Terminology	explanation
Access network	offers connectivity to residential users
ACK	acknowledgement field
Address resolution protocol (ARP)	data link layer (L2) protocol translates an IP address to the MAC address of a network card (dynamically links the two in an arbitrary ARP cache)
adhoc network	network consisting of a number of communicating devices (sensors, laptops, mobile phones) of various kind that are interconneted by a wireless link, but sometimes partly also by wired technology
anycast	one-to-any
ARP usage	In broadcast, IP is broadcast, and computer associated with it responds with IP and MAC address, IP-MAC pair is saved in the router (ARP cache); non broadcast, IP is send to ARP Server (name server) which has MAC addresses of all associated computers (they register when they join the network)
ARQ Go Back n protocol	Same as stop and wait, but discards all send packets after a lost or corrupted one (usefull when recievers possess a smal reciever buffer)
ARQ Selective Repeat protocol	Same as Go back N only uses a larger window size and does not discard packets, only resends the single lost packet
ARQ Stop-and Wait Protocol	Send, wait for ACK resend if no ACK received within reasonable time (2t) send next when ACK is received (can work with a sliding window)
Automatic Repeat Request (ARQ)	protocols privding both error detection and retransmission
best-effort delivery semantics	there is no notification about packet receipt
binary exponential backoff	sender delays transmission time randomly after first collission, then twice that after the second, 4 times after the third collision etc.
Black Box	Internals of the black box are hidden, and a user can only observe, from inputs and outputs, what the black box does, i.e. what service it provides.
broadcast	one-to-all (extreme form of multicast)
Carrier sense multiple access (CSMA)	A class of DMA in packet mode "sensing" the network before sending
centralized control	a master controls each interaction in the network of systems
circuit switched network	network with dedicated end-to-end connections
Clasless inter-domain routing (CIDR)	the possibility to construct an arbitrary length of the netid (since 1993) helps cope with the shortage of IP addresses
class A subnetwork	ip address starts with a 0 bit (between 0.1.0.0 and 126.0.0.0)
class B subnetwork	ip address starts with a 10 bit (between 128.0.0.0 and 191.255.0.0)
class C subnetwork	ip address starts with a 110 bit (between 192.0.1.0 and 223.255.255.0)
class D subnetwork	ip address starts with a 1110 bit (between 224.0.0.0 and 239.255.255.255)
class E subnetwork	ip address starts with a 11110 bit (between 240.0.0.0 and 247.255.255.255)
Clear to send (CLS) frame	reply on a RTS with the same length of message already specified by the host
Communication	Exchange of information
conectionless (CL)	each packet of the same flow is delivered from source to destination independently from each other
Congestion control	the actions take by the network to recover from overload situations where considerable losses have occurred
connection oriented (CO)	All packets of a same flow follow the same path
Core network	backbone combines several edge networks
CSMA with collission detection (CSMA/CD)	When a collission is detected, a JAM signal will be broadcast, and all hosts will wait before sensing/sending as specified by the sending rule
CSMA/CD with reservation	All nodes in range of the Sender and Reciever must be silent
CSMA/CD without reservation	All nodes in range of the Sender must be silent during transmission
Cyclic Redundancey Check (CRC)	C=M.2^r + R; divide word C by generator G gives 0; divide message M (+G-1 bits as 0 at the back) to give the CRC (R) as rest
distant vector protocol	flood a list fo distances to destinations and each router has to maintain their shortest distance to a destination and construct forwarding table
distributed control	a policy or protocol of communication controls each interaction in the network of systems
Domain Name System (DNS)	a hierarchy of many name servers each responsible for a zone which is a subtree of the DNS tree adminstered separately by a DNS administrator
Dynamic Host Configuration Protocol (DHCP)	Replacement for ARP and RARP, client-server communication where client queries server for configuration parameters
Edge network	combines several access networks
encapsulation	the subsequent placing of the control and data part of a higher layer into the data part of a lower layer
error causing phenomena	thermal noise, impulse noise, all kinds of signal distortion, crostalk, echoes and reflections, fading, synchronization errors, quantization noise etc.
Ethernet	Broadcast technology with best-effort delivery semantics and distributed access control
Ethernet addresses	48-bit IEEE 802 MAC address or Multicast or broadcast (all 1's)
FIN	informs the reciever that no more data will be send
Flow control	the actions taken to control the flow of data to prevent loss, or the occupation of too many network resources
Foreward Error Correction (FEC)	error correction technique assuming the packet contains enough redundant information to correct errors
Forewarding	The action of placing an incoming IP packet to an outgoing interface, consisting of two parts, the table look up part and the packet transfer part
Frequency-division multiplexing (FDM)	frequency spectrum is divided in a number of frequency bands and each user gets a frequency band (Wave-division multiplexing (WDM) in fibre optics)
History of the internet/internet organisations	not covered here :S
Host density ratio	HD=log(n)/log(N) = Nlog(n) (n= number of objects and N is maximum number of allocatable objects)
Internet	A collection of thousands of networks linked by a common set of protocols which enable communication or/and allow the use of the services located on any of the other networks
Internet architectural design principles	goal=connectivity;method=inter-networking layer;tool=the internet protocol (IP);intelligence= end-to-end rather than hidden in the network; faith=all networks are equal; freedom=nobody owns the internet
Internet checksum	Header is C which obeys Cmod(2^16-1)=0

Terminology	explanation
Internet Control Message Protocol (ICMP)	encapsulated in an IP Packet, two modes:query makes network state information such as echo, timestamp and address mask; or error which informs the soruce of the IP packet about an error
Internet Protocol (IP)	packet delivery service that is unreliable, connectionless, best-effort
IPv4 adressing	4 bytes, x.y.z.w. consists of host-id and net-id (all hosts connected to the same network share a net-id); not related to geography;
IPv4 flag	Bit controlling fragmentation (1=do not fragment)
IPv4 fragment offset	offset measured in octets with respect to original datagram
IPv4 Header checksum	ensures integrity, based on ones complement, see Internet Checksum
IPv4 hlen	header length, measured in 32-bit words
IPv4 identification	unique integer that identifies the datagram (used when fragmenting)
IPv4 optons	allows packet to request optional features, timestamp, specific path, router alert etc.
IPv4 padding	since IP header is multiple 32 bit words padding means complementing the variable length with 0's untill it is a multiple of 32 bit words.
IPv4 protocol	specifies the upper layer protocol that created the message for example 6=TCP;17=UDP;1=ICMP
IPv4 ToS	Type of Service designed to allow routers to adjust for delay throughput reliability etc. most routers ignore this
IPv4 Total length	length (in octets) of the complete information container (header&data)
IPv4 TTL	time to live (in seconds) (in practice, it's the number of hops) if TTL reaches 0 datagram is discarded
IPv4 vers	version (IPv4 = 0100)
IPv6	IP Next Generation Ipng; not a simple derivative of IPv4;
IPv6 Addressing	x1:x2:x3:x4:x5:x6:x7:x8 ; zero complement means 0's are left out (if x2,x3,x4,x5 are 0's : x1::x3::x6:x7:x8);
IPv6 addressing improvements	expanded addressing capability (from 32 bits to 128 bits) multicast scope added; simpler auto-configuration;anycast address added; new flow labeling capability
IPv6 Destination adress	IP address of destination
IPv6 extension headers	Hop-by-hop options; Routing; Fragmentation; Authentication; Encrypted payload; Destination options
IPv6 flow label	A source may label several flows or sequences of packets belonging to a certain QoS class
IPv6 header improvements	Fixed format to all headers: no option element, no header length, added extension headers;Omission of the header checksum; Omission of the hop-by-hop fragmentation fields
IPv6 Hop Limit	Same as TTL but now in hops instead of seconds
IPv6 Next Header	identifies the type of header following the IPv6 Header (last extension header points to UDB/TCP etc)
IPv6 other improvements	Extensions to support authentication, data integrity, data confidentiality ICMP is streamlined and enhanced plug&play
IPv6 Payload Length	length in octets, only data part following header (extension header is considered part of the data)
IPv6 reasoning	Addresses is the only complelling reason routing and QoS is the same between IPv4 and IPv6; server-less plug and paly; end to end IP-layer authentication and encryption; elimination of triangle routing for mobile IP are also reasons
IPv6 Source Address	address of the originator of the packet
IPv6 Traffic Class	ID field between different classes or priorities
IPv6 version	version number is 6
link state protocol	complete topology information (complete map) flood topology information and each router maintains the entire graph of the network.
Local Area Networking (LAN)	data link layer (L2) technology, small area
Logical Link Control (LLC)	supervises MAC sublayer and provides reliable transfer of packets (or not depending on the operation mode)
Maximum Transmission Unit (MTU)	IPv4 has MTU fo 2^16 -1, depends on physical network
Medium Access Control (MAC)	Specifies the data communication in a broadcast medium between two computers by providing a virtual point-to-point communication
Metropolitan area network (MAN)	combination of several office LANs to form a corporate office or even small city
multicast	one-to-many and many-to-many communication
Multiple acces communication	design problem that arises in a broadcast medium, where every station or person recieves or hears everything.
Name server	Like a telephone directory that stores name-to-address translation for IP addresses
Network address translation (NAT)	the process of translating an external IPv4 address to an internal IPv4 address, used when an organization can only obtain a limited set of IPv4 addresses (denk aan Ziggo & Duwo. 1 ip voor het complex, en een grote NAT server ertussen zodat je ueberhaupt nog kunt internetten)
non-persistent CSMA	host does not continously sense, but waits a random time after each sensing
Open shortest path first (OSPF)	one sort of link state protocol
Open System Interconnect (OSI)	conceptual framework that organizes the functionalities of any type of communication in a layered structure.
OSI 1 Physical layer	physical transmission of "bit"-signals
OSI 2 Data Link Layer	transformation of bit streams into data frames, sequential transmission of these frames (error handling and flow regulation).
OSI 3 Network Layer	control of subnet operations: routing and forwarding congestion control, accounting and interconnection over different, heterogenous networks
OSI 4 Transport Layer	Lowest end-to-end layer from soruce to destination, flow control, aggregation and multiplexing, communication mode (unicast or point-to-point, multicast, broadcast, anycast)
OSI 5 Session Layer	Manages a logical connection, called the session, between two communicating processes or applications
OSI 6 Presentation Layer	provides the selection of a common syntax for the representation of data and the transformation of application data into and form the common syntax
OSI 7 Application Layer	abstract network virtual terminal (incomputability in terminal types, cursor movements, etc…)
packet switched networks	network with end-to-end communications by chopping information flow into packets and delivering those independently
performance metrics	computation complexity, throughput, blocking, reliability, security, memory consumption, manageability, scalability

Terminology	explanation
piggybacking	attach acknowledgements or an error control sequence at the end of the data frame in order to reduce bi-directional exchange of acknowledgment information
Ping	Echo request via ICMP from source to host
p-persistent CSMA	host will not launch a packet when it senses an empty channel but has a chance p of launching a packet
Protocol data unit (PDU)	data unit used by the sender to convey a message (same layer communication)
PSH	requests receiving TCP to pass the in sequence ordered data tot eh application immediately instead of first buffering the segments
QoS requirements (Quality of Service)	defines a set of qualifiers for the information transport such as a minimal service rate, end-to-end delay and loss etc.
Reciever-Based Channel Selection (RBSC)	All nodes in range of the Reciever must be silent (fixing both hidden and exposed terminal problems)
Request to send (RTS) frame	short frame (30 bytes) contains the length of a message that host wants to send to reciever
Reverse ARP	the inverse of ARP
Round Trip Tim (RTT)	the time it takes for a message to get from sender to reciever x 2
router	hub with forewarding capabilities and the ability to compute
Routing algorithm	generally embedded as part of the routing protocol software
Routing information protocol (RIP)	one sort of distant vector protocol
Routing protocol	attempts to provide each node in the network with a consistent updated view of the topology, tries to take the time varying dynamics of the network into account
RST	requests receiving TDP daemon to abort the connection due to abnormal operation
scalability	increase in the complexity to operate, control or manage a network if relevant network parameteres such as the size or the number of nodes/system in the network, the traffic load, the interaction rate, etc. increase.
Service acces point (SAP)	point at which an interface can be accessed; telephony has sockets; TCP has a port number
Service data unit (SDU)	data unit used by interface-interface communications (layer to layer)
Single parity check	Operation is the sum off all bits in the word M modulo 2 which is appended or prepended to the message to form the codeword C which should always have C modulo 2 = 0
Subnet adressing	enables a large network to be split into several smaller subnetworks; if you AND the subnetmask with the complete ip adress you get the network-ID and the difference between the net-ID and the complete IP is the Host-ID
supernetting	the process of aggregating several class C- adresses to obtain an adress space larger than class C subnetwork but smaller than a class B
switch	hub with forewarding capabilities
SYN	requests a connection
TCP acknowledge number	sequence number of the next in order octet that the sender expects similar as selective repeat ARQ protocols
TCP AIMD	(additive increase multiplicative decrease) If RTO is exceeded window treshhold is set to half of the current window size and slow start is initiated
TCP Checksum	precisely the same way as UDP checksum
TCP clocking	self clocking: adjusting the sending of data to the receiving of data, by only sending upon receiving an ACK disadvantage is that queues that are built-up at bottlenecks can never shrink
TCP congestion avoidance	after crossign a window treshhold the window will not increase exponentially, but will be incemented by 1 to avoid congesting the network (once congestion is reached, multiplicative decrease, and additive increase happens to avoid further congestion)
TCP fast recovery	at the receipt of a 3rd duplicate ACK sstresh -> W/2; retransmit L and set congestion window W to sstresh + 3; each time another duplicate ack arrives increase congestion window W++ and transmit new not in transit packet; at the receipt of the ack of L set congestion window W -> sstresh and start congestion avoidance
TCP flags	URG, ACK, PSH, RST, SYN, FIN
TCP Maximum segment size (MSS)	largest block of data that the segment is allowed to contain
TCP Option field	MSS, windows scale and timestamp
TCP retransmission	happens when RTO is exceeded or when a small number of consecutive duplicate acks have been received; sender will retransmit all unacknowledged packets
TCP retransmission-time-out (RTO)	timer that resets no acknowledgements and that, if it runs out triggers a retransmission of a TCP packet
TCP Slow start	adjust the windows size while sending packets to become increasingly big upon receiving acknowledgements until reaching the advertised window (by the reciever)
TCP Socket	pair of integers (host, port) to identify the endpoint/starting point
TCP window size (as specified by the reciever)	available buffer space also called the reciever socket buffer
TCP/IP protocol suite	common set of protocols that forms the base of the internet
Time-division multiplexing (TDM)	network capacity is divided over time, and each user gets a time slot
Tracerout	Returns path of an IP packet from source to destination by sending with a TTL of 1 and increasing every time, mapping by error messages from routers
traffic profile	describes how the content of information as digitalized data (bits) stored in packets of certain length is delivered to the network as a function of time
Transmission Control Protocol (TCP)	reliable connection-oriented transport (also, flow control); provides kind of a virtual circuit connection in full duplex, analogous to telephony, point to point; does not support multicast or broadcast
tunneling	similar to encapsulation, except an entire L3 packet is enclosed in the data field of another L3 data packet; violates layering concept. Is used when some nodes understand a newer protocol, while others do not
UDP Checksum	16-bit one's complement of a pseudoheader consisting of IP header, UDP header and UDP Data padded with 0's
unicast	one on one communication between two parties
URG	Urgent pointer
User Datagram Protocol (UDP)	unreliable conectionless packet service; complements IP with error checkign and application distinction
Wide area network (WAN)	network of subnets (LANs) and hosts exceeds the spatial extend of a MAN
xDM (X-division multiplexing	gives rise to a xDMA

Terminology	explanation
xDMA (X-division multiple access)	corresponds to a xDM