How the Internet works

related sections to read
in Networked Life:
10.1-10.2
13.1
14.1
15.1-15.2
17.1

- Take a moment to think about how amazing the Internet is:
  - It’s always on
  - It is “free”
  - It’s (almost) never noticeably congested (though individual sites or access points might be)
  - you can get messages to anywhere in the world instantaneously
  - you can communicate for free, including voice and video conferencing
  - you can stream music and movies
  - it is uncensored (in most places) (of course, this can be viewed as good or bad)

- This talk focuses on the question of how the Internet can be so robust
  - Is there an “Achilles’ heel”? a single point of failure that can be attacked?
  - How does the network autonomously adapt to congestion?
- To answer these questions, we will discuss some of the underlying technologies that contribute to the robustness of the Internet
  - packet switching
  - Ethernet
  - TCP/IP
  - routing protocols

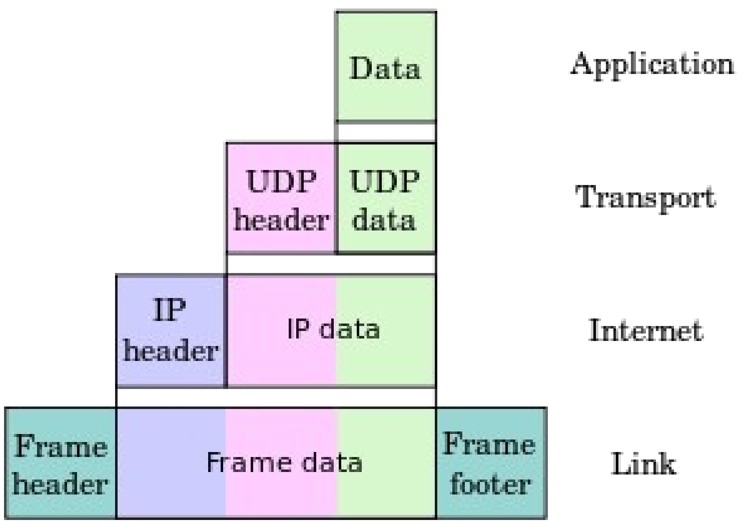
- Evolution of the technologies underlying the Internet
  - the Internet was not designed top-down by a single company or government organization
  - it evolved
    - many alternative technologies/protocols were proposed and tried out
    - eventually, the best were identified and adopted (in a “democratic” way)
    - when new people joined, they had to use whatever protocols everybody was using, until it grew into a standard
  - it is decentralized – no one owns it or controls it

- Compare with the old-style telephone networks
  - designed top-down by companies like AT&T, who built the network of telephone lines, and wanted (and had) complete control over their use
  - good aspect of design:
    - old handsets did not need electrical power
    - energy for dial-tone and speakers came from phone line
    - phones would work even if power knocked out in electrical strorm
  - con: they were circuit-switched (a dedicated path between caller and receiver had to be established, and most of that bandwidth was wasted)
- In contrast, given how the Internet “grew”, it is amazing it works at all (!)

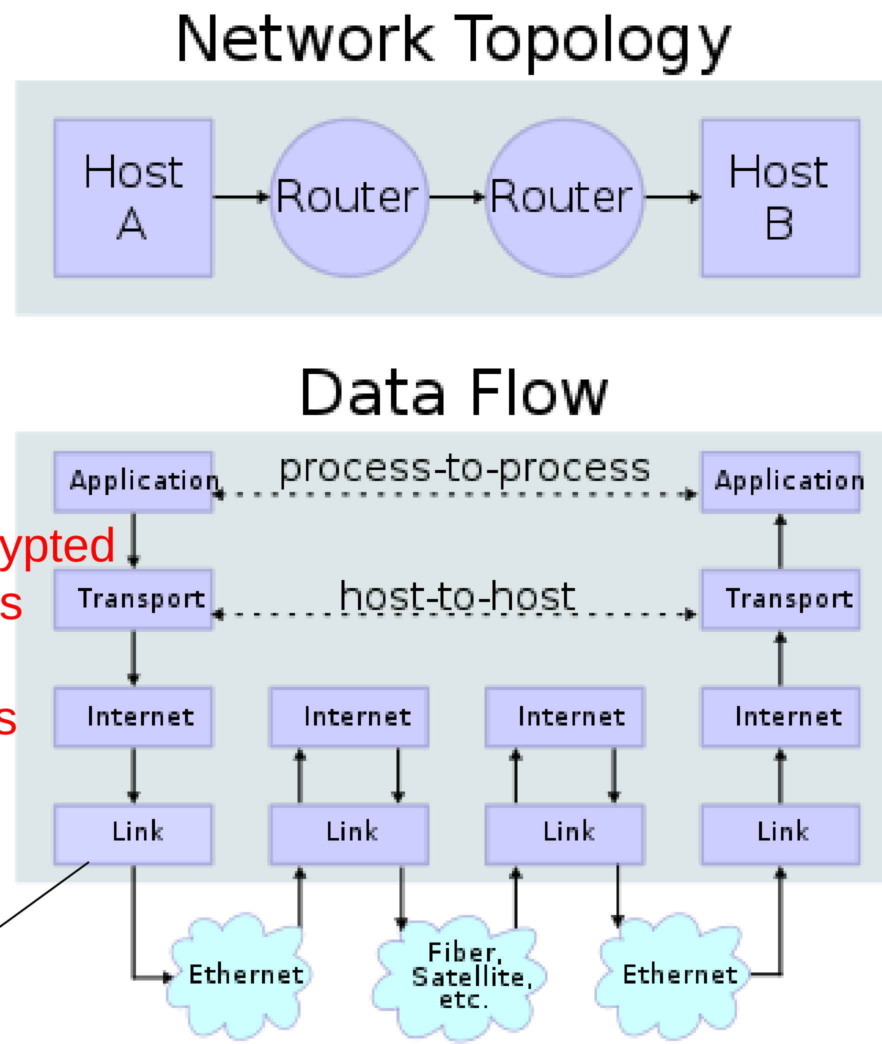
protocol stacks

- layered architecture

each layer is an *abstraction* that assumes the functionality of the layer underneath



files
unencrypted
streams
buffers
packets
frames
bytes
bits



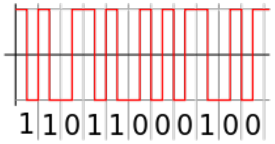
drivers,
network card

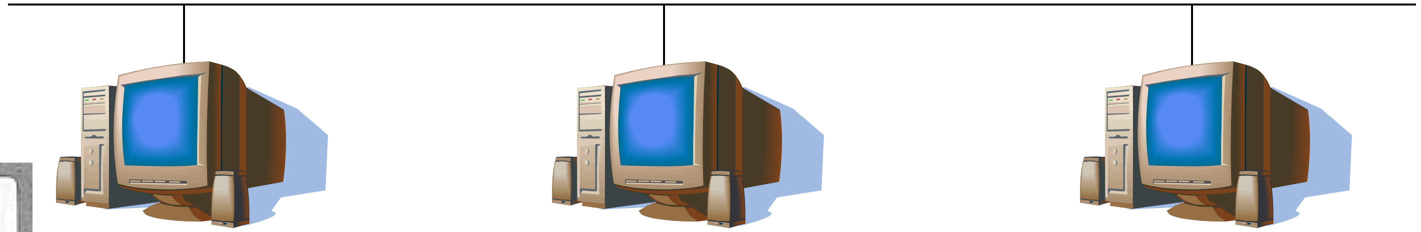
Ethernet

802.3 Ethernet frame structure

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	42[note 2]–1500 octets	4 octets	12 octets
		← 64–1518 octets (64-1522 octets for 802.1Q tagged frames) →						
← 84–1538 octets (88-1542 octets for 802.1Q tagged frames) →								

- local machines on common wire hear all transmissions
- in cases of packet collisions, use a “back-off” algorithm
- each machine waits a *random* time (gauged by the amount of congestion) to re-transmit





IP addresses

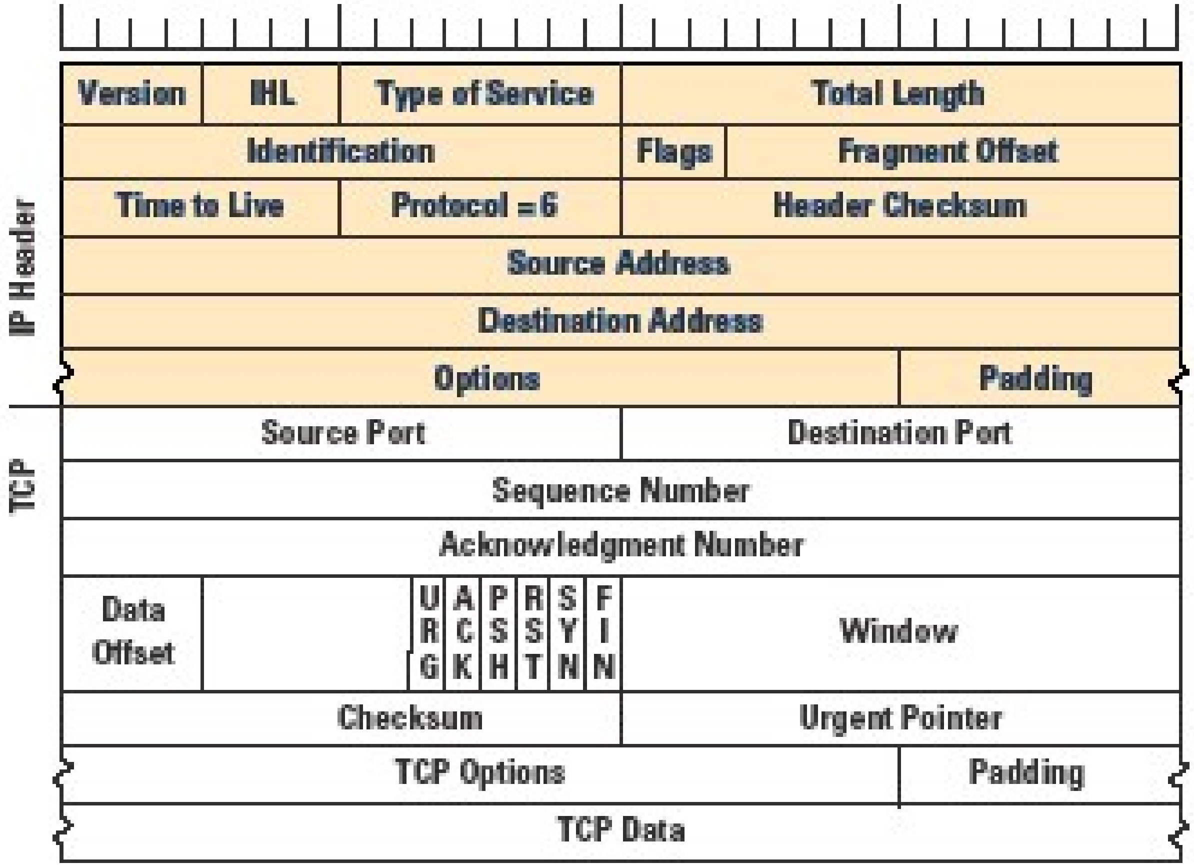
- [0-255].[0-255].[0-255].[0.255]
- 128.194.139.1 (associated with a specific MAC)
- <domain>.<domain>.<subnet>.<host>
- IPv4 (current standard, 4 billion IP addresses)
- IPv6 (extended address space: $2^{128}=10^{39}$ devices)
- 128.194.139.1 = sun.cs.tamu.edu
- DNS – domain name server
  - distributed network of servers that translate hostnames to IP addresses
  - TAMU campus has several DNS servers that communicate with others worldwide
  - *nslookup*: www.google.com = 74.125.227.145

TCP-IP

- transport layer
- built on top of IP
  - assumes can send datagrams to IP addresses
- UDP: User Datagram Protocol
  - simple, fast, checksums, no guarantee of delivery
- TCP-IP: Transmission Control Protocol
  - connection-oriented: hand-shaking, requires message acknowledgements (ACK)
  - guarantees all packets delivered uncorrupted in order

TCP-IP packets

- a file or message is divide up into packets



Geoff Huston, www.potaroo.net/ispcol

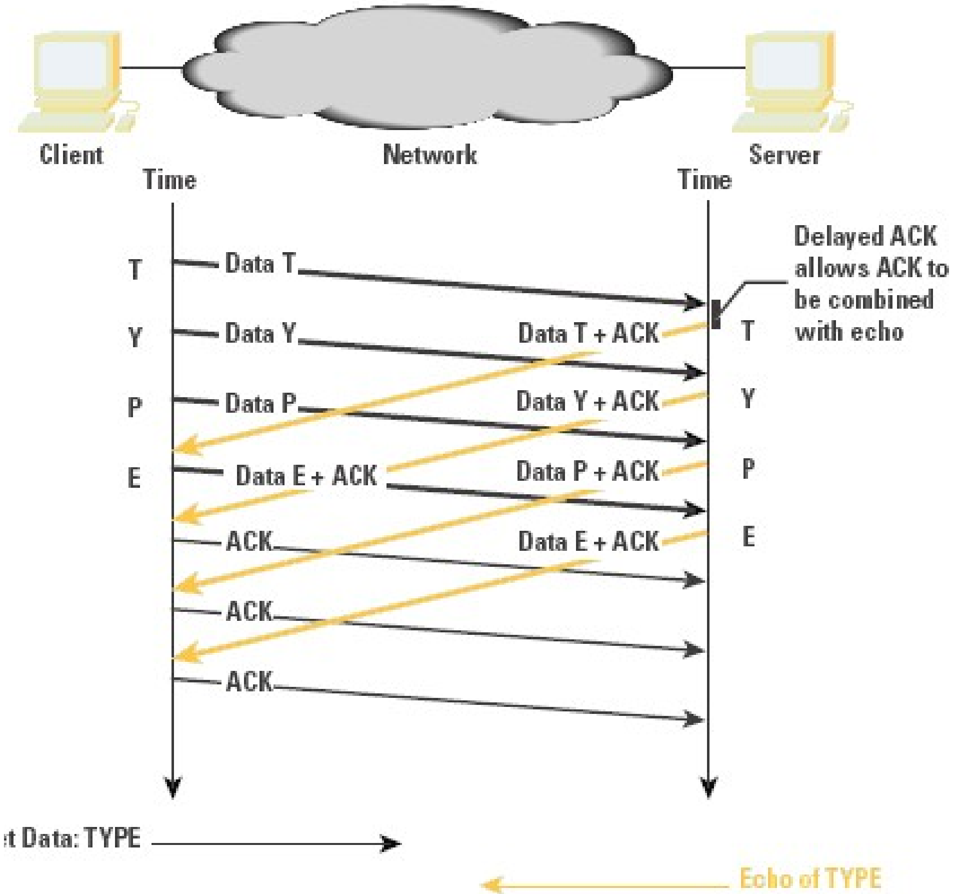
<u>information:</u>

- source IP address
- destination IP address
- mesg sequence number
- (for acknowledgement)
- payload size
- checksum

payload (e.g. 512 bytes)

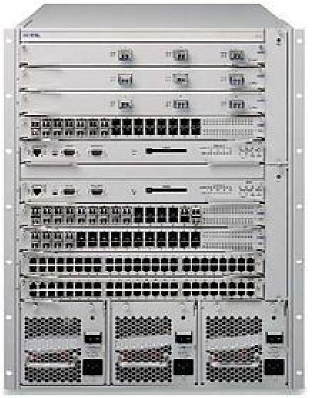
Congestion Control

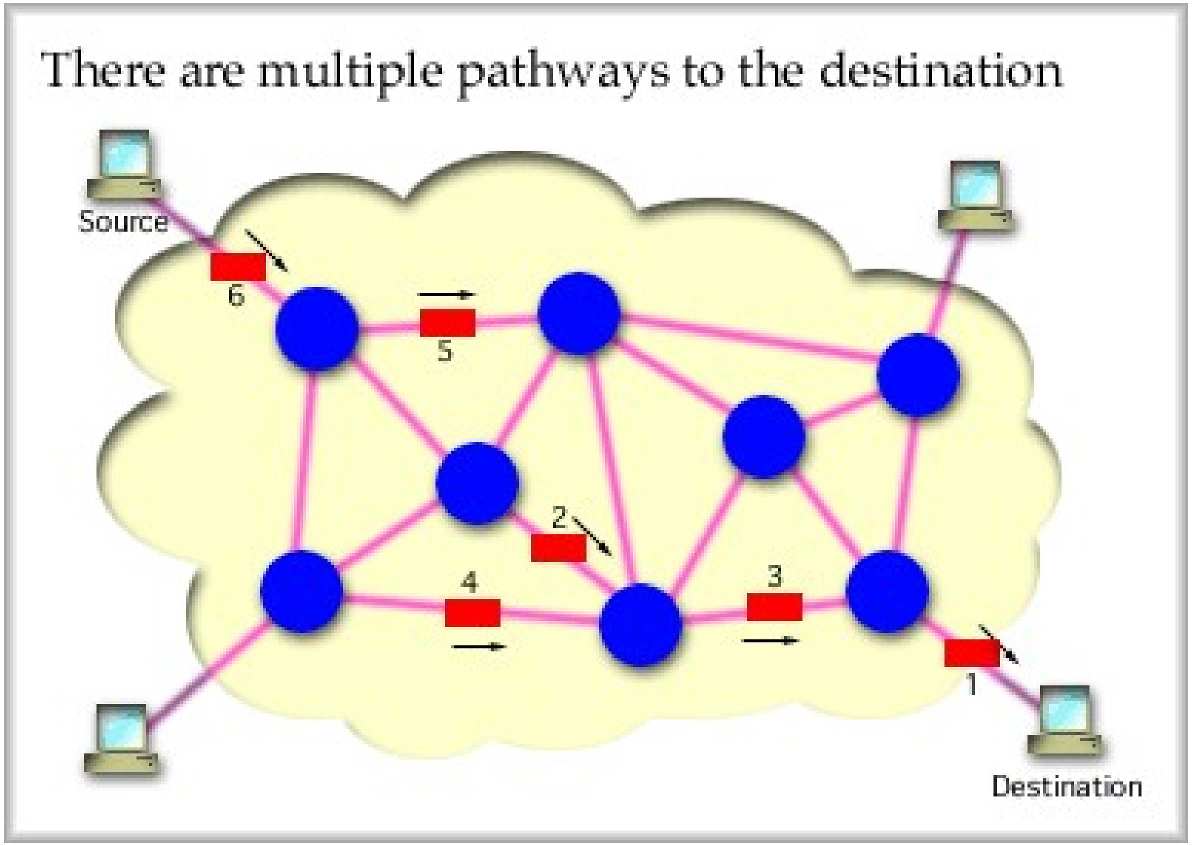
- TCP/IP senders track the response time of ACK messages
- separate latency (roundtrip) from throughput (bandwidth)
- adaptively adjust transmission frequency



Geoff Huston, www.potaroo.net/ispcol

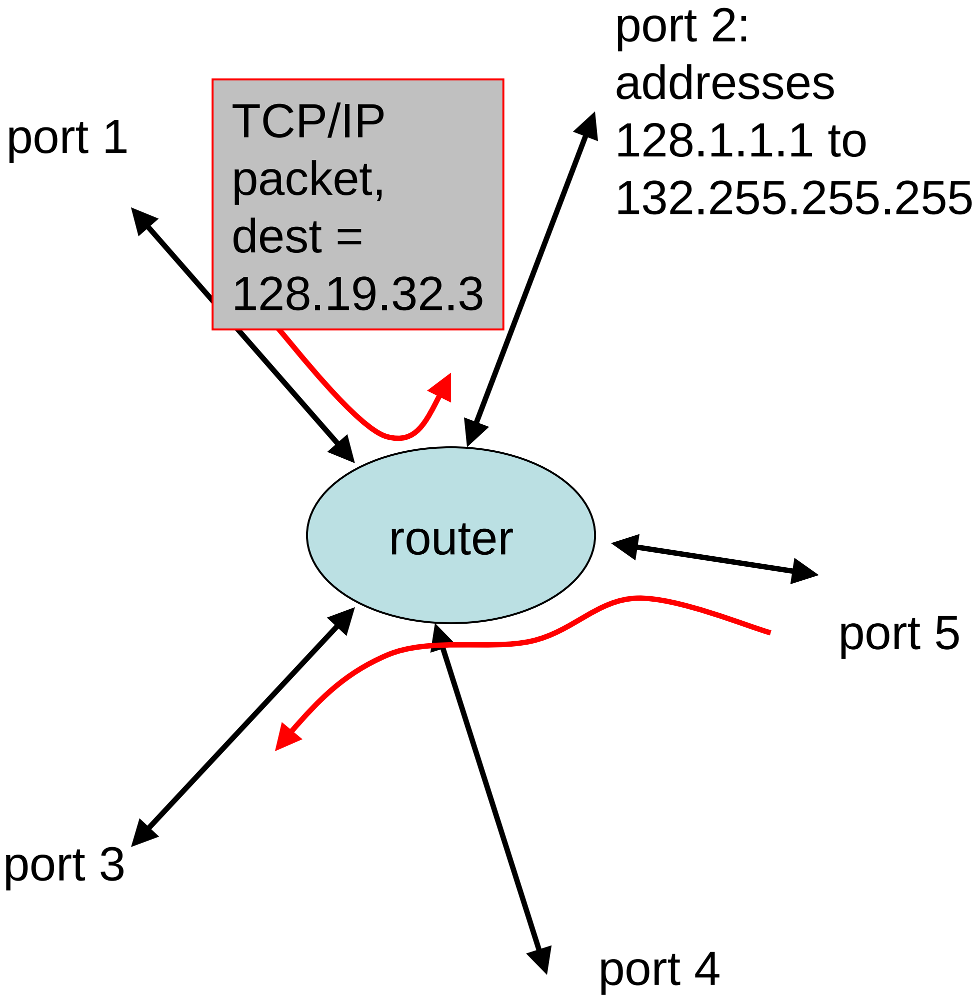
routers and routing





http://int.fhsu.edu/kevin/courses/datacom1VC/html/chapter_10.html

- each router switches packets among its local connections
- there are many paths from source to destination
- ideally, what we want is to identify the shortest path (Bellman-Ford algorithm)
- each router maintains a *router table* of IP addresses sent on out-going links (plus congestion information)



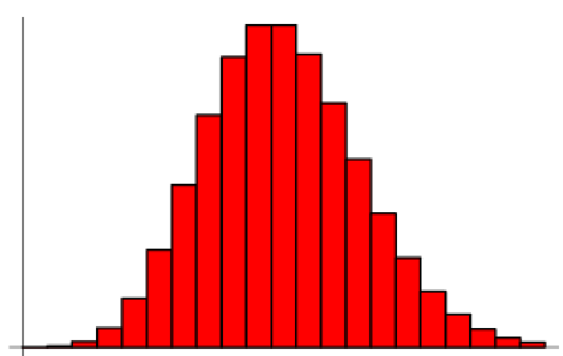
Router table

port	IP address range
1	001.*.*.* to 127.*.*.*
2	128.1.1.1 to 132.255.255.255
3	133.1.1.1 to 191.255.255.255
4	192.1.1.1 to 253.*.*.*
5	254.1.1.1 255.255.255.255

- Essentially what routers do is receive packets, extract destination IP,and switch them to an out-going port.
- Each router has a limited capacity (throughput or bandwidth, e.g. 10 GB/s).

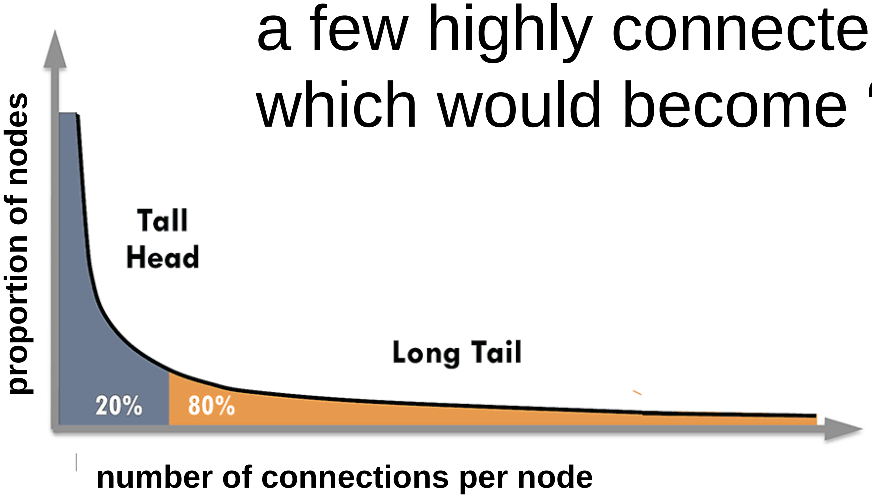
Robustness of the Internet

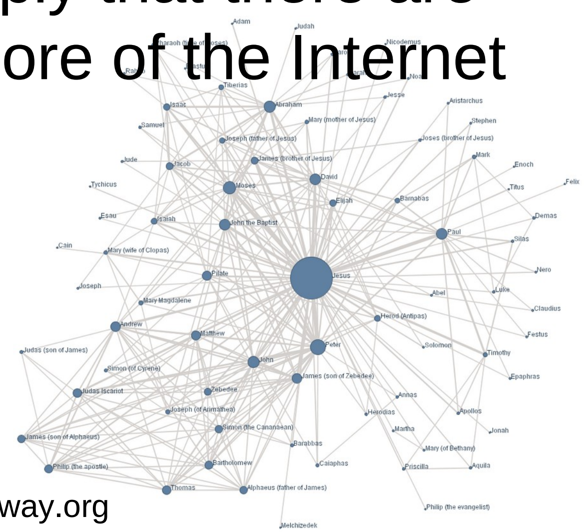
- does the Internet have an “Achilles’ heel”?
- is there a single point of failure (that could be attacked)?
- or is it designed to be fault tolerant?
- it is hard to know the overall topology
- does the connectivity follow a Poisson distribution?
  - is there an “average” number of connections, some with more, some with less?



Modeling the Internet's Topology

- The connectivity profile likely follows a Power Law (or Zipf) distribution
  - many nodes have few connections (on the edge?)
  - few nodes have many connections (in the core?)
  - if *d* is the degree of a node (# connections), then
    $p(d>x) \approx kx^{-\alpha}$ ("scale-free" networks)
  - however, this does not necessarily imply that there are a few highly connected nodes in the core of the Internet which would become "choke points"

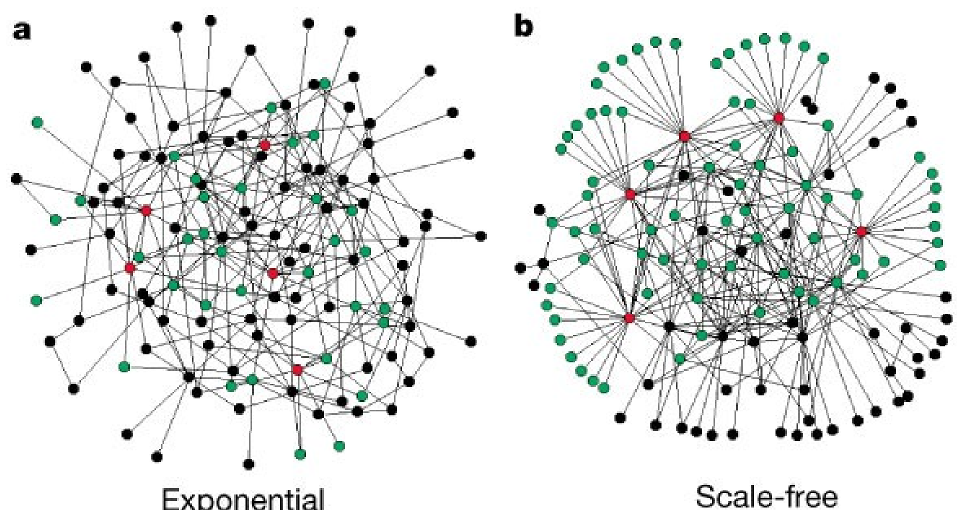




www.crossway.org

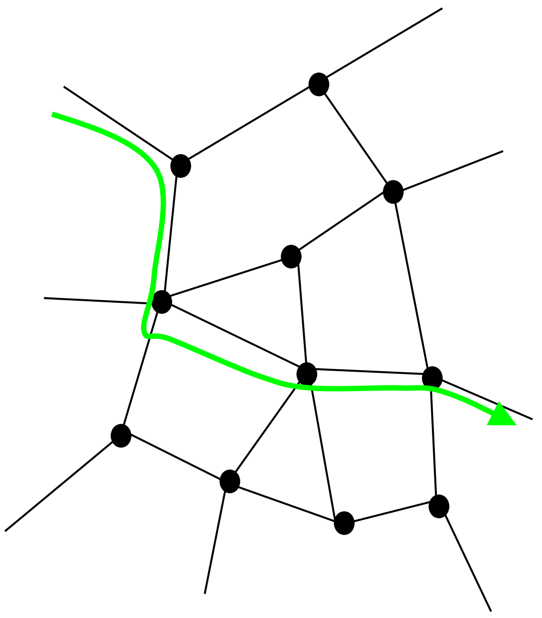
Modeling the Internet with Random Networks

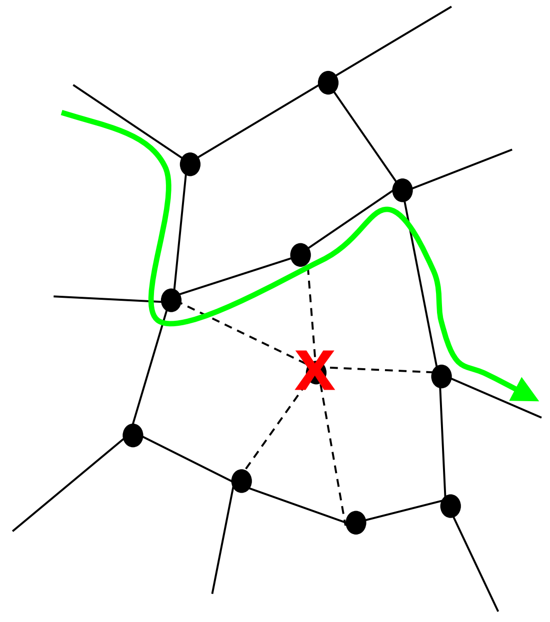
- Preferential Attachment (PA) model
  - new nodes probabilistically connect to popular nodes
- Constrained Optimization (CO) model
  - when a cable/router reaches capacity, add another
- both of these generate "scale-free" topologies
- however, CO has much better performance



http://www.nature.com/nature/journal/v406/n6794

“The Net routes around damage”

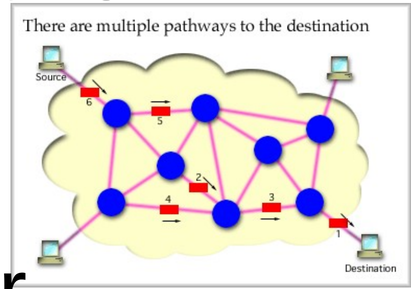




the adjacent nodes just
update their router tables

What about Internet Congestion?

- the packet-switched design solves this
- packets can take multiple paths to destination and get re-assembled

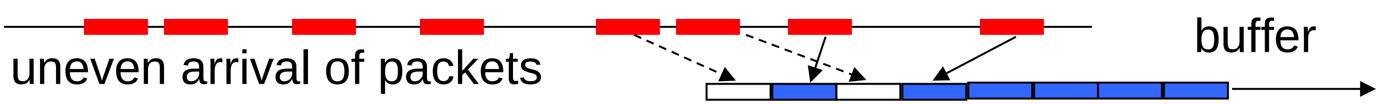


- if one router gets overloaded, buffer overflow messages tell neighbors to route around it
- also TCP/IP “back-off” algorithm
  - monitors throughput of connections and adjusts transmission frequency adaptively
- thus the Internet is amazingly robust, adaptive, and fault tolerant by design

Streaming

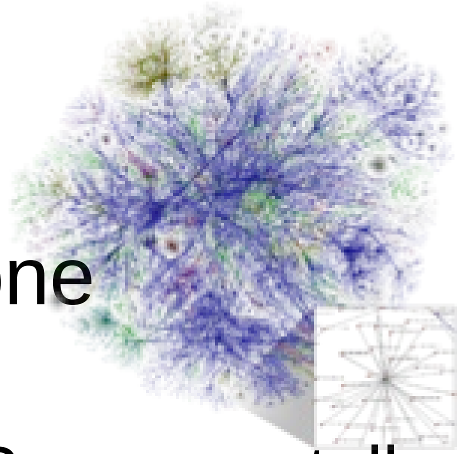
- Netflix, Pandora
- VOIP (voice-over-IP, Skype)
- video-conferencing
- multi-casting (Olympics)
- <u>dither</u> and <u>jitter</u>
- use *lossy compression* to adjust stream to end-to-end bandwidth
- use *buffering* to smooth out arrival of packets delayed and out-of-order
- intermediate servers staged for local distribution (e.g. Akamai)
- quality-of-service guarantees (QoS)

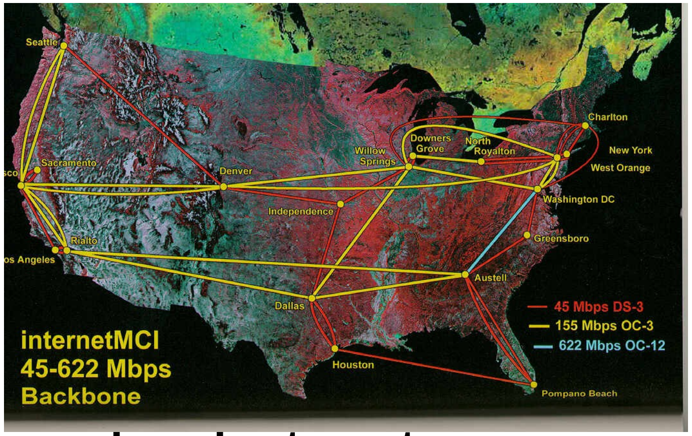
images from:
pagetutor.com/
imagecompression



even
play-
back

- Access speed is determined by service provider (bandwidth of connection, e.g. dialup to T1)





- Internet backbone
  - who owns it?
  - who controls it? can you tell somebody to stop streaming or hogging all the bandwidth? (the cable and phone companies would like to!)
- *Net Neutrality*
  - public policy issue; major economic impact
  - service providers cannot discriminate based on user, content, packet type or destination, similar to highways

Wireless/Mobile

- replace Ethernet (IEEE 802.3) with 802.11
- transport protocol (TCP/IP) and higher layers in stack remain the same
- issues
  - dynamic IP address assignment (DHCP)
    - ask router for temporary unique IP address
  - new nodes may join or leave anytime
  - roaming – device might change from one receiver/cell to another, take IP with it? causes changes in routing tables?
  - security – encrypt packets sent over the air