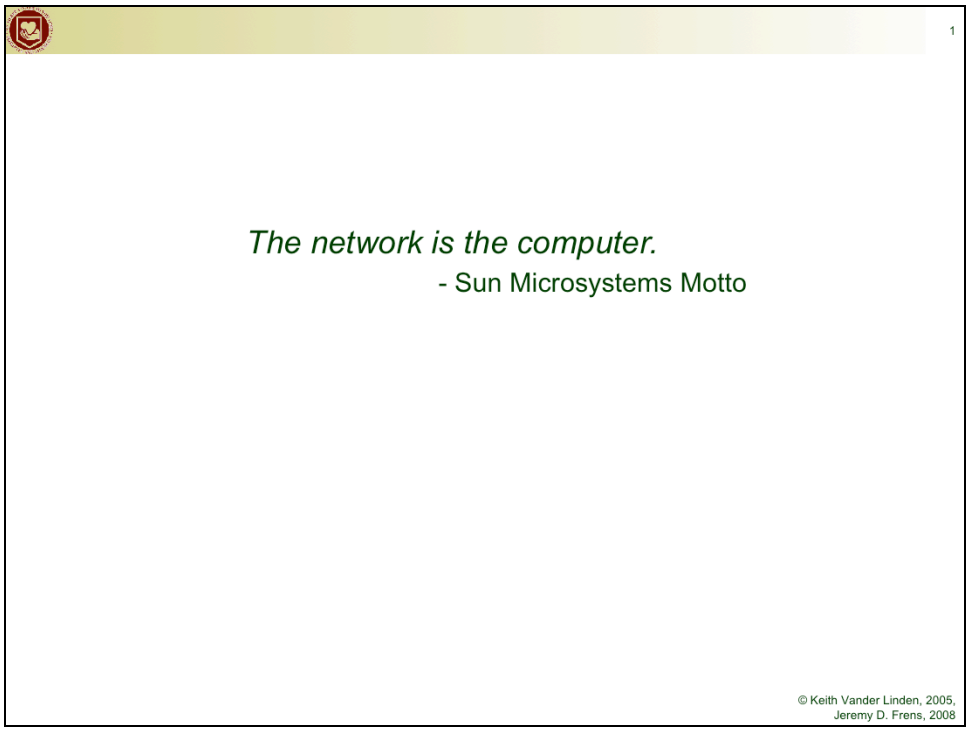
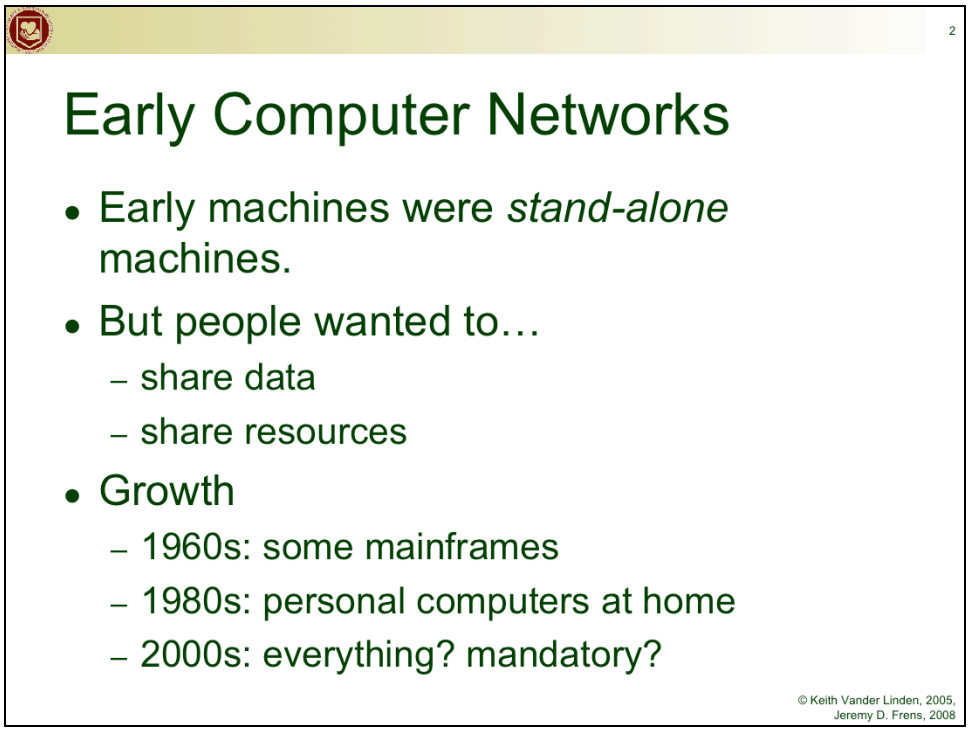


It's a mind-set, not a skill-set. Brilliance helps, but is not required. Instead, adopt these mantras: be stubborn, bossy, lazy, obsessive, cynical, **plodding**, and importunate. Why? So you can use IT as a tool to do cool stuff…



We'll pretty much skip directly to the internet.

Computer networks present:

Opportunities

users can share files

you only need 1 printer for a group of people

you can communicate via email and ftp

computing loads could be balanced between machines

Difficulties

hackers can get shared files

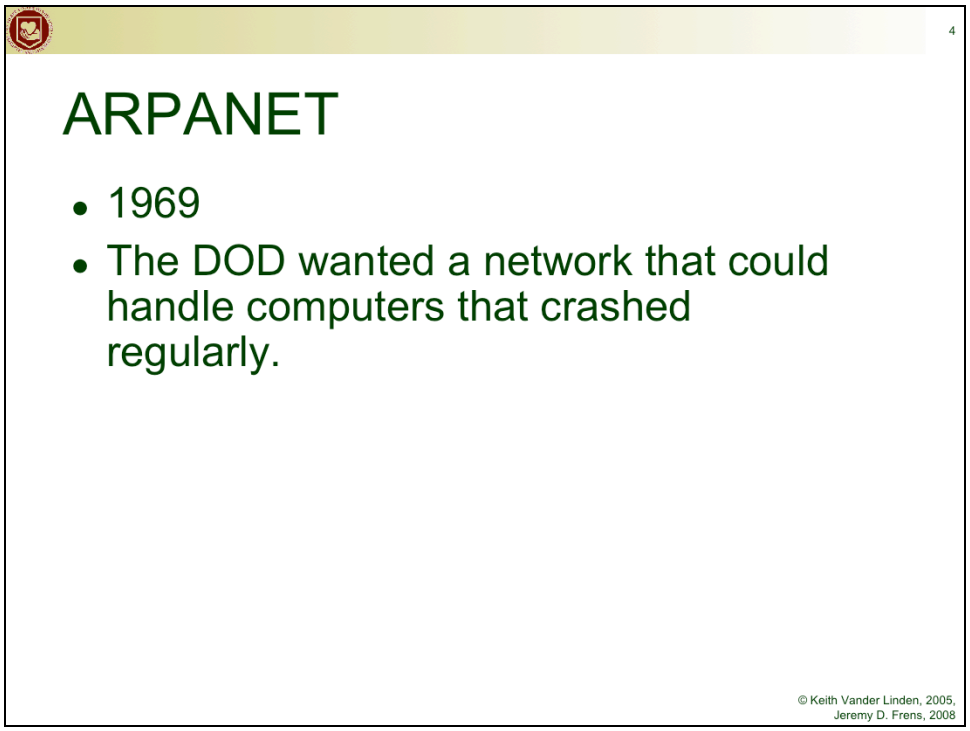
when the 1 printer goes down, everyone is toast

you can send spam

Security is a huge issue!

Distributed Network

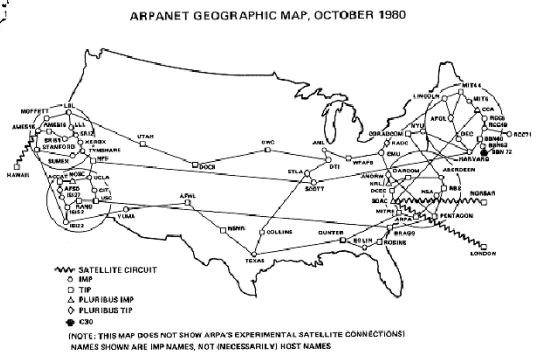
- No one computer is in charge of the Internet.
  - *All* computers are in charge!
  - Some take on more responsibilities.
- Computers are connected to each other in multiple ways.
- Each computer routes data closer to its destination.
  - Routers: extra routing responsibilities.



The DOD did not want a computer network in which communication lines could so easily be “disconnected”.

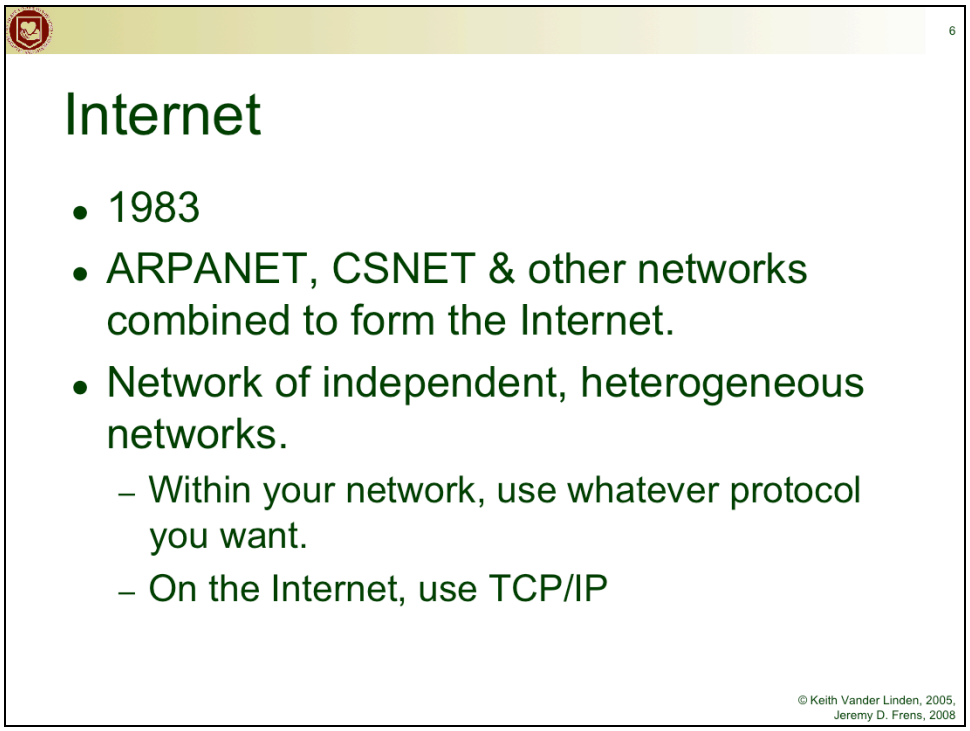
Growth of the ARPANET

ARPANET GEOGRAPHIC MAP, 1969



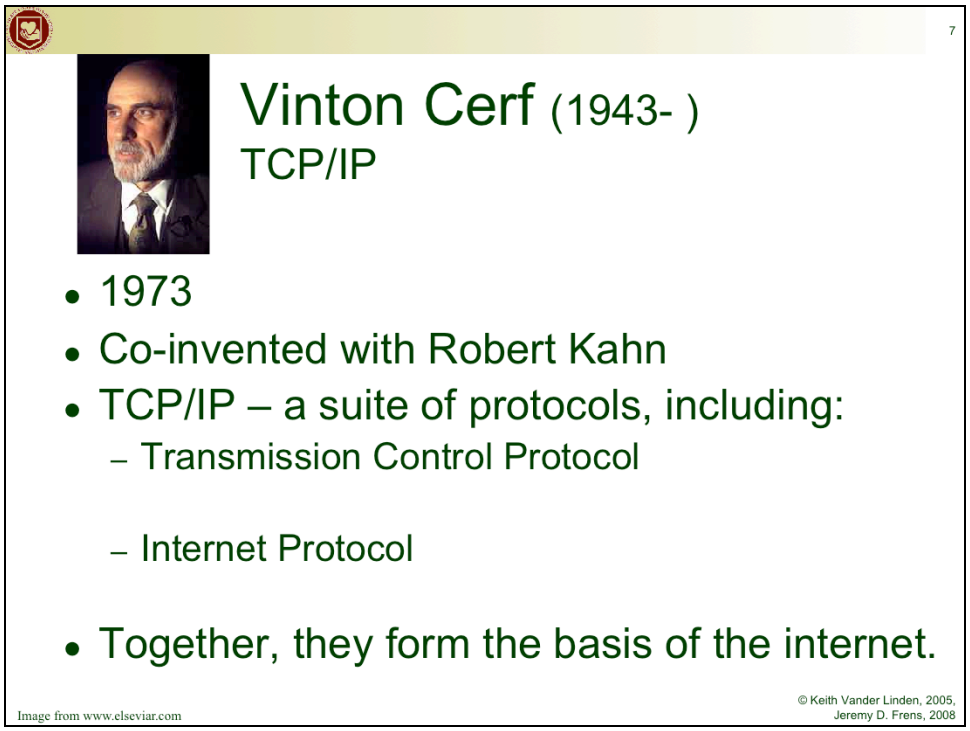
Images from Barry Leiner, et al., ©Keith Vander Linden, 2005, Jeremy D. Frens, 2008

No, I won't try to get a map of the whole internet today!



The internet is a network of networks, all using TCP/IP.

The instructor's station might have the address: pcnh180-1.calvin.edu. This is completely unique in the world.



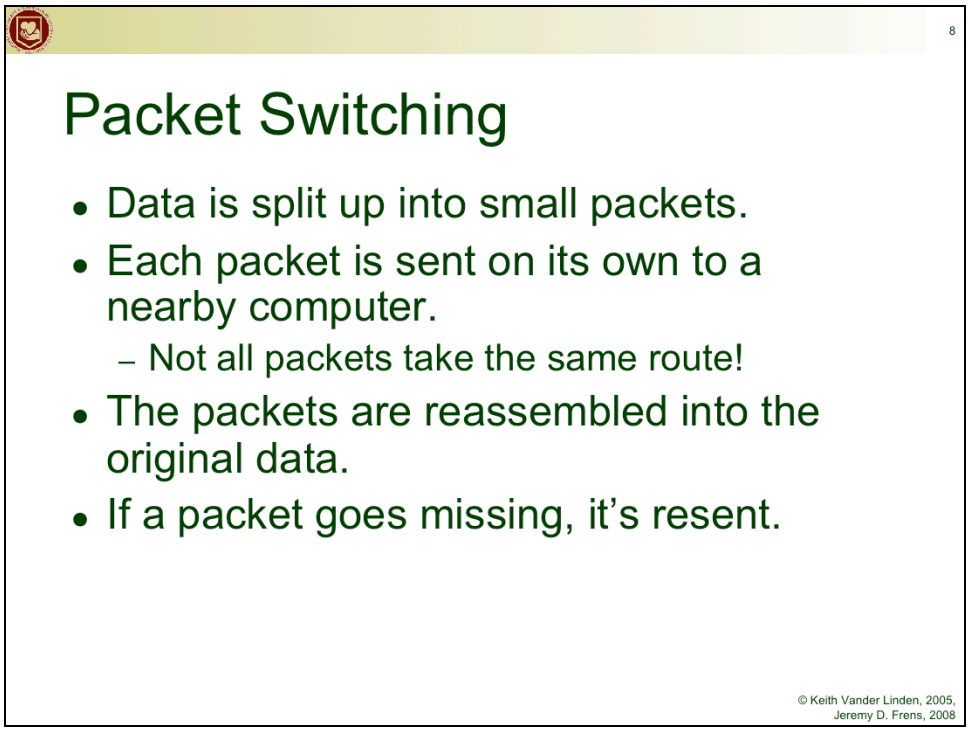
Transmission Control Protocol - rules for building and managing packets (chunks and reassembles)

Internet Protocol - rules for routing the packets

The basis of the internet for 2 reasons really:

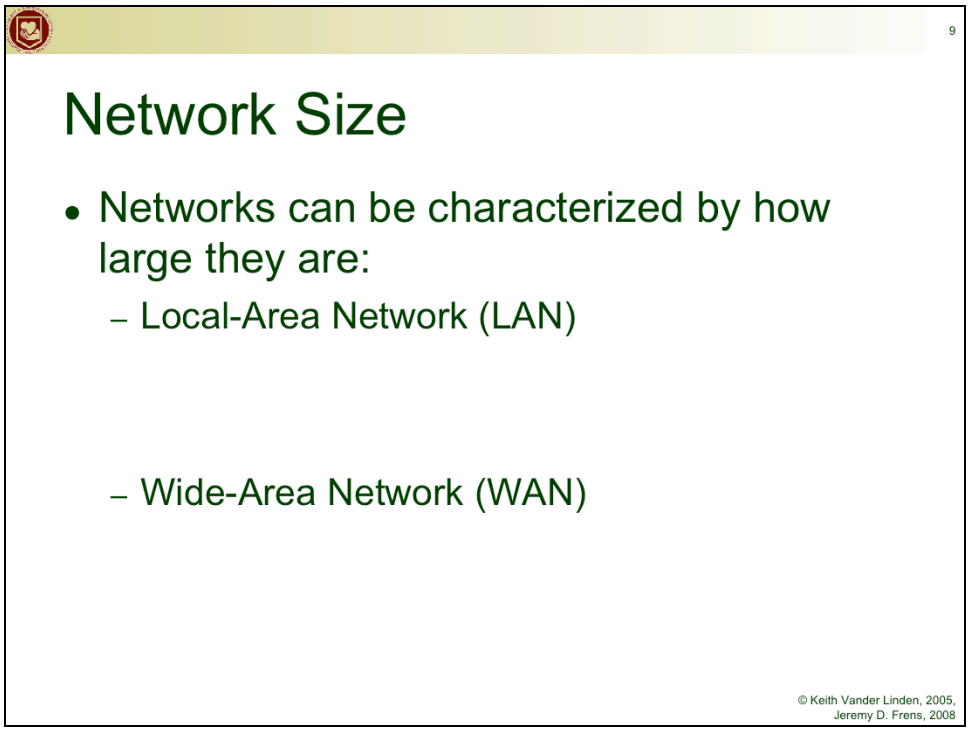
packet switching

it was an **open-network architecture**, not a proprietary one.



Packet switching is different from the explicit direct circuits used by the telephone system - if you are cut off there, you are cut off and need to re-establish a connection. In packet-switching, the packets just get re-routed. TCP/IP is one of the many packet switching protocols out there.

Note that this is very different from a centralized, switched telephone network.



Local Area Networks (*LAN*):

reach up to 1 mile – say for a single building or a campus (Calvin is a LAN)

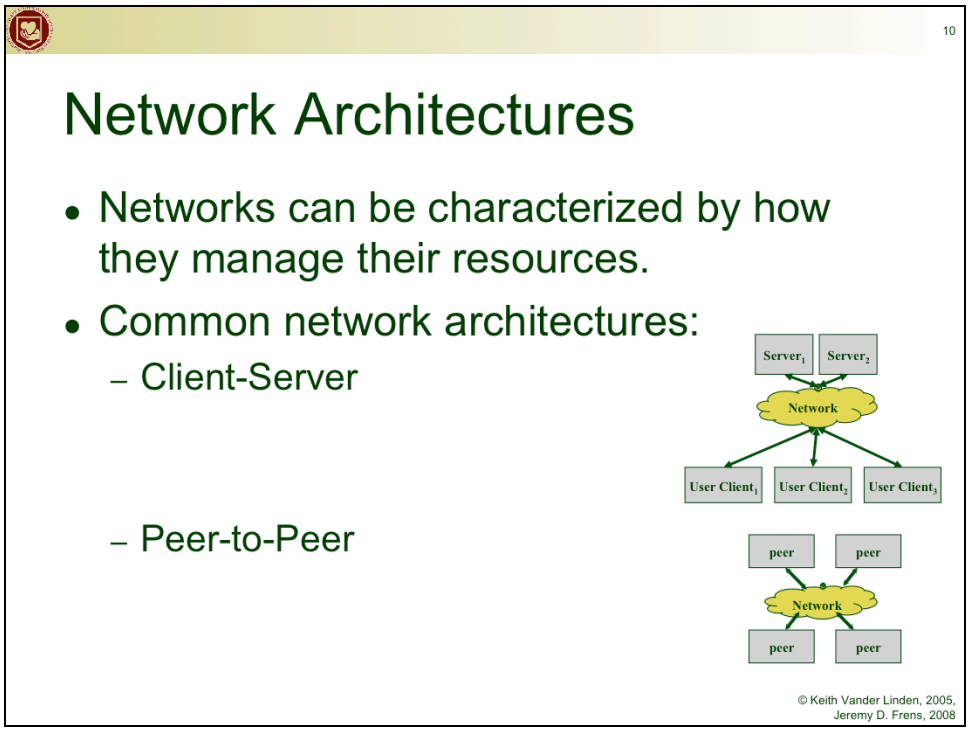
are relatively fast

Wide Area Networks (*WAN*):

can be global

e.g., the internet is a WAN (but not the only one)

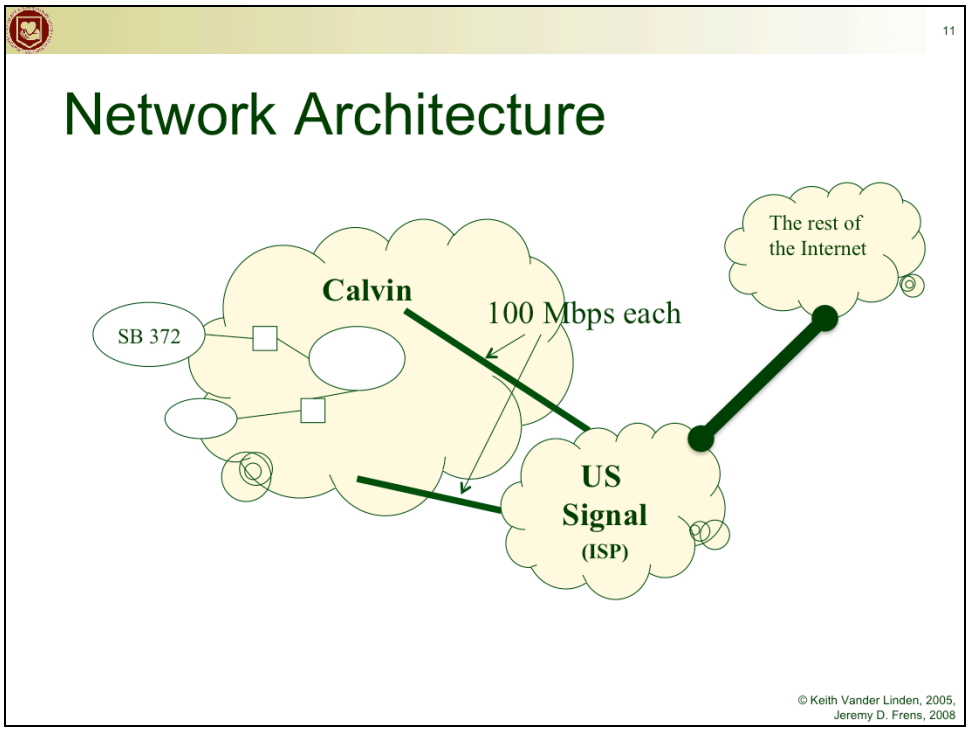
are relatively slower



Common network architectures:

Client-server – Separates front-end interfaces (clients) from centralized service providers (servers) – This is by far the most common architecture today.

Peer-to-peer – used direct network connections between egalitarian client/servers (clervers!?)



The internet is a network of heterogeneous networks, as can be seen in this myopic, SB372-centric view of the internet.

LANS (circles at Calvin, including SB 372)

Switches connect computers all with the same domain (i.e. Calvin is all 153.106.xx.xx)

Routers link one (potentially incompatible) network to another (little boxes). They can also have additional responsibilities like firewalls and other policy implementation

Modems (little circles): From Wikipedia: A **modem** (**mo**dulator-**dem**odulator) is a device that modulates an analog signal carrier to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data.

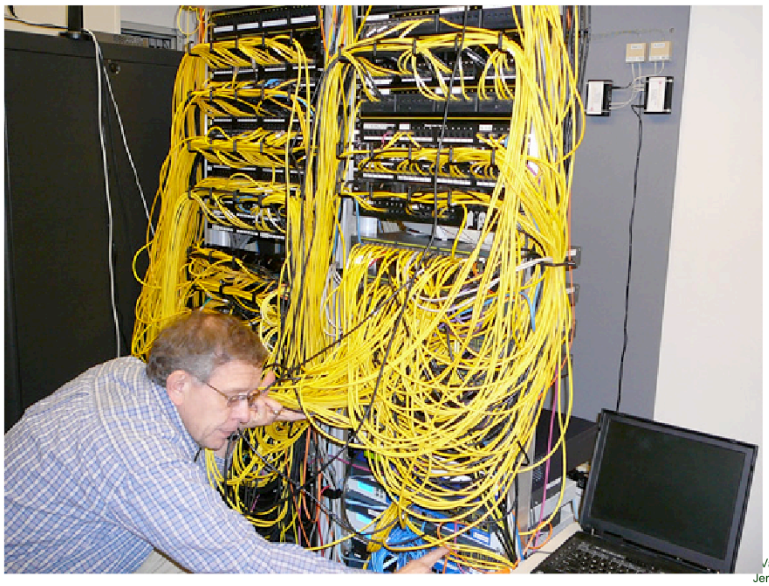
Internet Service Provider

Servers: deliver content

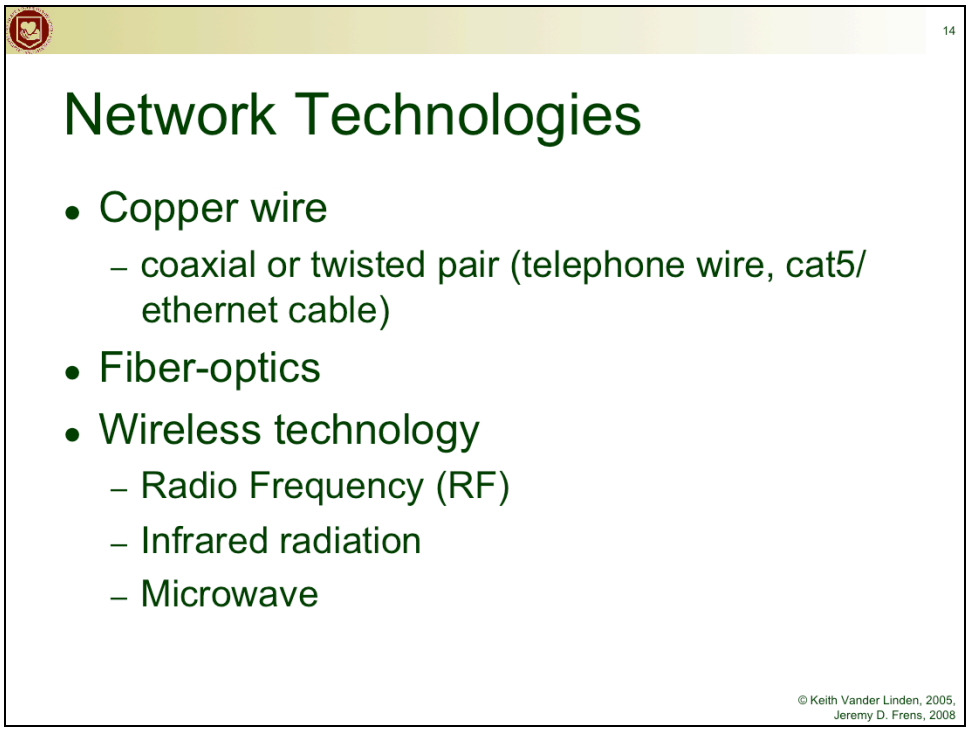
Calvin's Network

- Dual 100 Mbps fiber connections to/from US Signal
- 400 switches
- Distribution closets in all buildings – with big one in Bolt-Heyns-Timmer
- All data through a "packet shaper", "intrusion prevention device", and "external firewall".

Calvin's Network



Vander Linden, 2005,
Jeremy D. Frens, 2008



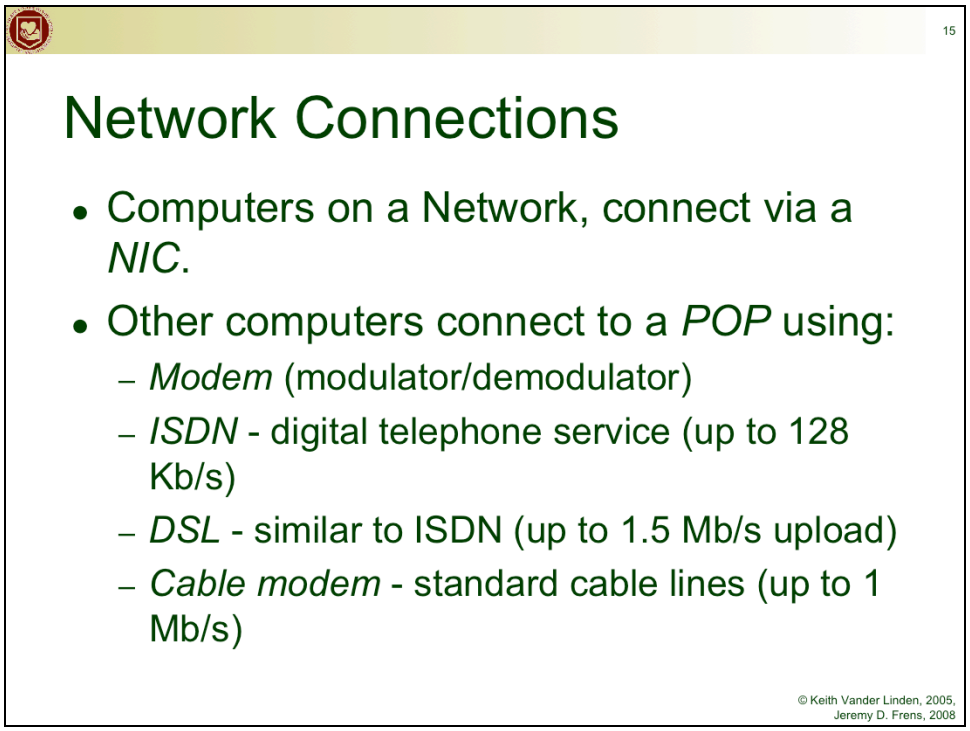
Fiber is cheaper to fabricate, but requires a laser (expensive). Breaks easily without protection, but works better for long distances.

Thus, **copper** is still common (more durable, works well for local connections)

RF is nice, but there are limited radio frequencies to use (this is what WIFI works with though)

infrared is restricted to a single room, and is still slower than the others (remote controls)

microwave can't penetrate metal either, and are potentially dangerous to humans



Computers on a Network, connect via a Network Interface Card (*NIC*)

high-speed connection to a LAN

Connecting to a Network point of presence (POP):

Modem (modulator/demodulator)

digital to analog telephone signals (up to 56 Kb/s)

connects to an *Internet Service Provider* (ISP)

Other technologies:

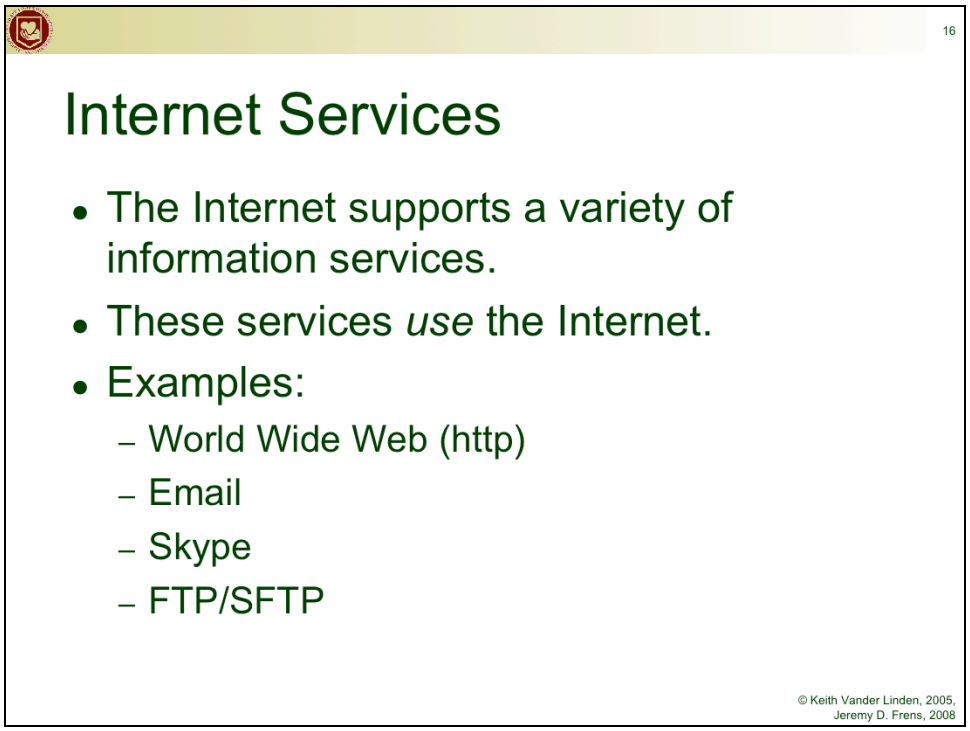
ISDN - digital telephone service (up to 128 Kb/s)

DSL - similar to ISDN (up to 1.5 Mb/s upload)

Cable modem - standard cable lines (up to 1 Mb/s)

ISDN/DSL are used because we're stuck presently with twisted pair technology.

"broadband" refers to high-speed (> 1Mbps) internet connections

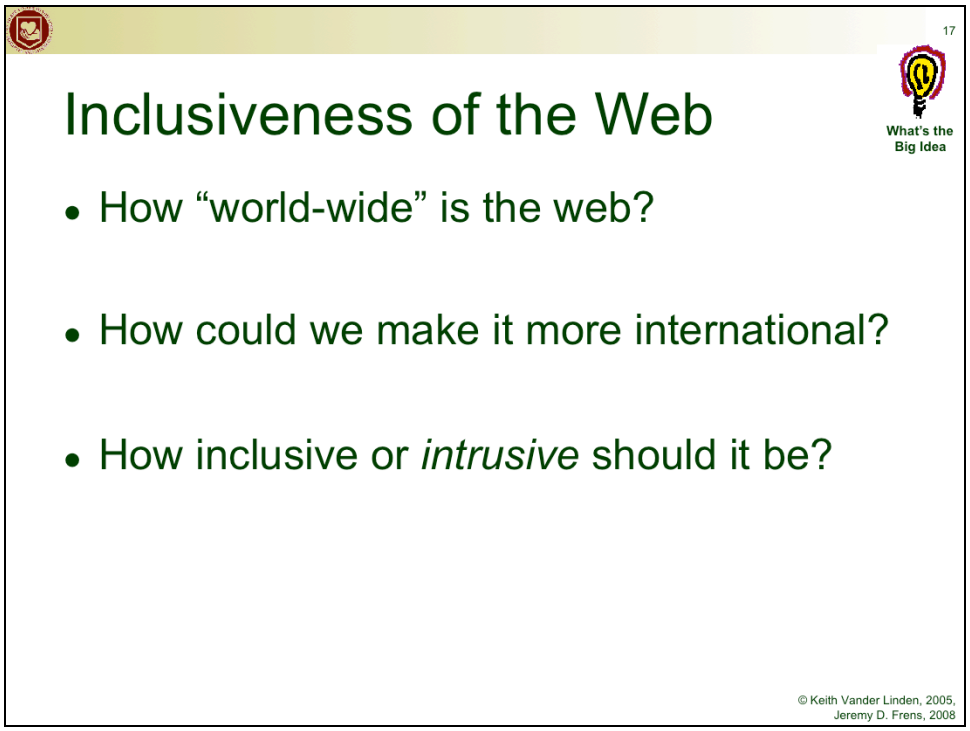


The internet now supports a vast array of programs/systems, called services.

The Web is an Internet service that supports the sharing of hypermedia. **Internet != WWW**

Email is a service for exchanging mail messages.

FTP/SFTP is a service for moving data between machines



Given the English-centric nature of the web, one might more accurately call it the ***Western*-wide web.**

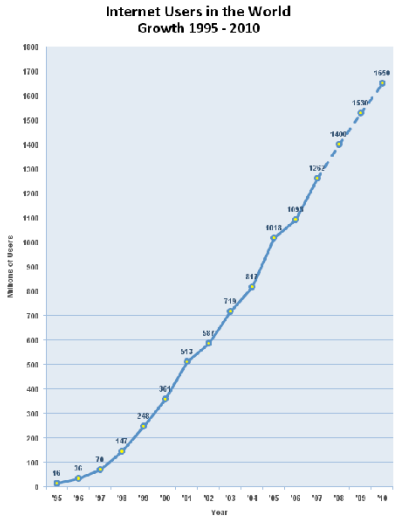
Digital divide – the WWW is hard to access in:

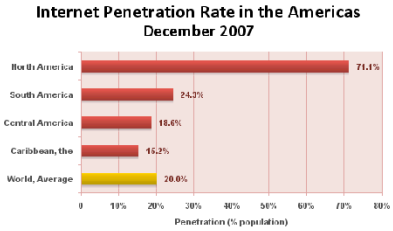
- the developing world
- the non-western world
- underpriviledged social classes
- the disabled community

What could we do to help bridge this divide?

- Unicode
- internationalized domain name resolution
- better translation tools
- better international/disabled design and testing

Growth of the Internet

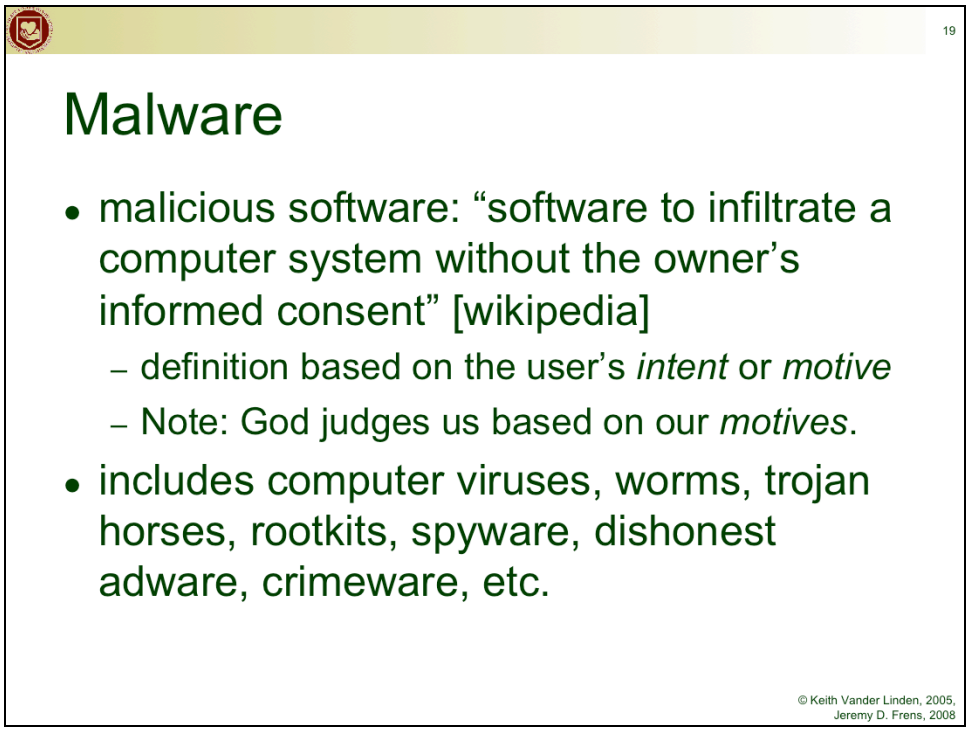




Source: Internet World Stats www.internetworldstats.com
Copyright © 2008, Miniwatts Marketing Group

penetration (% of population)

http://www.internetworldstats.com/stats.htm



What kinds of data:

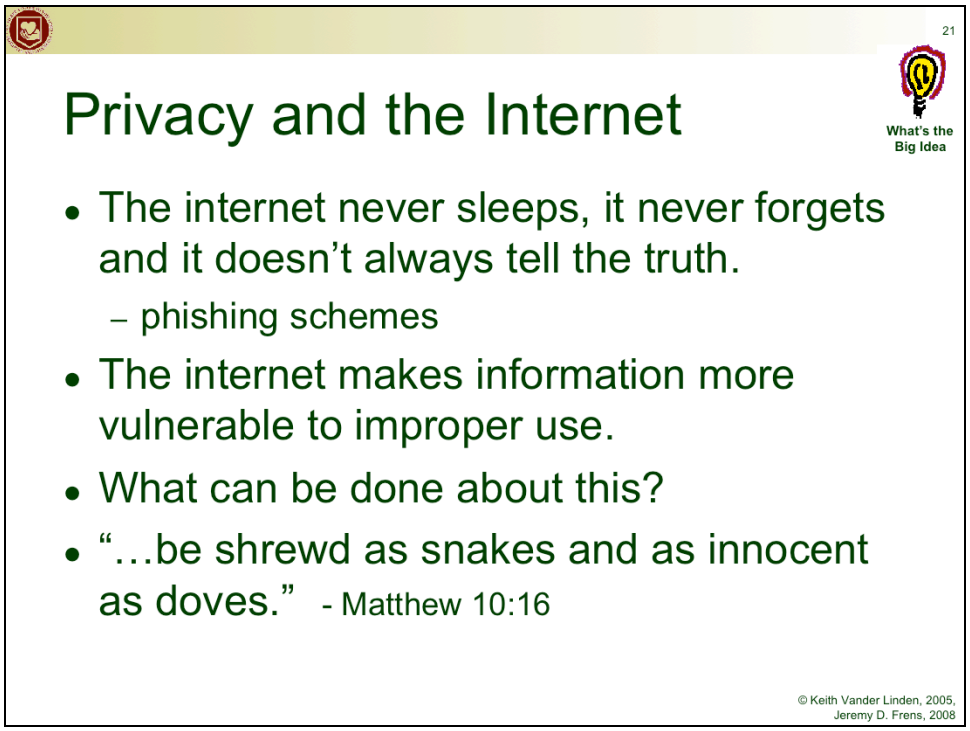
- internet usage patterns
- credit cards (even with encryption)
- informational databases
- proprietary systems or information
- passwords

how can they be compromised:

- copying
- hacking into protected sites
- sniffed in various ways
  - packet-sniffers
  - carnivore
  - companies monitoring stuff
- cookies
- identity theft

Malware (cont)

- virus: attached to an existing program, does damage to files, and copies itself.
- worm: unattached, damages the network, and copies itself.
- trojan horse: opens up a “backdoor” to the system for future unauthorized access; non-replicating.
- spyware: collects info about users.
- crimeware: for identity theft.



Privacy is somewhat of a fallacy on the internet.

What to do:

privacy legislation

proper security

ethical behavior.