CS3611 Computer Networks (Spring 2023) Final Exam Cheat Sheet

Xiangyuan Xue (521030910387)

Pysical Media

Bit propagates in the form of electromagnetic waves or optical pulse. **Physical media** lies between transmitter and receiver.

guided media: signals propagate in solid media e.g. twisted pair, fiber optics, coaxial cable.

unguided media: signals propagate freely e.g. radio, atmosphere, outer space.

twisted pair: two insulated copper wires, adequate performance and low cost. UTP (unshielded twisted pair) category: CAT3 10 Mbps, CAT5 100 Mbps.

coaxial cable: high bandwidth, noise immunity, about 1 GHz rate. Baseband: single channel, legacy Ethernet. Broadband: multiple channels, HFC.

fiber optics: light pulses, wide bandwidth 10 THz, 10 to 100 Gbps, low error rate, ultra low attenuation, noise immunity.

radio: electromagnetic spectrum, no physical wire, reflection, obstruction and interference. Link types: terrestrial microwave (up to 45 Mbps), LAN e.g. WiFi (11 or 54 Mbps), wide-area e.g. cellular (up to 100 Mbps), satellite (up to 45 Mbps, 270 msec delay, geosynchronous versus low altitude).

Protocol Layers

A **protocol** defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and receipt of a message or other event. **Why layering?** For design complexity, independence and flexibility.

protocal: two parties at the same level agree on how they will exchange information.

service: one party apply the communication services offered by the layer directly underneath it.

interface: services are specified in terms of an interface which makes them accessible.

Service Models

The **hybrid model** includes 5 layers: application (message), transport (segment), network (datagram), link (frame), physical (bit). The switch includes 2 layers, the router includes 3 layers.

Network Edge

end systems (hosts): run application programs e.g. Web, Email, at edge of network.

client-server model: client host requests and receives service from always-on server e.g. Web browser, Email client.

peer-to-peer model: minimal or no use of dedicated servers e.g. Skype, BitTorrent.

connection-oriented service: with connection, prepare for data transfer ahead of time, set up state in two communicating hosts, based on TCP.

connectionless service: transfer data between end systems, no connection, based on UDP.

Network Core

Refer to mesh of interconnected routers.

circuit switching: dedicated circuit, end-end resources reserved for call (link bandwidth, switch capacity, dedicated resources, circuit-like performance, call setup required), network resources divided into pieces, allocated to calls, divide bandwidth (time or frequency).

packet switching: data sent through network in discrete chunks, each end-end data stream divided into packets (share resources, full bandwidth, as needed), resource contention: aggregate demand can exceed amount available (queue up), store and forward (packets move one hop at a time).

Network Core (Continued)

comparison: packet switching allows more users to use network, great for bursty data (resource sharing and simpler), but excessive congestion (packet delay and loss), more on delay shortly.

Delay, Loss, Throughput

loss: packet arrival rate exceeds link capacity, packets dropped if no free buffers.

delay: nodal processing (check bit errors, determine output link, lower than msec), queuing delay (waiting time, depends on congestion level), transmission delay (packet length / link bandwidth), propagation delay (distance / speed).

throughput: rate at which bits transferred between sender and receiver (instantaneous, average), constrained by bottleneck link.

bandwidth: the range of frequencies transmitted without being strongly attenuated. **data rate**: the rate at which bits can be transmitted. **Shannon's theorem**: $R = B\log_2(1 + S/N)$, R is data rate, B is bandwidth, S/N is signal-to-noise ratio.

Application Architectures

client-server, peer-to-peer (scalable but hard to manage), hybrid of client-server and peer-to-peer (e.g. instant messaging).

Sockets

processes communicating: inter-process communication within same host, exchanging messages in different hosts, peer-to-peer applications have both client and server processes.

Process sends or receives messages to or from its **socket**. **Identifier** includes IP address and port number associated with process.

HTTP (Hypertext Transfer Protocol)

application layer, client-server model, use TCP.

non-persistent HTTP: at most one object over a TCP connection, client initializes TCP connection, server accepts, client sends HTTP request, server forms HTTP response, connection closed. Response time: one RTT (Round Trip Time) for connection, one RTT for request and response, totally 2 RTTs plus transmission time.

persistent HTTP: server leaves connection open after response, subsequent messages sent over open connection, without pipelining, one RTT per object, with pipelining, one RTT for all the objects.

HTTP request message: ASCII, request line, header lines, carriage return, line feed, entity body. HTTP Method: GET, POST, HEAD, PUT, DELETE, etc.

HTTP response message: status line (200 OK, 404 Not found, etc), header lines, requested data.

FTP (File Transfer Protocol)

transfer file from remote host, client-server model, separate control and data connection, use TCP, port 21, one connection for one file transfer, maintain state (current directory, earlier authentication). FTP Command: USER, PASS, LIST, RETR, STOR. Return code: 331 Username OK, etc.

Cookies

keep **state**, composed of: header line of response and request messages, cookie file kept on user's host, back-end database at website. Bring authorization, shopping carts, recommendations, user session state. Require more user privacy.

Web Caches

To satisfy client request without involving origin server, also called **proxy server**. If object in cache, return object, else request object from origin server and return.

Why caching? reduce response time for client request, reduce traffic on institution's access link, enables poor content providers to deliver content.

DNS (Domain Name System)

distributed database implemented in hierarchy of many name servers, application layer, use UDP. **Why decentralized?** single point of failure, traffic volume, distant centralized database, not scalable.

DNS services: hostname translation, host aliasing, mail server aliasing, load distribution.

hierarchy: root name servers, top-level domain (TLD) servers (com, edu, etc), authoritative DNS servers (organization or service provider), local name servers (not strictly, act as a proxy).

query: iterative query, recursive query.

caching: learn and store mappings, timeout.

DNS records: RR format: (name, value, type, ttl). type A: name is hostname, value is IP address, type NS: name is domain, value is hostname of authoritative name server for this domain, type CNAME: name is alias name for real name, value is canonical name, type MX: value is name of mailserver associated with name.

DNS messages: query and reply message (same format), message header (identification, flags), questions (name, type), answers (resource record), authority, additional information.

Multiplexing, Demultiplexing

Multiplexing: gather data from multiple sockets, enveloping data with header. Demultiplexing: deliver received segments to correct socket (use IP address and port number). UDP socket identified by 2-tuple: (dest IP, dest port), different datagrams same socket. TCP socket identified by 4-tuple: (src IP, src port, dest IP, dest port).

RDT (Reliable Data Transfer)

rdt 1.0: reliable transfer. rdt 2.0: error detection, receiver feedback (ACK, NAK). rdt 2.1: 0/1 state, handle garbled ACK/NAK. rdt 2.2: no NAK, duplicate ACK as NAK. rdt 3.0: underlying channel packet loss, countdown timer, ACK timeout, low utilization, performance stinks.

piplined protocols: go-back-N (GBN): cumulative ACK, timer for oldest unACKed packet, when timeout retransmit all the packets in window, discard out-of-order packets. selective repeat (SR): individual ACK, timer for each packet, when timeout retransmit only the packet, buffer out-of-order packets, update window base when ACKed. **SR dilemma**: duplicate packet may be passed incorrectly due to ACK loss, seq number size should be at least twice the window size.

UDP (User Datagram Protocol)

connectionless, segments may be lost or delivered out of order. **Why UDP?** no connection establishment (delay), no connection state (simple), small header size, no congestion control (fast), streaming apps (loss tolerant, rate sensitive).

UDP checksum: treat content as 16-bit integers, sum up, wrap around, take complement.

TCP (Transmission Control Protocol)

segment structure: src port, dest port, seq number (first byte in data), ACK number (next byte expected, cumulative), checksum, options, data.

timeout value: slightly longer than RTT. $E = (1-\alpha)E + \alpha S$, $D = (1-\beta)D + \beta|S-E|$, $T = E + 4D$, S is sample RTT, E is estimated RTT, D is deviation (quater of safety margin), T is timeout interval, typically $\alpha = 0.125$ and $\beta = 0.25$.

RDT: timer for oldest unACKed segment, update seq number when unknown ACK received, retransmit when timeout, fast retransmit when triple duplicate ACKs received.

flow control: receiver controls sender, receiver advertises free buffer space (rwnd value), sender limits amount of unACKed data, guarantee receive buffer will not overflow.

TCP (Continued)

connection management: **3-way handshake**: 1. client chooses seq number, sends SYN message (SYNbit $= 1$, Seq $= x$). 2. server chooses seq number, sends SYNACK message (SYNbit $= 1$, Seq $= y$, ACKbit $= 1$, ACKnum $= x + 1$). 3. client knows server alive, sends ACK message (ACKbit $= 1$, ACKnum $= y+1$), may contain valid data. 4. server knows client alive. **closing connection**: 1. client can no longer send but receive, sends message (FINbit $= 1$, Seq $= x$). 2. server can still send, sends message (ACKbit $= 1$, ACKnum $= x + 1$). 3. server can no longer send, sends message (FINbit $= 1$, Seq $= y$). 4. client can still send, sends message (ACKbit $= 1$, ACKnum $= y+1$). 5. server closes. 6. client waits for twice the segment lifetime before closing.

congestion: packet loss, long delay, caused by queue, loss and path, leads to low throughput, unneeded retransmission and capacity waste.

congestion control: additive increase, multiplicative decrease (AIMD), cwnd proportional to rate. **slow start**: initially cwnd is 1, double cwnd every RTT until reach ssthresh, then increase cwnd by 1 every RTT. **loss detection**: cut ssthresh to half of cwnd, for timeout, set cwnd to 1, for triple duplicate ACKs, set cwnd to 1 (Tahoe), set cwnd to ssthresh added by 3 (Reno).

fairness: if K sessions share bandwidth R, each should have rate R/K. TCP is fair, UDP is not.

Network Layer

transport segment between hosts, exist in every host and router. **forwarding**: move packets from router's input to appropriate router output. **routing**: determine route taken by packets from source to destination. **data plane**: local per-router forwarding table. **control plane**: network-wide logic, determine end-end path. traditional routing algorithms, software-defined networking (SDN), per-router or logically centralized control plane.

service model: best effort, no guarantee of bandwidth, loss, order, timing and congestion feedback.

Router

input and output ports, routing processor, switching fabric.

forwarding destination-based forwarding, generalized forwarding, longest prefix matching.

switching: via memory, via bus (32 Gbps), via interconnection network (60 Gbps).

queueing: head-of-line blocking, delay and loss.

scheduling: FIFO (discard policy: tail drop, priority, random), priority (multiple classes), round robin (cyclically scan, one packet each class), weighted fair queueing (weighted amount service).

IP (Internet Protocol)

MTU limits size of link-level frame, fragment and reassemble datagram within network.

IP address: 32-bit identifier for host or router interface. **interface**: connection between host or router and physical link. **subnet**: physically reach each other without intervening router.

CIDR: classless inter-domain routing, subnet portion of arbitrary length e.g. 200.23.16.0/23.

IPv6: fixed length 40-byte header, no fragmentation, checksum removed, outside options, new version of ICMP. **motivation**: address space running out, header format speed processing, header change facilitate QoS. **tunneling**: IPv6 datagram carried as payload in IPv4 datagram among IPv4 routers. **adoption**: still require long time for deployment.

CS3611 Computer Networks (Spring 2023) Final Exam Cheat Sheet

Xiangyuan Xue (521030910387)

DHCP (Dynamic Host Configuration Protocol)

allow host dynamically obtain IP address from server when it joins network. 1. host broadcasts DHCP discover message. 2. server responds with DHCP offer message. 3. host requests address with DHCP request message. 4. server sends address with DHCP ack message. return: allocated IP address, address of first-hop router, name and IP address of DNS server, network mask.

NAT (Network Address Translation)

translation table, maintain mapping between internal and external IP address and port number.

Pros: fewer addresses needed from ISP, change local address without notifying outside world, change ISP without changing addresses of local devices, local devices not visible, safer.

Cons: router processes more than network layer, violate end-to-end argument, hard to connect server behind, IPv6 compatibility.

Routing Protocol

determine good path from source to destination.

link state: link costs known to all nodes, Dijkstra's algorithm, oscillations possible.

distance vector: node knows costs to all neighbors, maintain neighbors' distance vectors, use Bellman-Ford equation, update DV when receiving DV from neighbor, notify neighbors when changed. iterative, asynchronous, distributed. count to infinity problem (bad news travels slowly, solve by poisoned reverse).

comparison: message complexity, convergence speed, algorithm robustness. LS: $O(n^2)$ algorithm with $O(nE)$ messages, good robustness. DV: exchange between neighbors only, time varies, error propagates through network.

Intra-AS Routing

aggregate routers as autonomous systems (AS). routing within same AS, run same intra-AS protocal. IGP (interior gateway protocol) e.g. RIP (DVR based), OSPF (LSR based), IGRP.

OSPF (Open Shortest Path First): apply LSR, flood message in entire AS, carried over IP. secure, multiple same-cost paths allowed.

Hierarchical OSPF: two-level hierarchy (local area, backbone), area boarder and backbone router connected inside, boundry router connected outside.

Inter-AS Routing

routing among multiple domains.

BGP (Boarder Gateway Protocol): provide each AS means: eBGP (obtain reachability from neighbors), iBGP (propagate reachability to all internal routers). **session**: exchange message over semi-permanent TCP connection. **route**: advertised prefix includes attributes (AS-PATH, NEXT-HOP). **policy**: accept or decline path, determine whether to advertise. **route selection**: policy decision, shortest AS-PATH, closest NEXT-HOP router (hot potato routing), additional criteria.

Why different? policy, scale and performance. Inter-AS: admin controls how and who routes, policy dominates over performance. Intra-AS: single admin, no policy decision needed, can focus on performance. Both: hierarchical routing saves table size and reduce update traffic.

ICMP (Internet Control Message Protocol)

used by hosts and routers to communicate network-level information (error reporting, echo request and reply), work above network layer, carried in IP datagram, contain type, code and first 8 bytes of IP datagram causing error.

Error Detection, Error Correction

error dectection and correction bits (EDC), data protected by error checking (D), not 100% reliable, larger EDC field yields better detection and correction.

Error Detection, Error Correction (Continued)

single bit parity: detect single bit error, cannot correct.

2-dimensional bit parity: detect and correct single bit error.

Internet checksum: same as described in UDP and TCP.

cyclic redundancy check (CRC): view data bits D as a binary number, choose $r+1$ bit pattern G, choose r CRC bits R such that $D \cdot 2^r \oplus R$ is exactly divisible by G (modulo 2), if remainder is non-zero, error detected, can detect all the burst errors less than $r+1$ bits, widely used in practice.

Multiple Access Protocol

two or more simultaneous transmissions by nodes lead to collision, distributed algorithm, determine how nodes share channel, communication uses channel itself.

ideal requirement: one node transmits at rate R, M nodes transmit at average rate R/M, fully decentralized, simple.

multiple acesss protocol: three types: channel partitioning, random access, taking turns.

TDMA (time division multiple access): access to channel in rounds, each station gets fixed length slot, unused slots go idle.

FDMA (frequency division multiple access): channel spectrum divided into frequency bands, each station assigned fixed frequency band, unused transmission time in frequency bands go idle.

random access protocol: specify how to detect collision and how to recover from collision e.g. slotted ALOHA, ALOHA, CSMA, CSMA/CD, CSMA/CA.

slotted ALOHA: **assumption**: all frames same size, time divided into equal size slots, node starts transmission only at beginning of slots, all nodes detect collision within slot. **operation**: if no collision, node sends new frame in next slot, if collision, node retransmits frame in each subsequent slot with probability p until success. **pros**: active node transmits at full rate, highly decentralized, simple. **cons**: collisions, idle slots, clock synchronization. **efficiency**: probability that some node succeeds is $Np(1-p)^{N-1}$, as $N \to \infty$, max efficiency approaches $1/e \approx 0.37$.

unslotted ALOHA: transmit immediately, simpler, no synchronization, more collisions, **efficiency**: probability that some node succeeds is $Np(1-p)^{2(N-1)}$, as $N \to \infty$, max efficiency approaches $1/(2e) \approx 0.18$, even worse.

CSMA: if channel sensed idle, transmit entire frame, if channel sensed busy, defer transmission, collision may still occur.

CSMA/CD (collision detection): collision detected within short time, colliding transmissions aborted, after aborting, enter binary exponential backoff: after m-th collision, choose K at random from $\{0, 1, \ldots, 2^m - 1\}$, wait $512K$ bit times, try again. **efficiency**: $\eta = 1/(1 + 5t_p/t_t)$, t_p is maximum propagation delay between two nodes in LAN, t_t is transmission time of maximum-size frame, as $t_p \to 0$ or $t_t \to \infty$, efficiency $\eta \to 1$, better performance than ALOHA, simple, cheap, decentralized.

CSMA/CA (collision avoidance): collision detection difficult in wireless, if channel sensed idle for DIFS, transmit entire frame, if channel sensed busy, start binary exponential backoff, timer counts down while channel idle, transmit when timer expires, if no ACK, increase random backoff, try again, if frame entirely received, send ACK after SIFS. **additional**: send RTS and receive CTS heard by all nodes, applied in IEEE 802.11.

taking turns protocol: polling: master node invites slave nodes to transmit in turn, typically used in dumb slave devices, concerned in polling overhead, latency and single point of failure. token passing: control token passed from one node to next sequentially, implemented by token message, concerned in token overhead, latency and single point of failure.

LANs

MAC address: used locally to get frame from one interface to another physically-connected interface, 48-bit address burned in NIC ROM e.g. 1A-2F-BB-76-09-AD, portable, allocated by IEEE.

ARP (address resolution protocol): determine interface's MAC address given its IP address. **ARP table**: each node on LAN has table, record mappings (IP address, MAC address, TTL), TTL (time to live) is time after which address mapping will be forgotten. **recipe**: 1. A broadcasts ARP query packet containing B's IP address. 2. B receives ARP packet and replies to A with its MAC address. 3. A caches IP-to-MAC address pair in its ARP table until timeout.

addressing: 1. A creates datagram with source A and destination B. 2. A uses ARP to get R's MAC address. 3. A creates frame with R's MAC address as destination. 4. R receives frame, removes header, checks destination and forwards to another interface. 5. R creates frame with B's MAC address as destination. 6. B receives frame and gets datagram.

Ethernet: dominant wired LAN technology, simple and cheap, rate from 10 Mbps to 10 Gbps, connectionless and unreliable, use unslotted CSMA/CD with binary backoff. **physical topology**: bus (all nodes in same collision domain), star (active switch in center). **frame structure**: preamble (7 bytes of 10101010 and 1 byte of 10101011, clock synchronization), addresses (6 bytes for both source and destination), type, CRC.

switch: link-layer, transparent, plug-and-play, self-learning. **multiple access**: dedicated connection, buffer packets, transmit simultaneously without collisions. **switch table**: record entry (MAC address, interface, time stamp), when frame received, record incoming link and MAC address of sending host, look up destination address, if entry found, forward frame to target interface, otherwise flood (except incoming interface).

compare switch and router: both store-and-forward, both have forwarding table. router: network-layer, IP addresses, compute by routing algorithm. switch: link-layer, MAC addresses, learn forwarding by flooding.

VLANs (virtual local area network): define multiple virual LANs over single physical infrastructure, ports grouped, single switch operates as multiple virtual switches. **effect**: traffic isolation, dynamic membership, forwarding between VLANs by routing. **trunk port**: carry frames between multiple VLANs, VLAN ID required in header field (802.1Q protocol).

Wireless Network

element: wireless host, base station, wireless link.

mode: infrastructure mode (base station connects mobiles into wired network), ad hoc mode (no base station, transmit to others within link coverage).

Wireless Link Characteristics

decreased signal strength (attenuation), interference from other sources, multipath propagation (reflection), SNR versus BER tradeoff (higher SNR, lower BER). **rate adaptation**: SNR decreases, BER increases as node moves away from base station, when BER crosses threshold, switch to lower transmission rate.

WiFi (IEEE 802.11)

base station is access point (AP), basic service set (BSS) contains wireless host, AP and ad hoc mode (hosts only).

channel: 2.4 to 2.485 GHz spectrum divided into 11 channels, admin chooses channel for AP, interference possible.

association: scan channels, listening for beacon frames containing AP's name (SSID) and MAC address, select AP, run DHCP, perform authentication.

WiFi (Continued)

scanning: passive scanning (beacon frames from AP, association request from host to AP, association response from AP to host), active scanning (probe request broadcast from host, probe response from AP to host, association request from host to AP, association response from AP to host).

addressing: MAC address of sender, MAC address of receiver, MAC address of router interface attached by AP.

mobility: host remains in subnet, self-learning switch remembers port to reach host.

advanced: rate adaptation (previous section), power management (if AP-to-host frame to be sent, node stays awake, otherwise sleeps until next beacon frame).

802.15: personal area network (PAN), ad hoc, low power, master slave, 2.4 to 2.5 GHz, up to 721 kbps e.g. Bluetooth.

Cellular Network

architecture: cell (base station, mobile users, air interface), MSC (connect cells to network, manage call setup, handle mobility).

sharing: combined FDMA with TDMA, CDMA (code division multiple access).

standard: 2G (voice), 3G (voice and data), 4G (LTE, all IP core, no separation between voice and data).

Mobility Management

visitied network (where mobile currently resides), care-of-address (address in visited network), foreign agent (entity in visited network that performs mobility functions on behalf of mobile), correspondent (node with which mobile is communicating).

registration: mobile contacts foreign agent on entering visited network, foreign agent knows about mobile, home agent knows location of mobile.

approach: indirect routing: correspondent sends to home agent, home agent forwards to remote target. direct routing: correspondent gets foreign address of mobile, sends directly to mobile.

indirect routing: use permanent address and care-of-address, triangle routing (correspondent, home, network, mobile), inefficient when in same network. **moving between networks**: on-going connections can be maintained. 1. register with new foreign agent. 2. new foreign agent registers with home agent. 3. home agent updates care-of-address. 4. packets continue to be forwarded to mobile.

direct routing: overcome triangle routing, non-transparent to correspondent.**moving between networks**: data always routed first to anchor FA (FA in first visited network), when moving, new FA arranges to have data forwarded from old FA.

impact: best effort service model remains unchanged, TCP and UDP can run without modification. more delay and packet loss due to bit errors and handoff, TCP decreases cwnd unnecessarily, impairments for real-time traffic, limited bandwidth.