Tokaj-Hegyalja Egyetem

Hálózati Architektúrák és Protokollok

7. Hálózati réteg - Az IP-címzés és a mai internet működése

Mileff Péter - Miskolci Egyetem

Az IP-címzés és a mai internet működése

- A modern számítógépes hálózatok egyik legfontosabb jellemzője, hogy nem elszigetelten működnek,
  - hanem egymással összekapcsolva alkotnak egy globális rendszert.
- Az internet valójában hálózatok hálózata, amely különböző technológiájú és méretű részrendszerekből épül fel.
- Az egyes helyi hálózatok (LAN-ok) önmagukban képesek biztosítani az eszközök közötti kommunikációt,
  - azonban a különböző hálózatok közötti adatátvitelhez egységes címzési és továbbítási mechanizmusra van szükség.
- Ezt a feladatot az **Internet Protocol**, azaz az **IP** látja el.

Az Internet Protocol szerepe

- Az Internet Protocol a hálózati réteg legfontosabb protokollja
- Biztosítja az adatok továbbítását különböző hálózatok között.
- **Az IP kapcsolatmentes, datagram alapú szolgáltatást nyújt**, amelynek során az adatcsomagok egymástól függetlenül kerülnek továbbításra.
- Az IP nem garantálja:
  - a csomagok sorrendhelyes érkezését
  - a csomagok kézbesítését
  - a csomagok duplikációjának elkerülését
- Ezeket a feladatokat a felsőbb rétegek, például a szállítási réteg protokolljai (pl. TCP) biztosítják.

Az IP cím

- **Az IP-cím egy logikai azonosító, amely egyedileg azonosít egy hálózatra csatlakozó eszközt**
- Az IP-cím lehetővé teszi, hogy az adatcsomagok megtalálják a célállomást még akkor is, ha az több hálózaton keresztül érhető el.
- Az IP-címek hierarchikus felépítésűek, ami azt jelenti, hogy két fő részből állnak:
  - hálózati azonosító
  - hoszt azonosító
- A hálózati rész az adott hálózatot azonosítja, míg a hoszt rész az adott hálózaton belüli eszközt.

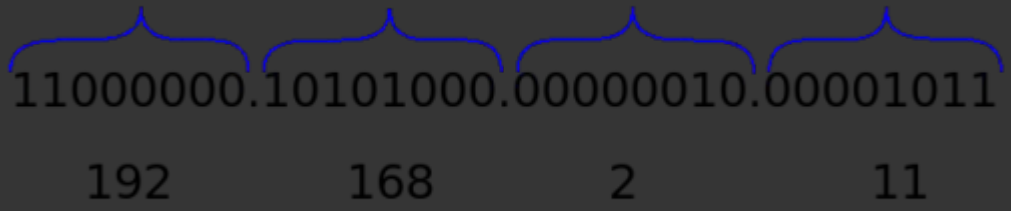
Az IPv4 címzés...

Az IPv4 cím

- Az IPv4 a legelterjedtebb IP-verzió, amely **32 bites** címeket használ
- Ez azt jelenti, hogy összesen 232, azaz körülbelül 4,3 milliárd egyedi cím áll rendelkezésre
- Az IPv4 címeket általában **négy darab 8 bites egység**ként, úgynevezett oktettek formájában írjuk fel, pontokkal elválasztva.
- Egy IPv4-datagram egy fejrészből és egy törzsrészből vagy hasznos részből áll
- A fejrésznek van egy 20 bájtos rögzített része és egy változó hosszúságú opcionális része.

Az IPv4 cím

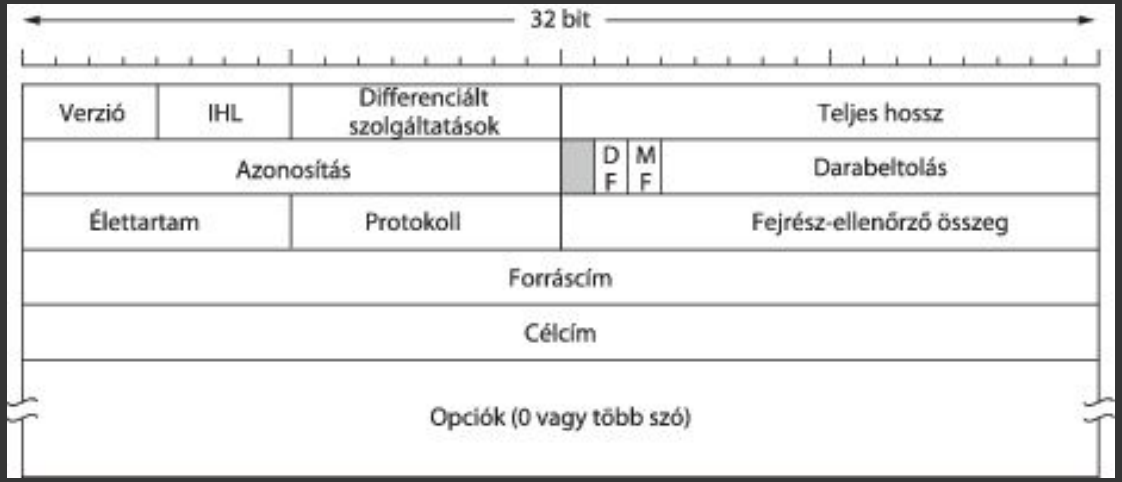
Decimális alakban jobban szeretjük



Minden bájt egy 0 és 255 közzé eső szám

Az IPv4 cím

- A bitek balról jobbra, fentről lefele kerülnek továbbításra, a Verzió mező legmagasabb helyi értékű bitje megy elsőnek.



Az IPv4 cím

- Az IPv4 a legelterjedtebb IP-verzió, amely **32 bites** címeket használ
- Ez azt jelenti, hogy összesen 232, azaz körülbelül 4,3 milliárd egyedi cím áll rendelkezésre
- Az IPv4 címeket általában **négy darab 8 bites egység**ként, úgynevezett oktettek formájában írjuk fel, pontokkal elválasztva.
- Egy IPv4-datagram egy fejrészből és egy törzsrészből vagy hasznos részből áll
- A fejrésznek van egy 20 bájtos rögzített része és egy változó hosszúságú opcionális része.

Az IPv4 cím

- A **Verzió** mező azt tartja nyilván, hogy a datagram a protokoll melyik verziójához tartozik
  - Jelenleg a 4-es változat uralkodó az interneten
- Azáltal, hogy a verziót minden datagram elején megadják, a verziók közti átmenet évekig is eltarthat
- Az IP következő változata, az IPv6, több mint tíz évvel ezelőtt jelent meg, de a bevezetése még mindig csak az elején tart
- **A fejrész hossza nem állandó:** a fejrész egyik mezője, az **IHL** szolgál arra, hogy 32 bites szavakban megadja a fejrész hosszát
- A legkisebb érték 5, ebben az esetben semmilyen opció nem szerepel
- Ennek a 4 bites mezőnek a maximális értéke 15, amely a fejrészt 60 bájtra, ennélfogva az Opciók mezőt 40 bájtra korlátozza
- Néhány opcióhoz, mint például ahhoz, amelyik a csomag által megtett utat jegyzi fel, a 40 bájt túl kicsi, ezáltal az opció értelmét veszti

Az IPv4 cím

- A **Differenciált szolgáltatások** mező az egyik azok közül a mezők közül, amelyek jelentése megváltozott az évek során
- Eredeti neve **Szolgáltatás típusa** volt.
- **Célja:** különbséget tegyen az eltérő szolgáltatási osztályok között
- A megbízhatóságnak és a sebességnek számos kombinációja képzelhető el
  - Pl. a digitalizált hangnál a gyors kézbesítés fontosabb, mint a pontosság
- A Szolgáltatás típusa mező 3 bitet biztosított a prioritás jelzéséhez
  - és 3 bitet annak jelzéséhez, hogy a hoszt megmondja, mi számára a legfontosabb:
    - a késleltetés,
    - az átbocsátóképesség
    - vagy a megbízhatóság.

Az IPv4 cím

- A **Teljes hossz**ba (Total length) a datagram minden része beleértendő, a fejrész is és az adatrész is.
- A maximális hossz 65 535 bájt
- Jelenleg ez a felső korlát még elegendő, de a jövőbeni gigabites hálózatoknál nagyobb datagramokra lehet majd szükség
- Az **Azonosítás** (Identification) mező a daraboláskor szükséges ahhoz, hogy a címzett hoszt eldönthesse, melyik datagramhoz tartozik az újonnan érkezett darab
- Egy datagram minden darabja ugyanazt az Azonosítás értéket tartalmazza.
- A következő egy **kihasználatlan bit**
    - meglepő, mivel a rendelkezésre álló hely az IP-fejrészben meglehetősen kevés.

Az IPv4 cím

- Majd **két 1 bites mező** következik, amely a darabolással kapcsolatos
- A **DF jelentése:** Ne darabold (Don’t Fragment).
- Ez az útválasztóknak szóló parancs, hogy ne darabolják fel a csomagot.
- Eredetileg az volt a célja, hogy támogassa azokat a hosztokat, amelyek nem tudják újra összerakni a darabokat.
- Jelenleg ezt az útvonal MTU-jának felderítésére szolgáló folyamat részeként alkalmazzák.
- **Az MTU a legnagyobb csomag, amely az útvonal mentén darabolás nélkül átküldhető**.
- Ha a datagram DF bittel van megjelölve, akkor az adó tudja, hogy egy darabban fog megérkezni, ellenkező esetben az adó hibaüzenetet kap vissza.

Az IPv4 cím

- **Az MF jelentése:** több darab (More Fragments).
  - Ezt a bitet minden darabban be kell állítani, kivéve az utolsóban.
  - Ez azért szükséges, hogy tudjuk, vajon egy datagram minden darabja megérkezett-e.
- A **Darabeltolás mező** megmondja, hova tartozik a mostani darab a datagramban
- Egy datagram minden darabjának – kivéve az utolsót – 8 bájt többszörösének kell lennie, mert ez az elemi darabméret.
- Mivel 13 bit áll rendelkezésre, ez legfeljebb 8192 darabot jelent datagramonként
  - amely 65 536 bájtos maximális datagramhosszt eredményez, eggyel nagyobbat, mint amit a Teljes hossz mező lehetővé tesz.
- Az Azonosítás, MF és Darabeltolás mező együtt valósítja meg a darabolást

Az IPv4 cím

- Az **Élettartam mező** egy számláló, amelyet a csomag élettartamának korlátozására használnak
- Elvileg az időt mérné másodpercekben, így maximálisan 255 másodperc hosszú életet tenne lehetővé.
- Minden ugrásnál csökkenteni kell, és ha egy csomag hosszú ideig állt sorban egy útválasztóban, akkor elvileg többször is csökkenteni kellene.
- **Gyakorlatilag csak az ugrásokat számolja:** amikor eléri a nullát, a csomagot el kell dobni, és egy figyelmeztető csomagot kell visszaküldeni a forráshoszthoz.
- Ez a tulajdonság megelőzi, hogy a datagramok a végtelenségig kóboroljanak,
    - ami egyébként megtörténhetne, ha az útválasztó táblázatokba valamikor hiba csúszna

Az IPv4 cím

- Amikor a vételi oldalon a hálózati réteg összeállított egy teljes datagramot, tudnia kell, mit tegyen vele.
- A **Protokoll mező** mondja meg, melyik szállítási folyamatnak adja át
- Lehetséges a TCP, de az UDP és pár másik protokoll is
- A protokollok számozása az interneten egységes.
- A protokollok számozását és a többi számkiosztást az RFC 1700 tartalmazta
- Ma már egy online adatbázisban találhatók: **www.iana.org**

Az IPv4 cím

- Mivel a fejrész lényeges információt hordoz, a védelem érdekében kiszámítja a saját ellenőrző összegét,
  - **Fejrész-ellenőrző összeg** (Header Checksum).
- **Az algoritmus:**
  - egyes komplemens aritmetikával az érkezés sorrendjében összeadjuk a 16 bites félszavakat, és vesszük az eredmény egyes komplemensét
  - Az algoritmus alapján a Fejrész-ellenőrző összeget a csomag érkezésekor nullának várjuk
  - Az ilyen ellenőrző összeg a csomag hálózaton való átküldése során fellépő hibák észleléséhez hasznos
  - Ne feledjük el, hogy ezt minden ugrásnál újra kell számítani, mivel legalább egy mező (az **Élettartam mező**) mindig változik,
    - de alkalmazhatók trükkök a számítás felgyorsítására

Az IPv4 cím

- A **Forráscím** és **Célcím** mutatja a forrás és a cél hálózati interfészének az IP-címét
- Az **Opciók mező** egy menekülési útvonal: arra terveztek, hogy a protokoll következő verzióinak lehetőségük legyen olyan információt belevenni a protokollba, amelyek az eredeti tervben nem szerepeltek,
  - kísérletezhessenek új ötletek kipróbálásával,
  - és hogy ne kelljen olyan információ számára is fejrészbiteket lefoglalni, amelyekre csak ritkán van szükség.
- Az opciók változó hosszúságúak
- Mindegyik az opciót azonosító egybájtos kóddal kezdődik
- Néhány opciónál ezt egy egybájtos hosszmező követi, majd egy vagy több adatbájt. Az Opciók mezőt négy bájt többszörösére töltik ki
- Eredetileg öt opció létezett

Az IPv4 cím

Opció	Leírás
Biztonság	Meghatározza, mennyire titkos a datagram
Szigorú forrás általi útválasztás	Megadja a teljes követendő utat
Laza forrás általi útválasztás	Felsorolja a felkeresendő útválasztókat
Útvonal feljegyzése	Felszólítás, hogy minden útválasztó fűzze hozzá az IP-címét
Időbélyeg	Felszólítás, hogy minden útválasztó fűzze hozzá az IP-címét és az időbélyegét

Az IPv4 cím

- A **Biztonság opció** azt mondja meg, milyen titkos az információ.
- Elméletben egy katonai útválasztó használhatná ezt a mezőt arra, hogy ne irányítson bizonyos, a katonaság szempontjából „rosszfiúnak” minősülő országokon keresztül.
- A gyakorlatban minden útválasztó figyelmen kívül hagyja
    - így az egyetlen gyakorlati funkciója az, hogy a kémek könnyebben megtalálhassák a jó dolgokat.
- A **Szigorú forrás** általi útválasztás opció IP-címek sorozataként megadja a teljes utat a forrástól a célig
- A datagramnak pontosan ezt az utat kell követnie.
- Ez nagyon hasznos rendszermenedzserek számára
    - hogy vészcsomagokat küldjenek az útválasztó táblák meghibásodása esetén, vagy időzítési méréseket végezzenek

Az IPv4 cím

- A **Laza forrás** általi útválasztás opció megköveteli a csomagtól:
  - hogy a megadott útválasztókon, a megadott sorrendben áthaladjon,
  - de útközben áthaladhat más útválasztókon is.
- Rendesen ez az opció csak egy pár útválasztót bocsát rendelkezésre, hogy egy bizonyos utat kényszerítsen ki
- Például, hogy egy Londonból Sydneybe tartó csomagot kelet helyett nyugat felé kényszerítsünk, ez az opció például megadhat New York-i, Los Angeles-i és honolului útválasztókat.
- Ez az opció nagyon hasznos, ha politikai vagy gazdasági megfontolásokból keresztül kell haladni bizonyos országokon, vagy el kell kerülni azokat

Az IPv4 cím

- Az **Útvonal feljegyzése** opció arra utasítja az útba ejtett útválasztókat, hogy az IP-címüket fűzzék hozzá az Opciók mezőhöz.
- Ez lehetővé teszi a rendszermenedzsereknek, hogy kinyomozzák a hibákat az útválasztó algoritmusokban.
- Amikor az ARPANET először létrejött, egyik csomag sem érintett kilenc útválasztónál többet,
  - így az opció 40 bájtja bőségesen elegendő volt. Most már túl kicsi.
- **Időbélyeg opció** olyan, mint az Útvonal feljegyzése opció, kivéve, hogy minden útválasztó a 32 bites IP-címe mellé egy 32 bites időbélyeget is feljegyez.
- Ez az opció is főleg az útválasztó algoritmusok hibakereséséhez való.
- Az IP-opciókat ma már nem részesítik előnyben. Számos útválasztó figyelmen kívül hagyja, vagy nem dolgozza fel azokat hatékonyan,

Előtagok

- **Az IP-címek, az Ethernet-címekkel ellentétben, hierarchikusak**
- Minden 32 bites cím változó hosszúságú hálózati részből (felső bitek) és hosztrészből áll (alsó bitek).
- A hálózati rész értéke az egy hálózaton – például Ethernet LAN-on – lévő összes hoszt esetén megegyezik.
- Ez azt jelenti, hogy a hálózat az IP-címtér folyamatos blokkjának felel meg. Ezt a blokkot **előtag**nak (prefix) hívjuk
- Az IP-címeket rendszerint pontokkal elválasztott decimális jelölésrendszerben (dotted decimal notation) írják.
- Ebben a formátumban minden 4 bájtot tízes számrendszerben írnak ki, 0-tól 255-ig
    - Pl. a 80D00297 32 bites hexadecimális cím decimális formája a következő: 128.208.2.151.

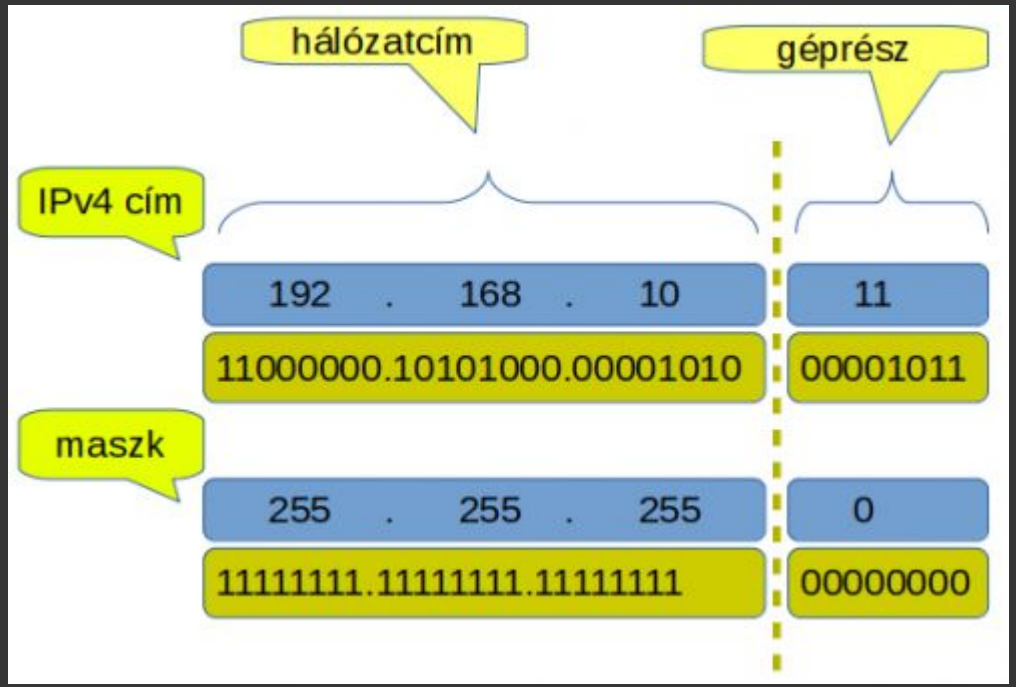
Előtagok

- Az előtagok megadják a legkisebb IP-címet a blokkban, illetve a blokk méretét
- A méretet a hálózati részben lévő bitek száma határozza meg
- A bitek a hosztrészben változhatnak:
  - Ez azt jelenti, hogy a méretnek kettő hatványnak kell lennie.
- Megegyezés szerint az előtag IP-címe egy perjellel van kiegészítve, és ezt követi a hálózati rész bitjeinek száma.
- Ha az előtag a példánkban 28 címet tartalmaz és 24 bit marad a hálózati részre, akkor a következőképpen fest: 128.208.0.0/24.

Előtagok

- Mivel az előtag hossza nem következtethető ki magából az IP-címből, az útválasztó protokolloknak át kell adniuk az előtagokat az útválasztóknak
- Bizonyos esetekben az előtagokat egyszerűen a hosszuk írja le,
  - mint a „/16” esetében (amelyet „per 16”-nak mondanak)
- Az előtag hossza megfelel az 1-esek bináris maszkjának a hálózati részben.
- Az ilyen írásmódot **alhálózati maszknak (subnet mask)** hívják.
- Ha ezt ÉS kapcsolatba hozzuk az IP-címmel, megkapjuk a hálózati részt.
- A példánkban az alhálózati maszk a 255.255.252.0.

IPv4 és subnet mask



Alhálózatok

- A hálózatszámokat az **ICANN** (**Internet Corporation for Assigned Names and Numbers**) nevű nonprofit intézmény kezeli a konfliktusok elkerülése végett
- Az ICANN különböző regionális hatóságokra bízta a címtér egy részét, hogy azok osszák ki az IP-címeket az ISP-nek és más vállalatoknak.
- Ez az a folyamat, amellyel egy vállalat IP-cím blokkot foglalhat le
- **Az alhálózatra osztás (subnetting):** az a folyamat, amely során egy nagyobb IP-hálózatot több kisebb, logikailag elkülönített alhálózatra bontunk
  - lehetővé teszi a hálózati erőforrások hatékonyabb kihasználását, valamint a hálózat jobb szervezését és kezelhetőségét
  - az alhálózatok létrehozása során a hoszt rész egy részét „kölcsönvesszük”, és azt hálózati azonosításra használjuk

Alhálózatok

- **Miért van szükség subnetelésre?**
  - csökkenti a broadcast forgalmat
  - javítja a hálózat teljesítményét
  - növeli a biztonságot (szegmentálás)
  - hatékonyabb címkiosztást tesz lehetővé
  - megkönnyíti a hálózat menedzselését

Példa

Vegyünk egy klasszikus hálózatot. IP-cím: **192.168.1.0/24**

- Ez azt jelenti:
  - 24 bit a hálózati rész
  - 8 bit a hoszt rész
  - Hosztok száma: **2^8=256 cím**
- Ebből:
  - 1 hálózati cím
  - 1 broadcast cím
  - Felhasználható:

256 − 2 = 254 hoszt

Példa - subnet felépítése

Tegyük fel, hogy ezt a hálózatot 4 alhálózatra szeretnénk bontani:

- Ehhez:
  - 2 bitet „kölcsönveszünk” a hoszt részből
  - Új prefix: **/26**

Ez azt jelenti:

  - 6 bit marad hosztnak
  - 2 bit alhálózati azonosító

Példa - subnet felépítése

Alhálózatok száma: **2^2=4 alhálózat**

Hosztok száma alhálózatonként

2^6 = 64 cím

Felhasználható:

64−2=62 hoszt

A 192.168.1.0/24 hálózat felosztása /26-ra:

- 192.168.1.0 – 192.168.1.63
- 192.168.1.64 – 192.168.1.127
- 192.168.1.128 – 192.168.1.191
- 192.168.1.192 – 192.168.1.255

Példa - subnet felépítése

Egy alhálózat részletesen

- Hálózati cím: 192.168.1.0
- Első hoszt: 192.168.1.1
- Utolsó hoszt: 192.168.1.62
- Broadcast: 192.168.1.63

Subnet mask

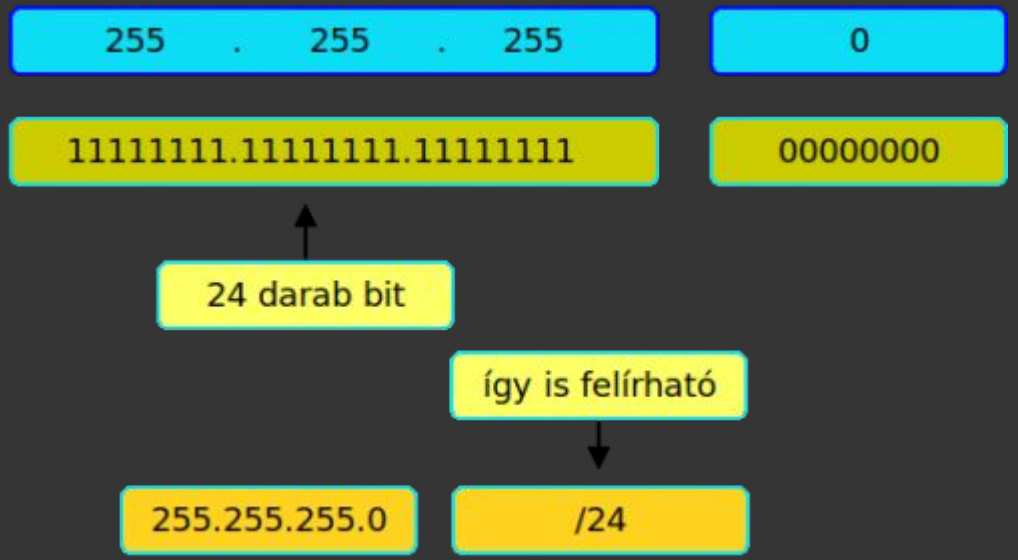
- A /26 maszk: **255.255.255.192**
- Binárisan: **11111111.11111111.11111111.11000000**

A subnetelés valójában bitművelet:

- a bal oldali bitek → hálózat
- a középső bitek → alhálózat
- a jobb oldali bitek → hoszt

Előtagok

- Ha van egy 255.255.255.0 maszkunk, az CIDR formában: /24. A 255.255.0.0 CIDR formában: /16. A 255.0.0.0 CIDR formája /8



Előtagok

Egy hálózatban lehetséges címek /24 maszk esetén

Hálózatcím	10.1.1.0/24	10.1.1.00000000
első gép cím	10.1.1.1	10.1.1.00000001
utolsó gép cím	10.1.1.254	10.1.1.11111110
szórászcím	10.1.1.255	10.1.1.11111111

Gépek száma: 2^8-2 = 254 gép

Előtagok

Egy hálózatban lehetséges címek /25 maszk esetén

Hálózatcím	10.1.1.0/25	10.1.1.00000000
első gép cím	10.1.1.1	10.1.1.00000001
utolsó gép cím	10.1.1.126	10.1.1.01111110
szóráscím	10.1.1.127	10.1.1.01111111

Gépek száma: $2^7-2 = 126$ gép

Előtagok

- A hierarchikus címeknek számos előnye és hátránya van
- Az előtagok fő előnye az, hogy az útválasztók a csomagokat továbbítani tudják a cím hálózati része alapján
  - amíg minden hálózat egyedi címblokkal rendelkezik
- A hosztrész az útválasztók számára érdektelen, mivel az egy hálózaton lévő összes hoszt csomagját ugyanabba az irányba kell küldeni.
- Csak akkor kell a megfelelő hoszthoz továbbítani a csomagokat, amikor azok elérik a célhálózatot
  - Ezáltal kisebbek lesznek az útválasztó táblák, mint egyébként lennének
- Képzeljük el, hogy a hosztok száma az interneten eléri az egymilliárdot. Így nagyon nagy táblázatot kellene minden útválasztónak fenntartania
- A hierarchia alkalmazásával azonban az útválasztóknak csak körülbelül 300 000 előtagot kell fenntartaniuk a táblázatban

Előtagok

- **A hierarchia használatával lehetővé válik az internet útválasztásának skálázása**
  - amelynek két hátránya is van

1. A hoszt IP-címe a hálózaton belüli helyétől függ

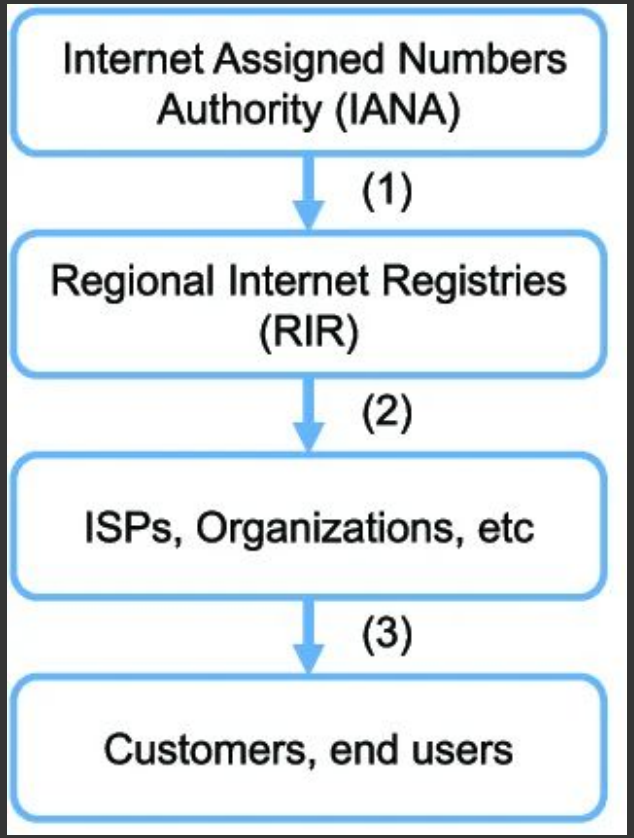
- Az Ethernet-cím bárhol a világon használható
  - de minden IP-cím adott hálózathoz tartozik, és az útválasztók csak az erre a címre küldött csomagokat tudják kézbesíteni a hálózatra.
  - Ezért szükség van olyan kialakításra – mint például a mozgó IP –, amely támogatja azokat a hosztokat, amelyek mozognak a hálózatok között, de meg akarják tartani IP-címüket

Előtagok

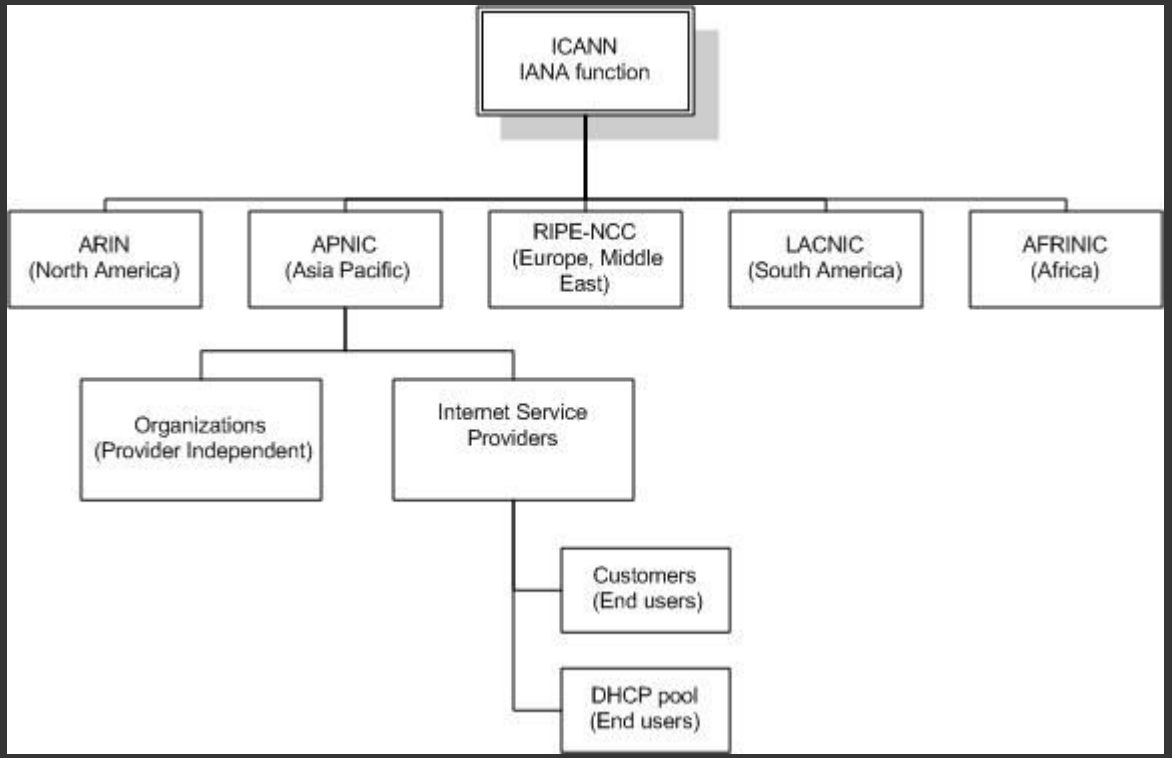
2. a hierarchia címpazarlás, hacsak nem kezelik körültekintően

- Ha a címeket (túl) nagy blokkokban rendelik a hálózatokhoz, akkor számos kihasználatlan cím kerül lefoglalásra
- Ez nem számítana, ha bőségesen állnának rendelkezésre címek
- Már több mint 20 évvel ezelőtt rájöttek arra, hogy az internet nagymértékű növekedése gyorsan kimeríti a szabad címteret
- Az IPv6 megoldást jelent erre, de ennek széles körű bevezetéséig nagy a nyomás, hogy az IP-címeket minél hatékonyabban használják ki

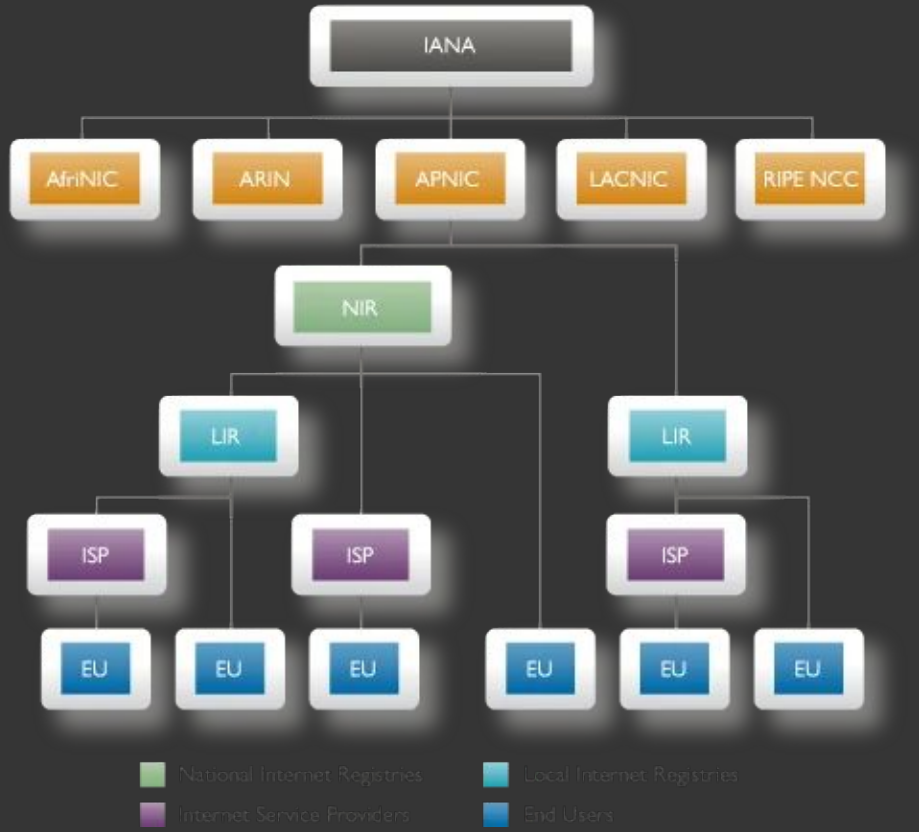
IP hiearchia



IP hiearchia



IP hiearchia



Osztályalapú címzés...

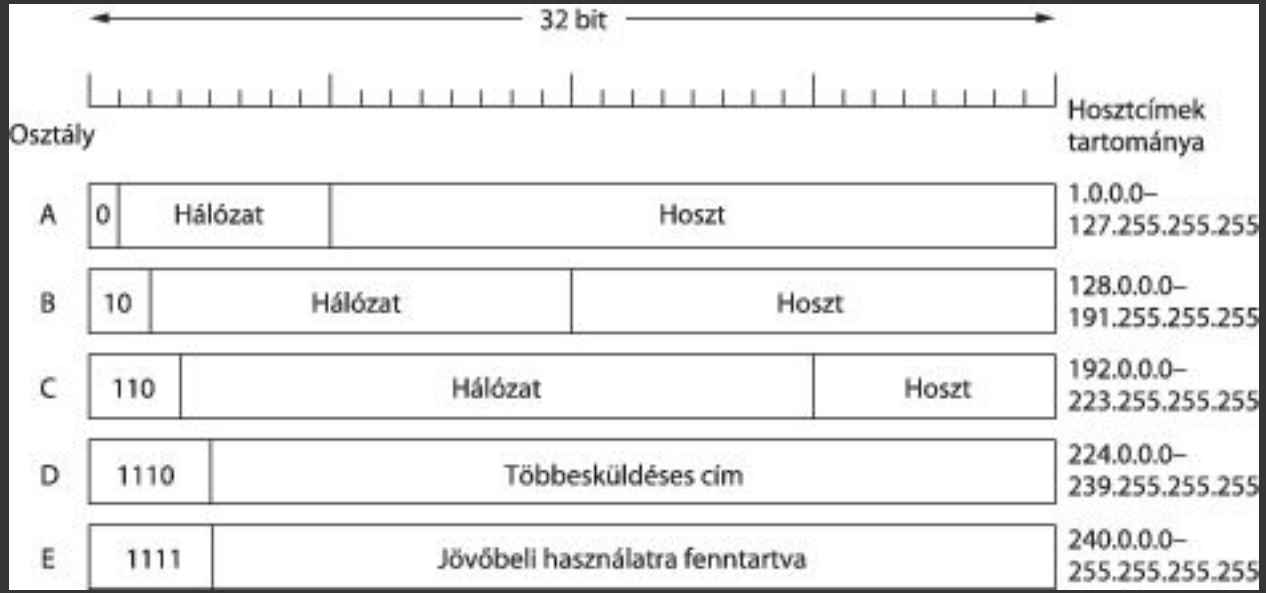
Osztályalapú címzés

- Az IP-címzés korai szakaszában a hálózatok az úgynevezett osztályalapú (classful) címzési rendszert alkalmazták.
- Ebben a megközelítésben az IP-címeket előre meghatározott méretű csoportokba, úgynevezett osztályokba sorolták.
- Ezt a kiosztást **osztályalapú címzés**nek (**classful addressing**) nevezték.
- Az osztályalapú címzés célja az volt, hogy egyszerűsítse a címkiosztást és az útválasztást egy viszonylag kis méretű internet esetében.
- Az IP-cím felépítése ebben a rendszerben fix módon határozta meg a hálózati és a hoszt részek határát.

Osztályalapú címzés

- Az IPv4 címeket öt különböző osztályba sorolták:
  - A osztály
  - B osztály
  - C osztály
  - D osztály
  - E osztály
- Az első három osztályt (A, B, C) használták hagyományos címzésre, míg a D és E speciális célokat szolgált.
- Az osztály meghatározása az IP-cím első bitjei alapján történt

Osztályalapú címzés



Osztályalapú címzés

A osztály

- Az A osztályú címek nagy hálózatok számára lettek kialakítva.
- Jellemzők:
  - első bit: 0
  - első oktett tartománya: 0–127
  - hálózati rész: 8 bit
  - hoszt rész: 24 bit
- Formátum:
  - **N.H.H.H**
- Példa: **10.0.0.1**
- Kapacitás:
  - hálózatok száma: 128 (gyakorlatban kevesebb)
  - hosztok száma hálózatonként:
  - $2^{24}-2 \approx 16\,777$

Osztályalapú címzés

- **B osztály**
  - A B osztály közepes méretű hálózatok számára készült.
  - Jellemzők:
    - első két bit: 10
    - első oktett tartománya: 128–191
    - hálózati rész: 16 bit
    - hoszt rész: 16 bit
  - Formátum:
    - N.N.H.H
  - Példa: 172.16.0.1
  - Kapacitás:
    - hálózatok száma: 214
    - hosztok száma hálózatonként:
    - **$2^{16}-2 = 65\,534$**

Osztályalapú címzés

C osztály

- A C osztály kis hálózatok számára lett kialakítva.
- Jellemzők:
  - első három bit: 110
  - első oktett tartománya: 192–223
  - hálózati rész: 24 bit
  - hoszt rész: 8 bit
- Formátum:
  - N.N.N.H
- Példa: 192.168.1.1
- Kapacitás:
  - hálózatok száma: nagyon sok
  - hosztok száma hálózatonként:
  - **$2^8-2=254$**

Osztályalapú címzés

D és E osztály

- **D osztály**
  - első négy bit: 1110
  - tartomány: 224–239
  - cél: multicast
- **E osztály**
  - első négy bit: 1111
  - tartomány: 240–255
  - cél: kísérleti felhasználás

Osztályalapú címzés

- Az IP-cím osztálya az első oktett alapján egyszerűen megállapítható:

Első oktett	Osztály
0–127	A
128–191	B
192–223	C
224–239	D
240–255	E

Az osztályalapú címzés egyszerűsége miatt kezdetben jól használható volt:

- könnyen értelmezhető struktúra
- egyszerű útválasztás
- gyors implementáció

Osztályalapú címzés

- **Az osztályalapú címzés problémái:**
  - Az internet növekedésével az osztályalapú rendszer súlyos korlátokba ütközött
  - **1. Címek pazarlása**
    - A fix méretű osztályok miatt gyakran túl nagy vagy túl kicsi hálózatokat kellett kiosztani.
    - Például: egy közepes szervezetnek túl kevés a C osztály, de túl sok a B osztály
  - Ez hatalmas címveszteséghez vezetett.
  - **2. Rugalmatlanság**
    - Az osztályok fix határai nem tették lehetővé a hálózatok rugalmas méretezését.
  - **3. Routing táblák növekedése**
    - A sok különálló hálózat miatt az útválasztási táblák gyorsan növekedtek, ami skálázási problémákat okozott.

CIDR

- Az osztályalapú címzés egyik legnagyobb hibája a címek pazarlása volt.
- Sok szervezet számára a C osztály túl kevés címet biztosított, míg a B osztály túl sokat.
    - Emiatt hatalmas mennyiségű IP-cím maradt kihasználatlanul
- E problémák megoldására vezették be a **CIDR (Classless Inter-Domain Routing)**-ot,
    - rugalmasabb címzési és útválasztási rendszert jelent
- **Mi a CIDR?**
    - A CIDR egy osztályfüggetlen IP-címzési módszer, amely lehetővé teszi, hogy a hálózati prefix hossza tetszőleges legyen.
        - Ennek köszönhetően a hálózatok mérete pontosabban igazítható a tényleges igényekhez.
    - A CIDR megszünteti az A, B és C osztályok merev határait, és helyettük prefix alapú címzést alkalmaz.

CIDR

- **Prefix alapú jelölés**: A CIDR a hálózati rész hosszát egy perjel utáni számmal jelöli
- Például:

192.168.1.0/24

- Ez azt jelenti, hogy:
- az első 24 bit a hálózati rész
- a maradék 8 bit a hoszt rész
- A prefix hossz közvetlenül meghatározza:
  - a hálózat méretét
  - a hosztok számát
  - az alhálózati maszkot

Prefix értelmezés

Prefix	Maszk	Hosztok száma
/8	255.0.0.0	kb. 16 millió
/16	255.255.0.0	kb. 65 ezer
/24	255.255.255.0	254
/30	255.255.255.252	2

CIDR és subnet mask kapcsolata

- **A CIDR jelölés valójában a subnet mask rövidített formája**

- **Példa:**

  /24

  11111111.11111111.11111111.00000000

- **Ez decimálisan:**

  255.255.255.0

CIDR

- **A CIDR működésének alapelve:**
  - A CIDR lehetővé teszi, hogy a hálózatok mérete ne előre meghatározott osztályokhoz igazodjon, hanem a szükséges hosztszámhoz.
  - Például:
    - egy kis hálózat kaphat /28-as prefixet
    - egy nagyobb hálózat /20-at
    - egy szolgáltató akár /13-at
  - Ez jelentősen javítja a címek kihasználását.

CIDR és útvonal-aggregáció

- A CIDR egyik legfontosabb előnye az **útvonal-aggregáció**
  - route aggregation vagy route summarization
- Ennek során több kisebb hálózat egyetlen nagyobb prefixként jeleníthető meg az útválasztási táblákban

- Tegyük fel, hogy egy szolgáltató a következő hálózatokat birtokolja:
  - 192.168.0.0/24
  - 192.168.1.0/24
  - 192.168.2.0/24
  - 192.168.3.0/24
  - Ezek összevonhatók:
    - 192.168.0.0/22
- Az aggregáció csökkenti a routing táblák méretét, gyorsabb útválasztást tesz lehetővé javítja a hálózat skálázhatóságát és csökkenti a routerek memóriaigényét.

CIDR és a leghosszabb prefix egyezés

- CIDR használata esetén előfordulhat, hogy egy IP-cím több útvonalhoz is illeszkedik
- Ilyenkor a router a legspecifikusabb útvonalat választja
- Ezt nevezik **leghosszabb prefix egyezés**nek (Longest Prefix Match)

Példa:

Routing tábla:

- 192.168.0.0/16
- 192.168.1.0/24

Célcím:

- 192.168.1.25

- Mindkét útvonal illeszkedik, de /24 hosszabb prefix, ezért ezt választja a router

CIDR és VLSM

- A CIDR szorosan kapcsolódik a **VLSM**-hez (Variable Length Subnet Mask)
  - lehetővé teszi különböző méretű alhálózatok létrehozását
- Például:
  - nagy részleg → /23
  - kisebb részleg → /28
- Ez rugalmasabb hálózattervezést biztosít

CIDR előnyei

A CIDR számos problémát megoldott az osztályalapú címzéshez képest

1. Hatékonyabb címhasználat

- A címkiosztás jobban igazodik a valós igényekhez

2. Kisebb routing táblák

- Az aggregáció jelentősen csökkenti az internet routing tábláinak méretét

3. Jobb skálázhatóság

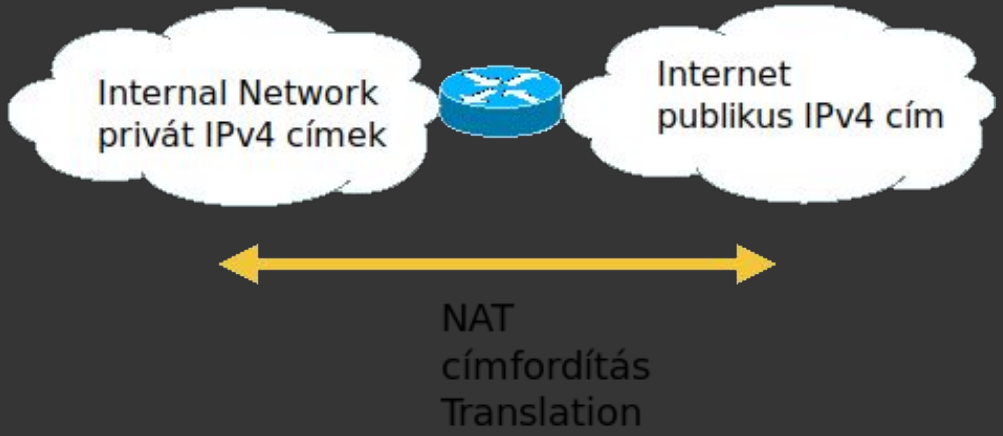
- A CIDR lehetővé tette az internet további növekedését.

NAT - hálózati címfordítás...

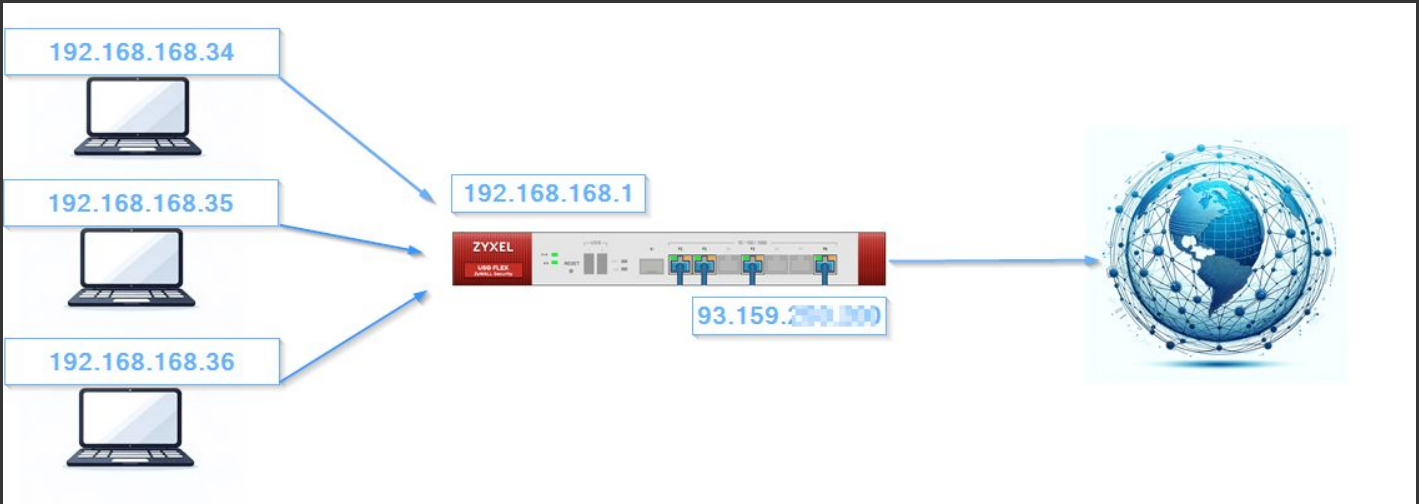
NAT - hálózati címfordítás

- **A hálózati címfordítás: Network Address Translation - NAT**
- Egy olyan mechanizmus, amely lehetővé teszi, hogy egy helyi hálózat több eszköze egyetlen vagy néhány publikus IP-címen keresztül kommunikáljon az internettel
- A NAT során a router módosítja az IP-csomagok forrás- vagy célcímét, miközben azok áthaladnak rajta
- **Miért van rá szükség?**
  - A NAT elsősorban az IPv4 címhiány problémájának enyhítésére jött létre, mára az internet működésének alapvető részévé vált.
  - Az IPv4 címek korlátozott száma miatt nem lehetséges minden internetre csatlakozó eszköz számára egyedi publikus IP-címet biztosítani.
  - E probléma megoldására vezették be a privát IP-címek használatát, amelyek nem routolhatók az interneten
  - A NAT lehetővé teszi, hogy ezek a privát címekkel rendelkező eszközök mégis elérjék az internetet, egy közvetítő eszköz, általában egy **router** segítségével

NAT - hálózati címfordítás



NAT - hálózati címfordítás



A NAT működési elve

- A NAT egy határponti eszközben, tipikusan egy routerben működik, amely a helyi hálózat és az internet között helyezkedik el
- **Kimenő forgalom esetén:**
    1. A belső eszköz egy csomagot küld egy külső cél felé
    2. A csomag forrás IP-címe egy privát cím (pl. 192.168.1.10)
    3. A NAT-eszköz ezt lecseréli a saját publikus IP-címére
    4. A csomag így kerül ki az internetre
    - A NAT egy táblázatban eltárolja az átalakítást, hogy a válaszcsomagokat vissza tudja irányítani a megfelelő belső eszközhöz.

A NAT működési elve

- **Bejövő forgalom esetén:**
    1. A válaszcsomag megérkezik a NAT-eszközhöz
    2. A NAT a táblázata alapján meghatározza a belső célcímet
    3. A csomag cél IP-címét módosítja
    4. A csomagot továbbítja a megfelelő belső eszköz felé
- A NAT működésének kulcsa a NAT tábla, amely tartalmazza:
    - belső IP-cím
    - belső port
    - külső IP-cím
    - külső port
- Ez biztosítja, hogy több eszköz is használhassa ugyanazt a publikus IP-címet

NAT típusok

- **Dinamikus NAT**
  - Ha egy belső, privát címmel rendelkező host szeretne külső hálózat felé kommunikálni, akkor a csomagot először elküldi az alapértelmezett átjárónak
  - Mivel a forgalomirányító látja, hogy ez a csomag külső hálózatba tart, kijelöl a küldő gép számára egy globális címet, ami egy címtárból (pool) kerül ki
  - Ez a címtár tartalmazhat egy vagy több címet, vagy akár címtartományokat is.
  - Továbbítás előtt a kimenő csomagban átírja a küldő IP címet erre a globális címre és megjegyzi a párosítást.
  - Amíg a kapcsolat él (tehát még várunk a címzett válaszára), a forgalomirányító érvényesnek tekinti a globális címet és a nyugtákat küld a kezdeményező eszköznek
  - Amint a kapcsolat véget ér (azaz megérkezett a válasz a címzettől), a forgalomirányító megszűnteti a párosítást és visszajuttatja a belső globális címet a címtárba
  - **Fontos:** egy globális címre küldött csomagot csak akkor továbbít a belső hálózat felé a router, ha van hozzá érvényes párosítás, egyébként eldobja.
    - egyfajta biztonságot nyújt a belső eszközök számára

NAT típusok

- **Statikus NAT**
  - A dinamikus NAT egyik előnye, hogy az egyes hostok nem érhetők el közvetlenül a külső hálózatból.
  - De mi a helyzet akkor, ha egy belső hálózaton található állomáson/szerveren olyan szolgáltatások futnak, amelyeknek az Internet felől is elérhetőnek kell lenniük?
  - Egy belső eszközt kívülről is elérhetővé tehetünk úgy, hogy a NAT-ot végző routernek előírjuk, hogy ezt a privát címet mindig ugyanarra a globális címre fordítsa le
  - A rögzített címre fordítás biztosítja, hogy ez a globális cím mindig ugyanahhoz az eszközhöz fog tartozni és más állomás garantáltan nem használja
  - Így már lehetséges, hogy a nyilvános hálózaton lévő állomások egy magán hálózaton lévő kiválasztott állomásokhoz csatlakozzanak

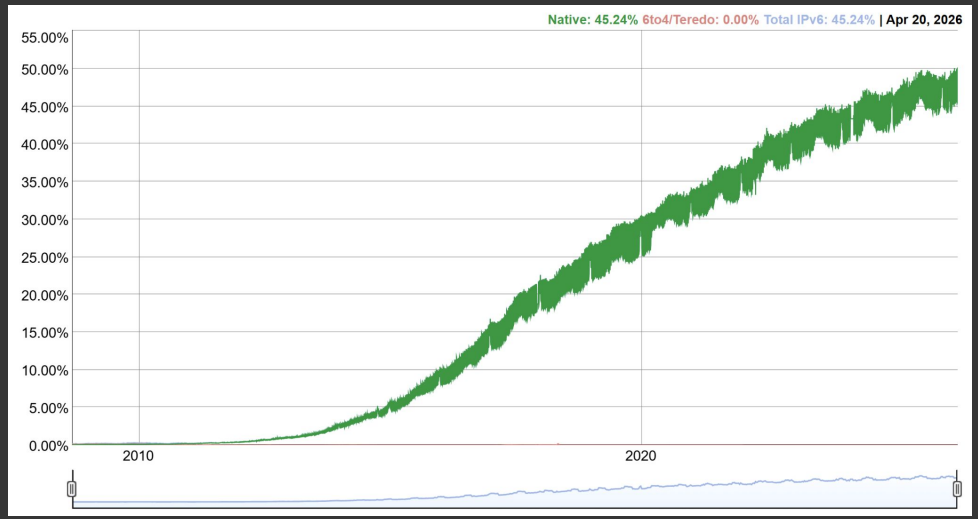
IPv6...

IPv6

- Az IP-t már évtizedek óta intenzíven használják
- Eddig rendkívül jól működött, ahogy azt az internet exponenciális növekedése is mutatja
- Sajnos az IP gyors tempóban lesz saját népszerűségének áldozata: kezd kifogyni a címekből
- **Az egyetlen hosszú távú megoldás a hosszabb címekre való áttérés**
- Az IPv6 (az IP 6-os változata) helyettesítő kialakítás, amely éppen ezt teszi: 128 bites címet használ.
    - Nem túl valószínű, hogy ezek a címek az előre látható jövőben elfogyjanak
- Az IPv6 bevezetése azonban nagyon bonyolult.
- Ez a hálózati rétegnek egy másik protokollja, amely a sok hasonlóság ellenére nem működik igazán együtt az IPv4-gyel

IPv6

- A vállalatok és felhasználók egyáltalán nem biztosak abban, hogy miért kell valaha is alkalmazniuk az IPv6-ot.
- Ennek következtében az IPv6-ot csak az internet lassan adoptálja
    - körülbelül 45-50%-ában használják annak ellenére, hogy 1998 óta internetszabvány.



IPv6

- Az IETF – látván, hogy ezek a problémák feltűnnek a horizonton – 1990-ben elkezdte a munkát az IP új verzióján,
  - egy olyan verzión, amely soha nem fogy ki a címekből, mindenféle egyéb problémákat is megold, és ezek mellett rugalmasabb és hatékonyabb is
- A fő célok a következők voltak:
  - Támogatni a több milliárd hosztot, még nem hatékony címtartomány-hozzárendelés árán is.
  - Csökkenteni az útválasztó táblázatok méretét.
  - Egyszerűsíteni a protokollt, lehetővé téve ezzel az útválasztóknak a csomagok gyorsabb feldolgozását.
  - A jelenlegi IP-nél jobb biztonságot (hitelesítés és titkosság) biztosítani.
  - Nagyobb figyelmet szentelni a szolgáltatás típusának, különösen a valós idejű adatoknál.
  - Segíteni a többesküldést azáltal, hogy megadják a hatósugarakat.
  - Lehetőséget adni arra, hogy egy hoszt a címének megváltoztatása nélkül barangoljon.
  - Lehetővé tenni a protokoll fejlődését.
  - Meg kell engedni, hogy az új és a régi protokoll még évekig egymás mellett létezhessen

IPv6

- Az IPv6 egészen jól megfelel az IETF céljainak
- Megtartja az IP jó tulajdonságait, elveti vagy kevésbé hangsúlyossá teszi a rosszakat, és új tulajdonságokkal egészíti ki, ahol szükség van rá
- **Általánosságban, az IPv6 nem kompatibilis az IPv4-gyel, de az összes többi internetprotokollal igen**:
    - beleértve a TCP-, UDP-, ICMP-, IGMP-, OSPF-, BGP- és DNS-protokollokat,
    - néhol úgy, hogy kisebb módosításokra van szükség (főleg a hosszabb címek kezelése miatt)
- Az IPv6-nak hosszabb címei vannak, mint az IPv4-nek: **128 bit** hosszúak
    - megoldja azt a problémát, amelyet az IPv6-nak meg kell oldania: egy gyakorlatilag végtelen internetcím-ellátmányt biztosít
- Az IPv6 második fő fejlesztése a fejrész egyszerűsítése:
    - Csak 7 mezőt tartalmaz (szemben az IPv4 13 mezőjével).
    - Ez a változás lehetővé teszi az útválasztóknak, hogy gyorsabban dolgozzák fel a csomagokat, és ezáltal javítsák az átbocsátást.

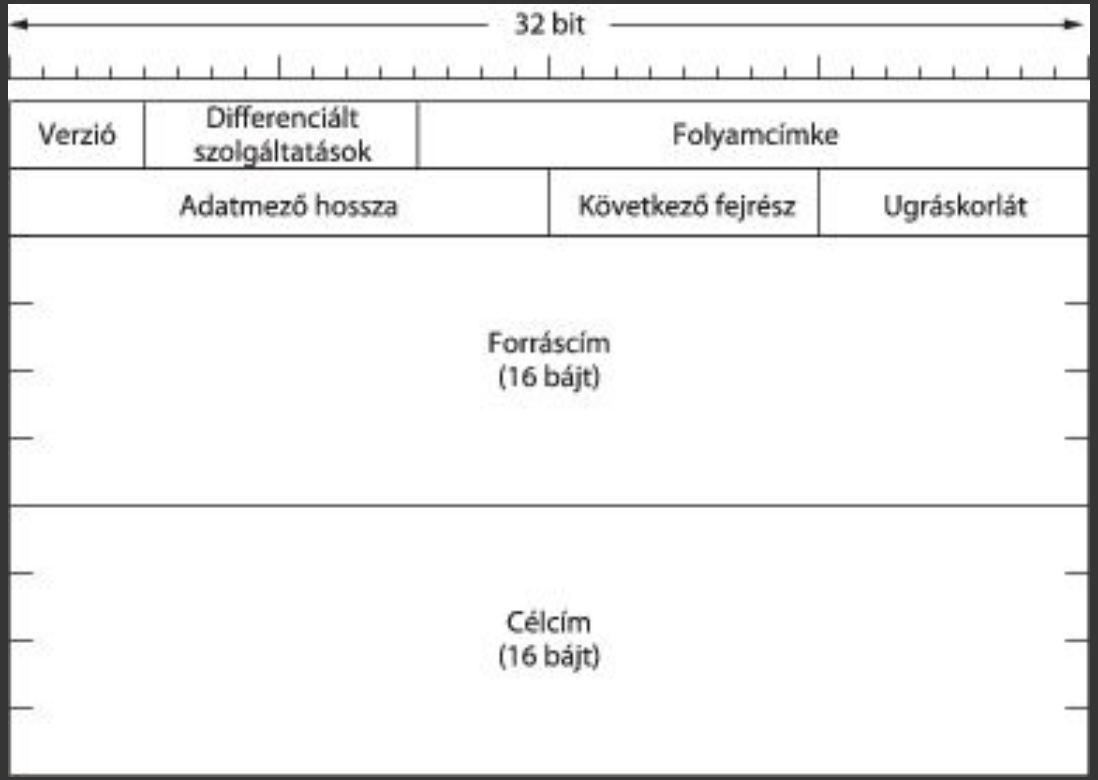
IPv6

- **A harmadik fő előrelépés az opciók jobb támogatása**
- Ez a változás szükségszerűen együtt jár az új fejrésszel, mert a korábban megkövetelt mezők most opcionálisak lettek
- Ezenkívül az opciók megjelenésének a módja is más, így az útválasztóknak egyszerű átlépni a nem nekik szánt opciókon
- Ez a tulajdonság a csomagfeldolgozási időt gyorsítja fel
- **A negyedik terület:** a biztonság.
    - A hitelesítés és a titkosság az új IP kulcstulajdonsága.
    - Ezeket aztán visszamenőleg az IPv4-be is beépítették, így a biztonság területén a különbségek ma már nem olyan jelentősek

IPv6-fejrész

- A Verzió mező IPv6-nál mindig 6
- Az alatt az idő alatt, amíg átállnak az IPv4-ről, az útválasztók megvizsgálhatják ezt a mezőt, hogy eldöntsék, milyen fajta csomagjuk van.
- Viszont ez az ellenőrzés mellékhatásként elveszteget pár utasítást a kritikus úton, mivel az adatkapcsolati fejrész rendszerint jelzi a demultiplexeléshez szükséges hálózati protokollt, így néhány útválasztó esetleg átlépi ezt az ellenőrzést.
- Az Ethernet Type mezője például különféle értékekkel rendelkezik egy IPv4 vagy IPv6 adatmező jelzésére.

IPv6-fejrész



IPv6 fejrész

- **Differenciált szolgáltatások:**
  - mező szolgál arra, hogy különbséget tegyenek a csomagok között, amelyeknél különbözőek a követelmények a valós idejű szállítással kapcsolatban.
  - Ezt a differenciált szolgáltatás architektúránál használják a szolgáltatásminőséghez ugyanúgy, mint ahogy az azonos nevű mezőt használták az IPv4-csomagban.
  - Az első két bit az explicit torlódás jelzésére szolgál ugyanúgy, mint az IPv4 esetén.
- **Folyamcímke mező:**
  - lehetővé teszi, hogy a forrás és a cél megjelölje azon csomagok csoportját, amelyek azonos követelményeket támasztanak,
    - amelyeket a hálózatnak azonos módon kell kezelnie, ezáltal egy álösszeköttetést létesítve
  - Például egy bizonyos forráshoszt egy folyamatától egy meghatározott címzett hoszt egy folyamatáig tartó csomagfolyamnak szigorú késleltetési igényei lehetnek,
    - és ezért fenntartott sávszélességre van szüksége

IPv6 fejrész

- **Folyamcímke mező (folyt.):**
  - A folyamot előre fel lehet állítani, és egy azonosítót adni neki
  - Amikor egy nem nulla Folyamcímke mezőjű csomag tűnik fel, minden útválasztó kikeresheti a belső táblázataiból, hogy milyen különleges elbánást igényel
  - A folyamok bevezetése kísérlet arra, hogy egyszerre lehessen kihasználni a datagramalapú hálózat rugalmasságát és a virtuálisáramkör-alapú hálózat garanciáit
  - A szolgáltatásminőség biztosításához minden folyamot forráscím, célcím és folyamszám alapján azonosítanak.
  - Ez azt jelenti, hogy 2^{20} folyam lehet egy időben aktív két adott IP-cím közt.
  - Ilyen módon, ha más hosztoktól jövő, de ugyanolyan folyamszámú folyamok ugyanazon az útválasztón haladnak keresztül, az útválasztó meg tudja azokat különböztetni a forrás- és célcím segítségével.
  - Várhatóan a folyamszámokat véletlenszerűen fogják választani ahelyett, hogy 1-től kezdve folyamatosan osztanák ki azokat, hogy az útválasztók könnyen tudják azokat hash-elni

IPv6 fejrész

- **Adatmező hossza mező:**
  - megmondja, mennyi bájt következik 40 bájtos fejrész után
  - A név megváltozott az IPv4 Teljes hossz mezőjéhez képest, mivel a jelentés is módosult: a 40 fejrészbájtot már nem számolják bele a hosszba, mint régebben
  - Ez a módosítás azt jelenti, hogy az adatmező 65 535 bájtot tartalmazhat 65 515 bájt helyett
- **Következő fejrész mező:**
  - A fejrészt azért lehetett egyszerűsíteni, mert lehetnek további (opcionális) kiegészítő fejrészek.
  - Ez a mező mondja meg, melyik kiegészítő fejrész következik a (jelenleg) hat közül, ha egyáltalán van ilyen.
  - Ha a fejrész az utolsó IP-fejrész, a **Következő fejrész mező** azt mondja meg, melyik szállítási protokoll kezelőjének (TCP, UDP) kell a csomagot továbbítani.

IPv6 fejrész

- **Ugráskorlát mező:**
  - Ez a mező gátolja meg a csomagokat abban, hogy azok örökké élhessenek.
  - Ez gyakorlatilag ugyanaz, mint az **Élettartam mező az IPv4-ben**, vagyis egy olyan mező, amelyet minden ugrásnál csökkentenek.
  - Elméletben az IPv4-ben ez másodpercekben mért idő volt, de egy útválasztó sem használta így, ezért megváltoztatták a nevét, hogy az a tényleges működésre utaljon.

IPv6 fejrész

- **Forráscím és Célcím mezők:**
  - Eredetileg 8 bájtos címeket használtak, de a felülvizsgálási folyamat során sok ember érezte úgy, hogy 8 bájtos címekkel az IPv6 néhány évtizeden belül ki fog fogyni a címekből
    - míg a 16 bájtos címek soha nem fogynak el.
  - Más emberek érvelése szerint a 16 bájt túlzás, megint mások pedig 20 bájtos címeket részesítettek volna előnyben, hogy az IPv6 kompatibilis legyen az OSI-datagramprotokollal
  - Egy másik frakció változó hosszúságú címeket akart.
  - Sok vita után úgy határoztak, hogy a legjobb kompromisszum a rögzített hosszúságú 16 bájtos címek alkalmazása
  - **A 16 bájtos címek leírására új jelölésrendszert is javasoltak:**
    - Nyolc, négy-négy hexadecimális számjegyből álló csoportként írjuk le a címet, a csoportok között kettősponttal:

8000:0000:0000:0000:0123:4567:89AB:CDEF

IPv6 fejrész

- **Forráscím és Célcím mezők:**
  - Mivel a sok cím sok nullát fog tartalmazni, három ésszerűsítést engedélyeztek.
  - 1) egy csoporton belül a bevezető nullák elhagyhatók, így a 0123 helyett 123 írható.
  - 2) egy vagy több, 16 nullából álló csoport két kettősponttal helyettesíthető.
    - Így a fenti címből a következő lesz:

      8000::123:4567:89AB:CDEF
  - Végül, az IPv4-címek két kettőspont és a régi, pontokkal elválasztott decimális szám formájában írhatók fel, például:

    ::192.31.20.46

  - Rengeteg 16 bájtos cím létezik: 2^{128} darab

Internet vezérlőprotokolljai...

ICMP protokoll

- Az internet működését az útválasztók szorosan figyelemmel kísérik.
- Amikor valami váratlan esemény történik a csomag feldolgozása során egy útválasztóban:
  - ezt az eseményt az **ICMP** (**Internet Control Message Protocol – internetes vezérlőüzenet protokoll**) segítségével jelenti
- Az ICMP-t az internet tesztelésére is használják. Körülbelül egy tucat ICMP-üzenetet definiáltak

Üzenet típusa	Leírás
Cél elérhetetlen	A csomagot nem lehetett kézbesíteni
Időtúllépés	Az Élettartam mező elérte a 0-t
Paraméter probléma	Érvénytelen fejrész mező
Forráslefojtás	Lefojtócsomag
Átirányítás	Egy útválasztót tanít meg a földrajzra
Visszhang kérés és visszhang válasz	Annak ellenőrzése, hogy egy gép életben van-e
Időbélyeg kérés/válasz	Ugyanaz, mint a visszhang kérés, csak időbélyeggel
Útválasztó hirdetés/kérelmezés	Egy közeli útválasztó megtalálása

ICMP protokoll

- A **cél elérhetetlen üzenet:**
  - akkor használják, ha az útválasztó nem tudja megtalálni a célt, vagy egy DF bittel rendelkező csomagot nem lehet kézbesíteni, mert egy „kiscsomagos” hálózat az útjába állt

- Az **időtúllépés üzenet:**
  - akkor küldik, ha egy csomagot azért dobnak el, mert a számlálója elérte a nullát.
  - Ez az esemény annak a tünete, hogy a csomagok hurokba kerültek, hogy hatalmas torlódás van, vagy az időzítő értékét túl alacsonyra állították be
  - A hibaüzenetnek az egyik értelmes használata a **traceroute** (útkövetés) segédprogram,
    - Van Jacobson fejlesztett ki 1987-ben.
    - A traceroute megtalálja a hoszt és a címzett IP-címe közötti útvonal mentén lévő útválasztókat.

ICMP protokoll

- **Traceroute működése:**
  - A módszer egyszerű: csomagok sorozatának elküldése a cél felé, az Élettartam mezőbe írt először 1-es, majd 2-es, 3-as stb. értékkel.
  - A csomagokban lévő átlépésszámlálók elérik a nullát, ahogy végighaladnak az útvonal mentén lévő egymás utáni útválasztókon.
  - Ezek az útválasztók egyenként időtúllépés üzenetet küldenek vissza a hosztnak.
  - Ezekből az üzenetekből a hoszt meg tudja határozni az útvonal mentén lévő útválasztók IP-címét, illetve statisztikát és időzítéseket tarthat fenn az útvonal egyes részeiről.
  - Ez nem az, amire az időtúllépés üzenetet eredetileg szánták, de talán a valaha alkalmazott leghasznosabb hálózati hibakereső eszköz.

ICMP protokoll

- **A paraméterprobléma üzenet:**
  - azt jelzi, hogy egy fejrészmezőbe érvénytelen érték került
  - Ez hibát jelez az adóhoszt IP-szoftverében, vagy esetleg egy, az út során érintett útválasztó szoftverében
- **A forráslefojtás üzenet:**
  - régebben a túl sok csomagot küldő hosztok visszafogására használták.
  - Amikor egy hoszt ilyen üzenetet kapott, le kellett lassítania.
  - Manapság már ritkán használják, mert amikor torlódás következik be, ezek a csomagok csak olajat öntenek a tűzre
- **Az átirányítás üzenetet:**
  - akkor használják, ha egy útválasztó észreveszi, hogy egy csomag rosszul irányítottnak tűnik.
  - Az útválasztó használja, hogy a küldő hosztot értesítse a valószínű hibáról.

ICMP protokoll

- **A visszhang kérés és visszhang válasz üzenetek:**
  - arra használják, hogy meggyőződjenek arról, hogy egy adott hoszt elérhető-e és pillanatnyilag életben van-e.
  - A visszhang kérés üzenetet megkapva, a címzettnek vissza kell küldenie egy visszhang válasz üzenetet.
  - Ezeket az üzeneteket a ping segédprogram használja, amely ellenőrzi, vajon a hoszt működik-e és elérhető-e az interneten
- **Az időbélyeg kérés és időbélyeg válasz üzenetek:**
  - hasonlók, kivéve, hogy az üzenet érkezési ideje és a válasz indulási ideje is szerepelnek a válaszban.
  - Ezt a tulajdonságot a hálózati teljesítőképesség mérésére használják
- **Az útválasztó hirdetés és útválasztó kérelmezés üzenetek:**
  - segítségével a hosztok meg tudják keresni a közeli útválasztókat.
  - A hosztnak meg kell tanulnia legalább egy útválasztó IP-címét ahhoz, hogy csomagokat küldhessen a helyi hálózatnak

ARP protokoll

- A számítógépes hálózatok működése során az adatcsomagok továbbítása különböző rétegek együttműködésével valósul meg.
- A hálózati réteg az IP-címek segítségével azonosítja a célállomást, míg az adatkapcsolati réteg fizikai (MAC) címeket használ a tényleges adatátvitelhez.
- Ez a különbség problémát vet fel: **hogyan jutunk el egy IP-címből a megfelelő fizikai címhez?**
- Ezt a feladatot az **Address Resolution Protocol (ARP)** látja el
    - lehetővé teszi az IP-címek és a hozzájuk tartozó MAC-címek közötti leképezést egy helyi hálózaton belül.

ARP protokoll

- **Az ARP alapelve**
  - Az ARP egy egyszerű kérdés–válasz mechanizmuson alapul:
    - egy eszköz ismeri a cél IP-címét
    - de nem ismeri a cél MAC-címét
    - ezért lekérdezést küld a hálózaton
    - a megfelelő eszköz válaszol a saját MAC-címével

Az ARP működése

1. ARP kérés (ARP Request)

- Amikor egy eszköz adatot szeretne küldeni egy másik eszköznek ugyanazon a helyi hálózaton, először meg kell tudnia a cél MAC-címét.
- Ehhez egy ARP kérés üzenetet küld:
  - cél: minden eszköz a hálózaton (broadcast)
  - tartalom: „Kié ez az IP-cím?”
- Ez az üzenet broadcast formában kerül elküldésre, vagyis minden hálózati eszköz megkapja.

2. ARP válasz (ARP Reply)

- Az a gép, amelynek az IP-címe megegyezik a kérésben szereplő címmel:
  - visszaküld egy választ
  - megadja a saját MAC-címét
- Ez az üzenet már unicast, tehát közvetlenül a kérdezőhöz érkezik.

Az ARP működése

ARP cache

- Az ARP cache egy ideiglenes tároló, amely az IP–MAC megfeleltetéseket tartalmazza.
- **Jellemzői:**
  - időkorlátos (timeout)
  - automatikusan frissül
  - csökkenti a hálózati forgalmat

ARP és a routing

- az ARP csak helyi hálózaton működik. Ha a cél egy másik hálózatban van:
  - az eszköz nem a cél MAC-címét kéri le
  - hanem az alapértelmezett átjáró (router) MAC-címét
- Ezután a csomag a routerhez kerül, amely továbbítja azt a megfelelő irányba.

ARP üzenetek jellemzői

- Az ARP egy alacsony szintű protokoll, amely:
- nem használ TCP-t vagy UDP-t
- közvetlenül az adatkapcsolati rétegen működik
- Ethernet keretekbe ágyazódik

Az ARP működése

3. ARP tábla frissítése

- A kérdező eszköz eltárolja az IP–MAC párost egy úgynevezett ARP táblában (cache)
- Ez lehetővé teszi, hogy a későbbi kommunikáció során ne kelljen újra lekérdezést küldeni.

Példa működés

Tegyük fel, hogy egy eszköz a következő címmel rendelkezik:

IP: 192.168.1.10

És adatot szeretne küldeni a következő címre:

IP: 192.168.1.20

A folyamat:

- Megnézi az ARP táblát
- Ha nincs benne a cím → ARP kérés
- A cél válaszol a MAC-címével
- A forrás eltárolja az adatot
- Megkezdődik az adatküldés

DHCP – dinamikus hosztkonfigurációs protokol

- Az ARP (ahogy más internetprotokollok is) feltételezi, hogy a hosztokat ellátták alapvető információval, mint amilyen például a saját IP-címük.
- Hogyan kapják meg a hosztok ezt az információt?
- Be lehet állítani ezt minden számítógépen kézzel is, de ez hosszadalmas és nagy a hibázás lehetősége.
- Van erre egy jobb módszer: **DHCP** (**Dynamic Host Configuration Protocol** – dinamikus hosztkonfigurációs protokoll)

DHCP – dinamikus hosztkonfigurációs protokol

- DHCP alkalmazása esetén minden hálózaton kell lennie egy DHCP-kiszolgálónak, amely a konfigurációért felelős.
- A számítógépek elindításkor beépített Ethernet- vagy egyéb, a hálózati kártyába ágyazott adatkapcsolati rétegbeli címmel rendelkeznek, de IP-címmel nem.
- Az ARP-hez hasonlóan a számítógép adatszórással IP-címet kér a hálózaton.
- Ezt **dhcp felfedezés csomag** küldésével teszi.
- A csomagnak el kell érnie a DHCP-kiszolgálót:
    - Ha ez a kiszolgáló nem közvetlenül csatlakozik a hálózathoz, akkor az útválasztót úgy állítják be, hogy fogadja a DHCP adatszóró üzeneteket és továbbítja azokat a DHCP-kiszolgáló felé, bárhol is található az.

DHCP – dinamikus hosztkonfigurációs protokol

- Amikor a kiszolgáló megkapja a kérést, kioszt egy szabad IP-címet és elküldi azt a hosztnak a dhcp ajánlat csomagban.
- Ahhoz, hogy a hosztok ezt IP-cím nélkül is meg tudják tenni, a kiszolgáló a hosztot az Ethernet-címével azonosítja (amelyet a dhcp felfedezés csomag tartalmaz).
- Az IP-címeknek egy külön készletből (pool) történő automatikus kiosztása felveti azt a kérdést, hogy vajon mennyi időre osszanak ki egy IP-címet:
  - Ha egy hoszt elhagyja a hálózatot, és nem adja vissza az IP-címét a DHCP-kiszolgálónak, akkor ez a cím tartósan elveszik.
  - Ennek megelőzésére kioszthatjuk az IP-címeket rögzített időtartamra is. Ezt a módszert **lízingelésnek (leasing)** nevezik.
  - A hosztnak röviddel a lízing lejárta előtt újítást kell kérnie a DHCP-kiszolgálótól.
  - Ha nem sikerül ilyen kérelmet küldenie vagy a kiszolgáló elutasítja a kérelmet, akkor a hoszt nem használhatja tovább a korábban kapott IP-címet.

Köszönöm a figyelmet!