

CYBER SECURITY

New Internet Research Shows 30,000 Spoofing Attacks Per Day

December 12, 2018 | Read Time: 5 Minutes

NEWS

January 30, 2012

Student Admitted to ARP Spoofing His School Network through Android Device

  63 Shares  Christine Torralba

IP and ARP Security, Earlence Fernandes

Today's agenda

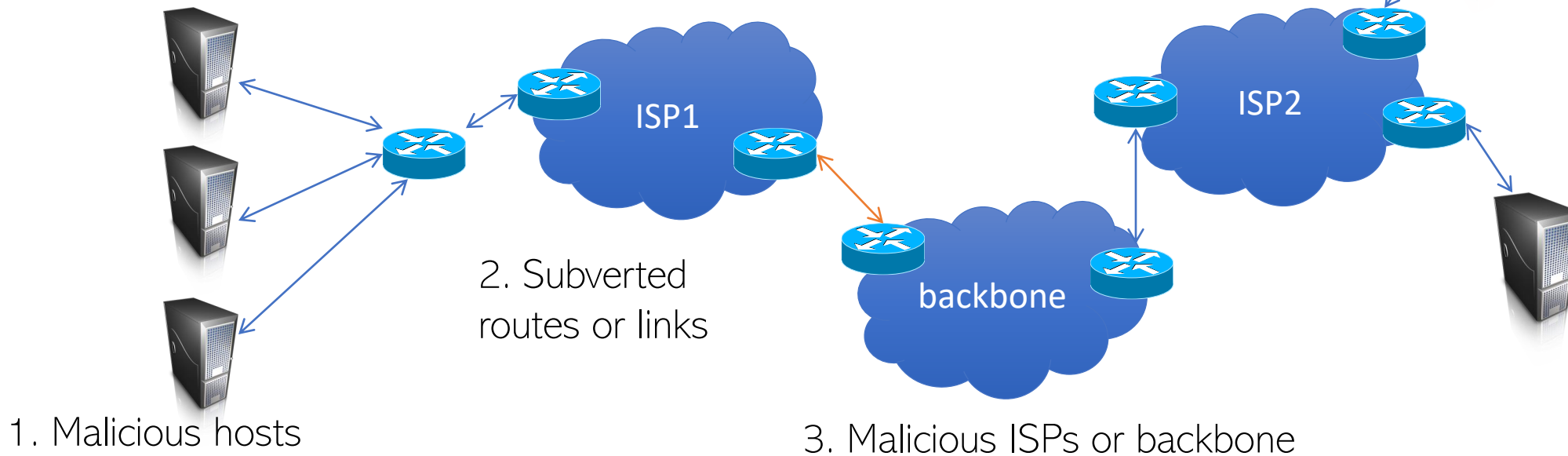
- IP Spoofing
 - Denial of Service attack (DoS)
 - Distributed DoS (DoS)
 - Source address validation
- Link layer security
 - Address resolution protocol (ARP)
 - Mapping IP to MAC address
 - MAC address spoofing



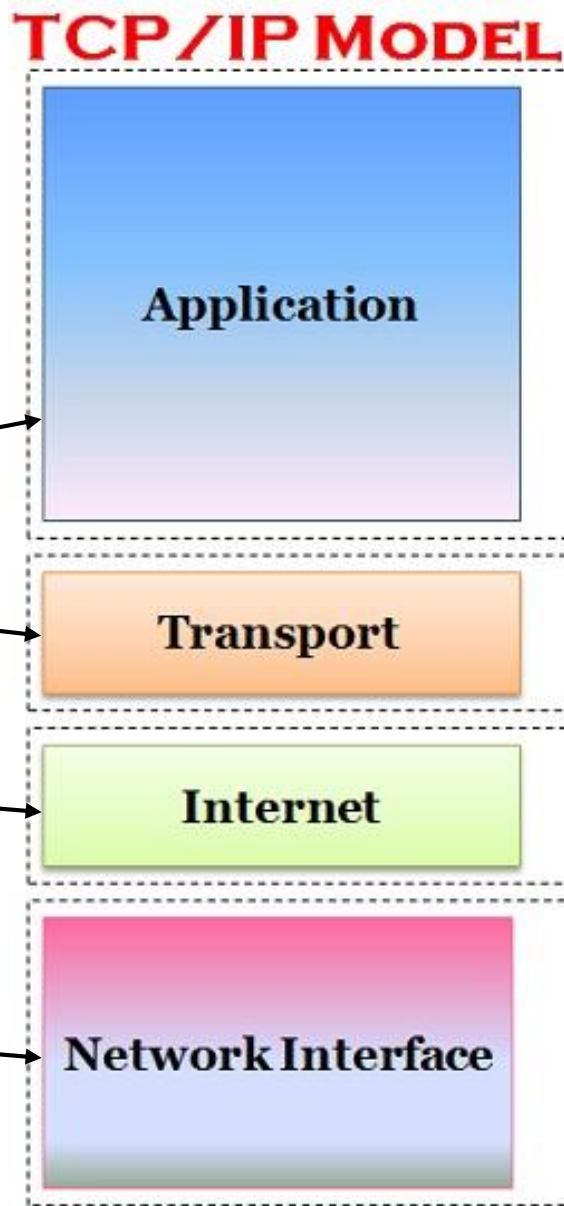
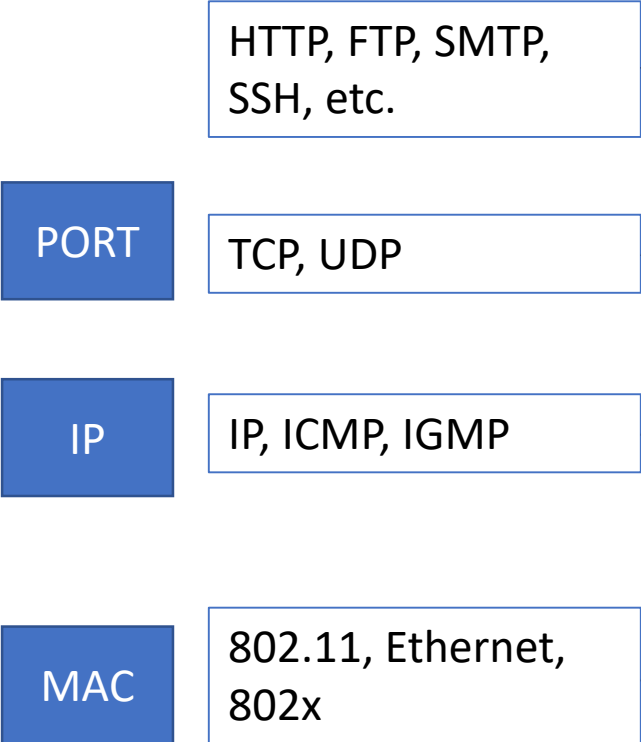
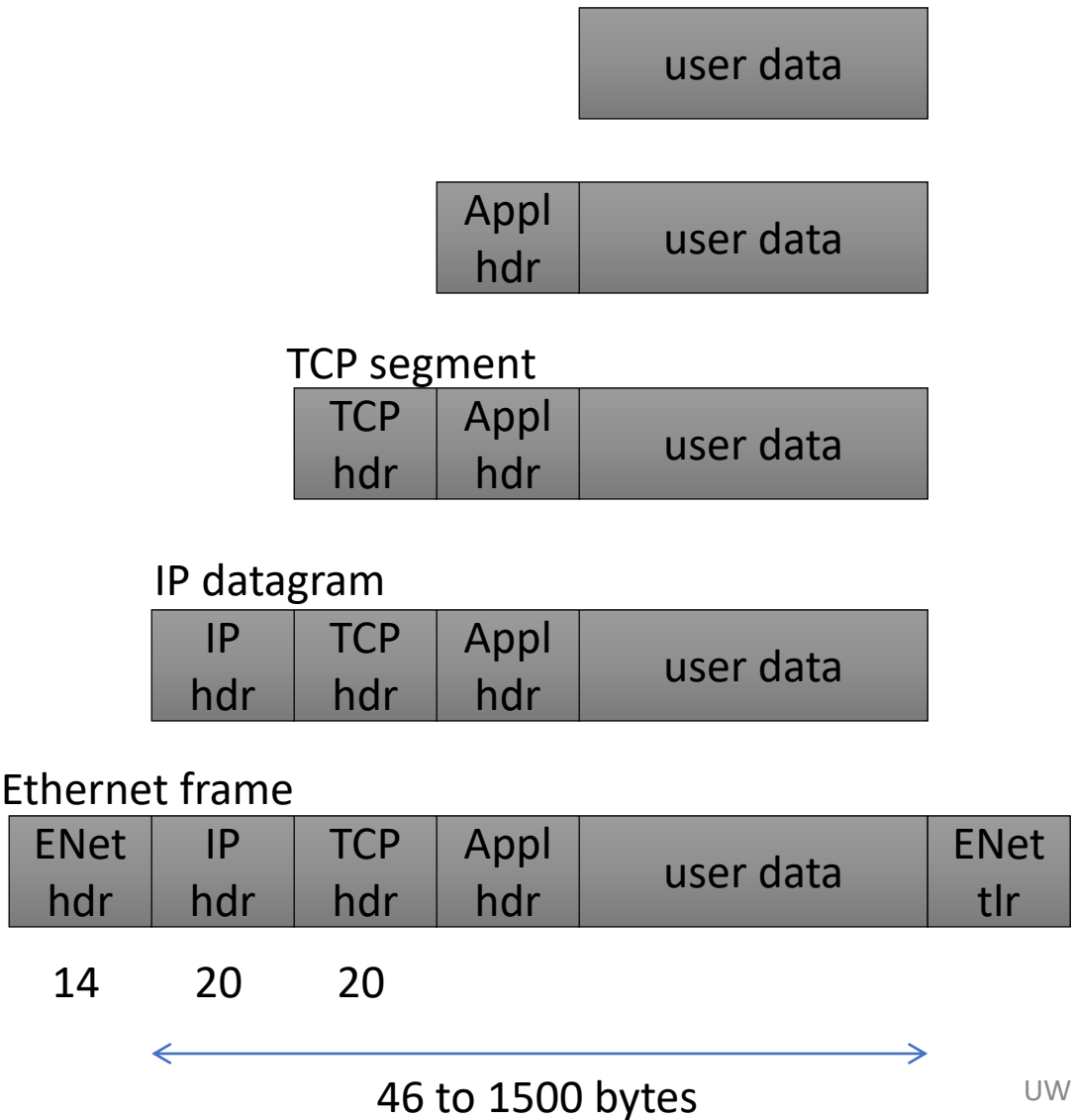
Announcements

- Midterm 1 in class Mar 10 Tuesday
 - Open notes/books with laptop but NO INTERNET
 - 70 minutes, 70 points
 - Everything we've covered until and including today
 - Questions biased towards earlier material
 - Free form, recall and creative thinking
- Feedback forms are out
 - Take a minute now to put some feedback in
 - Very helpful for us

Recap: Network threat model



Recap: Internet Protocol Stack

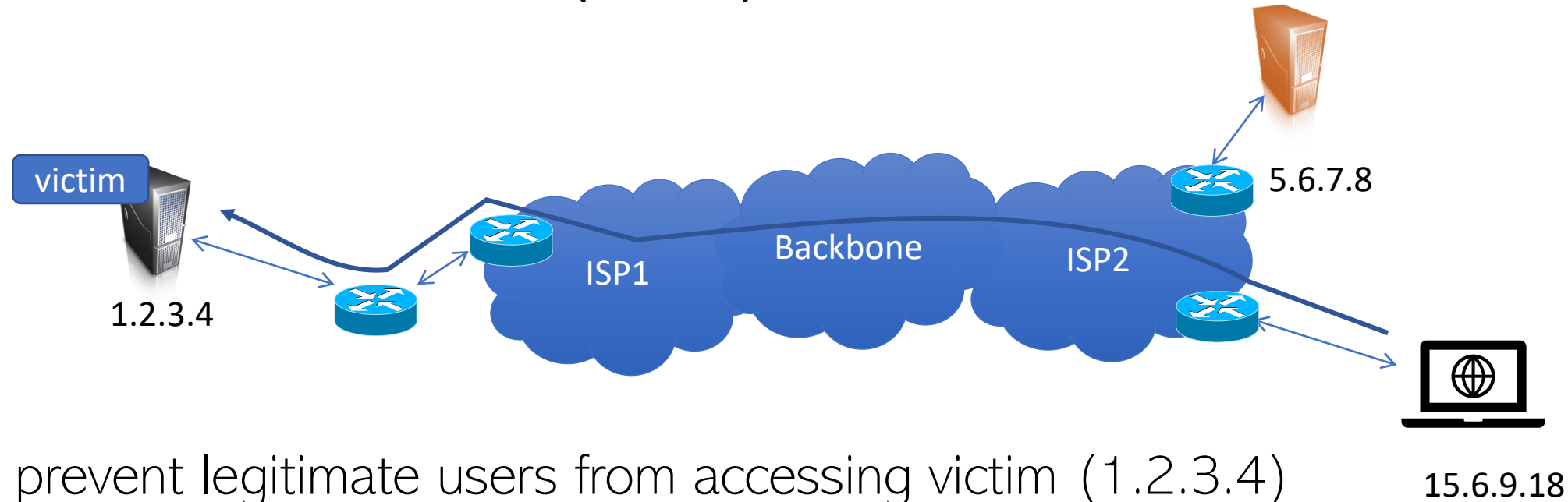


Recap: Identifiers on the internet


- **Port: 0 – 65535 (16-bit)**
 - 0 – 1023 : System reserved, 80: HTTP, 443: HTTPS, 53: DNS,
 - 1024 – 49151 : Semi-reserved, used by application developer
 - 49152 – 65535 : Used by client programs, e.g. Browser
- **IP: 32-bit (IPv4) or 128-bit (IPv6) identifier**
 - a . b . c . d – four unsigned integers
 - CIDR (Classless Inter-Domain routing): a . b . c . d / x
 - x – bit prefix is “owned” by the entity,
 - Or, IP addresses with same /x prefix share some portion of route
- **MAC # (Media access control): 48-bit identifier**
 - Unique for the ethernet/wifi card
 - Often preset by manufacturer, but one can change them easily



Denial of Service (DoS) attacks



Goal: prevent legitimate users from accessing victim (1.2.3.4)

 The Verge

Telegram blames China for 'powerful DDoS attack' during Hong Kong protests

Bloomberg reports that encrypted messaging apps like Telegram and FireChat are currently trending in Apple's Hong Kong App Store, ...
Jun 13, 2019



 TechRadar

Wikipedia goes offline following DDoS attack

A major cyberattack took down Wikipedia in several markets over the ...
denial of service (DDoS) attack that took down its sites across part of ...
1 month ago



DoS

- Overwhelm the victim with malicious traffic
 - E.g., ICMP Flood, SYN flood
- Many types
 - Application layer DoS
 - Locking all user accounts in a system (by repeated password guesses)
 - Distributed DoS
 - Get a pool of (compromised) machines/devices to send malicious traffic
 - SYN floods
 - Reflected DoS
 - Send spoofed IP packets to benign servers who responds with large amount data



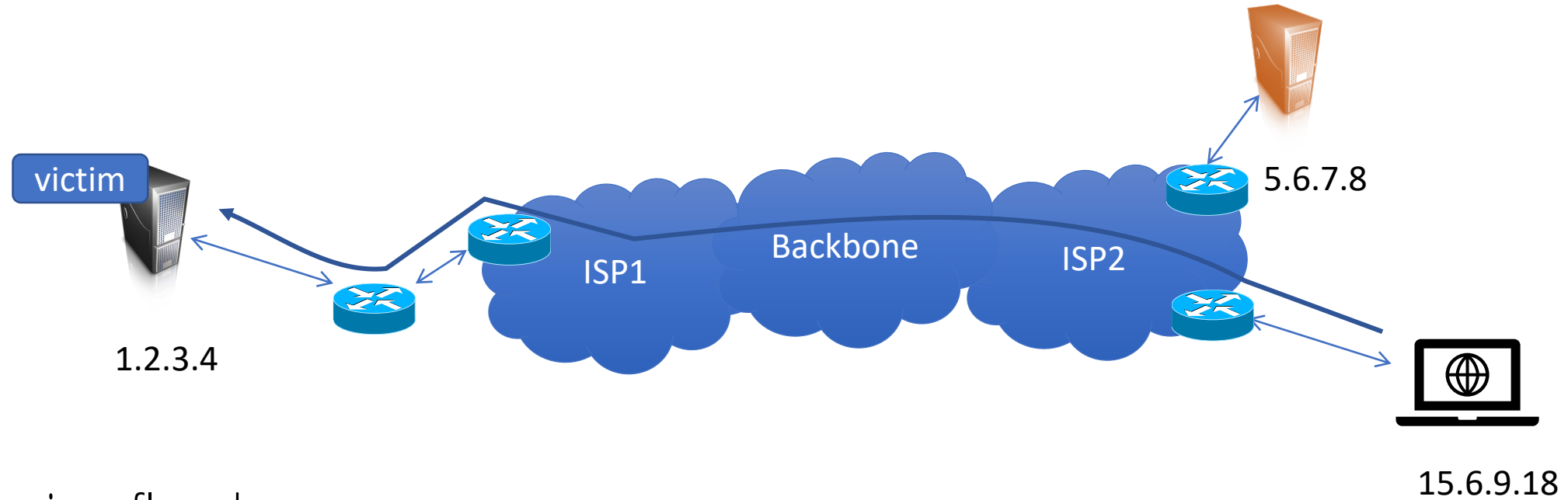
ICMP (Internet Control Message Protocol)

IP hdr	ICMP hdr	ICMP message
-----------	-------------	--------------

8-bit type	8-bit code	16-bit checksum
4-byte more of header (depends on type)		
message ...		



ICMP Flood



ICMP ping flood

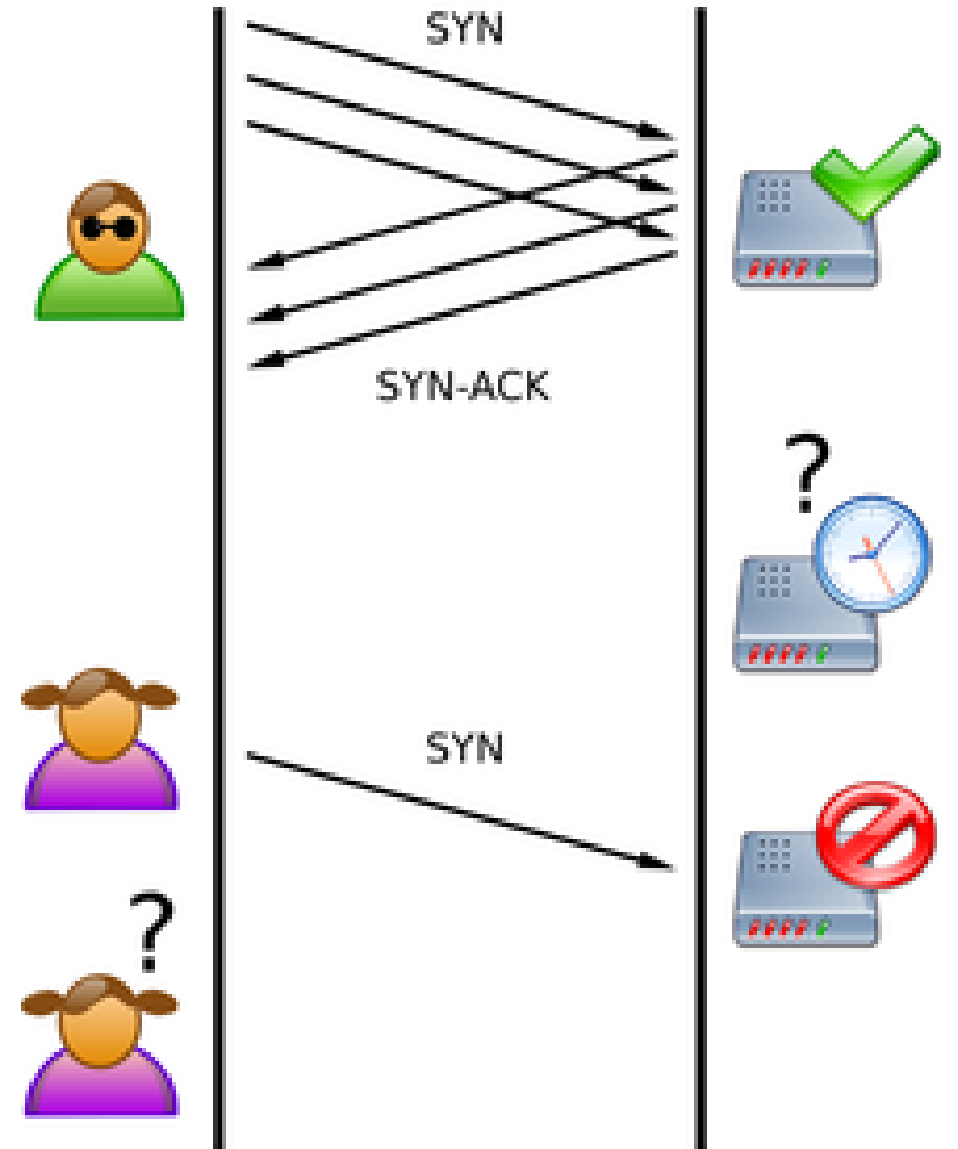
- Attacker sends ICMP pings as fast as possible to victim
- When will this work as a DoS? Attacker resources > victim's
- How can this be prevented? Ingress filtering near victim



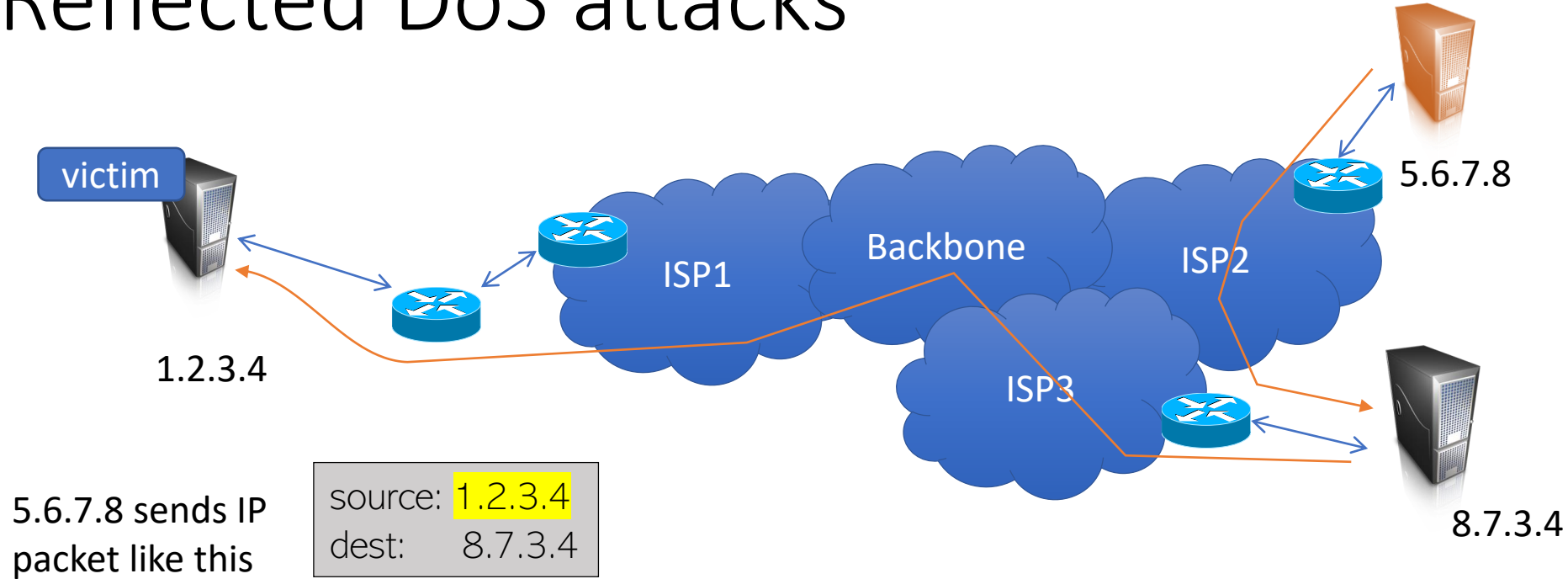
TCP SYN Flood

Send a bunch of **SYN** packet to a router/server

- Never respond with an **ACK**
- Half-open TCP connections hold resources in the server
- Legitimate users cannot access the server



Reflected DoS attacks

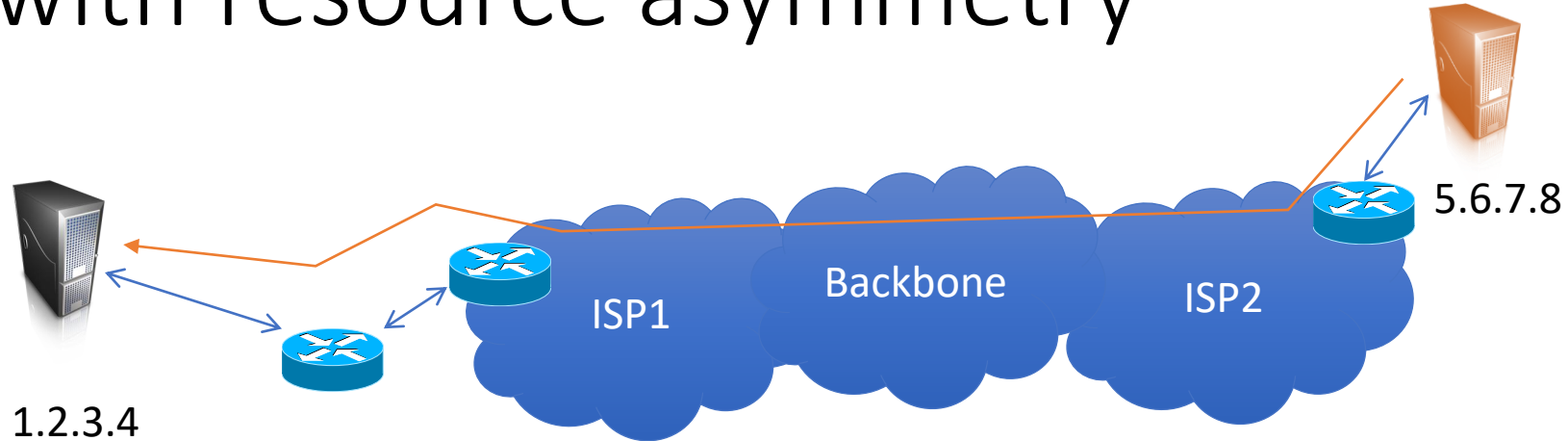


Attacker sends packets with spoofed source address

Filter based on source may be incorrect



DoS with resource asymmetry

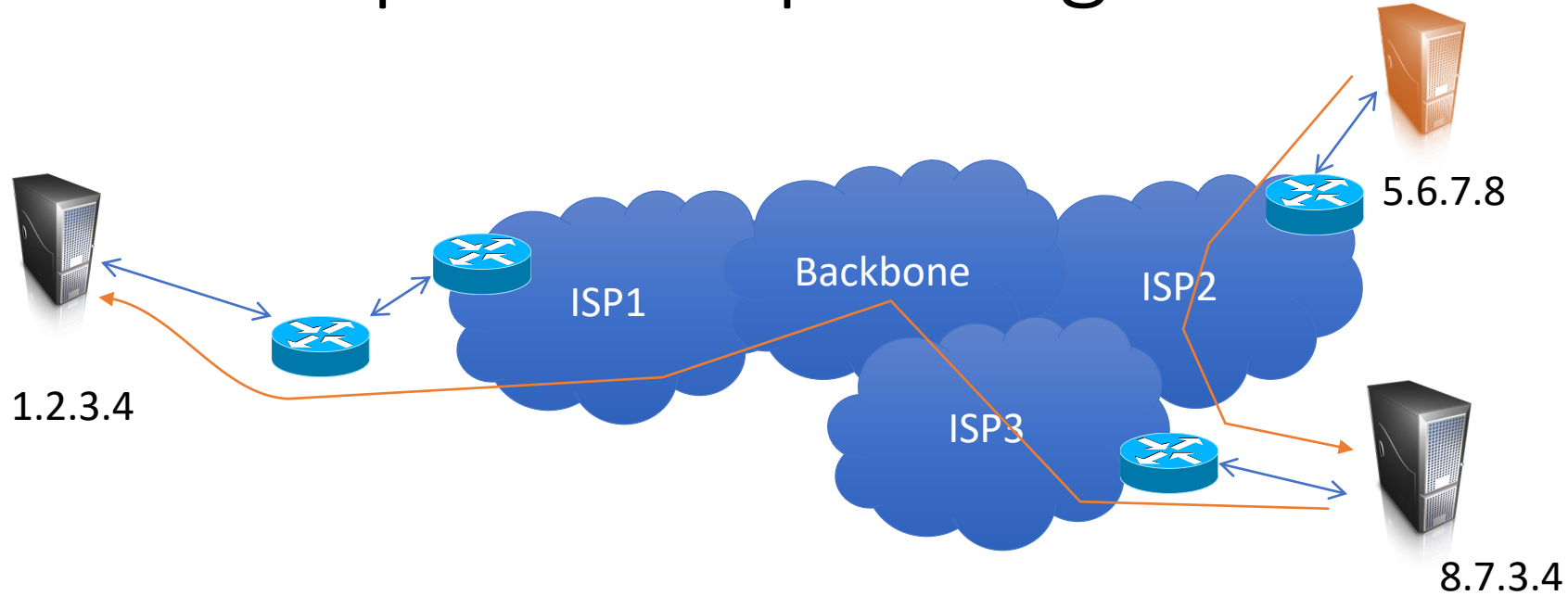


Attacker uses few resources to cause victim to consume lots of resources

- DNS amplification attack
 - Send DNS request w/ spoofed target IP (~64-byte request)
 - DNS replies sent to target (~512-byte response)
- Smurf Attack
 - Broadcast ICMP ping on a router with spoofed victim's IP address
 - (not allowed with newer router)
- Ping of death
 - A single packet that causes crash on remote system
 - Early on: ping packet with size > 65,535



How to prevent spoofing?



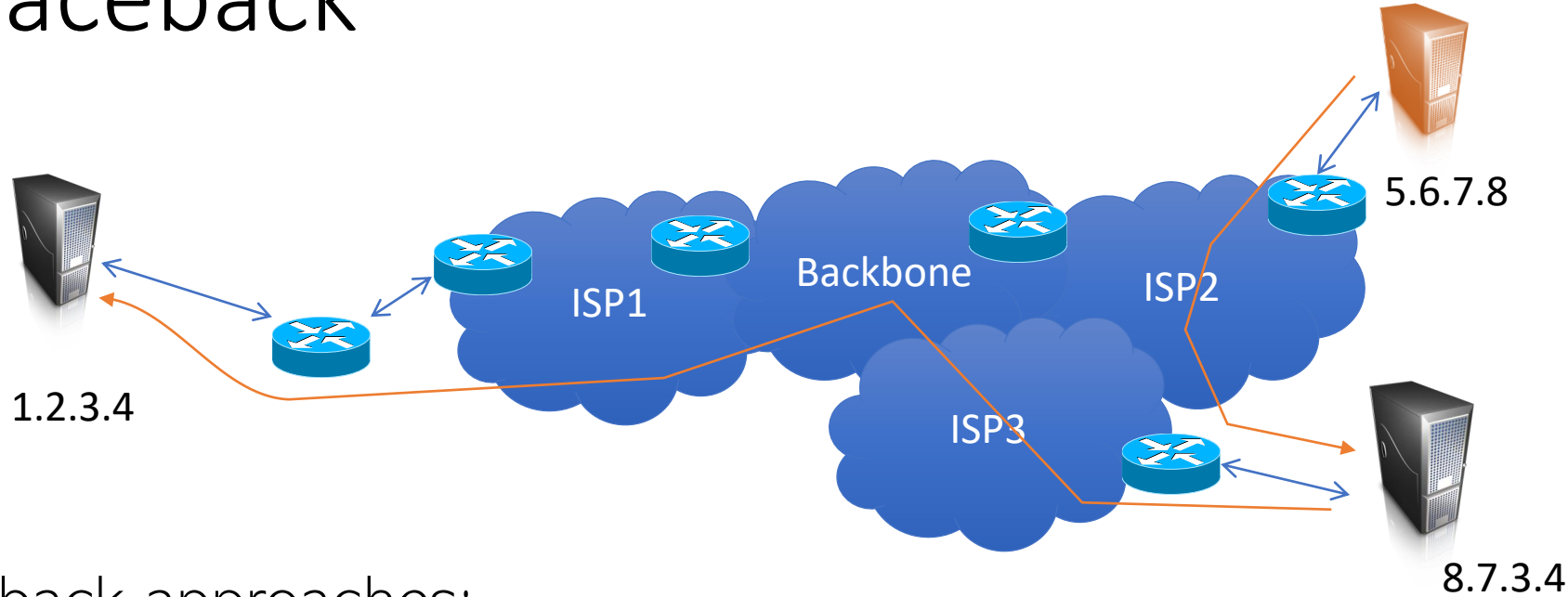
Spoofed IPs means we cannot know where packets came from.

Solution:

- BCP 38 (RFC 2827)
 - upstream ingress filtering to drop spoofed packets
 - source address validation
- IP traceback
 - Identify sources of attack



IP traceback

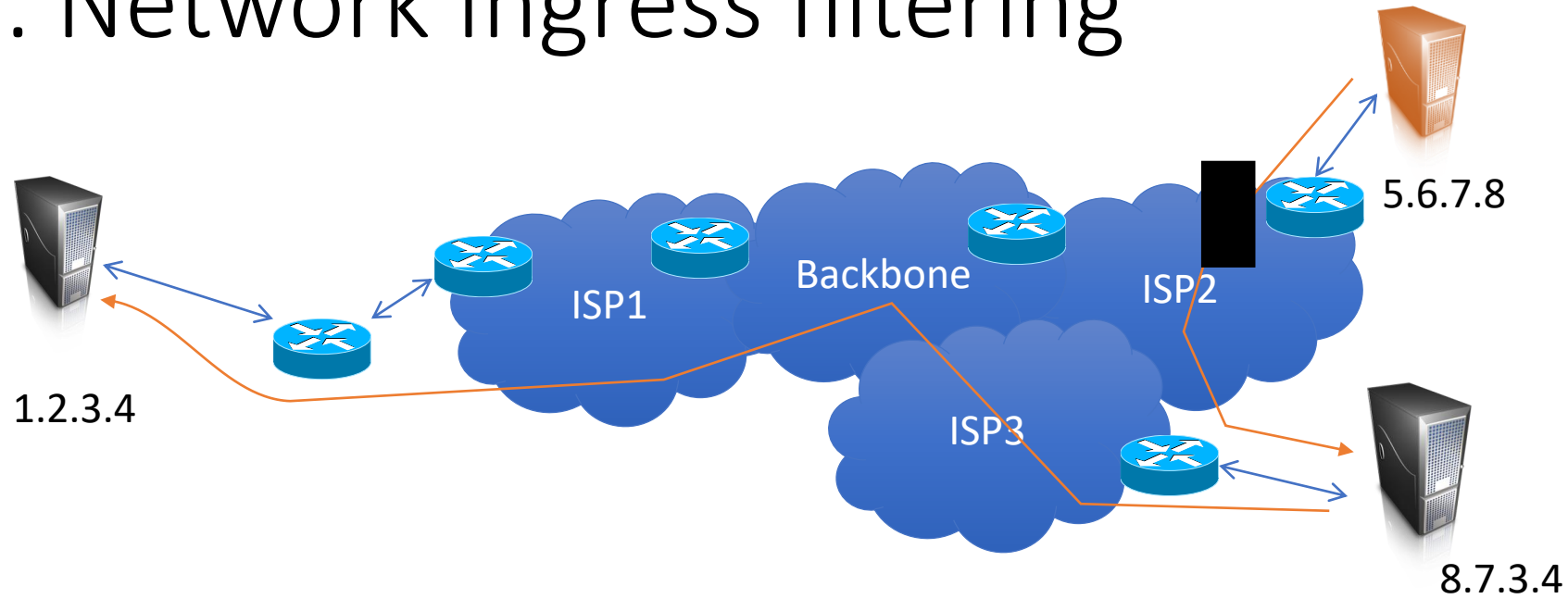


IP traceback approaches:

- **Logging** – each router keeps logs of packets going by
- **Input debugging** – feature of routers allowing filtering egress port traffic based on ingress port. Associate egress with ingress
- **Controlled flooding** – mount your own DoS on links selectively to see how it affects malicious flood
- **Marking** – router probabilistically marks packets with info



BCP38: Network Ingress filtering

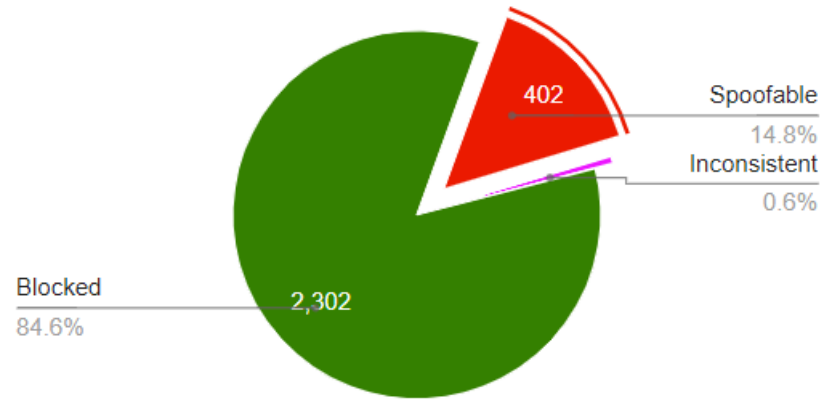


Before forwarding on packets, check at ingress that source IP legitimate



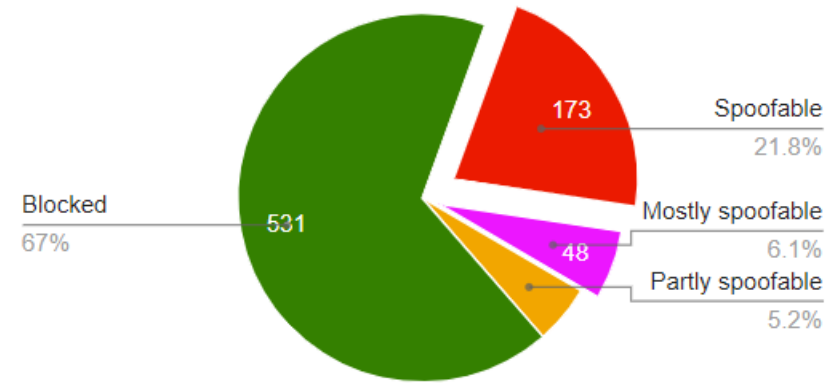
BCP 38: We are getting there...

IPv4 blocks (excluding NAT)



Status	Count
Spoofable	402
Inconsistent	17
Blocked	2302

IPv4 autonomous systems (excluding NAT)

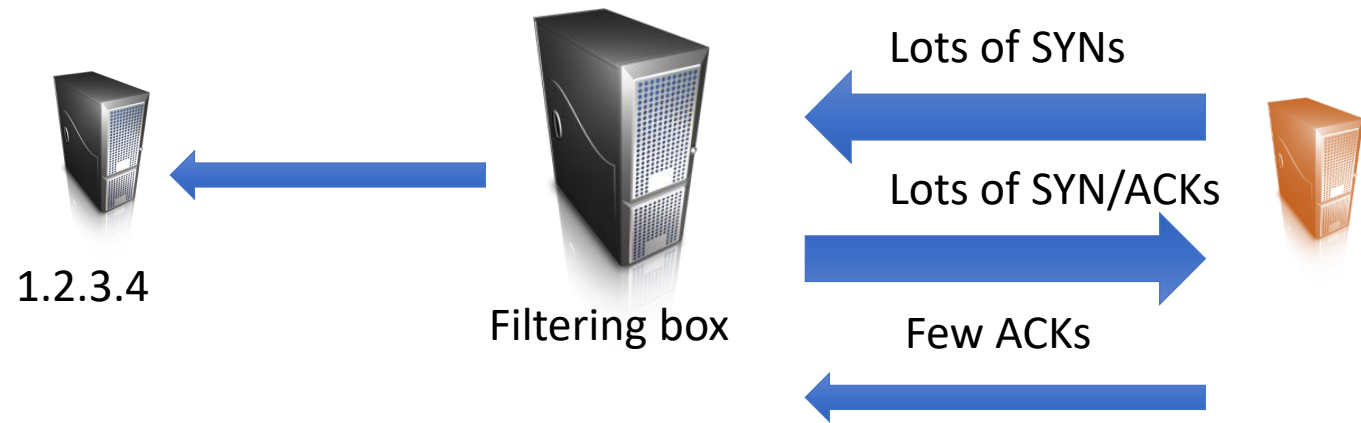


Status	Count
Spoofable	173
Mostly spoofable	48
Partly spoofable	41
Blocked	531

Still 14-21% are still spoofable



Preventing DoS: beat the power



Just need a beefy box to help with filtering. There are several anti-DoS protection

- Prolexic (acquired by Akamai)
- Cloudflare
- Google Cloud Armor

PROLEXIC
Now part of 




CLOUDFLARE®



Mirai

- September 2016, 600 Gbps attack on Krebs, Dyn.
- IoT devices: IP Cameras
- Peak infection: 600k devices, steady state: 200 to 300k
- Default username/passwords on IP Cameras

60 lines (60 sloc) | 778 Bytes

```
1  root xc3511
2  root vizxv
3  root admin
4  admin admin
5  root 888888
6  root xmhdipc
7  root default
8  root jauntech
9  root 123456
10 root 54321
11 support support
12 root (none)
13 admin password
14 root root
15 root 12345
```

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)



Anna-senpai 

L33t Member



Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's a hot market. However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Krebs DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Paras Jha, co-author of Mirai

- 2500 hours community service
- Home confinement
- 8.6 million USD in restitution
- Why DDoS?
 - Juvenile reasons (student at Rutgers CS)
 - Delay calculus exam
 - Prevent others from registering for an advanced CS course he wanted to take



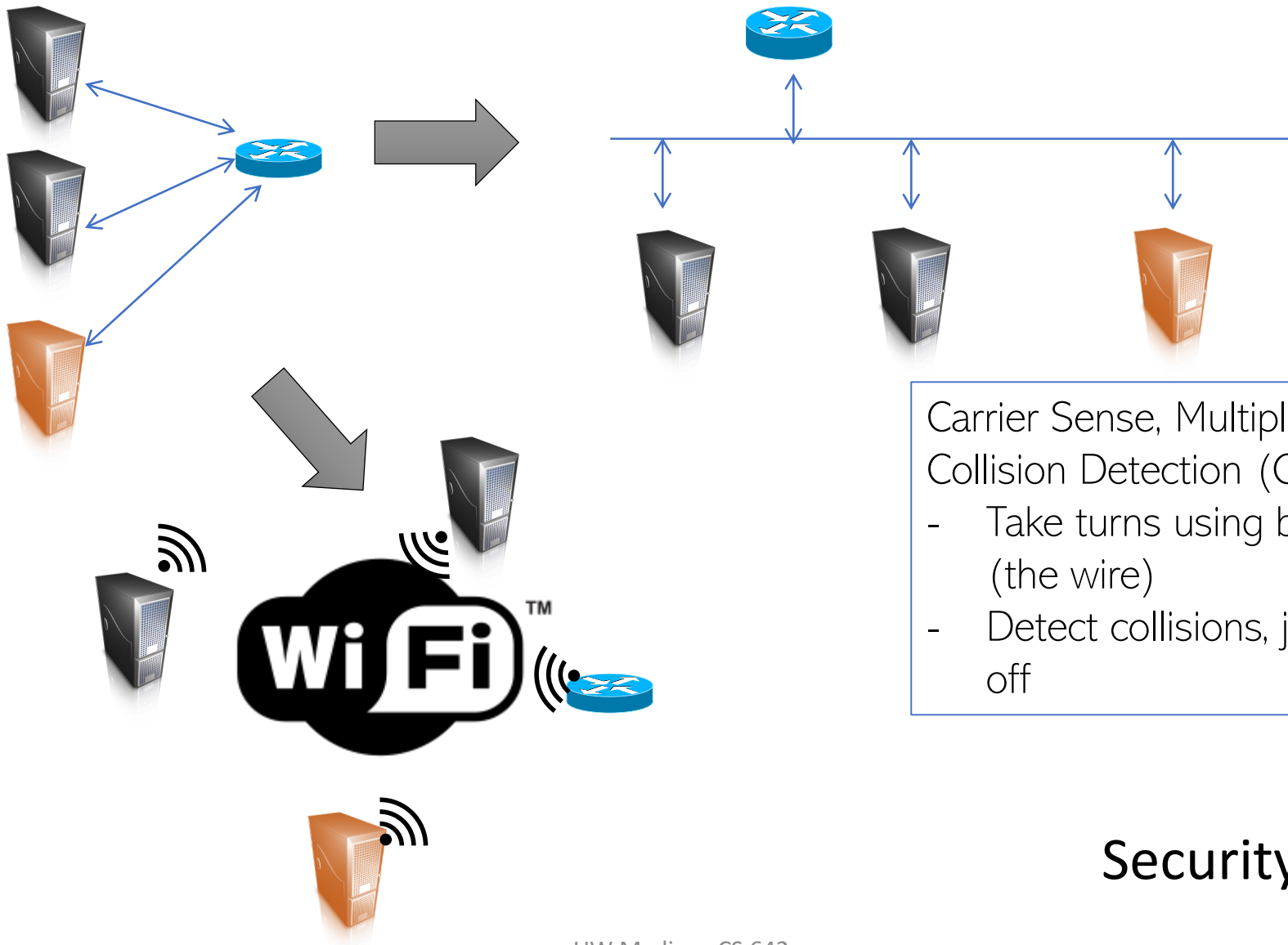
<https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/>

<https://krebsonsecurity.com/2018/10/mirai-co-author-gets-6-months-confinement-8-6m-in-fines-for-rutgers-attacks/>

Link layer security



Link layer: Ethernet/WiFi



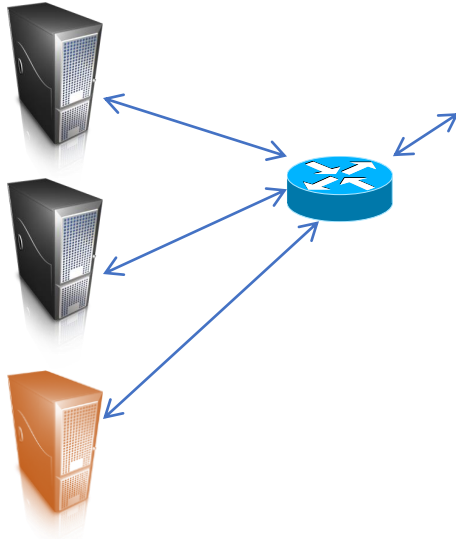
Carrier Sense, Multiple Access with Collision Detection (CSMA/CD)

- Take turns using broadcast channel (the wire)
- Detect collisions, jam, and random back off

Security issues?



Address resolution protocol (ARP)



IP routing:

- Figure out where to send an IP packet based on destination address.
- Link layer and IP layer must cooperate to get things sent
- ARP/RARP enables this cooperation by mapping IPs to MACs

32-bit IP address

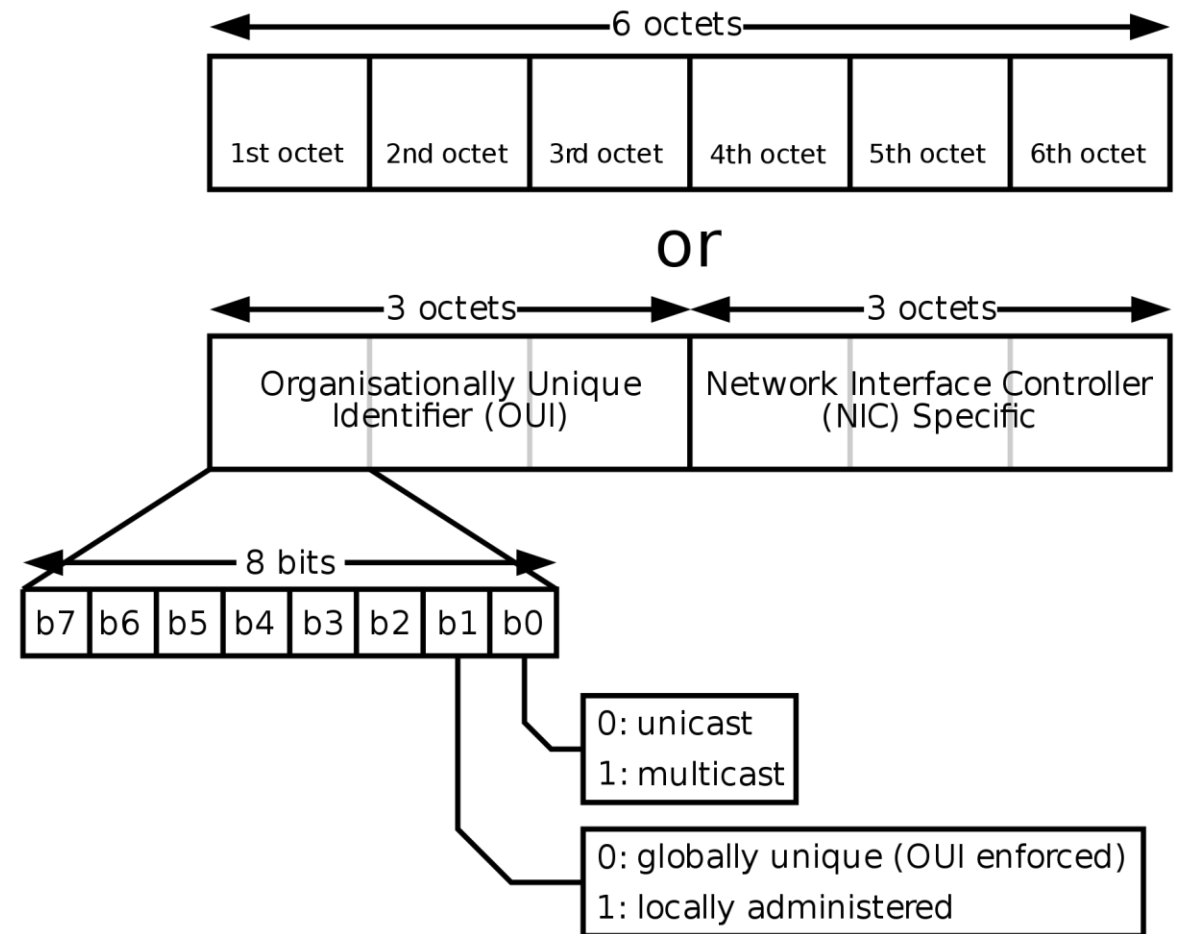
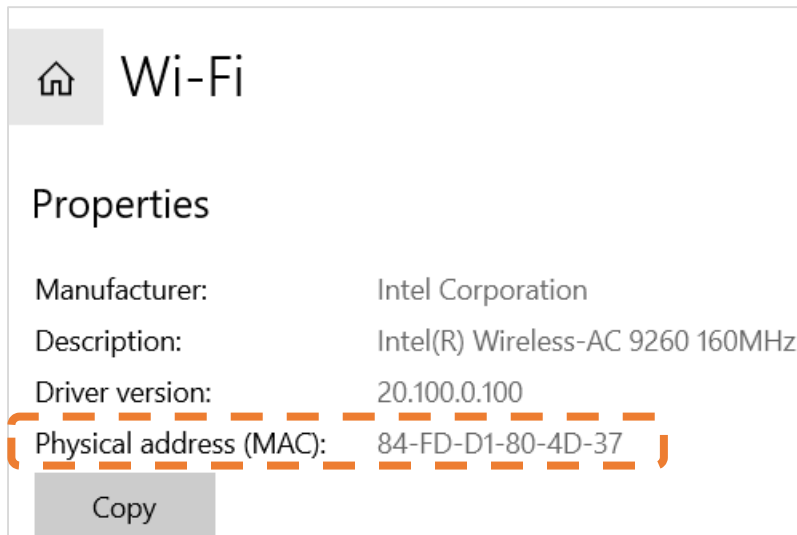


48-bit MAC address



Media Access Control Number (MAC)

- “Unique” identifier for a device.
Two types
 - Globally administered
 - Locally administered
- OS can “change” MAC



MAC Spoofing

APPLE:

```
$ sudo ifconfig en0 ether xx:xx:xx:xx:xx:xx
```

LINUX

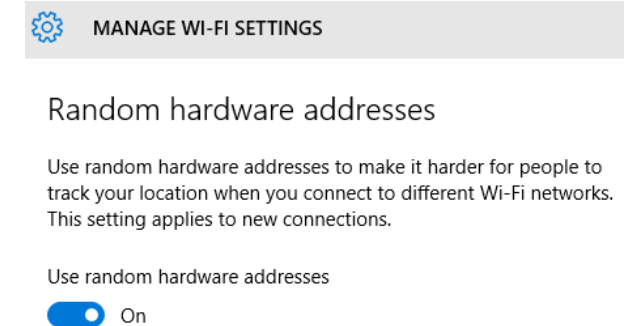
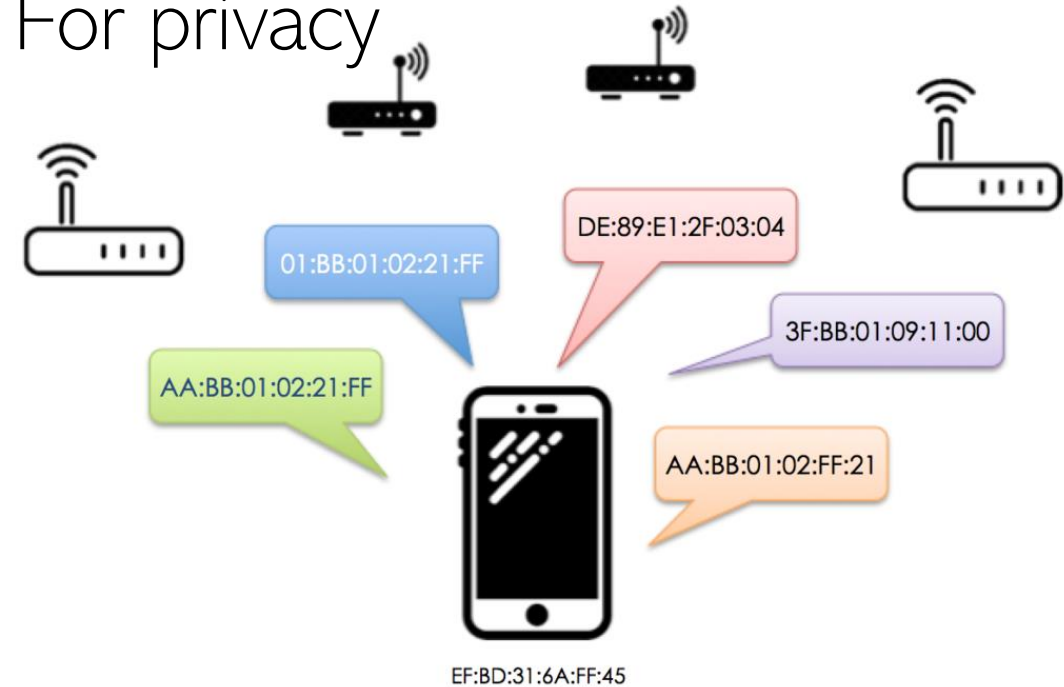
```
$ sudo ip link set eth0 address xx:xx:xx:xx:xx:xx
```

For stealing

Hack Open Hotel, Airplane & Coffee Shop Wi-Fi with MAC Address Spoofing

BY KODY © 03/15/2018 10:36 AM WI-FI HACKING

For privacy



MAC spoofing is not illegal, but can show criminal intent

Aaron Swartz, a fellow at Harvard University's Center for Ethics and an open source programmer involved with creating the RSS 1.0 specification and more generally in the open culture movement, has been arrested and charged with **wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer** after he entered a computer lab at MIT in Cambridge, Massachusetts and downloaded two-thirds of the material on JSTOR, an academic journal repository.

http://en.wikinews.org/wiki/Aaron_Swartz_arrested_and_charged_for_downloading_JSTOR_articles

<https://www.internethalloffame.org/inductees/aaron-swartz>

When Aaron Swartz Spoofed His MAC Address, It Proved He Was A Criminal; When Apple Does It, It's Good For Everyone

Aaron Swartz



Swartz at a meetup in August 2009

Born	Aaron Hillel Swartz ^[1] November 8, 1986 Highland Park, Illinois, ^[2] U.S.
Died	January 11, 2013 (aged 26) Brooklyn, New York City



INTERNET
HALL of FAME®

Celebrating people who bring the Internet to life

HOME **INDUCTEES** NOMINATIONS INTERNET HISTORY SPEAKERS

INDUCTEES

HOME / INDUCTEES / AARON SWARTZ



©Quinn Norton

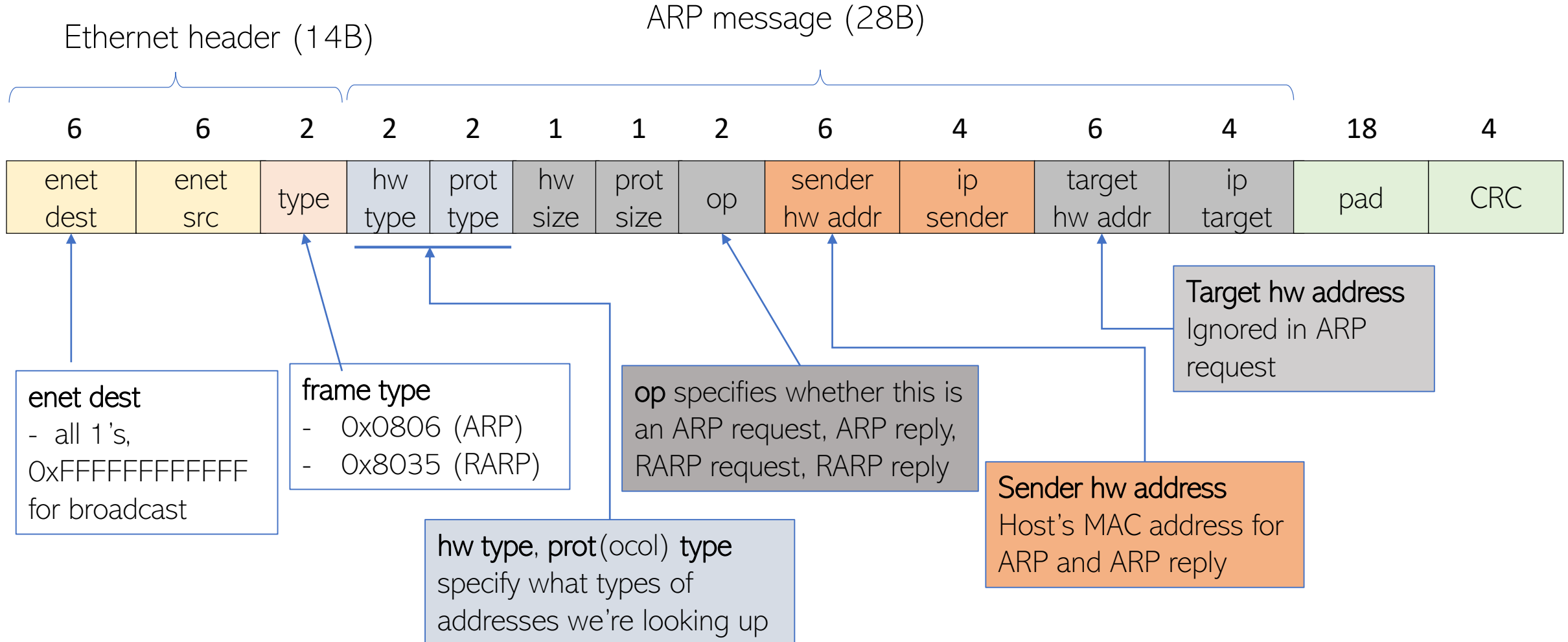
INTERNET HALL of FAME INNOVATOR

Aaron Swartz

Posthumous Recipient

Aaron Swartz was a computer programming prodigy and activist who played an instrumental role in the campaign for a free and open Internet and used technology to fight social corporate and political injustices.

Address resolution protocol



ARP caches

- Hosts maintain cache of ARP data
 - just a table mapping between IPs and MACs

```
C:\Users\earle>arp -a

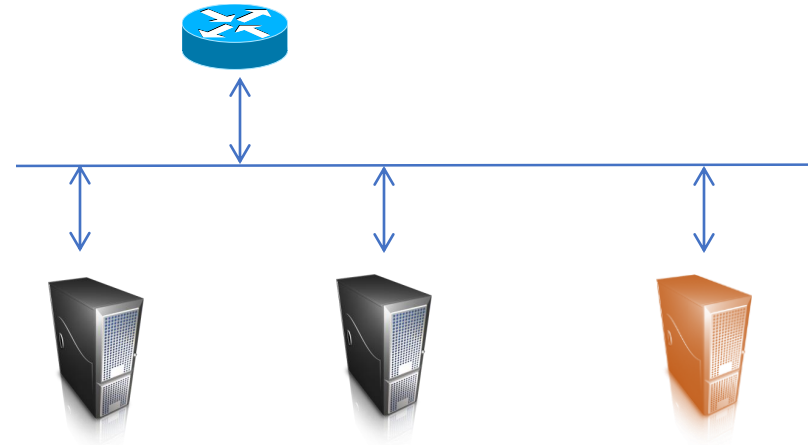
Interface: 192.168.86.63 --- 0x13
    Internet Address      Physical Address      Type
    192.168.86.1          28-bd-89-e0-b1-8b    dynamic
    192.168.86.22         f0-72-ea-42-05-90    dynamic
    192.168.86.28         a4-77-33-4e-50-40    dynamic
    192.168.86.35         48-d6-d5-86-4a-2f    dynamic
    192.168.86.255        ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static
```



ARP has no authentication

- Easy to sniff packets on (non-switched) ethernet
- What else can we do?

Easy Denial of Service (DoS):
Send ARP reply associating
gateway 192.168.1.1 with a
non-used MAC address



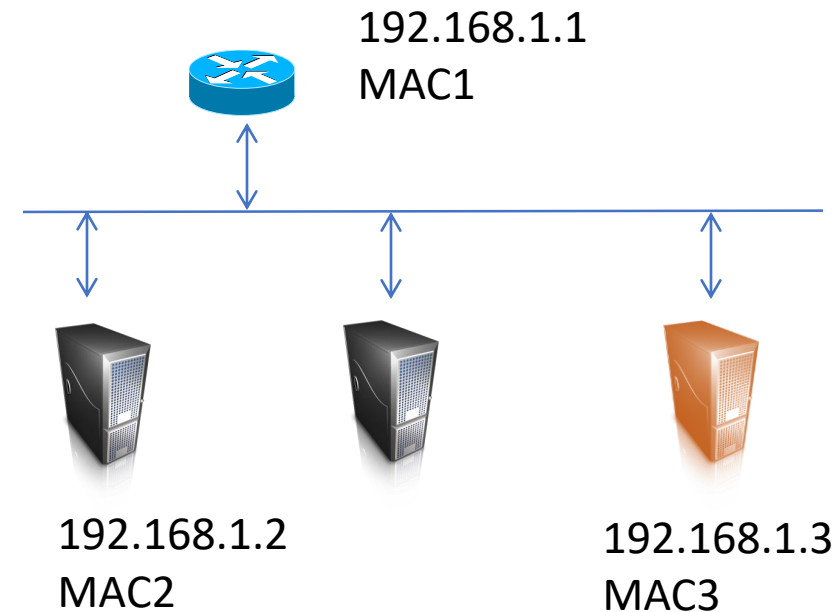
ARP has no authentication

- Easy to sniff packets on (non-switched) ethernet
- What else can we do?

Active Man-in-the-Middle:

ARP reply to MAC2
192.168.1.1 -> MAC3

ARP reply to MAC1
192.168.1.2 -> MAC3



Now traffic “routed” through malicious box



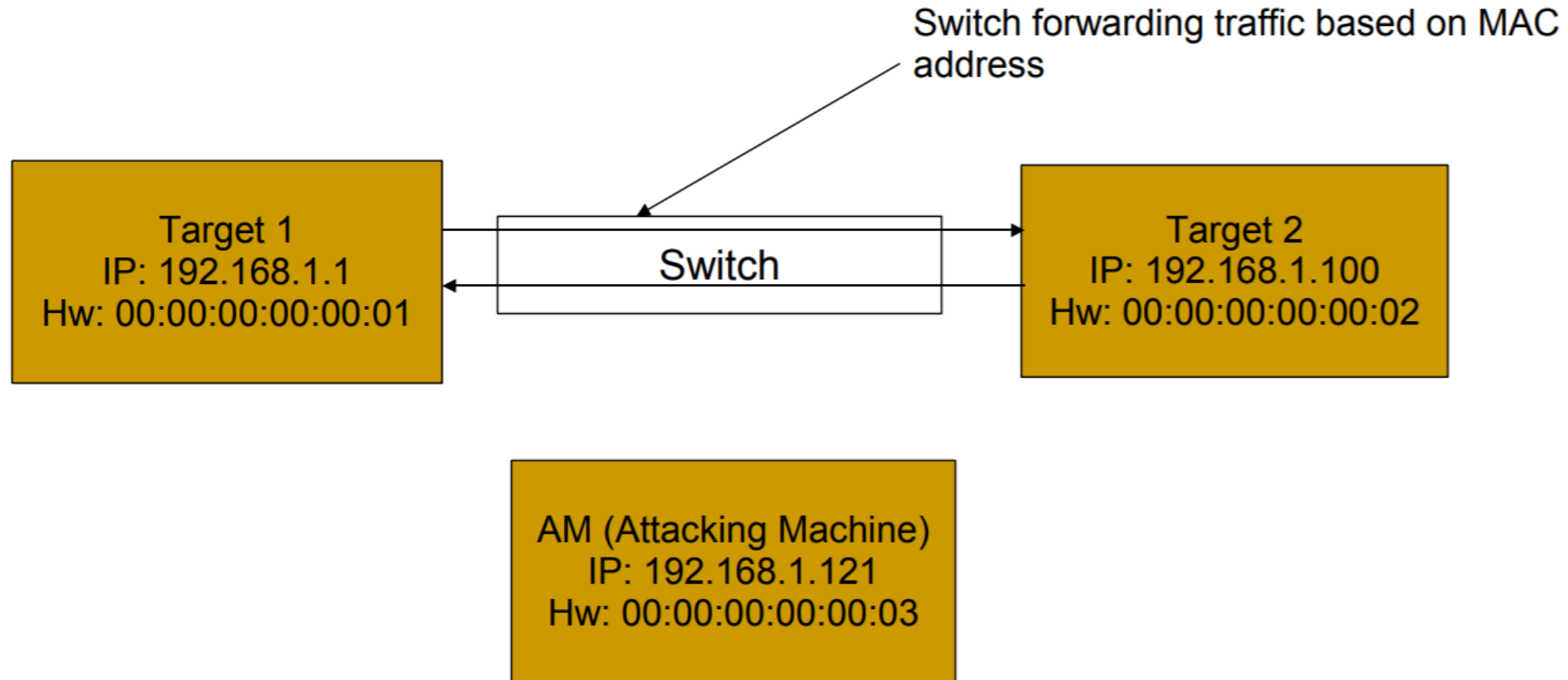
ARP Poisoning

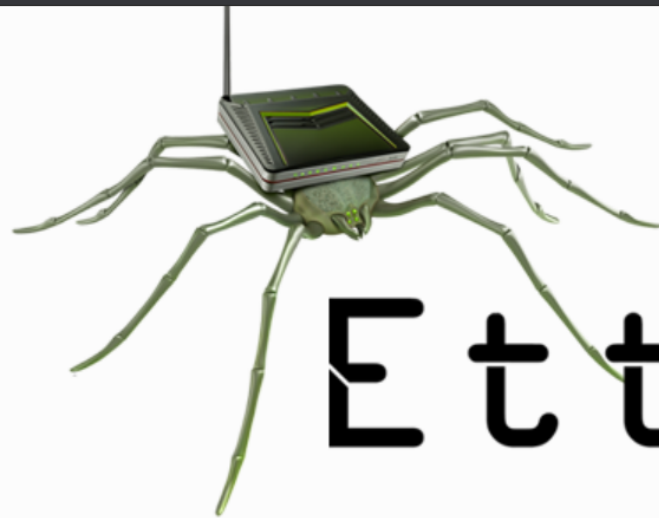
T1(192.168.1.1):

192.168.1.100	00:00:00:00:00:02
192.168.1.123	00:00:00:00:00:14

T2(192.168.1.100):

192.168.1.1	00:00:00:00:00:01
192.168.1.123	00:00:00:00:00:14





Ettercap

ETTERCAP HOME PAGE

[HOME](#)[ABOUT](#)[DOWNLOADS](#)[GET INVOLVED](#)[BUG SUBMISSION](#)[USERS MAILING LIST](#)

WELCOME TO THE ETTERCAP PROJECT

Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

Detection and prevention

- **ARPCWATCH**
 - logs ARP mapping changes
 - emails admin if something suspicious comes up
- **Static ARP Map**
 - For critical services, pre-load IP <-> MAC mapping
- **Antidote**
 - Linux daemon that monitors for unusually large number of ARP packets
- **Switched networks with real authentication**
 - Check MACs against AAA system (authentication, authorization, accounting)



Recap in Network Security

- TLS: End-to-End confidentiality, integrity, and authenticity
 - Server verification via certificate
 - Client verification?
- TCP/IP/Link layer protocols
 - DNS: domain -> IP => DNS cache poisoning
 - ARP: IP -> MAC => MAC spoofing/ ARP spoofing
 - BGP: find path from IP -> IP => IP spoofing, BGP hijack
- Talked about physical layer attacks, and defenses
 - Switched network with real authentication of MAC -> IP (CS n/w)
 - You cannot just plug your machine and get connected to the internet