Tutorials

- Transmission delay is the time where the last bit leaves the sender
- If propagation delay < transmission delay, then first bit should reach receiver
- Message segmentation
  - Pros: reduces delay, single bit error does not require whole message to re-transmit, huge messages can block the smaller messages
  - Cons: packets must be put in sequence to destination (network may re-order packets), result in more overhead per packet
- Given N devices
  - Minimum links: N – 1 (tree, chain, star)
    - Pros: simple topology
    - Cons: Single point of failure, longer path between 2 nodes
  - Maximum links: $\frac{N\times(N-1)}{2}$
    - Pros: most robust topology, 1 hop distance between all nodes
    - Cons: most expensive
- IP address is not shown in HTTP request messages
- Connection: keep-alive used to indicate persistent connection, value of close means no persistent connection
- Content-Length does not include header size
- 1 request to 1 response, but 1 connection can have many requests
- Persistent connection maintained with server, not with URL
- DNS cache poisoning: rogue DNS records introduced into DNS resolver’s cache to cause name server to point to wrong IP address, diverting traffic to attacker’s computer
- POST used to upload a file or submit web form to server, GET used to retrieve information from server
- TCP client -> needs server to run, UDP client -> does not need server to run
- Checksum detects presence of bit error, not absence of bit error
  - Bits can swap for 0 and 1 and this won’t be detected
- If using UDP for transmission, reliable data can be achieved by implementing it on application level
- Random start value for TCP used to ensure that a sequence number is not reused until the sender is sure that the same sequence number is no longer in the network, paired with using TTL to avoid circulating infinitely in network
- Maximum L (file size in bytes) if TCP sequence number field is N bits long: 2^N
- NAT must assign new port per private IP address, but the NAT public IP remains the same
- Distance vector algorithm is basically Bellman-Ford for all nodes (that’s why need local view or cost vector for all neighbors)
- Only ID and checksum change for IP fragmentation
- TCP is never redundant since it helps with handling out-of-order packets and packet losses
- By default, assume EVEN parity scheme
- For 2-D parity, focus on what changes/does not change the parity bits
- When evaluating use of multiple access protocol, focus on utilization (i.e. rate of collision to rate of sending)
- Remember to convert any packets to bits for CSMA/CD to match the bit time
- CSMA/CD backoff algorithm delay calculated using
$$K * \frac{512}{Bandwidth}$$
- Switch table entries get updated when **RECEIVING** packets
- When sending to outside of the subnet, the destination MAC address must be the router’s MAC address (defaults to this when cannot find anything in ARP and no entries)
  - If the router does not see the destination IP address in any of its subnets, it will forward it to the next hop router again
  - Router also re-creates the frame with the proper MAC address
  - If frames are received from outside, the source MAC will always be the router’s MAC
- For symmetric key encryption, total number of keys are the number of edges in the graph
- For public key encryption, total number of keys is the number of nodes x 2
- BitTorrent file contains hash per block and this value is calculated to be compared
- Steps to decrypt secure email:
  1. Bob computes $K_B^-\left(K_B^+(K_S)\right) = K_S$ to recover the session key using his private key

2. With K_S, Bob decrypts the message $K_S\left(K_S\left(m \oplus K_A^-(H(m))\right)\right) = m \oplus K_A^-(H(m))$
3. Use Alice’s public key to recover H(m): $K_A^+\left(K_A^-(H(m))\right) = H(m)$
4. With m, Bob computes H(m) and verifies that it is equals to the H(m) obtained from step 3

- Quantization implies that each sample requires N bits to encode so the total bit rate is the samples/sec x N bit/sample
- TCP receive buffer is not the same thing as the client application buffer
- Late packets cannot be played because it will make the video jump
- RTP uses UDP since loss can be tolerated and video should be fast but RTSP uses TCP since loss cannot be tolerated and slowness is less visible
- XOR for simple FEC only works if 1 chunk is invalid, anymore and XOR cannot determine which is the wrong chunk