

*Handoff* = the wireless unit changes base station.  
*RTS/CTS handshake* = for reserving the medium.

## TCP:

- Transportprotokollet finns normalt i operativsystemet och tillhandahåller kommunikationstjänster till tillämpningar.
  - *Provide logical communication between app processes running on different hosts*
- Transport protocol runs in end-systems
- More than one transport protocol available to apps: TCP & UDP
- **Transport vs Network Layer:**
  - *Network Layer: Logical communication between hosts*
  - *Transport Layer: Logical communication between processes*
- **Reliable, in-order delivery**
  - Congestion control
  - Flow Control
  - Connection setup
- **Connection-oriented**
  - Handshaking
- **Reliable data transfer**
- **Full duplex data**
  - Bi-directional data flow in same connection
  - MSS: maximum segment size
- **TCP timeout too short** → premature timeout, unnecessary retransmissions
- Retransmissions triggered by duplicate acks & timeout events
- **TCP fast transmit**
  - *Sender receives 3 acks (triple duplicate acks) → resend unacked segment with smallest seq #*
- **Flow control**
  - *Receiver controls sender so that the sender won't overwhelm the receiver's buffer by transmitting too much, too fast.*
- **TCP closing connection:**
  - *Client & server each close their side of the connection by sending TCP segment with FIN bit = 1 and ack these FIN bits.*
  - *Simultaneous FIN exchanges can be handled*
- **Congestion:** "too many sources sending too much data too fast for *network* to handle"
- **TCP slow start** = exponentially
- **TCP Congestion avoidance** = linearly
- **TCP decides** how much data you can send in a segment, not the implementation that uses TCP.
- **TCP and UDP dataflow over the same link** → TCP-traffic will eventually split the capacity fairly that is not being used by the UDP traffic.
- **Congestion control** means that TCP presumes that a congestion has occurred in the network if the sender does not receive an ack in time on sent data, hence, the transmission rate is changed.
- **TCP connection established** → three-way handshake

## UDP:

- Unreliable, unordered delivery
- UDP segments may be lost
- Delivered out of order to app.
- Connectionless, which is good because the connection phase might add additional delay.
- Used in streaming multimedia apps (loss tolerant, rate sensitive), DNS, SNMP.
- No congestion control
- No connection state or receiver
- UDP can detect bit errors in packets, but cannot notify the sender about it.

### APPLICATION LAYER:

- Bittorrent
- DHCP
- DNS
- FTP
- HTTP
- IMAP
- POP3
- SNMP

### TRANSPORT LAYER:

- TCP
- UDP

### NETWORK LAYER:

- ARP
- BGP
- ICMP
- IP (IPv4, IPv6)
- RIP
- The network layer defines how devices (such as computers and routers) can communicate with each other, possibly going through intermediate routers between the devices.

### LINK LAYER:

- Ethernet
- WiFi
- IS-IS
- PPP

### PHYSICAL LAYER:

- IEEE 802
- Bluetooth

### About emails (SMTP, IMAP)

- SMTP → SMTP → IMAP
- An email-client is configured with an outgoing email-server, hence the client will send an outgoing email with SMTP. From here, the email is sent to the recipients incoming email-box server.

### IP

- The field *Header Checksum* is recalculated in each router along the packet's path.

### DNS

- DNS servers stores the answers for queries in a cache but it is a possibility that the information stored in the cache might get updated. This scenario can always happen, hence, DNS has limited storage time for information.
- A root server knows which DNS servers that are responsible for the Internet's TLD (top-level domains), e.g. "se" or "com".

The root servers refers to TLD-servers.

### CSMA/CD & CSMA/CA

- **For both CSMA/CD & CSMA/CA:**
  - A node that has data to send first listens to the medium to decide if any other node is currently sending data before the node itself sends data.

- If a collision occurs where multiple nodes send data simultaneously, then the sending nodes will wait for a randomized time and then retransmit again.

- CSMA/CD is more effective than CSMA/CA. CSMA/CA doesn't require full-duplex (if it requires full-duplex, then you don't even need any medium access protocols!)

## **SWITCH**

- Two nodes connected to the same switch can send packets simultaneously without collisions.

## **LAN (WLAN, IEEE 802.11)**

- There are different versions of the 802.11 – protocol. Access points usually have support for different versions and adapt according to the wireless units that are connected
- A successful transmission from a unit to the access point is confirmed with an ACK from the access point. In case of collision, there will be no ACK frame.

“All units share the same channel according to the random access principle. The absence of an ACK is the only way to detect that something went wrong.

## **ICMP**

- **ICMP** does not use any transport protocol. ICMP messages are directly put in the IP-packet.
- If a router does not know where to send an IP-packet, it sends out a ICMP-error message to the packet's sender.
- If a router detects TTL = 0, then it sends an ICMP-message back to the packet's sender.

## **RIP**

- RIP uses Bellman-Ford algorithm to find the best path between two nodes in the network.

## **DHCP**

- DHCP is used to tell a computer which router should be used when outgoing traffic is going outside of the subnet.
- Configuring WiFi is not supported by DHCP. That specific task is for the Link Layer.
- DHCP can be used for time-limited assignment of IP addresses.
- Does NOT use TCP as a transport protocol.
- DHCP exception: IP source address 0.0.0.0.
- DHCP can be used to inform a unit about what DNS server it should use.

## **HTTP**

- The amounts of requests/responses needed depends on how many objects you want.

For instance, a page consists of two videos and an image. One request for the page itself, and then 3 requests for the objects

## **CRC (Cyclic Redundancy Check)**

- CRC can detect burst errors. All consecutive bit errors up to a certain length will be detected.
- ARP does not assign addresses, it only reports on the current configuration.

## **ARP (Address Resolution Protocol)**

- The purpose of ARP is to translate IP addresses to MAC addresses.

## **MAC**

- MAC addresses are tied to the network adapter hardware, and not to the network to which the device currently is connected.
- The MAC address space is flat (non-hierarchical) and MAC addresses are unique, which makes it possible to move a device between networks without reconfiguration.

## **IPv4**

- Information in the IP packet header is changed every time the packet is forwarded through a router.
- An IP packet has an upper bound on the number of times it can be forwarded by routers.
- A router can split an IP packet into several smaller IP packets when it is forwarded.

## **IPv6**

- Making sure that IPv6 nodes have dual-stacks with support both for IPv4 and IPv6.

## **OSPF**

- OSPF uses *flooding* to distribute link state updates to all other nodes in the network.

## **DISTANCE VECTOR**

Distance vector is based on each node sending information to its neighbors about what nodes it can reach and how many hops there are to these nodes.

- Bellman-Ford algorithm
- RIP (Routing Information protocol)

## **LINK STATE**

- OSPF
- IS-IS