Networked System Security

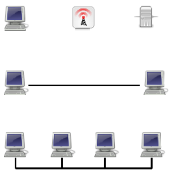
Introduction to Networking

Module TA: **Stylianos Gisdakis**, gisdakis@kth.se

Panos Papadimitratos
Networked Systems Security
http://www.ee.kth.se/nss

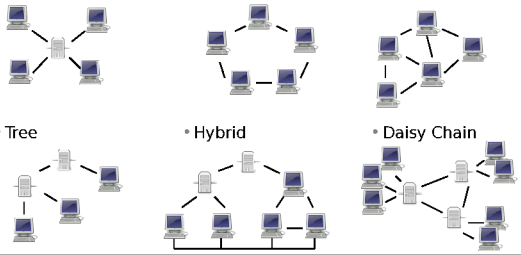
Networks

- System of lines / channels / links that interconnect
  - E.g. Railroad, highway, plumbing, power grid, telephone, computers
- Computer Network
  - Nodes:
    - Computers, routers, switches
  - Links
    - Point-to-point
      - Cables, twisted pair, fiber
    - Multiple access (Bus)
      - Coaxial cable, radio frequencies

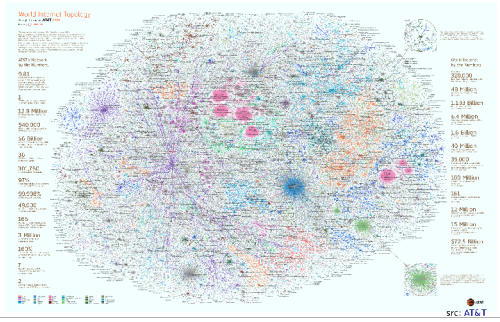


Network Topologies

- Star
- Ring / Circular
- Mesh
- Tree
- Hybrid
- Daisy Chain



Internet



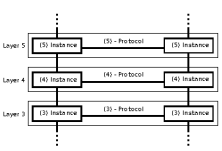
Networking

- Communication between two ends across the network
  - Alice wants to exchange information with Bob

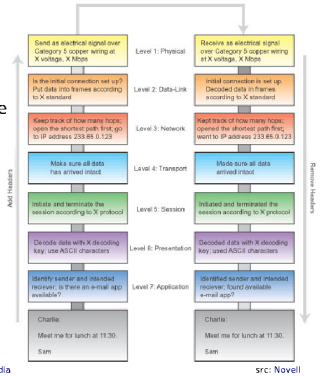
- Knowledge of:
  - Where is Bob
  - How to reach him
  - How to talk with him
  - How to establish the link

Protocols

- Standard way to communicate
- Network is heterogeneous
- Agreements between ends
- Different layers



src: wikipedia



src: Novell

Layers

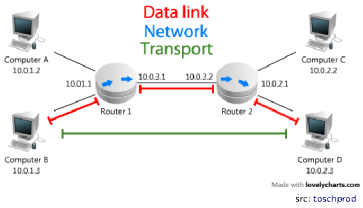
1. Physical
   - Send bits over a physical link
   - Connects 2 devices directly, using:
     - Cables
     - Radio waves
     - Light
2. Data Link
   - Send frames over the physical link
   - Handle access to the medium

src: hyperline.com

src: xtremecomputers

Layers (cont'd)

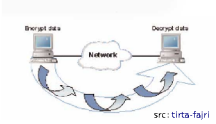
3. Network
   - Delivers packets
   - Route
4. Transport
   - Transmit segments
   - Can provide reliability
   - Flow control



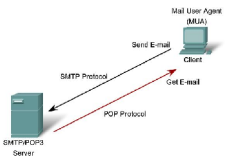
src: toschprod

Layers (cont'd)

5. Session
   - Can tie together multiple streams
6. Presentation
   - Conversion between representations
   - Encryption
7. Application
   - Interface to the End User



src: tirta-fajri

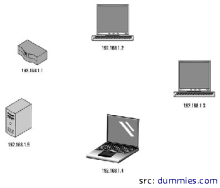


Clients send e-mails to a server using SMTP and receive e-mails using POP3.

src: itcebuadministrator

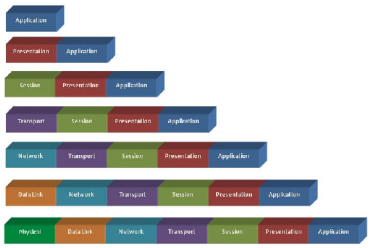
Addresses

- Each node has an unique address (identifier)
- Each layer can have its own addressing
  - Link layer: e.g. 48-bit Ethernet address (interface)
  - Network layer: 32-bit / 128-bit IP address (node)
  - Transport layer: 16-bit TCP port (service)
- Special addresses for groups of nodes



src: dummies.com

Encapsulation



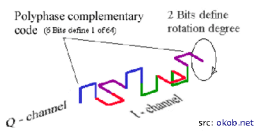
OSI Model Packet Encapsulation

src: k2esec.com

Physical Layer

- Describes:
  - Physical medium
    - Category 5 cable
    - WiFi 2.4 GHz
  - Signal
    - Pulse amplitude modulation
    - Phase shift keying (BPSK, QPSK)
  - Bit encoding
    - 4-to-6 bit-to-chip, 3 chip symbols
    - Baker code, complementary code keying
- Channel Capacity (Shannon)

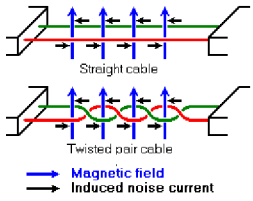
  $C = B \log_2(1 + S/N)$
  - B is the bandwidth
  - S and N average signal and noise



src: okob.net

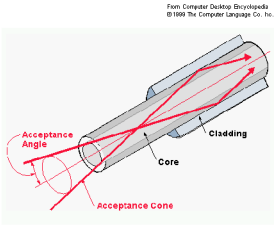
Physical Layer: Cable

- Twisted Pair



src: lammertbies.nl

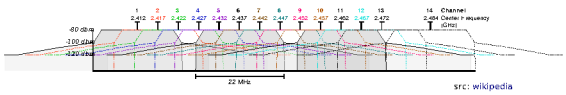
- Optical Fiber



Physical Layer: Wireless

- Electromagnetic spectrum
  - Licensed (GSM, television)
  - Industrial, Scientific and Medical (ISM) band (WiFi)

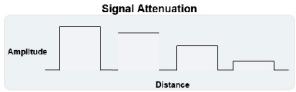
- E.g. WiFi



src: wikipedia

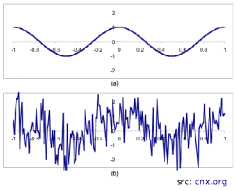
Physical Layer: Wireless (cont'd)

- Signal attenuation
  - Depends on the distance
  - Fading



src: learn-networking.com

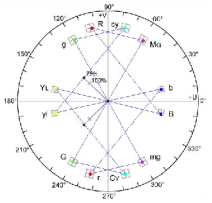
- Background noise



src: cnx.org

Physical Layer: Wireless (cont'd)

- Mitigation
  - Multiple channels
  - Use robust coding
    - Easily recognizable symbols
    - 1 symbol = multiple bits
  - Redundancy



src: wikipedia

Data Link Layer

- Single-hop addressing

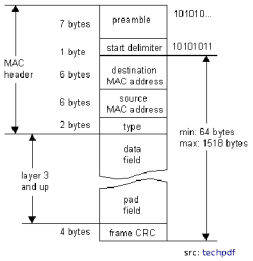
- Media access control
  - Link-layer congestion control
  - Multiple access
  - Collision Detection / Collision Avoidance

src: hill.com

Ethernet: IEEE 802.3

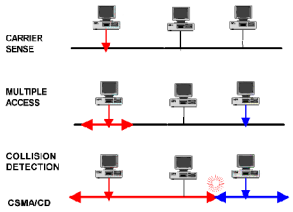
- Frame Header:
  - Preamble: *syncword*
  - Destination and source addresses
  - Type or Length of the Payload
- Frame Trailer:
  - Frame checksum
  - Interframe gap

- Addressing:
  - Each card has unique 48-bit ID
  - Half (24-bit) is organizationally fixed
    - http://standards.ieee.org/develop/regauth/oui/oui.txt



src: techpdf

Ethernet: IEEE 802.3 (cont'd)

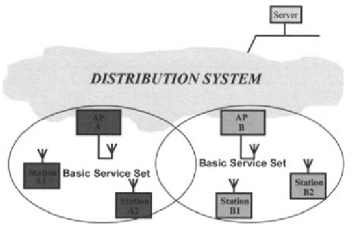


src: payer

- When a node detect a collision:
  - Broadcasts jam signal
  - Other nodes drop the frame
- Protocol constrains:
  - Minimum packet size
  - Maximum network size

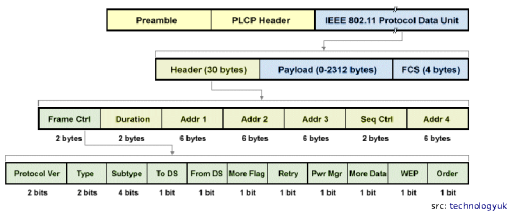
WiFi

- Distribution System
- Basic Service Set
- Access Point
- Stations / Nodes



src: flylib

WiFi: IEEE 802.11a/b/g/n

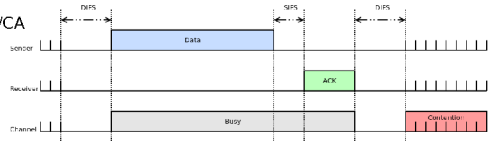


src: technologyuk

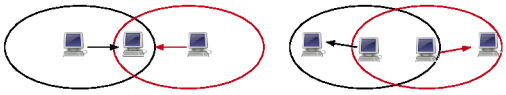
- Different (PHY Layer Convergence Procedure) PLCP a/b/g/n header
- Same addressing as IEEE 802.3
- 4 Address to include traversing different Distribution Systems

WiFi: Medium Access

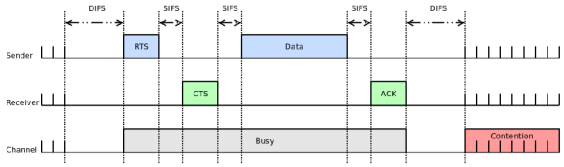
- CSMA/CA



- Hidden Terminal / Exposed Terminal



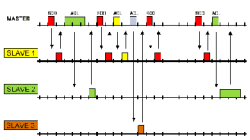
WiFi: Medium Access (cont'd)



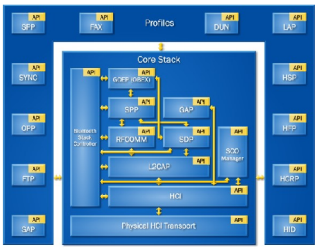
- Request To Send / Clear To Send
- Network Allocation Vector (NAV)
- Allocate the channel for usage nearby the sender and the receiver
  - Reduced Hidden and Exposed terminal problems

Bluetooth

- Frequency Hopping Spread Spectrum (FHSS)
  - Rapidly switching a carrier
  - Resistant to interference



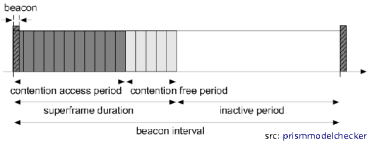
src: swedetrack



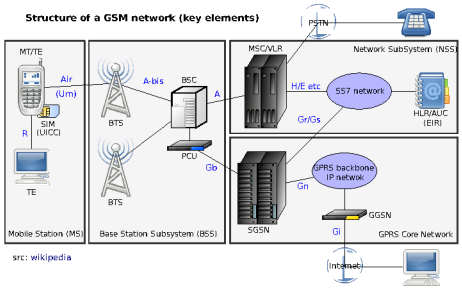
src: stonestreetone

IEEE 802.15.4: ZigBee

- Duty Cycled
- Time Slotted
- Beaconing

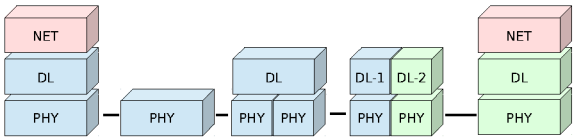


Global System for Mobile Communications (GSM)

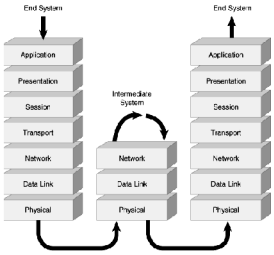


Interconnections

- Hub
  - Replicate or repeat the signal
- Switches
  - Connects two different segments
- Bridges
  - Interconnect different data links



Network Layer

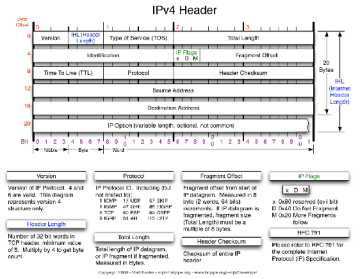


src: sheetudeep

- Connectionless communication
  - Packet travels from source to destination without ACK
- Host addressing
  - Unique address
  - Determines the location
  - Hierarchical
- Message forwarding
  - Intra-network
  - Inter-networks

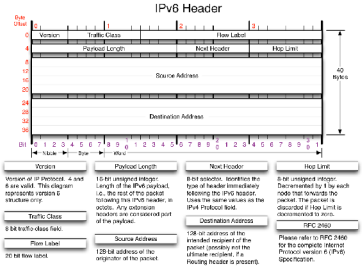
Internet Protocol (v4)

- Network is unreliable
- Best effort delivery
- Addresses:
  - 32-bit: exhaustion
  - Private address:
    - 10.*.*.*
    - 172.31.*.*
    - 192.168.*.*
  - Network Address Translation (NAT)



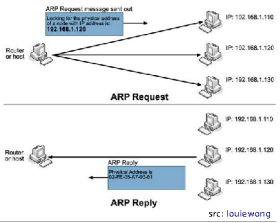
Internet Protocol (v6)

- Introduces features
  - Address assignment
  - Simplified processing by routers
- Mobility
- Extensibility
- Integrates network security
- Addresses:
  - 128-bit → 3.4×10^{38}



Address Resolution Protocol (ARP)

- Resolution of *network* layer addresses into *link* layer addresses
- Operates inside the single network
- Broadcast (request):
  - Who has IP x.x.x.x tell y.y.y.y
- Unicast (reply):
  - x.x.x.x is at z:z:z:z:z:z
- Proxy ARP
  - Used by switches

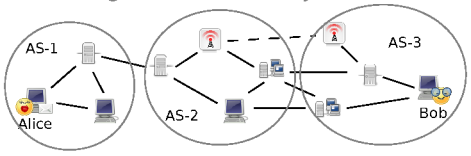


src: louiewong

Routing

- Connection between neighbors
  - How to send data directly to the next hop
- How to forward the message to Bob?

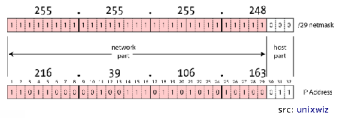
Routing: Autonomous Systems (AS)



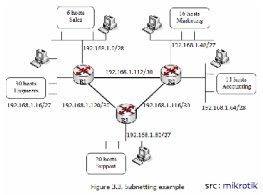
- AS: set of interconnected networks under common administration
- Intra-Domain Routing:
  - Send packets within the AS
  - Examples
    - Routing Information Protocol (RIP)
    - Open Shortest Path First (OSPF)
- Inter-Domain Routing:
  - Send packets across multiple ASes
  - Examples
    - Border Gateway Protocol (BGP)

Routing: Subnets

- Network mask
  - 32-bit mask
  - Separate host and network



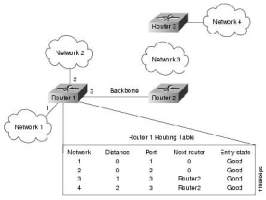
src: unixwiz



src: mikrotik

- Subnets
  - Internal hosts Common most-significant bit-group address
  - Hierarchical
  - Can be aggregated
  - Traffic is routed by *routers*

Routing: Table

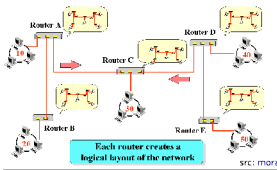


src: Cisco

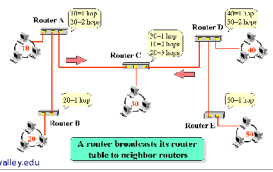
- Information of
  - Destination Network ID
    - Network Destination
    - Netmask
  - Link identification
    - Physical port
    - Next hop / gateway
  - Metric associated to the link
    - Cost
    - Number of hops

Routing: Build the table

- Link state routing (OSPF)
  - Global view
  - Flood all nodes
  - Send info of connected links
  - Dijkstra's algorithm



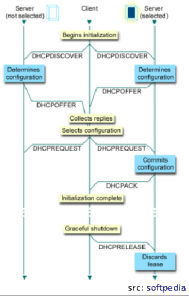
- Distance vector routing (RIP)
  - Local view
  - Exchange data with neighbors
  - Send info of reachable nodes
  - Bellman-Ford algorithm



src: morainevalley.edu

Dynamic Host Configuration Protocol (DHCP)

- Automatize the configuration of:
  - Local IP address
  - Subnet Mask
  - Gateway
  - Name Servers
  - ...
- Built for IPv4, valid also for IPv6
  - DHCPv6
  - Stateless Address Autoconfiguration
    - Using Neighbor Discovery Protocol

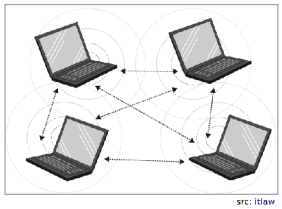


src: softpedia

Ad Hoc Networks

- Decentralized
- Multi-hop
- Each node helps to forward data
- Re-think routing protocol

- Applications:
  - Mobile Ad-hoc Network (MANET)
    - E.g Vehicular networks
    - Routes changes due to mobility
  - Wireless Sensor Network (WSN)
    - Monitoring
    - Energy / Hardware constrains



src: itlaw

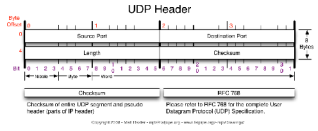
Transport Layer

- *"The network's job is to transmit datagrams as efficiently and flexibly as possible. Everything else should be done at the fringes."*
  – [RFC 1958]

- Datagram
  - Connection-less
  - Unreliable
  - Unordered
- Stream
  - Connection-oriented
  - Reliable
  - Ordered

User Datagram Protocol (UDP)

- Unreliable and unordered datagram service
- Endpoints identified by ports
- Checksum aids in error detection
- Lightweight, minimal, direct interface with IP, low latency
- No congestion control

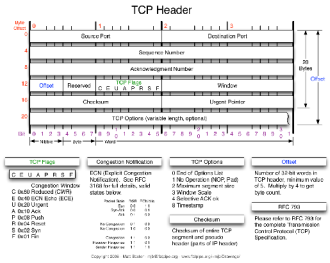


- Applications
  - Single request/response
    - RIP, DHCP
  - No loss constrain
    - Voice / Video streaming

Transmission Control Protocol (TCP)

- Reliable (acknowledgment)
  - Retransmission of lost data
- Ordered (sequence num)
  - Delay for ordering
- Connection-oriented
  - Handshaking
- Congestion and flow control
- Higher latency
- Full duplex

- Applications
  - Almost everything else



TCP: Handshaking

- Connection Opening
  - 3-way handshaking
- Connection Closing
  - 4-way handshaking

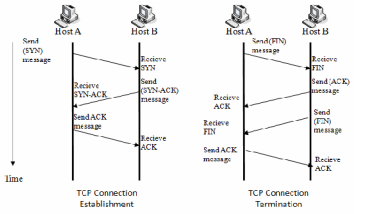


Figure 2.1. TCP session establishment and termination src: mikrotik

TCP: Flow and Congestion Control

- Avoid to outrun the receiver
  - Flow Control
    - Sliding Window
- Avoid to overflow the network
  - Congestion control
    - Slow-start
    - Congestion avoidance
    - Fast retransmit
    - Fast recovery

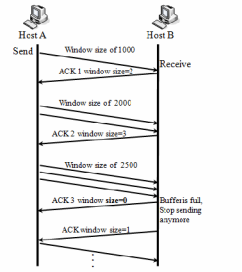
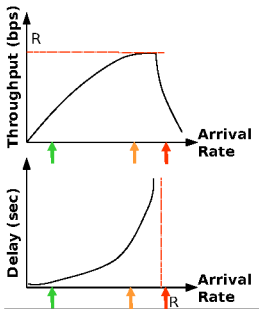


Figure 2.2. TCP flow control using *windowing*
src: mikrotik

TCP: Congestion



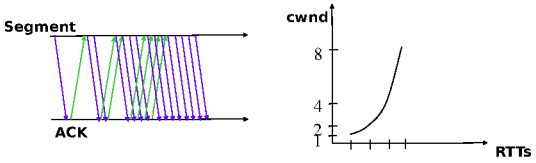
Light traffic
- Arrival rate << R
- Low delay
- Can accommodate more

Congestion onset
- Arrival rate approaches R
- Delay increase rapidly
- Throughput begins to saturate

Saturation
- Arrival rate > R
- Large delays, packet loss
- Useful application throughput drops

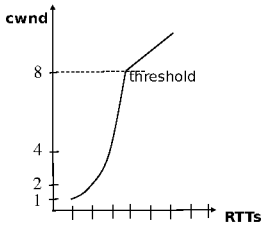
TCP: Congestion (cont'd)

- Slow Start
  - Increase congestion window size (**cwnd**) by one segment for each received ACK
  - Congestion window increase exponentially



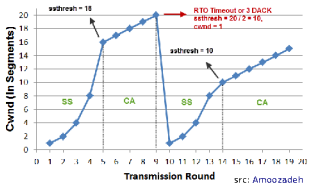
TCP: Congestion (cont'd)

- Congestion avoidance
  - Progressively sets a *congestion threshold*
    - When cwnd > threshold, increase cwnd slowly
  - Cwnd++ per round-trip-time (RTT)
    - Each time an ACK arrives, cwnd is increased by 1/cwnd
    - In one RTT, cwnd segments are sent, so total increase in cwnd is cwnd x 1/cwnd = 1
    - Cwnd grows linearly



TCP: Tahoe

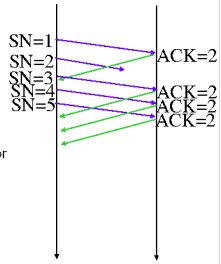
Congestion Onset
- Congestion detection:
  - Timeout or
  - Receipt of duplicate ACKs
- Assumption: current cwnd corresponds to available bandwidth
- Adjust congestion threshold = ½ (current cwnd)
- Reset cwnd to **1**
- Go back to slow-start
- Over several cycles expect to converge to congestion threshold equal to about ½ the available bandwidth



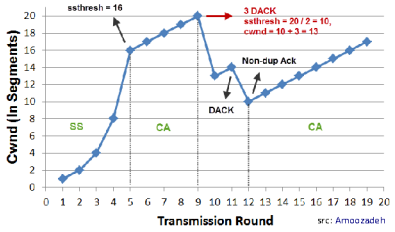
src: Amoozadeh

TCP: Reno

- Congestion causes many segments to be dropped
- If only a single segment is dropped, then subsequent segments trigger duplicate ACKs before timeout
- Can avoid large decrease in cwnd as follows:
  - When three duplicate ACKs arrive, retransmit lost segment immediately
  - Reset congestion threshold to ½ cwnd
  - Reset cwnd to congestion threshold + 3 to account for the three segments that triggered duplicate ACKs
  - Remain in congestion avoidance phase
  - However if timeout expires, reset cwnd to 1
  - In absence of timeouts, cwnd will oscillate around optimal value
- Fast Recovery

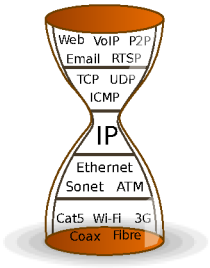


Fast Retransmit & Fast Recovery



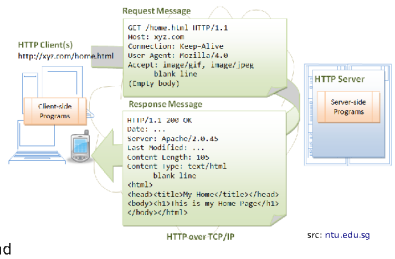
Application Layer

- Web browsing
  - Hypertext Transfer Protocol (HTTP)
    - Domain Name System (DNS)
- Remote Shell
  - Telnet
  - Secure Shell (SSH)
- File sharing
  - Network Filesystems
  - BitTorrent
- Messaging / Video
  - Simple Mail Transfer Protocol (SMTP)
  - Skype
- ...



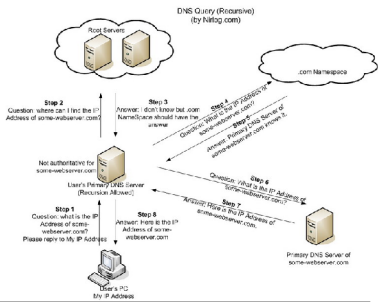
Hypertext Transfer Protocol (HTTP)

- Client / Server architecture
- Distributed
- Collaborative
- Hypermedia based
- Request Methods
  - GET, POST, PUT...
- Response Codes
  - 200 OK, 404 Not found

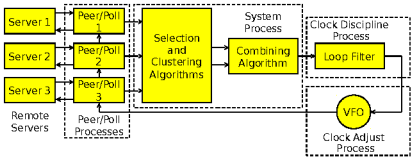


Domain Name System (DNS)

- Uniform Resource Locator (URL)
  - http://xyz.com/home.html
- How to translate it into an IP Address?
- DHCP gives also:
  - Name (DNS) server IPs



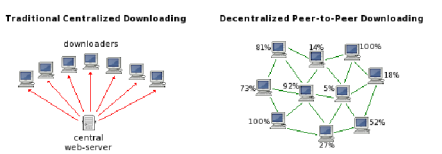
Network Time Protocol (NTP)



- Multiple servers/peers provide redundancy and diversity
- Clock filters select best from a window of eight time offset samples
- Intersection and clustering algorithms pick the best discard false
- Combining algorithm computes weighted average of time offesets
- Loop filter and Variable Frequency Oscillator (VFO) for feedback loop

src: Mills, D.

Peer-to-Peer (P2P)



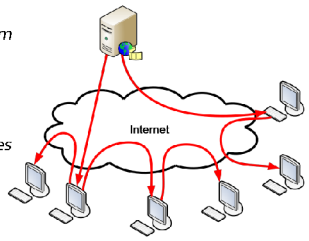
- Slow
- Single point of failure
- High bandwidth usage for server

- Fast
- No single point of failure
- All downloaders are also uploaders

src: tixati

P2P: Bittorrent

- File is divided in *pieces*
- Peers (nodes) constitute a *swarm*
  - Download data from each other
- Tracker
  - Coordinates the file distribution
  - Tells the peers who has the *pieces*



Summary