Számítógépes hálózatok - 4. előadás

ARP, RARP, BOOTP, DHCP

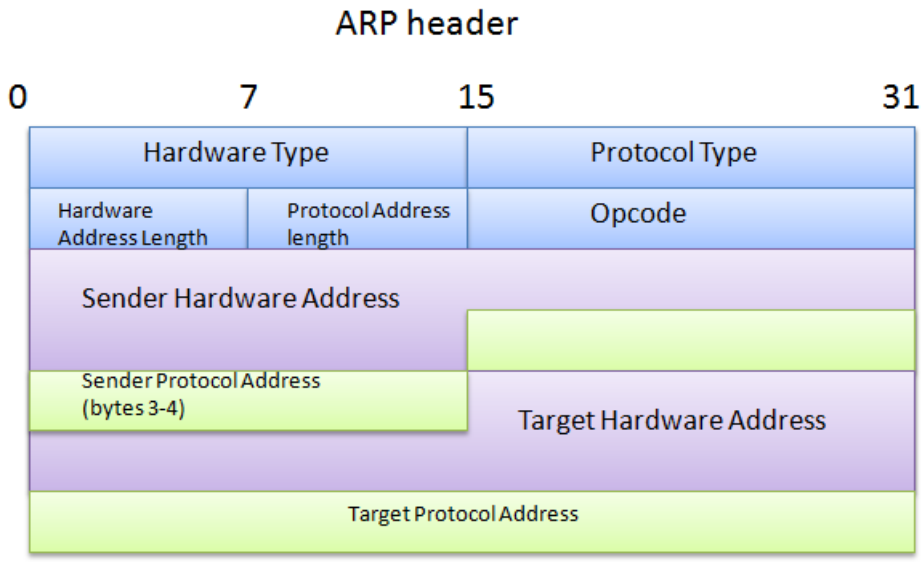
Hogyan tudja meg a link layer (ethernet) címet egy hálózati állomás?

- ARP - Address Resolution Protocol
- **RFC826**
- Elsősorban etherneten

ARP csomag formátum

```
6          6         2        2        2        1      1      2      6
+--------+---------+-------+-------+-------+-----+-----+-----+
|Ethernet| Ethernet| típus |hardw  | proto |Hardw| Prot|Opcod|
|cél     |  forrás |       | típus | típus | size| size|     |
+--------+---------+-------+-------+-------+-----+-----+-----+
   <- Ethernet header ->    |                          <- ARP he
```

Vagy másképp felrajzolva:



- Az ethernet type: `0x806`
- A kérés broadcast, a válasz unicast
- Hardware type: ethernetnél 1
- Protocol type: IP-nél `0x800`
- Hardware size (address length): 6 (ethernet cím hossza)
- Protocol size (address length): 4 (IP cím hossza)
- Opcode: 1 ha kérés, 2 ha válasz, 3 ha RARP request, 4 ha RARP válasz

```
22:25:58.477643 0:b:cd:8:24:22 Broadcast arp 42: arp who-has 1
22:25:58.477818 0:7:e9:2e:74:99 0:b:cd:8:24:22 arp 60: arp rep
```

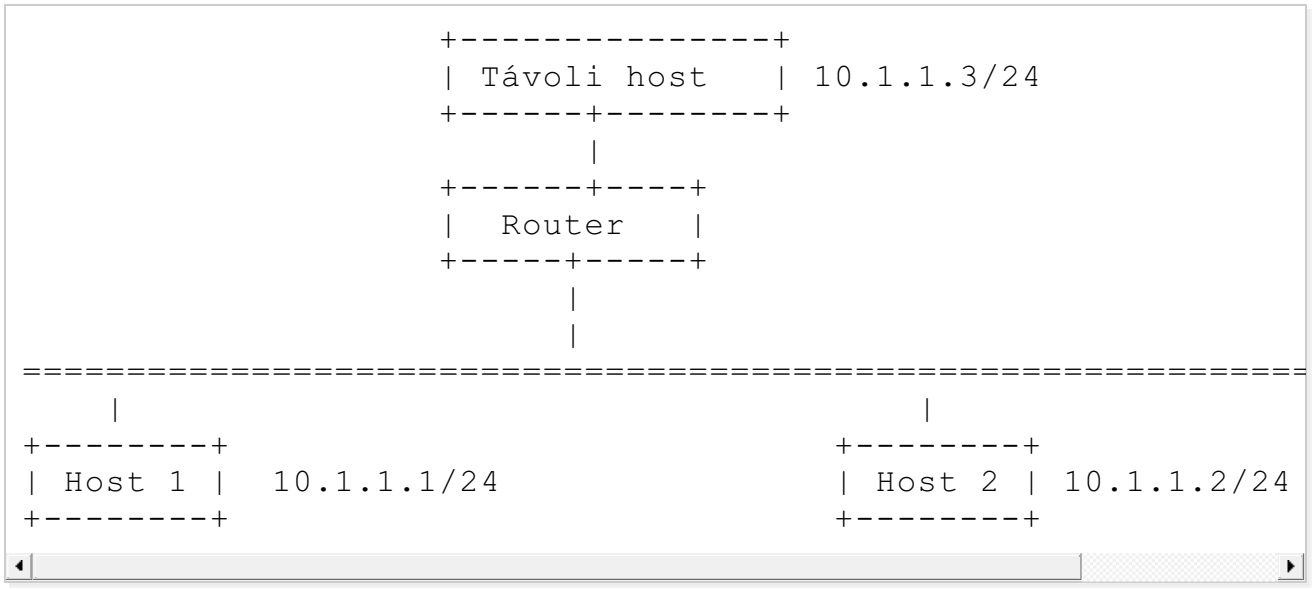
ARP kérés nem létező hostra

- A broadcast-ra nem jön válasz
- A kérdező timeout után újra próbálkozik
  - Implementáció függő
- Egy idő után feladja, értesíti a felsőbb réteget a hibáról
  - Implementáció függő

ARP cache

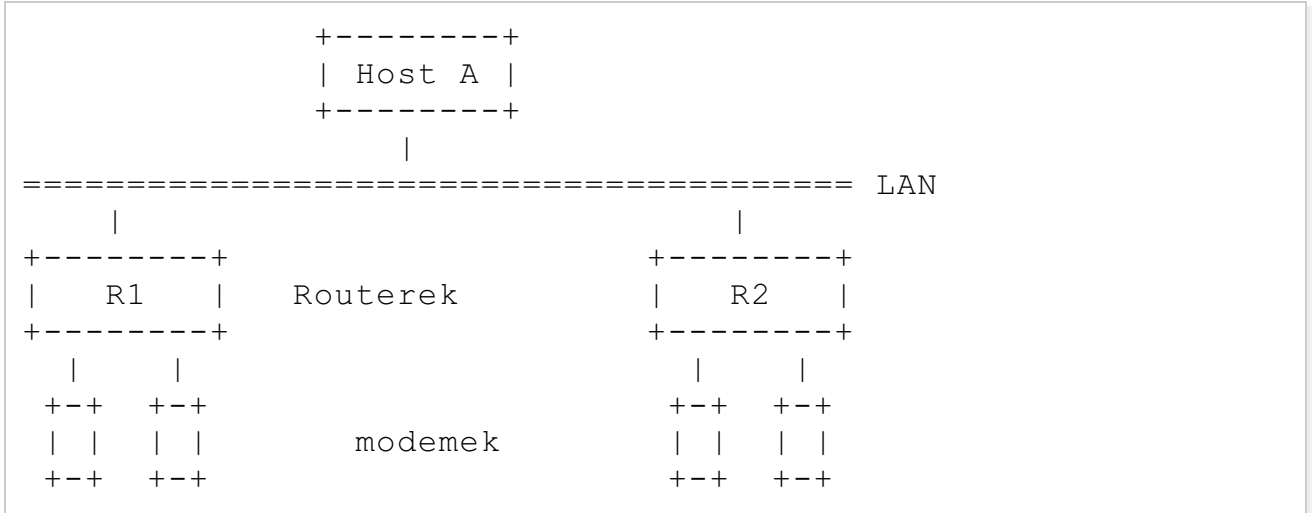
- A megtanult megfeleltetéseket az állomások megjegyzik
- Timeout: néhány perc
  - Implementáció függő
- Erővel is lehet ARP entryket betenni, kivenni
  - Unixokon arp parancs

Proxy ARP



- A router a távoli host-ot a LAN-on jelenlevőnek mutatja
- Válaszol a 10.1.1.3 IP címre érkező ARP kérésekre

UNARP



UNARP probléma

- Modemeken át jönnek állomások
  - Modemek helyett manapság VPN, Virtual Private Network végződések
- A LAN-on használt IP címekből használnak
- R1 és R2 proxy arp-t ad nekik
- Egyik pillanatról a másikra átkerülhetnek R1-ről R2-re
- Host A rossz ARP információt hihet !

UNARP megoldás

- **RFC1868**
- Ethernet ARP broadcast **reply**
- A source ethernet cím üres!
- A cache-ekből mindenki kiüríti az IP címhez tartozó ARP entry-t

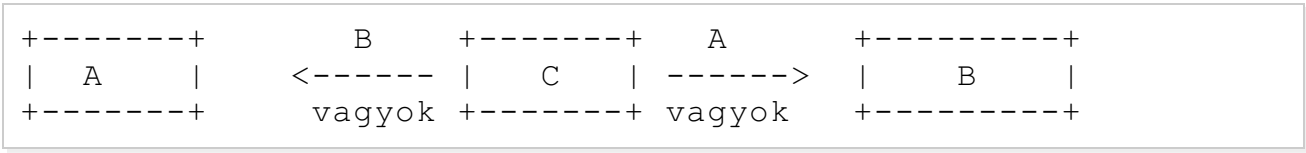
Gratuitous ARP

- A saját IP címemre adok ki ARP kérést
- Segít felfedezni, ha tévedésből többször osztották ki ugyanazt az IP címet
- Sokszor az operációs rendszerek ezzel kezdik az IP cím használatát
  - Nem veszik birtokba a címet, ha választ kapnak

ARP cache poisoning

- Egy rosszindulatú támadó hamis ARP adatokkal mérgezhet
- Elterelhet forgalmat
- Túlcsordíthat ARP cache-t: DoS (Denial of Service)
- WiFi növeli a veszélyét !
- Védekezés: ARP táblákat be lehet vasalni
  - Fáradságos lehet, de nagy biztonságot követelő helyeken szükséges
  - Szerver esetén, ahol a forgalom akár 100%-ban csak **egyetlen** router felé irányul, könnyű és célszerű lehet használni

Man in the Middle támadás ARP cache poisoninggal



ettercap

- ARP hamisításon alapuló eszköz
- Egy *broadcast domain*-on belül működik
- Switch-elt hálózaton hallgatózásra (snooping)
  - Úgy lehet hallgatózni, mint a régi jó busz topológiájú hálózaton
  - VLAN-ok - viszonylagos - védelmet jelentenek
- Man in the Middle támadás végrehajtására
- Grafikus felület
- A debian linux disztribució része
- Diagnosztikai, hibakeresési céllal jól használható
- „Script kiddie” támadásokra is alkalmas

Mi van, ha nem tudjuk a saját IP címünket?

RARP

- **RFC903**
- Külön ethernet frame type: `0x8035`
  - Lehetne ARP is
- Broadcast kérés
- A formátum megegyezik az ARP-vel
- A válaszban a címzett IP címe és ethernet címe
- A válasz már unicast

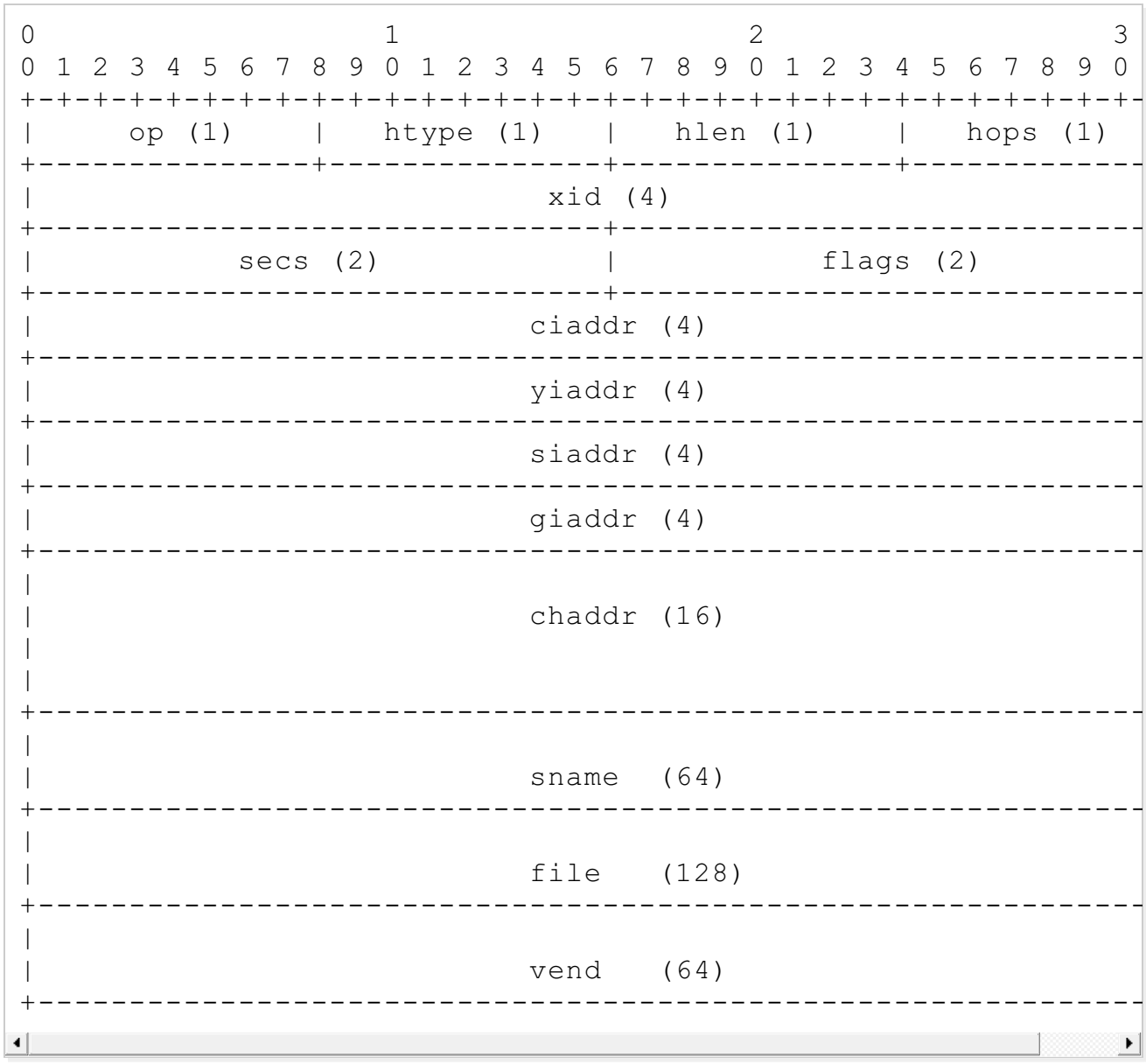
RARP hátrányok

- Csak egy puszta IP címet ad vissza (routert, netmaskot nem)
- Nem route-olható

BOOTP

- Kliens gépek automatikus konfigurálása, indítása
  - Pl. X terminálok, „vékony” kliensek
- **RFC951**, **RFC1542**
- IP címen kívül visszaad
  - Netmaskot
  - Router címet
  - Boot server host címet
  - Boot fájlnevet
  - …
- UDP csomagok
  - server port: `67` (bootps)
  - kliens port: `68` (bootpc)
- A kérés ethernet broadcast, a válasz rendszerint unicast
  - Lehet broadcast, ha a BOOTP flag-ben azt kérte a kliens
- Hogyan használhat a kliens UDP-t, amikor még IP címe sincs?
  - A `0.0.0.0` forrás címet használja (unspecified address)
  - A `255.255.255.255` cél címet használja (broadcast)

BOOTP csomagformátum



- opcode: 1 - request, 2 reply
- htype, hlen: mint arp-nél
- hop count: a kliens 0-ra állítja, proxy szerverek (= bootp-t közvetítő router-ek) eggyel növelik
  - A BOOTP route-olható, de gyakorlatban ritkán route-olják
- xid: tracnsaction id. Ezzel derül ki, hogy mi mire válasz
- secs: az első bootp kérés óta eltelt idő
  - Ha a kliens nem kap választ *exponential backoff* szerint újra próbálkozik
- flags: Itt kérheti a legfelső biten a kliens, hogy a BOOTP reply is broadcast legyen
- ciaddr: Client IP address. Kérésben a kliens kitöltheti: ezt kérem
- yiaddr: Your IP address. Ezt a címet kapja a kliens
- siaddr: Server IP address. A következő szerver IP címe, akivel a boot folytatható
- giaddr: Gateway IP address. Ha relé (bootp átengedésre konfigurált router) van, annak a címe
- chaddr: a kliens hardware (ethernet) címe - akkor van jelentősége, ha reléken át éri el a szervert a kliens
- sname: server host name
  - Annak a szervernek a neve, ahonnan majd az operációs rendszert letöltheted
- file: boot fájlnév
  - Az operációs rendszeredet tartalmazó fájl, amit le kell töltened
  - A fájl maga TFTP protokollal tölthető le

- vend: különböző kiegészítések (*vendor specific information*)
  - magic cookie: az első 4 byte
    - Elvben többféle szintaxis következhet, ezt határozza meg
    - A gyakorlatban mindig ugyanazt az értéket látjuk: (`0x63825363`)
  - tag kód, hossz, érték
  - Netmask
  - Router(ek) IP címe
    - Több is lehet
  - DNS szerver IP címe

DHCP

- Dynamic Host Configuration Protocol, **RFC2131**
- BOOTP kompatibilis
  - Portok, üzenet formátum megegyezik a BOOTP-vel, de bővül a lehetőségek köre
  - A ‚vend' helyett az ‚options' szó használatos
  - 312 byte hosszú lehet (64 volt)
  - DHCP ,,message type'' opció
- Rugalmasan lehet IP címeket kiosztani
  - Permanens IP cím - nem jár le
  - Dinamikusan - egy poolból véletlenszerűen, meghatározott időre
    - Egy IP cím/kliens/időintervallum együttes: **lease**
  - Manuálisan - ugyanaz a kliens mindig ugyanazt kapja
- Nem lehet DHCP-vel
  - DNS bejegyzést eszközölni
  - Egy routert konfigurálni
- Message types
  - DHCPDISCOVER
  - DHCPOFFER
  - DHCPREQUEST
  - DHCPACK
  - DHCPNAK
  - DHCPRELEASE
    - A kliens elengedi a lease-t (IP címet)
  - DHCPINFORM
    - A kliens csak konfigurációs paramétereket (opciókat) kér
  - DHCPDECLINE
    - A kliensnek mégse kell a cím, mert úgy tudja, hogy már használatos
- 4 lépcsős kezdeti handshake
  - DISCOVER (broadcast) →
  - OFFER ←
  - REQUEST →
  - ACK ←
- Lease-ek
  - A szerver az összes kiosztott lease-ről nyilvántartást vezet

Leases adatbázis részlet

```
lease 10.2.19.105 {
        starts 3 2004/10/13 11:07:41;
        ends 3 2004/10/13 23:07:41;
        hardware ethernet 00:0d:60:8d:49:34;
        uid 01:00:0d:60:8d:49:34;
        client-hostname "Pingvin";
}
lease 10.2.19.110 {
        starts 2 2004/10/12 13:12:05;
        ends 2 2004/10/12 13:14:05;
        hardware ethernet 00:11:92:fa:ee:00;
}
```

DHCP szerver konfiguráció fájl részlet

```
subnet 10.18.48.0 netmask 255.255.255.0{
  range 10.18.48.150 10.18.48.200;
  option subnet-mask 255.255.255.0;
  option broadcast-address 10.18.48.255;
  option domain-name-servers 193.224.194.225;
  option routers 10.18.48.254;
  option domain-name "sapientia.hu";
}


host eva {hardware ethernet 00:b0:d0:08:02:79; fixed-address 1
```

PXE - Preboot Execution Environment

- Az Intel szabvány, PC-k hálózati boot-olására
  - **http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf**
- DHCP-n és TFTP-n alapul
- DHCP kiegészítéseket tartalmaz
  - Pl: csak olyan DHCP szervertől fogad el a kliens választ, ami – az opcióban közölt – hardware architektúrájának megfelelő
- Szabványos user interfészről is szól
- Nem csak Intel hardware-en használható

Szerző: Pásztor Miklós, Máray Tamás