Intro to Network Security

CSE 548 Spring 2024
jedimaestro@asu.edu

“For the mind does not require filling like a bottle, but rather, like wood, it only requires kindling to create in it an impulse to think independently and an ardent desire for the truth.”

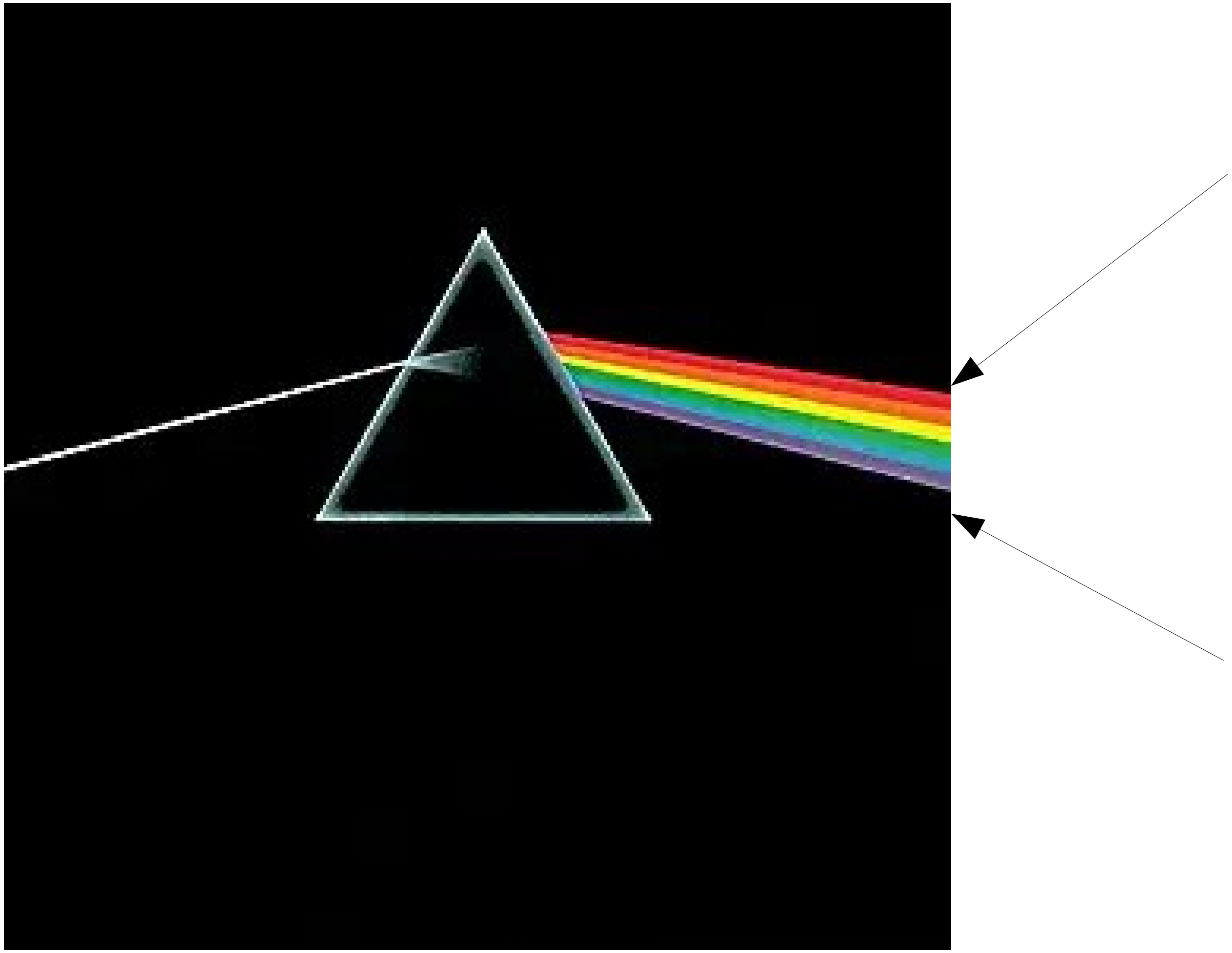
-Plutarch

Three Parts of the course...

- Part 1: Internet and Crypto
  - Introducing this today
- Part 2: Network Intrusion Detection Systems (NIDS)
  - Deep Packet Inspection (DPI) and ways to evade it
- Part 3: Malware and Side Channels
  - Attacks on the DNS system, *etc.*

Part 1: Internet and Crypto

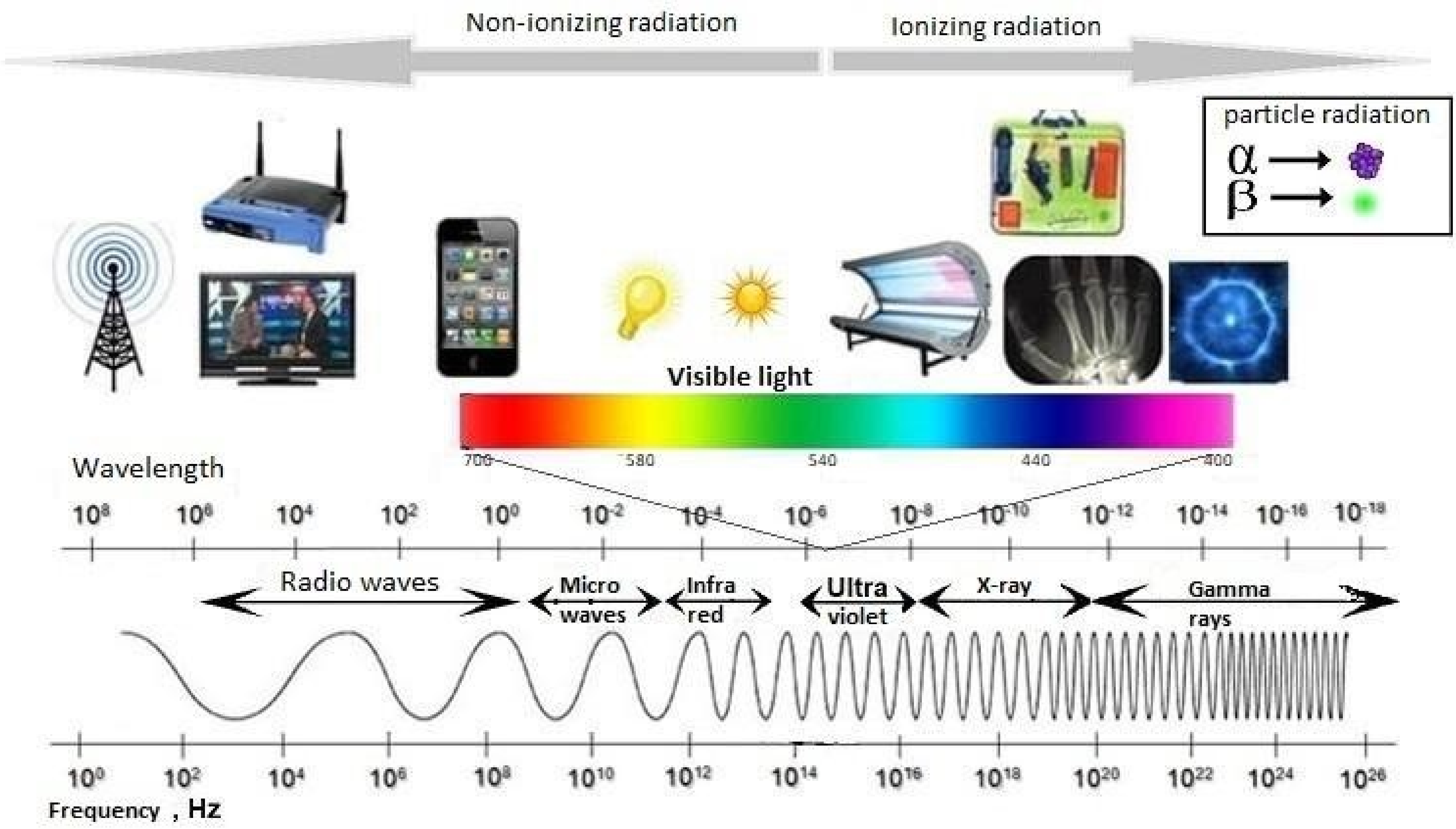
- What are the fundamentals of how the Internet is built that determine how we do confidentiality, integrity, and availability?
  - Or, what do rainbows have to do with network security?



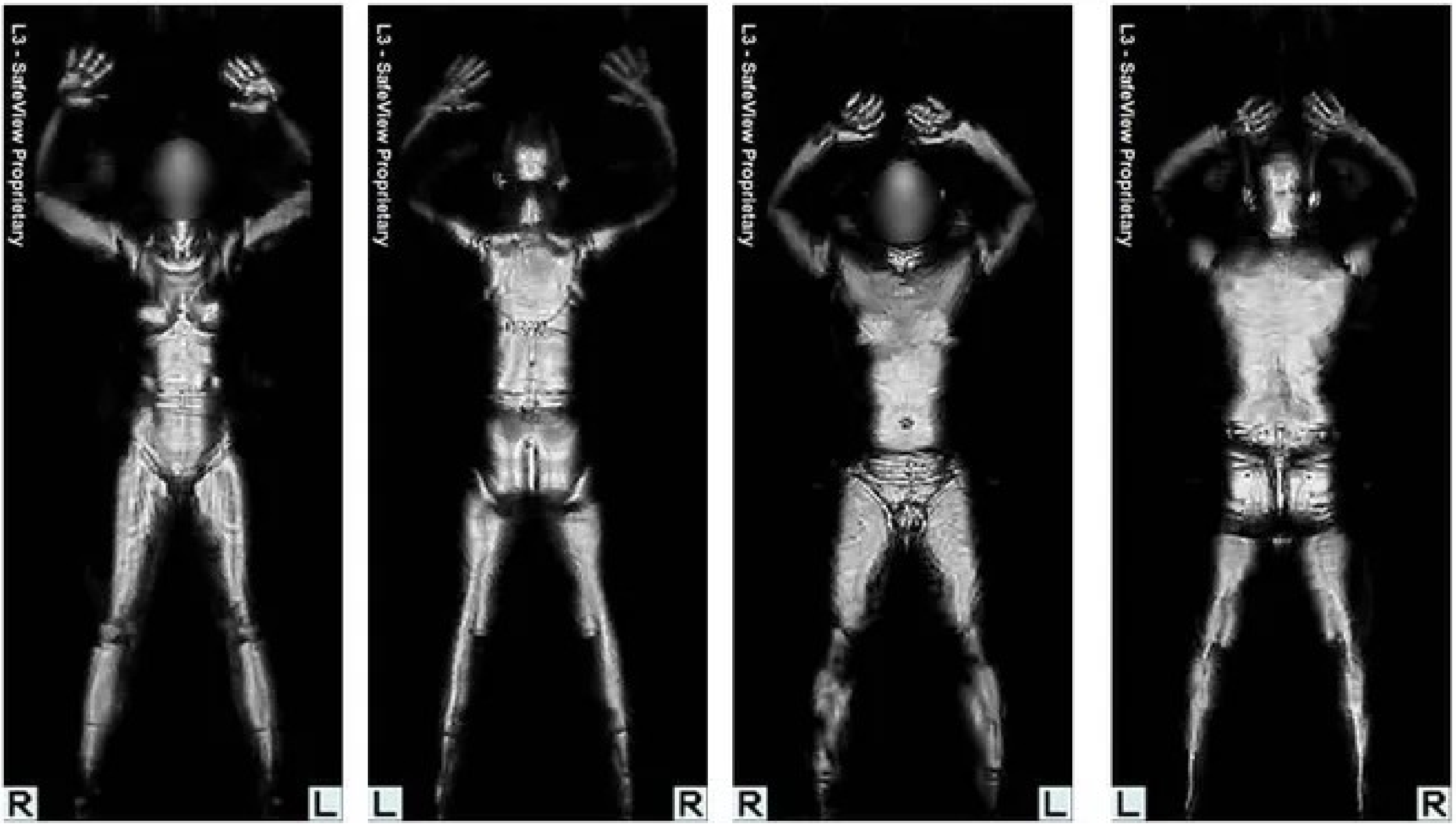
Warmth

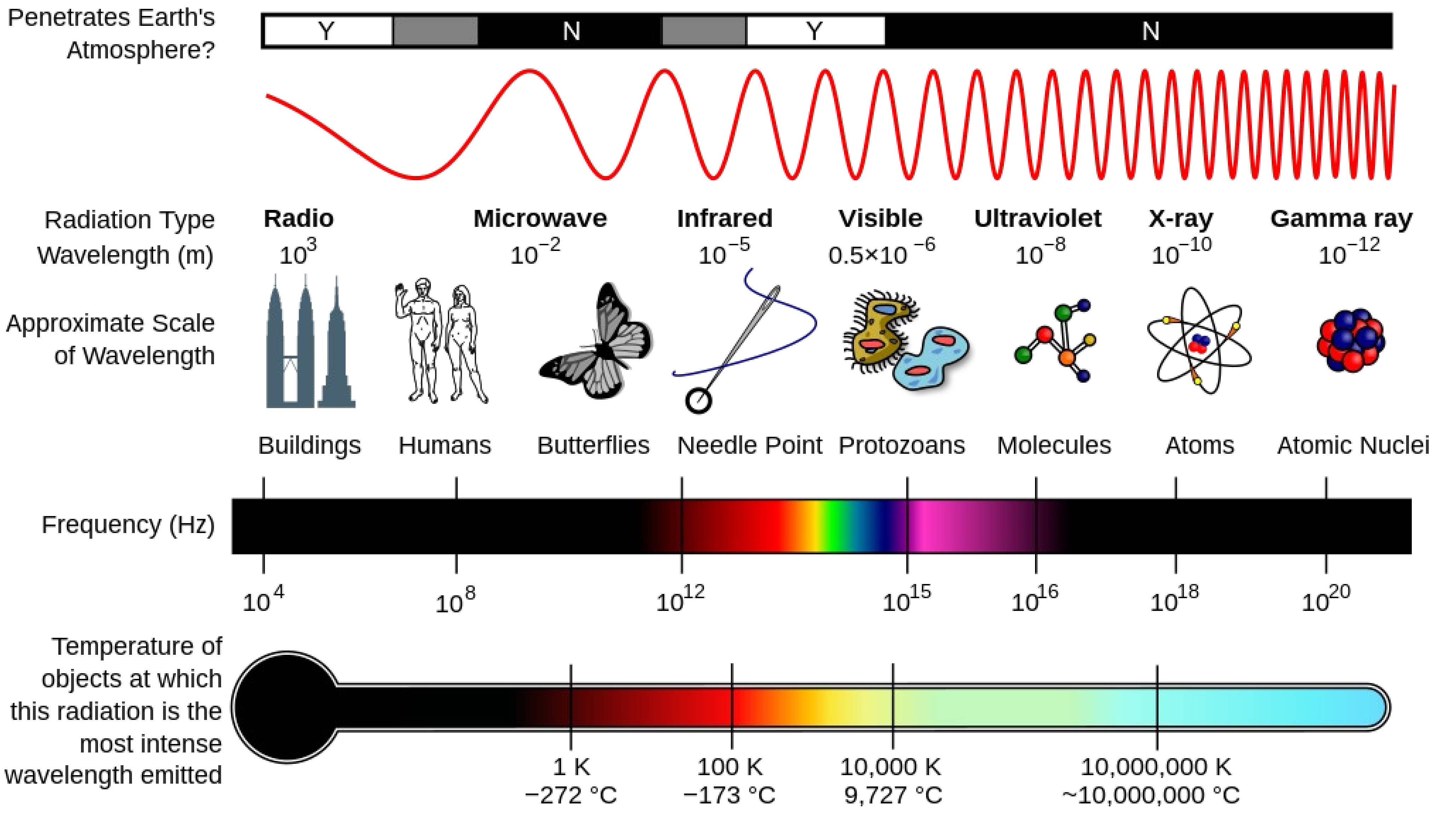
Sunburns

The electromagnetic spectrum

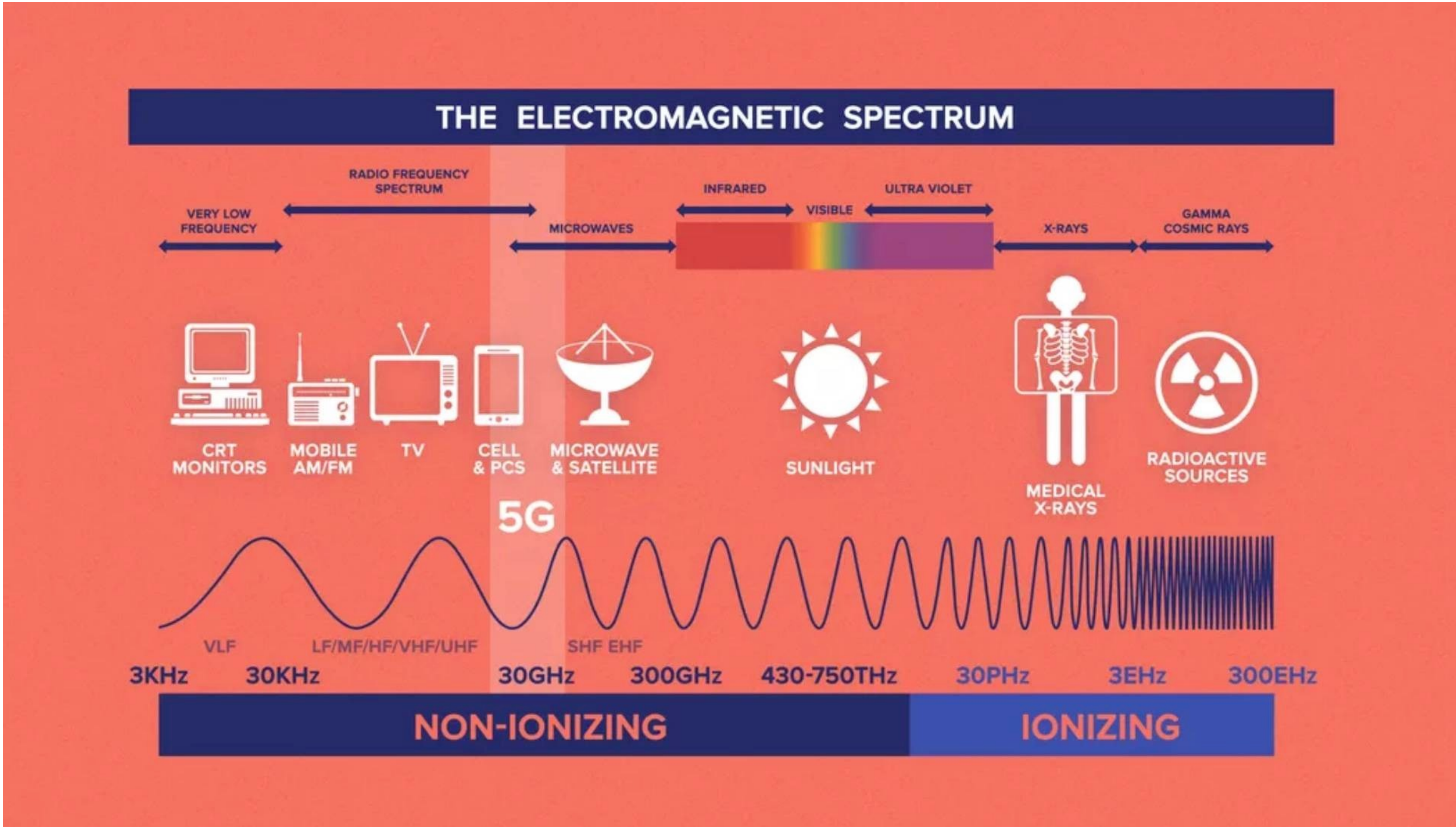


https://www.uib.no/en/hms-portalen/75292/electromagnetic-spectrum https://www.usatoday.com/story/travel/roadwarriorvoices/2015/08/17/tsa-has-spent-160-million-on-body-scanners-and-theyre-still-terrible/83288622/


L3 - SafeView Proprietary
R
L
L3 - SafeView Proprietary
L
R
L3 - SafeView Proprietary
R
L
L3 - SafeView Proprietary
L
R



https://commons.wikimedia.org/wiki/File:EM_Spectrum_Properties_edit.svg



https://www.islandssounder.com/news/part-i-the-hype-about-5g/

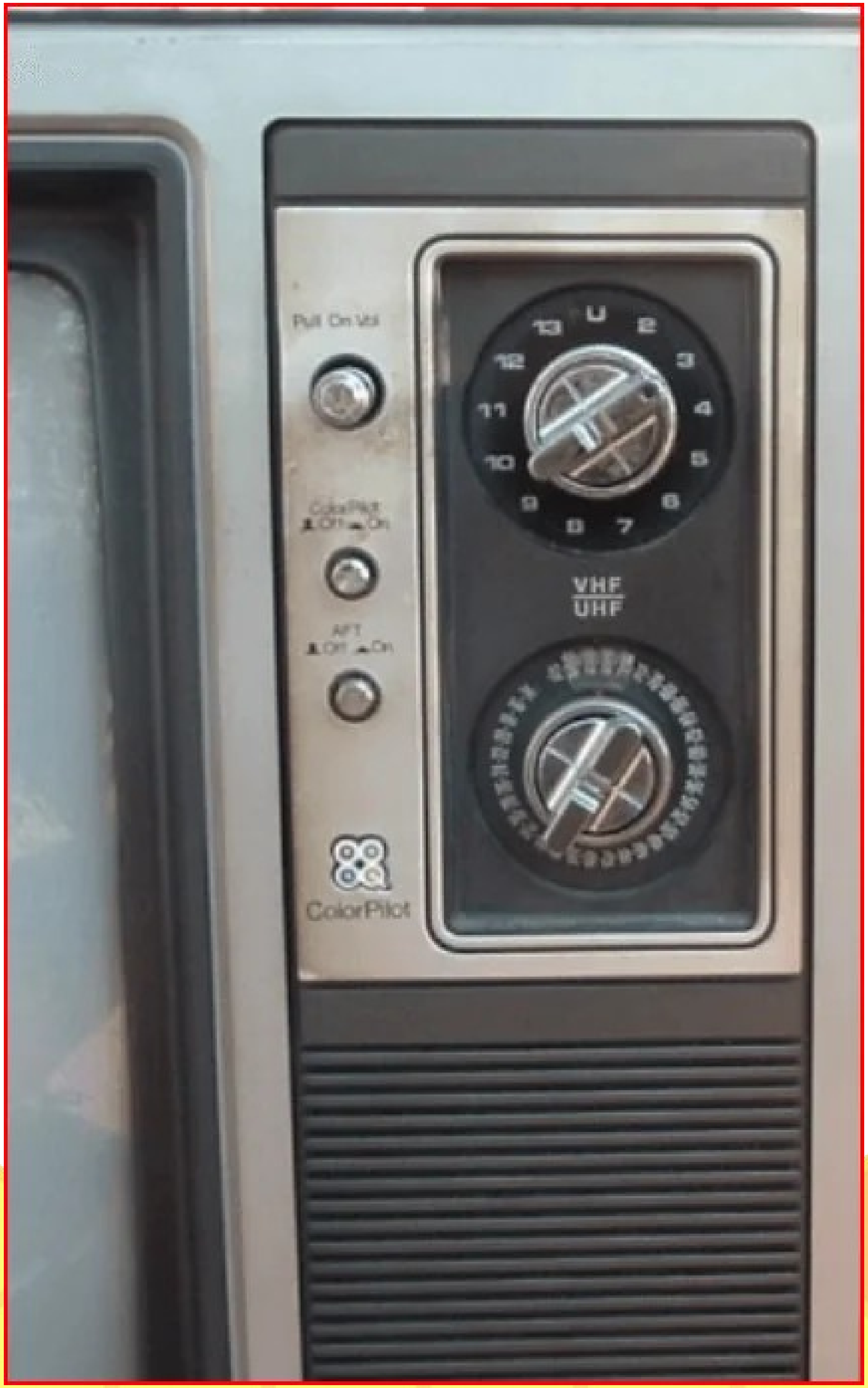
Doctors at the X-Ray be like: "This is completely safe, don't worry"

Also doctors at the X-Ray:

Microwaves

- EHF (Sir Jagadish Chandra Bose – Bengali scientist) 30 to 300GHz
  - Point-to-point, satellite, IEEE 802.11ay (20 Gbps), security screening at the airport, 5G
- SHF – 3 to 30 GHz
  - Point-to-point, radar, satellite phones, microwave ovens, 5G
- UHF – 300 MHz to 3 GHz
  - TV, cell phones, satellites, GPS, WiFi, Bluetooth, walkie talkies, garage door openers, industrial controllers

https://www.reddit.com/r/nostalgia/comments/ut3emp/80s_tv_knobs_bonus_points_for_describing_the_feel/



Radio waves

- VHF – 30MHz to 300MHz
  - Line of sight, but refracted up to 100 miles or so
  - FM radio, TV, amateur radio
- HF – 3MHz to 30MHz
  - Reflected off the ionosphere
  - Military, amateur radio, maritime, CB radio
- MF – 300KHz to 3 MHz
  - AM radio, maritime

As you go lower than 300 KHz...

- Weather, beacons, time, radio in other parts of the world, RFID, submarine communications

I’m not an expert in psychology or marketing, but I think it’s safe to assume...

- Humans don’t like to be fried alive
- Humans don’t like their devices to have wires

In general, for practical CSE 548 purposes...

- Higher frequencies carry more information
  - We’ll touch on information theory later in the semester
- Infrared and visible light cannot pass through objects (like walls)
  - Microwaves and radio waves can, basically
- Everything at a higher frequency than visible light is bad for us

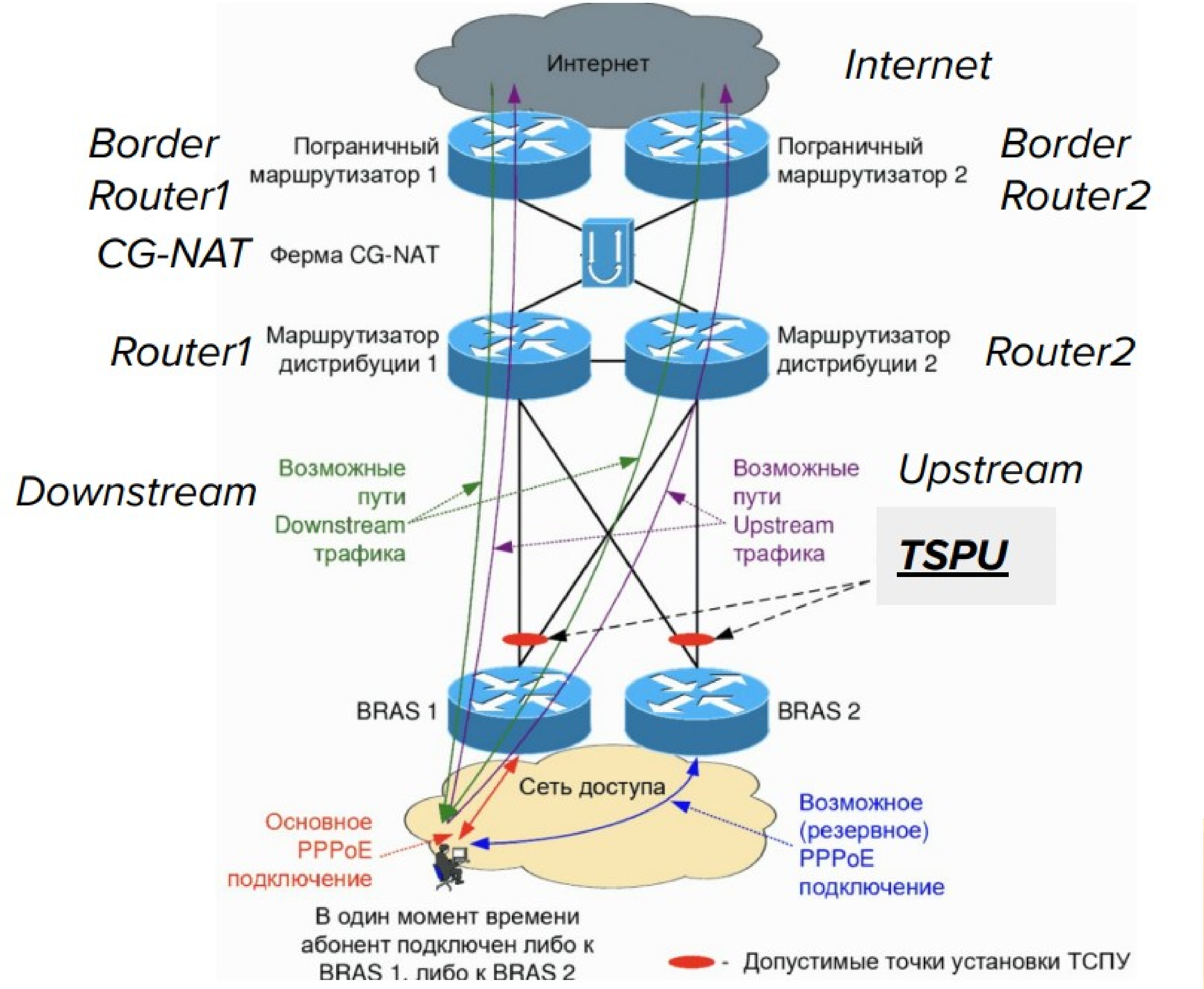
Because of these reasons...

- The backbone of the Internet and servers are wired
  - Specifically, fiber optics (180 THz to 330 THz)
  - Need blessings from governments to bury the wires
    - Confidentiality: Light is ***easy*** to copy
    - Integrity: Light is ***hard*** to change in transit
    - Availability: Censorship, throttling, and shutdowns

Because of these reasons...

- The other (not servers) edges of the network (*i.e.*, people and their devices) are increasingly wireless
  - Need blessing from governments to use broadcast frequencies
    - Easy to find a high-powered transmission (see *Pump up the Volume*)
  - Attackers can ***easily*** receive and transmit at any frequency
    - Governments (*e.g.*, local law enforcement), stalkers, cartels, human traffickers, financially motivated attackers, nosy neighbors, *etc.*
    - Eavesdropping (C), spoofing (I), jamming (A)

Still electric paths between the edges and the backbone


Интернет
Internet
Border Router1
Пограничный маршрутизатор 1
Пограничный маршрутизатор 2
Border Router2
CG-NAT
Ферма CG-NAT
Router1
Маршрутизатор дистрибуции 1
Маршрутизатор дистрибуции 2
Router2
Downstream
Возможные пути Downstream трафика
Возможные пути Upstream трафика
Upstream
TSPU
BRAS 1
BRAS 2
Сеть доступа
Основное PPPoE подключение
Возможное (резервное) PPPoE подключение
В один момент времени абонент подключен либо к BRAS 1, либо к BRAS 2
- Допустимые точки установки ТСПУ

Because of these reasons...

- Residential and mobile networks are a great place for information controls
  - Close to users
    - Less delay
    - No Network Address Translation (NAT) to create ambiguity about *who* sent a packet
  - Need blessing from governments to
  - Attackers can ***easily*** view and modify packets

We need cryptography

- Make your messages sent and received over the Internet unreadable to eavesdroppers **(confidentiality)**
  - Hide metadata about who you’re talking to and what you’re doing to evade censorship **(availability)**
- Make sure your messages sent and received over the Internet are not modified **(integrity)**

Crypto is more than “CIA”

- Non-repudiability
- Perfect forward secrecy
- Backward secrecy (*a.k.a.* future secrecy)
- Deniable encryption
- ...

Alternatives to crypto

- Code division multiple access (CDMA)
  - Invented (in the U.S., at least) by Hedy Lamarr (basically)
- Information theory, randomized algorithms, *etc.*
  - Currently not practical in terms of solving all our problems
- Line-of-sight, directional antennae
  - Not entirely practical for security reasons, but increasingly common for other reasons
  - Line of sight attacker (*e.g.*, drone or in the Internet backbone)

This semester

- Studying PCAPs to understand…
  - ***Why*** things (*e.g.*, header fields and payloads) are encrypted/obfuscated the way they are
  - ***Why*** everything is about to change
  - ***Why*** deep packet inspection (DPI) is not straightforward
- Because we care about fundamentals, *i.e.*, the ***"why"*** part, we won't be able to avoid…
  - Computational complexity, abstract algebra, quantum physics, relativity, classical physics...

OSI model

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

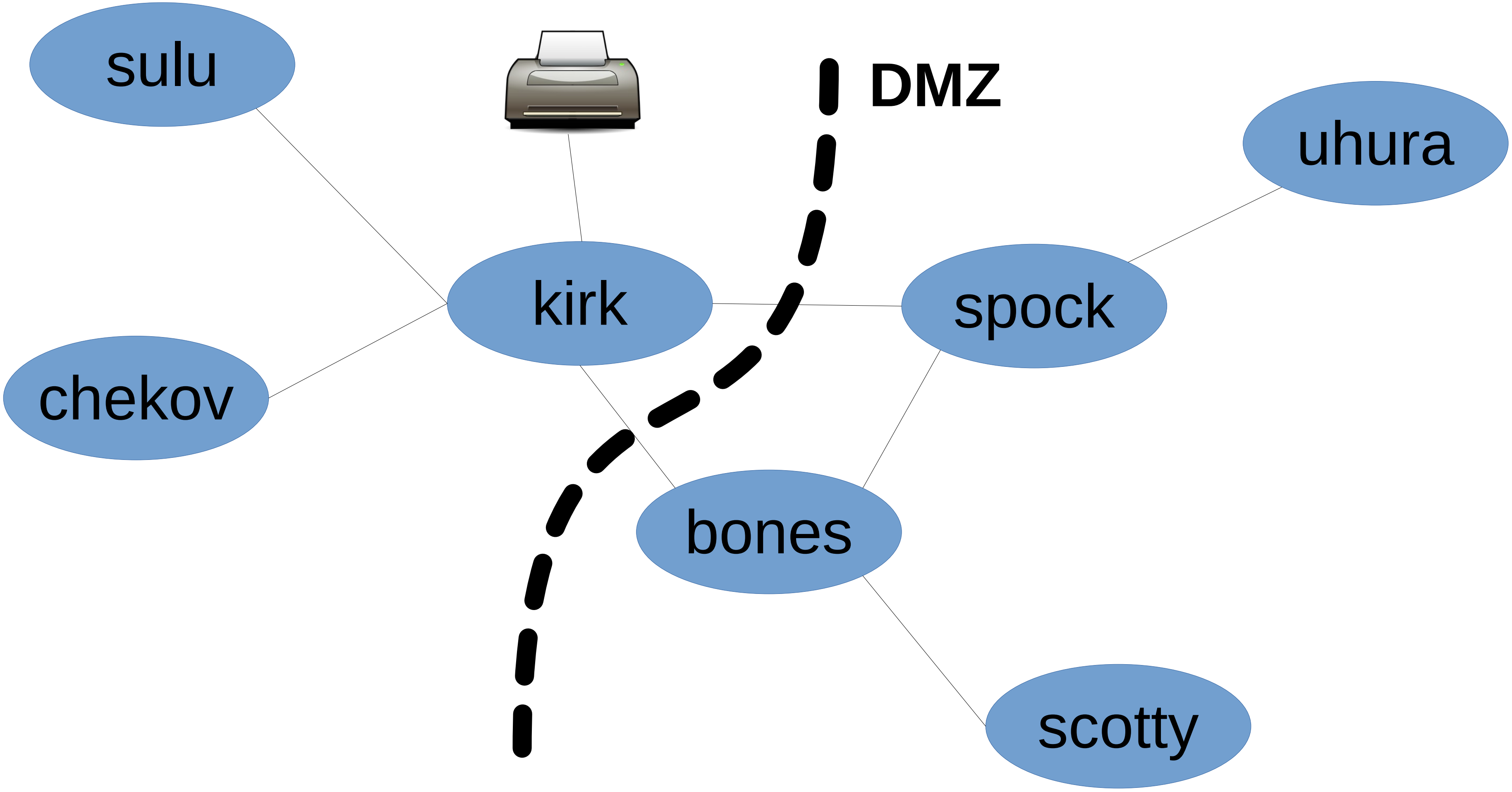
Why do we need crypto?

- Application layer (think banking): Confidentiality, Integrity, Authentication, Non-Repudiation
- Application layer (think off-the-record): Confidentiality, Integrity, Authentication with repudiation, perfect forward secrecy
- Routing layer (think VPNs or IPSec): Confidentiality, Integrity, Authentication, perfect forward secrecy
- Physical and link layer (think WiFi): Confidentiality, Integrity, Authentication, perfect forward secrecy

Network Adjacency

- Do two machines interact below layer 3?
- If they interact in layer 1, one can record the traffic of the other
- If they interact in layer 2, one can perform machine-in-the-middle on the other
- First goal of an attack on a network is usually to land on the network using a soft target
  - Because of network adjacency or DMZ

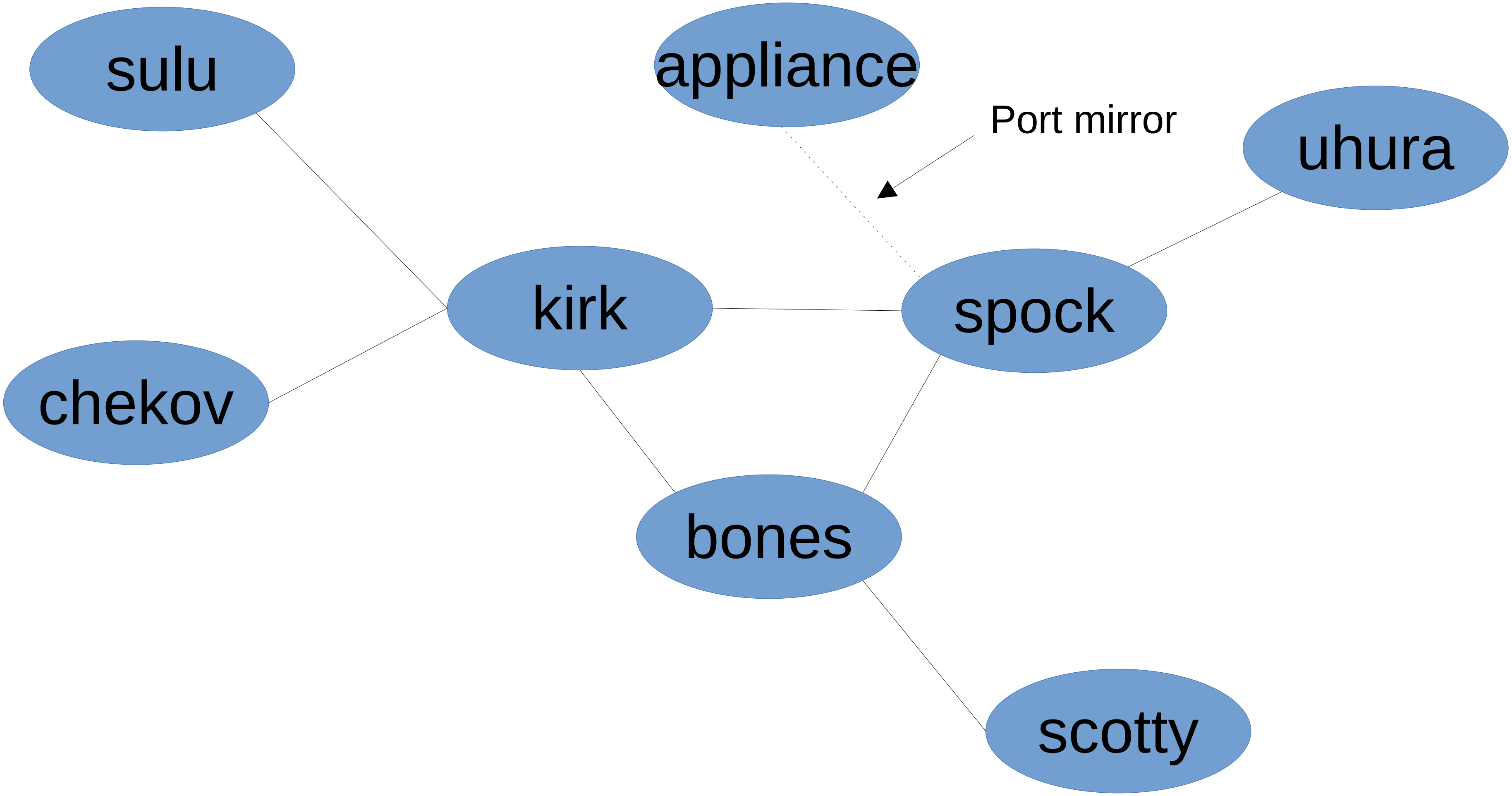
DMZ example



How to get network adjacent or inside the DMZ

- Physically (*e.g.*, a rubber ducky)
  - Sometimes physical access for potential attackers is authorized, like a university WiFi
- Remote exploit
- Compelled by law (think Russia’s TSPU)
- Phishing, water hole attacks, bribery, *etc.*
- Submarines, radio equipment, *etc.*

Uhura talking to Sulu



In- *vs.* On- *vs.* Off-path

- Kirk and Spock are in-path
  - Also called machine-in-the-middle
  - Chekov or other attackers network adjacent to Sulu or Uhura can put themselves in-path with layer 2 attacks
- Appliance is on-path (gets a copy of packets)
  - Also called machine-on-the-side
  - Any attacker with physical access anywhere in the network is on-path

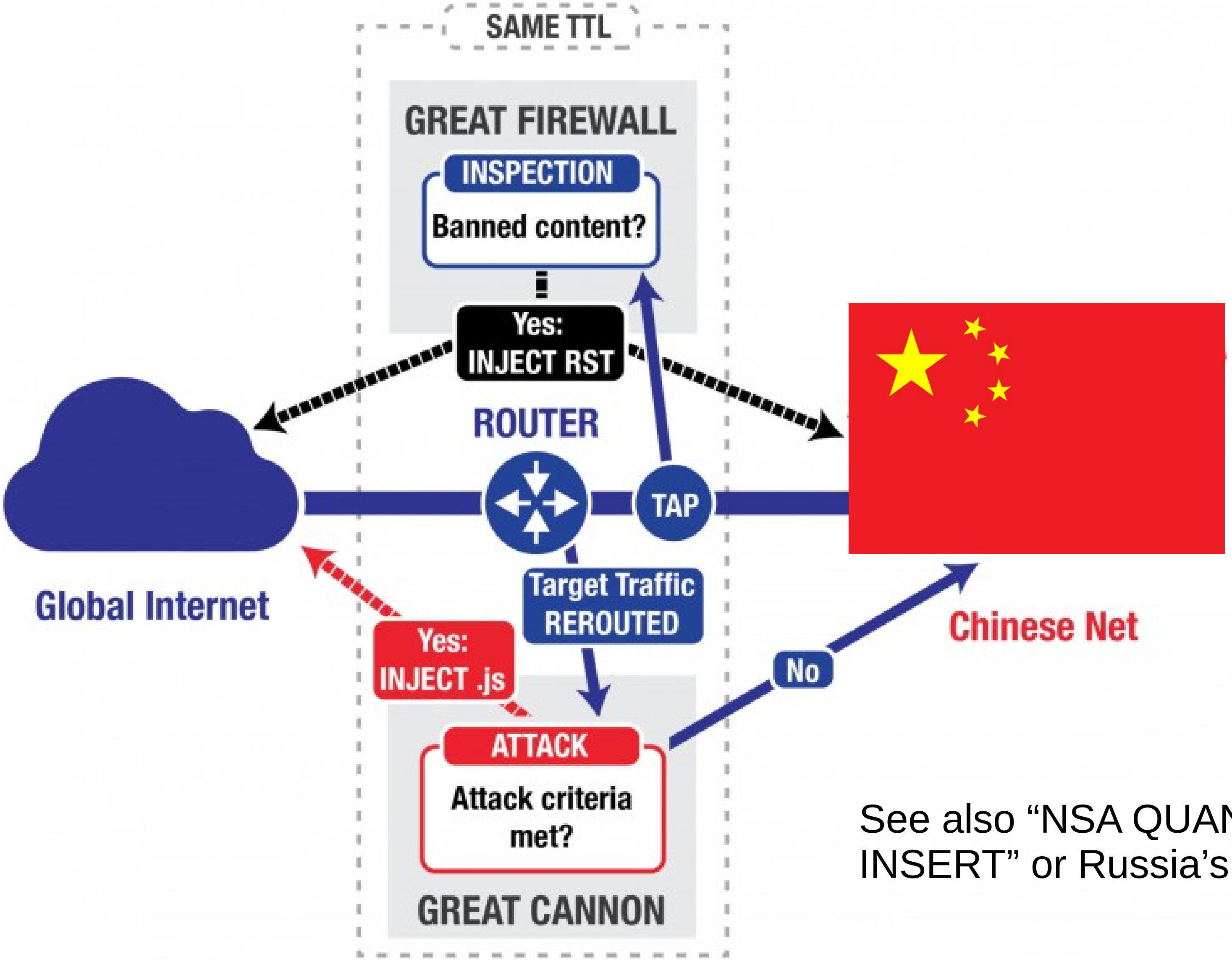
In- *vs.* On- *vs.* Off-path (continued)

- Bones and Scotty are off-path
  - Can put themselves in-path with attacks on application layer protocols that change the routing layer, like BGP or DNS
    - *E.g.*, BGP prefix attack or DNS cache poisoning (network adjacent or blind)
  - Can execute so-called “blind” attacks
    - *E.g.*, IP fragmentation attack on Domain Validation

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 “NSA QUANTUM INSERT” or Russia’s TSPU

Off-path attacks

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

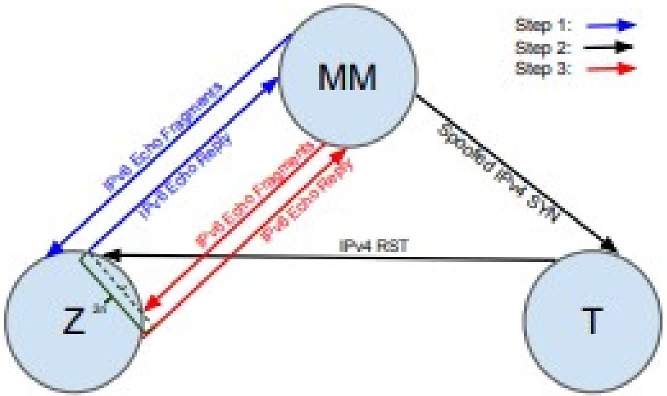


Fig. 4. Scan of a closed port with a dual stack zombie using ONIS.

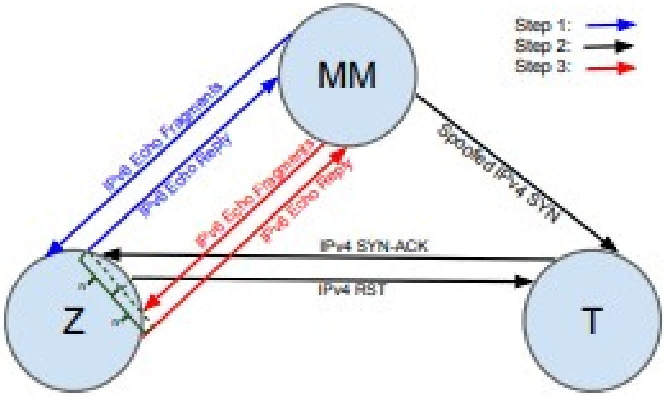
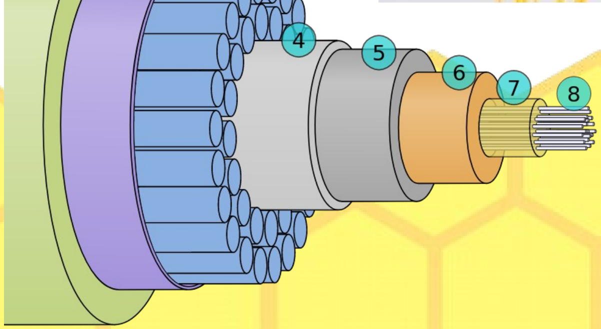


Fig. 5. Scan of an open port with a dual stack zombie using ONIS.

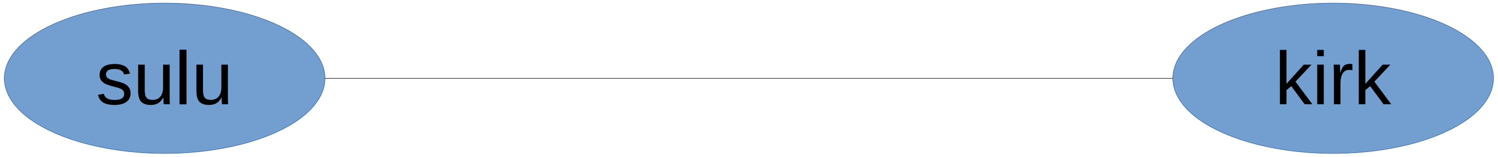
Internet in a nutshell...

You want to connect two machines...

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

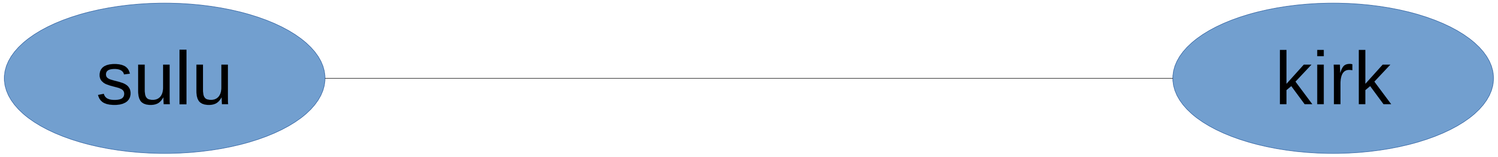


A “hop”

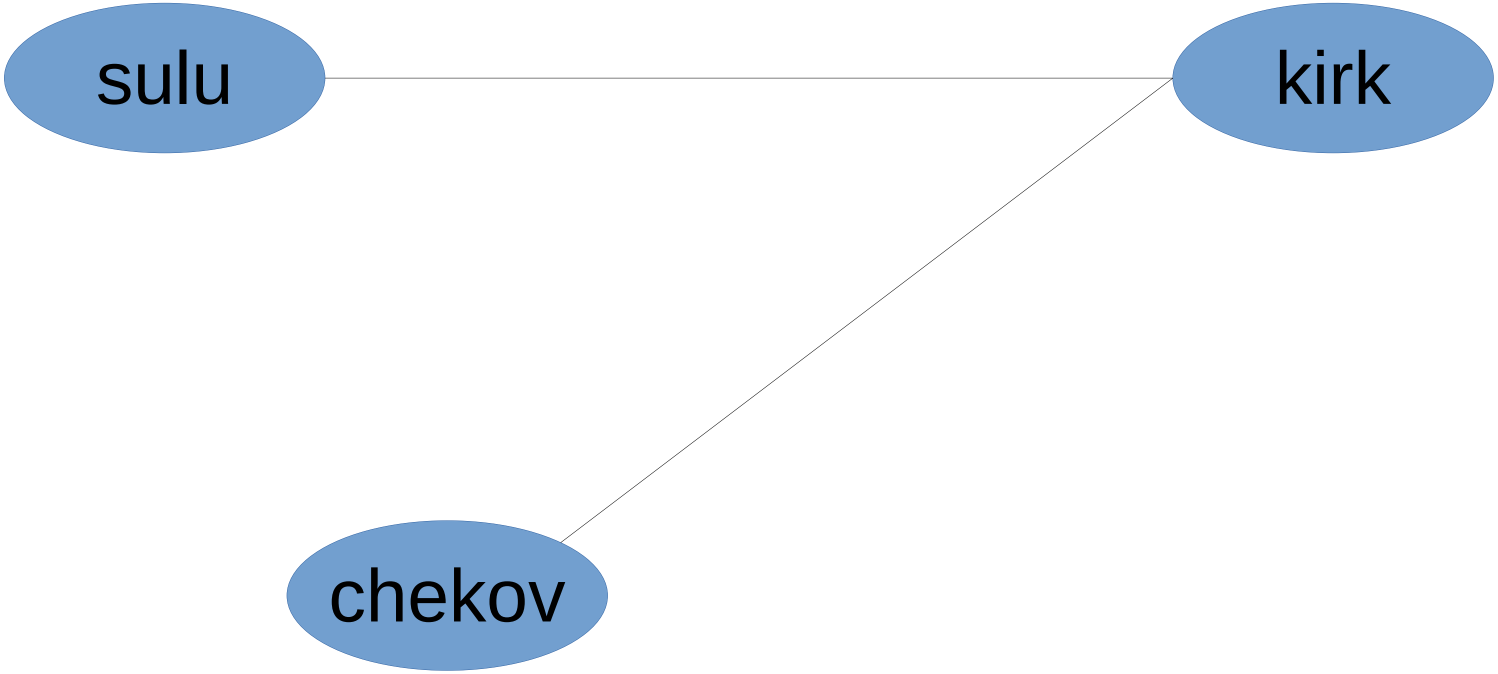


A “hop”

Ethernet

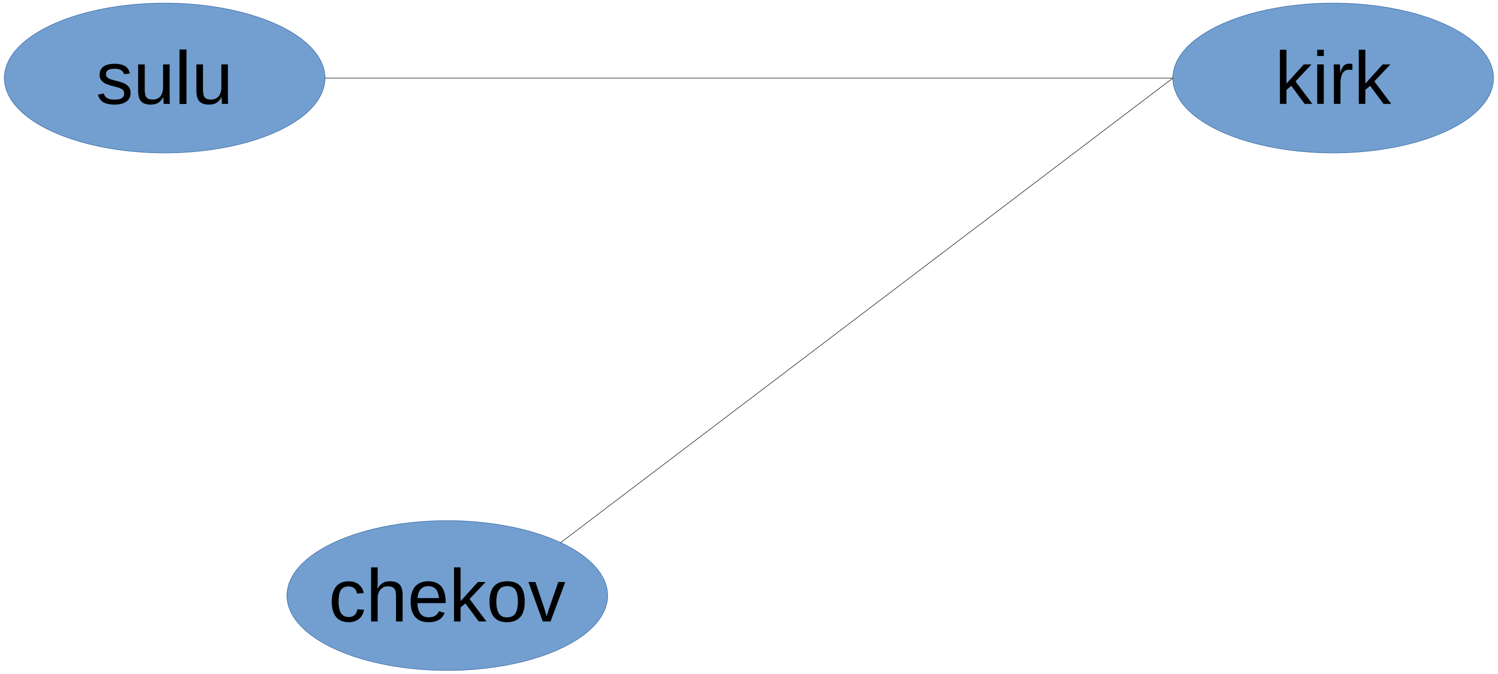


A “subnet”

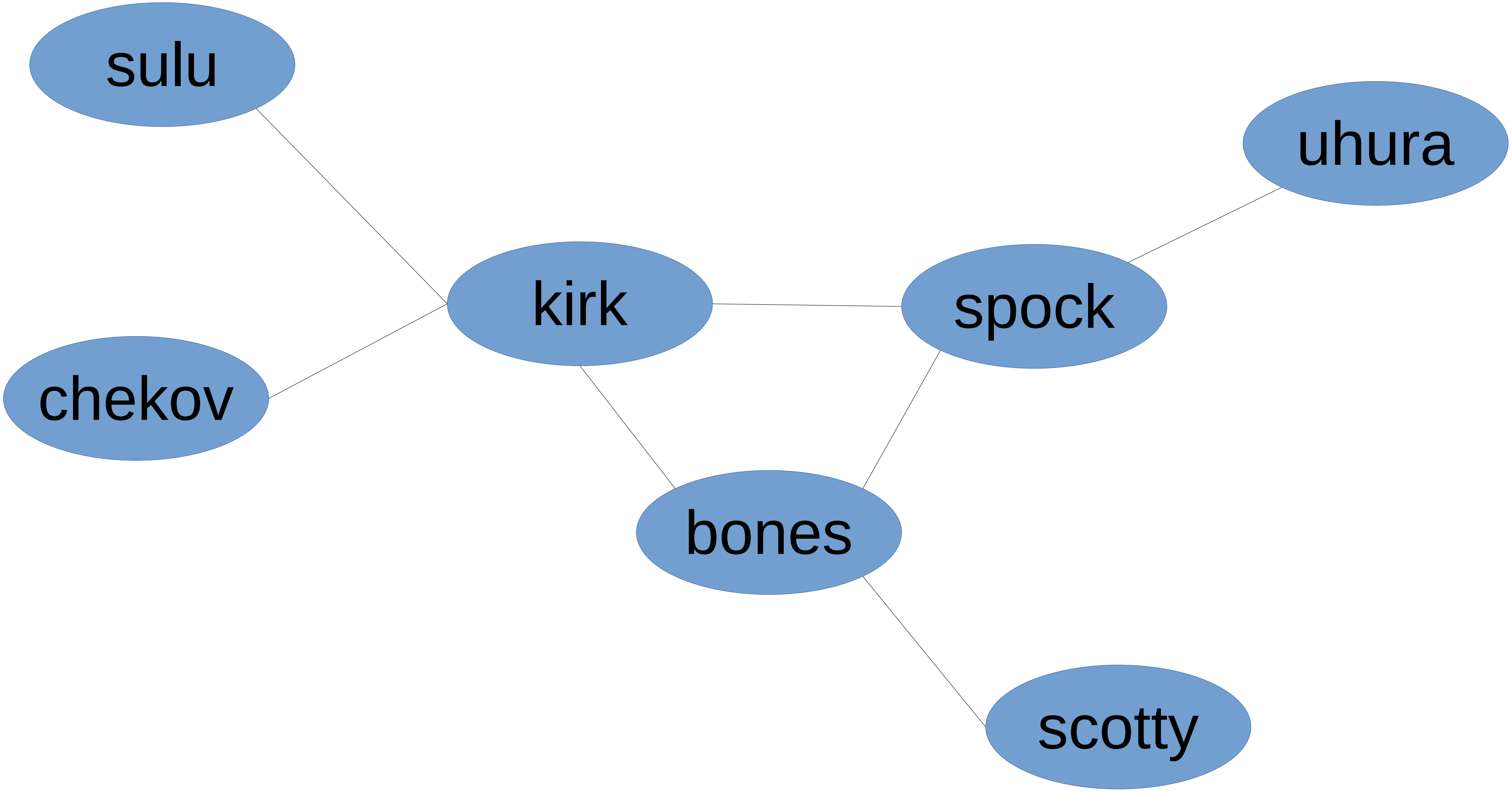


A “subnet”

ARP = Address Resolution Protocol



A network with routers



More terminology

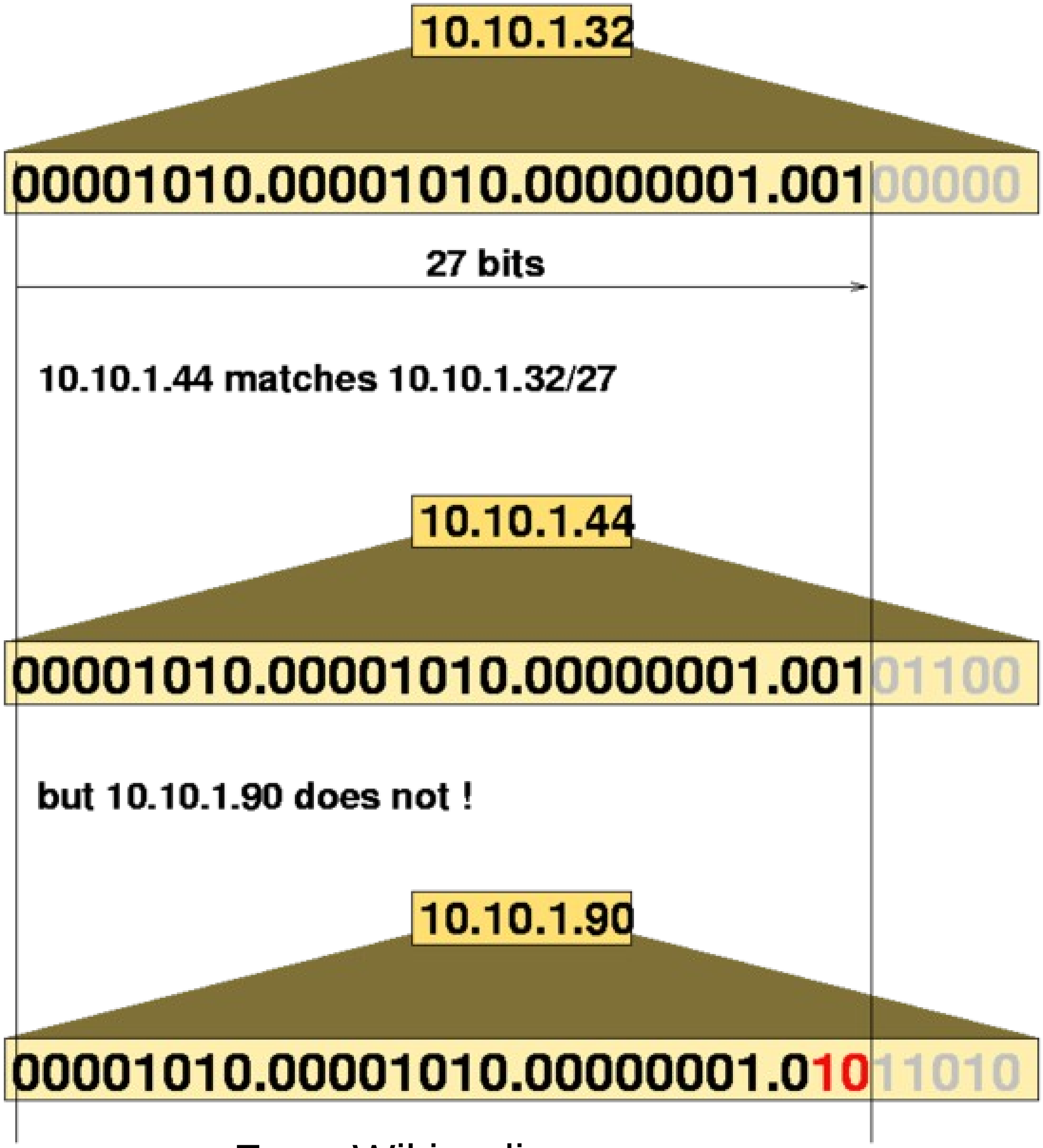
- IP = Internet protocol
- Forwarding, or “routing”
  - How packets get across the network
- Interface
  - WiFi, cellular, ...
- Path (or “route”), reverse path

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



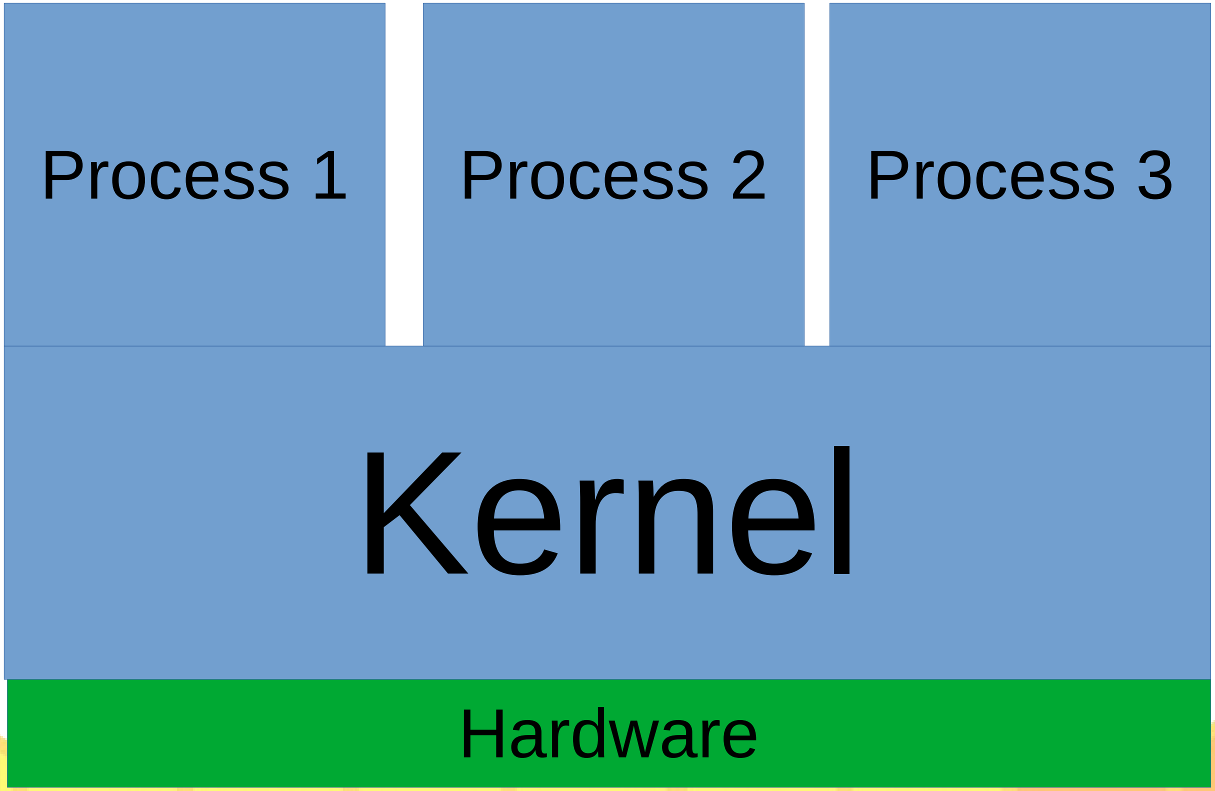
From Wikipedia

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?

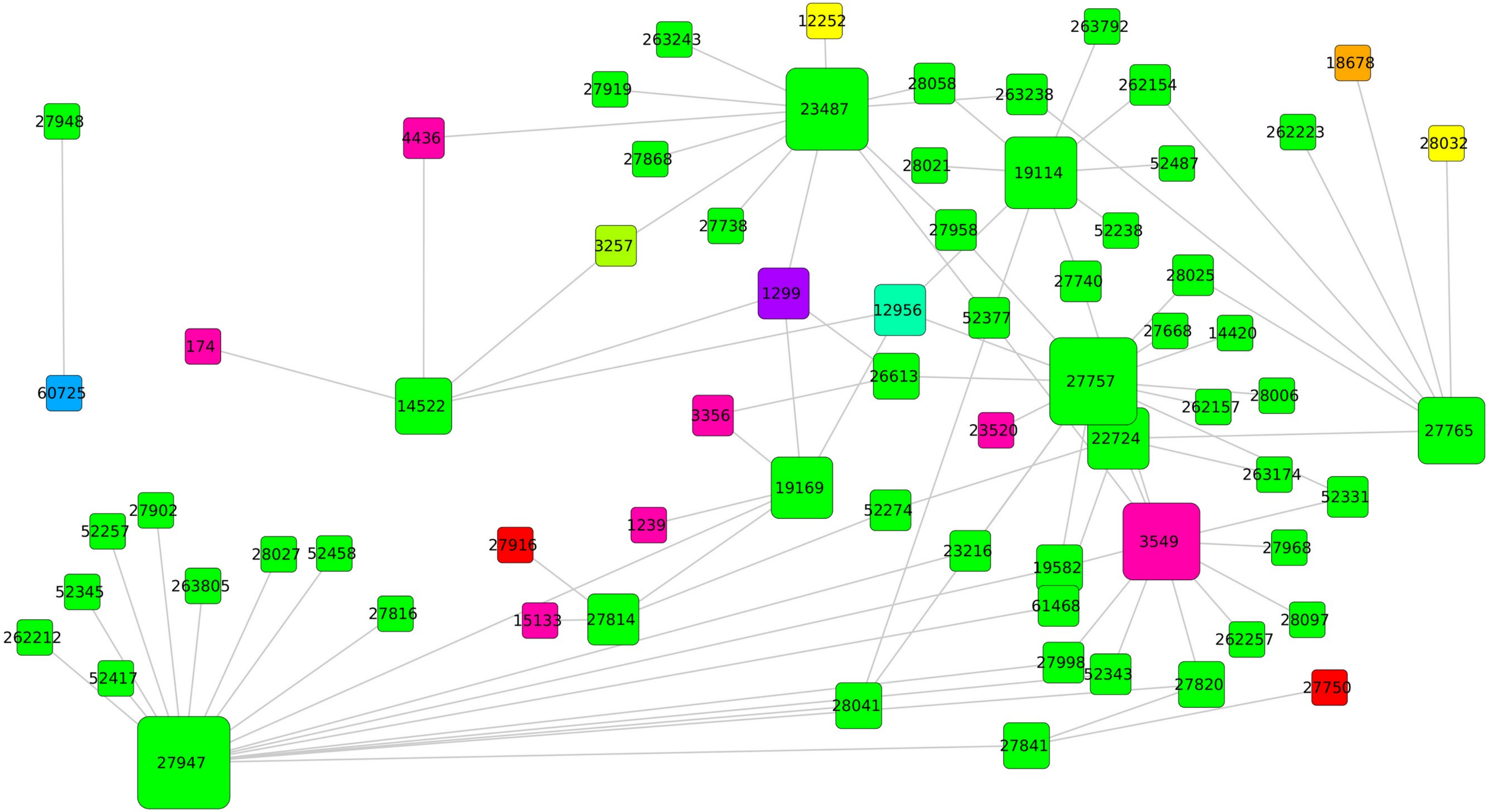
Separated by virtual memory, access system resources *via* system calls.

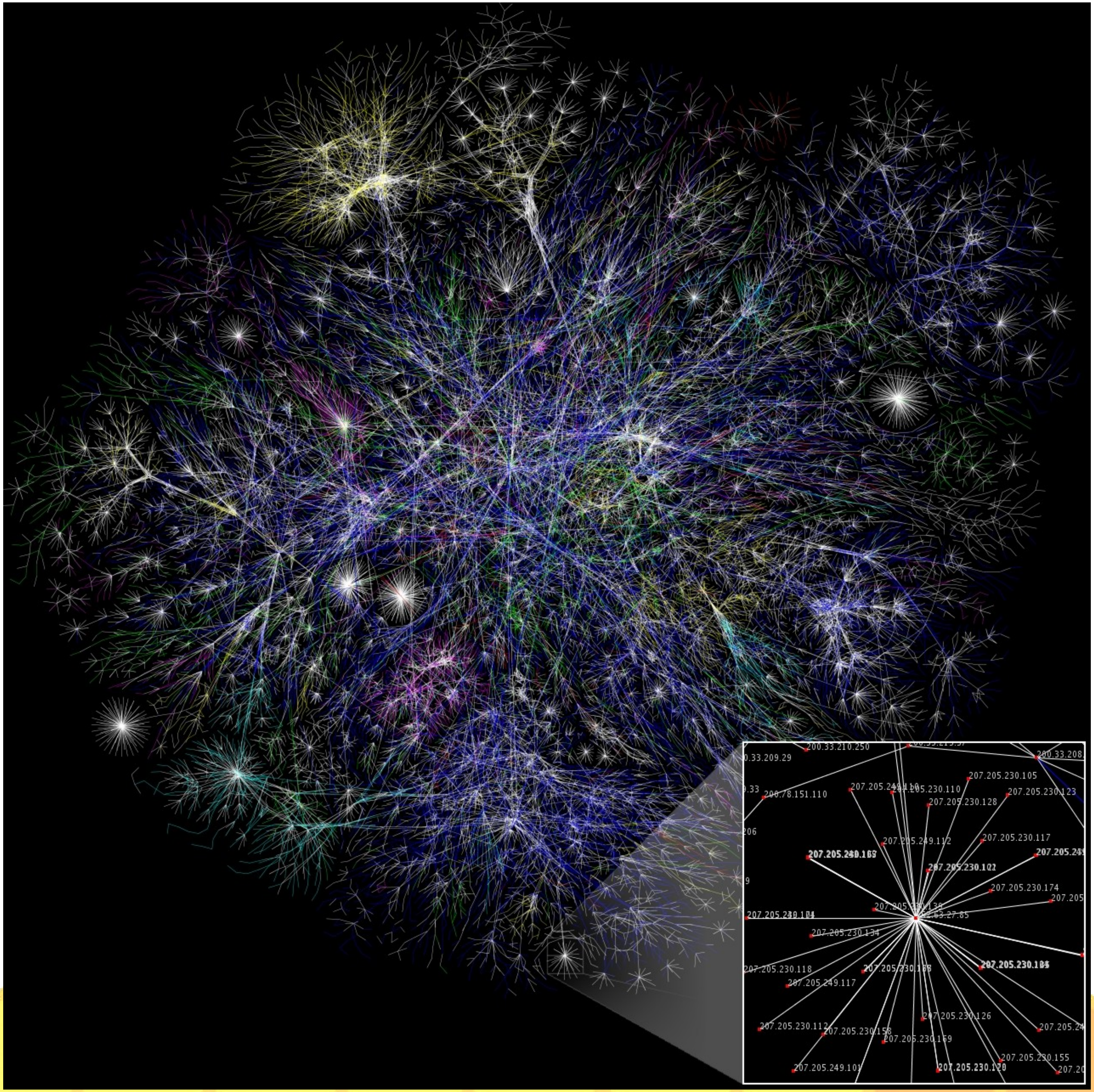


Almost there…

- 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.
0.33
200.78.151.110
207.205.230.105
207.205.230.110
207.205.230.123
207.205.230.128
206
207.205.249.112
207.205.230.117
207.205.24
9
207.205.230.174
207.205
207.205.230.139
.63.27.85
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

Thinking holistically

- Processes exist somewhere on the network
- Processes communicate
- Processes have privileges
  - Local machine
  - Network
- Routers have processes, too

Attacker high-level goals

- Eavesdrop on network communications between processes
- Modify or disrupt network communications between processes
- Control a remote process
  - Access to their local network, files, *etc.*

Attacker intermediate goals

- Go from on-path to in-path
- Go from off-path to in-path
- Go from off-path to on-path

Attacker high-level goals

Surveillance DPI

- Eavesdrop on network communications between processes

Crypto WiFi cracking

Rogue certificates Crypto

- Modify or disrupt network communications between processes

machine-in-the-middle throttling

Censorship evasion Censorship Blind attacks

- Control a remote process

Remote exploits

  - Access to their local network, files, *etc.*

phishing nmap MetaSploit Drive-by download attacks

Vulnerability scanners firewalls NIDS

NIDS evasion

Attacker intermediate goals

MAC authentication

- Go from on-path to in-path

ARP cache poisoning

DoH

DNS cache poisoning

- Go from off-path to in-path

BGP prefix attacks

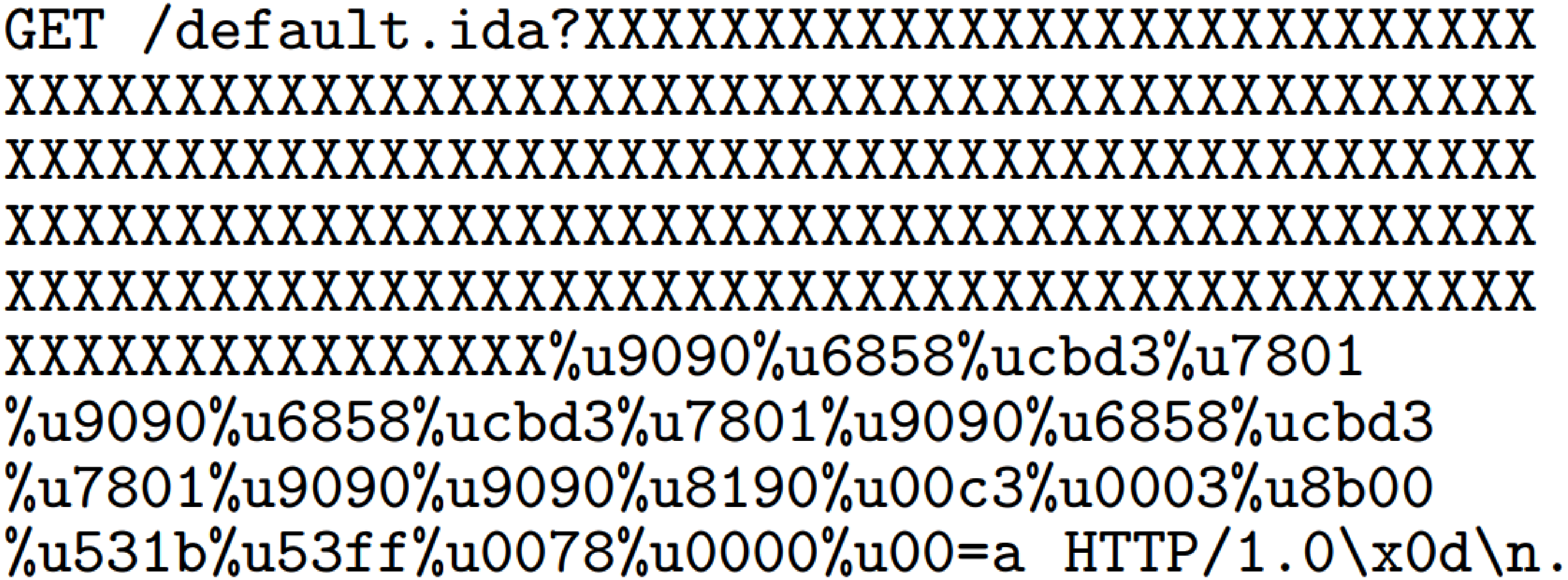
randomized ports

- Go from off-path to on-path

Crypto

physical 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.
```

“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*)