LAN security for MoCA and powerline

Brian Dipert - August 25, 2015

In my recently published "Deciphering wiring" post, I discussed (among other things) the multiple spans of Ethernet cable that shuttle LAN packets between various areas of the house and the downstairs furnace room cable modem-plus-router network nexus:

- Between the furnace room and the upstairs master bedroom
- Between the furnace room and my upstairs office
- Between the furnace room and the downstairs family room, and
- Between the family room and the upstairs living room

The residence is fairly well covered from a network topology standpoint as a result. And 5 GHz 802.11n access points in the living room and master bedroom, two ends of the upstairs, supplement the 2.4 GHz and 5 GHz beacons sourced by the router downstairs and in the middle of the house, delivering a reasonably robust Wi-Fi footprint for mobile LAN clients. However, there are three other areas in the house (all downstairs) that I'd still like to serve with faster-than-wireless bandwidth for entertainment-center and other static-client purposes: the two guest bedrooms and my wife's office.

The latter's easiest, albeit invasively so; her office is next to the family room and shares a wall with the entertainment center there, already fed by Ethernet and containing a multi-port switch. Drilling a hole through the wall in the office will enable me to tap into the existing next-door network connections. However, the guest bedrooms aren't nearly as simple to packet-serve via conventional Cat5e or Cat6 cable.

I realized the other day, though, that, like the furnace room, both guest bedrooms are pre-wired with coax cable. So I've decided to revisit my several-year-old MoCA (multimedia over coax) experiments. Regular readers may remember my December 2012 benchmarking series, which initially produced positive results in spite of the MoCA adapters' speed-capping 100 Mbps wired Ethernet transceivers:

- Benchmarking MoCA: Does coax meet your bandwidth quota?
- Benchmarking MoCA: Single-stream results suggest that HomePlug AV shouldn't worry MoCA one iota
- Benchmarking MoCA: Multi-stream testing pushes more TCP data through the connection 'straw'

Unfortunately, I ended up running into severe network performance problems while simultaneously watching cable television and loading down the LAN and cable WAN connections. But in retrospect, one aspect of my earlier setup may explain the hiccup. Recall that MoCA adapters are nominally intended for use with a Verizion FiOS modem-plus-router or other integrated gateway device that already embeds a MoCA-supportive coax-to-Ethernet bridge function. In my particular case, I needed to use a distinct adapter at the router to implement the bridge. But, as I wrote at the time, the MoCA
adapter was "in-line between the wall connector and both the CableCARD tuner and cable modem."

MoCA's press relations contact hadn't included instructions with the two Actiontec ECB2200 MoCA adapters he sent me and the online documentation isn't much better. But Internet research suggests that the ECB2200's coax output isn't a pure pass-through, as I'd previously thought; it's a "TV out" connection that's seemingly altered by internal filtering of other frequency bands. This might explain why, especially when cable television service was in active use, my WAN bandwidth adversely suffered. Alternatively, I plan this time to use a three-way coax splitter to effectively install the cable modem, CableCARD tuner, and MoCA adapter in parallel, all fed by the same (split) wall feed and with the MoCA adapter's coax output not in use.

My decision to revisit MoCA was sealed by a promotion Amazon was running at the time, on a pair of ECB2500C adapters for $79.99 (one adapter normally costs around this same price). The ECB2500C is the successor to the ECB2200; both generations are based on MoCA 1.1-supportive silicon, but the ECB2500C moves all external connections to one side of the device and potentially makes other (undocumented) changes. However, when I added the ECB2500C pair to my Amazon shopping cart, I was encouraged to also purchase a $13-and-change filter. What I discovered upon researching the product's intended use was fairly alarming.
MoCA adapters, as it turns out, ship by default with encryption turned off. Enabling encryption, along with configuring a custom encryption password (since you won't just go with the factory default ... right?) is by no means intuitive (assuming the necessary hardware switch even exists, which isn't always the case). See for yourself: here are the PDF-formatted instructions for the
ECB2200 and ECB2500C. And in the absence of a blocking filter such as the one Amazon recommended to me, if your MoCA adapters have encryption disabled or enabled with the default password, it's straightforward for neighbors sharing a street-side splitter to snoop your LAN.

This revelation next got me thinking about powerline networking. Thankfully, all of the powerline adapters I know of come with encryption enabled, albeit with a common factory-default password (56-bit DES “HomePlug” for early-generation HomePlug-standard devices, for example, and 128-bit AES “HomePlugAV” for newer-generation products). Equally thankfully, on-device push buttons for secure “pairing” are frequently available as an alternative to non-intuitive software configuration utilities. And as long-time readers already know from my regular testing of multiple technologies-, generations- and manufacturers-worth of powerline adapters, it's difficult enough to get powerline-transported packets to jump across the two phases of the 220V source within a home, far from traveling outside the home.

However, as abundant Internet case studies suggest, LAN data leakage beyond any particular residence is indeed possible, especially in apartment complexes and other close-proximity housing configurations where multiple residences are served by the same street-side transformer. Ignorance may indeed be bliss in some cases, as the saying goes, but I daresay not when unwanted access by others of your personal information is concerned. Equally disconcerting is the possibility of others using your broadband connection for their own nefarious purposes, with law enforcement subsequently being unable to discern that the illegal activity wasn't coming from you. And true, wireless networking has the same conceptual security issue ... I'm easily able to "see" my next-door neighbors' SSIDs. But I think that LAN equipment manufacturers have been much more upfront in educating consumers of the need to set unique and secure Wi-Fi encryption passwords than they have been with MoCA and powerline. And that's too bad.

Also see:

- Benchmarking MoCA: Does coax meet your bandwidth quota?
- Narrowband Powerline Communication--Applications and Challenges—Part I
- Low-cost Arduino Wi-Fi shield provides security & intelligence needed for IoT apps
- HomePlug AV: Partial Powerline Progress (And Other LAN Thoughts)