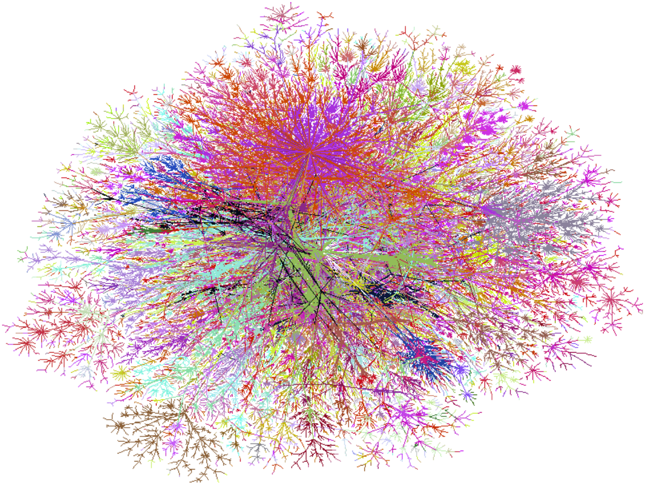
The Internet and its Architecture

Daniel Zappala

CS 360 Internet Programming
Brigham Young University

The Internet



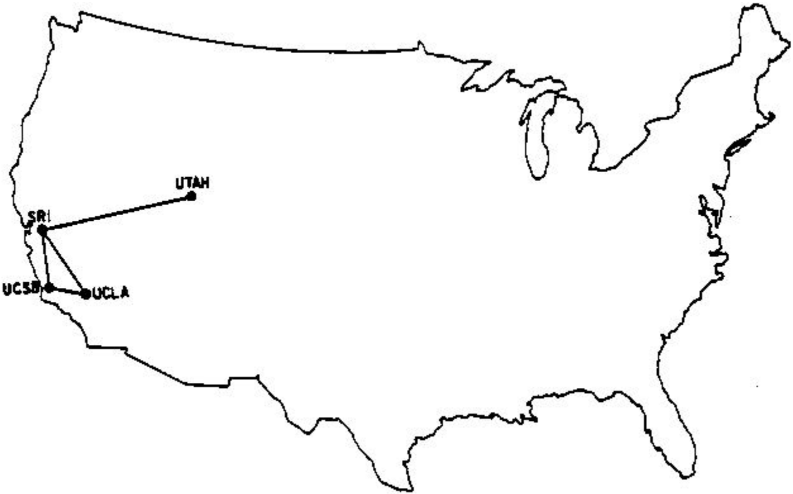
Internet Mapping Project, Bill Cheswick

Internet Map

Interactive Tool

The Beginning

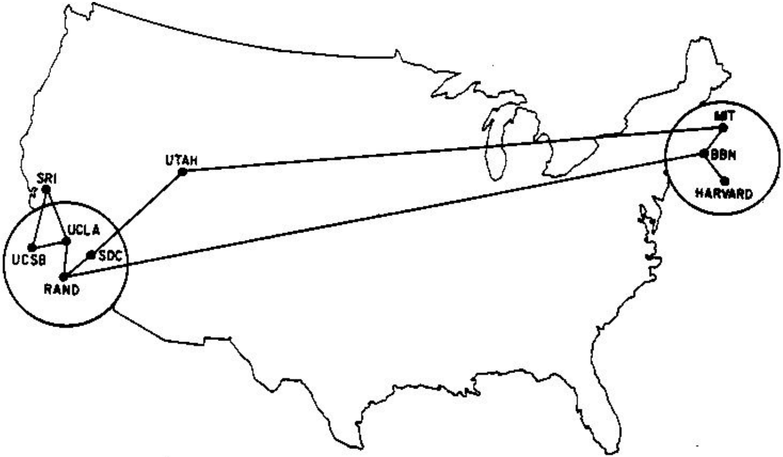
Arpanet Maps



December 1969

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

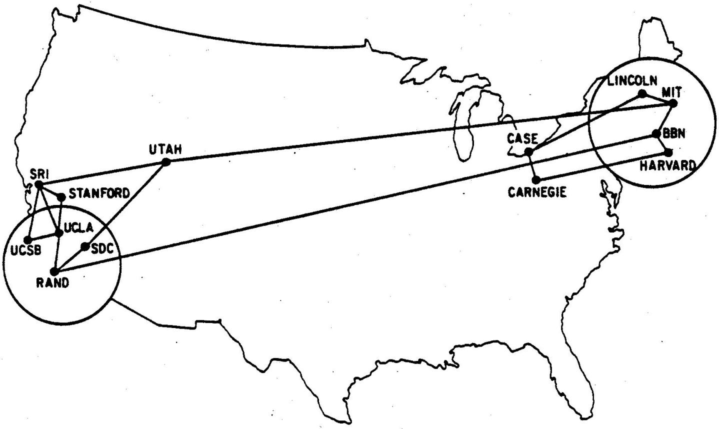
Arpanet Maps



June 1970

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

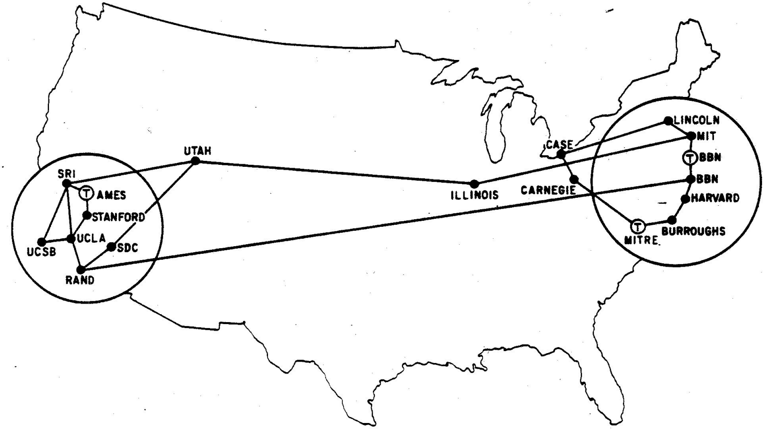
Arpanet Maps



December 1970

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

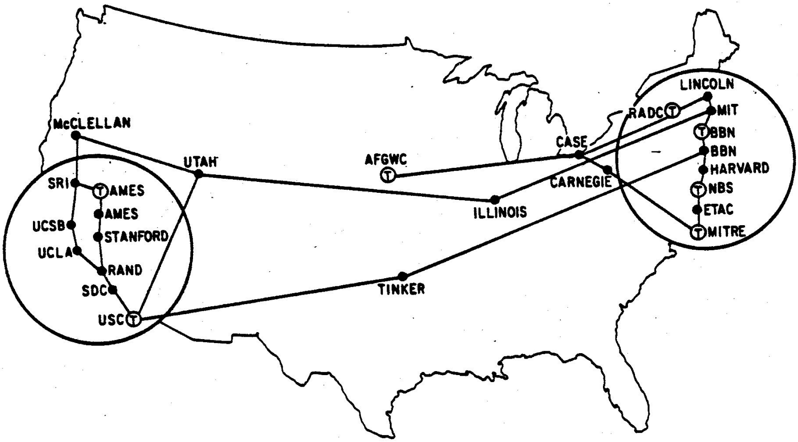
Arpanet Maps



September 1971

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

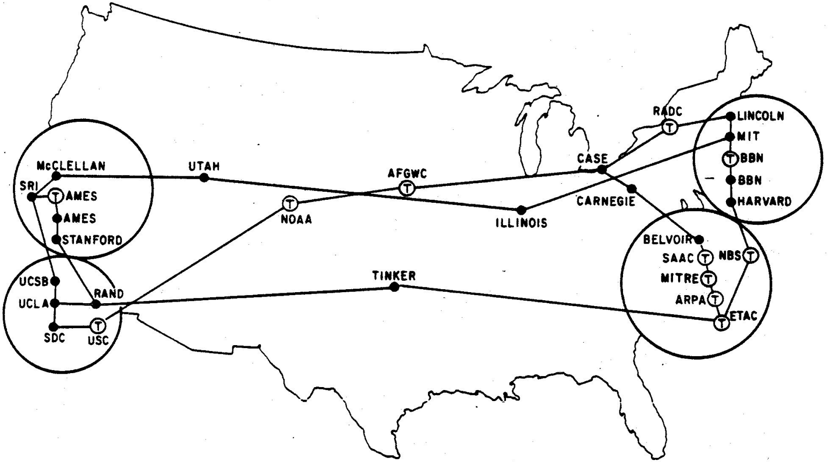
Arpanet Maps



March 1972

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

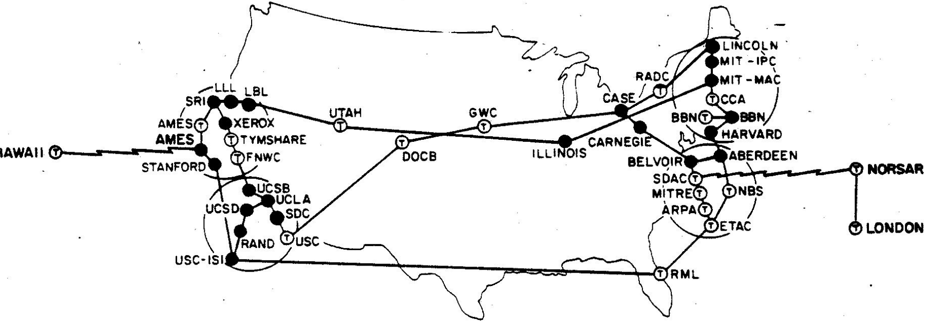
Arpanet Maps



August 1972

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

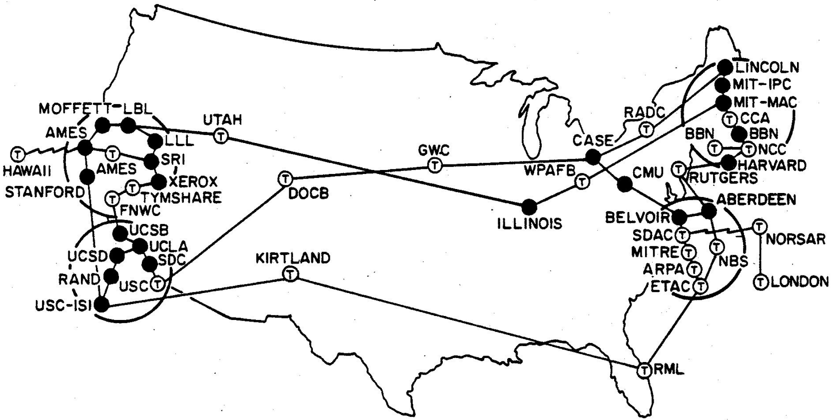
Arpanet Maps



September 1973

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

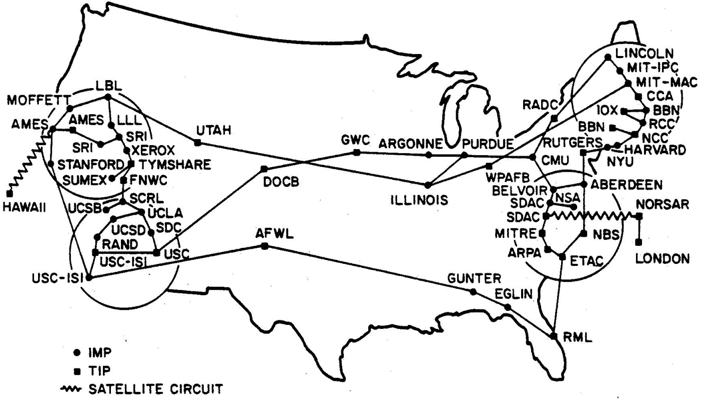
Arpanet Maps



June 1974

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

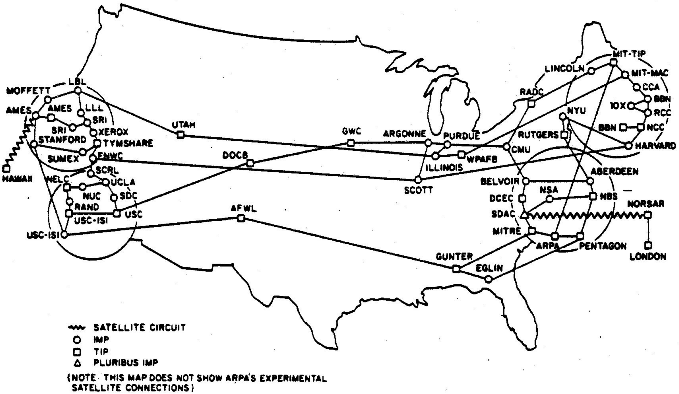
Arpanet Maps



July 1975

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

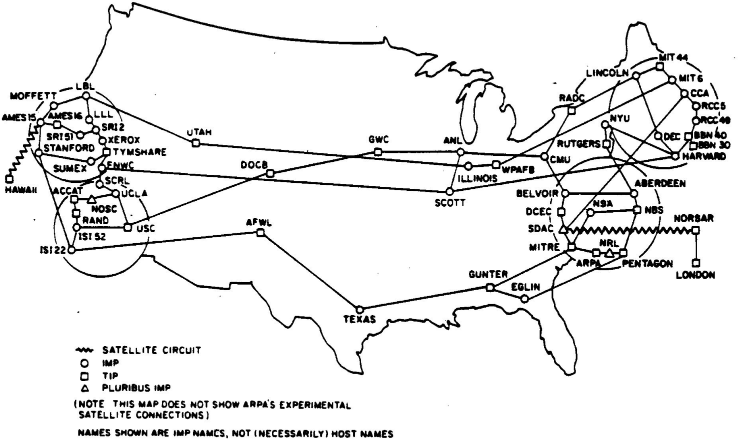
Arpanet Maps



July 1976

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

Arpanet Maps

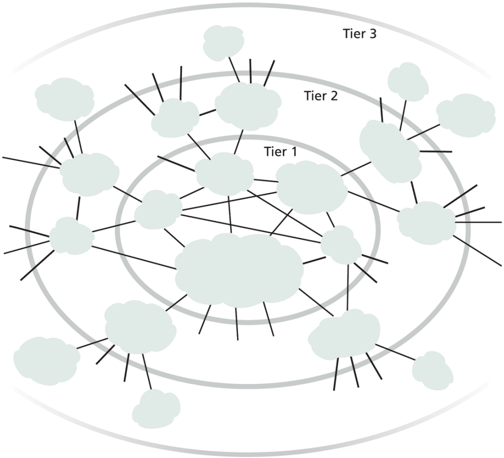


July 1977

Heart, McKenzie, McQuillian, and Walden, ARPANET Completion Report, BBN, 1978

Today

A Network of Networks

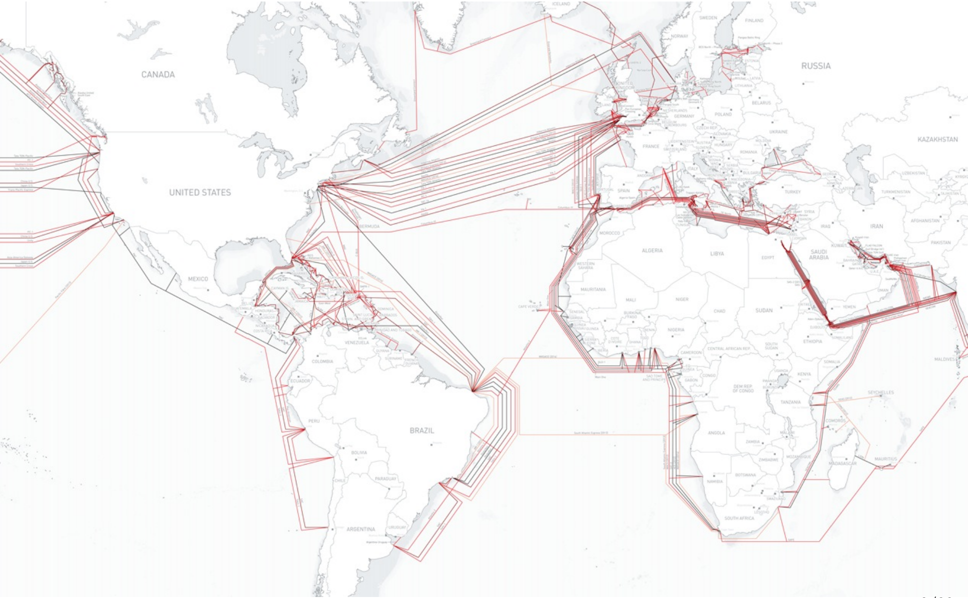


- roughly hierarchical
  - Tier-1 ISPs provide national, international coverage
  - Tier-2 ISPs provide regional coverage
  - Tier-3 and lower levels provide local coverage
- any tier may sell to business and residential customers
- any ISP may have a link to any other ISP (not strictly hierarchical)

Level 3 Tier-1 Map

▸ Interactive Map

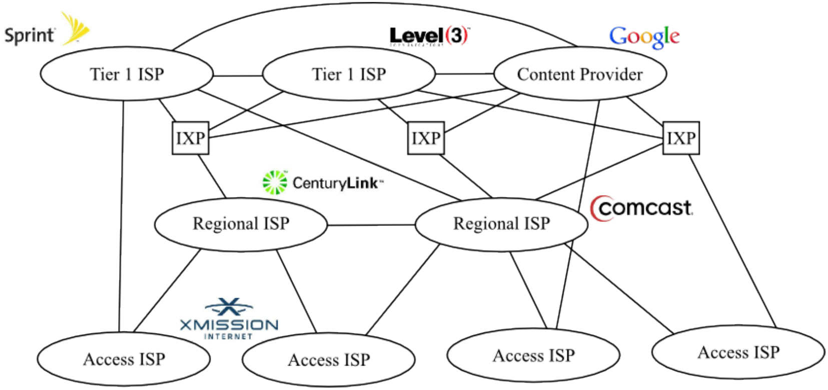
Submarine Cable Map



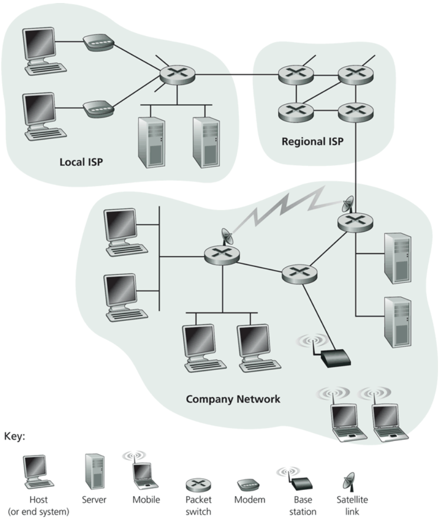
Additional Complexity

- PoP (Point of Presence)
  - router(s) in the provider's network where customer ISPs can connect
- multi-homing
  - customer ISPs may connect to more than one provider, for fault tolerance
- peering
  - connect directly to another ISP at the same level, instead of going through a provider, usually without any cost
- IXP
  - third-party location where ISPs can peer with each other
- content provider networks
  - large content providers (e.g. Google) have large networks, connect directly to lower-level ISPs and IXPs

Internet Structure



Many Different Internet Service Providers



- Each network is independent
- Interoperability requires using Internet standards: IP, TCP
    - the <u>Internet</u> is global and must run these standards
    - your private <u>intranet</u> can do whatever you want it to do

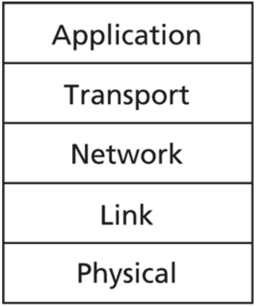
The Key to Making it all Work

Standardization

- standards are essential to interoperability on the Internet
- Internet Engineering Task Force *www.ietf.org*
  - standardizes Internet protocols: IP, TCP, HTTP, etc
  - open to all to participate, free of charge
  - relies on working code and rough consensus
- W3C *www.w3c.org*
  - standardizes web protocols and formats
  - industry-oriented consortium
  - requires approved and paid membership ($6,350 - $63,500 per year)
  - many standards do not require Internet-wide deployment

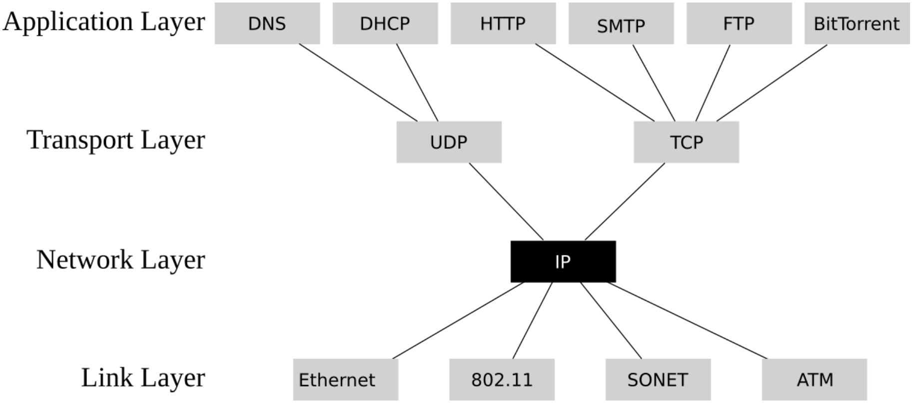
Internet Architecture

Internet Architecture

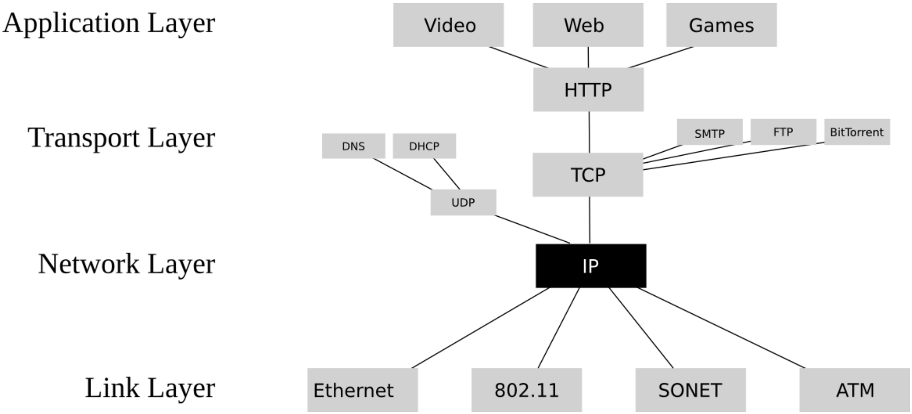


- an architectural model that separates communication protocols into layers
  - defines the functionality of each component and the interfaces between components
  - layering helps to build complex systems, like using modules to build large programs
- a particular implementation is free to combine layers or create new layers to create a more efficient or flexible system

The Internet Hourglass



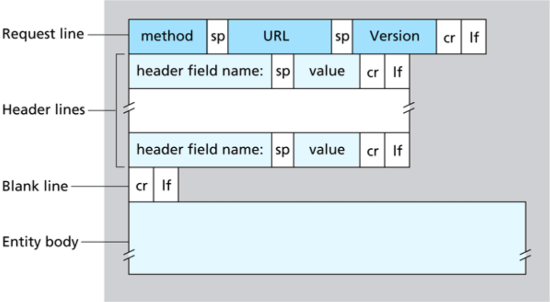
The HTTP Hourglass



Protocols

- a formal definition of how two or more entities communicate
- includes
    - format of messages
    - actions taken when a message is sent or received
    - actions taken when an event occurs

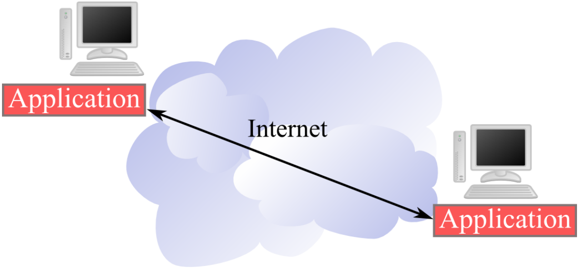
Protocol Example



- HTTP Request message format
  - sent in ASCII format
  - *request line*: method, URL, version
  - *header lines*: additional method parameters
  - ends with a carriage return and line feed
- actions: what happens when a server gets a request?

The Layers

Application Layer

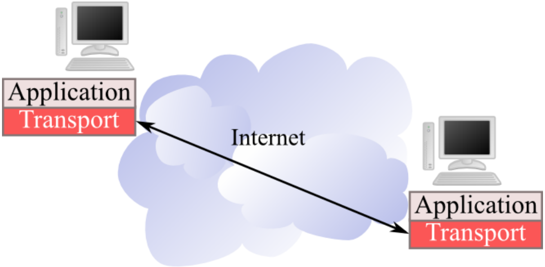


- the focus of this class: client-server, peer-to-peer, web apps
- important topics
  - design
  - concurrency
  - performance evaluation
  - security
- use socket API to access transport protocols

Application Layer Services

- query-response: basic services
    - DHCP
    - DNS
- client-server communication: a server provides a service to clients
    - web
    - video and audio streaming
    - email
    - file transfer
- peer-to-peer communication: host collaborate to share content, acting as both clients and servers
    - Gnutella (and variants): file searching and sharing among peers
    - BitTorrent: file distribution from a well-known source
    - Coral: peer-to-peer web caching

Transport Layer

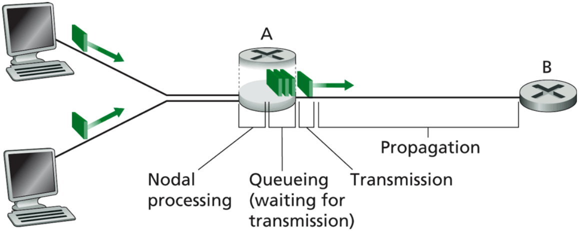


- delivers data between hosts on the Internet
- treats the Internet as a service that provides a virtual, but unreliable link between two computers

Transport Layer Services: TCP

- connection-oriented: requires state setup at sender and receiver
- provides a reliable, ordered byte stream
  - reliable: retransmits any segments that are lost
  - ordered: buffers and re-orders segments before delivery to application
  - byte stream: transfers bytes, not messages
- provides flow control: avoid overflowing the receiver's buffer
- provides congestion control: avoid persistently overflowing network buffers
- applications: web, file transfer, remote login, email

Queues and Congestion Control

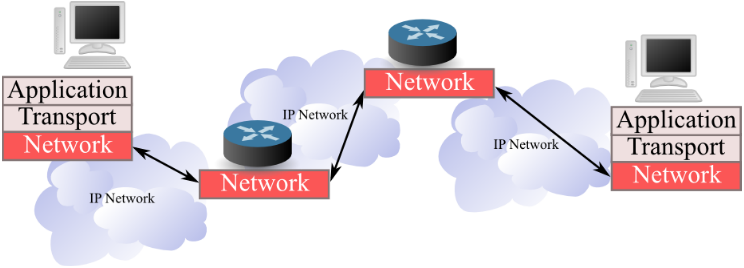


- delay is primarily caused by queueing
- loss is caused by queue overflow
- both are signs of congestion
  - packets are arriving faster than they can be serviced
  - delay and loss are signals to TCP congestion control algorithm – slow down
  - **the Internet needs congestion control to avoid persistent queue overflow**
  - fundamental control problem

Transport Layer Services: UDP

- connectionless: no state setup
- unreliable: lost packets are not re-sent
- no flow control
- no congestion control
- applications: query-response (DNS, DHCP), streaming media (voice, video), some peer-to-peer protocols

Network Layer



- forwards packets between computers and routers on the Internet

Network Layer Services: IP

- common protocol needed to interoperate with other computers on the Internet
- data from transport layer is divided into packets (about 1.5 KB) and sent individually
- implements a best-effort service model - routers make their best effort to deliver all packets, but packets may be
  - delayed (long queues in the network)
  - dropped (queue overflow)
  - duplicated (mistaken retransmission by TCP)
  - re-ordered (packets may take different paths)
- reliability and ordering are the responsibility of TCP

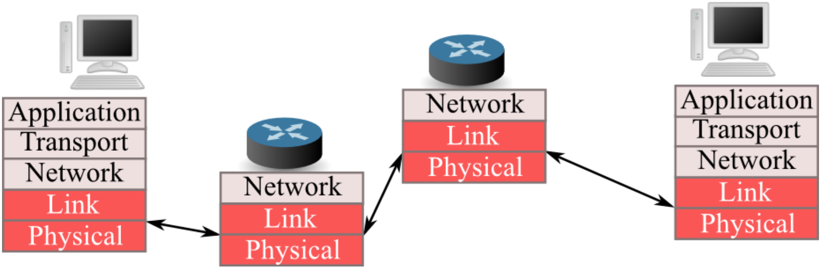
Host Names and Internet Addresses

- hosts can have one or more names
- each name can be associated with one or more addresses
- 32 bits, written in *dotted decimal form*
  - byu.edu: 128.187.16.167
  - google.com: 74.125.127.99, 74.125.127.103, 74.125.127.104, 74.125.127.105, 74.125.127.106, 74.125.127.147
- the Domain Name System DNS maps names to addresses
- a network is a group of hosts with the same prefix
  - 128.187.16.167 with a netmask of 128.187.16.167
  - 128.187.0.0
  - 128.187/16

Network Layer Services: Routing

- routing protocols decide which path to use when sending packets to a given destination
  - organized hierarchically: BGP in the backbone, anything you want (OSPF, IGRP, RIP) in your own network
  - choose the best path for each destination and tell the router to use this path
- primary goals
  - stability: paths must not change too often
  - scalability: must handle every possible destination on the Internet
  - policy: allow network adminstration to choose paths based on economic agreements between providers
  - security: prevent unauthorized re-routing and other attacks
- **scalable routing is currently a major concern for the Internet**

Link and Physical Layers



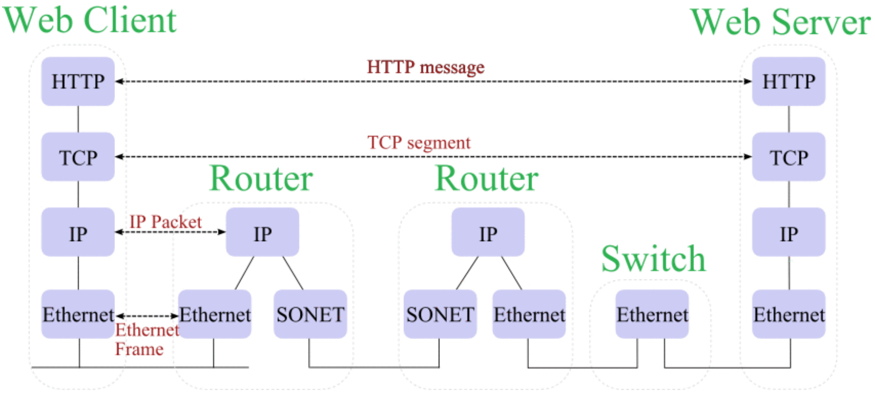
- link layer: sends a frame on one link
- physical layer: sends bits on one link

Types of Links

- key features
  - bandwidth - number of bits that can be transmitted per second, measured in bps, Kbps, Mbps or Gbps
  - latency - the time it takes to propagate a bit down a link
  - shared vs dedicated resources
- examples
  - modem: $<$ 56 Kbps
  - DSL: 256 Kbps up / 1 Mbps down (example)
  - Cable Internet: 2 Mbps up / 10 Mbps down, shared (example)
  - Ethernet: 10 - 1000 Mbps, shared or dedicated
  - wireless: wide range of bandwidths (54 Mbps for 802.11g), shared or dedicated with directional antenna

Putting it Together

The Internet at each Hop



Security

Why is the Internet so Vulnerable to Attacks?

- The Design Philosophy of the DARPA Internet Protocols, Clark, 1988
- fundamental goal
  - develop an internetwork for existing networks
- second-level goals
  1. survivability
  2. multiple types of service (delay vs bandwidth, reliable vs datagram)
  3. variety of networks
  4. distributed management
  5. cost effective
  6. host attachment with low effort
  7. accountable resources

Security Was Not Considered

Cat And Mouse

- security is a bandaid for the Internet
- constant game of cat and mouse
- numerous attacks
  - malware (e.g. viruses, worms) to create botnets
  - denial-of-service attacks (DoS, DDoS)
    - exploit vulnerabilities
    - bandwidth flooding
    - connection flooding
  - packet sniffing
  - IP spoofing
  - ...and many more