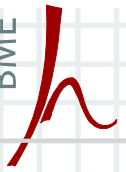
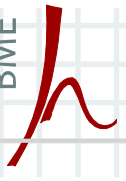


Hálózati alapismeretek

Schulcz Róbert
BME-HIT



- Kommunikációs hálózat: *node* és *link*
- Node, azaz (vég)pont:
 - Felhasználói eszköz; egyéb végpont;
 - Közbenső hálózati eszköz (router, switch, multiplexer, mobil hálózati eszköz)
 - ezek is (cél)számítógépek
 - „láthatatlannak” kell maradniuk
 - Fizikai node: egy eszköz
 - Logical node: egy funkció
- Link, azaz összeköttetés:
 - A pontokat köti össze
 - Fizikai link: egy kábel
 - Logikai link: egy összeköttetés (pl. VPN)

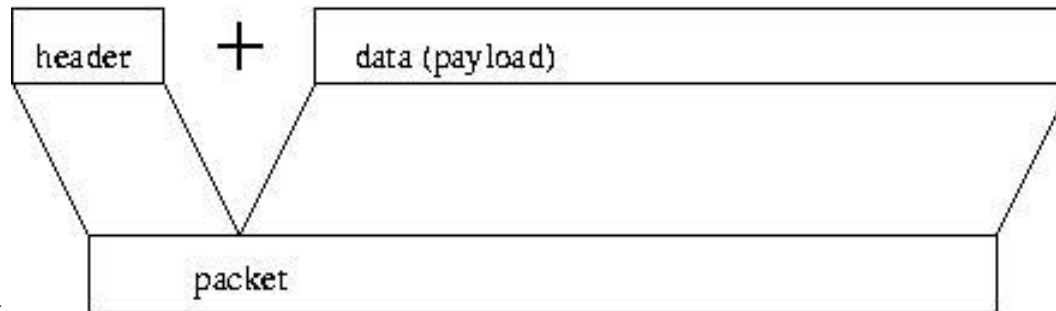


Digitális kommunikáció

- Digitális átvitel:
 - Minden információt (kép, szöveg, video, stb.) *bináris adattá* alakítunk
 - *bináris adatot* viszünk át a hálózaton
- Bináris adat:
 - nullák és egyesek sorozata
 - *bit*: 0, v. 1
 - 8 bit egy *byte*, de inkább *octet* a távközlésben
- Példák
 - nagy A betű: 01000001;
 - egy 125 microsec szegmense a hangnak: 01011100

Digitális kommunikáció

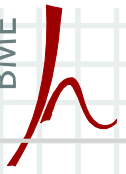
- Az adatot szervezni (szegmentálni, darabolni) kell:
 - Keret, vagy csomag
- Fejléc (header), megmondja, hogy mi van benne
 - A hálózati elemek számára információ, hogy mit kell csinálni vele
- Hasznos adat (body, payload): az adat (egy része)



- Hiba javítás, vagy detektálás
- Nyugtázás (ACK): visszajelzés egy csomag vételéről
- Újra adás: hiba esetén

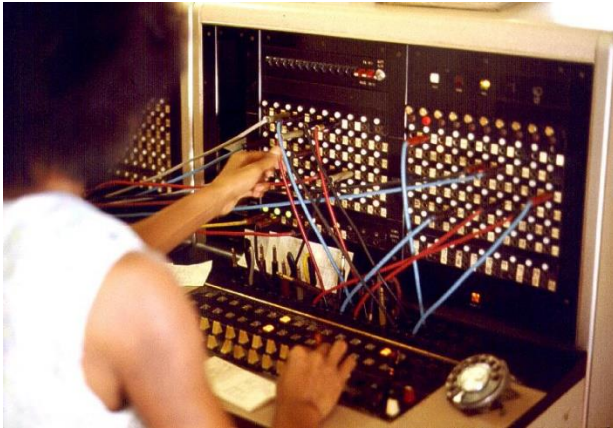
- A digitális adatok átviteléhez fizikai jel szükséges
- *Digitális jel:*
 - Megadott pillanatokban változhat
 - Véges értékkészlettel rendelkezik
- Átviteli (bit)sebesség:
 - Másodpercenként átvitt adatok mennyisége
 - bps, kbps, Mbps, Gbps: $\times 1000$ a távközlésben
 - $\times 1024$ az IT-ben
 - Pl. 1 Gbps Ethernet link: kb. 61000 oldalnyi szöveg másodpercenként
(6,1 méter magas kupac, egy oldalas A4-es)

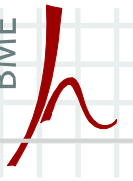
- Kapacitás:
 - link: a másodpercenként átvihető bitek mennyisége
 - node: a percenként feldolgozható (továbbítható) bitek mennyisége
- Bitsebesség, bitráta:
 - Mennyi adatot szeretne továbbítani
 - Vagy mennyi adatot tud küldeni



Áramkörkapcsolt átvitel (CS)

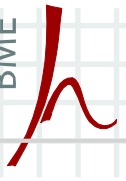
- Áramkörkapcsolt (circuit switched) átvitel
 - A telefóniából jön
 - A régi analóg rendszerekben a végpontok között „fémes” kapcsolat jött létre
 - Az ún. cross-bar és rotary központok is így működtek



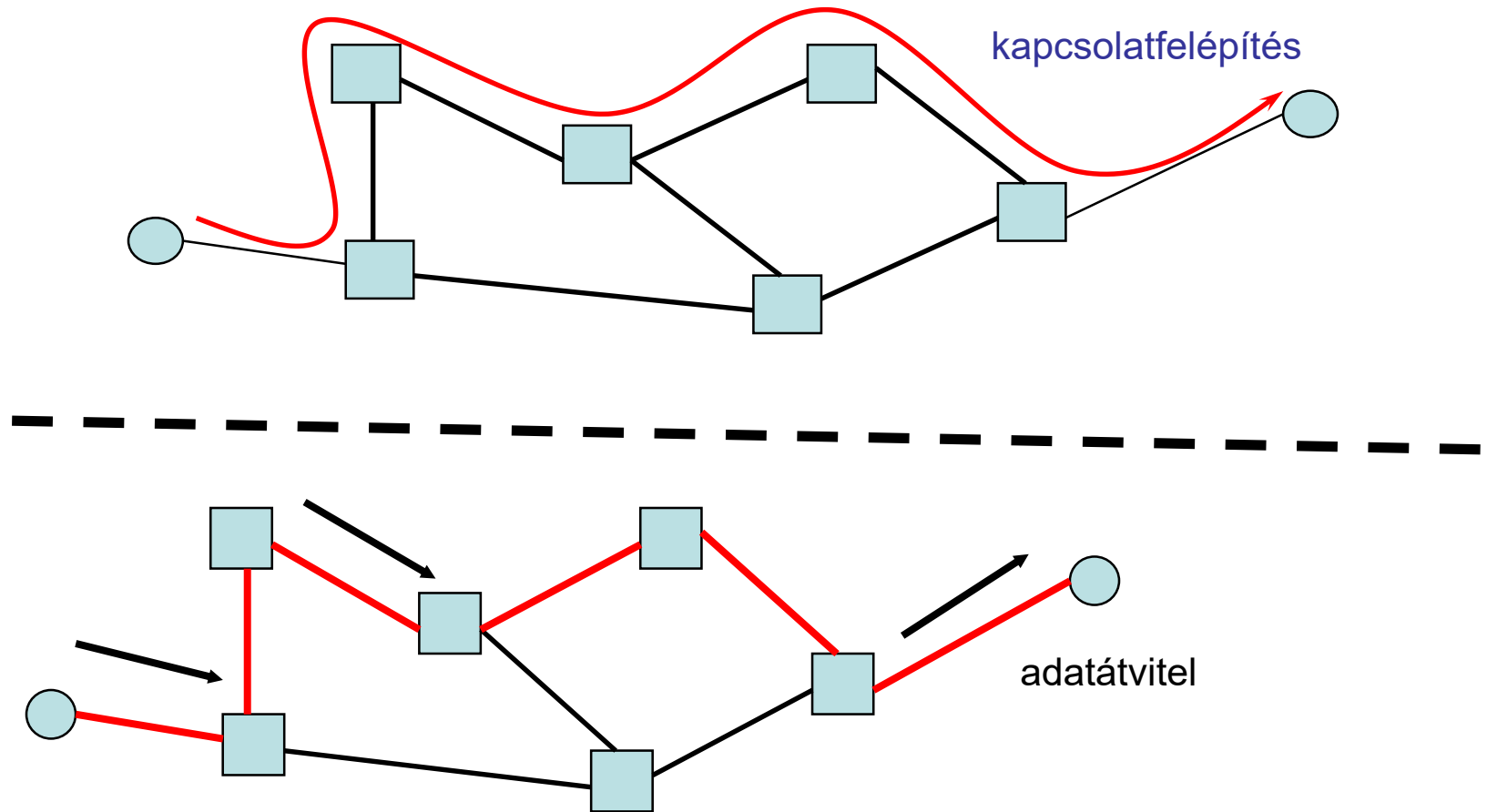


Áramkörkapcsolt átvitel (CS)

- Áramkörkapcsolt átvitel a digitális kommunikációban
 - Az adatátvitelt megelőzően *jelzési* fázis, ami felépíti a kapcsolatot
 - *jelzések*: a végpontok és hálózati pontok adatot cserélnek: „hívásfelépítés”, erőforrás foglalás
 - Az adatfolyam a megadott útvonalon zajlik a felek között
 - A kapcsolat annak lebontásáig tart (explicit le kell bontani)



Áramkörkapcsolt átvitel (CS)



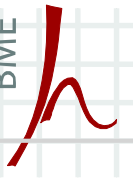
Csomagkapcsolt átvitel (PS)

- Csomagkapcsolt (packet switched) átvitel
 - Analógia: postai csomag
 - Az adatot csomagokba rendezzük
 - Minden node „függetlenül” kezeli a csomagokat
 - A továbbításhoz szükséges minden információ minden csomagban benne van (fejléc)
 - Feladó, címzett, kezelési instrukciók, prioritás, stb.

IP PACKET HEADER
24 BYTES MAXIMUM

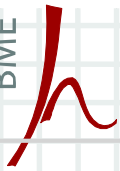
Version	Length	Service Type	Packet Length		
Identification			DF	MF	Fragment Offset
Time To Live	Transport		Header Checksum		
SENDER IP ADDRESS (32 Bits)					
DESTINATION IP ADDRESS (32 Bits)					
Options					Padding
PAYLOAD					





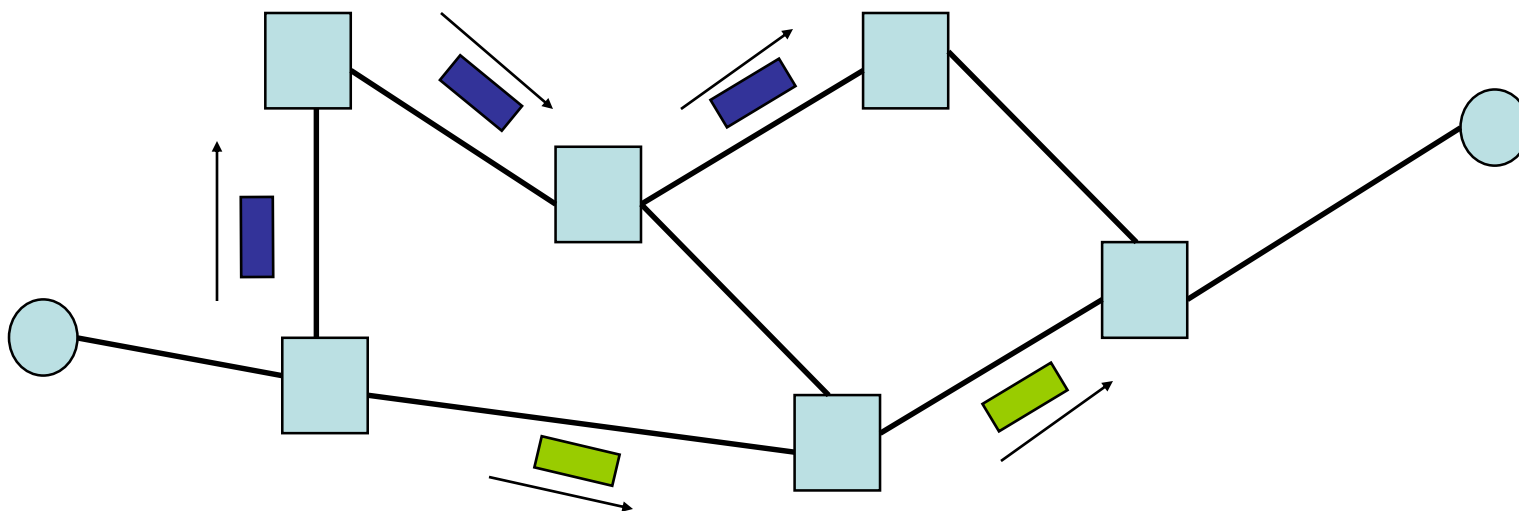
Csomagkapcsolt átvitel (PS)

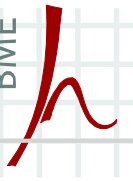
- Ha egy csomag készenáll, kiküldjük a hálózatba
- A hálózati csomópontok felelnek a továbbításért
- Ennek alapja a címzés
- A csomagok egymástól függetlenül utaznak a hálózatban
- Nincsenek fix összeköttetések, útvonalak és lefoglalt kapacitások a hálózatban



Csomagkapcsolt átvitel (PS)

- Az útvonal akár csomagonként eltérő lehet
- Nincs garancia a sorrendhelyes érkezésre, a végpontnak kell azokat sorba rendezni

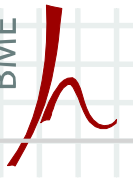




Áramkör-, vagy csomagkapcsolt

■ CS hálózatok

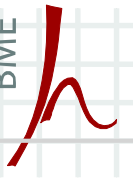
- tipikusan: PSTN telefon
- Központi iroda, nagy operátor, nagy infrastruktúra, saját hálózat
- Hálózatcentrikus gondolkodás: végponttól végpontig kontroll, számlázás, stb.
- Központosított, kontrollált
- Fix, garantált QoS
- Időgarantált átvitel
- Állandó adatfolyam
- A számlázás alapja: összeköttetés ideje
- Nagy rendelkezésre állás



Áramkör-, vagy csomagkapcsolt

■ PS hálózatok

- tipikusan: IP (Internet Protocol) hálózat
- Kisebb számítógép hálózatokból jönnek
- Kisebb mennyiségű, többfelé küldött adat
- Elosztott, a szolgáltatás egy-egy pont meghibásodásakor is működőképes
- Időgaranciának nincsen jelentősége
- Felhasználócentrikus gondolkodás: A pontból B-be jusson el az adat, a hálózat „oldja meg”
- A számlázás alapja: átvitt adatmennyiség

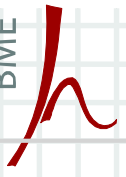


Áramkör-, vagy csomagkapcsolt

- A valódi hálózatokban ezek keverednek
 - Az infrastruktúra maximális kihasználása
- Internet Protocol (IP) alapú átvitel „klasszikus” SDH hálózaton
- circuit emulation over Ethernet
- vagy CS (hang) szolgáltatás PS hálózaton
 - VoIP

Áramkör-, vagy csomagkapcsolt

- *Kapcsolat orientált (connection oriented)*
 - Hívásfelépítési szakasz megelőzi az adatfolyamot
 - Ez akár a PS hálózaton is lehetséges
 - Pl. TCP / IP
- *Kapcsolatmentes (connection-less)*
 - Nincs kapcsolatfelépítés (hívásfelépítés)



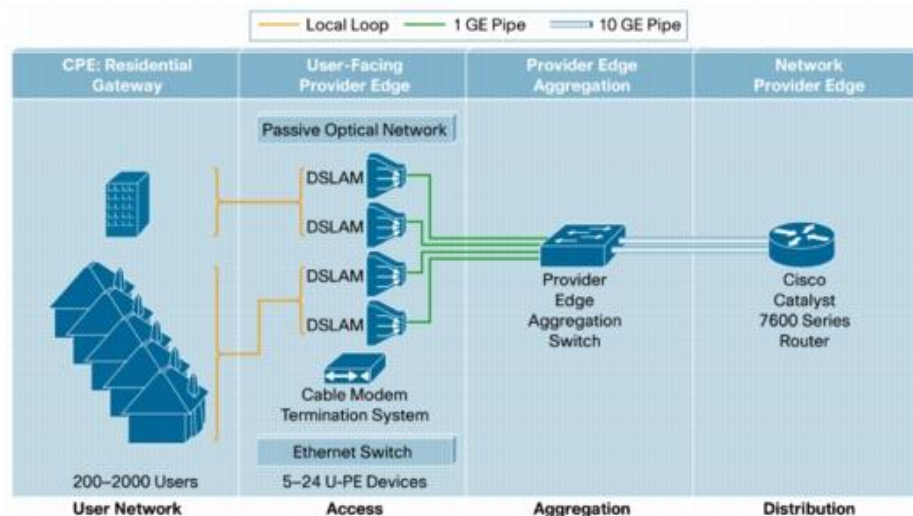
Hálózati szolgáltatások

- *valós idejű szolgáltatás*
 - az információt akkor kell továbbítani, amikor létrejön (vagy minimális késleltetéssel)
 - például. hanghívás, videotelefon
 - minőség: késleltetés, és a késleltetés változása (jitter)
 - késleltetés: a másodperc tört része
 - csomag (információ) veszteség: elfogadható
- *„kvázi” valós idejű*
 - (élő) streaming hang és videó
 - késleltetés: másodpercek is lehetnek
- *nem valós idejű szolgáltatás*
 - a késleltetés nem jelent problémát
 - késleltetés: másodpercek (böngészés), tíz másodperc: fájl átvitel, e-mail
 - adatvesztés nem megengedett!

Hálózatok hierarchiája

- Hozzáférési hálózat
 - Az a rész, amely eléri az előfizetőket („az utolsó mérföld”)
 - Többféle típus, akár egyetlen üzemeltetői hálózatban
 - DSL, ADSL, WiMAX, CATV, mobil 3G, passzív optikai
 - Példa: lakótövezet, irodaházak, utcák stb.
- Aggregációs hálózat
 - Manapság tipikusan: IP / Gigabit Ethernet / optikai; vagy alacsonyabb bitsebességű SDH
 - Példa: kerület, város
- Maghálózat (core), elosztó hálózat
 - Jellemzően MPLS / IP / 10Gigabit Ethernet / optikai
 - Példa: regionális, országos hálózat, csomópontok a nagyobb városokban

példa: CISCO

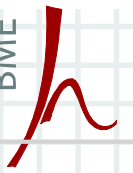


A hálózatok földrajzi mérete

- Személyes hálózat (PAN):
 - közel egy emberhez, általában 1-10 méterre
 - vezetékes PAN: USB és FireWire kapcsolatok
 - vezeték nélküli PAN: Bluetooth UWB és infravörös
- Helyi hálózat (LAN):
 - korlátozott földrajzi területen, mint például otthon, iskola, irodaház
 - vezetékes LAN-ok: általában az Ethernet technológián alapulnak (koaxiális kábelek, áramvezetékek stb.)
 - vezeték nélküli LAN: 802.11a, ac, ad, b, g, n
 - nagyobb adatátviteli sebesség; egy routerrel egy WAN-hoz csatlakoztatható
- Városi hálózat (MAN):
 - általában városra vagy nagy kampusra terjed ki
- Nagyobb területre kiterjedő (országos) hálózat (WAN):
 - nagy földrajzi területet fed le
 - például ország, vagy akár interkontinentális is lehet
 - többféle média: telefonvonal, kábel és rádióhullám
 - A WAN hálózatok általában az OSI referenciamodell alsó három rétegében működnek: a fizikai réteg, az adatkapcsolati réteg és a hálózati réteg

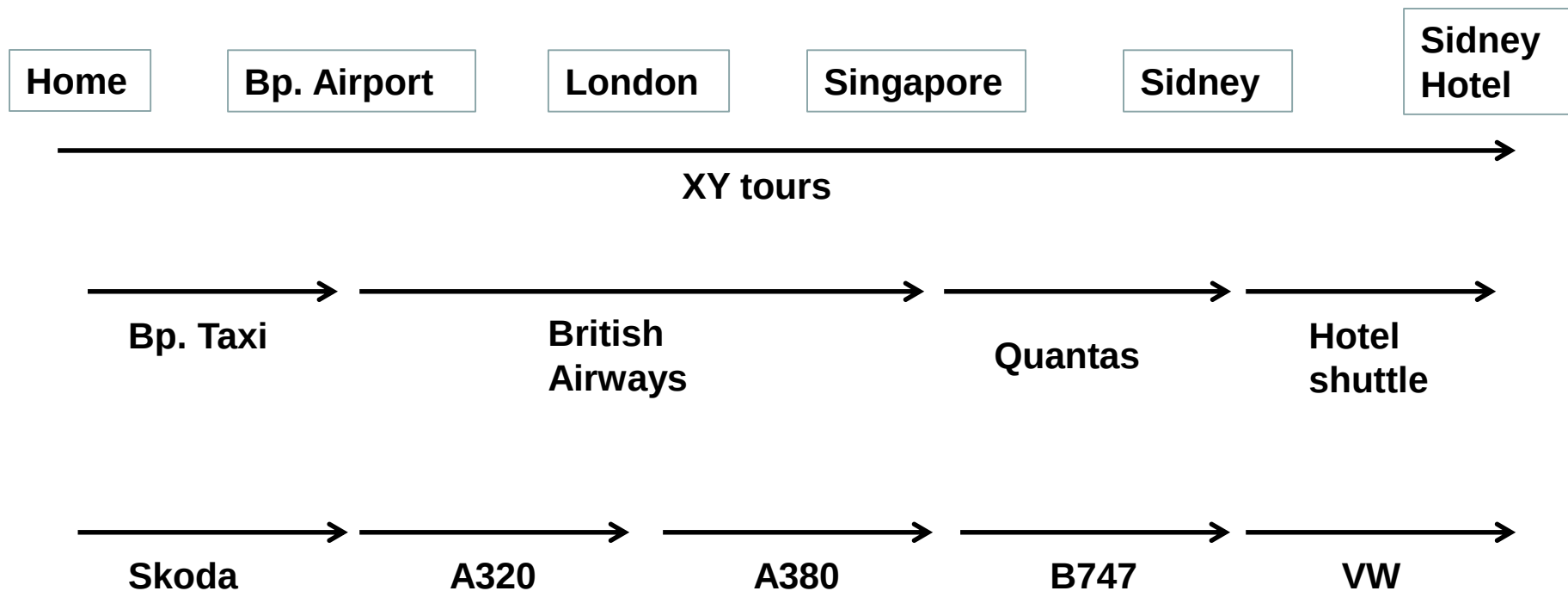
Hálózati rétegek

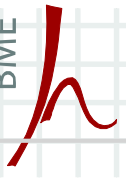
- egy nagy hálózaton keresztül történik a két végpont között az adattovábbítás
- a hálózat, különböző elemeket tartalmaz(hat)
 - különböző szabványok, gyártók, hálózati megoldások
 - különböző hozzáférési módok, átviteli kapcsolatok stb.
- sokféle funkció van megoldva a hálózatokban
 - ezek logikai rétegekké szerveződnek



Hálózati rétegek

- Utazási példa rétegekre bontva
 - információ: én magam
 - honnan: Otthon; hová: Sydney hotel
 - végponttól végpontig átvitel: XY tours





Hálózati rétegek

- OSI (Open System Interconnection) hét rétege minden funkciót tartalmaz
 - Funkciók rétegekbe szervezve
- Az alsó négy réteget a hálózat kezeli (általában)
 - Az afeletti rétegek a kliensekben vannak
- Példák:
 - SS7: Signalling System No. 7, over TDM: telefon hálózati jelzések: mind a 7 OSI réteg
 - TCP/IP és Ethernet: 1-4 réteg

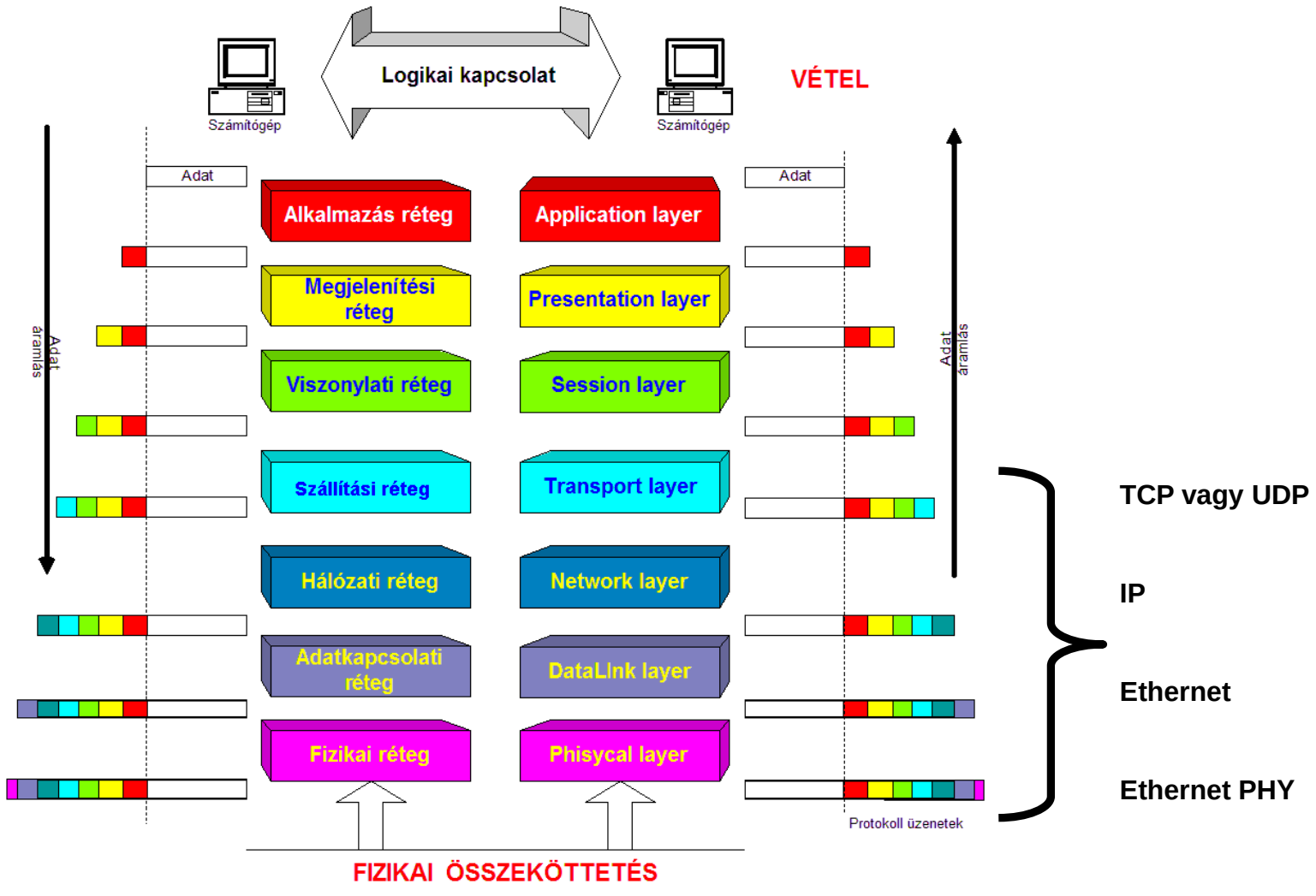
Protocol stack (hálózati rétegek)

- Protokollok hierarchiája
- Az ISO OSI 7 protokollrétegek a funkcionalitás általános logikai elválasztását szolgálják
- A protokoll rendszerint két másik csoporttal kommunikál a stack-ben (alsóbb és felsőbb réteg)
- Az alsóbb rétegbeli protokollok szolgáltatásokat nyújtanak a felső rétegbeli protokollok számára
- Az alsóbb rétegbeli protokoll az alacsonyabb rétegű protokollt/funkciót elrejt a felsőbb réteg előtt → áttetszőség/transzparencia
- Az alsóbb rétegbeli protokollok a felső rétegbeli protokollokat (csomagokat) magukba foglalják (encapsulation)
- A modularitás, a „kicserélhetőség” fontos:
IP over Avian Carriers RFC 1149



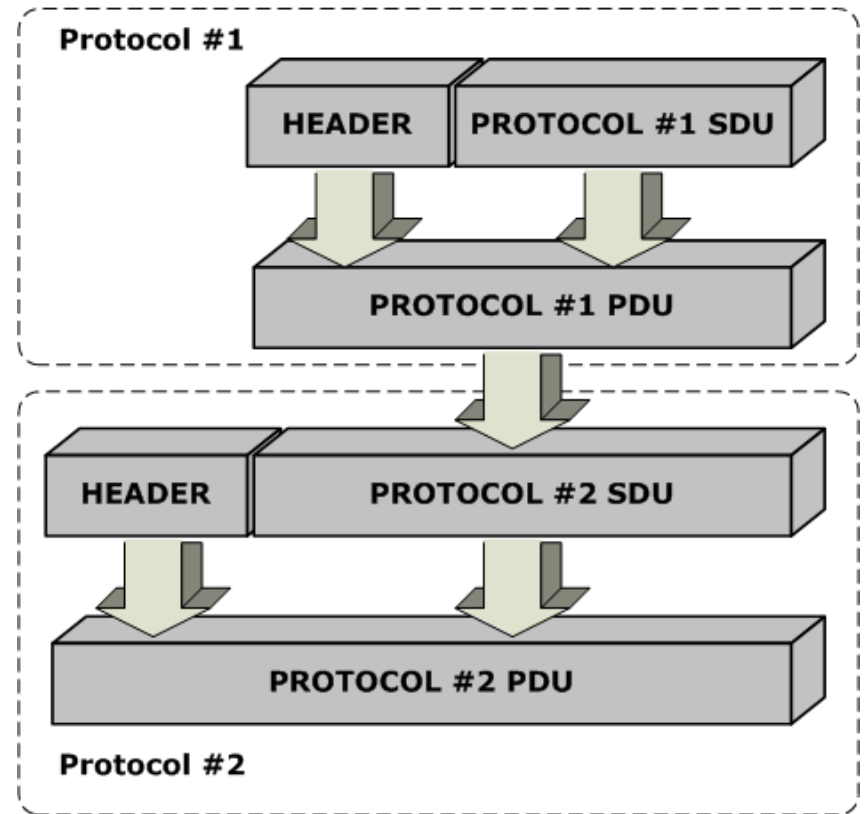
An example of packet loss.

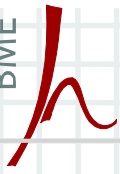
Protocol stack (hálózati rétegek)



Csomagok egymásba ágyazása

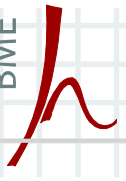
- Minden rétegnek saját formátuma van (pl. cím eltér, hibajavítás, stb.)
 - PDU: protocol data unit (amit továbbít)
 - SDU: service data unit (amit felsőbb rétegtől kap)





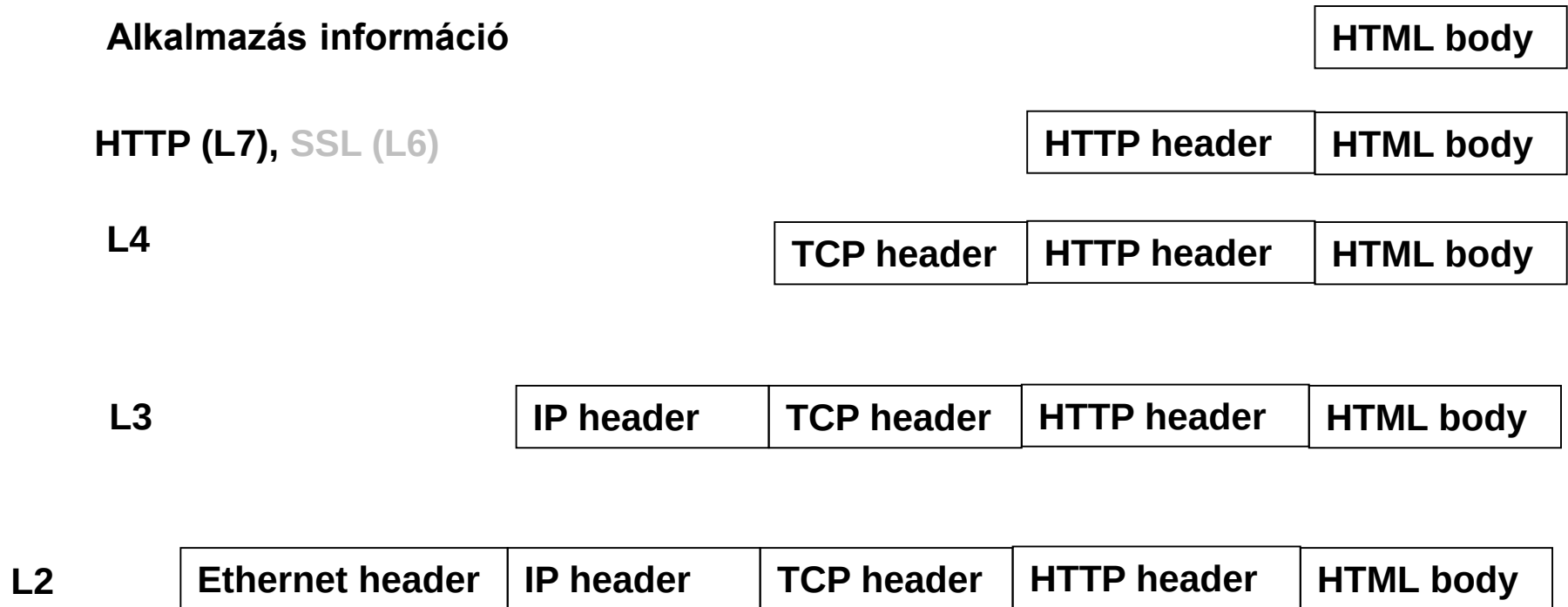
Hálózati rétegek

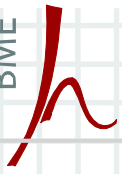
- PDU: A protokoll fejlécet és az SDU-t „hasznos információként” tartalmazza
- Fejléc: további információ arról, hogyan kell kezelni a csomagot a hálózat és az SDU között
- SDU, Service Data Unit: Egy felső réteg protokoll PDU-ja vagy a stack tetején, maga a hasznos adat
- Az SDU neve a protokolltól függ: pl. az Ethernet SDU-jának neve keret, a TCP SDU-ja szegmens (!)



Hálózati rétegek

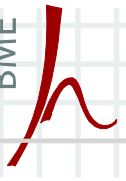
- pl. weboldal





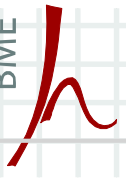
L1: fizikai réteg (PHY)

- tényleges átvitel a fizikai közeg felett
- aktiválja, fenntartja és deaktiválja a fizikai kapcsolatot
- az adatot a fizikai közeghez igazítja
- biztosítja, hogy a kapcsolat végpontjai felismerjék az átviteli jeleket
- létrehozva a tényleges fizikai jelet
- bitek sorrendhelyes továbbítása
- mechanizmus a bit hibák észlelésére / kijavítására
- stb.



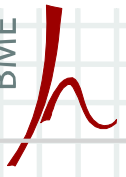
L2: adatkapcsolati réteg

- eredetileg: két, közvetlenül összekapcsolt eszköz közötti kommunikáció;
- az adatot adatkeretek létrehozásával szervezi, keret határolók észlelésével, hibakezeléssel és az adatkeretek sorrendhelyes szállításával átviszi
- hibák észlelése (elveszett / hibás keretek), nyugtázások küldése és fogadása
- hibák esetén: újraadások
- hibamentes szállítást biztosít a hálózati réteg felé
- alrétegei:
 - MAC, Medium Access Control, közeg hozzáférés-vezérlés: hogyan és mikor küldenek vagy fogadnak a végpontok
 - LLC, Logikai Link Control: a többi funkció



L3: Hálózati réteg

- biztosítsa a végpontól végpontig történő szállítást egy nagy (globális) hálózaton
- heterogén hálózatok összekapcsolása
 - pl. a Facebook elérése a mobilhálózattól
- csomagok vagy folyamatok útválasztása a hálózatban
- a hálózati forgalom vezérlése
- címzés

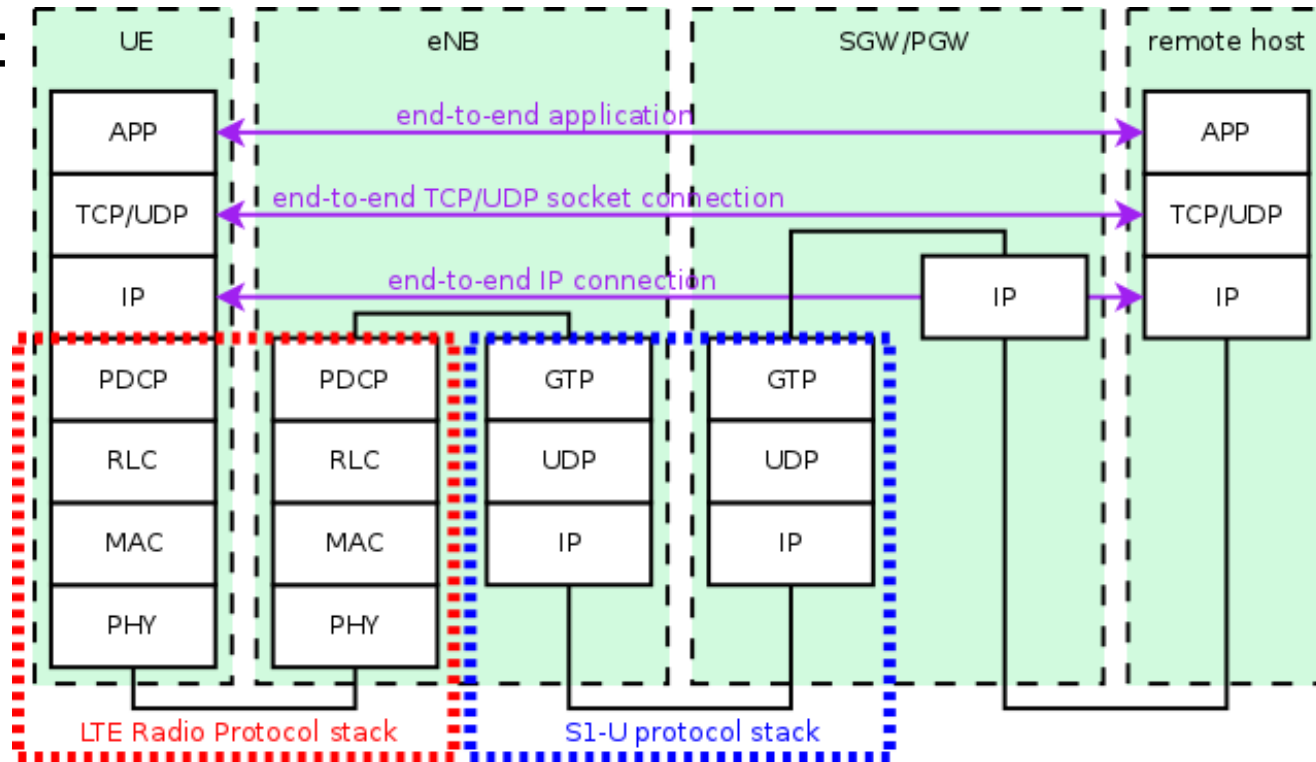


L4: szállítási réteg

- Végponttól végpontig hibamentes és a sorrendhelyes átvitel
- anélkül, hogy az alsóbb rétegekről bármit is tudnánk
- hibadetektálás
- nyugtázás és újra küldés (ha van értelme)
- az elküldött adatok mennyiségének vezérlése
- egyetlen végpont több párhuzamos kapcsolatának biztosítása

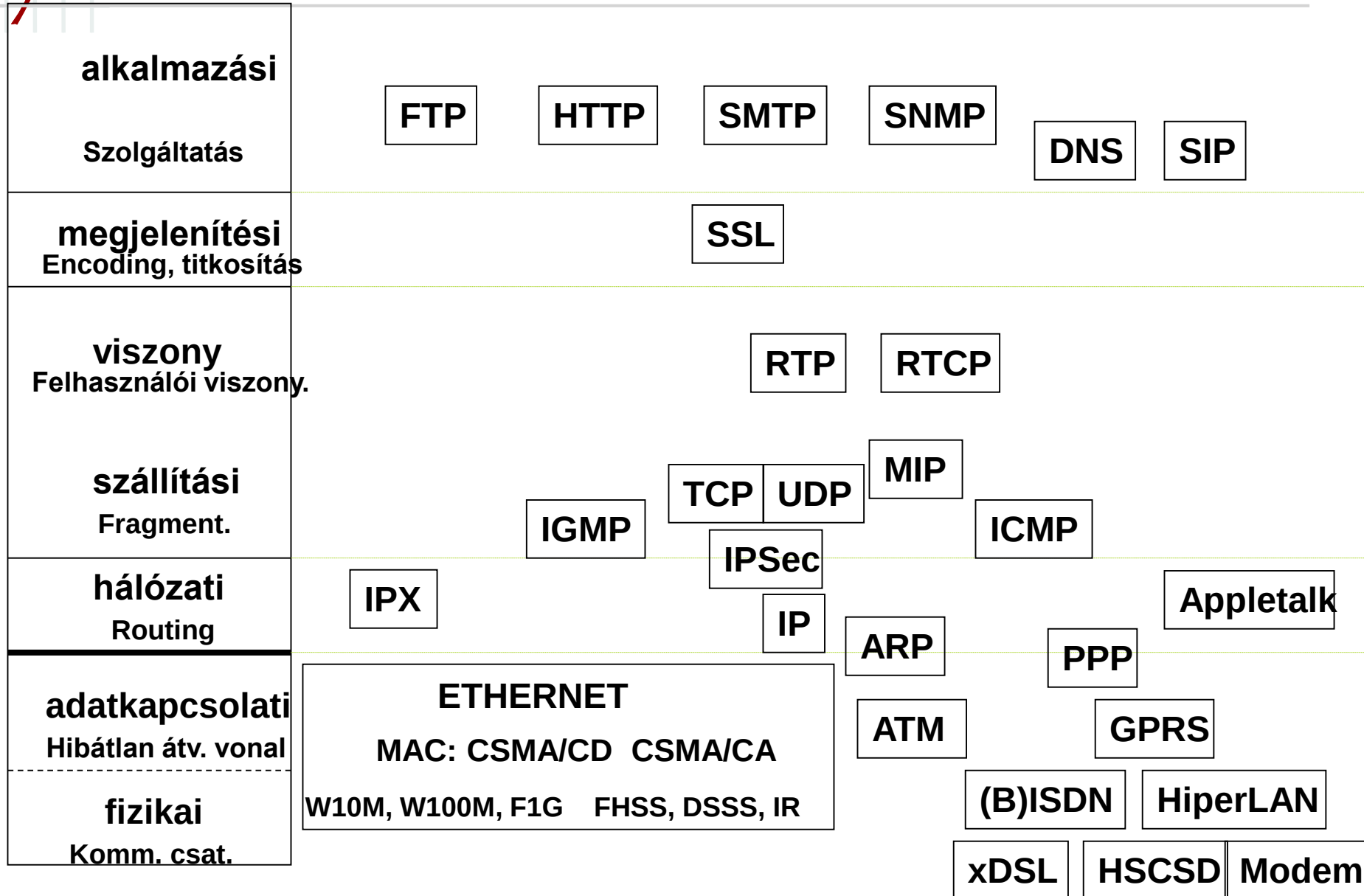
OSI 7 réteg

- Ilyen szép, tankönyvi példa ritkán
- Rétegek összevonása, vagy
- Több réteg (alrétegek)
- pl. 4G hálózat:

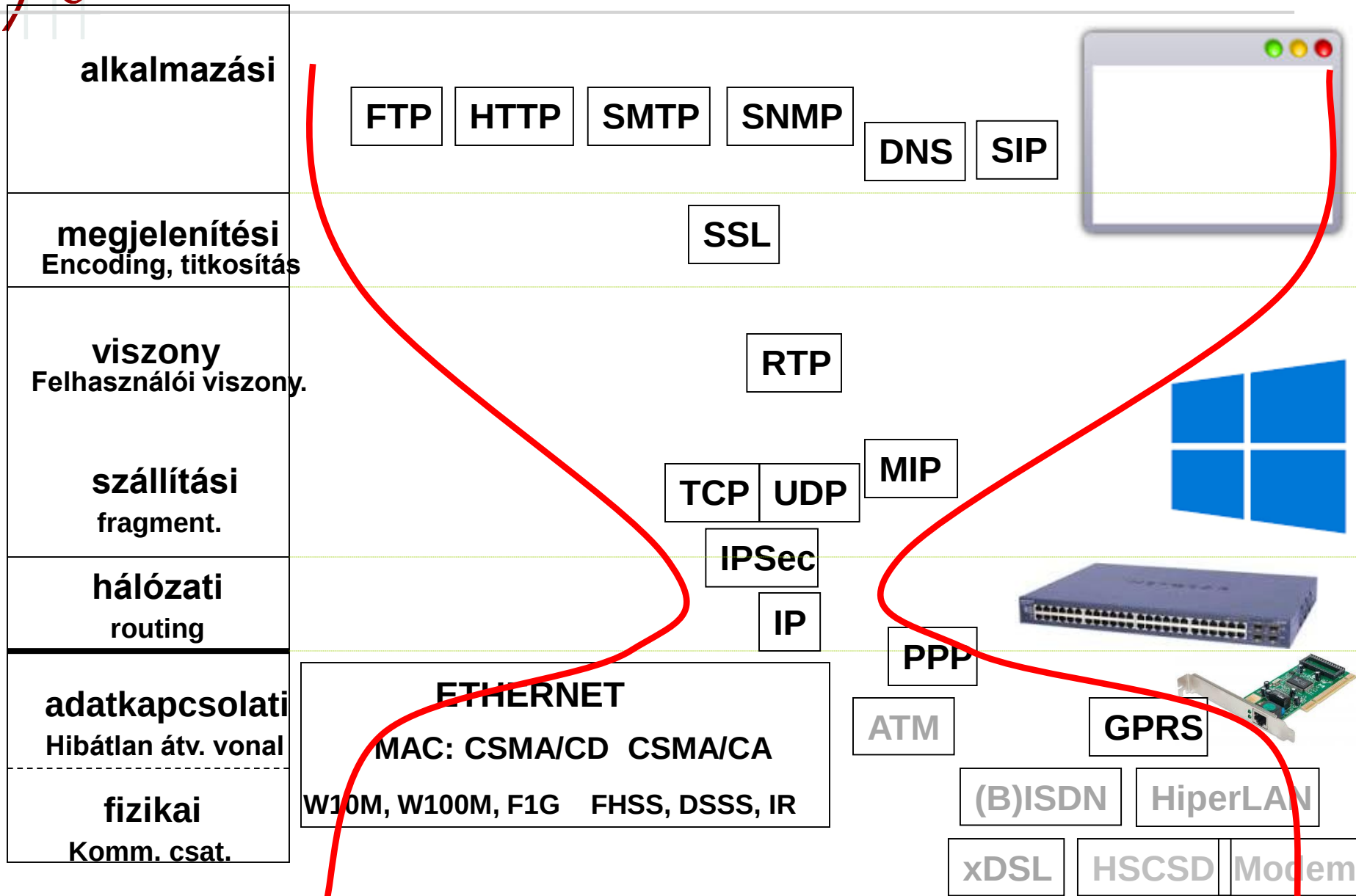


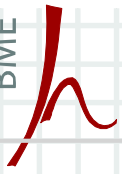
source: www.nsnam.org

A létező protokollok



A gyakorlatban ma használt protokollok





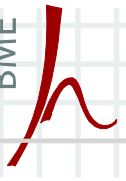
Mi az a protokoll



WIKIPÉDIA
A szabad enciklopédia

- „a **protokoll** egy egyezmény, vagy szabvány, amely leírja, hogy a hálózat résztvevői miképp tudnak egymással kommunikálni. Ez többnyire a kapcsolat felvételét, kommunikációt, adat továbbítást jelent.
- Gyakorlati szempontból a protokoll azt mondja meg, hogy milyen sorrendben milyen protokoll-üzeneteket küldhetnek egymásnak a csomópontok, illetve az üzenetek pontos felépítését, az abban szereplő adatok jelentését is megadja.
- A protokolloknak igen sok, és teljesen eltérő filozófiájú formája létezik. Vannak olyan protokollok, melyek minden apró részletet definiálnak (például ATM), és vannak, amelyek sok technikai kérdést nyitva hagynak, és rábízzák az implementálóra (például TCP protokollnál implementáció függő a csomagküldés sebességének megválasztása). Az előbbiek főleg a távközlésre jellemzőek, utóbbiakat főleg a kommunikációt informatikai oldalról közelítőkre jellemző. Előbbi előnye a jó kompatibilitás, utóbbié a rugalmasság.”

- Szervezetek:
 - IEEE (Institute of Electrical and Electronics Engineers)
 - Wifi, Bluetooth etc.
 - ITU (International Telecommunication Union)
 - xDSL, SS7, JPEG
 - 3GPP (3rd Generation Partnership Project), ETSI (European Telecommunications Standards Institute)
 - GSM-LTE
- résztvevők: 3 fél
 - Gyárók (vendor): Ericsson, Nokia, Intel, Qualcomm
 - Operátorok (service provider): Telekom, Vodafone, Verizon
 - Hatóságok (regulators): NMHH, FCC



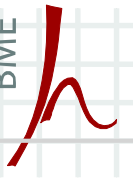
Szabványosítás

- A szabvány megvalósításának meg kell felelnie a szabványnak
- Interoperabilitás: a különböző gyártók különböző megvalósításai / termékei képesek kommunikálni egymással
- Növeli a versenyt a gyártók között

TCP/IP

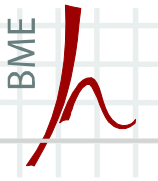
ISMÉTLÉS

Az előadáson *ismétlésként* hangzott el, ismeretét korábbról is feltételezzük, a tárgy megértéséhez szükséges, a számonkérésnek része lehet.



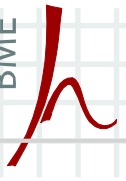
Internet protocol

- meanwhile in computer networks ...
 - local networks of computers
 - interchanging files, mails, data
 - servers and clients
 - autonomous systems (AS)
- let's connect autonomous systems
 - as simply and as distributed as possible



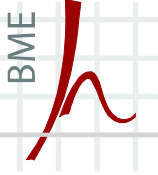
Internet protocol

- Internet: ~ devices using Internet Protocol
 - unified, global addressing method, devices connecting to the network can be reached through this IP address
 - given standard packet format
 - more precisely: IP datagram
 - given packet forwarding method and routing methods and supporting mechanisms
 - various applications



Internet protocol

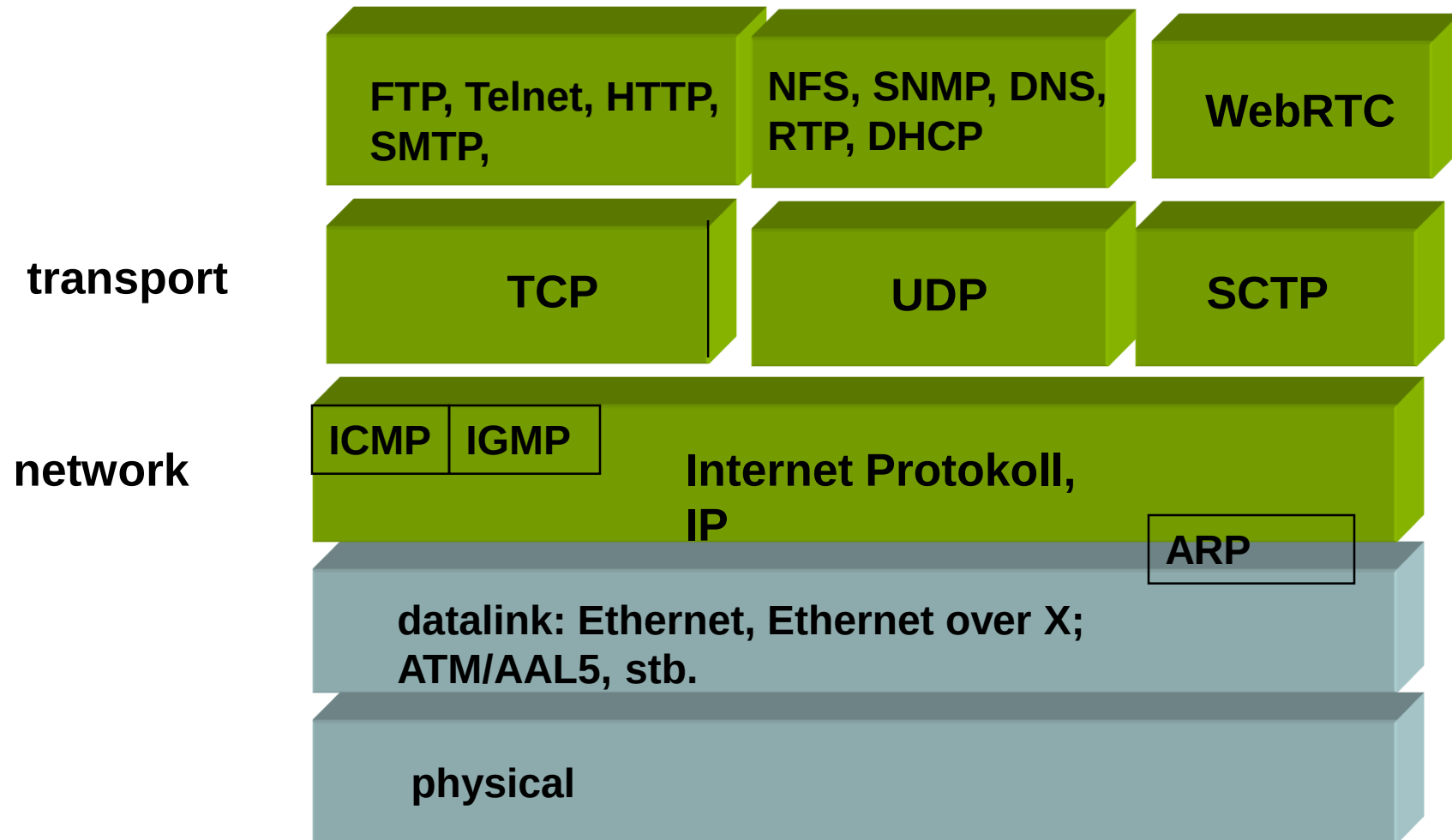
- a family of protocols using IP protocol packets for transmission
- above network layer (3. layer)
 - transport layer
 - TCP Transmission Control Protocol: reliable transfer of files
 - UDP User Datagram Protocol: unreliable transfer of streams
 - SCTP Stream Control Transmission Protocol – designed to carry telephony signalling
- „control plane application” protocols
 - ICMP Internet Control Message Protocol
 - SNMP Simple Network Management Protocol
 - IGMP Internet Group Management Protocol: manage multicast
 - DHCP Dynamic Host Configuration Protocol: to ask an IP address from a server

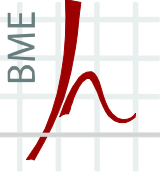


Internet protocol

- application protocols
 - HTTP Hypertext Transfer Protocol
 - SMTP Simple Mail Transfer Protocol
 - FTP File Transfer Protocol
 - TELNET : remote login
 - SSH Secure Shell: remote login
 - RTP Real Time Protocol: for real time voice/video
 - NTP Network Time Protocol: time synchronisation
 - SIP Session Initiation Protocol: call signalling
 - H323: voice and videoconferencing
 - etc, there is a lot

Internet protocol



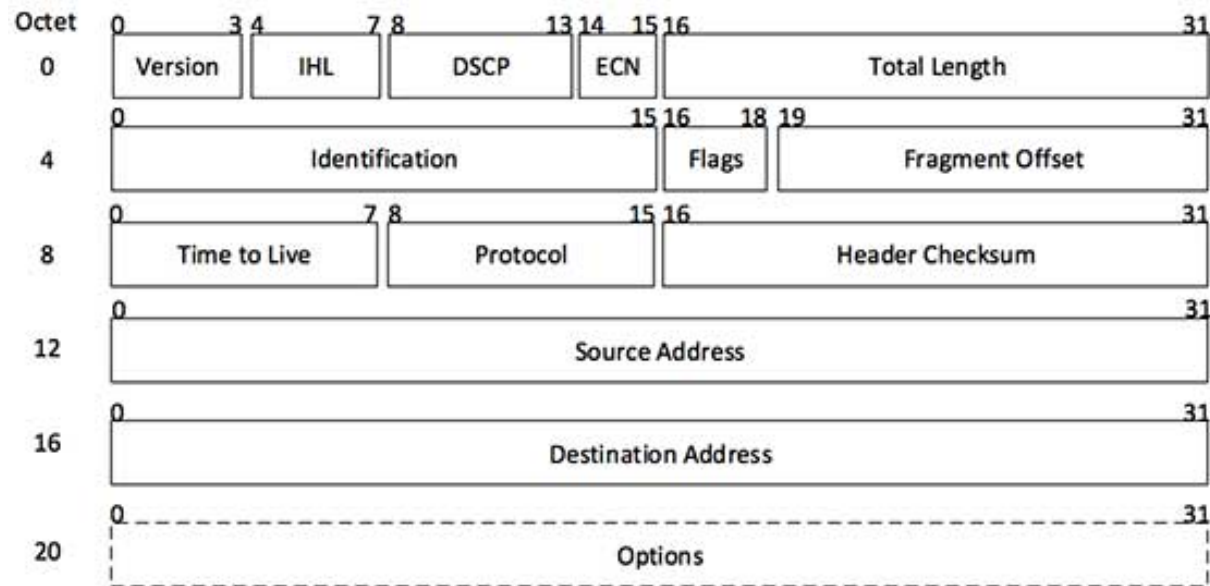


Internet Protocol

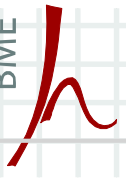
- IP packets, datagrams
 - connectionless: no connection setup, etc.
 - best effort
 - basically no QoS
- Later extensions
 - means for providing QoS (Intserv, Diffserv)
 - means for security (IPSec)

Internet Protocol

- version: 4
- TTL time to live: decreased by one at each router
- protocol: what is carried as payload?
- addresses



[Image: IP Header]

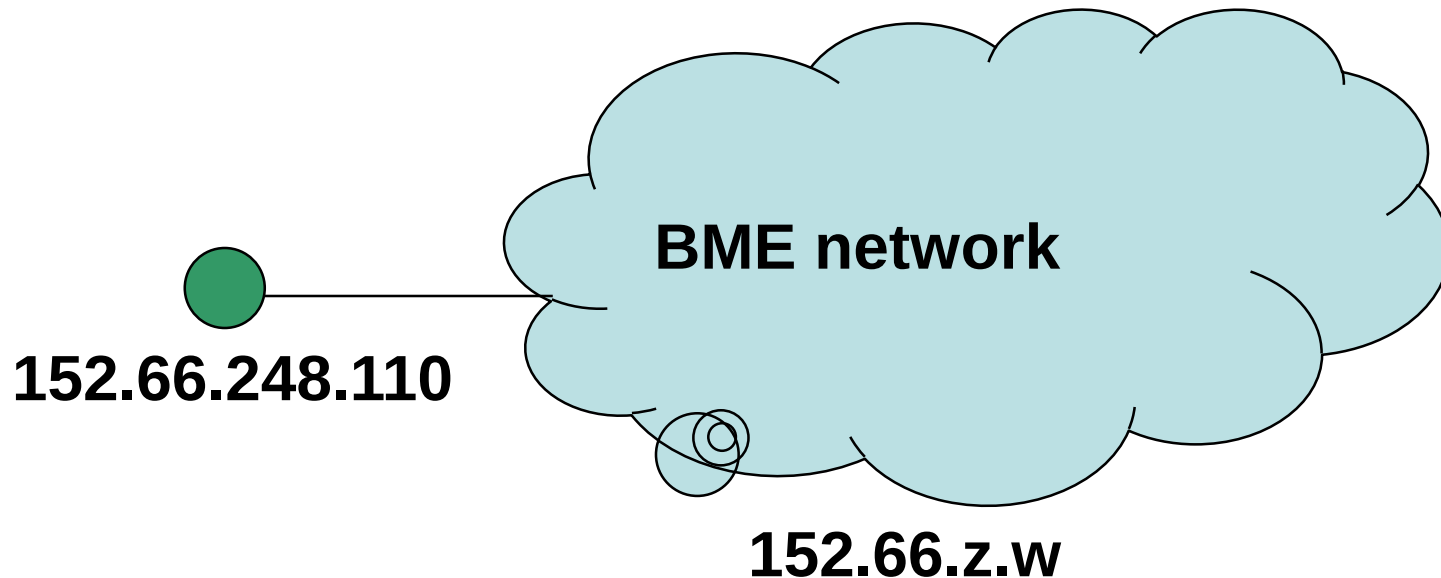


Internet Protocol

- IP networking, „all IP” $\leftrightarrow$ addressed by IP address
 - not a device, but rather a connecting interface of a device
- 4 bytes: 4 numbers between 0 255
 - usually: $x.y.z.w$, $0 \leq x, y, z, w < 256$
 - e.g. 152.66.248.74
- usually: dynamically and temporarily allocated IP addresses $\rightarrow$ DHCP
- other: permanent IP addresses set by the network operator
 - user with admin rights can set in operating systems
- IANA: Internet Assigned Numbers Authority

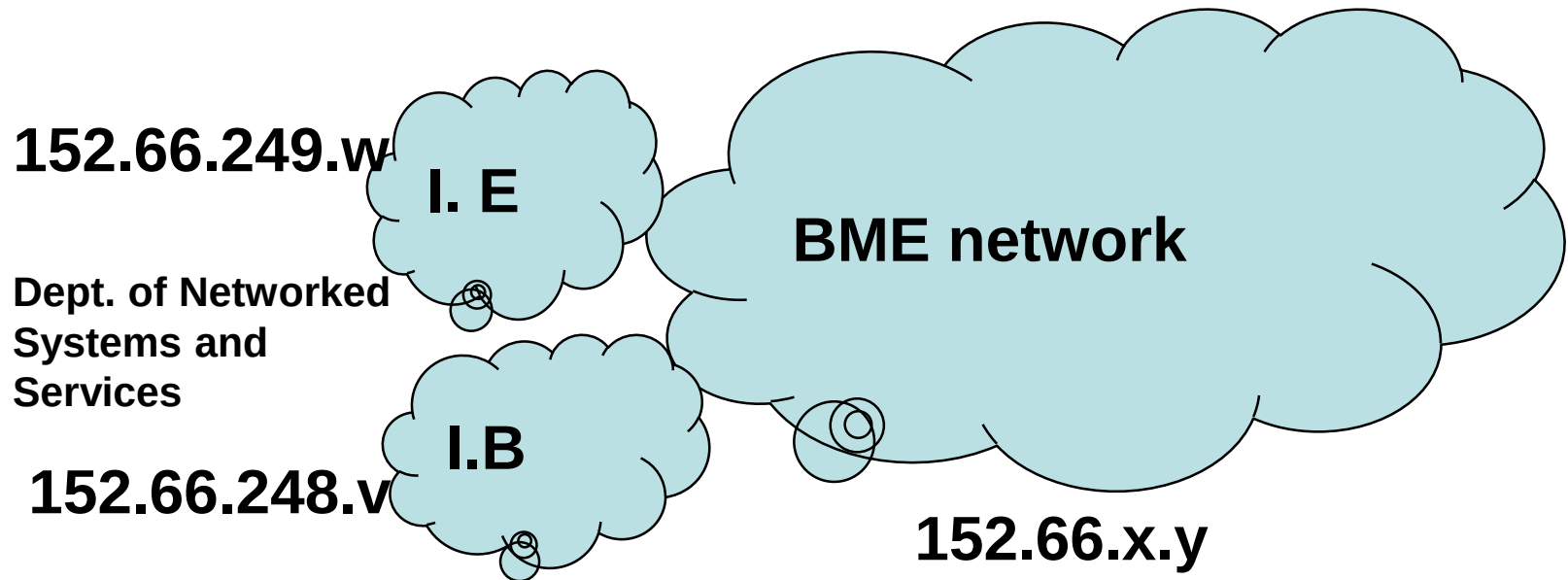
Internet Protocol

- first part of the address identifies the network
- second part is the device in the network
 - e.g. only ~64000 devices can be addressed within BME



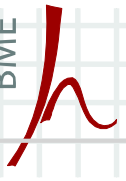
Internet Protocol

- big networks divided into smaller subnets
- the part identifying terminal also identifies subnet



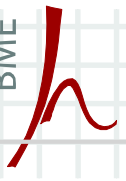
Internet Protocol

- private addresses, shared address space
 - addresses that are only used inside a private network
 - not routable to outside the network
 - not addressable from outside the network
 - create an own mini – internet
 - intranet
 - everyone at home WiFi (acquiring network address)
 - DHCP allocates 192.168.x.y
 - e.g. my phone logged in to department server:
 - netacc-gpn-5-199-11.pool.telenor.hu
 - 84.225.199.11 -> globally visible and accessible
 - but I see (Settings/About phone/Status): 100.80.29.135 :
shared address space



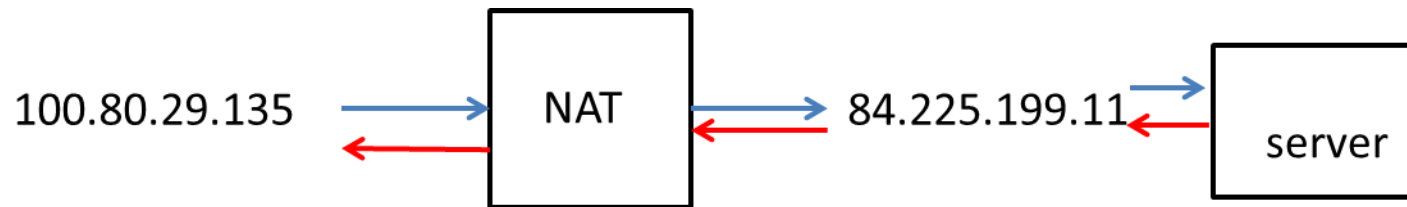
Internet Protocol

- how/why
 - more users/devices than global IP addresses available for the ISP
 - solution one:
 - assign when needed one IP address from the pool
 - hope that the total number of customers that want to use Internet is less than the available addresses



Internet Protocol

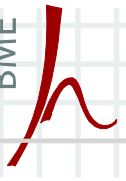
- solution two:
 - use local IP addresses, we can have more
 - and expand the namespace visible to outside
 - translate between the two: NAT Network Address Translation
 - we don't gain



Internet Protocol

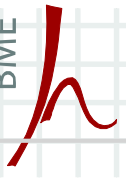
- solution three:
 - expand the namespace: use TCP/UDP port
 - use the same IP address for several terminals towards outside world, with different ports
 - this is official NAPT Network Address Port Translation, but we usually call NAT
 - it works but there are a lot of problems





Internet Protocol

- How to connect autonomous systems
 - router
 - looks at the Destination address of the IP packet
 - routing table:
 - Destination Address -> output network interface
 - decrements Time To Live field
 - voilà
 - usually does a lot more
 - e.g. Network Address Translation; firewall; packet filtering
 - IP security, IP QoS
 - IPv4/v6 coexistence
 - have various interface (line) cards
 - handling of virtual networks
 - act as L2 (Ethernet) switch as well, with L2 header processing
 - knows a lot of protocols



Internet Protocol

- sending between two devices
 - in a local network: L2 address can reach the node
 - (although the IP address and everything must be put to the packet, of course)
 - packets can be forwarded based on the L2 address only
- if I want to send to a device on my network, I need to know its L2 address

Internet Protocol

sender:
152.66.248.21

152.66.248.34

web server
152.66.248.201

Ethernet

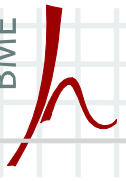
IP packet



Ethernet frame

L2 addresses

L2 addresses



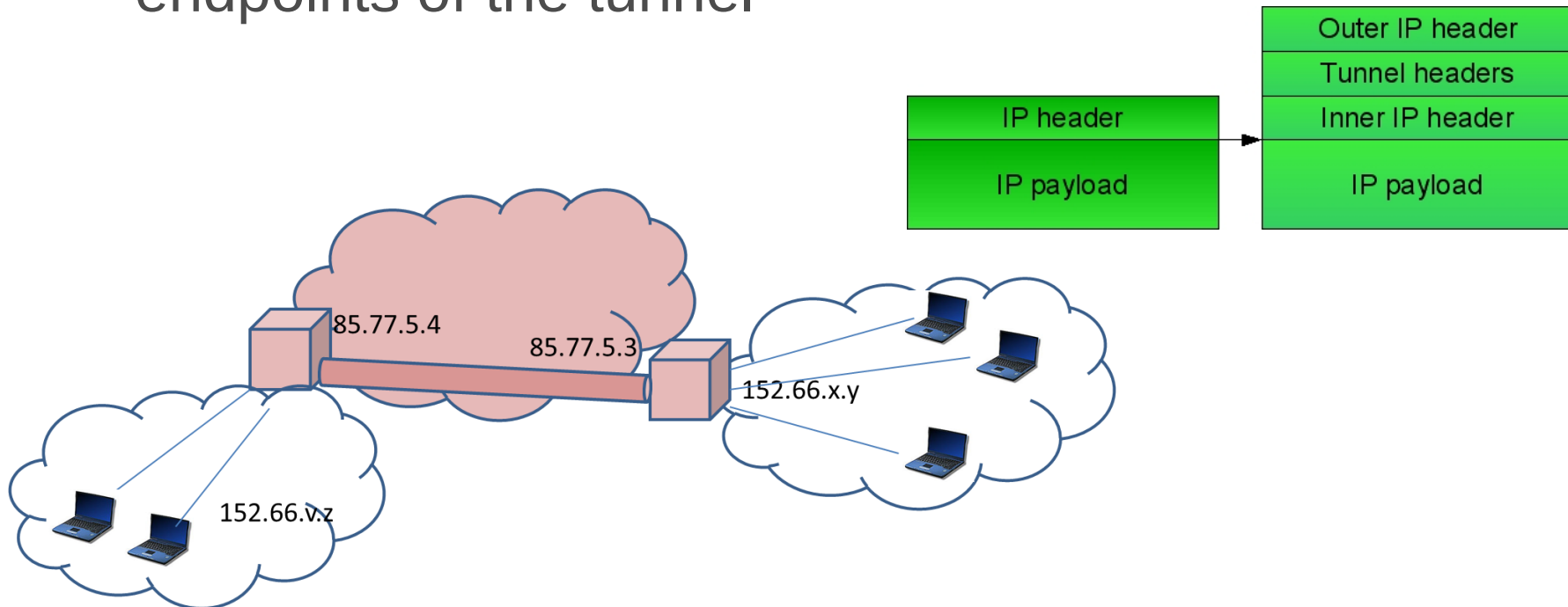
Internet protocols

- ARP Address Resolution Protocol
- I know the IP address, but what is the Ethernet address , so to whom should I send in Ethernet directly?
- a broadcast is sent to the network with the above question 😊
 - the one that I searched for answers
 - typically: the router
 - in Windows: default gateway

Internet Protocol

■ tunneling

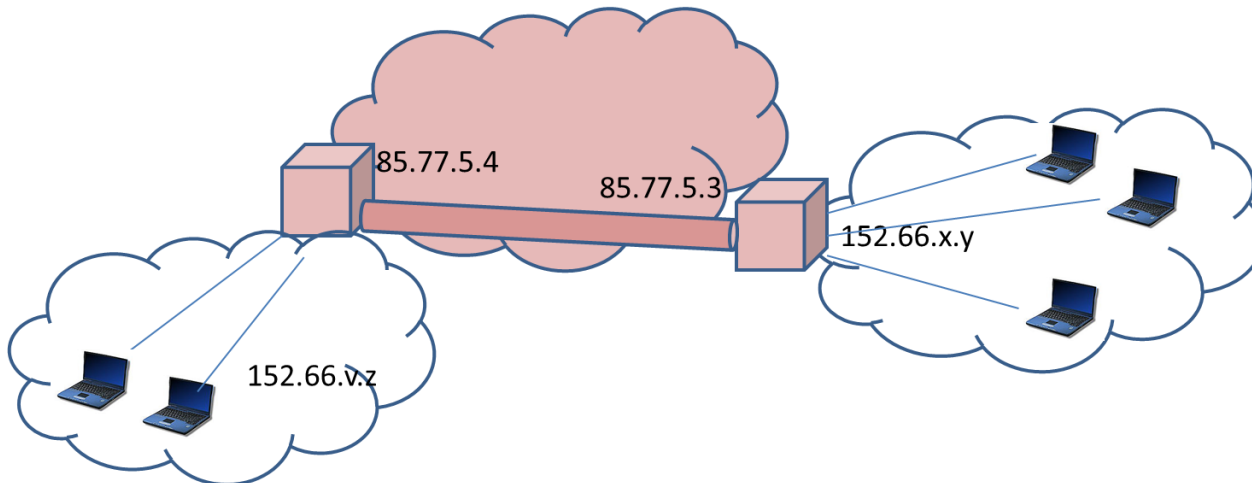
- put a new IP header before the original IP packet
- new header contain source/destination address: endpoints of the tunnel



Internet Protocol

■ tunneling

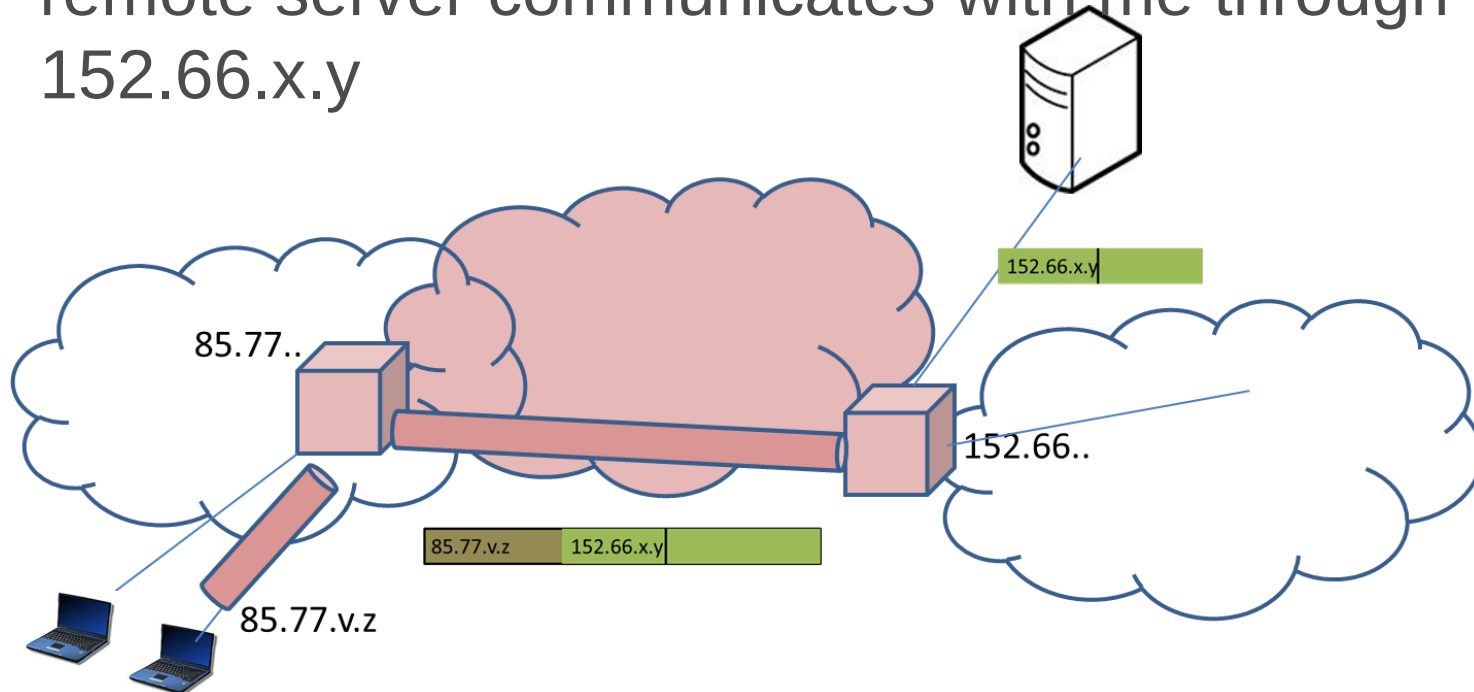
- additional features of tunneling: adding security measures (authentication, ciphering) – IPsec
- creating a fixed, secure channel between two networks: VPN Virtual Private Network

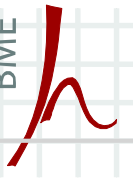


Internet Protocol

■ tunneling

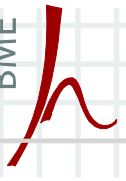
- connecting a remote client as if it was in my IP domain
- VPN server in my home network 152.66.. tunnels all my packets to my IP address 85.77.v.z
- remote server communicates with me through 152.66.x.y





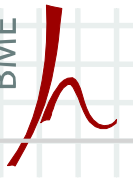
Internet protocols

- ICMP Internet Control Message Protocol
 - control messages at IP layer, in the payload of IP packets
 - signalling of errors, messages for discovering routes, paths
 - e.g.: *ping* : ICMP „echo” messages
 - check availability of a device
 - e.g. traceroute
 - show nodes in between two endpoints

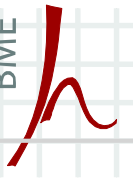


Internet protocols

- BGP Border Gateway Protocol
 - large routers of different network providers can exchange routing table information with this
 - neighbors are configured manually
 - there's a heartbeat messaging to ensure the link is still alive

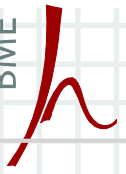


- version 6
- „new” version (December 1998)
 - „IPv4 addresses will be exhausted, IPv6 will spread in the next 10 years” – random lecturer in 2000; 2010; 2020 ...
- why
 - IPv4 address exhaustion: only roughly 4.3 billion addresses
 - everything on Internet
 - can be much better than IPv4
- why not
 - not backward compatible
 - address problem can be handled
 - if not solved



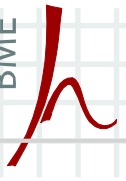
IPv6

- new IPv6 addresses: 128 bits
- 2^{128} possible addresses
 - this is a huge number
 - but there are restrictions, allocations, etc
- most pessimistic allocations estimate around 1500 addresses to each square meters of the surface of Earth (including oceans)



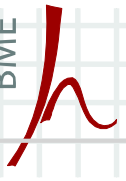
IPv6

- simplified header
- security measures built in IP layer
- mobility support
 - address auto-configuration: device can derive an own IP address when arrived to a new IP subnetwork
 - permanent IP address <-> temporary IP address binding in remote nodes
- support of IP flows
 - to handle IP packet of the same flow identically
 - to reserve capacities
 - -> ~ provide what circuit switched needs



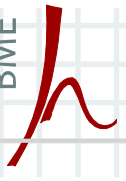
IPv6

- IPv6 is introduced in islands, slowly
- mechanisms to interconnect IPv6 domains over IPv4
- several standardized means to solve the interoperability



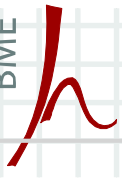
IPv6 protocol features

- Larger Address Space:
 - ~1564 addresses can be allocated to every square meter of this earth
- End-to-end Connectivity:
 - Every device will have unique IP address
 - every device can directly reach other devices on the Internet (with some limitations involved)
- Simplified Header:
 - (header: additional information for proper message delivery and processing)
 - all unnecessary information and options are moved to the end of the IPv6 header



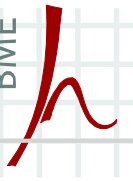
IPv6 protocol features

- Auto-configuration:
 - Whenever a node plugs in and wants to be part of a network, IP address information and router information is required to properly configure the node and get it running
 - IPv6 supports both stateful and stateless auto configuration mode of its host devices
 - stateful – DHCP (Dynamic Host Configuration Protocol):
 - host obtains the address as well as other required information such as the configuration information and parameters from a server
 - stateless:
 - a host can automatically configure its own IPv6 address and does not need any assistance from a stateful address server



IPv6 protocol features

- **Faster Forwarding/Routing:**
 - the information contained in the first part of the header is adequate for a router to take routing decisions
 - therefore making routing decision as quickly as looking at the mandatory header
- **IPSec (Internet Protocol Security):**
 - security features for the IPv6 packet: ciphering and authentication features
 - end-to-end: protects all application traffic over an IP network
- **Mobility:**
 - IPv6 was designed keeping mobility in mind
 - this feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address
 - the mobility feature of IPv6 takes advantage of auto-configuration

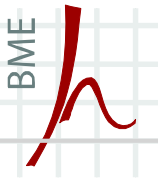


Transport protocols

- **TCP Transport Control Protocol**

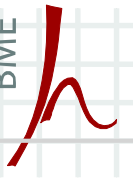
- basic goal: to send large (compared to packet sizes) files/data
 - bytestream of data
- it defines a connection-oriented transport over the connectionless IP
- reliable and in-sequence delivery based on the unreliable IP
 - acknowledgement/retransmission mechanism
 - flow control (load control) mechanism
 - two-way data transfer, multiplexing of several higher layer transfers (e.g. file downloads) over single TCP connection

- **TCP/IP**



Transport protocols

- role: transmit the data between the actual user endpoints
- TCP packets are called TCP segments
- before actual transmission, there is a connection setup phase
 - the two parties agree upon an initial sequence number, to start with
 - signaling of being ready to transmit/receive
- ending a connection explicitly
- acknowledgement of connection end

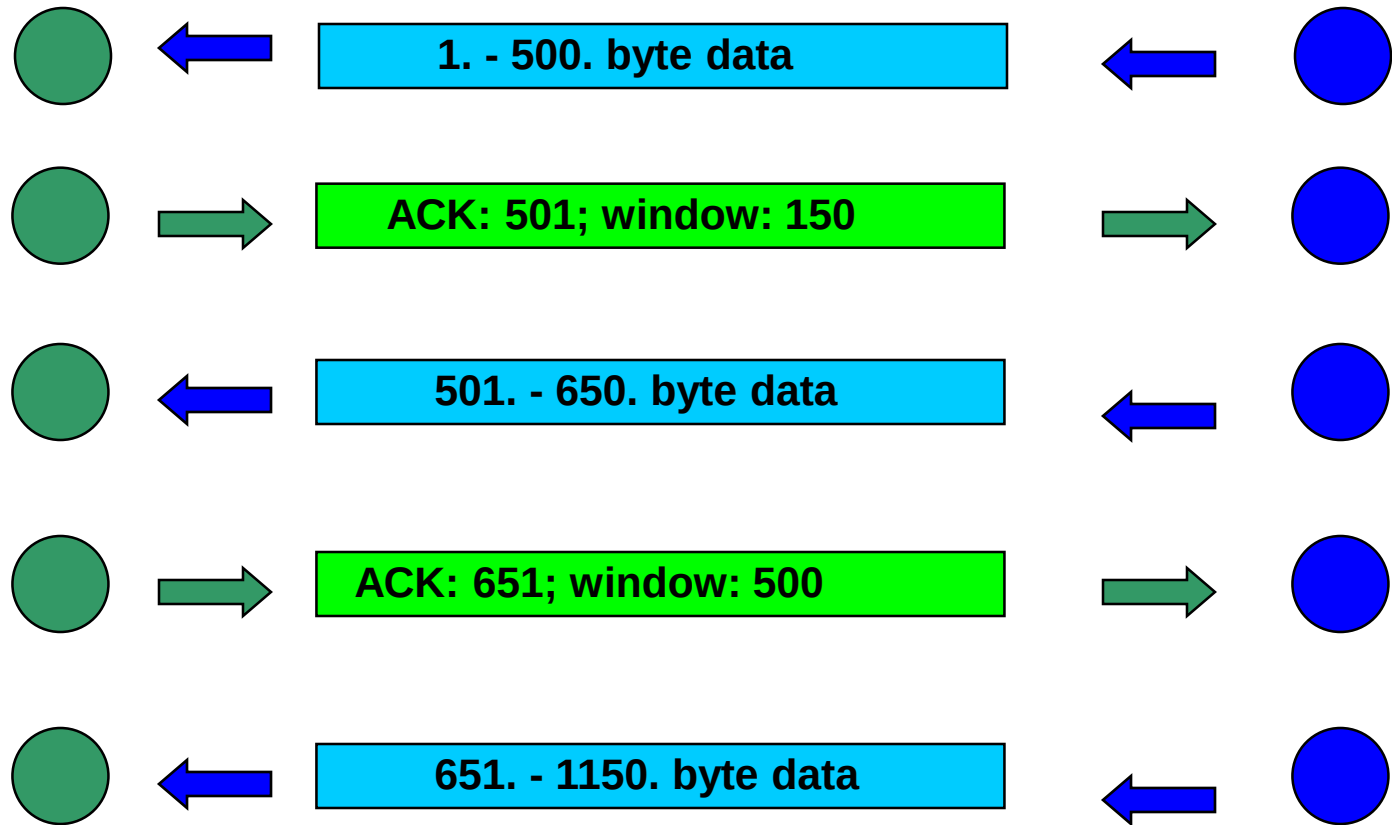


Transport protocols

- transmission over connection
 - sliding window mechanism for flow control and acknowledgement procedure
 - ack-ing: receiver tells the sender in the header of TCP segment that what is the last byte received correctly
- flow control:
 - receiver tells the window size: how many more bytes can it receive
 - this enables talking of endpoints with different bitrate and processing rates
 - the sender does not overflow the receiver
- slow start: initial window size is small and increases
- congestion control:
 - in case of ACK timeout the sender assumes congestion and smaller window is used

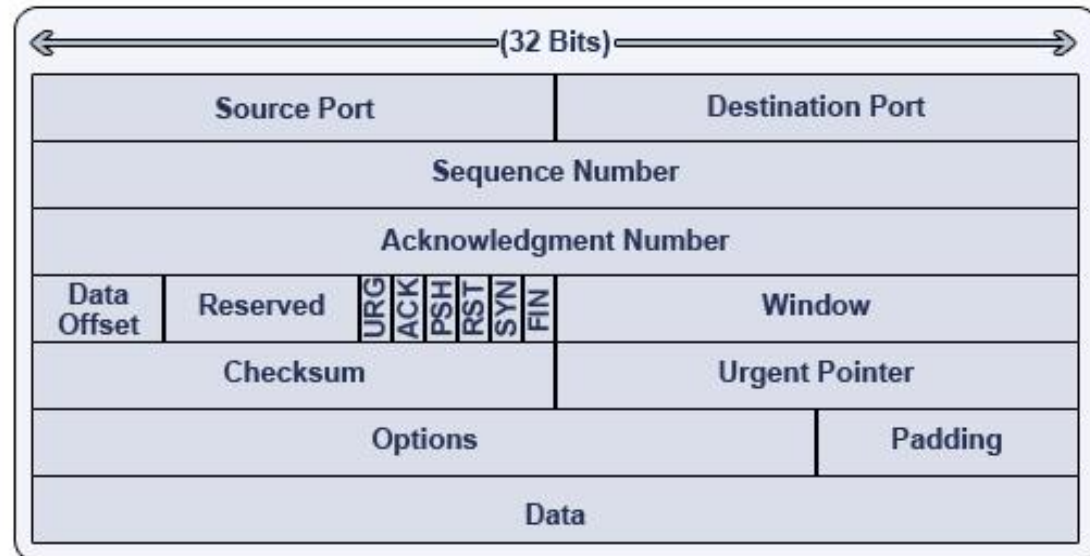
Transport protocols

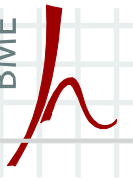
E.g.



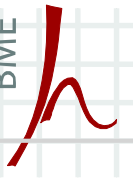
Transport protocols

- TCP segment
 - source port and destination port: a 2 byte identifier of the TCP connection
 - TCP port + IP address: a network socket
 - „server listens to port”: check incoming packets’
Destination Port
 - well known ports:
 - client should know in advance
 - IANA
 - e.g. HTTP: 80





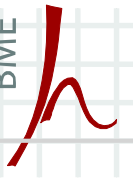
- TCP (Transmission Control Protocol):
 - provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating (host-to-host connection) over an IP network
 - At the lower levels of the protocol stack, due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets may be lost, duplicated, or delivered out of order.
 - TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. If the data still remains undelivered, its source is notified of this failure.
 - Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the receiving application.



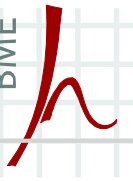
Transport Protocols

■ **UDP User Datagram Protocol**

- connection-less transport protocol
- simple, low overhead
- no flow control, no retransmissions
 - UDP packet based
- typically: for small, periodic data units
 - voice, video
 - better to lose some packets than being delayed because of the retransmissions
- interesting: connection setup is handled in above layers in this case
- simply: source port, destination port, error detection

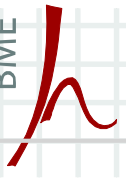


- UDP (User Datagram Protocol):
 - simple, connectionless and stateless transmission model with a minimum of protocol mechanism
 - there is no guarantee of delivery, ordering, or duplicate protection – unreliable
 - provides checksums for data integrity
 - time-sensitive/real-time applications often use it
 - no notification for upper layers about data delivery



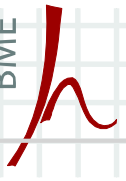
Upper layers

- DNS Domain Name System
- delivery based on IP address
- but it is not known in advance, rather a name
 - e.g. `www.hit.bme.hu` <-> IP address ?
- to handle the name <> IP address relations
- in ancient times it was in a file



Upper layers

- hierarchical, distributed directory of names around the world
- DNS concept:
 - domains of names
 - more domains in domains
 - domains are managed by authorities
 - name servers for the domains
 - supervision: IETF (<http://www.i-d-n.net/>)
 - root name servers

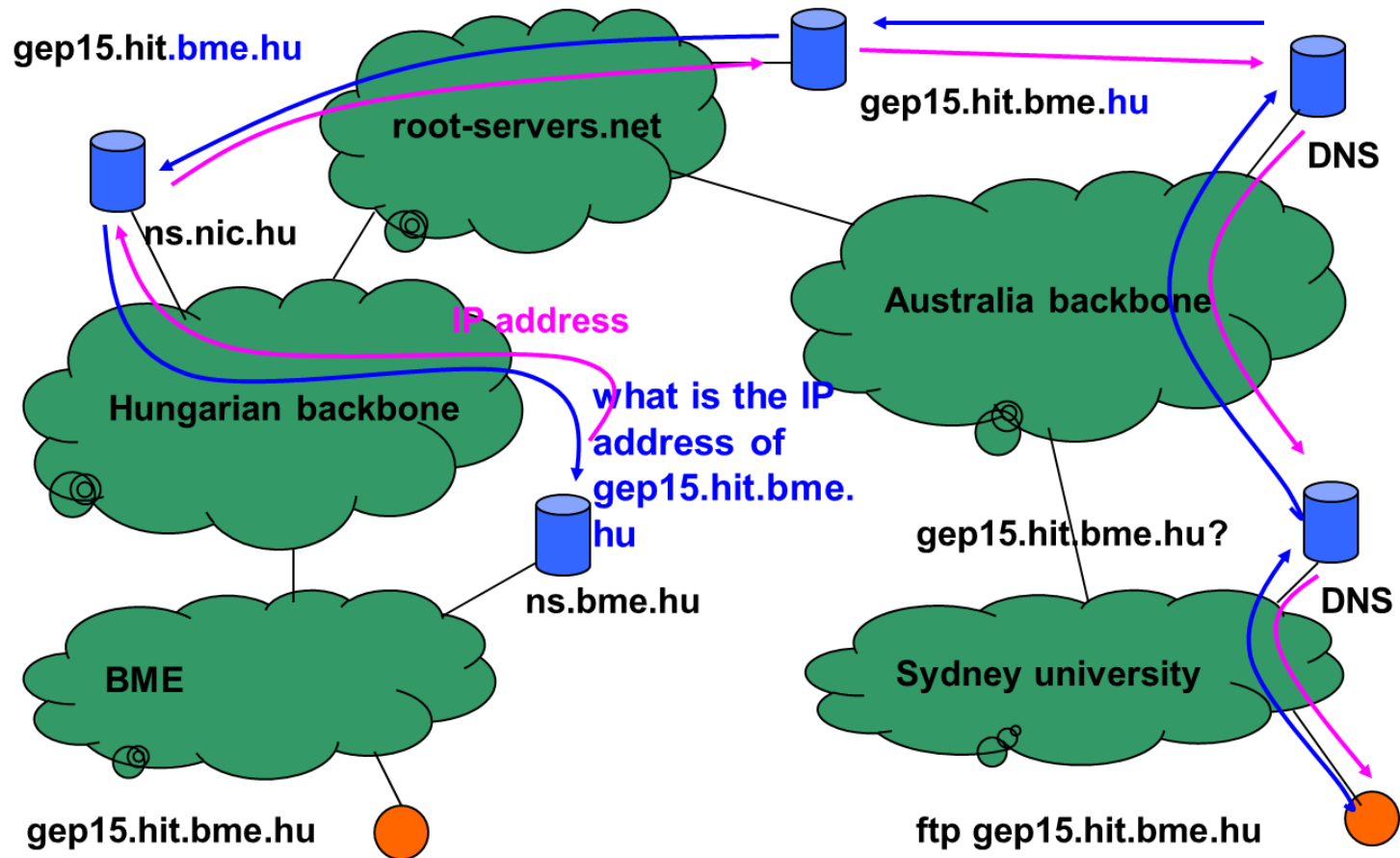


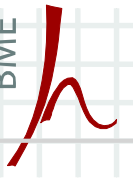
Upper layers

- names or domains not necessarily (but often) mean network/organisational relations
- devices of any domain can be distributed anywhere physically
 - e.g. .com domain servers
- name servers know the IP address of devices in the domain
 - or the IP address of name servers of subdomains

BME Upper layers

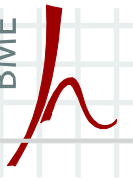
- example of recursive query
- can be query chain





Ethernet

- „the” layer 2 of IP networks
 - first: local networking technology
 - create a small computer network
 - coaxial cable
 - now: local to metropolitan network sizes
 - twisted pair cable in local, optical fibre in metropolitan solutions
- Some notions of Ethernet
 - 10; 100; 1000 at the beginning means the network operates at 10, 100, 1000 Mbps
 - BASE means the type of signaling used is baseband
 - 2 or 5 at the end indicates the maximum cable length in 100 meters.
 - T: twisted pair, F: fiber; X: duplex
 - 1000 Base FX
- state of the art: 40 Gbps, 100 Gbps Ethernet links
- switches/routers with multiple 40 Gbps Ethernet interfaces



Ethernet

- addressing:
 - MAC address (often called physical address) of the interface
 - 6 bytes, source address, destination address
- switching:
 - based on destination address, similar to how it is in IP router
 - does not consider anything beyond the Ethernet header
 - switch learns MAC addresses
- no provisioning for QoS or bandwidth allocation

Ethernet

- 802.1q extension of the protocol
 - new part in the Ethernet header
 - to implement priorities
 - 7 priority classes, switches forward higher priorities first
- VLAN Id.
 - Virtual LAN
 - single VLAN id.: as if the hosts were on the same LAN

