TCP/IP INTRODUCTION

by Paul Nicolay
ON7DJU

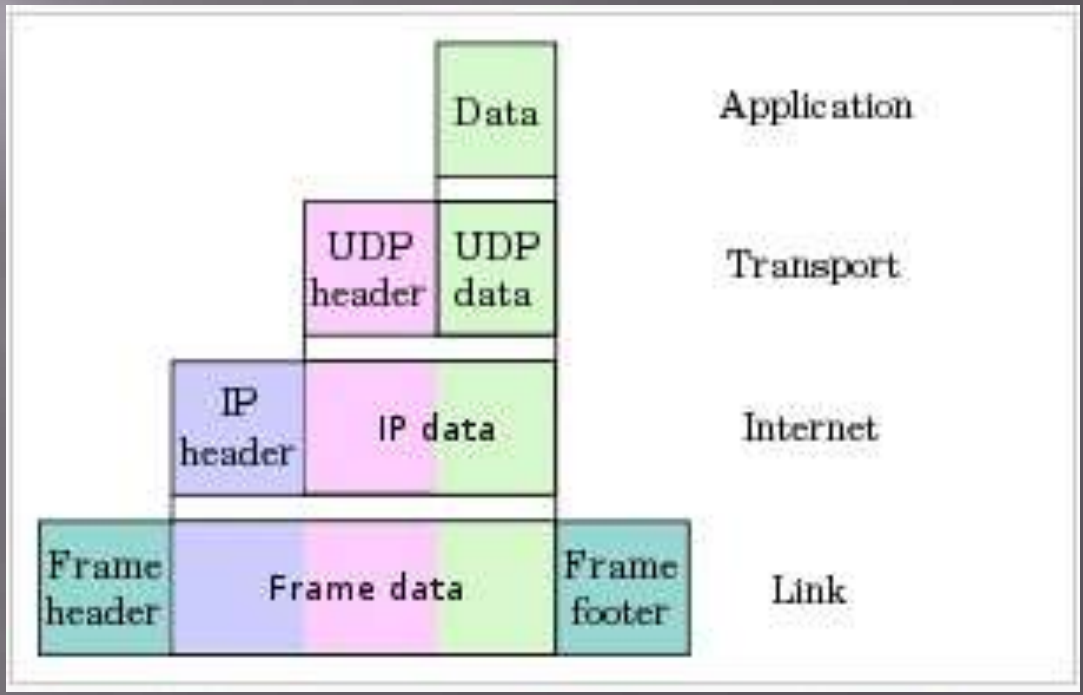
December 2010 – Sectie MCL

TCP/IP

- Resulted from research by DARPA in early 1970s after pioneering work by ARPANET
- Designed for essential functions; transmitting data efficiently and routing traffic
- First RFC in December 1974 by Robert E. Khan en Vincent Cerf
- A two network test in 1975 (Stanford – London), a three network test in 1977 (US, UK and Norway)
- Declared as standard for military computer networking in 1982 by Department of Defense
- Migration from ARPANET to TCP/IP on January 1st, 1983

Layered Concept

- Four (five) layers
  - Application
  - Transport
  - Network
  - Link
  - (Physical)



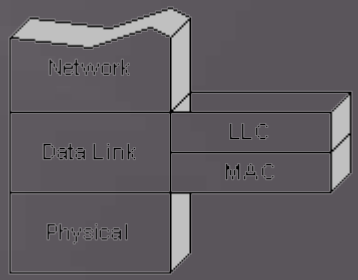
- OSI Model has 7 layers

Physical Layer

- Layer 1 of the OSI model
  - Does not apply to TCP/IP directly
- Definition of hardware specifications
  - But hardware can be more than physical layer
  - Pin layout, voltages, cable specifications, ...
- Encoding and signaling
  - Conversion between data and signals, ...
- Data transmission and reception
  - Modulation, ...
- Topology and physical network design
  - Hubs, repeaters, network adapters

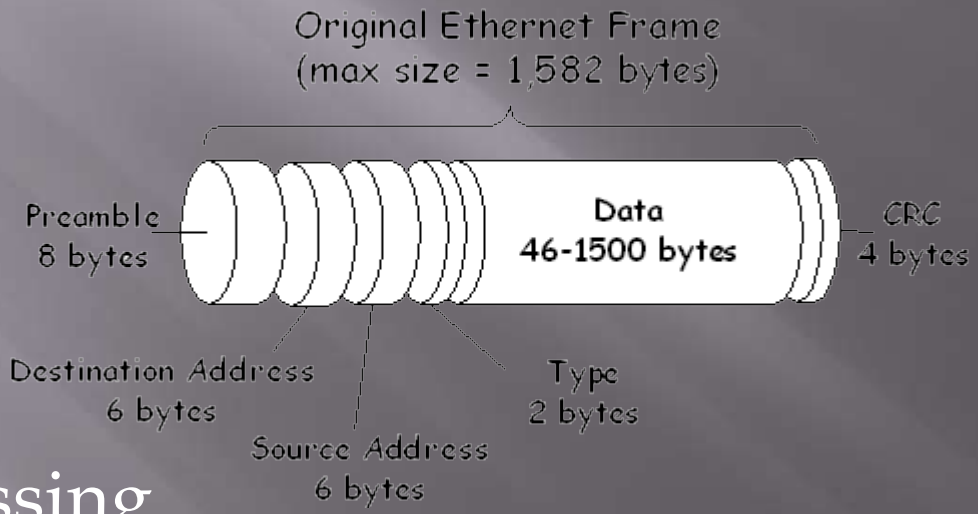
Data Link Layer

- IEEE 802 project (February 1980)
  - IEEE 802.2 media independant
  - IEEE 802.3 ethernet, IEEE 802.11 wireless, ...
- Logical link control
  - Upper part of DLL, links to network layer
- Media access control
  - Lower part of DLL, links to physical layer
  - Ethernet uses CSMA/CD, Token ring use a token
- Error detection
  - Correct errors in physical layer, ie. CRC



Data Link Layer

- Data framing
  - Encapsulation in frames



- Addressing
  - Each device has a hardware or MAC address
  - Ethernet has 48 bit address (xx:xx:xx:xx:xx:xx)

ARP

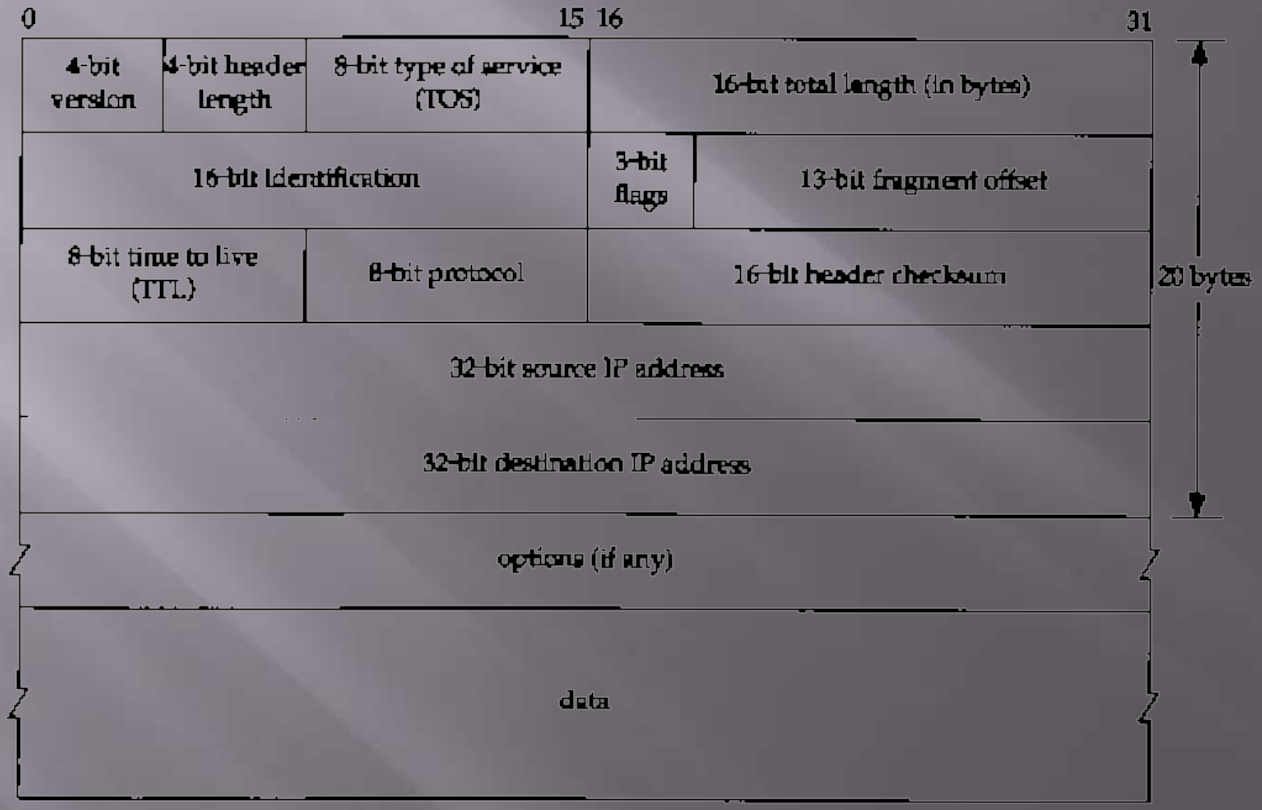
- Address Resolution Protocol (ARP)
  - Used to translate IPv4 addresses (layer 3) to MAC addresses (layer 2)
  - IPv6 uses NDP (Neighbor Discovery Protocol)
- Low level
  - ARP is payload of ethernet frame
- Broadcast mechanism
  - Who has x.x.x.x ?
  - Computer knows if it is local, or remote host
    - Router can reply to broadcast
- ARP cache, arp -a

Network Layer

- Logical adressing
  - Layer 3 address, independant of hardware
  - IP-address, unique accross entire network
- Addressing and Routing
  - IP
- Datagram encapsulation
  - Messages are placed in datagrams (packets)
  - 46 to 1500 bytes (header, data)
- Fragmentation and reassembly
  - Based on MTU (Maximum Transmission Unit)
- Error handling

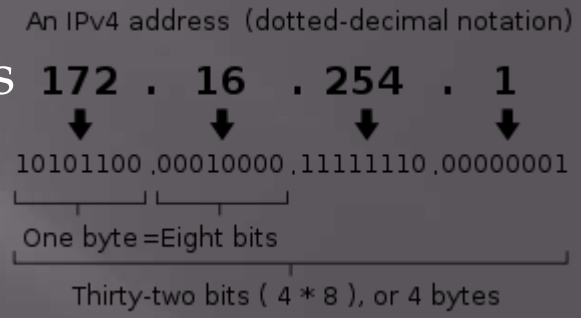
IP

- Internet Protocol (IP)



Addressing

- IP-address
  - Numerical label assignd to each device
  - 32 bit number (IPv4), 128 bit number (IPv6)
    - 4.294.967.296 (2^{32}) combinations
    - about 3.403×10^{38} (2^{128}) combinations
  - Human readable formats
    - 172.16.254.1 (IPv4)
    - 2001:db8:0:1234:0:567:8:1 (IPv6)
  - Managed by Internet Assigned Numbers Authority (IANA), delegated to five regional registrars (AfriNIC, ARIN, APNIC, LACNIC and RIPE NCC)



Subnetting

- Subnetting
  - Network, host
  - Subnet mask
- Classful network architecture (1981)

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

- Classless Inter-Domain Routing CIDR (1993)
  - CIDR notation (/notation)

Routing

- Routing
  - Also called layer-3 switching
    - Switches work at layer-2
  - Static versus dynamic routing
  - Routing tables
    - route print
- Routers
  - Used to connect two or more logical networks
  - Can have multiple interfaces, multiple physical types
  - Can exchange information (RIP, OSPF, BGP)

ICMP

- Internet Control Message Protocol (ICMP)
  - Core protocol of Internet Protocol suite
- Typically not used to transfer data, but for error messages
- All ICMP packets have an 8 byte header
  - ICMP Type, code and checksum
  - Echo request/reply (0, 8), Destination unreachable (2 , 3), Time Exceeded (11), Tracerout (30)...
- Application layer tools that used ICMP
  - Ping, traceroute

Transport Layer

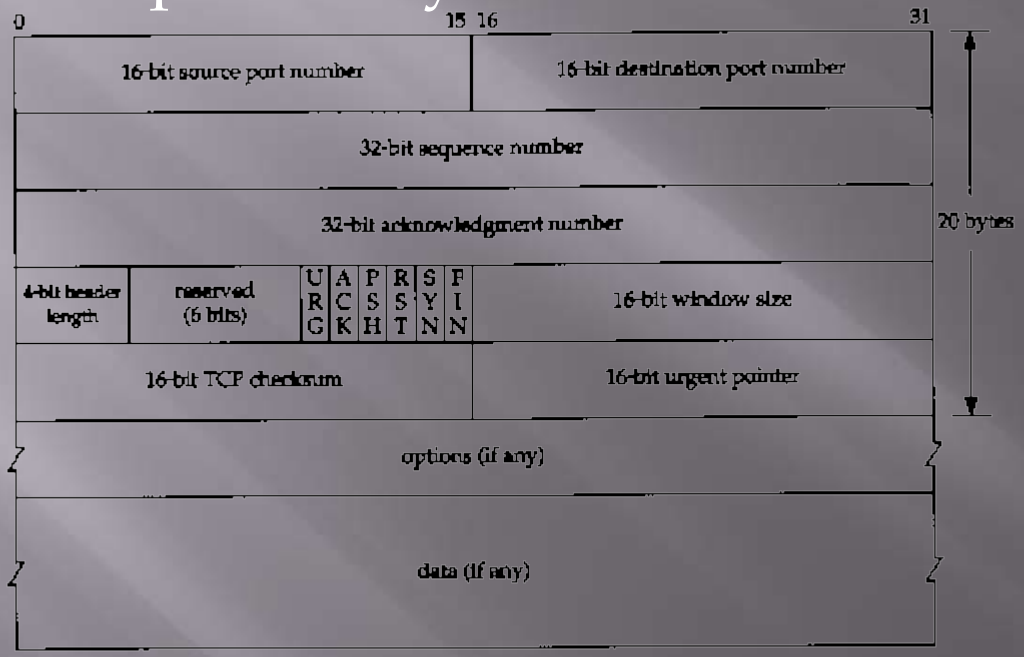
- Provides transparent transfer of data
- Services, optional for some protocols
  - Connection oriented
  - Byte orientation
  - Same order delivery
  - Reliability
  - Flow control
  - Congestion avoidance
  - Multiplexing (ports)
- Most well know protocol is TCP

TCP

- Transport Control Protocol (TCP)
- Connection oriented
  - Requires 3 packets to setup connection
- Provides reliability
  - Retransmissions, ordering, error-free, flow and congestion control
  - Positive acknowledgements
- Used for many protocols
  - DHCP, HTTP, SMTP, FTP, ...

TCP

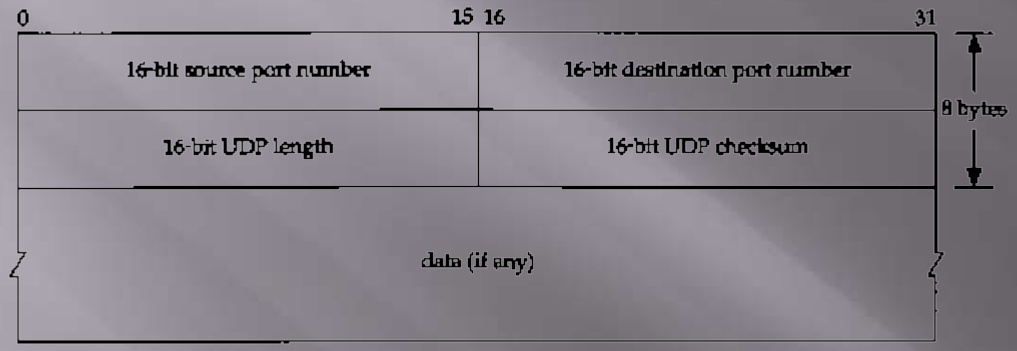
- TCP packet layout



- Protocol phases
  - Listen, SYN-SYN, SYN-ACK, ACK, FIN-WAIT-1/2, Close Wait, Closing, Last-ACK, Time-Wait, Closed

UDP

- User Datagram Protocol (UDP)



- Connectionless protocols
  - Packets are sent individually
- Not reliable
  - No retransmission, unordered, checksum optional...
- Used for broadcasting, multicasting, ...
  - IPTV, IP Telephony, ...
- Higher throughput, lower latency

Application Layer

- Process to process communication
  - OSI Layer 7
- Examples
  - HyperText Transfer Protocol (HTTP)
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol (POP3)
  - File Transfer Protocol (FTP)
  - Terminal (TELNET)
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS)
- Operate at well known ports

NAT

- Network Address Translation (NAT)
  - Popular since 1990s for address exhaustion
  - Modifies network address information
  - Remaps an IP-address space
  - IP-masquerading hides network (often private)
- Drawbacks
  - Affects certain applications
    - FTP (active), SIP, ...
    - Various solutions (NAT traversal, UPnP, ...)
  - No end-to-end connectivity
    - Initiate connections from outside