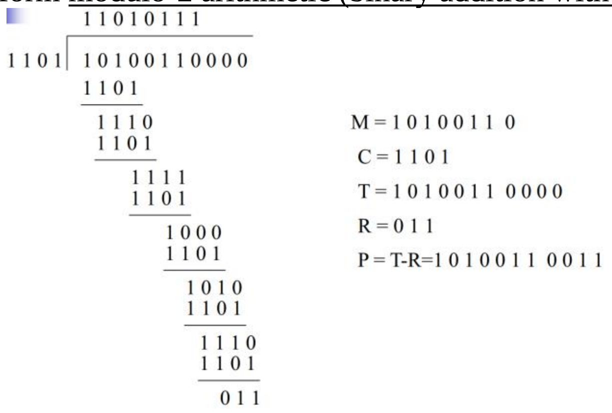
EE4204 Final Examination Cheat-sheet

1. Introduction & Basis

1) *ISO-OSI seven layers architecture:* physical layer, data link layer, IP layer, transport layer, session layer, presentation layer, application layer.
2) *IETF five layers:* (hourglass design) physical layer, data link layer – frame, IP layer – datagram, transport layer – segment, application layer – message.
3) *Layering:* ensure encapsulation and fragmentation, protocols provide service interface and peer-to-peer interface (cross layer design, possible?).
3) *Two kinds of packet switches:* router (IP layer), switch (data link layer).
4) *Network components:* core network (ISP), access network (telephone-based, cable-based, fiber-based, wired, wireless), network edges (hosts + servers).
a. Digital subscriber line (DSL): existing telephone, < 2.5/2.4 Mbps up/down;
b. Hybrid fiber coax (HFC): frequency multiplexing, < 2/30 Mbps up/down;
c. Fiber to the home (FTTH), passive optical network (PON);
d. Wi-Fi 802.11b/g < 11.54 Mbps (local), 3G/4G LTE 1 – 10 Mbps (wide).
5) *Link performance:* bandwidth (Hz), data rate (bps), channel capacity (noise).
6) *In local area networks:* broadcast link, point-to-point link, token ring.
7) *Multiplexing methods:* time division multiplexing (fixed – FTDM, statistical – STDM), frequency division multiplexing.
8) *Switching methods*: circuit switching (fixed TDM), packet switching (store and forward, statistical TDM).
9) *Address translation:* domain name to IP address – DNS (over UDP), IP address to MAC address – ARP (under the same LAN).
10) *Delays:* transmission delay (T_t), propagation delay (T_p), queuing delay (T_q), processing delay, packetization delay, etc.
11) *Transmission speed:* one-way unacknowledged transfer – $T_t + T_p + T_q$, one-way acknowledged transfer – $T_t + 2 \cdot T_p + T_q$.
12) Delay (D) and bandwidth (B) product = amount of data "in the pipe".
13) Effective throughput: $RTT + message\ size/bandwidth$.

2. Data Link Layer

1) When a packet is transferred around in the network, the source/destination MAC address changes between each two hops, while IP address remains the same (always the initial source or eventual destination address).
2) Link layer ensures channel reliability; transport layer ensures end-to-end reliability.
3) Shannon's capacity theorem: $C = B \cdot \log_2(1 + S/N)$.
4) *Framing approaches:*
a. sentinel-based: delineate with byte 7E, bit staffing in HDLC– insert 0 after five consecutive 1s, byte staffing in PPP – use 7D as escape character;
b. counter-based: count field in header, back-to-back frames could be affected;
c. clock-based: 810 bytes per 125 µs = 51.84 Mbps (STS-n = n * 51.94 Mbps).
5) *Cyclic Redundancy Check (CRC):* represent the message and divisor as polynomial, perform modulo-2 arithmetic (binary addition with no carry).



6) Flow control ensures that the sender does not overwhelm the receiver (stop and wait, sliding window with ACK n or RR n).
7) *Automatic repeat request (ARQ):* introduce NACK, REJ, SREJ.
a. Stop and wait: TIMEOUT mechanism, alternate between ACK0 and ACK1;
b. Go back N: ACK n or RR n, REJ i will trigger sender to go back to i;
c. Selective reject: ACK n or RR n, SREJ i will trigger sender to re-transmit i.
8) *Performance:* let $a = T_p/T_f$ represent the number of frames held in the link.
a. Stop and wait: link utilization $U = (1 - P_f)/(1 + 2a)$;
b. Sliding window (error-free): assume window size is W, $U = W/(1 + 2a)$ if $W < 1 + 2a$ or $U = 1$ if $W \geq 1 + 2a$;
c. Selective reject: $U = (1 - P_f) \cdot W/(1 + 2a)$ if $W < 1 + 2a$ else $U = 1 - P_f$;
d. Go back N: $U = \frac{(1-P_f)\cdot W}{(1-P_f+P_f\cdot W)(1+2a)}$ if $W < 1 + 2a$ else $U = \frac{1-P_f}{1+2a\cdot P_f}$.
9) *Ethernet:* max 2500m by 5 segments (separated by 4 repeaters).
a. Collision detection: carrier sense multiple access (CSMA), use exponential back-off algorithm (randomly wait $[0, 2^n-1]$ slots at n^{th} collision, give up after);
b. Minimum frame size: 64 bytes (512 bits for 10 Mbps link = 51.2 µs RTT);
c. LAN connection: bus (single collision domain), hub (copy frames to all other ports) and switch (store and forward, port to port);

d. LAN extension: bridge (source routing, transparent, spanning tree);
e. Forward table & backward learning: dynamic record down source port;
f. Distributed spanning tree bridge: to avoid loop (assign each bridge a unique ID, use the bridge with smallest ID as root, initially claim itself as root, stop forwarding when a neighbor is nearer to the actual root).
10) *Wireless network:* Bluetooth, Wi-Fi and 3G/4G LTE.
a. Spread spectrum technique: frequency hopping (transmit over a sequence of frequencies, from a pseudo-random generator with pre-agreed seed);
b. Direct sequence technique: n-bit chipping code (XOR with n random bits);
c. 802.11 does not have collision detection (due to hidden & exposed node problem), but has collision avoidance (request to send, clear to send);
d. Scanning (active – Probe, Probe Response, Association Request, Association Response, passive – Beacon, Association Request, and Association Response).

3. IP (network) Layer

1) *Two key functionalities:* forwarding (longest prefix matching), routing.
2) *Datagram network* – "smart" end systems, *virtual circuit (VC) network* – "dumb" end systems, complexity inside network.
3) *Router:* run routing algorithm, forward datagrams from in-port to out-port.
a. Switching fabrics: memory, bus, crossbar (interconnection network);
b. Input port: decapsulation, decentralized switching, queuing (HOL blocking);
c. Output port: buffering (queuing), scheduling discipline;
d. Queuing (delay) and loss leads to input/output buffer overflow.
4) By class-less interdomain routing (CIDR), each isolated network is a subnet.
5) Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses (DHCP discover, DHCP offer, DHCP request, DHCP ack).
6) *Network Address Translation (NAT):* replace all internal IP addresses with one single IP address differentiated by ports. Although NAT solves the address shortage problem, the optimal solution should be IPv6 instead.
7) *NAT traversal problem:* static configuration, Universal Plug and Play (UPnP), relaying (used in Skype).
8) *Tunneling:* IPv6 carried as payload in IPv4 datagram among IPv4 routers.
9) *Link state routing algorithm:* Dijkstra's algorithm, global algorithm.
a. May not be able to produce correct answer for negative weights;
b. Cannot work when there is negative cycle (since answer is -∞).
10) *Distance vector routing algorithm:* Bellman-Ford algorithm, decentralized.
a. Bellman-Ford equation: $d_x(y) = min_v\{c(x,v) + d_v(y)\}$;
b. Each node waits for any change, recompute the estimates and broadcasts;
c. Could result in "count to infinity" problem if links breaks;
d. Poisoned reverse: Z tells Y $d_z(x) = \infty$ if Z routes to X via Y;
e. BGP-4 solves the "count to infinity" problem ultimately by using AS_PATH attribute (to list the full path and thus it does not include the current AS).
11) We need to aggregate routers into autonomous systems (AS), thus require intra-AS routing protocol and inter-AS routing protocol.
a. Inter-AS and intra-AS routing reflects the hierarchical network structure;
b. Inter-AS protocol propagates reachability information to all internal routers.
12) *Interior Gateway Protocol (IGP)* in the Internet, intra-AS protocols:
a. Routing information protocol (RIP): based on distance vector with poison reverse (infinite distance = 16 hops);
b. Open shortest path first (OSPF): based on link state, flooding via IP;
c. Interior gateway routing protocol (IGRP): Cisco proprietary.
13) *Border Gateway Protocol (BGP)* in the Internet, inter-AS protocol: based on distance vector, exchange routing information over BGP sessions (via TCP).
14) *Broadcast routing:* use in-network duplicate along a spanning tree.
15) *Multicast routing:* use Steiner Tree as the minimum cost tree to connect all routers with attached group members.

4. Transport Layer

1) Most services use TCP, but some (like DHCP, DNS and traceroute) use UDP due to no setup required.
2) *TCP reliable delivery:* checksum, sequence number, re-transmission.
a. Three-way handshake: SYN, SYN ACK, ACK;
b. Tearing down connection: (FIN, FIN ACK) * 2, RST;
c. Stop and wait: keep timeout length as a function of (estimated) RTT;
d. Sliding window: receiver advertises the window size to sender;
e. Fast re-transmission: re-transmit data after receiving 3 duplicate ACKs;
f. Congestion control: actual window size is min of congestion window and flow window, slow start & additive increase & multiplicative decrease;
g. Facing 3 duplicate ACKs, Reno cuts CW by half, Tahoe treats as timeout;
h. Congestion avoidance: implicit – random early dropping (RED), explicit – intermediate router sets the DEC bit in packet header.
3) *TCP throughput:* controls the amount of traffic by adjusting window size.
a. Instantaneous send rate: W/RTT;
b. Instantaneous receive rate: $\leq$ send rate;
c. Average send rate under AIMD: $((W + 0.5W)/2)/RTT = 0.75 \cdot W/RTT$.
4) *Rethinking end-to-end (e2e):* (approximated) flow recognition is the key.