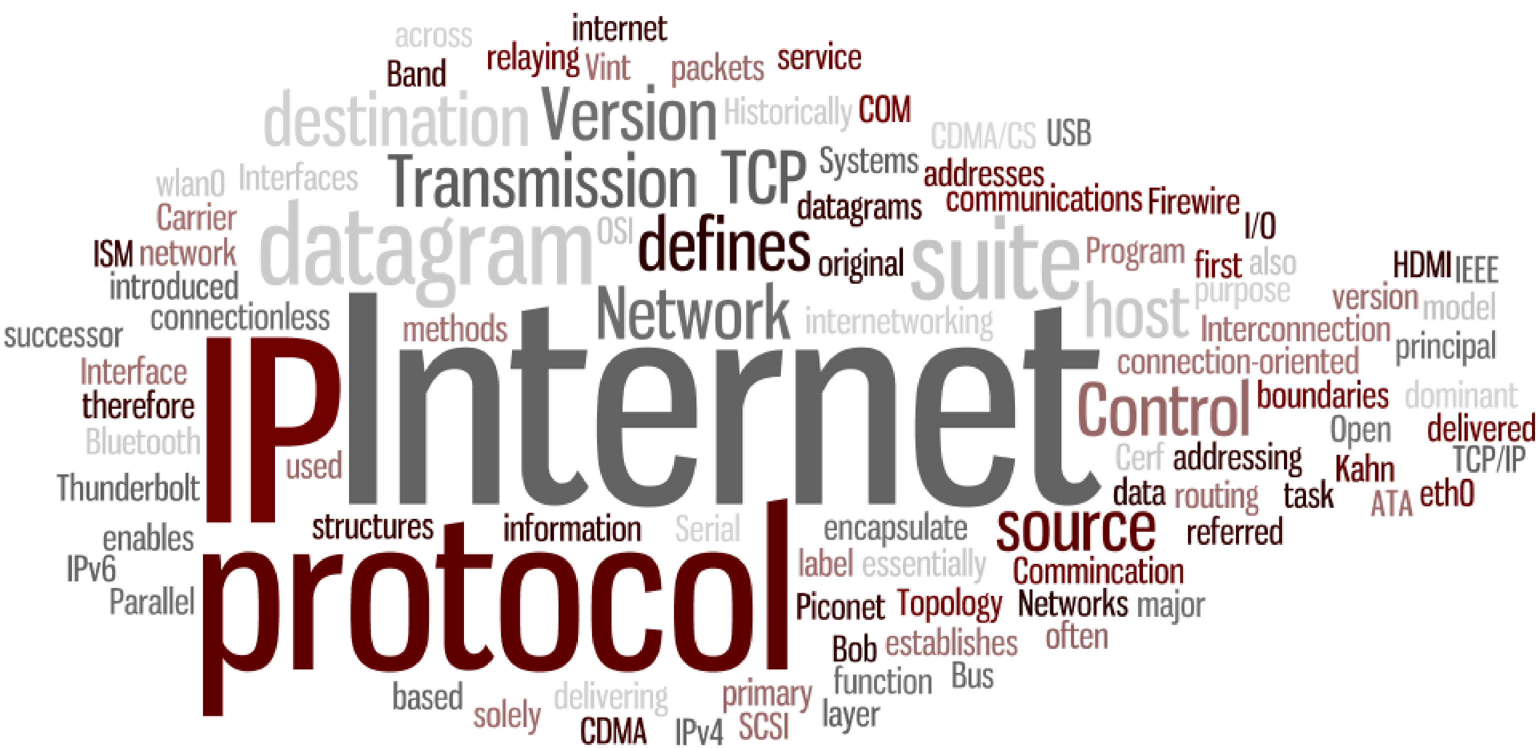
Networks


across
internet
Band
relaying
Vint
packets
service
destination
Version
Historically
COM
CDMA/CS
USB
wlan0
Interfaces
Transmission
TCP
Systems
addresses
datagrams
communications
Firewire
Carrier
I/O
ISM
network
datagram
OSI
defines
original
suite
Program
first
also
HDMI
IEEE
introduced
purpose
version
model
connectionless
Network
internetworking
host
Interconnection
successor
methods
principal
connection-oriented
Interface
IP
Internet
Control
boundaries
dominant
therefore
Open
delivered
Bluetooth
Cerf
addressing
Kahn
TCP/IP
used
data
routing
task
ATA
eth0
Thunderbolt
structures
information
Serial
encapsulate
source
referred
enables
label
essentially
Commincation
IPv6
protocol
Piconet
Topology
Networks
major
Parallel
Bob
establishes
often
function
Bus
based
delivering
primary
solely
layer
CDMA
IPv4
SCSI

Components of a computer network

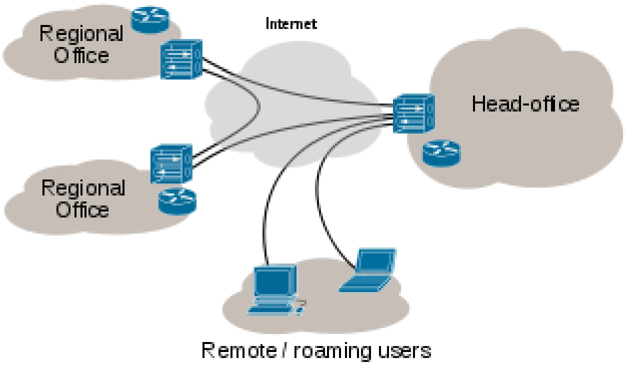
- Logical and physical elements
  - Hardware – Server, Bridge, …
  - Software – (Network-OS), Protocols

  - Server
    - Dedicated
    - non dedicated
  - Client

  - Interface, Media

Network vs. Client/Server vs. Cluster

- Network: Connected autonomous computers
- Network vs. Master/Slave
  - No Master/Slave dependency
  - Terminals at Mainframe is not a network
- Cluster vs. Network
  - Identification
  - Authentication
  - Access intend



How to characterize a network

- Transmission methodology
  - Broadcast
    - Transmission from one to all nodes
    - Addressing information in data
  - Point-to-Point
    - Multiple lines, multiple paths
    - Hops between A and Z
    - Routing

- Media
  - Copper, Fibre, Wireless, RFC 1149
  - Coax vs. twisted pair

- Organizational scope
  - Intranet / Extranet

How to characterize a network: Scale

- WAN   Wide
  - GAN (Gobal)

- MAN   Metropolitan

- LAN   Local Area Network
  - Legal boundaries
  - Usually high access rights
  - Multiple networks connected via backbone
  - (HAN Home)

- PAN   Private Area Network
  - Ad hoc
- NFC   Near Field Communication

- VPN   Virtual Private Network
- SAN   Storage

How to characterize a network: Circuit- or paket-switched

- Circuit-switched networks (leitungsvermittelt) provide a connection which is exclusive between the communication partners and transparently carries bit or byte streams between them
  – can exist “permanently” (as public service usually rather expensive)
  – in most cases are switched line, i.e. established on demand and dropped when no longer needed (dial-up line).
  – Typical examples: Modem links, ISDN connections

- Packet-switched networks (paketvermittelt)
  – carry data not as continuous bit/byte streams but in chunks of data which are limited in size, clearly separated from each other and identifiable
  – data is split into standardized packets by sender
  – packets contains actual payload data plus a packet id and information about sender and recipient(s)
  – network transfers packets over (different) routes from sender to recipient(s), often with intermediaries
  – recipient collects packets and re-arranges them in proper order to get actual payload data
  – can be connection-oriented or connectionless
  – Typical examples: LAN, Internet

Network communication protocols - characteristics

Maintaining of a connection and session (virtual or physical)

- Connection-oriented
  - Handshaking, e.g. TCP
- Connectionless

Switching (direct, virtual, …)

- Circuit-switched
- Packet-switched

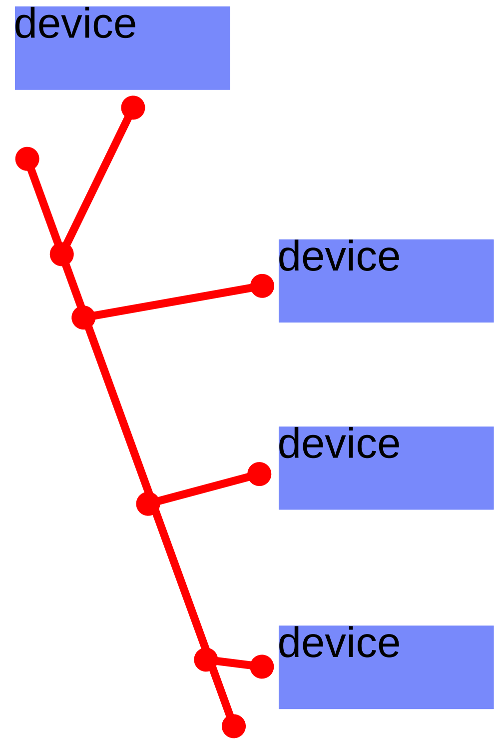
Is the sender checking whether the data has arrived?

- Reliable
  - e.g. TCP
- Unreliable
  - e.g. UDP

How to characterize a network: Topology

- Bus
  - Passive media
  - Terminated
  - Stations are not part of the bus

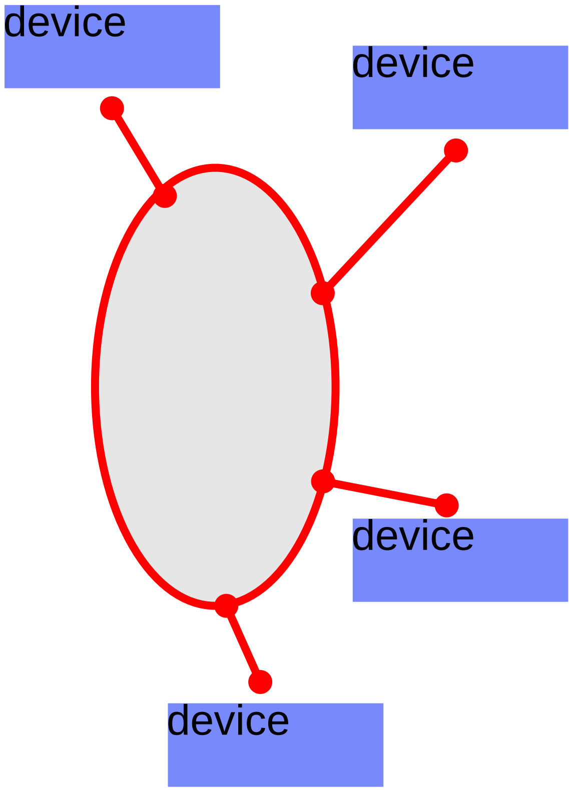
- Easy scale-out
- Dead station != dead network
- Low Costs
- Length limitations
- Terminations and adressing
- Bus failure is fatal



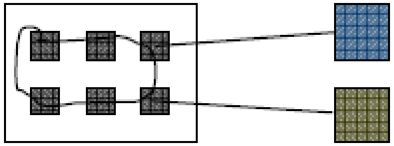
How to characterize a network: Topology

- Ring
  - No center
  - Store and Forward principle
  - Stations are part of the ring
- Dead station
  - Closed-circuiting
  - Two rings

- Easy scale-out
- Unlimited nodes
- Transmission duration depended on the number of nodes
- Dead station problem

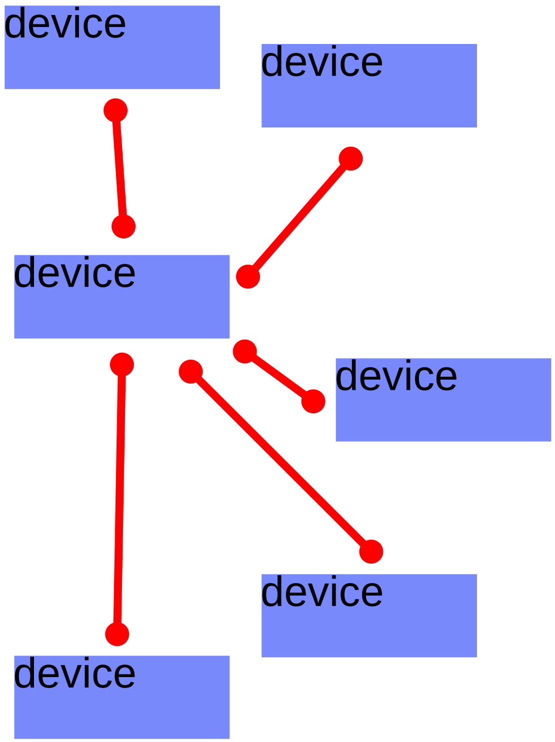


Token Ring „Patchfelder":



How to characterize a network: Topology

- Star
  - Central management node
  - Classic client/server and terminal methodology
- Passive or active star networks
  - Active routing
- Easy scale out
- No dead station problem
- Central node problem
- Cost intensive



Carrier sense multiple access/collision detection CSMA/CD

- CSMA/CD stands for carrier sense multiple access/collision detection
  - CSMA/CD is the method how Ethernet devices in the same network segment communicate with each other.

WHY?

- All Ethernet nodes share the medium/cable.
  - Any signal travels through the whole cable in both directions.
  - At both ends of the cable the terminating resistors make sure that there are no reflections going back.
  - Signal speed is limited, i.e. it takes a while until the signal could be heard by all nodes.
  - Two signals on the medium at the same time result in garbage and neither can be used.

Carrier sense multiple access/collision detection CSMA/CD

Carrier Sense Multiple Access

- Any Ethernet station which wants to send, first listens to the cable, whether there is already a signal on it.
- If the cable is in use, the station waits and tries again after a while.
- If the cable is free the station starts sending a limited amount of data–a so-called packet.

Collision Detection

- While the station is sending, it continues to listen whether another signal shows up. (E.g. two stations may see a free medium and both start sending.)
- When a sending station sees a collision of its signal with another signal it stops sending and
  - sends a special jamming signal to tell all others that the signals on the cable are corrupted.

Carrier sense multiple access/collision detection CSMA/CD

After a Jam

- After a while the jamming signal travelled through the whole cable and the cable is free of signals again.
- After a random (!) delay, the stations which did not succeed to send will try again.
  - Hopefully, they will be more lucky this time.

Really?

- CSMA/CD works astonishingly well even under high load i.e. ≥80% bandwidth utilization.
  - With today's elaborate switches and concentrators
    - Full duplex mode in switches resulting in several distinct point-to-point connection
    - only a few packets have to be sent to all stations
    - for the bulk of data there is no collision at all

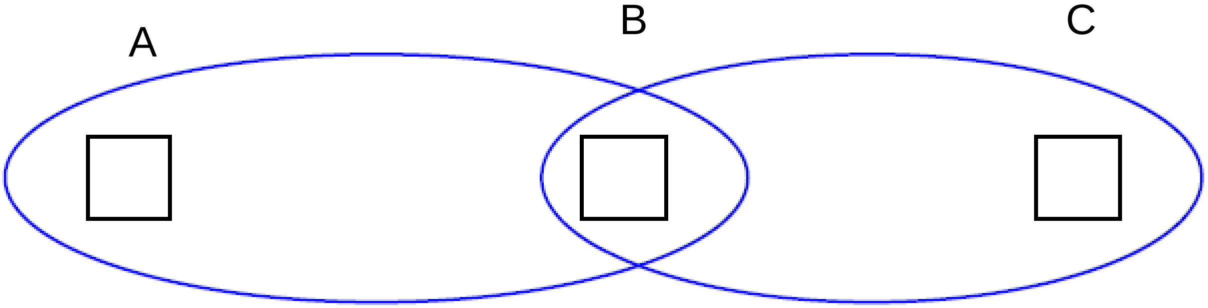
Data Link Layer in WLAN: Hidden Terminal problem

Hidden Terminal Problem

- Station A and C do not see each other
  - If A is communicating with B, C does not know about it
  - If C would communicate with B, a collision would occur

→ Collision avoidance

→ CSMA/CA



CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

- We need to avoid collisions instead of just detecting and reacting

- Carrier Sensing
  - Free for a certain timeframe → Wait a backofftime and start sending
- Receive a packet:
  - Wait, then send ACK
- Congestion: two nodes with same backoff time → ACK Timeout → Random ait

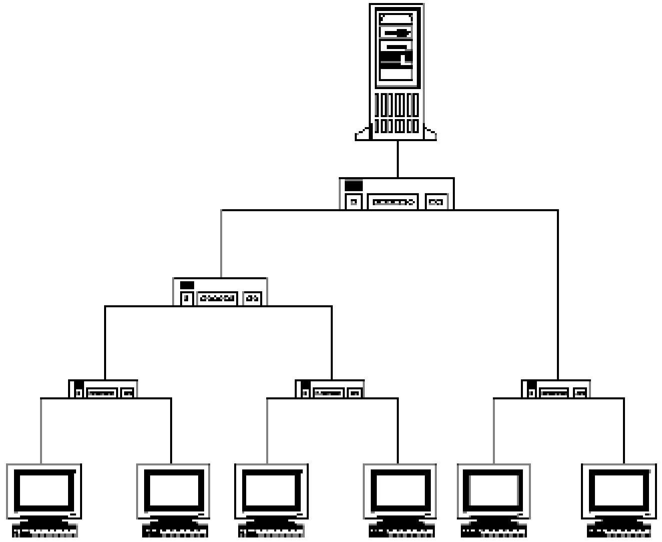
- Addressing the Hidden station problem:
  - A station which sees a hidden station problem, sends a signal package
  - RTS/CTS – Request to Send / Clear to Send mechanism
    - RTS → CTS
    - During the communication, all other stations are quite

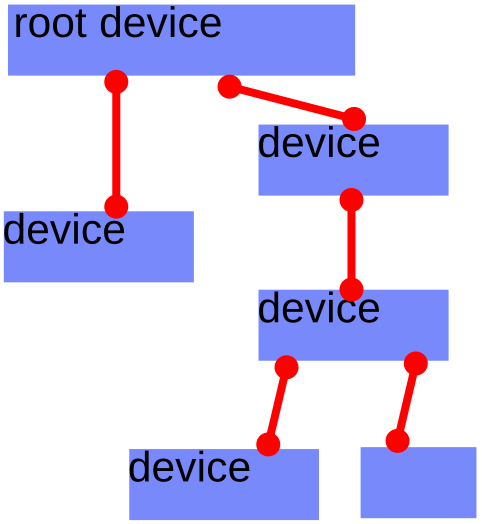
How to characterize a network: Topology

- Tree
  - Hierarchical
  - Messages travel to their parental nodes
  - Extension to the star topology

- Cheaper compared to star
- Root node failure is fatal
- Split brains

- Network usage: SNA

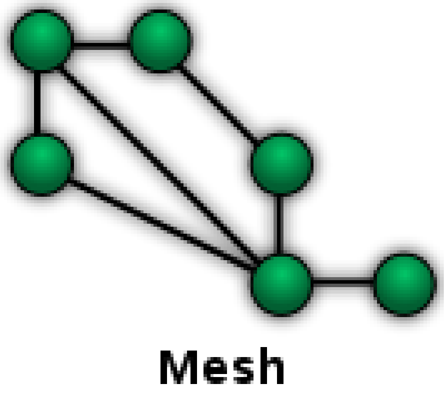


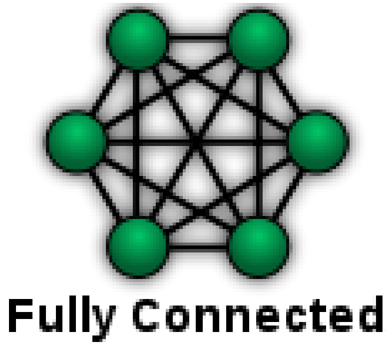


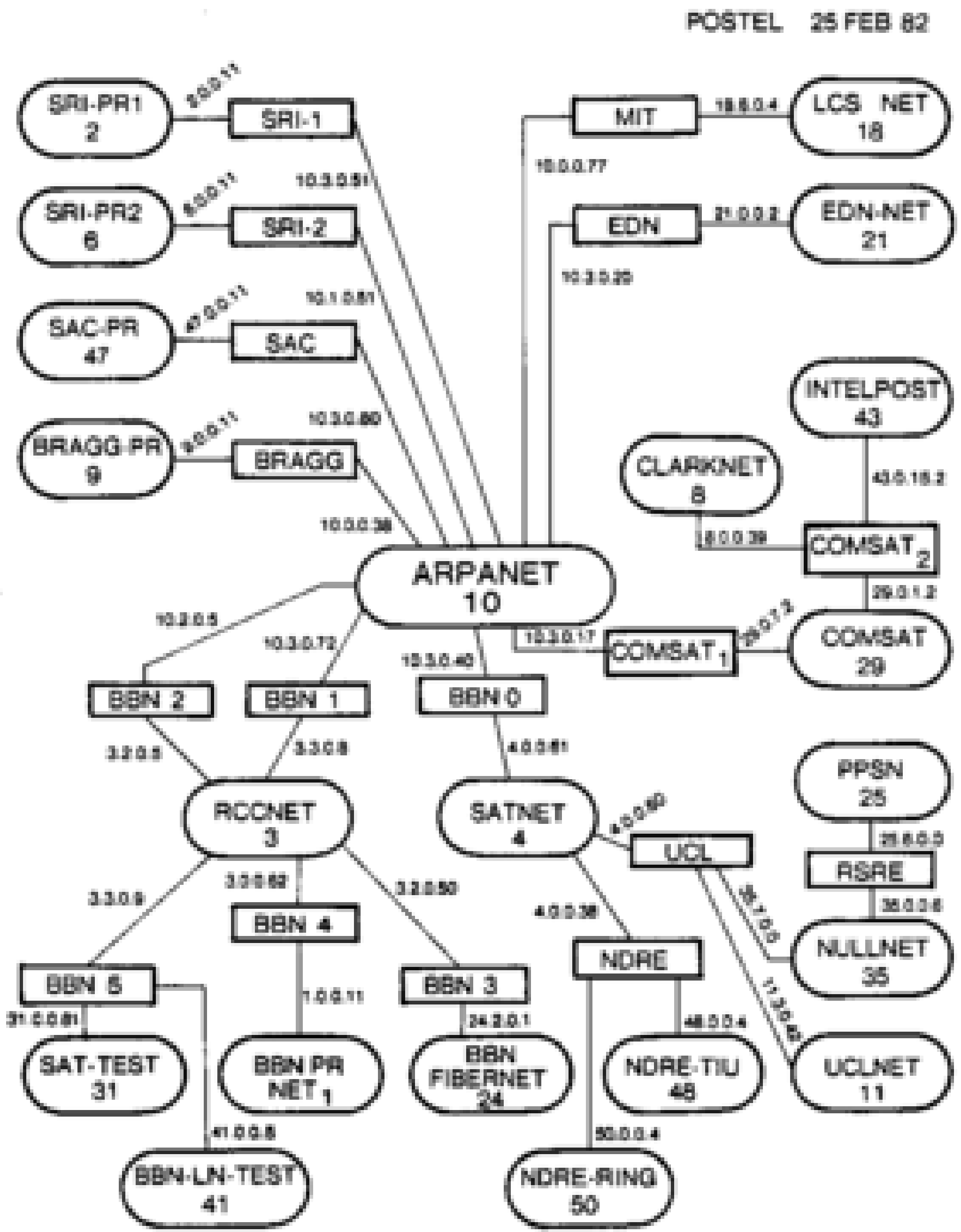
How to characterize a network: Topology

- Meshs
  - Partially or fully connected
  - Full graph:
    - All points are rearchable via point-to-point link

- Low distances or high costs
- Maximize availability and latency
- Dead station and dead link problem (partially) eliminized
- Routing necessary

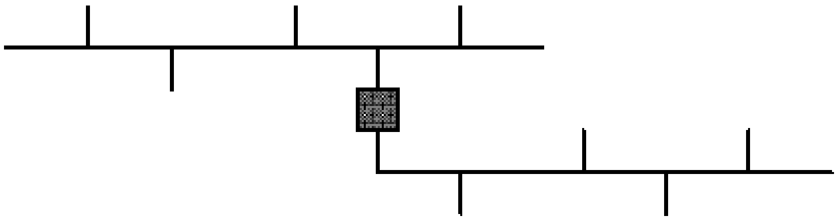




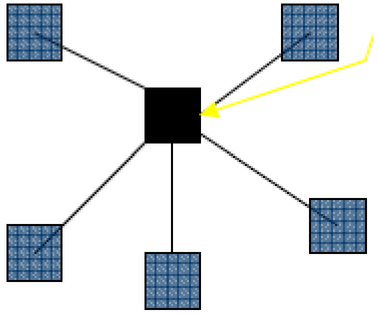

POSTEL 25 FEB 82
SRI-PR1
2
SRI-1
SRI-PR2
6
SRI-2
SAC-PR
47
SAC
BRAGG-PR
9
BRAGG
MIT
LCS NET
18
EDN
EDN-NET
21
INTELPOST
43
CLARKNET
8
COMSAT 2
ARPANET
10
COMSAT 1
COMSAT
29
BBN 2
BBN 1
BBN 0
RCCNET
3
SATNET
4
UCL
PPSN
25
RSRE
NULLNET
35
BBN 4
BBN 5
BBN 3
NDRE
SAT-TEST
31
BBN PR
NET 1
BBN
FIBERNET
24
NDRE-TIU
48
UCLNET
11
BBN-LN-TEST
41
NDRE-RING
50

Network elements

- Repeater
  - Physical layer
  - Electromagnetic signal



- Hub
  - Physical layer



- Switch
  - Active Routing
- Bridge
  - Connecting two different networks
- Structured cabling Plant, Building, Plugs
- Gateway

Network communication protocols

- **Ethernet**
  - IEEE 802
  - TCP/IP protocol stack
  - Connection orientation possible
  - Packed switched

- ATM
  - Asynchronous with variable sized packages
  - Packed/circuit, connection-orientated
  - Last mile, ISDN, Telco carrier backbones

- SONET, SDH
  - Synchronous Optical Networking (SONET)
  - Synchronous Digital Hierarchy (SDH)
  - Fully synchronic, optical based, rather protocol-stack neutral (transport protocol), circuit switched
  - Telecommunication / Carrier networks and backbones

- Miscellaneous
  - AppleTalk
  - IPS/SPX
    Novell Netware
  - NetBIOS, NetBEUI / NetBIOS Enhanced User Interface
    Microsoft
  - SNA
    IBM Systems Network Architecture
    Mainframe

Standardization: ITU

- International Telecommunication Union
- UN Agency, Geneva

- ITU-T Standard (CCITT)
  - Frequencies (→ ISM)

  - V.## Standard for analogue communication
    - Modem com
  - X.## Standard for networks
    - X.500 – Directories
    - X.509 – Asymmetric Encryption and Authentication

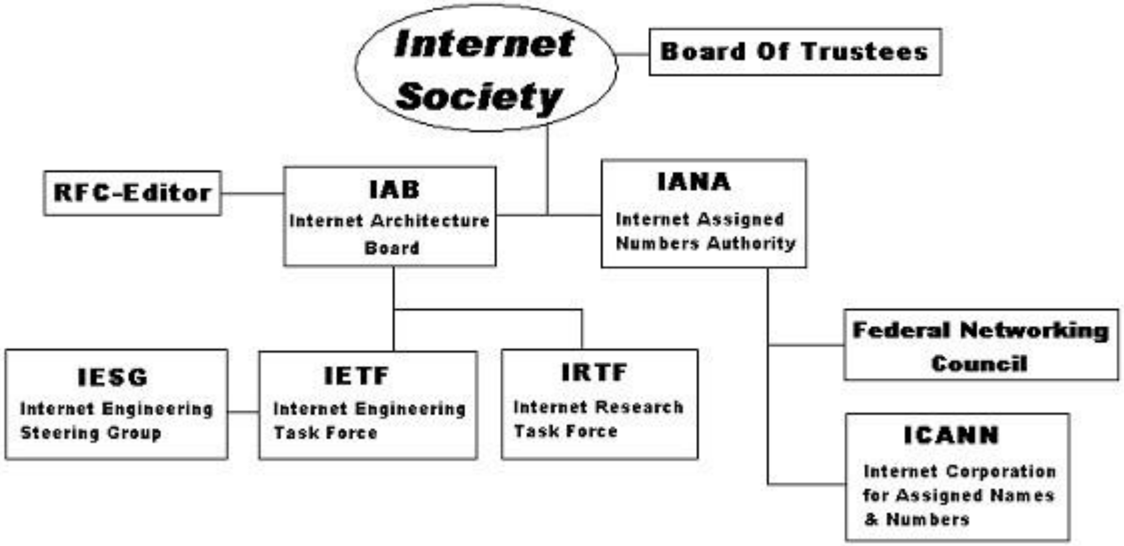
Standardization: IEEE

- Institute of Electrical and Electronics Engineers
  - Industry standards
  - Electrical, Electronics, Communications, Computer Engineering, Computer Science and Information Technology
  - Lots of recommendations are taken over as ISO standards

- IEEE working groups and standards
  - 1284 – parallel interface
  - 802 – LAN, WLAN, Bluetooth, …
  - 1003 – POSIX
  - 1149 – JTAG
  - 1394 – Firewire

- IEE standards usually are physical standards and standards concerning the lower level access methodologies

Standardization: Internet Society, IETF, RFCs…



- Internet Engineering Task Force
  - Open discussion groups (Working groups)
- Internet structure (registrar, DNS, networks)
  - Internet Assigned Names and Numbers Authority (IANA)
    - Internet Corporation for Assigned Names and Numbers (ICANN)

Standardization: Internet Society, IETF, RFCs…

- **Request for Comments - RFC**
  - 1969 (ARPANet decade)
  - IETF memorandums
  - Discussions, specifications, protocols, procedures, …
    - Informational, Experimental,
    - BCP   Best current practice
    - STD   Standard
  - Precise technical language

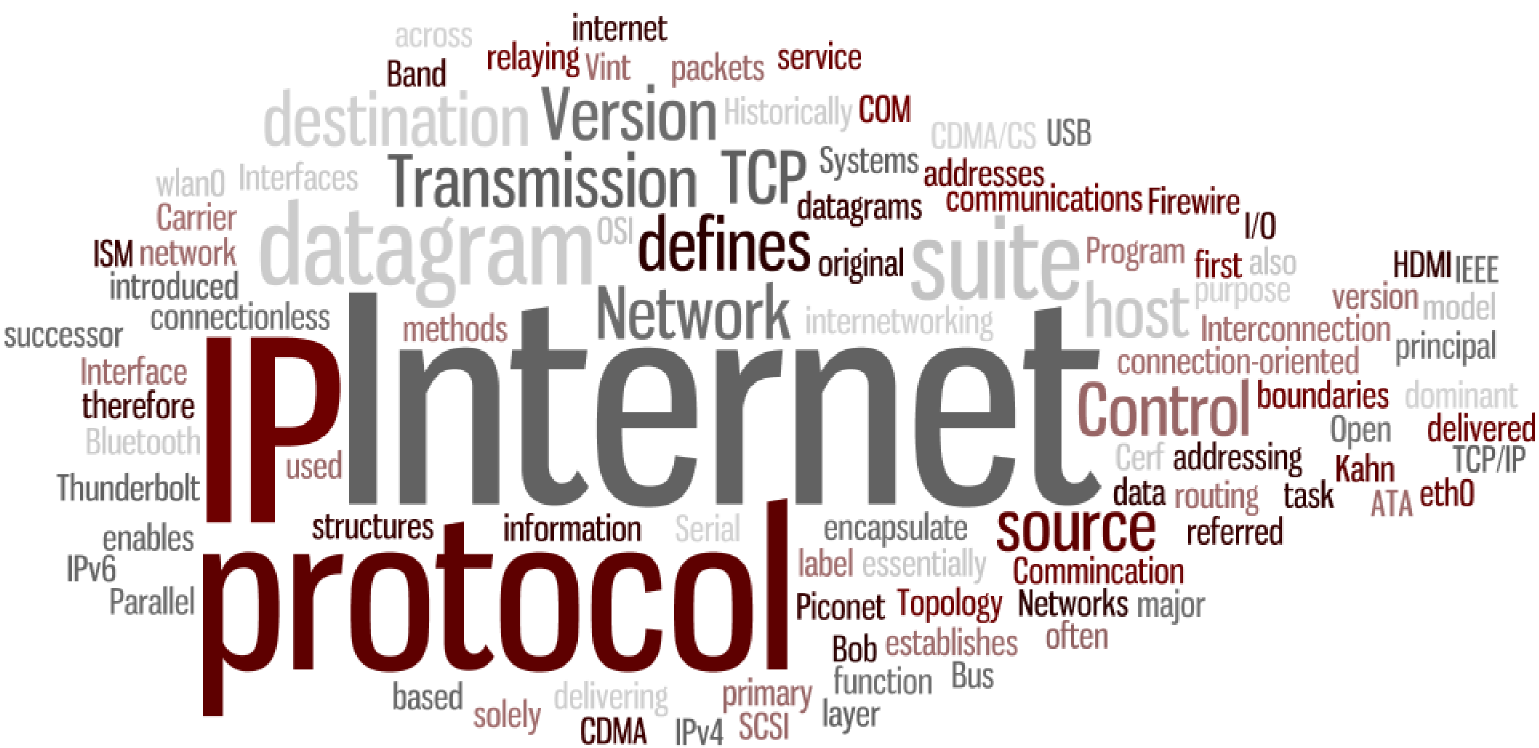
RFC 791	IP
RFC 768	UDP
RFC 793	TCP
RFC 821	SMTP
RFC 959	FTP
RFC 1034	DNS
RFC 1700	IANA
RFC 2616	HTTP 1.1

- All RFCs are openly available
  - http://www.rfc-editor.org/rfc.html
- An RFC is not a standard per se
  - Acceptance through general IETF discussions and by other organizations

RFC 1462 = FYI on What is the Internet?
RFC 2606 = Reserved Top Level DNS Names
RFC 2795 = The Infinite Monkey Protocol Suite
RFC 1149 = A Standard for the Transmission of IP Datagrams on Avian Carriers

Sebastian Welter

OSI Reference Model



OSI Reference Model

- Developed by the ISO, International Standardization Organisation, starting 1977
  - ISO/IEC 7498-1
  - Originally intended as a full set of protocols for cross platform, vendor independent data communication:
    - **Open System Interconnect**
  - Most OSI protocols took too much time and were too complex to become accepted.

- **Nowadays used as an abstract model to explain and understand data communication between systems.**
  - 7 layers
  - The goal is to exchange data between systems.
  - The involved systems – sender, receiver and optional intermediate nodes – are structured according to the 7 layers.

OSI Model

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

http://en.wikipedia.org/wiki/OSI_model

OSI Model

7	**Application layer**	**Anwendung**	HTTP, SMTP,…
6	**Presentation layer**	**Darstellung**	MIME
5	**Session layer**	**Kommunikations-steuerung**	Pipes, SOCKS
4	**Transport layer**	**Transport**	TCP, UDP, …
3	**Network layer**	**Vermittlung**	IP, ARP, ICMP, …
2	**Data Link layer**	**Abschnittsicherung**	Ethernet, ATM, …
1	**Physical layer**	**Bitübertragung**	Ethernet, Bluetooth,…

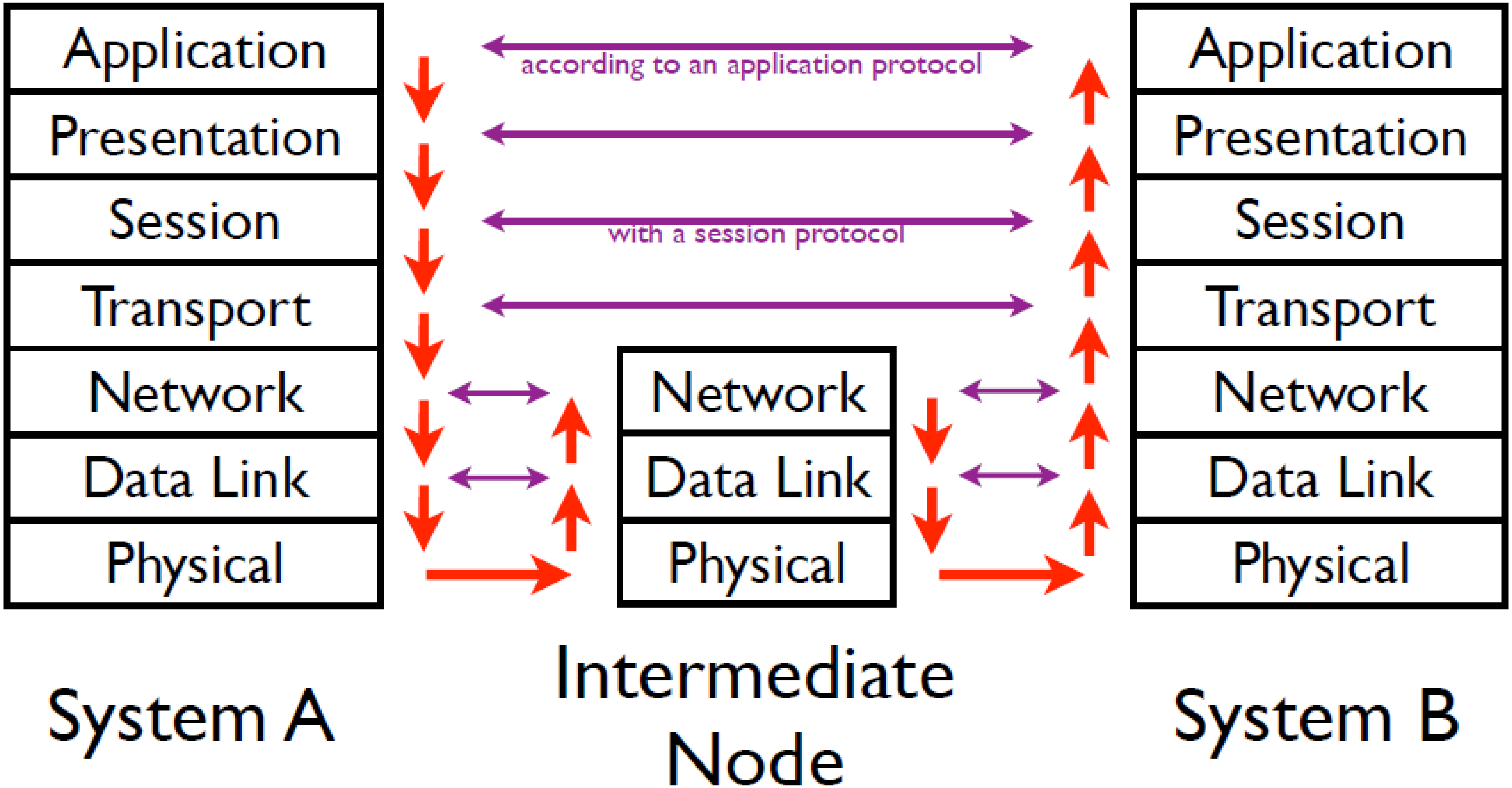
Communication in OSI

1. Data is passed down (in packets) through the layers from application layer to physical layer in the sender.
1. Then the physical layer transfers the data across the medium
2. Eventually the data moves up in reverse order from physical layer to application layer in the receiver.

- Only the corresponding peer layers of two systems communicate logically with each other by means of their special protocols.

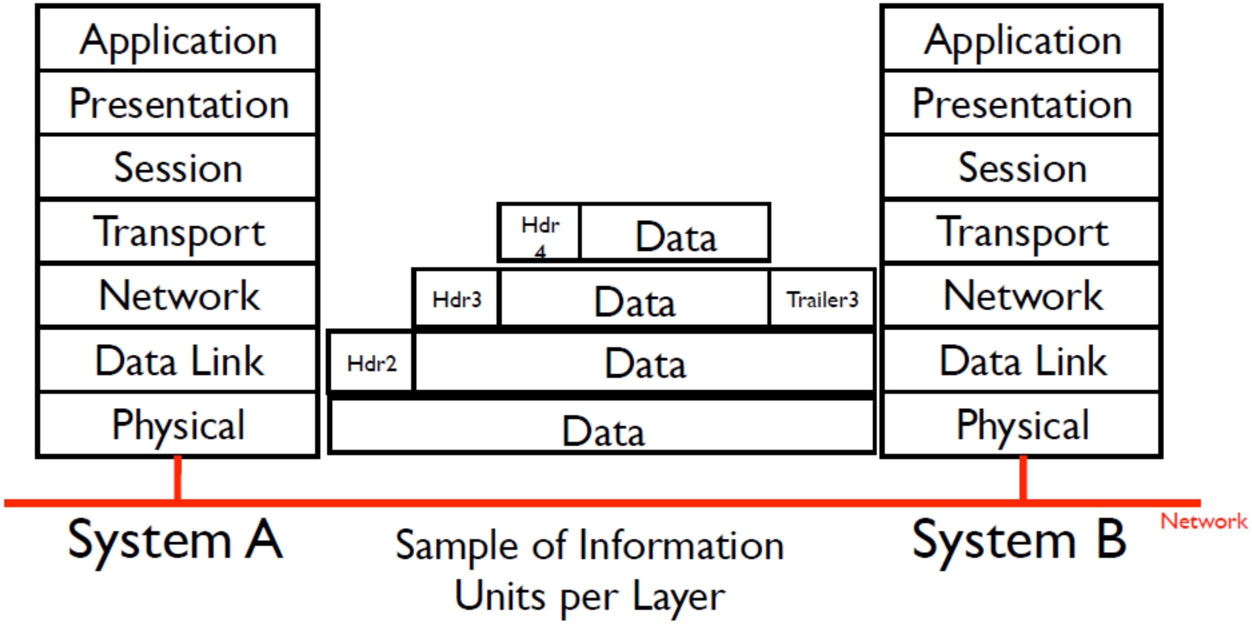
Application	Data
Presentation	
Session	
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

Communication in OSI

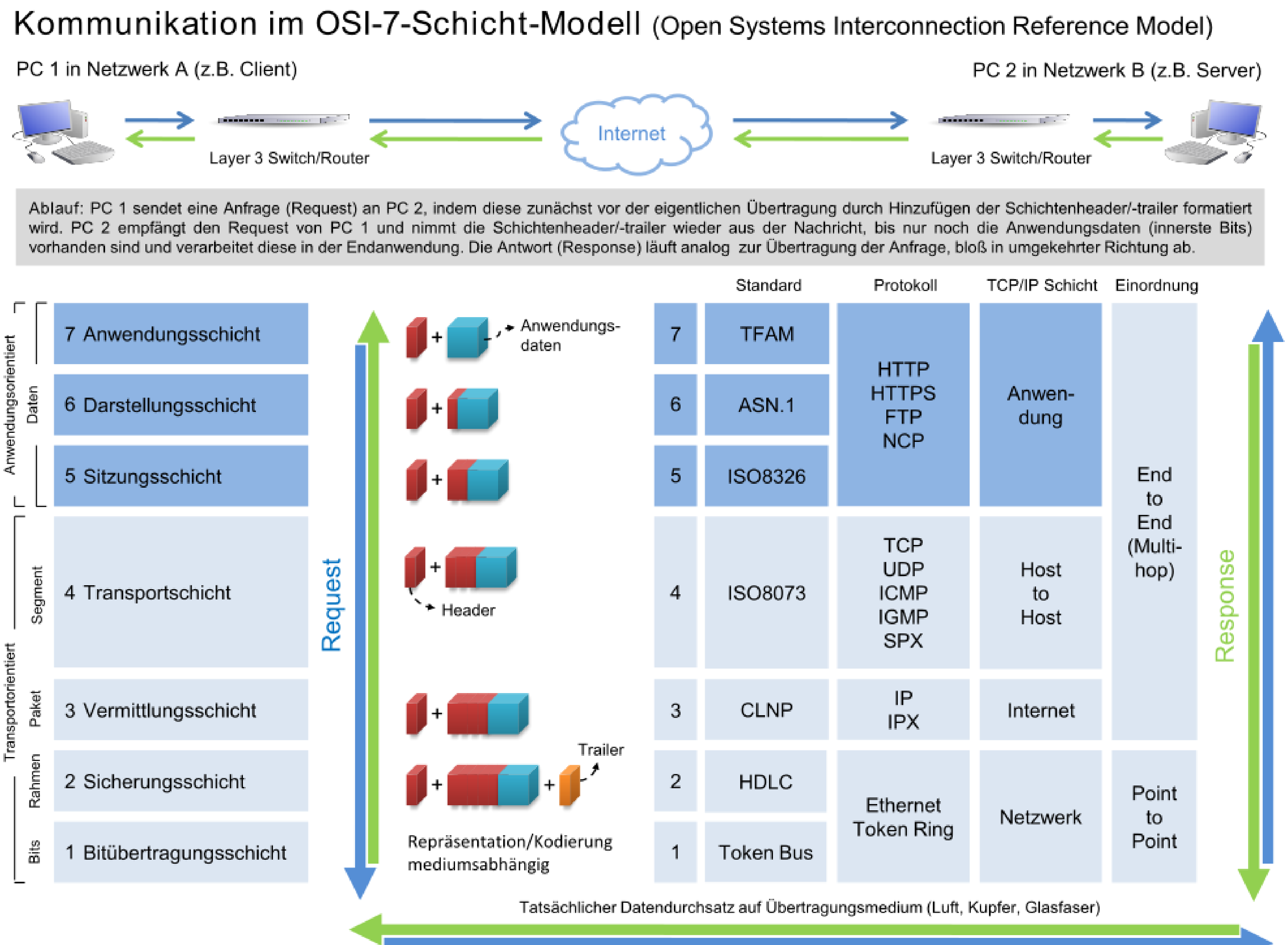


OSI Layer communication

- Each layer fulfills specific tasks.
  - Each layer provides services for the next higher layer and in order to do so requests services from the adjacent lower layer.
  - Layers may modify data from the upper layer e.g. encryption or packetizing.
- Layers may add their own data in the form of special headers and/or trailers
  - e.g. addressing information, error checking, sequence order
  - Of course, layers also have to remove header and trailer data at the end



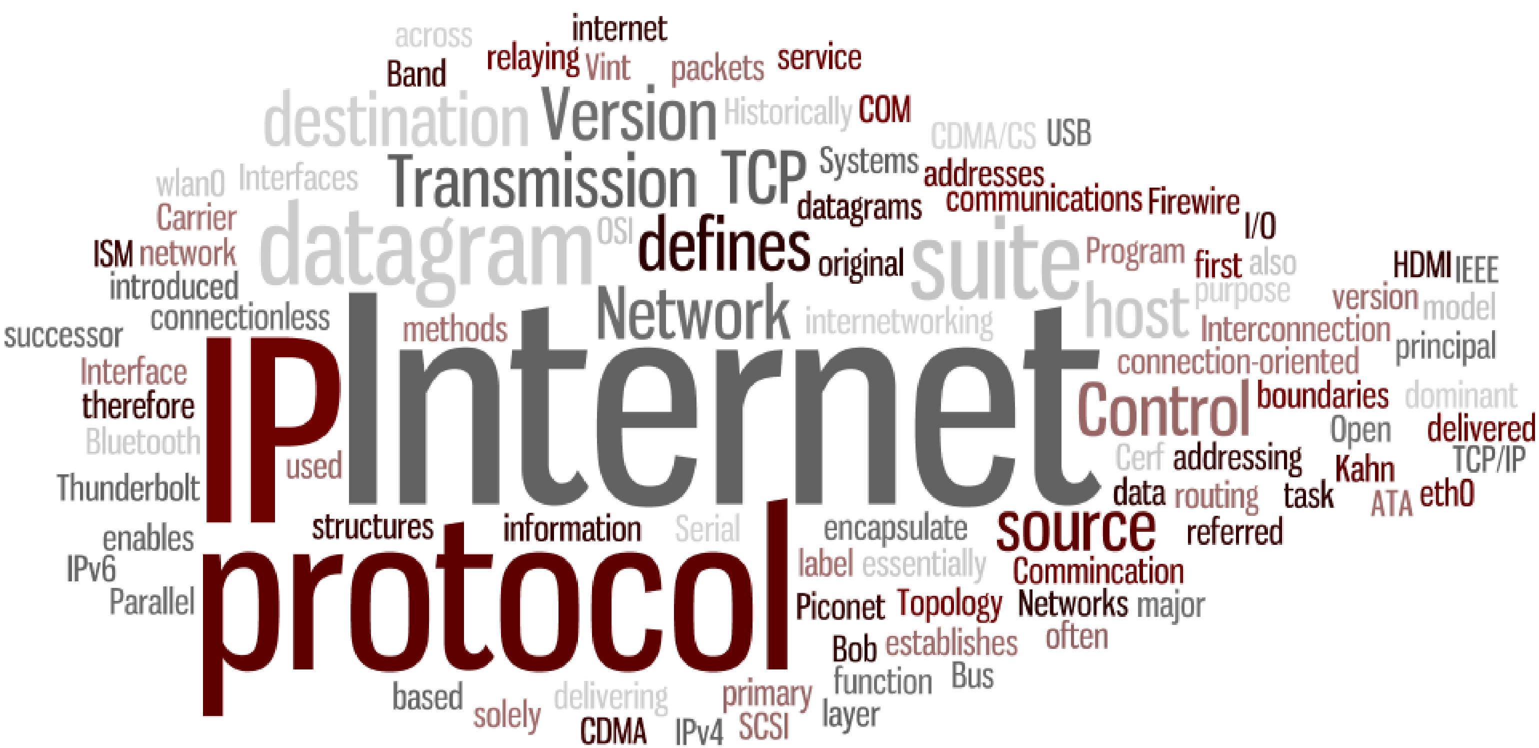
OSI Reference Model



http://de.wikipedia.org/w/index.php?title=Datei:Osi_7_layer_model.svg

Sebastian Welter

Ethernet



Ethernet

- Is a great success story with enormous technical advances and more to come.
  - Can be used with many protocols at the same time: TCP/IP, SNA, DECnet, LAT, Transdata, Netbios, Netware IPX, AppleTalk,
  - … Main protocol today is TCP/IP.
- Is available in many devices not just computers!

- Developed in the 70s by Xerox, DEC, Intel
  - Later on standardized as IEEE 802.3, ISO 8802.3

- The main networking protocol base for IT communication
- Ethernet is a transport protocol – it takes care of the low-level details

Ethernet - Speed

- Initially Ethernet was 10 Mbps
  - i.e theoretically about ≥1.2 MBps data
  - Postscript printers (without spool system) handle print jobs with about 300-400 kBps, i.e. three active PostScript printers saturate a standard Ethernet
- Fast Ethernet 100 Mbps
- Gigabit Ethernet: 1000 Mps (1 Gbps)
  - 1000 BASE SX Short wavelength fibre
  - 1000 BASE LX Long wavelength fibre
  - 1000 BASE CX Copper (Cluster, Racks… < 25 m)
  - 1000 BASE T 4 Pairs Cat 5 UTP or 2 Pairs Cat 6 (or higher)
- Now shipping: 10 Gbps
- Autosensing

IEEE Nomenclature - Ethernet

- ##BASE## 10BASE2/5

- 10BASE2
  - 10 – Transmission rate in Mbs
  - BASE – Transmission method
  - 2 – maximal segment length in factors of 100 meter

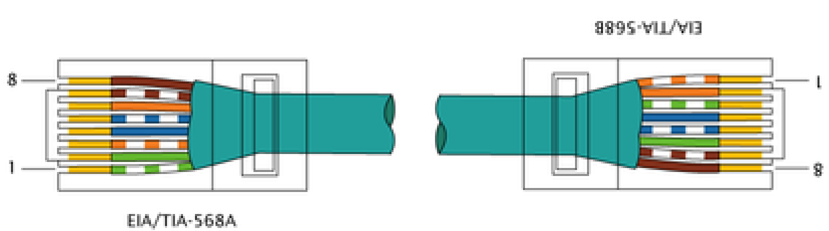
- 100BASET
  - 100 – Transmission rate in Mbs
  - BASE – Transmission method
  - T – Twisted Pair or Token Ring
  - F – Fibre Channel

IEEE	*Name*	*Yr*
802.3a	10BASE2 Thin Ethernet	85
802.3c	10 Mbps Repeater	85
802.3d	FIORL Fibre Optical Inter Repeater Link	87
802.3i	10BASE T	90
802.3j	10BASE F	93
802.3u	100BASE T	95
802.3ab	1000BASE T	99

Ethernet cabling

- Main stream today: twisted pair cabling
  - 10Base-T Ethernet
  - two pairs of twisted copper, one for sending and one for receiving
  - RJ45 connectors
  - star or tree topology with hubs, switches, …
- Attention: Direct link between two devices (without hub) usually requires cross-over cable–but some PCs don’t care about (Autosensing)

- Fast Ethernet 100Base-T uses cables with 2 or 4 pairs of twisted copper wires
  - Gigabit Ethernet 1000Base-T uses cables with 4 pairs of twisted copper wires or optical fibres
  - 10 Gigabit Ethernet requires optical fibres or twinax (one coax for sending and one for receiving) or limited length copper.



CAT Cabling

CAT	Max. frequency	Example
1	100 Khz	ISDN Base
2	1 Mhz	ISDN Multiplex
3	16 Mhz	10 BASE T
4	20 Mhz	16MBit Token Ring
5	100 Mhz	Fast Ethernet
6	200 Mhz	ATM (155 Mbit)
7	600 Mhz	Gigabit Ethernet, 622-ATM

- 1000 BASE T 4 Pairs Cat 5 UTP or 2 Pairs Cat 6 (or higher)

Ethernet Frame

- Ethernet Frame

PRE	SOF	DA	SA	L/T	Data	CRC
7b	1b	6b	6b	4b	46-1500b	4b
Preamble	Start of Frame	Destination Address	Source Address	Data length and type	Data	
101010…	10101011	MAC	MAC	*Ethertype* VLAN Tag	(Data)	32 bit CRC Checksum
Synchronization	fix			Prio, Signal, 12 bit VLAN ID	(Padding)	

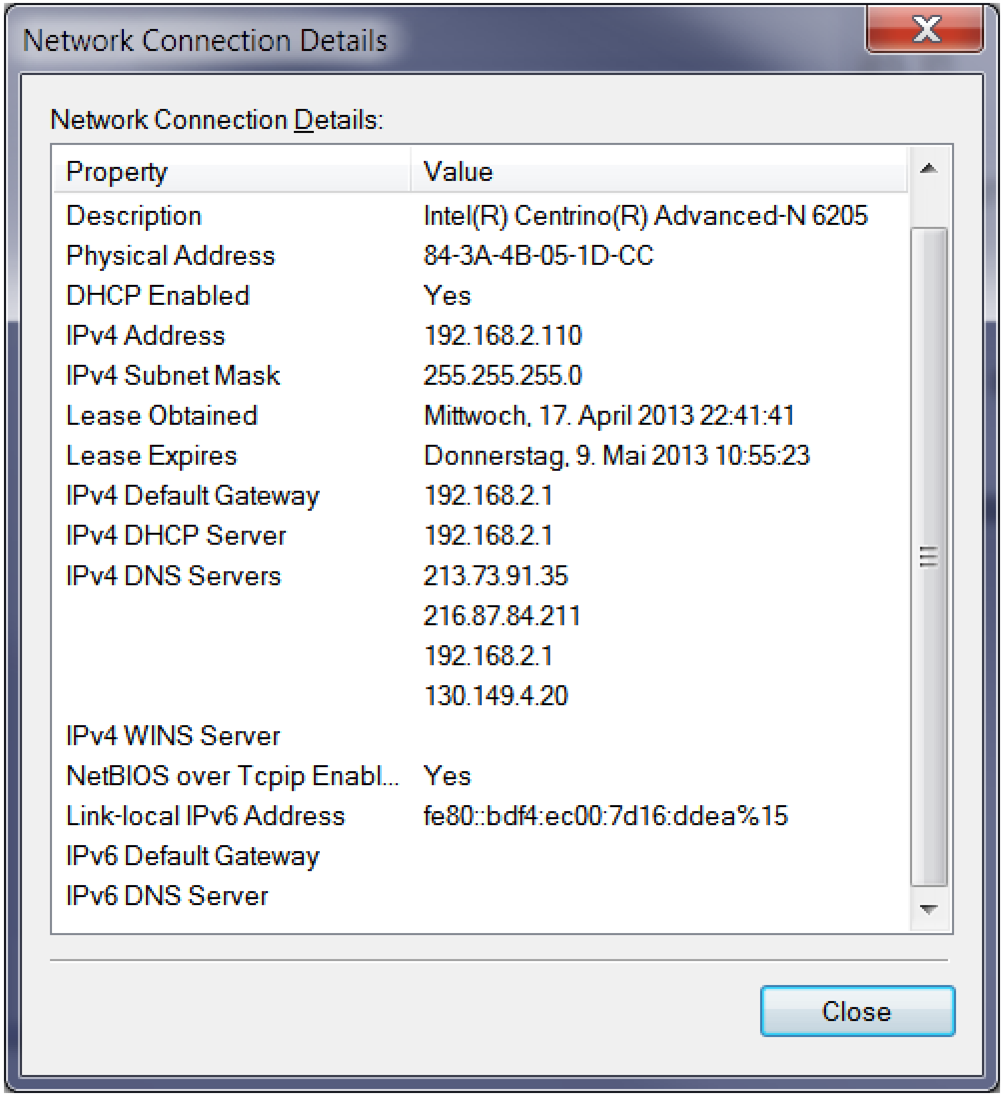
Ethertype: 0800 IPv4, 0806 ARP, 0842 WOL, 809B AppleTalk, 86DD IPv6, 8870 Jumbo Frames

Addressing in Ethernet with TCP/IP

- Physical Address: MAC
  - Ethernet
  - IEEE 802 MAC, 48bit
  - 00:00:00:00:00:00

- Logical Address: IP
  - IPv4
    - 32 bit
    - 192.168.100.100
  - IPv6
    - 128 bit

- Network layer routing



MAC

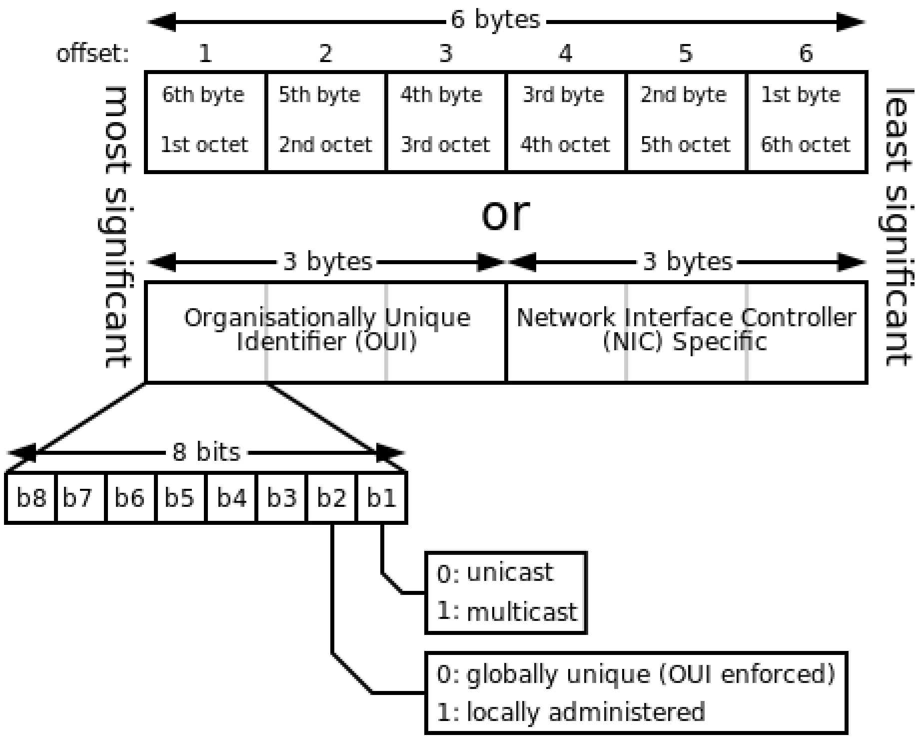
- Every network adapter has its own unique MAC address usually made up
  - of a unique vendor identification and
  - a unique id managed by the vendor for its products.
  - “burned in”

00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF

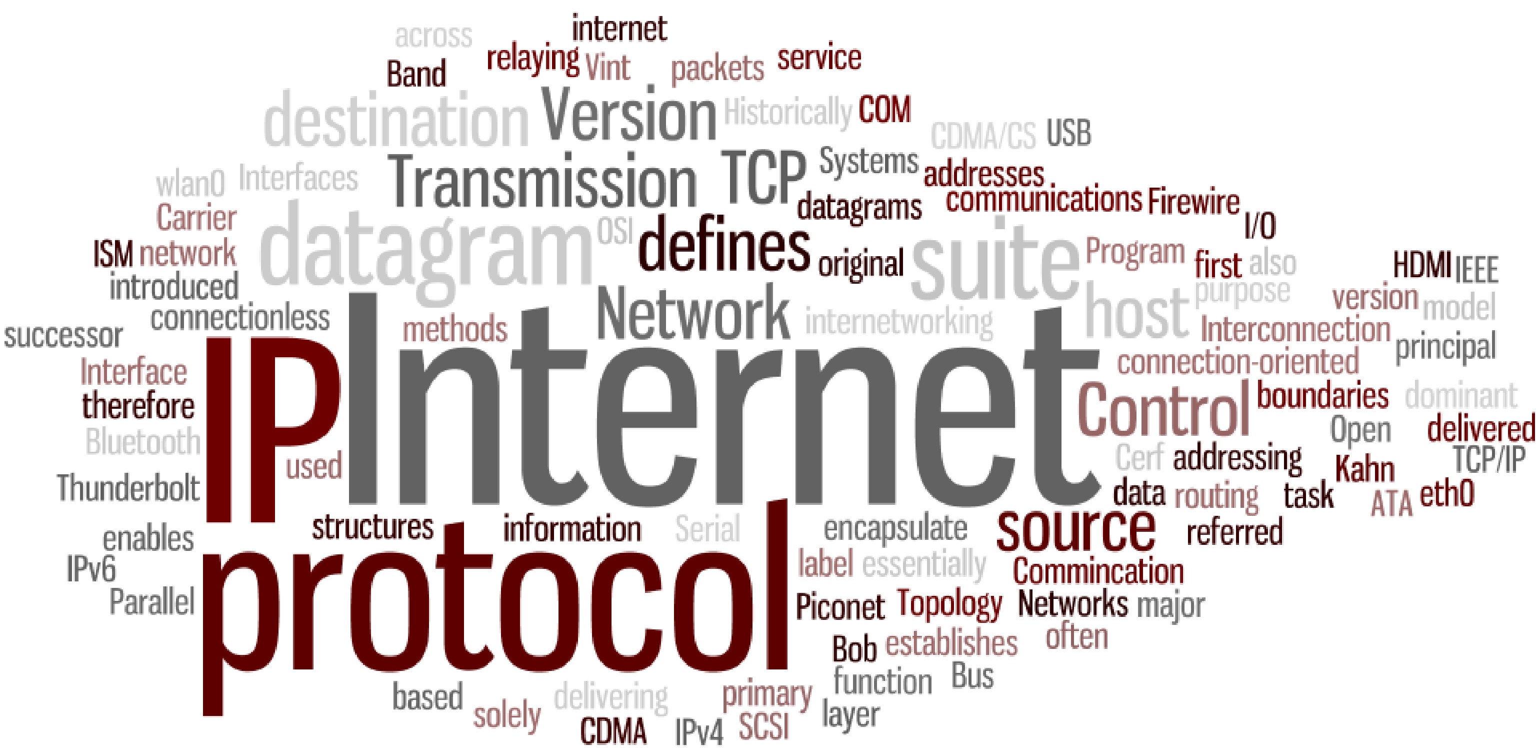
- Most MAC addresses are 6 byte / 48-bit long, e.g. for
  - Ethernet, WLAN, Bluetooth;
  - IEEE 802 MAC – MAC-48
  - FireWire: 8 byte

- In addition to the unique network adapter hardware addresses there are MAC group addresses for broadcasts and multicasts as well.

- MAC Spoofing
- Promiscuous mode



OSI Reference Model Layers



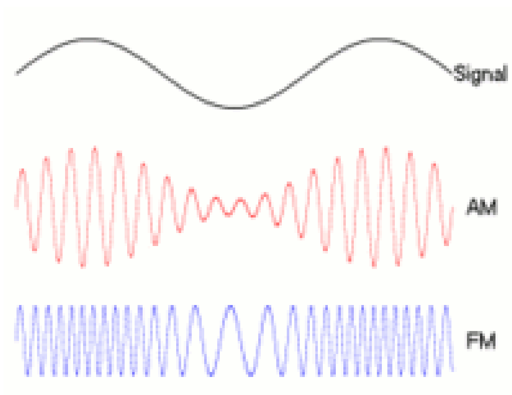
OSI Layer 1: Physical Layer

Application
Presentation
Session
Transport
Network
Data Link
Physical

- Transmits a raw bit stream over the physical medium – by cable or wireless – between two adjacent nodes
  - Defines physical aspects cables, cards, voltage levels, etc.
  - Specifies hardware and how it is attached: size and shape of connectors, antenna, etc.

- E.g.:
- 10BASE2 Ethernet: Coaxial cable, 200m, 10MBit/s
- 100BASET Ethernet: Twisted Pair cable, RJ45 jack, 100MBit/s
- RS2323C: Serial, Pin 1: in, Pin 2: Out, Pin 3: CTRL, …

- Wireless, e.g. WLAN: Modulation
  - Frequency (FM)
  - Amplitude (AM)
  - Phase (PM) – phase change by 180°



OSI Layer 2: Data Link Layer

- Takes care how to convert between data frames and raw bits (10011001001101l…)
  - Responsible for error-free transfer of frames to other node via the physical layer
  - Defines the methods used to transmit and receive data
    - signaling involved to transmit and receive data
    - the ability to detect signaling errors

- Usually the data link layer is split into two:
  - Logical Link Control
    - error correction and flow control
    - manages link control
- Media Access Control
  - communicates with the adapter card
  - controls the type of media being used (coax, twisted pair, optical fibre, wireless etc.)
  - provides MAC addresses for the network adapter

Application
Presentation
Session
Transport
Network
Data Link
Physical

OSI Layer 2: Data Link Layer

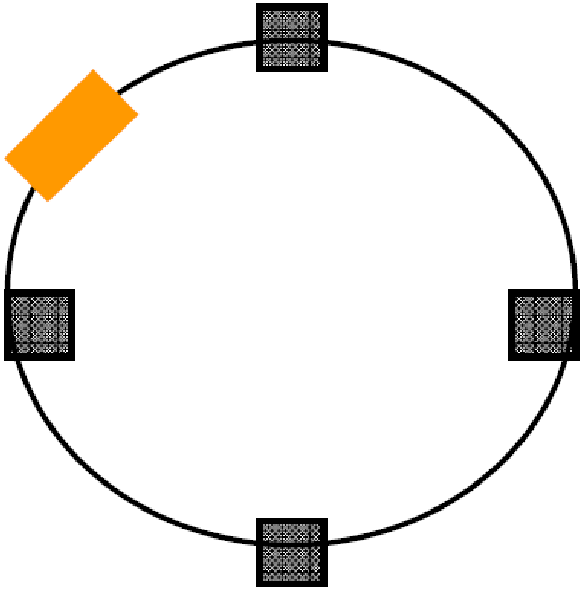
Application
Presentation
Session
Transport
Network
Data Link
Physical

1. Place the data into a frame
   – Frameformat and address
   – Each network type and protocol has its own type of frame and its own frame size: MTU
     • Ethernet: 1550b
     • ATM: 53b
     • Token Ring: 4000b

2. Place the frame into the network
   → Collision detection / avoidance
   → CSMA/CD

Token Ring: Token Parsing

- 802.5
- 3 Byte Token
  - Präambel | Access Control | …
- Wenn nun jemand sendet, schnappt er sich den Token, ersetzt, Präambel und Access control durch MAC-Adresse des Ziels und Daten.
- Der Empfänger sieht seine Adresse, nimmt die Daten raus und lässt den leeren Token wieder aufs Medium



OSI Layer 3: Network Layer

- Routing
- Fragmenting – along with the MTU
- Addressing

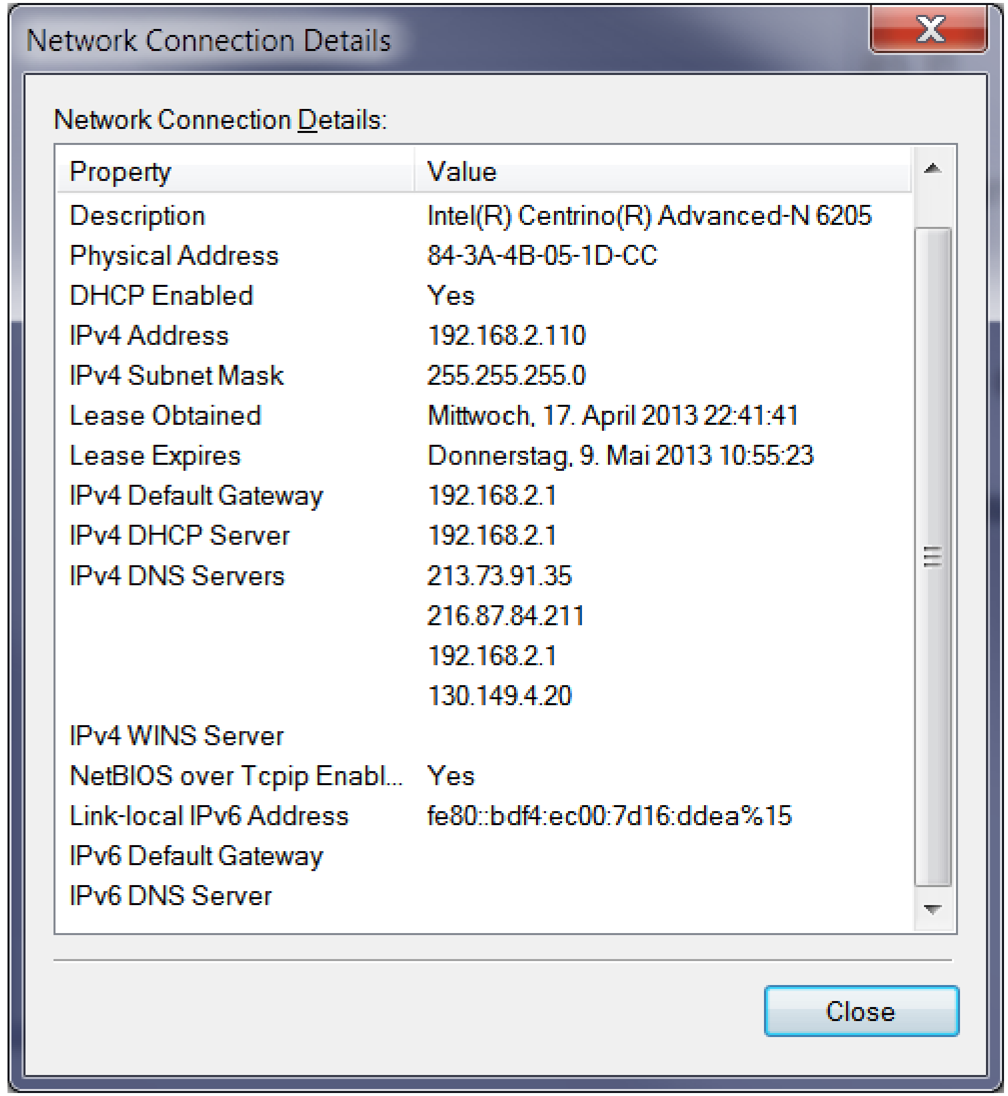
- Handles addressing and routing. Also layer 3 knows unicast, multicast and broadcast addresses.
  - Translates logical network address and names to their physical address e.g. IP to MAC address (for **unicast** as well as for multi- and **broadcast**).
  - Responsible for addressing

- Determines routes for sending data
  (Attention: Some non-IP protocols cannot be routed!)

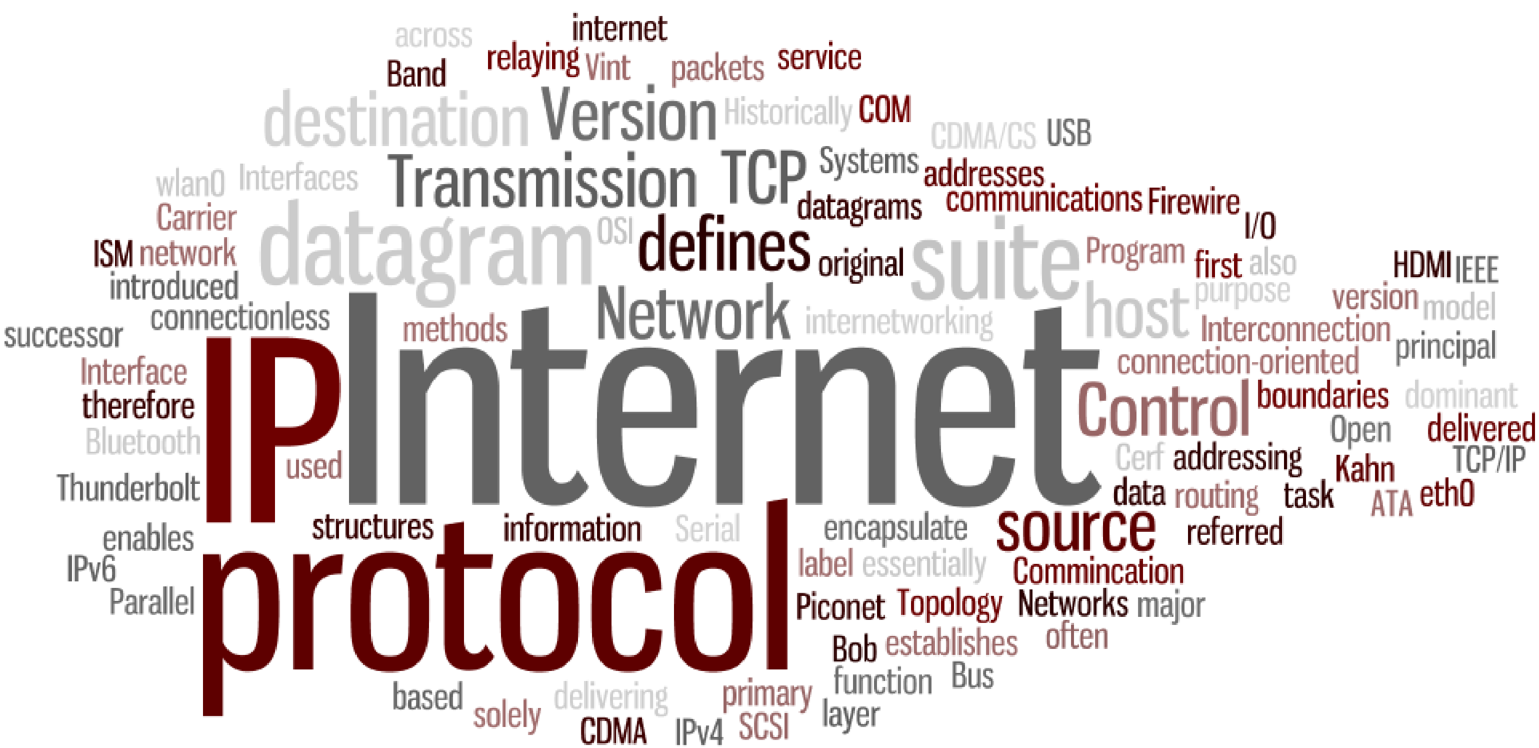
Application
Presentation
Session
Transport
Network
Data Link
Physical

Addressing in Ethernet with TCP/IP

- Physical Address: MAC
  - Ethernet
  - IEEE 802 MAC, 48bit
  - 00:00:00:00:00:00
- Logical Address: IP
  - IPv4
    - 32 bit
    - 192.168.100.100
  - IPv6
    - 128 bit
- Network layer routing



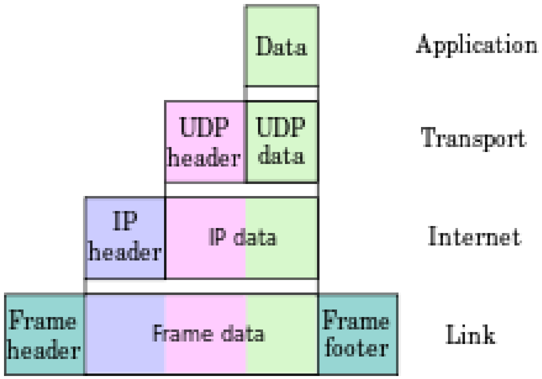
Internet Protocol (IP)



IP – Internet Protocol

- History: starting 1974…
  - Designed as the base below the Transmission Control Protocol –TCP
  - Modularized as:
    - IP base protocol, package-switched
    - TCP connection-orientated
    - UDP connection-less
    - (Others)

- Internet Protocol
  - Packages
  - Designed for
    - unreliable network components
    - dynamic network layouts
  - Connection-less
  - Logical adressing



IP – Internet Protocol

- Communication over the Internet as well as in LANs is mainly based on TCP/IP protocols.
  - All systems, nodes or hosts are identified by unique IP addresses.
    - A node can carry one or more IP addresses.
  - The IP addresses can be static or is assigned dynamically (usually when the node starts up)
    - Dynamic network layout – IP address is a logical address
- The IP address is mapped to the MAC address by the network layer.
  - e.g. ARP protocol

IPv4 header

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">Time To Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="32">Source IP Address</td></tr>
<tr><td colspan="32">Destination IP Address</td></tr>
<tr><td colspan="32">Options (if IHL > 5)</td></tr>
</table>

- IHL = Internet Header Length in 32bit words
- DSCP = Differentiated Services Code Point, partially used in Voice-over-IP
- ECN = Explicit Congestion Notification, optional
- Length of the total package
- Identification = multiple fragment identification
- Flags: 0|DF|MF -- Don’t Fragment | More Fragments
- Fragment Offset, in 8-byte units
- TTL, Header checksum – changed by every router
- Protocol indication of the transported data (TC, UDP, ICMP, …)
- Source and target addresses

IP v4 vs. IP v6

- The current IP addressing scheme is called “IP v.4” and uses 32 bit (4 byte) per address.
  - Address space: 2^{32} - 4’294’967’296 addresses, approx. 3.7 billion usable
  - e.g. 9.155.23.123

- The next system is called “IP v.6” and will use 128 bit (16 byte) per address.
  - Address space: 2^{128} – 340 sextillion addresses
  - e.g. 2001:0db8:85a3:0042:1000:8a2e:0370:7334

  - IP v.6 handles many more addresses e.g. for every mobile phone, car, coffee machine.
  - IP v.6 offers enhancements in other areas

- Adoption of IPv6:
  - Implemented in all major operating systems and many applications
  - Backbones and major routers are becoming IPv6 compatible
  - Very less usage in the general public

Addressing in Ethernet with TCP/IP

- Physical Address: MAC
  - Ethernet
  - IEEE 802 MAC, 48bit
  - 00:00:00:00:00:00

- Logical Address: IP
  - IPv4
    - 32 bit
    - 192.168.100.100
  - IPv6
    - 128 bit

- Network layer routing

ARP: Address Resolution Protocol (RFC 826)

1. Sender is checking is Destination and Target are in the same network → subnet mask check
2. If it is outside of the network → deliver to Gateway
3. If it is in inside the network →
   - Check if we have the MAC in the ARP cache
   - → Enter the address into the DLL frame and send
4. If we don't have the address pair in the ARP cache:
   - Send an ARP message as broadcast to all nodes in the network
     - Node with the asked IP shall return its physical address back
   - Every node in the network is receiving the message
     - The right one sends an ARP-REPLY back
5. Both nodes append their ARP cache

Internet Protocol (IPv4) over Ethernet ARP packet		
bit offset	0 – 7	8 – 15
0	Hardware type (HTYPE)	
16	Protocol type (PTYPE)	
32	Hardware address length (HLEN)	Protocol address length (PLEN)
48	Operation (OPER)	
64	Sender hardware address (SHA) (first 16 bits)	
80	(next 16 bits)	
96	(last 16 bits)	
112	Sender protocol address (SPA) (first 16 bits)	
128	(last 16 bits)	
144	Target hardware address (THA) (first 16 bits)	
160	(next 16 bits)	
176	(last 16 bits)	
192	Target protocol address (TPA) (first 16 bits)	
208	(last 16 bits)	