CSE 468 Course Intro

Computer Network Security

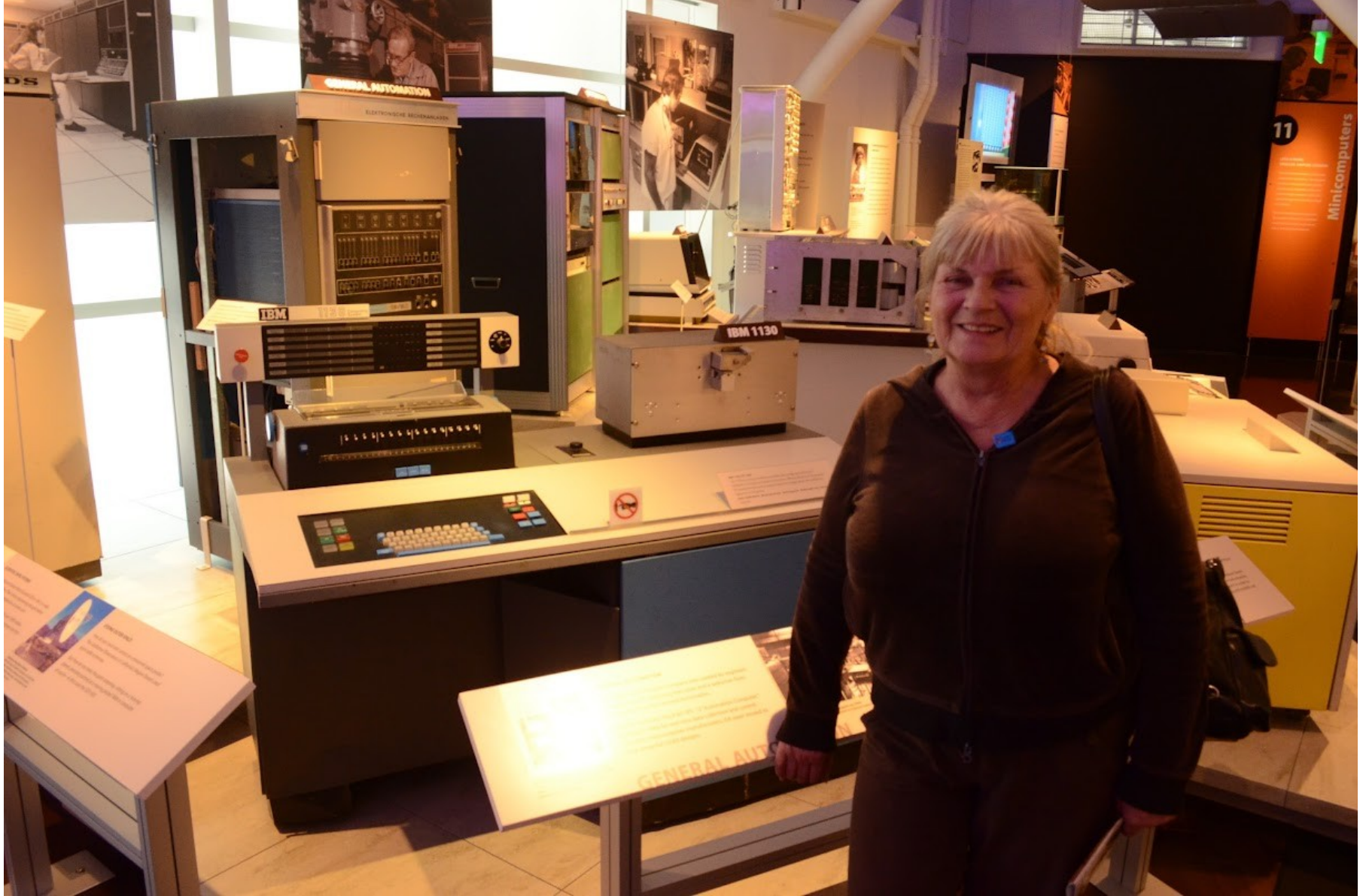
Jed Crandall
jedimaestro@asu.edu

Syllabus in a nutshell

- Attendance not recorded
- Midterm and final are in-person
- Check both Canvas and the course website

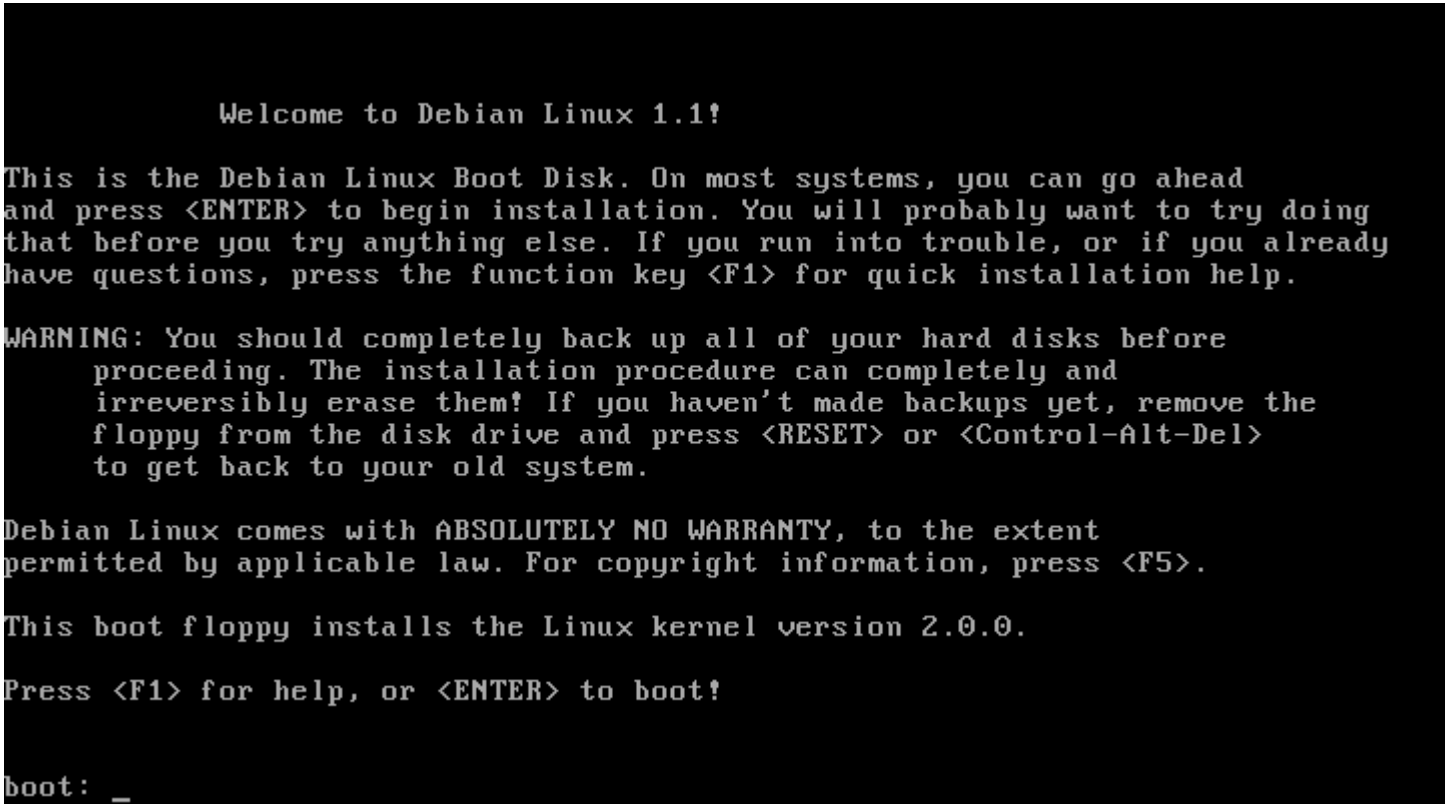
A bit about me…

- Associate Professor, SCAI *and* Biodesign Center for Biocomputation, Security, and Society
- Research is about Internet Freedom, including:
  - Internet censorship and censorship evasion
  - Machine-in-the-middle attacks, adversarial networking
  - Privacy, forensics, and a few other things


IBM
IBM 1130
11
Minicomputers


IBM
1130
IBM
GENERAL AUTOMATION
Not every minicomputer company was created by engineers
jumping ship. A marketing executive and a sales
Honeywell founded General A

https://commons.wikimedia.org/wiki/File:Apple_II_typical_configuration_1977.png

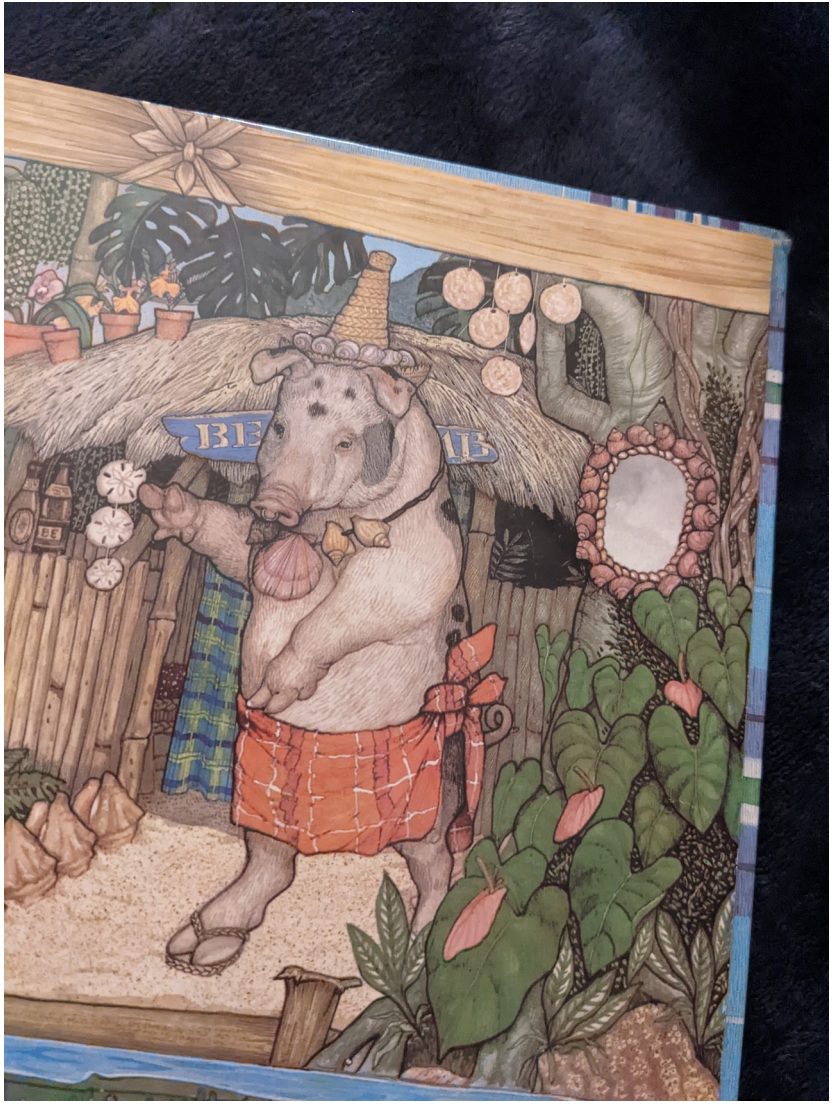


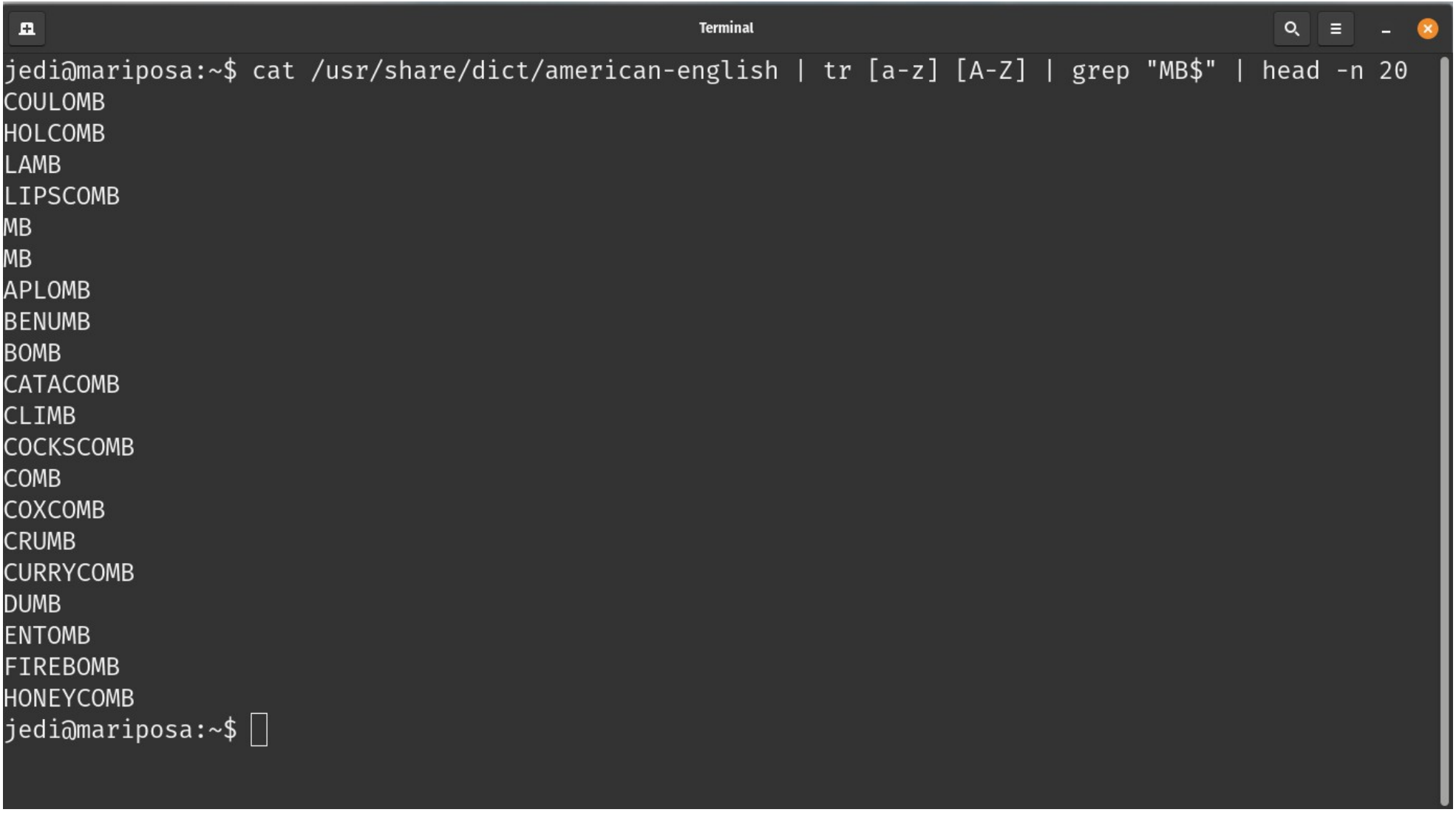
https://archive.org/details/debian_1.1

UNIX, C, and the Internet...

- UNIX was developed to run on anything
  - Bell Labs, 1969 (Thompson and Ritchie)
  - Contrast with TOPS10
- C provides direct access to hardware, virtually no runtime environment
  - Bell Labs, 1972-1973 (Ritchie)
  - Contrast with COBOL

UNIX example...




Terminal
jedi@mariposa:~$ cat /usr/share/dict/american-english | tr [a-z] [A-Z] | grep "MB$" | head -n 20
COULOMB
HOLCOMB
LAMB
LIPSCOMB
MB
MB
APLOMB
BENUMB
BOMB
CATACOMB
CLIMB
COCKSCOMB
COMB
COXCOMB
CRUMB
CURRYCOMB
DUMB
ENTOMB
FIREBOMB
HONEYCOMB
jedi@mariposa:~$

TOPS10 example...

A TOPS-10 command primer

But

```
C:\> mkdir foo
C:\> cd foo
C:\FOO> dir
```

becomes:

```
.r credir
Create directory: [,,foo]
  Created DSKC0:[42,42,
FOO].SFD/PROTECTION:775
Create directory: ^Z

.r setsrc
*cp [,,foo]
*^Z
EXIT
.dir
%WLDDEM Directory is empty
```

https://www.slideshare.net/bhlarsen/the-pdp-10-and-me

https://commons.wikimedia.org/wiki/File:DECSystem10-KI10.JPG

https://commons.wikimedia.org/wiki/File:CP%E2%81%84M_Ad,_InfoWorld,_November_29,_1982.jpg


MICROSOFT
MICROSOFT
MICROSOFT

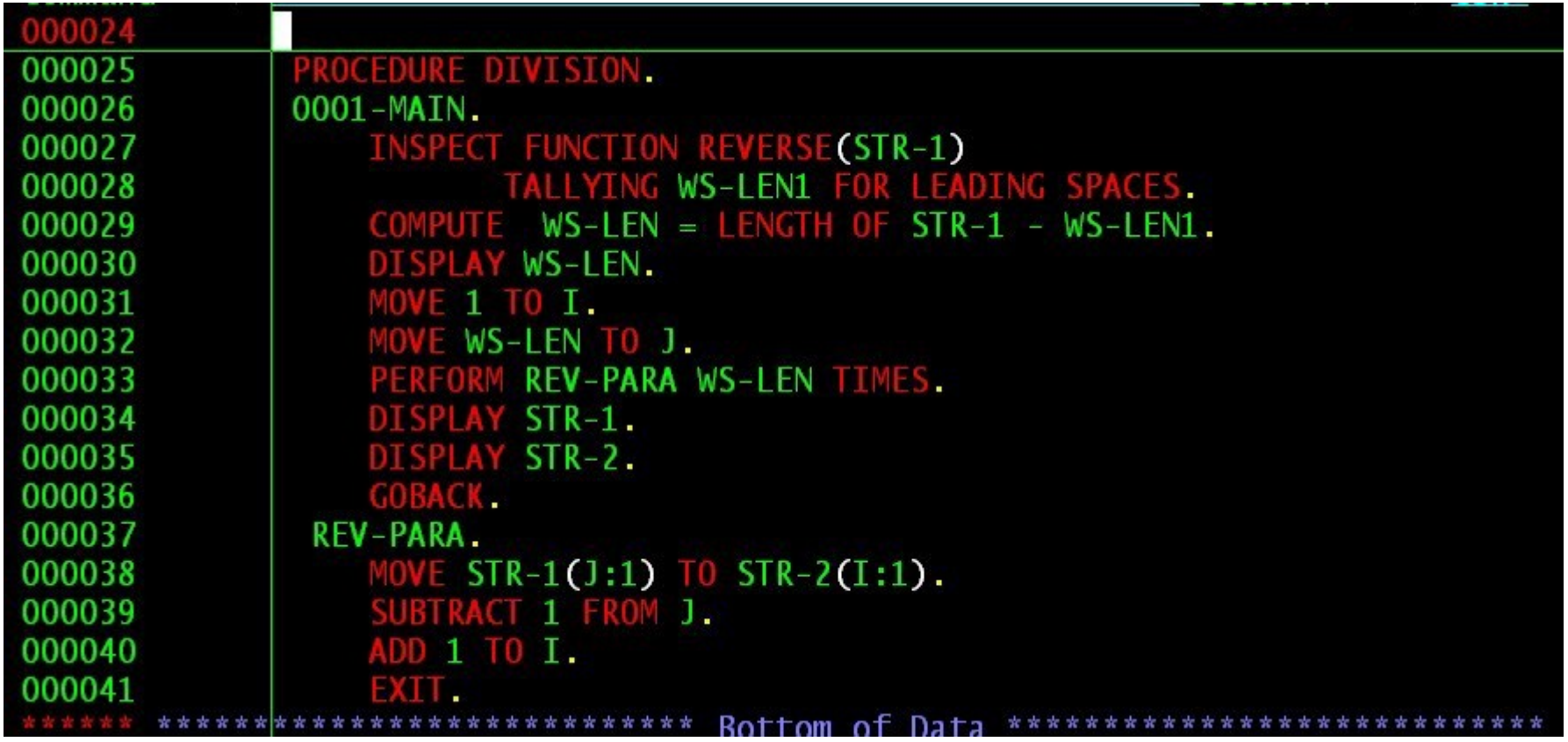
C example...

```
jedi@mariposa:/tmp$ cat cast.c
#include<stdio.h>

int main(int argc, char **argv)
{
        for (char *p = (char *) *argv; p < (char *) *argv + 20; p++)
                printf("%02x", *p);
        puts("\n");
        return 0;
}
jedi@mariposa:/tmp$ gcc cast.c -o cast
jedi@mariposa:/tmp$ ./cast AAAA BBBB
2e2f6361737400414141410042424242200534845

jedi@mariposa:/tmp$
```

COBOL example...



```
000024
000025      PROCEDURE DIVISION.
000026      0001-MAIN.
000027          INSPECT FUNCTION REVERSE(STR-1)
000028                  TALLYING WS-LEN1 FOR LEADING SPACES.
000029          COMPUTE  WS-LEN = LENGTH OF STR-1 - WS-LEN1.
000030          DISPLAY WS-LEN.
000031          MOVE 1 TO I.
000032          MOVE WS-LEN TO J.
000033          PERFORM REV-PARA WS-LEN TIMES.
000034          DISPLAY STR-1.
000035          DISPLAY STR-2.
000036          GOBACK.
000037       REV-PARA.
000038          MOVE STR-1(J:1) TO STR-2(I:1).
000039          SUBTRACT 1 FROM J.
000040          ADD 1 TO I.
000041          EXIT.
****** ********************************** Bottom of Data ********************************
```

https://medium.com/@yvanscher/7-cobol-examples-with-explanations-ae1784b4d576

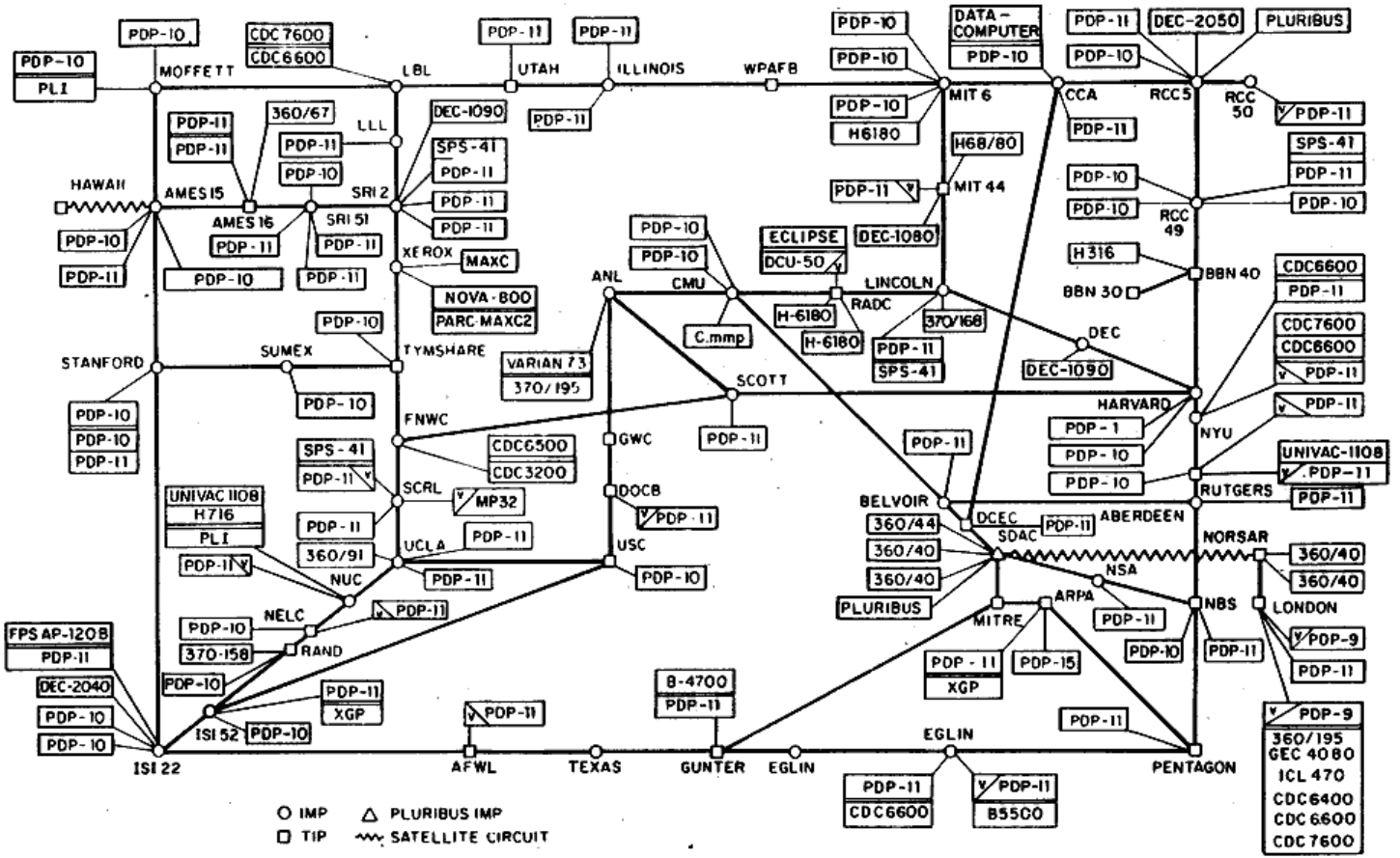
What does all this mean?

The Internet is more like UNIX and C than it is like TOPS-10 or COBOL. This means the smarts are in the end hosts, not the internal routing nodes, and it’s really hard to tell what two machines are saying to each other even if you know the protocol.

What to expect this semester

- You should be able to look at any PCAP and critically analyze it *w.r.t.* network security and privacy
  - So, we need to study crypto and physics (and build a quantum computer)
  - We need to understand the ways in which our tools (*e.g.*, Wirseshark) can be wrong
    - *E.g.*, overlapping IP fragments
  - We need to think critically about what can make a bit pattern “malicious”

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

https://commons.wikimedia.org/wiki/File:Arpanet_logical_map,_march_1977.png

Postel’s Law

- “be conservative in what you do, be liberal in what you accept from others”
- https://en.wikipedia.org/wiki/Robustness_principle

End-to-end principle

- Put the smarts in the end nodes (security, reliability, QoS, *etc.*)
- https://en.wikipedia.org/wiki/End-to-end_principle

https://commons.wikimedia.org/wiki/File:ARPANET_first_router_2.jpg

Example: Congestion control

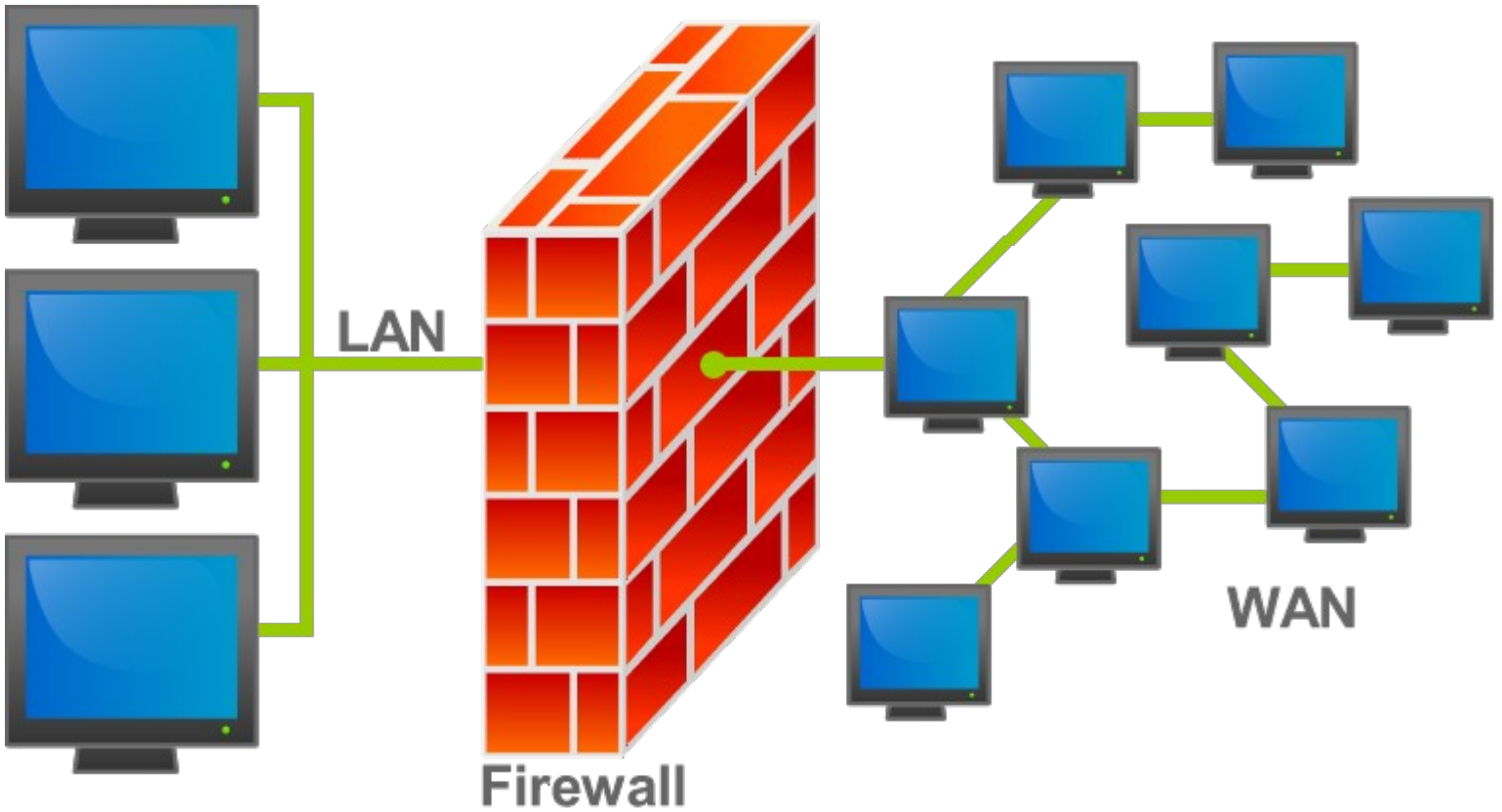
- Congestion collapse
- Van Jacobson
- TCP Tahoe, Reno, Vegas, CUBIC…
- Random Early Detection (RED)

https://alchetron.com/Sally-Floyd

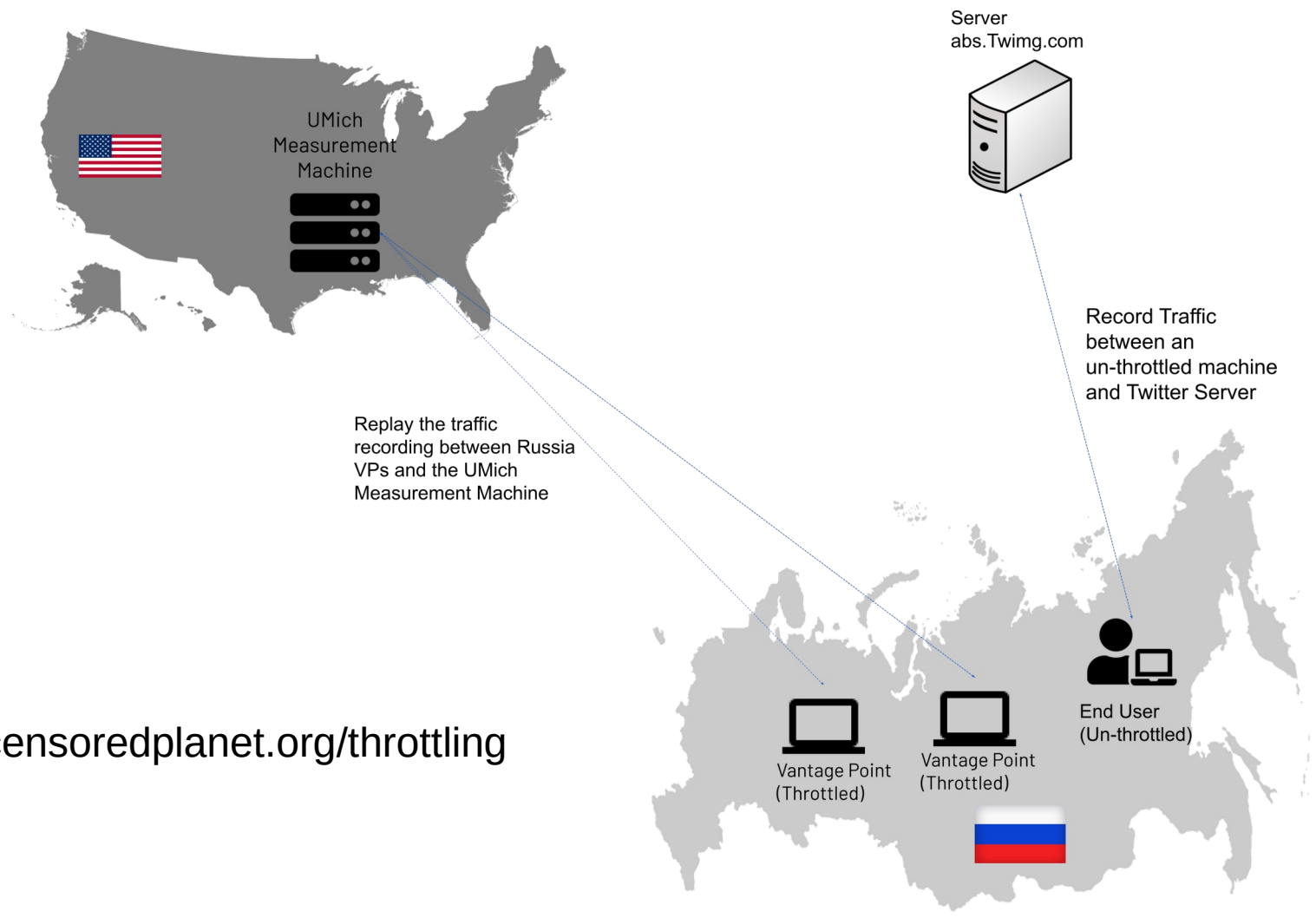
Good design, w/ consequences...

- Every device on the Internet is basically “doing its own thing” *w.r.t.* what packets it sends and how it interprets the packets it receives. (Postel’s Law)
- State is kept in many places without any explicit synchronization mechanisms. (End-to-end principle)

Why all this matters today...

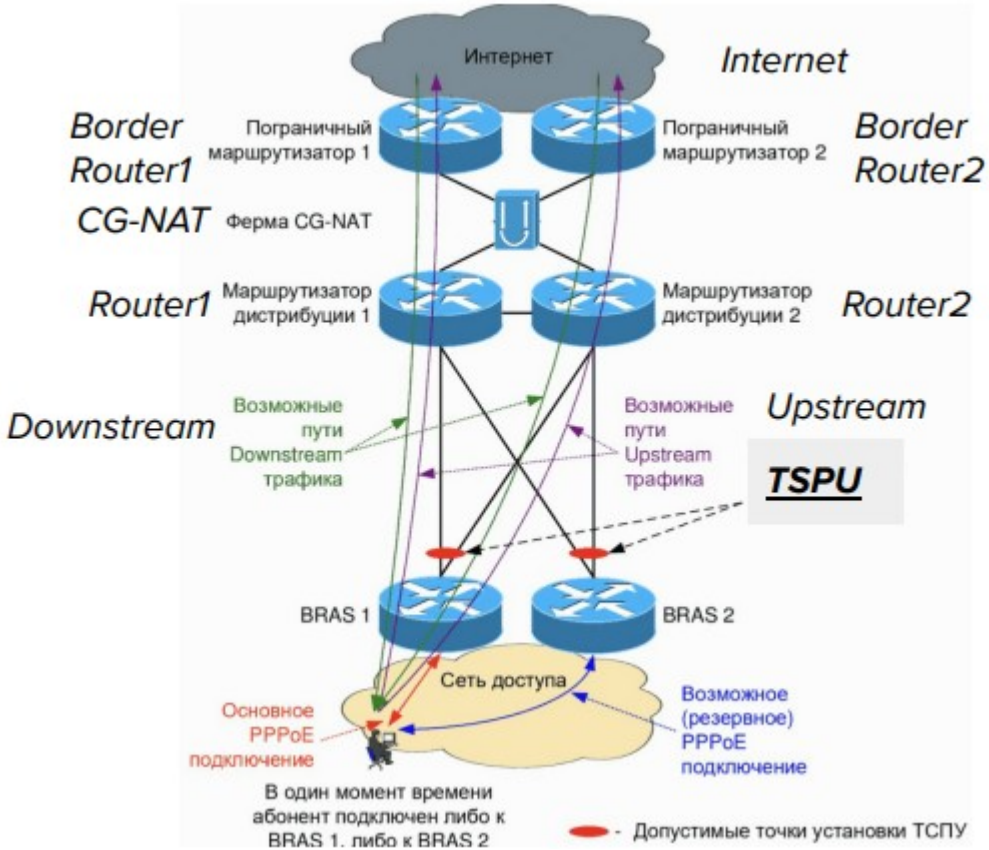


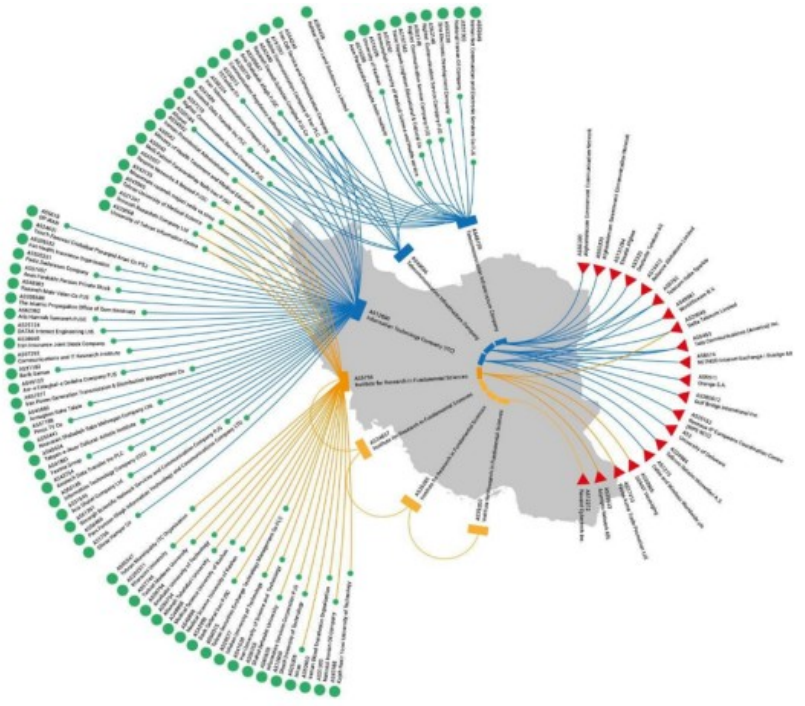
https://commons.wikimedia.org/wiki/File:Firewall.png



https://censoredplanet.org/throttling

https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/more_isp_maps.html

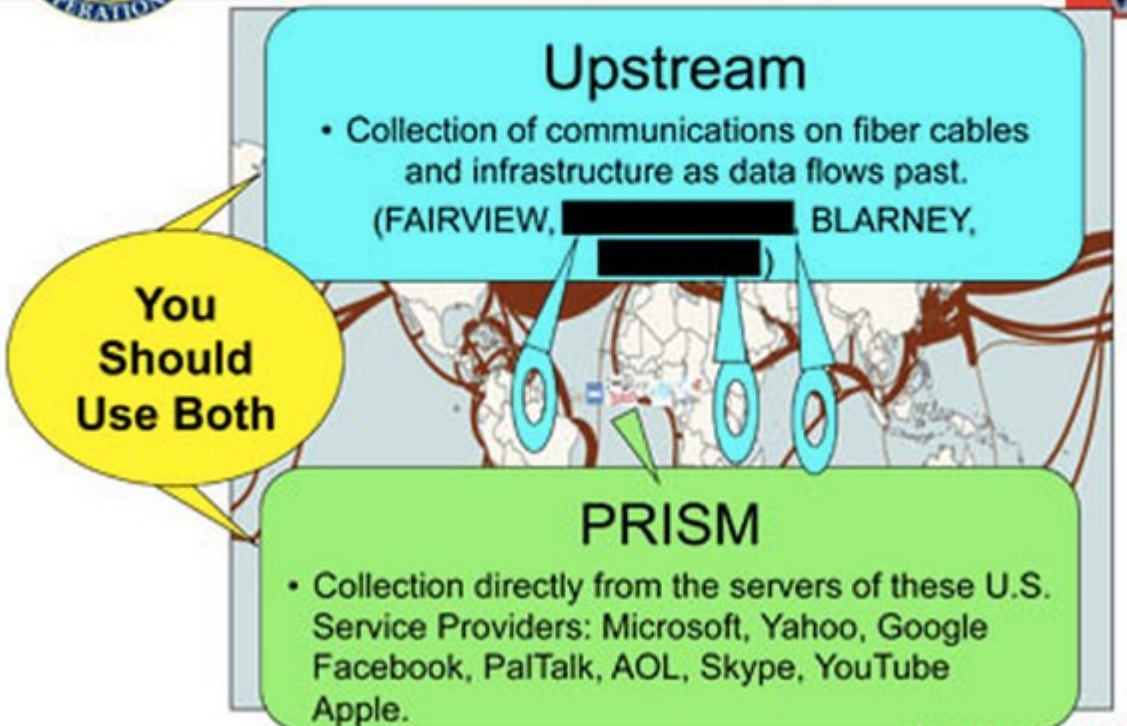




Reproduced and cropped from https://www.article19.org/ttn-iran-november-shutdown/

(TS//SI//NF) FAA702 Operations

Two Types of Collection



[Cypherpunks want] “a guarantee -- with physics and mathematics, not with laws -- that we can give ourselves real privacy of personal communications.”

“We are literally in a race between our ability to build and deploy technology, and their ability to build and deploy laws and treaties. Neither side is likely to back down or wise up until it has definitively lost the race.”

--John Gilmore

Why does light “bend” when it goes through a medium (like a glass of water)?