SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

WebElektronika

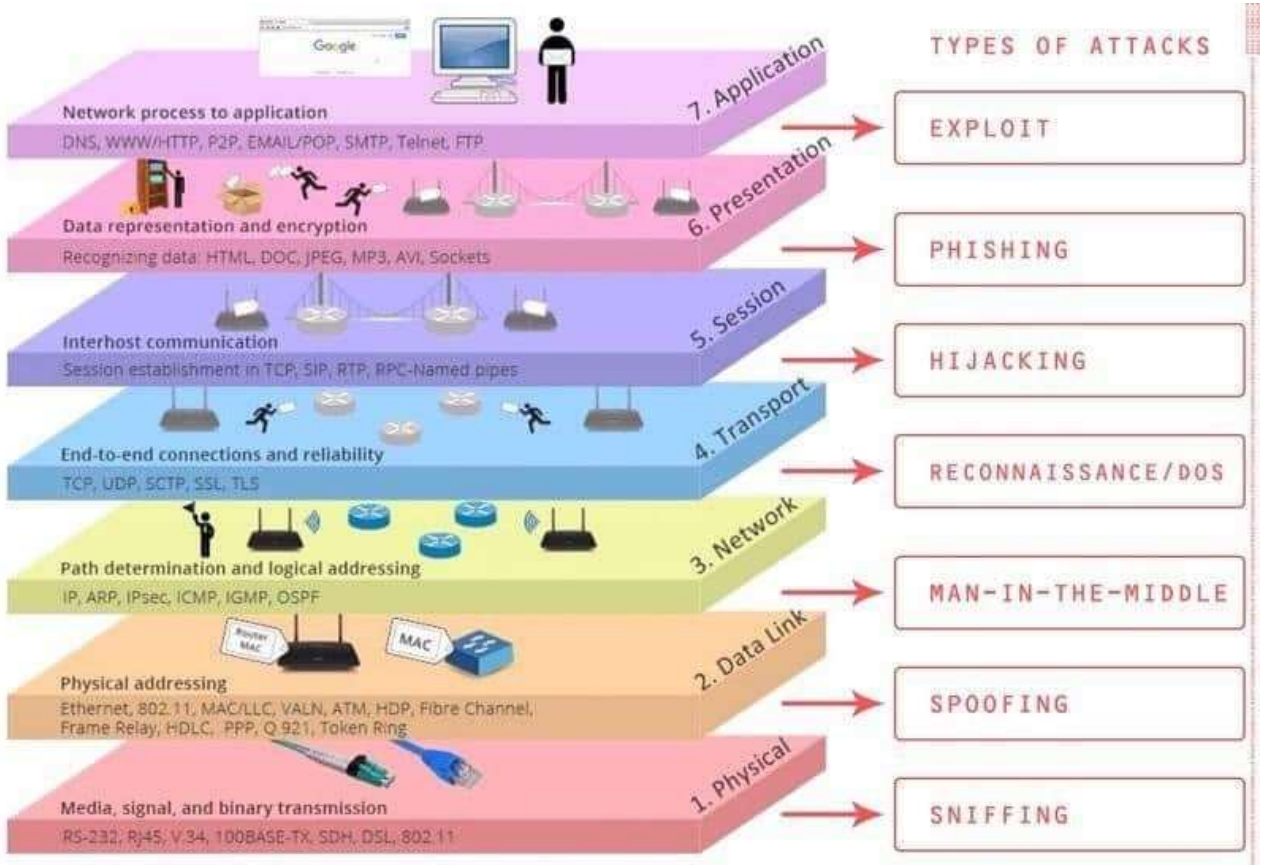
Etikus hackelés alapjai

Alapok, néhány protokoll

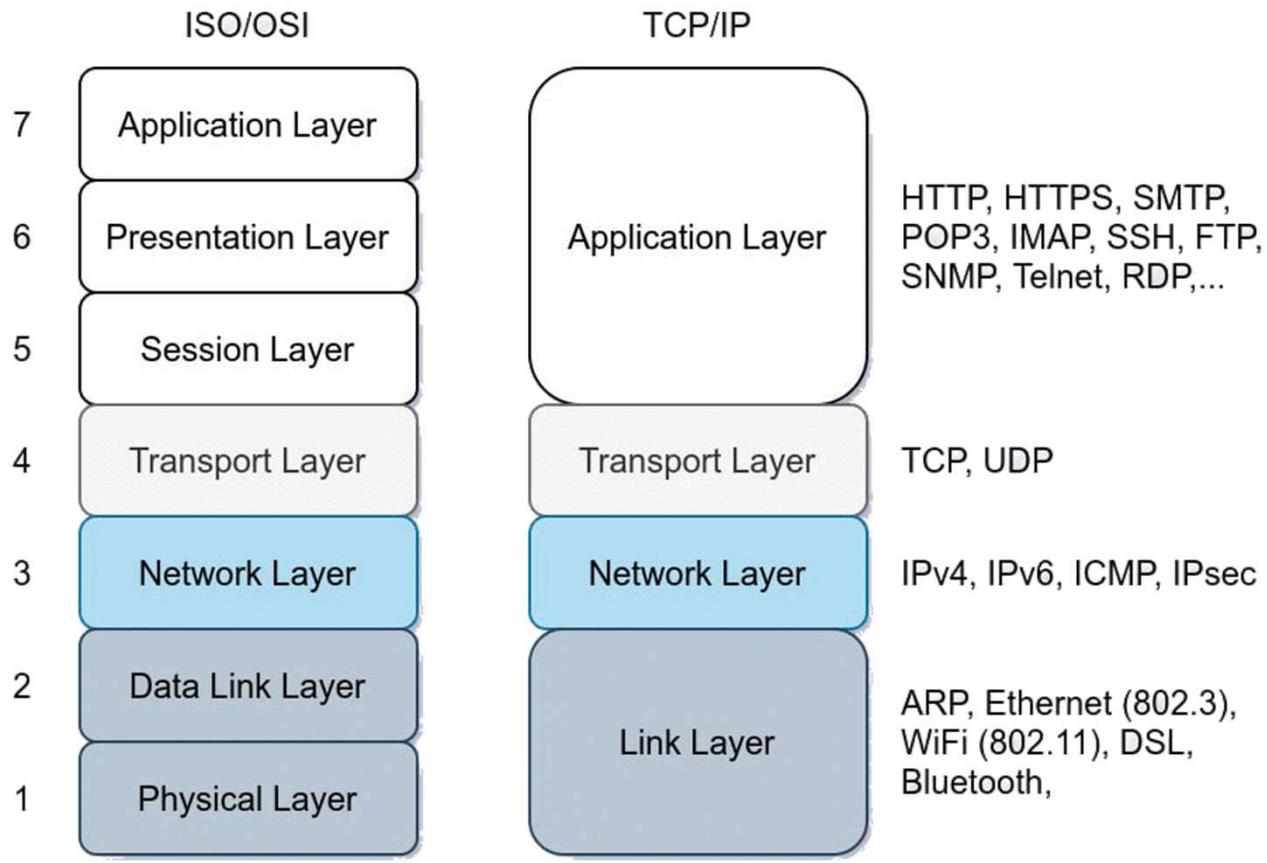
Dr. Hidvégi Timót
egyetemi docens

OSI modell (hálózati réteg)

LAYER 7	APPLICATION	Network process to application
LAYER 6	PRESENTATION	Data representation and encryption
LAYER 5	SESSION	Interhost communication
LAYER 4	TRANSPORT	End-to-end connections and reliability
LAYER 3	NETWORK	Path determination and IP
LAYER 2	DATA LINK	MAC and LLC (Physical addressing)
LAYER 1	PHYSICAL	Media, signal and binary transmission

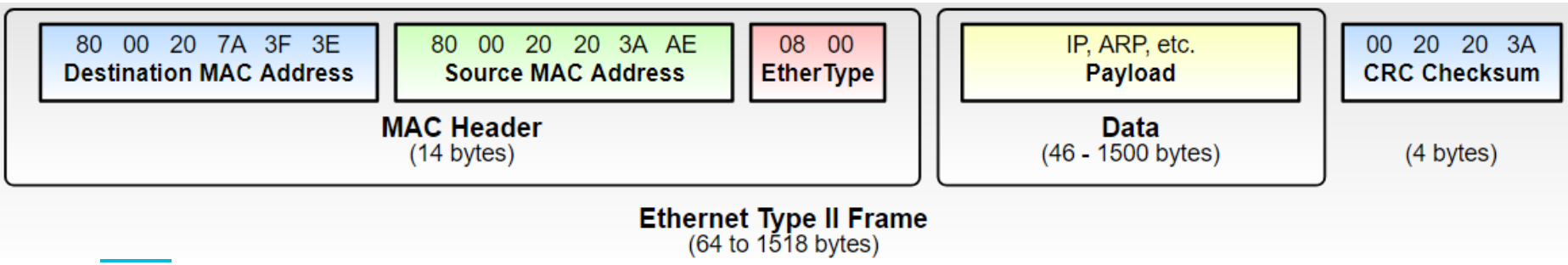


OSI – TCP/IP

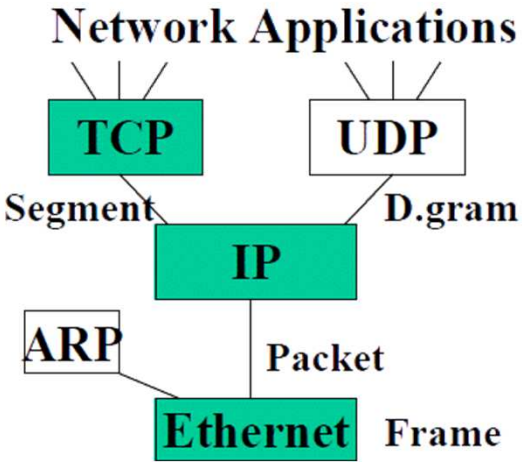

ISO/OSI
TCP/IP
7
Application Layer
6
Presentation Layer
5
Session Layer
4
Transport Layer
3
Network Layer
2
Data Link Layer
1
Physical Layer
Application Layer
Transport Layer
Network Layer
Link Layer
HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, SNMP, Telnet, RDP,...
TCP, UDP
IPv4, IPv6, ICMP, IPsec
ARP, Ethernet (802.3), WiFi (802.11), DSL, Bluetooth,

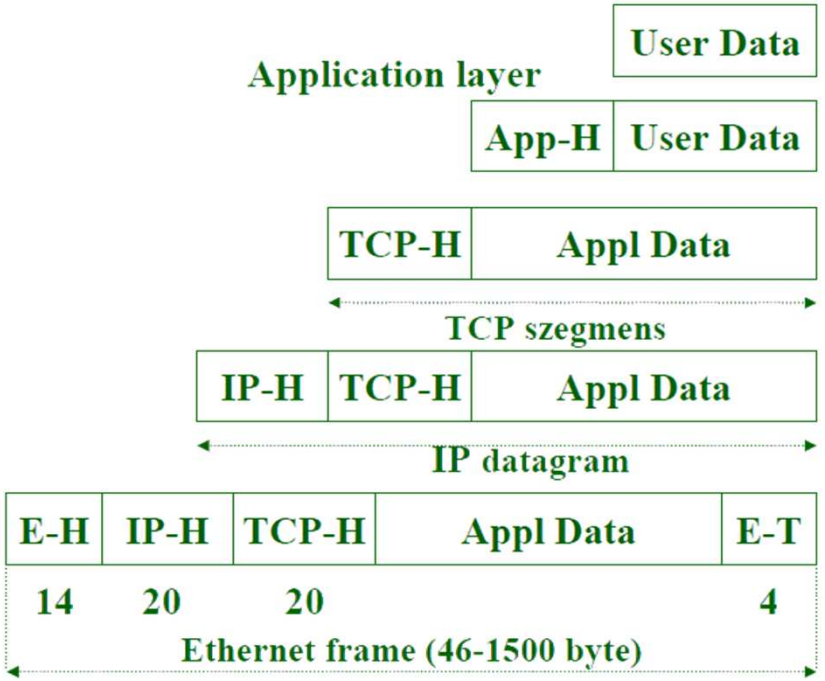
Ethernet frame-ek

Layer	Preamble	Start frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1522 octets →						
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →



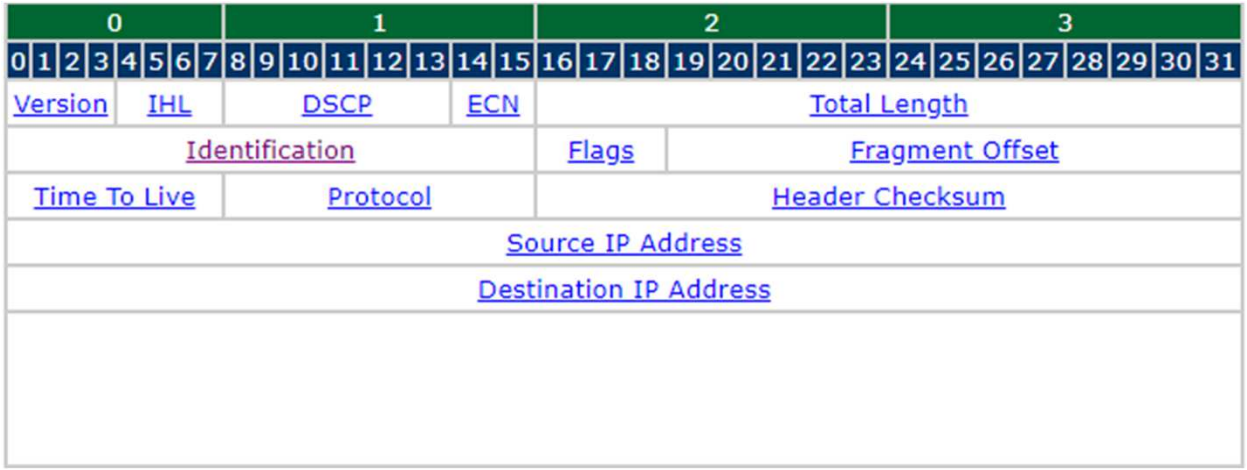
Enkapszuláció





Internet Protokoll (IP)

- IP hálózat vezérlése: ICMP
- IP hálózat felhasználása: TCP, UDP
- IP fejléc



IP címek fejlődése

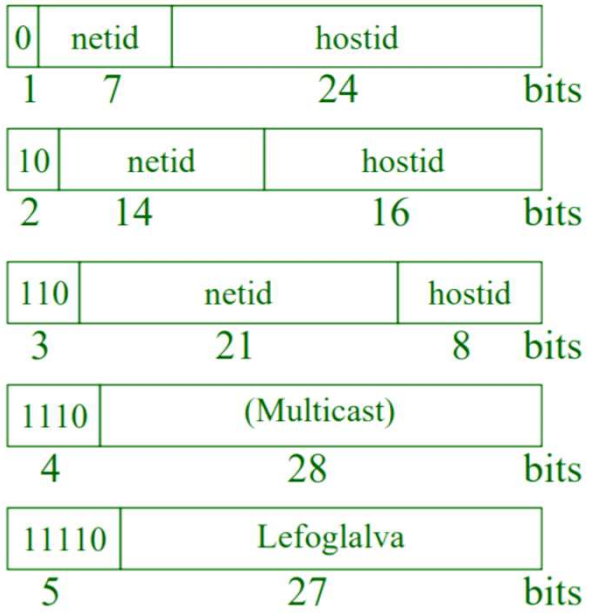
- Bármely hoszt bármely hoszttal kapcsolatba léphet az IP protokollal -> IP cím kell
- IP címek fejlődése
  - Klasszikus címosztályok: 1981
  - Alhálózatok: 1985
  - Változó méretű alhálózatok: 1987
  - Osztálymentes címzés: 1993
  - Címfordítás: 1994

IP cím

- Ipv4: 32 bites, 4byte, négy mezőből (oktet) áll
  - 0 < oktet < 255
  - Pl.: 192.168.1.5: 1100 0000.1010 1000. 0000 0001.0000 0101
- IPv6: 128 bits
- Egy gépnek több IP címe: pl.: több hálózati interfész egy gépben, router
- Több gépnek egy IP címe: NAT, proxy
- Max címszám: 2^32: 4 milliárd cím (ennyi nincs, IP osztályok vannak)
- Speciális IP címek
  - 0.0.0.0: határozatlan IP cím
  - 255.255.255.255: szórási cím, mindenkinek
  - 127.X.X.X: visszacsatolási cím

IP cím

- Logikailag „netid” és „hostid”-ből áll a cím
  - netid mérete határozza meg az osztályt
    - *8bit: A*
    - *16bit: B*
    - *24bit: C*
- Hálózat címe + hoszt címe
  - „A” osztály: 1.0.0.0 – 127.0.0.1
    - *10.0.0.0 belső hálózat*
  - „B” osztály: 128.0.0.0 – 191.255.0.0
    - *172.16.0.0 – 172.31.0.0 belső hálózat*
  - „C” osztály: 192.0.0.0 – 223.255.255.0
    - *192.168.1.0 – 192.168.255.0*
  - „D” osztály: 224.0.0.0 – 239.0.0.0
    - *Multicasting eljárásra használják*
  - „E” osztály: 240.0.0.0 – 255.0.0.0



IP cím, privát tartomány

- Ezek az IP címek nincsenek közvetlenül az Interneten, nem lehet regisztrálni -> a saját hálózatokon belül használható -> sok egyforma IP cím lehet a világon gond nélkül.

```
10.0.0.0        -   10.255.255.255  (10/8 prefix)
172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

Címfoglalás

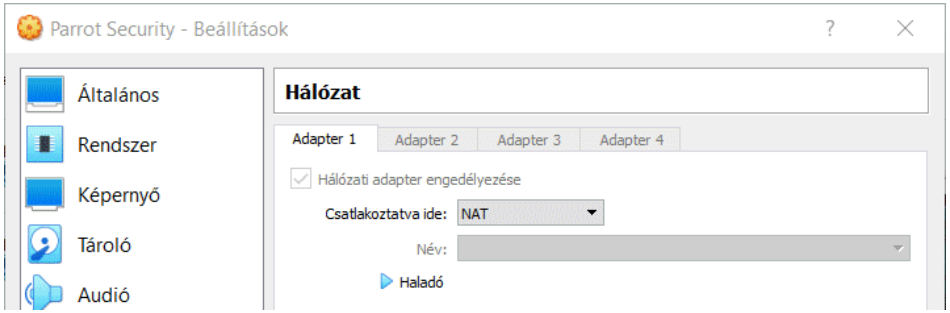
- Az Interneten minden IP egyedi cím. Engedélyezés: IANA, RIPE
- Internetről nem elérhető (magán) hálózaton:
  - Tetszőleges kiosztás
  - Lokális címtartományok (RFC1918)
    - *10.0.0.0/8*
    - *172.16.0.0/12*
    - *192.168.0.0/16*
  - Magánhálózat csatlakoztatása az Internetre:
    - *NAT (Network Address Translation, címfordítás), RFC1631 (magánhálózatról bejegyzett címtartományra való áttérés) a külső és a belső IP címek összerendelése*

      193.45.56.67/32 NAT 10.0.1.0/24

    - *Proxy használata*

NAT

- Külső cím:
  - Belső címet kicseréli a külsőre
  - A belső port szabad a külső részen is?
    - *Igen: az kerül kiválasztásra*
    - *Nem: a szabad portokból egy kerül kiválasztásra*
  - Nincs szabad port -> eldobásra kerül a csomag
  - Sikeres fordításnál ezek az adatok bejegyzésre kerülnek egy táblázatban



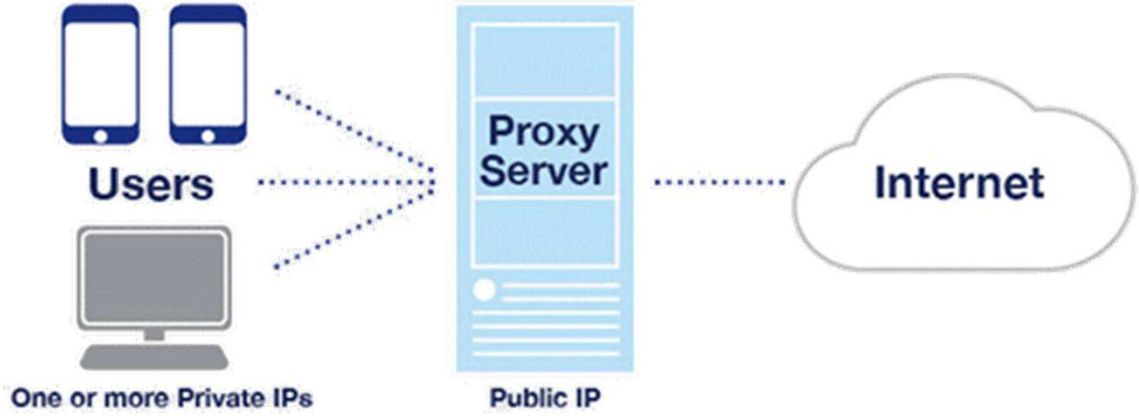

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
oup default qlen 1000
    link/ether 08:00:27:93:52:a3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86018sec preferred_lft 86018sec
    inet6 fe80::5115:c8f8:cc90:be9a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
┌──[user@parrot]─[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=15.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=13.1 ms
```

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1…	7.117938	192.168.0.15	8.8.8.8	ICMP	98	Echo (ping) request
1…	7.132411	8.8.8.8	192.168.0.15	ICMP	98	Echo (ping) reply
1…	8.120031	192.168.0.15	8.8.8.8	ICMP	98	Echo (ping) request
1…	8.134045	8.8.8.8	192.168.0.15	ICMP	98	Echo (ping) reply
1…	9.129924	192.168.0.15	8.8.8.8	ICMP	98	Echo (ping) request
1…	9.142241	8.8.8.8	192.168.0.15	ICMP	98	Echo (ping) reply
1…	10.131000	192.168.0.15	8.8.8.8	ICMP	98	Echo (ping) request
1…	10.144896	8.8.8.8	192.168.0.15	ICMP	98	Echo (ping) reply

Proxy

- Egy „csomópont” a privát és a publikus IP között



- Anonimitást biztosító proxy-k
  - http://proxy.org
  - http://dontfilter.us
  - https://newipnow.com

IP címtartomány

- https://users.iit.uni-miskolc.hu/~szkovacs/GAMFNetD/NetDE4.pdf

Osztály	Oszt.+hálózati bitek száma	Hálózatok száma	Gép bitek száma	Gépek száma	Címmező foglalás
A	1 + 7	$2^7 - 2 = 126$	24	$2^{24} - 2 = 16777214$	49,21%
B	2 + 14	$2^{14} = 16384$	16	$2^{16} - 2 = 65534$	24,99%
C	3 + 21	$2^{21} = 2097152$	8	$2^8 - 2 = 254$	12,40%
D Multicast	4 + 28	$2^{28} = 268435456$	-	-	6,25%
E Fenntartva	4	-	32 - 4	$2^{28} - 1 = 268435455$	6,25%

Address Resolution Protocol (ARP)

- IP címek <-> MAC címek
- https://datatracker.ietf.org/doc/html/rfc826

ARP Packet Header	
Hardware type (2B)	Protocol type (2B)
Hardware Address length (1B)	Protocol Address length (1B)
Opcode (2B) 1: ARP_request 2: ARP_reply	
Sender IP Address	
Sender MAC Address	
Target IP Address	
Target MAC Address	
Ethernet Header	
Ethernet Sender Address	
Ethernet Target Address	
Ethernet Frame Type	

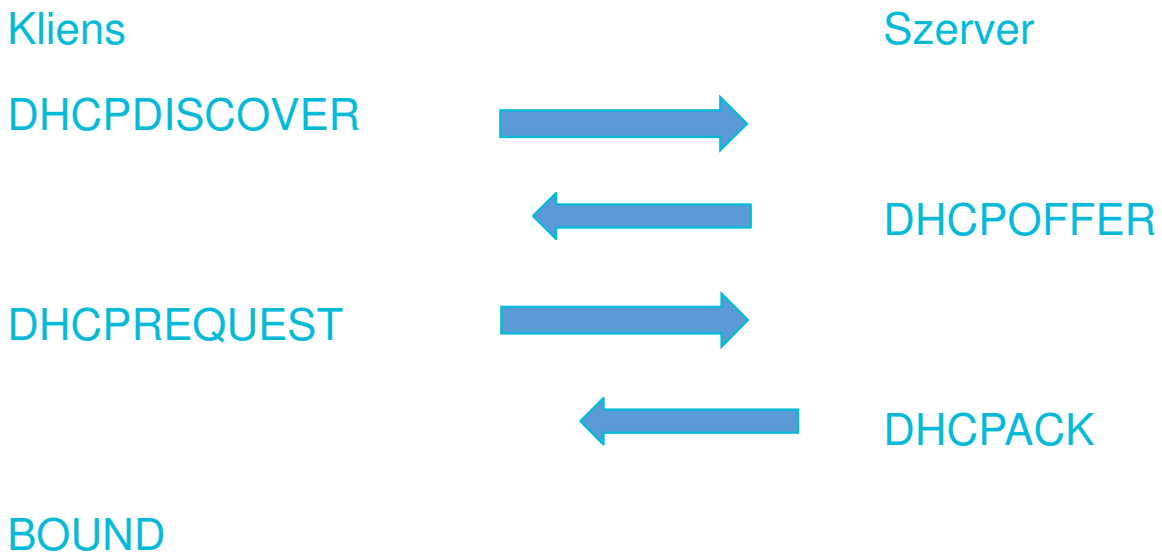
```
    5 0.119299    00[redacted]  ARP      60 Who has 172.24.0.167?
    6 0.119382    Goo[redacted]  ARP      42 172.24.0.167 is at 00:
Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \De
Ethernet II, Src: [redacted], Dst: [redacted] (00
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: [redacted]
    Sender IP address: 172.[redacted]
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.[redacted]
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_34:…	Broadcast	RARP	42	Who is 00:0c:29:34:0b:de? Tell 00:0c:29:34:0b:de
2	0.002000	VMware_c5:…	VMware_34:…	RARP	42	00:0c:29:34:0b:de is at 10.1.1.100

```
Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface Unknown/not availa
Ethernet II, Src: VMware_c5:f6:9b (00:0c:29:c5:f6:9b), Dst: VMware_34:0b:de (00:0c:29:34:0b:de)
Address Resolution Protocol (reverse reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reverse reply (4)
    Sender MAC address: VMware_c5:f6:9b (00:0c:29:c5:f6:9b)
    Sender IP address: 10.1.1.10
    Target MAC address: VMware_34:0b:de (00:0c:29:34:0b:de)
    Target IP address: 10.1.1.100
```

DHCP

- Hogyan szerezzünk IP címet?
  - Statikus (rendszergazda kell)
  - RARP (Reverse ARP) – elavult
  - Bootp – elavult
  - DHCP
    - *RFC 1541, 2131, 2132*
    - *UDP protokoll: 67-es port: szerver, 68-as port: kliens*
    - *Folyamat:*



DHCP üzenettípusok

- DHCPDISCOVER: hol az a szerver?
- DHCPOFFER: Itt vagyok, IP-vel rendelkezem, tudom adni
- DHCPREQUEST: kérem azt az IP-t
- DHCPACK: Oké, tiedé az IP, plusz paraméterek
- DHCPNAK: nem OKÉ, nem adom az IP-t
- DHCPDECLICE: nem jó, amit adtál
- DHCPRELEASE: visszaadom az IP-t
- DHCPINFORM: IP nem kell, de a paraméterek igen

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

Néhány opció

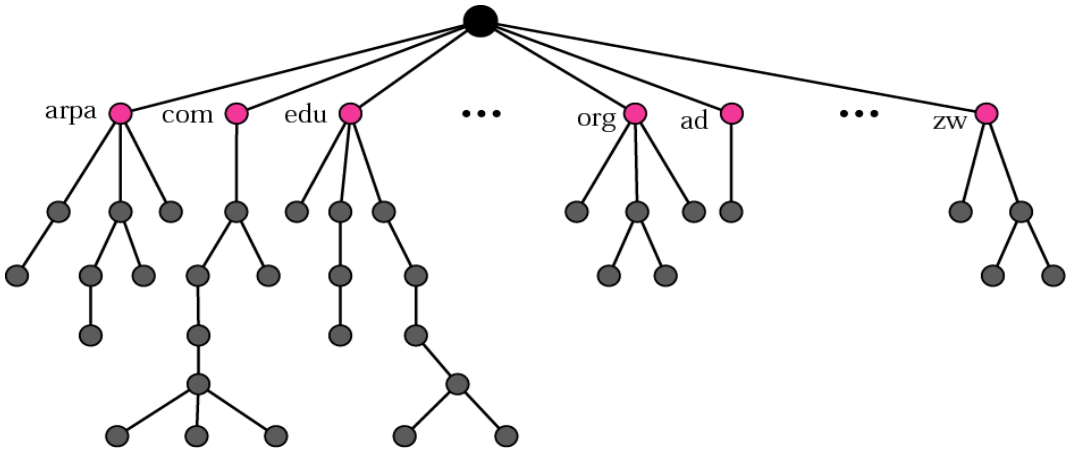
- 53 – DHCP üzenettípus (kötelező)
- 50 – Kért IP cím
- 51 – Kölcsönzési idő
- 1 – subnet-mask
- 3 – routers
- 4 – ntp-servers
- 5 – domain-name-servers
- 15 – domain-name
- 12 – host-name
- 28 – broadcast-address

Domain Name System (DNS)

- IP címek megjegyzése??? -> inkább könnyen megjegyezhető nevek legyenek
- Cím – Név hozzárendelés
- Struktúra
  - Egyszintű – pl. lajosbacsiszamitogepe, htpc
  - Hierarhikus – pl. pandora.inf.elte.hu
- Egyértelműség
  - Kölcsönösen egyértelmű
  - Több név egy cím → pl. virtuális webszerverek
  - Egy név több cím → pl. terhelésmegosztás
    - *Több unicast cím*
    - *Egy anycast cím (IPv6) vagy trükközés a BGP-vel (IPv4)*

DNS

- Elosztott adatbázis
  - Nem központosított
- Egyszerű kliens-szerver architektúra
  - UDP 53-as port, vannak TCP implementációk is
  - Rövid kérések – rövid válaszok; kérés-válasz típusú kommunikáció
- Hierarchikus névtér
  - Szemben a hosts.txt alapú flat megoldással
  - pl. .com → google.com → mail.google.com
  - Fordított fa – a gyökere a tetején
  - Maximum 128 szint – gyökér=0



Névfeloldás

- Minden hoszt ismer egy lokális DNS szervert
  - Minden kérést ennek küld
- Ha a lokális DNS szerver tud válaszolni, akkor kész…
  1. A lokális szerver a felügyelő szerver az adott névhez
  2. A lokális szerver cache-ében van rekord a keresett névhez
- Különben menjünk végig a teljes hierarchián felülről lefelé egészen a keresett név felügyeleti szerveréig
  - Minden lokális DNS szerver ismeri a root szervereket
  - Cache tartalma alapján bizonyos lépések átugrása, ha lehet
    - *Pl. ha a root fájl tárolva van a cache-ben, akkor egyből ugorhatunk az „.edu” szerverére.*

Internet Control Message Protocol (ICMP)

- Feladata:
  - Hálózati diagnosztika
  - Hibák és azok típusainak a megismerése
- Néhány példa
  - Nem garantált a csomagok megérkezése, és azok sorrendje sem
  - Elérhetetlen cél
  - Időtúllépés
  - Visszahang kérés/válasz
- IP protokollnál az ICMP azonosítója: 1
- ICMP csomagok csak az IP-n belül lehetnek
- https://datatracker.ietf.org/doc/html/rfc792

	0								1								2								3							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Type								Code								Checksum															
32	Rest of header																															

Mikor használjuk? (ICMP)

- Lejárt a csomag élettartama. Router küldi, ha
  - TTL nullára csökken
  - A célállomás küldi, ha a fragmentek összevárására kijelölt idő letelt
- Címzett elérhetetlen, a router küldi a Sendernek, ha:
  - Címzett nem létezik
  - Címzett túl messze van
- Hibás IP csomag
- Időbélyeg kérése és válasz
  - Állomások óráinak a szinkronizálása
- Túl gyors a csomagküldés, küldheti a router vagy a címzett
- Átirányítás
- Echo echo replay. Címzett elérhető? „ping” Echo-ra a címzett „echo replay”-t küld

Demo (ping)

- ping /h
  - -a
  - -n
  - -i
  - stb

```
C:\Users\[redacted]>ping /h
Bad option /h.

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
```

Hypertext Transfer Protocol (HTPP)

- HTTP/1.0 → RFC1945 (1996)
- **HTTP/1.1 → RFC2616 (1999)**
- WebDAV → RFC4918 (2007)
- WebSocket → RFC6455 (2011)
- HTTP/2 → RFC7570 (2015)

HTTP

- Alkalmazás szintű protokoll
- Megbízható stream alapú protokoll felett – TCP, TLS
- Adatáramlás modellje: üzenet, válasz
- Állapotmentes
- Átvitt adat:
  - Hypertext, hypermedia

Kérés

- <metódus> <erőforrás> <verzió> <CRLF>
  "Host: " <hosztnév> <CRLF>
  [<header kulcsszó> "="string<CRLF>]*
  <CRLF>
  [<body>]
- metódus ::= "GET" | "POST" | "HEAD" | "PUT" | "DELETE " | "TRACE" | "OPTIONS" | "CONNECT"
- erőforrás ::= <URL>
- verzió ::= "HTTP/1.1"

- Metódusok
  - GET
    - *Elkéri az URL-ben megadott erőforrás egy példányát. A válasz az 1.1-nél a TCP kapcsolatban érkezik.*
  - HEAD
    - *Ugyanaz, mint a GET csak nem hozza el a tartalmat csak a fejlécet.*
  - OPTIONS
    - *Megadja milyen metódusok támogatottak*
  - TRACE
    - *Visszaküldi a kapott kérést*
  - PUT
    - *Feltölti az erőforrás helyre a tartalmat.*
  - DELETE
    - *Törli az erőforrás helyén levő tartalmat.*
  - POST
    - *változók feltöltése a body részben*

Válasz

- <verzió> <status kód> <ok-emberi-nyelven>
- Pl.: HTTP/1.1 404 Not found
- 1XX Információ
  - pl.: Webdav esetén 102 Processing Várni kell folyik a munka (több is jöhet)
- 2XX Sikerült
  - 200 OK vagy 204 No content – minden rendben de nem kell válasz
  - 206 Partial content – nem az egészet kérték ezért nem az egész ment
- 3XX Átirányítás
  - 301 Moved permanently vagy 304 Not modified (ha a kliens If-Modified-Since headert küldött), azaz jöhet a gyorsítótárból.
- 4XX Kliensoldali hiba
  - 400 Bad request vagy 403 Forbidden vagy 404 Not Found
- 5XX Szerveroldali hiba
  - 500 Internal server error vagy 507 (WebDAV) Insufficient Storage

Industrial and Research Lab for Cybersecurity

- Web
  - https://cyberseclab.eu
- Facebook
  - https://www.facebook.com/IndustrialandResearchLab
- Github
  - https://github.com/cyberseclabor
- Linkedin
  - https://www.linkedin.com/company/industrial-and-research-lab-for-cybersecurity

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

CYBERSECLAB

Industrial and Research Lab for Cybersecurity