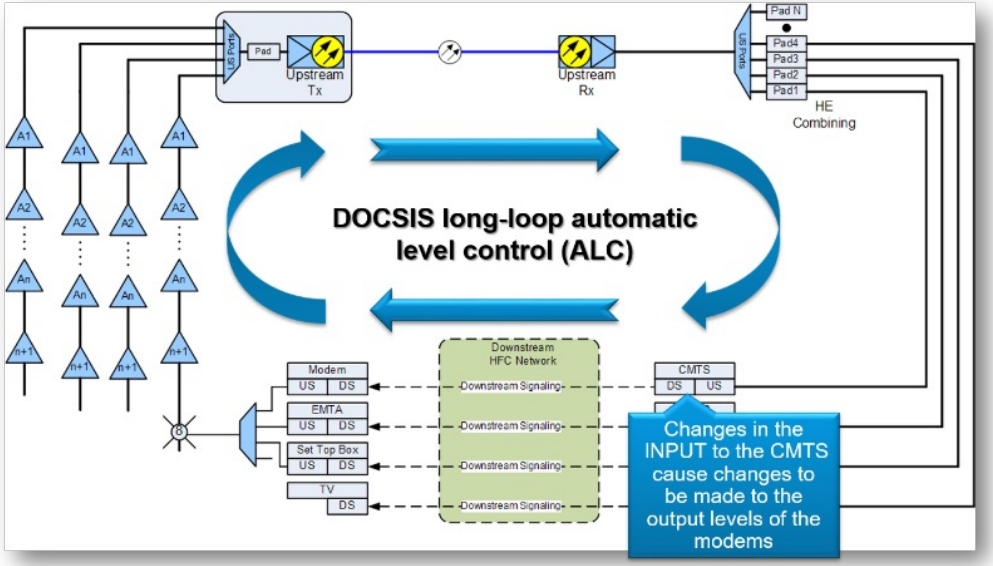


Cable modem reaches maximum transmit level, or high level clips laser

Managing ingress: A look at current techniques

Upstream RF signal levels

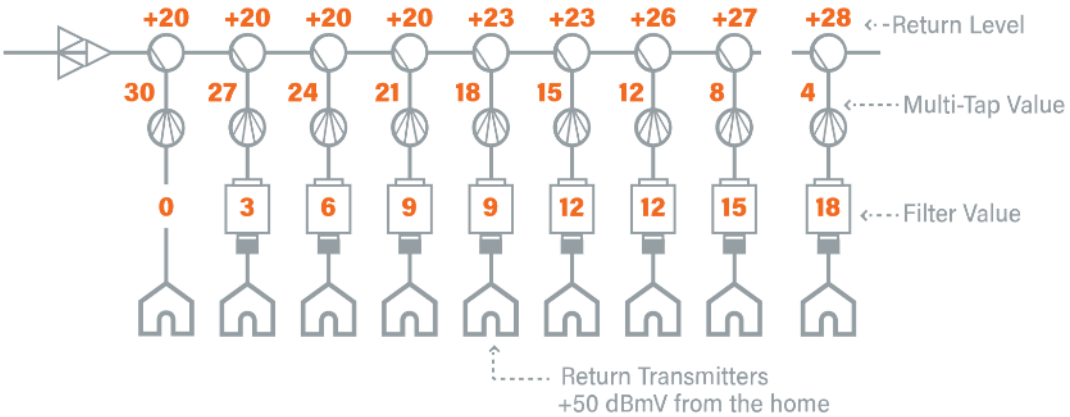
- Long-loop ALC functionality between the CMTS and modems helps to manage modem upstream transmit levels, although long-loop ALC doesn't really do anything about the ingress itself.



Managing ingress: A look at current techniques

Upstream RF signal levels

- To improve the upstream “signal-to-junk” ratio, return path equalizers or attenuators (also called return step attenuators) are installed in drops by some operators. These devices add insertion loss to the return path in the subscriber drop – but negligible insertion loss in the downstream – which forces modems in the homes to transmit at higher levels.

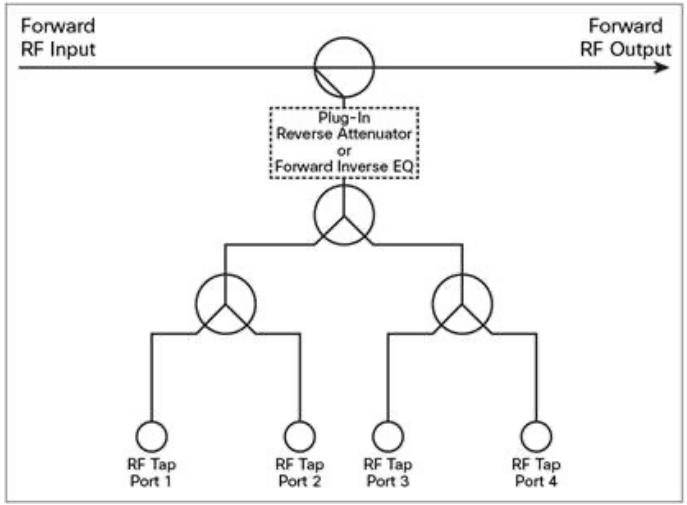


Graphic courtesy of Arcom Digital

Managing ingress: A look at current techniques

Upstream RF signal levels

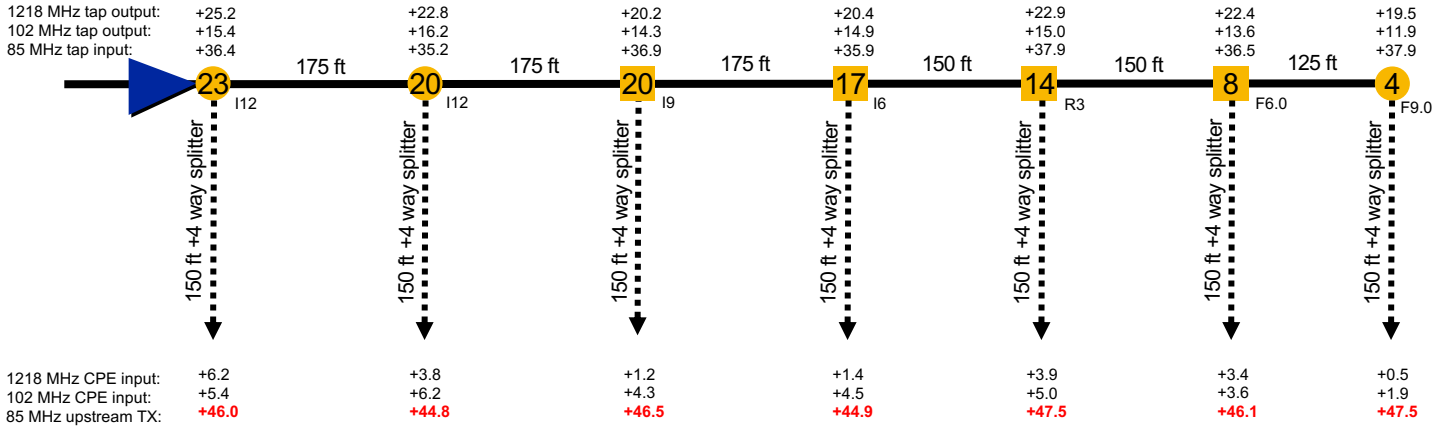
- Taps with plug-in conditioning pads or equalizers take the concept in the previous slide a step further by incorporating it in the tap, allowing the modem transmit window to be narrowed and upstream levels increased.



Managing ingress: A look at current techniques

Sample 1.2 GHz feeder design

Downstream output
102 MHz: +39 dBmV
1218 MHz: +60 dBmV
Upstream input
85 MHz: +13 dBmV

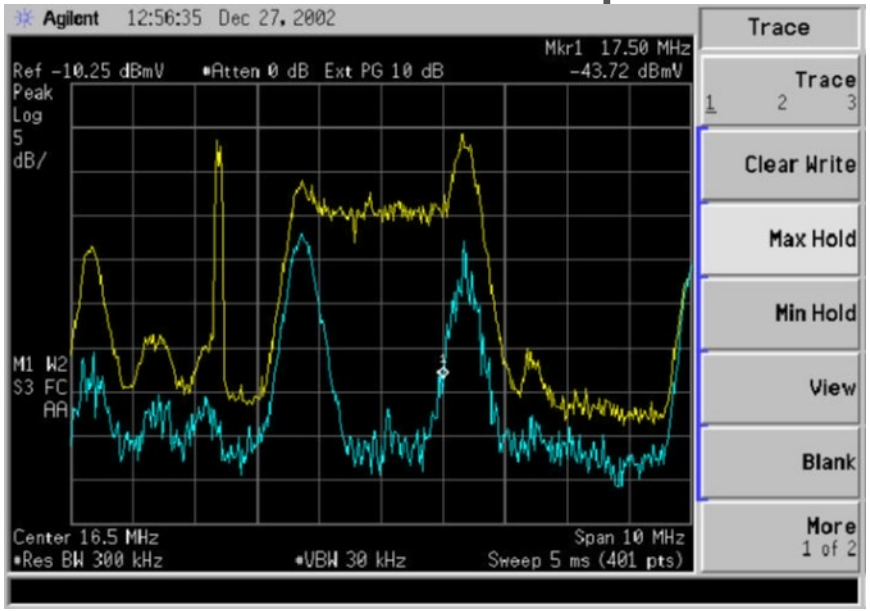


Note: Design uses taps with plug-in reverse attenuator (e.g., “R3”), forward equalizer (e.g.,” F6.0”), or forward inverse equalizer (e.g., “I12”) as needed.

Managing ingress: A look at current techniques

Ingress cancellation

- One important tool is ingress cancellation in the CMTS (or RPD) upstream burst receiver. This does a decent job of managing in-channel ingress, at least as it impacts in-channel performance. It won't do anything about out-of-channel ingress, nor will it prevent upstream laser clipping.
  - *Ingress cancellation was introduced as part of DOCSIS 2.0's advanced PHY umbrella of technologies to improve upstream data transmission robustness, and is still used today. Make sure the CMTS is configured to have this feature turned on. Note: Ingress cancellation is not defined in DOCSIS, but is supported.*



This screen shot is from a 2002 demonstration of ingress cancellation's effectiveness. A 3.2 MHz-wide 16-QAM cable modem signal was centered at 16.5 MHz in an operating cable network with ingress present. There was no perceived degradation in cable modem performance.

Managing ingress: A look at current techniques

CMTS configuration

Some examples include:

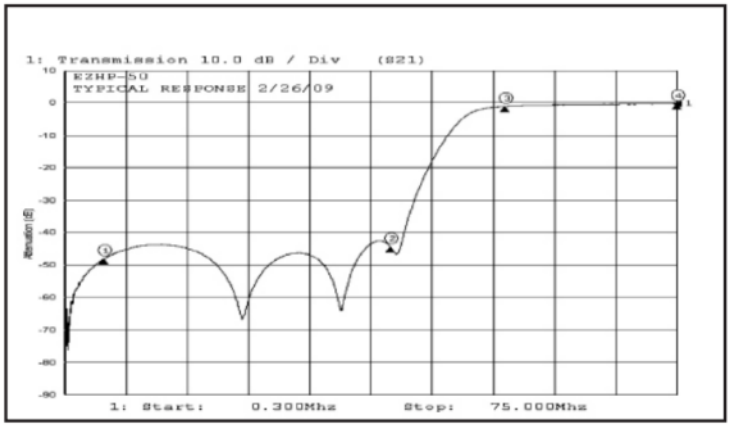
- Upstream RF levels (“signal-to-junk”)
  - CMTS commanded nominal receive power
  - CMTS power-adjust-continue
- Forward error correction
- Dynamic modulation
- Load balance
- Modulation profiles

```
Int c5/0/0
cable upstream 0 frequency 24000000
cable upstream 0 docsis-mode atdma
cable upstream 0 channel-width 6400000 6400000
cable upstream 0 threshold snr-profiles 24 19
cable upstream 0 threshold corr-fec 0
cable upstream 0 threshold uncorr-fec 1
cable upstream 0 modulation-profile 224 223 222
cable upstream 0 threshold hysteresis 4
cable upstream 0 equalization-coefficient
```

Managing ingress: A look at current techniques

Other tools

- Many cable operators installed high-pass filters (aka “noise filters”) – small filters that block the return spectrum while passing the downstream spectrum – in the subscriber drops of one-way customers, and either removed those filters for two-way service or used what are called windowed high-pass filters. While a few operators still use high-pass filters, most no longer do.



Graphics courtesy of Eagle Comtronics

Managing ingress: A look at current techniques

Other tools

- A couple companies have introduced dynamic return path switches over the past several years. The switches remain open when upstream data is not being transmitted. When the devices detect upstream signals, the switches close allowing the return signals to pass through the network. When the switches are open, they block all return signals, including noise and ingress.
- Proxilliant is an example of a manufacturer of this technology (theirs is called *Dynamic Ingress Blocker*). A downside is that this technology was not compatible with S-CDMA (and is said to be incompatible with OFDMA). Proper operation of the switches sometimes required the cable operator to increase the length of the upstream data preamble on A-TDMA signals. Because the switches respond to RF power, especially strong ingress can cause the switches to close.

Managing ingress: A look at current techniques

Other tools

- Technetix sells a series of mainline passives (splitters, directional couplers) that have a 180 degree phase shift between the two output ports. They call this line “Ingress Safe.” The idea is that the same ingress signal that comes from two different feeder legs but in the same neighborhood will have the same (more or less) phase and amplitude, and by shifting the phase of one splitter leg relative to the other, the same ingress signal coming from two directions will combine out-of-phase in the splitter, theoretically canceling the ingress. In practice, the ingressing signal will be of somewhat different amplitudes and phases on each of the legs connected to the splitter, so cancellation won’t be complete. Instead, there will be a reduction of the level of some of the ingress (Technetix claims an average of about 6 dB to 12 dB reduction).

Managing ingress: A look at current techniques

Keep the plant tight

- The root of the problem is degraded shielding, so it's critical to prevent ingress from getting in the network to begin with, and when it does, to find and fix the problem.
- In most instances, the presence of ingress means that signal leakage is also occurring. If that leakage exceeds FCC limits (or causes harmful interference), it MUST be found and fixed per FCC Rules.

Managing ingress: A look at current techniques

Keep the plant tight

- Keeping signal leakage and ingress under control is the biggie, and is what hits operations. This includes the use of quality components (cable, connectors, passives, and so on), proper installation practices (lot of room for improvement here), on-going leakage monitoring and repair, and tracking down and fixing problematic ingress when it occurs. This will never go away as long as coaxial cable is used for signal distribution.

Managing ingress: A look at current techniques

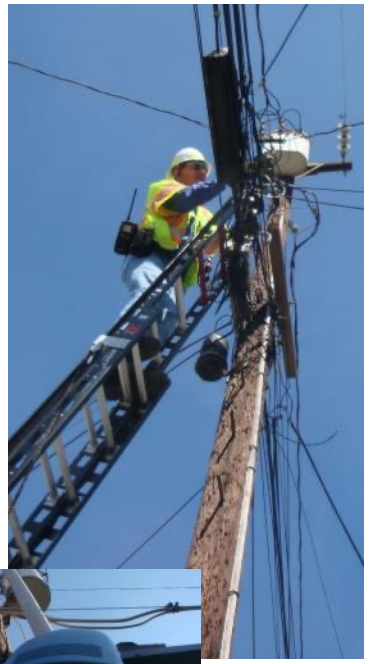
Keep the plant tight

- ✓Aggressive downstream signal leakage monitoring and repair program
  - The FCC's 20 µV/m leakage limit isn't good enough! Most cable operators have found it necessary to keep leakage below 5 to 10 µV/m to ensure reliable two-way operation. At least one cable operator has a company spec of 2 µV/m.
  - Aeronautical flyovers should target 98th or 99th percentile performance, rather than the FCC's 90th percentile.
- ✓Use high-quality drop materials; installer training (in-house and contractors); follow-up installation QC
- ✓Monitor upstream and downstream ingress, identify problem nodes, dispatch crews to repair critical problems

Managing ingress: A look at current techniques

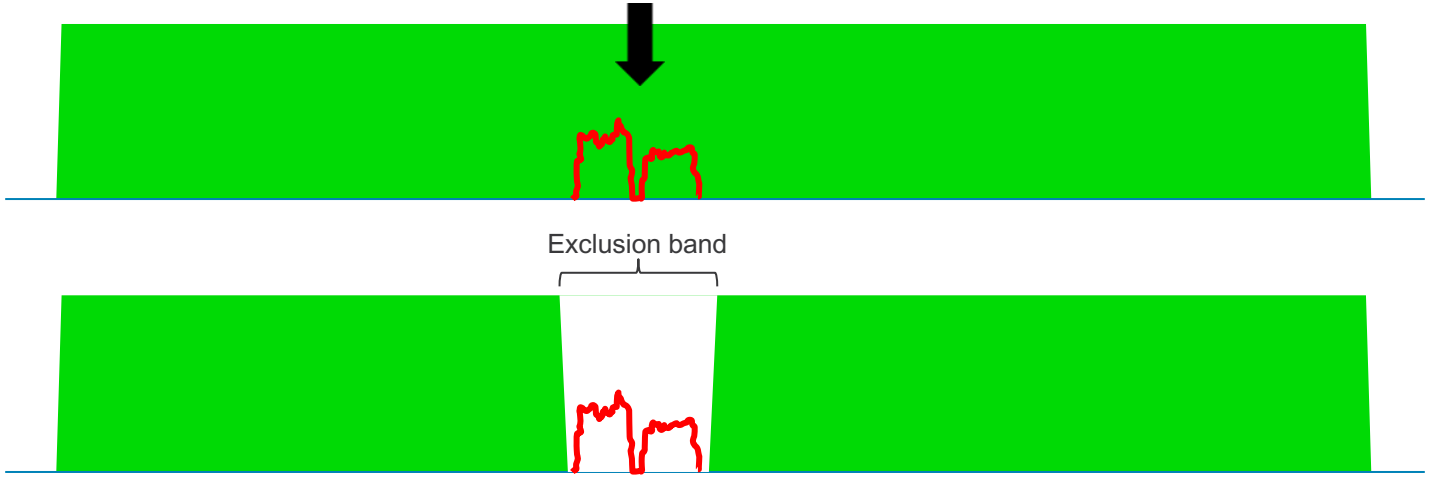
Start with leakage

- The major test equipment manufacturers – Arcom Digital, ComSonics, Effigis, and Trilithic (acquired by Viavi) – have been shipping digital-compatible multi-band signal leakage detection equipment for several years.
- Single-frequency leakage monitoring is no longer good enough: A VHF *and* UHF leakage monitoring program is essential.



Managing ingress: A look at current techniques

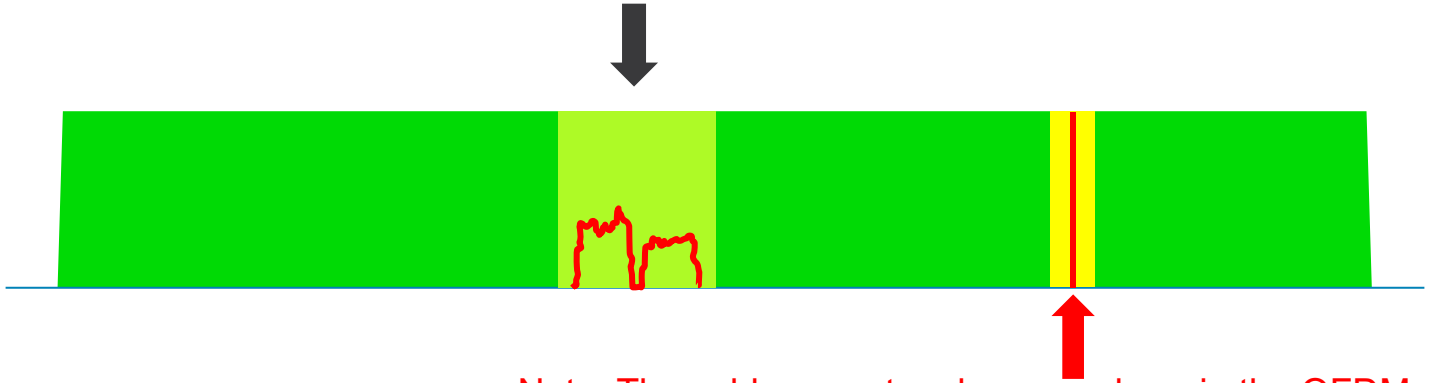
Exclusion bands can be created within a DOCSIS 3.1 OFDM signal for problems such as strong in-channel ingress (e.g., LTE interference).



An exclusion band is a set of contiguous subcarriers within the OFDM signal bandwidth that is set to zero-value by the transmitter to avoid interference or to accommodate co-existing transmissions such as legacy SC-QAM signals.

Managing ingress: A look at current techniques

As an alternative to an exclusion band in that part of an OFDM channel experiencing interference, the bit loading can be changed to allow continued carriage of data, but using a more robust lower modulation order. (Profile management is useful for optimizing the OFDM signal to plant conditions.)

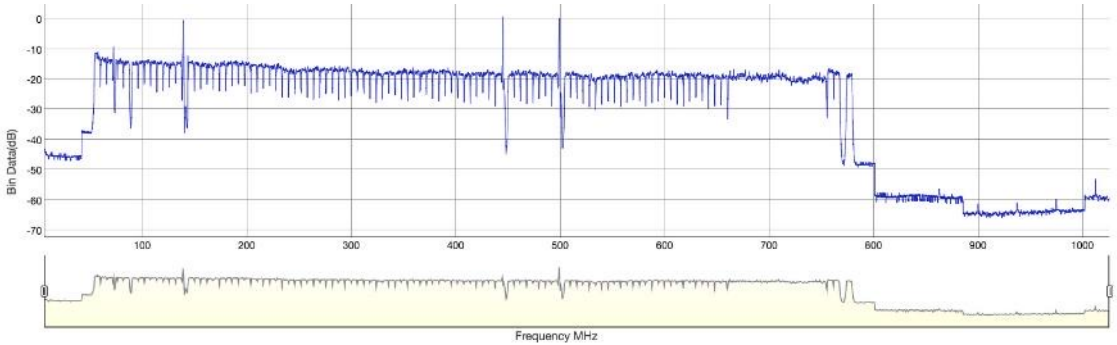


Note: The cable operator chooses where in the OFDM signal to place the PHY link channel (PLC). Ideally, the PLC should be located in a known clean part of the OFDM signal that is not susceptible to ingress, direct pickup, and other types of interference.

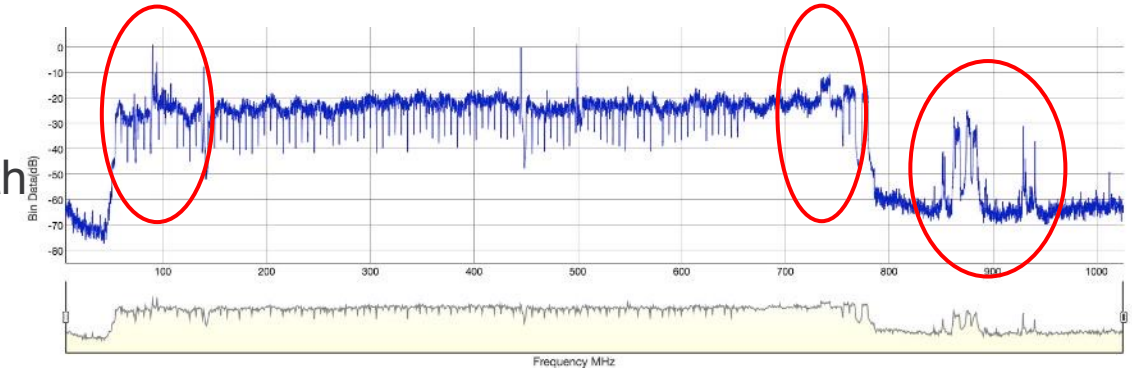
Managing ingress: A look at current techniques

- Use full band capture-capable CPE to help identify and locate ingress

Clean downstream spectrum:



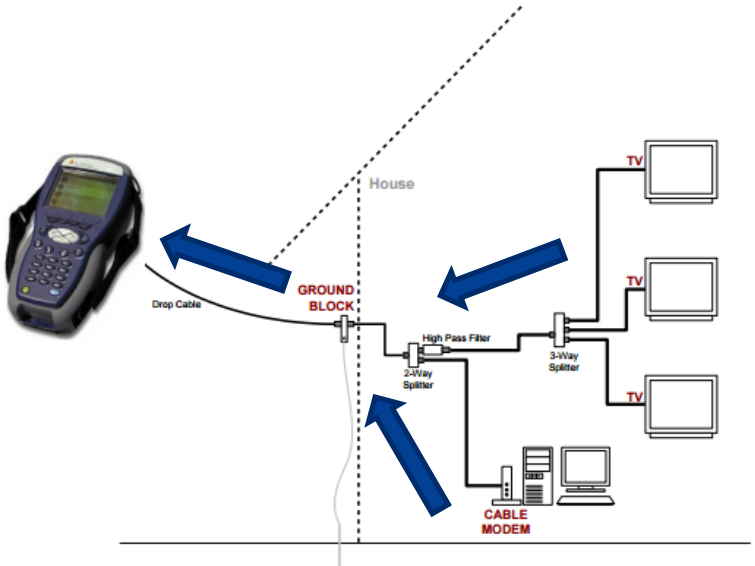
Impaired downstream spectrum with noise and ingress:



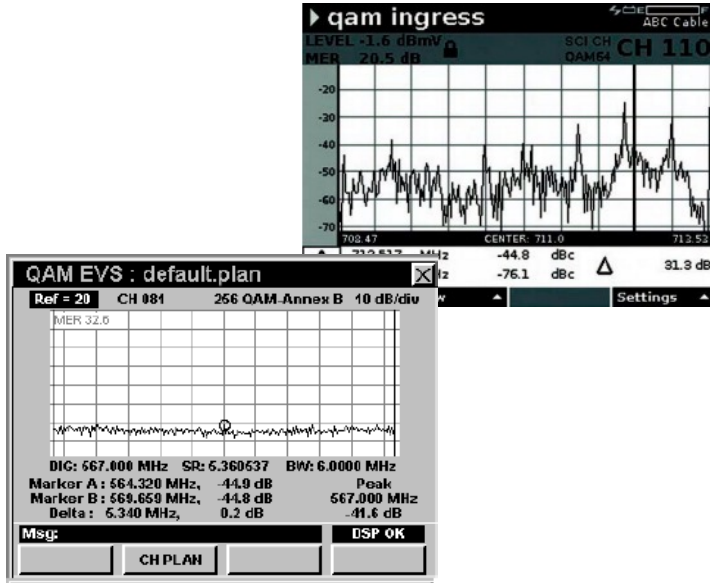
Full band capture graphics courtesy of Comcast

Managing ingress: A look at current techniques

Use field test equipment's "ingress scan mode" to check every subscriber drop when at the subscriber premises for installations and service calls



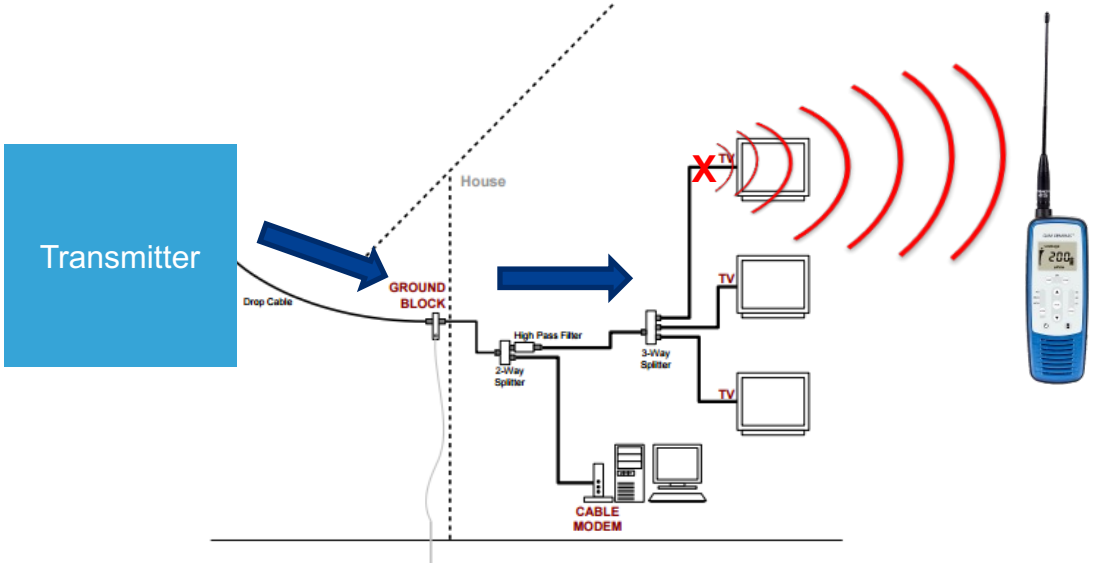
Use field test equipment's "ingress-under-the-carrier mode" to check for ingress under active QAM signals



Graphics courtesy of Trilithic and Viavi Solutions

Managing ingress: A look at current techniques

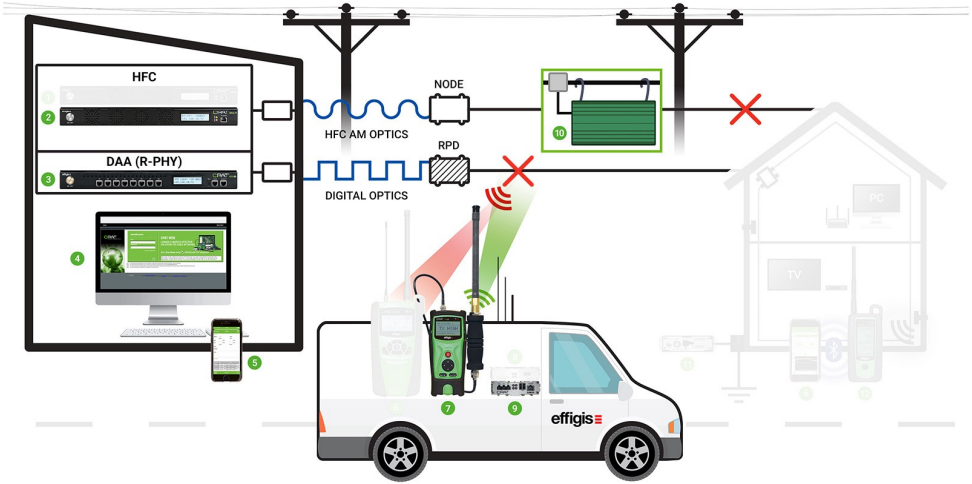
“Pressure test” the subscriber drop by injecting high-level leakage test signals into the subscriber wiring at the ground block, then monitor for leakage throughout the premises. Some leakage equipment manufacturers’ products support this technique, which can identify points in the drop where both leakage and ingress occur.



Graphics courtesy of ComSonics, Trilithic and Viavi Solutions

Managing ingress: A look at current techniques

One product, CPATFlex, does GPS-based geolocation of ingress points by transmitting an over-the-air carrier in the 6 MHz ISM band. The carrier includes geolocation data that is received at the headend. The equipment in the vehicle simultaneously monitors for downstream leakage. This method helps find where upstream ingress is entering the network, and where downstream leakage is occurring.



Graphic courtesy of CPATFlex

Key points to remember

All three of the following are related to *degraded RF shielding performance*:

- Signal leakage can interfere with over-the-air services
- Ingress from over-the-air signals can interfere with cable signals
  - Some cable operators have abandoned affected frequencies, but this is not a viable long-term solution
- Direct pickup interference can affect CPE and other devices
  - Older CPE usually more susceptible; newer CPE has better shielding. Poorly shielded “retail” cables and components installed by subscribers can offset the benefits of good CPE shielding.
  - Some headend and test equipment is susceptible to direct pickup interference

Wrapping up

Approach from several perspectives:

- Manage the CMTS and cable modem configurations for optimum performance
- Manage RF signal levels – especially in the upstream – to help improve the “signal-to-junk” ratio
- Proper return path alignment (distribution actives *and* optical links)
- VHF *and* UHF signal leakage detection, monitoring, and repair program
  - Find and fix VHF and UHF leaks, which will also help to reduce ingress problems
- Avoid future leakage and ingress problems (use high-quality components; train staff on proper installation techniques; implement quality control program)
- Use various tools to monitor for ingress: upstream spectrum monitoring (e.g., PathTrak or similar), in-home spectrum monitoring (e.g., CPE full band capture)
- Use newer, better-shielded CPE, test equipment, etc., to reduce direct pickup problems
- Educate cable subscribers about the use of poor-quality retail-grade cables and components

Additional resources

- FCC Rules, Part 76, Subpart K, Technical Standards
- SCTE 209 2015 – “Technical Report: UHF Leakage, Ingress, Direct Pickup” (https://www.scte.org/standards/library/catalog/scte-209-technical-report-uhf-leakage-ingress-direct-pickup/)
- Hranac, R., G. Tresness. “Another Look at Signal Leakage: The Need to Monitor at Low and High Frequencies,” Technical Workshop Proceedings, SCTE Cable-Tec Expo, Oct. 17-19, 2012, Orlando, FL
- Hranac, R., N. Segura. “UHF Signal Leakage and Ingress: Understanding the Liability and Risk”, Technical Workshop Proceedings, SCTE Cable-Tec Expo, Oct. 21-24, 2013, Atlanta, GA

Join us next time for Part 2

If you missed Part 1 of **Signal leakage, ingress, and direct pickup**, you can find a recording on YouTube at

https://www.youtube.com/watch?v=bYuydmmJohs