

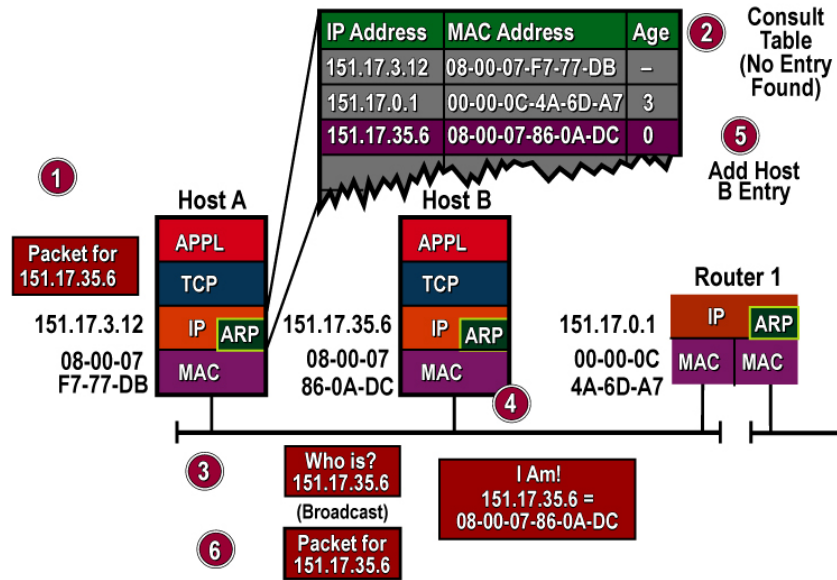
ARP és DHCP

*Médiakommunikációs hálózatok (VIHIM161)
2013. évi fóliái alapján készült*

Dr. Lencse Gábor
tudományos főmunkatárs
BME Hálózati Rendszerek és Szolgáltatások Tanszék
lencse@hit.bme.hu



- Address Resolution Protocol
- Dynamic Host Configuration Protocol



Forrás: http://www.hill2dot0.com/wiki/index.php?title=Image:G0314_Address-Resolution-Pr.jpg

ADDRESS RESOLUTION PROTOCOL

Az ARP helye és feladata

Alkalmazási	(7. Application)
Megjelenítési	(6. Presentation)
Viszonylati	(5. Session)
Szállítási	(4. Transport)
Hálózati	(3. Network)
Adatkapcsolati	(2. Data Link)
Fizikai	(1. Physical)

ISO OSI

Alkalmazási	(Application)
Szállítási	(Transport)
Hálózati	(Internet)
Hordozó- hálózat	(Link)

TCP/IP

- Feladata a hálózati rétegbeli cím alapján az adatkapcsolati rétegbeli cím kiderítése
- Mindkét rétegben többféle protokollal működik
- Számunkra fontos leképzés: IP-cím \Leftrightarrow MAC-cím

- *Teendők helyi és távoli hálózat esetén*
 - *Közvetlenül kapcsolódó (helyi) hálózat*
 - *A címzettnek közvetlenül küldeni*
 - ⇒ Ehhez a címzett adatkapcsolati rétegbeli címére van szükség
 - *Nem közvetlenül kapcsolódó (távoli hálózat)*
 - *A megtalált „következő csomópont” útválasztónak kell küldeni*
 - *Az IP-címet tilos módosítani*
 - *Csak adatkapcsolati rétegben kell az útválasztónak címezni*
 - ⇒ Ehhez szükség van az útválasztó adatkapcsolati címére
- **Megfigyelés: a leképzésre mindkét esetben a leképzést igénylővel szomszédos (vele azonos hálózatbeli) host vagy útválasztó címével kapcsolatban van szükség!**
- **Az IPv4 megoldása: ARP (IPv6-ban más megoldás van!)**

- Az információt igénylő eszköz az IP alatti rétegben (pl. Ethernet) üzenetszórással megszólít minden eszközt:
„Kinek az IP-címe az x.y.z.w?”
 - A kérdés tartalmazza a kérdező IP-címét és MAC-címét is.
- Az üzenetszórással küldött kérdést mindenki megkapja, és akihez a keresett IP-cím tartozik, az válaszol.
 - Mivel a választ adó ismeri a kérdező MAC-címét, a választ küldheti unicast címezéssel a kérdezőnek, ezt RFC 826 implicálja is, de az üzenetszórást sem tiltja meg.
- *Vegyük észre, hogy a kérdés-válasz után már mindkét fél birtokában van a másik félre vonatkozó IP-cím – MAC-cím összerendelési információnak!*

ARP adategységének felépítése

- Az ARP adategysége bizonyos mezőinek hossza a használt protokolloktól függ
 - Ha IPv4 címhez Ethernet MAC-címet szeretnénk kideríteni, akkor az ARP adategységének felépítése az alábbi:

0	8	16	31
Hardware Type (Ethernet: 1)		Protocol Type (IPv4: 0x0800)	
Hw. Addr. Length	Prot. Addr. Len.	Operation	
Sender Hardware Address (1-4 bytes)			
Sender Hardware Addr. (5-6 bytes)		Sender Protocol Addr. (1-2 bytes)	
Sender Protocol Addr. (3-4 bytes)		Target Hardware Address (1-2 bytes)	
Target Hardware Address (3-6 bytes)			
Target Protocol Address (1-4 bytes)			

- Ahol:
 - Hardware Address Length: 6
 - Protocol Address Length: 4

- „A” szeretné megtudni „B” MAC-címét (az IP-címe alapján)
- „A” Ethernet szinten a FF:FF:FF:FF:FF:FF (broadcast) célcímre küld egy *ARP Request*-et, a forráscím a sajátja, az EtherType mező értéke 0x0806.
- Az ARP Request (nem triviális) mezői:
 - Operation: ARP Request = 1
 - Sender HA: <„A” MAC-címe>
 - Megegyezik a keret fejrészében találhatóval
 - Sender PA: <„A” IP-címe>
 - Target HA: 00:00:00:00:00:00 (ismeretlen)
 - De a keret fejrészében a cél MAC-cím: FF:FF:FF:FF:FF:FF !!!
 - Target PA: <B IP-címe>
- Az ARP Request üzenetet a *broadcast domain* összes állomása veszi, és tárolja az „A” IP-cím – MAC-cím párosát az *ARP Cache* táblájában

- „B” felismeri a saját IP-címét az ARP Request üzenetben
- „B” Ethernet szinten az „A”-nak címezve küld egy *ARP Reply*-t, melyben a forráscím a sajátja, az EtherType mező értéke most is 0x0806.
- Az ARP Reply (nem triviális) mezői:
 - Operation: ARP Reply = 2
 - Sender HA: <„B” MAC-címe>
 - Megegyezik a keret fejrészében találhatóval
 - Sender PA: <„B” IP-címe>
 - Target HA: <„A” MAC-címe>
 - Megegyezik a keret fejrészében találhatóval
 - Target PA: <„A” IP-címe>
- „A” veszi a választ, és eltárolja „B” IP-cím – MAC-cím párosát

ARP Cache tábla kezelése

- Az állomások bizonyos ideig tárolják az ARP-vel megszerzett névfeloldási információkat.
- Mivel az *ARP Request* adatkapcsolati szinten broadcast címre kell küldeni, a küldő IP-cím – MAC-cím párosát minden állomás el tudja tárolni.
- Ha esetleg a választ is broadcast címre küldik, akkor azt is el lehet tárolni.
- A dinamikus bejegyzéseken kívül statikus bejegyzések is felvehetők (az `arp` menedzsment szoftverrel).
- Az ARP Cache tartalma általában az `arp -a` paranccsal meg is jeleníthető, az `arp -d` paranccsal pedig bejegyzések törölhetők belőle.

Az ARP Cache tábla felépítése – 1

- Címpárok: Adatkapcsolati rétegbeli és IP-címek
- Két bejegyzéstípus
 - Statikus
 - Manuálisan felvitt bejegyzés
 - Dinamikus
 - ARP címfeloldás eredménye
 - Gyorsítótár (cache) funkció: ne kelljen mindig lekérdezni
 - Egy idő után elévül és törlődik
- Elvi felépítése:

<i>IP-cím</i>	<i>HW-cím</i>	<i>típus</i>
<IP-cím1>	<MAC-cím1>	statikus
<IP-cím2>	<MAC-cím2>	dinamikus

- A gyakorlatban még egyéb információt is tárolnak, például:
 - a hardver típusát (ami Etherneten kívül más is lehet)
 - az interfészt, amelyiken keresztül az a hálózat elérhető, amelyen az adott szomszéd található.
- Például Linux alatt az ARP Cache táblát megvizsgálva:

```
root@dev:~# arp -n
```

Address	HWtype	HWaddress	Flags	Mask	Iface
193.224.130.161	ether	00:15:17:54:99:78	C		eth0

A **C** flag jelzi a cache-elt (dinamikus), az **M** pedig a manuálisan beállított (statikus) értékeket.

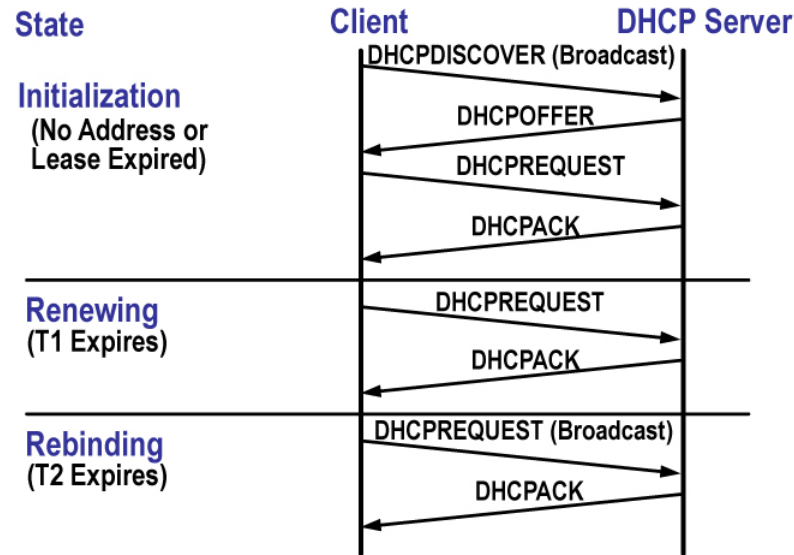
- RFC 5227: IPv4 Address Conflict Detection
- Mielőtt egy host elkezd egy IP-címet használni, meg kell (SHOULD) vizsgálnia, hogy nincs-e már használatban.
- Erre való az **ARP Probe** üzenet: ez egy speciális *ARP Request*, amellyel a használni kívánt IP-címre kérdez rá (target), de a küldő (sender) IP-címe mezőben csupa 0 található (nem szennyezi mások ARP Cache-ét)
- Ha az ARP Probe üzenetre választ kap, akkor tudja, hogy más valaki már használja a kérdéses IP-címet.
 - Ha DHCP-vel kapott IP-címről derül ki, hogy más valaki már használja, akkor kötelező (MUST) a DHCP szerver felé DHCPDECLINE üzenetet küldeni.

Címütközés vizsgálata – 2

- Az RFC 5227 nem rendelkezik róla konkrétan, hogy az ARP Probe üzenetet hányszor kell elküldeni, de megemlíti, hogy a megfelelően alacsony hibavalószínűség érdekében többször.
- Ha a cím szabadnak bizonyult, akkor a fentiek szerint eljáró host köteles (MUST) **ARP Announcement** üzenettel jelezni mindenki számára, hogy az adott IP-címet ő fogja használni.
- Ez olyan *ARP Request* típusú üzenet, ahol a sender és a target IP-cím mezőben egyaránt az adott IP-cím szerepel.
- Mivel broadcast címre küldik, mindenki megkapja, és az ARP Cache tábláját frissíteni tudja.

- Sajnálatos módon *ARP Probe* helyett bizonyos implementációkban *Gratuitious ARP* (kéretlen ARP) üzeneteket használnak
 - Így hívják mind az *ARP Request* nélkül, broadcast címre küldött *ARP Reply* üzeneteket, mind az *ARP Probe* nélkül küldött *ARP Announcement* üzeneteket
- Ez a módszer azért nem jó, mert:
 - Nem óvja meg a már működő gépek működőképességét
 - Nem teszi lehetővé a most induló gépnél sem azt, hogy automatikusan (emberi beavatkozás nélkül) más IP-címet használjon

- Adatkapcsolati rétegbeli címből IP-címet (RFC 903)
- Felhasználási terület
 - Hálózatmenedzsment
 - Permanens tár nélküli eszközök
 - Semmi ismeretük sincs a hálózatról
 - Hálózatról töltődik be az operációs rendszer
 - IP-cím nélküli kezdeti kommunikáció
- RARP kiszolgálók
 - RARP broadcast üzenetekre válaszolnak
- RARP helyett sokkal elterjedtebb megoldások
 - Előbb BOOTP: IP-cím kérésére és hálózatról történő betöltésre
 - A fejlettebb DHCP miatt már nem igazán használatos
 - Ma DHCP: IP-cím és hálózati információk kérésére



Forrás: <http://wiki.hill.com/wiki/index.php?title=Image:DHCP.jpg>

DYNAMIC HOST CONFIGURATION PROTOCOL

A DHCP helye és feladata

Alkalmazási	(7. Application)
Megjelenítési	(6. Presentation)
Viszonylati	(5. Session)
Szállítási	(4. Transport)
Hálózati	(3. Network)
Adatkapcsolati	(2. Data Link)
Fizikai	(1. Physical)

ISO OSI

Alkalmazási	(Application)
Szállítási	(Transport)
Hálózati	(Internet)
Hordozó-hálózat	(Link)

TCP/IP

- Segítségével a hostok automatikusan juthatnak hozzá a kommunikációjukhoz szükséges hálózati azonosítókhoz: IP-cím, hálózati maszk, alapértelmezett átjáró, stb.
- Eredetileg az RFC 1531 a BOOTP kiterjesztéseként definiálta. Újabb RFC-k: 1541, 2131 (aktuális)

- IP-címek osztása MAC-cím alapján DHCP szerverrel
 - Szükség esetén (a DHCP szerveren előre beállított módon) egyes kliensek számára azok MAC-címéhez fix IP-cím rendelhető
- IP-címek osztása dinamikusan
 - A DHCP szerveren beállított tartományból „érkezési sorrendben” kapják a kliensek az IP-címeket
 - Elegendő annyi IP-cím, ahány gép egyidejűleg működik
- Az IP-címeken kívül további szükséges hálózati paraméterek is kioszthatók
 - Hálózati maszk
 - Alapértelmezett átjáró
 - Névkiszolgáló
 - Domain név
 - Hálózati rendszerbetöltéshez szerver és fájlnev

A címek bérlésének szabályai

- A DHCP szerver a klienseknek az IP-címeket bizonyos *bérleti időtartamra* (lease time) adja „bérbe”
 - Az időtartam hosszánál a szerver figyelembe veszi a kliens esetleges ilyen irányú kérését
 - Az időtartam hosszát a szerver beállításai korlátozzák
- A bérleti időtartam lejárta előtt a bérlet meghosszabbítható
- Az IP-cím explicit módon vissza is adható

A DHCP kommunikációja

- A kliens és a szerver *DHCP* üzenetekkel kommunikálnak
- A DHCP üzenetek BOOTP üzenetekben opcióként jelennek meg
- A BOOTP üzenetek IP fölött, UDP-be ágyazva haladnak
 - Amíg a kliensnek nincs érvényes IP-címe, addig 0.0.0.0-t használ
 - Broadcast esetén IP szinten természetesen 255.255.255.255 címre küldi az üzenetet (Ethernet szinten pedig FF:FF:FF:FF:FF:FF-re)
 - UDP-ben a kliens portszáma: 68, a szerveré: 67
- A továbbiakban a DHCP üzenetek neve mellett feltüntetjük, hogy ki küldi kinek: „küldő → címzett” formában. Jelölések:
 - K: kliens
 - S: szerver
 - B: broadcast (IP és Ethernet szinten is)
 - K/B: magyarázat a következő fólián!

- Amikor egy DHCP szerver válaszol egy kliens üzenetére
 - A kliens MAC-címét ismeri, címezheti neki.
 - Sőt, a gyakorlatban már IP szinten is a kliensnek címzi, annak ellenére, hogy a kliensnek még érvénytelen (azaz 0.0.0.0) az IP-címe (lásd: RFC 2131, 24. oldal, 1-5. sor)
 - Azonban nem minden operációs rendszer képes arra, hogy egy érvénytelen IP címmel rendelkező hálózati interfész MAC szinten neki címzett unicast forgalmat fogadjon.
 - Például a Linux képes rá, a Windows 7 esetén beállításfüggő.
 - Broadcastot azonban ilyenkor is képes venni.
 - Ezért a kliens a kérésében jelzi, hogy unicast vagy broadcast választ vár.
 - Ezt az információt a DHCP üzenetet opcióként szállító BOOTP üzenetben egy jelzőbit (flags mezőben *broadcast* bit) hordozza.
 - A hálózat szempontjából a unicast előnyösebb, mert nem terheli a többi eszközt, tehát ha a kliens alkalmas rá, akkor a szerver azt használja.

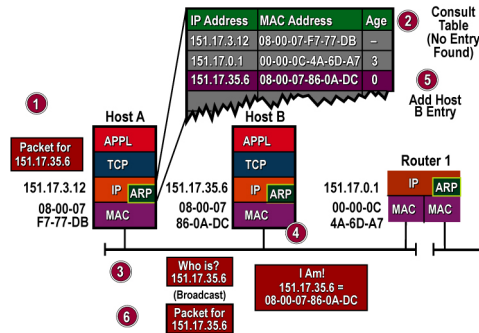
- **DHCPDISCOVER K→B**
 - Egy kliens küldi broadcast címre, hogy feltérképezze az elérhető DHCP szervereket és ajánlataikat
 - A kliens opcionálisan (nem az IP fejrészben, hanem DHCP opcióként) megadhatja a legutoljára használt IP-címét, de ez NEM azonos a bérlet meghosszabbításával!
- **DHCPOFFER S→K/B**
 - Egy DHCPDISCOVER üzenetre egy vagy több szerver válaszol, megadja milyen IP-címet és paramétereket tud kínálni.
 - Ekkor még ezek a kliens számára NEM használhatók!
- **DHCPREQUEST K→B**
 - A kliens ezzel az üzenettel egyidejűleg elfogadja valamely szerver ajánlatát, és implicit módon elutasítja a többiekét (broadcast miatt minden szerverhez eljut)
 - A kliens megjelölheti benne a kért bérleti időtartamot is.

- DHCPACK S→K/B
 - A szerver ekkor megerősíti a kliensnek az IP-cím bérletét és megadja, hogy milyen időtartamra kapja meg a kliens.
 - A kliens utána a bérleti idő lejártáig használhatja az IP-címet, de a címütközés elkerülése érdekében erősen ajánlott (SHOULD) *ARP Probe* segítségével ellenőriznie, hogy más nem használja-e.
 - Ha más nem használja, *ARP Announcement*tel kihirdeti
 - Ha más használja, *DHCPDECLINE*-nal jelzi a DHCP szervernek, és természetesen másik IP-címet kér.
- DHCPNAK S→K
 - Ezzel az üzenettel jelzi a szerver, hogy a kliens kérése nem teljesíthető.
- DHCPDECLINE K→S
 - A kliens jelzi a szervernek, hogy az adott IP-címet már más használja.

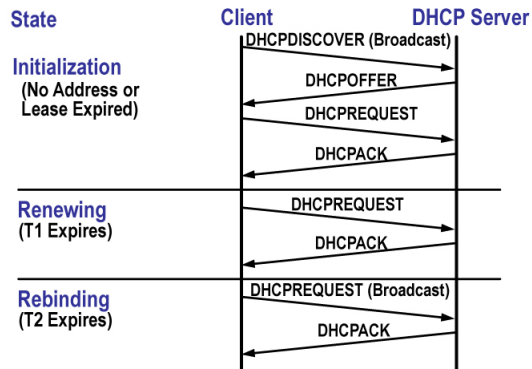
- A bérleti idő lejártán belül a kliens hosszabbítást kérhet, ekkor nem kell az egész folyamatot lejátszania, elegendő:
- DHCPREQUEST K→S
 - Az üzenet küldésekor a kliens még használja az érvényesen bérelt IP-címét és a kérést nem broadcast címre, hanem a szervernek küldi.
- DHCPACK S→K
 - A szerver ekkor meghosszabbítja kliensnek az IP-cím bérletét és megadja, hogy milyen időtartamra kapja meg a kliens.
 - Természetesen ilyenkor a kliensnek nem kell további ellenőrzést végeznie
- DHCPNAK S→K
 - Ezzel az üzenettel jelzi a szerver, hogy a kliens kérése nem teljesíthető.

- A bérleti idő lejártán belül a kliens korábban is visszaadhatja az IP-címet:
- DHCPRELEASE K→S
 - Ezzel a kliens lemond a hátralevő bérleti időről, a szerver újra kioszthatja a címet.
- Amennyiben egy kliensnek már van IP-címe (például statikusan be van állítva), akkor is kérhet más paramétereket:
- DHCPINFORM K→S
 - Ezt a kliens a szervernek unicast üzenetként küldi
 - Válaszul a szerver ugyanígy unicastként küldi egy DHCPACK üzenetben a további hálózati beállításokat
 - Ilyenkor a szerver nem ellenőrzi, hogy a kliens rendelkezik-e érvényes IP-cím bérlettel.

- Address Resolution Protocol

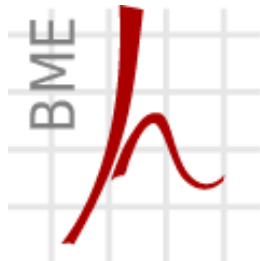


- Dynamic Host Configuration Protocol



Kérdések?

KÖSZÖNÖM A FIGYELMET!



Hálózati Rendszerek és
Szolgáltatások Tanszék

Dr. Lencse Gábor
tudományos főmunkatárs
BME Hálózati Rendszerek és Szolgáltatások Tanszék
lencse@hit.bme.hu

