Tavasz | 2014

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Számítógép hálózatok 9. gyakorlat
IP címzés

Deák Kristóf

Tartalomjegyzék

Bevezetés

Az előző gyakorlatokon megtanultuk az Ethernet hálózatok alapvető felépítését, illetve azt, hogy a hálózatok növekedésével, globálissá válásával a cél egy magasabb hierarchia megvalósítása lett ahhoz, hogy el tudjuk érni a hálózatok nagyobb rendszerét.
A mai anyagban pedig megnézzük, hogy ez az IP címekkel hogyan is valósítható meg ez, hogyan épül fel pontosan egy cím, milyen részei vannak, és ezek mire használatosak.
Ennek keretében az IPv4 és IPv6 címekkel fogunk foglalkozni. Ugyan a kettő között volt még egy IPv5-ös protokoll, amely kísérleti jellegű, valós idejű, élő közvetítéses protokoll volt, de sosem használták szélesebb körben, így mi sem foglalkozunk vele.
Maga az IP az OSI modell harmadik, azaz hálózati rétegét valósítja meg. Így ennek feladata, hogy biztosítsa a változó hosszúságú adatok küldőtől a címzettig való eljuttatását akár több hálózaton keresztül is. E protokoll segítségével valósul meg a hálózati forgalomirányítás is.

Az IPv4 fejrész

Fejlesztését a DARPA (Defense Advanced Research Projects Agency, akkori nevén ARPA), ami az USA Védelmi Minisztériumának egy részlege, kezdte el, de jelenleg az IETF (Internet Engineering Task Force) felügyeli. A protokoll teljes specifikációja megtalálható az RFC 791-ben.
A protokoll alapvető célja az, hogy a különböző hálózatok közötti összeköttetést megvalósítsa. Ezt úgy éri el, hogy egyetlen címben adja meg az alhálózat, és azon belül is az állomás pontos címét.
A címek megvizsgálása előtt viszont hasznos, ha rátekintünk magára az IP fejrész felépítésére is, amelyet a következő táblázatban láthatunk:

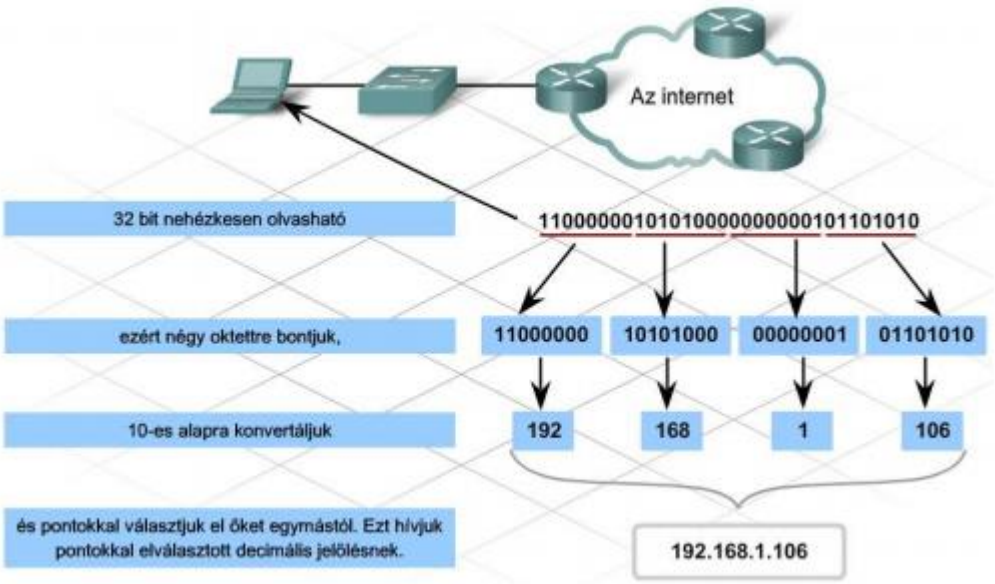
<table>
<tr><th colspan="2">0-7 bitek</th><th colspan="2">8-15 bitek</th><th colspan="3">16-23 bitek</th><th>24-31 bitek</th></tr>
<tr><td>Verzió</td><td>IHL</td><td colspan="2">Szolgáltatás típusa</td><td colspan="4">Teljes hossz</td></tr>
<tr><td colspan="4">Azonosítás</td><td></td><td>D F</td><td>M F</td><td>Darabeltolás</td></tr>
<tr><td colspan="2">Élettartam</td><td colspan="2">Protokoll</td><td colspan="4">Fejrész ellenőrző összege</td></tr>
<tr><td colspan="8">Forrás címe</td></tr>
<tr><td colspan="8">Cél címe</td></tr>
<tr><td colspan="8">Opciók (0 vagy több szó)</td></tr>
</table>

A **Verzió** (Version) azt tartja nyilván, hogy az adatcsomag (datagram) a protokoll melyik verziójához tartozik. Mint korábban szerepelt, itt a 4-es és 6-os verzió a gyakori. Bár az IPv6 fejrésze máshogyan néz ki, ez a mező megegyezik mindkét protokollban éppen amiatt, hogy meg lehessen állapítani, melyik verzió szerint épül fel a fejrész többi eleme.
Mivel a fejrész hossza nem állandó, így a fejrész egy mezője, az **IHL** szolgál arra, hogy a fejrész hosszát megadja 32 bites szavakban. A legkisebb érték 5 szó, ez esetben semmilyen opció (utolsó mező) nem szerepel, a maximális érték pedig 15, amivel 60 bájtra korlátozza az üzenet maximális méretét.

A **Szolgáltatás típusa** (Type of Service) mezőt arra használják, hogy különbséget tegyen az eltérő szolgáltatási osztályok között. Például a digitalizált hang számára fontos, hogy gyorsan érjen célba, de fájlátvitelnél pedig inkább a pontosságra kell figyelni. Elméletben ezek a mezők teszik lehetővé a router számára, hogy válasszanak egy nagy átbocsátóképességű és nagy késleltetésű műholdas kapcsolat, és egy kis átbocsátóképességű és kis késleltetésű bérelt vonal között. Ez a mező 6 bit, és 2 nem használt bit követi.
A **Teljes hossz**ba (Total Length) az egész csomag hossza beleértendő, tehát a fejrész és az adatrész is. A maximális hossz 65536 bájt.
Az **Azonosítás** (Identification) mező ahhoz szükséges, hogy a célhoszt eldönthesse, melyik datagramhoz tartozik az újonnan érkezett darab. Egy datagram minden darabja ugyan azt az értéket tartalmazza.
A router a forgalomirányításkor dönthet úgy, hogy több részre osztja az IP csomagot. Ezzel elkerülhető, hogy nagyon beduguljon a hálózat, ugyanis kisebb üzeneteket hatékonyabban lehet továbbítani. A **DF** jelzőbit jelentése „Don't Fragment", azaz „Ne darabold". Ez csak 0 vagy 1 értéket vehet fel. A routerek számára jelzik, hogy ne darabolják fel az üzenetet, mert a cél képtelen az újbóli összerakására.
Az előbbivel szemben az **MF** a „More Fragments", azaz „Több darab" kifejezés rövidítése. Ez jelzi a router számára, hogy az üzenet részletekben érkezik. Minden darabban be kell állítani ezt a bitet, kivéve az utolsóban.
A **Darabeltolás** (Fragment Offset) megmondja, hogy hova tartozik az aktuális darab a datagramban.
Az **Élettartam** (Time to Live) mező egy számláló, amelyet a csomag élettartamának korlátozására használnak. A 8 bit összesen 255 egység hosszú életet tesz lehetővé. Gyakorlatilag ez a mező azt számolja, hogy hány routeren haladt át a csomag, és minden átugrásnál csökkenteni kell az értékét. Amikor eléri a nullát, egy figyelmeztető üzenetet kell küldeni a forrásnak. Így megakadályozható, hogy a végtelenségig kóboroljanak a csomagok.
Amikor a vételi oldalon a hálózati réteg összeállított egy teljes datagramot, tudnia kell, hogy mit tegyen vele. A Protokoll (Protocol) mező mondja meg, hogy melyik szállítási rétegbeli protokollnak adja át.
A **Fejrész ellenőző összeg** (Header Checksum) csak a fejrészt ellenőrzi. Az ellenőrzés algoritmusa alapján az ellenőrző összeget nullának várjuk, ekkor lesz helyes az üzenet. Ezt a műveletet minden ugrásnál (egyik routerről a másikra küldésnél) el kell végezni, hiszen legalább egy mező (Élettartam) változik.
A **Forrás címe** (Source Address) és **Cél címe** (Destination Address) a hálózat és a hoszt számát mutatja, ezekkel a későbbiekben fogunk foglalkozni.
Az **Opciók** (Options) mezőt egy „menekülési útvonalként" találták ki a későbbi verziók számára, így extra információkat is tudnak a fejrészbe bevenni.

IPv4 címek

A korábbi anyagokból már tudhatjuk, hogy egy hagyományos IP cím 32 darab bináris számjegyből áll, így egy 32 bites címet kapunk. Mivel azonban az ember számára gyakran nehezen értelmezhető ez a forma, így fel szoktuk bontani nyolcas csoportokra, és ezeket egy-egy decimális számként értelmezzük. A lenti ábrán szemléletesen is látható ez a felosztás.



Címosztályok

A hálózatok hierarchiáját úgy valósítjuk meg, hogy az IP címet két részre osztjuk. Így a 32 bites cím első valahány bitje a hálózatot fogja jelölni, az utána következők pedig az egyes állomásokat.
Az Internet hőskorában olyan kevés szervezetnek volt szüksége IP címekre, hogy úgy határozták meg az előbb említett felosztást, hogy az első 8 bit (első oktett) jelölje a hálózat címét, a többi pedig az egyes hosztokat. Így meg tudtak címezni 256 különböző hálózatot, illetve 16 millió állomást. Viszont az Internet gyors terjedésével kevés lett a kioszthatók hálózatok száma, ezért létrehozták a már korábban is ismertetett címosztályokat.

- **A osztály**: ez éppen az előbbi leírásnak felel meg, tehát az első 8 bitet használjuk a hálózat azonosítására, a maradék 24-et pedig a hálózaton belüli hostok azonosítására.
- **B osztály**: itt az első 16 bit lesz a hálózat címe, és a maradék 16 pedig a hálózaton belüli állomások címe.
- **C osztály**: ebben az osztályban az első 24 bitet használják a hálózat azonosítására, és a maradék 8-at az egyes hostok jelölésére.
- **D osztály**: ezek az úgynevezett többesküldéses (multicast) címek, amelyeknek speciális alakjuk van.
- **E osztály**: ez a tartomány speciális, jövőbeli felhasználásra szánt címek halmaza.

Az alábbi ábrákon példát láthatunk az egyes osztályok felépítésére, illetve megfigyelhetjük, hogy az első valahány bit minden osztály esetében lekötött. Ezt részben technikai okokból valósították meg így, hiszen ha a cím 0-val kezdődik, akkor a router már rögtön tudja, hogy egy A osztályos címmel van dolga, illetve ha 10-val, akkor B osztályos, és így tovább.

A osztály				
0	Hálózat	Host	Host	Host
0	0100111	00010100	00010111	00000110
39		20	23	6

Az A osztály címtartománya így 1.0.0.0-tól egészen 127.255.255.255-ig terjedhet. Viszont mint látni fogjuk picit később, ennek sem használják ki a teljes spektrumát.

B osztály					
1	0	Hálózat	Hálózat	Host	Host
1	0	000110	10110010	00011100	01011001
134		178		28	89

Kis számolgatással rájöhetünk, hogy a B osztály tartománya 128.0.0.0-tól egészen 191.255.255.255-ig terjedhet. Ennek is vannak az A-hoz hasonlóan különleges részei.

C osztály						
1	1	0	Hálózat	Hálózat	Hálózat	Host
1	1	0	01100	10101000	11110000	00001111
204				168	240	15

Ezen osztály címtartománya 192.0.0.0-tól egészen 223.255.255.255-ig tart. Itt is fenntartanak bizonyos címeket.

D osztály							
1	1	1	0	Többesküldéses cím			
1	1	1	0	0110	10101001	11110001	00001110
230					169	241	14

Az elérhető tartomány 224.0.0.0-től 239.255.255.255-ig tart. A többesküldés, azaz multicast hasonló a korábban is már tárgyalt üzenetszóráshoz, azzal a kivétellel, hogy itt nem az összes állomáshoz, hanem csak azok egy csoportjához küldjük el az üzenetet. Így tehát, akinek a megfelelő multicast címe van, az kapja meg az üzenetet. Tehát például mindegyik 224.10.10.10-es IP-vel rendelkező címzett megkapja a 224.10.10.10-re menő üzeneteket.

E osztály							
1	1	1	1	Jövőbeli felhasználásra fenntartva			
1	1	1	1	0110	00110011	11110000	00010000
246					51	240	16

Itt az elérhető tartomány már a 240.0.0.0-tól nem meglepő módon a 255.255.255.255-ig tart. Ezt az osztályt csak néhány kutatás-fejlesztési szervezetek használják kísérleti célból. Ha éles helyen egy ilyen IP címet állítunk be, akkor lehet, hogy nem fog megfelelően működni a hálózatunk.

Különleges IP címek

A fentieken kívül még alkalmazhatunk egyes gépek azonosítására más módszereket is. Ezek pedig a következők:

- csupa nulla cím: „ez a host”
- a hálózat része nulla, a host része nem nulla: egy bizonyos host ezen az alhálózaton, pl. a 192.168.1.34-es cím (255.255.255.0 hálózati maszkkal) a 192.168.1.0 alhálózaton jelenti a 34-es gépet, tehát a 0.0.0.34 a jelenlegi

alhálózaton a 34-es gépet jelöli. Ez feltételezi, hogy mi is az adott alhálózatban vagyunk.

- csupa 1-es cím: ez a helyi alhálózaton történő adatszórás.
- A hálózat címe érvényes cím, a host címe pedig csupa 1-es: ez adatszórás a távoli hálózaton. Egy ilyen cím például a 192.168.1.255. Ez azt jelenti, hogy a csomag amit küldünk, az a 192.168.1.0-s alhálózaton végez majd adatszórást.

Privát és publikus IP címek

Az előbbi osztályozás létrehozásán kívül az IP címeket felosztották a szerint is, hogy milyen hálózatra szánják. E szerint lettek olyan címek, amelyeket csak magánhálózaton lehet használni, és ezekkel az Internetre nem tudnak kimenni, illetve a publikus IP címek, amelyekkel tudtak szörfözni a neten. Az alábbi táblázat összefoglalja, hogy a fenti osztályokból milyen tartományok esnek a privát részre.

Osztály	Privát IP-címek (RFC 1918)	Az alapértelmezett alhálózati maszk	A hálózatok száma	Állomások hálózatonként	Az összes állomás
A	10.0.0.0-tól 10.255.255.255-ig	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0-tól 172.31.255.255-ig	255.255.0.0	16	65,534	1,048,544
C	192.168.0.0-tól 192.168.255.255-ig	255.255.255.0	256	254	65,024

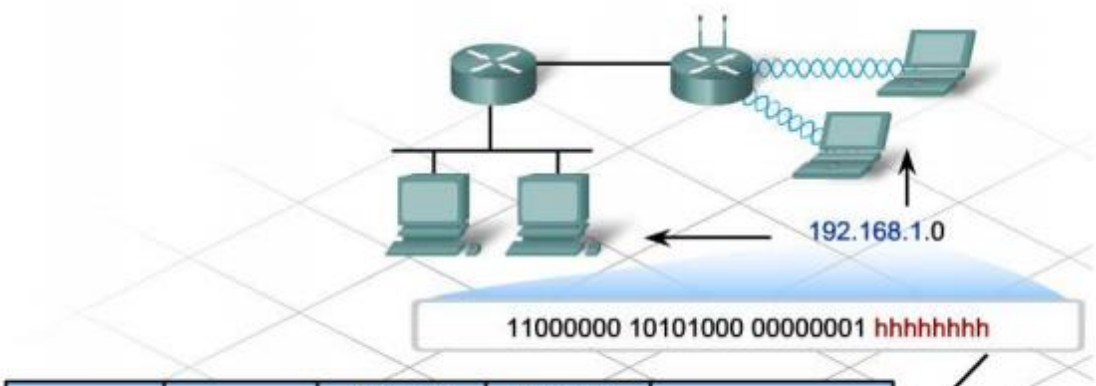
További előnye ennek a felosztásnak, hogy kevesebb IP címet kell kiosztani, mivel a cégek belső hálózata úgy sem látszik a külvilág felé. A legtöbben manapság ezeket a privát címeket használják, és csak az Internetre közvetlenül kapcsolódó eszközök kapnak publikus címet.

Alhálózatok

Vegyünk egy nagyvállalatot, amelyben több ezer állomás van a céges hálózatban. Ennek kiszolgálására tulajdonképpen megfelelne egy B osztályú hálózat, de a szervezetben több probléma is felléphet. Először is, feltételezhetjük, hogy nincs egy helyen az összes számítógép, és valószínűleg valamilyen hierarchiát akarnak kialakítani. Másodszor egy ekkora hálózaton rengeteg szórásos üzenet haladhat végig, ami ekkora méretekben igen leterhelheti a hálózatot.

Ezért az IP cím kezeléséért felelős szervezet (IETF) úgy határozott, hogy megengedi, hogy néhány extra bitet a host-ok részéről elvegyenek, és egy úgynevezett alhálózati azonosítóként használják. Az alábbi ábrán egy C osztályos IP cím lehetséges felbontásai láthatók.

Ennek eredményeképpen tehát az eddigi hierarchiába középre egy harmadik szint is beékelődik, ez az azonos méretű alhálózatok szintje.



Alhálózat ID Bitek	Állomás ID Bitek	Azonosító az Alhálózatoknak	Azonosító az Állomásoknak	Bitminta
0	8	1	254	hhhhhhhh
1	7	2	126	shhhhhhh
2	6	4	62	sshhhhhh
3	5	8	30	sshhhhhh
4	4	16	14	ssshhhhh
5	3	32	6	sssshhhh
6	2	64	2	ssssshh

Annak érdekében, hogy szemmel is viszonylag könnyen be lehessen határolni egy IP címet pontosan, egy külön jelölést vezettek be: a cím után odaírják egy perjellel elválasztva, hogy hány bit alkotja a hálózatot (és alhálózatot), pl. 192.168.11.24/26 – ez azt jelenti, hogy 24 a hálózat, 2 az alhálózat, és 6 a hosztok címére szánt bitek száma.
Az alhálózatra bontás a technikájával nem csak a címeket osztottuk fel, hanem létrehoztunk mindegyik tartományban újabb különleges címeket is, mint például a hálózatot jelölő csupa nullás, vagy a szórási cím csupa egyes címei.
Például a lenti ábrán jól látszik, hogy például a szórási cím utolsó oktettje a 0 alhálózat esetén 127, mivel binárisan ábrázolva 01111111 lesz, amiből az első az alhálózat, a többi pedig a host címe, és ez utóbbit számítjuk csak.

Címzési séma: példa két hálózatra

Alhálózat	Hálózatcím	Állomáscímek tartománya	Szórási cím
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Hálózati és alhálózati maszkok

Azt eddig még nem tárgyaltuk, hogy egy router hogyan tudja megmondani egy IP címről, hogy az melyik hálózatba, vagy ami nehezebb, melyik alhálózatba tartozik.
Az első probléma egyszerűen megoldható, hiszen egy címről, ha nincsenek alhálózatot jelölő bitek, akkor egyszerűen adódik, hogy melyik hálózathoz tartozik, hiszen az első oktettje alapján meg lehet mondani. Viszont az alhálózatok esetén már trükkösebb a helyzet, hiszen itt a host mezőinek egyes értékeit is felhasználjuk, ami alaphelyzetben nem látszik. Ezért vezették be az alhálózati maszkokat. Ezek olyan „címek”, amelyek hálózati és alhálózati részén

csupa egyes szerepel, így egy adott IP címen, és a maszkon végrehajtott logikai ÉS művelettel könnyen kinyerhetjük az alhálózathoz tartozó biteket.
Az alábbi ábrán ez a művelet látható:

```
1100100 01110100 00001101 01101011
1111111 11111111 11111111 11000000
-----------------------------------
1100100 01110100 00001101 01000000
```

Decimális ábrázolásban:

```
100.116.13.107
255.255.255.192
---------------
100.116.13.64
```

IPv6 fejrész

Pár évvel ezelőtt még csak cikkek jelentek meg arról, hogy hamarosan elfogynak a címek. Ma ez viszont már valóság, néhány későbbre fenntartott osztályon kívül kiosztottak minden IPv4 címet. Ezt a veszélyt még az IETF az 1990-ben felismerte, és elkezdte kidolgozni az IPv4 egy újabb verzióját, amely ezeket a gondokat megoldja, valamint rugalmasabb és hatékonyabb is. A fő célok a következők voltak:

1. Több milliárd hoszt támogatása még nem hatékony címtartomány-hozzárendelés árán is, ezen javítani kell.
2. A forgalomirányító táblázatok méretének csökkentése (ezekről bővebben később, a forgalomirányításról szóló gyakorlaton fogunk tanulni).
3. A protokoll egyszerűsítése, lehetővé téve ezzel a routereknek a csomagok gyorsabb feldolgozását.
4. A jelenlegi IP-nél jobb biztonság (hitelesítés és titkosítás) biztosítása.
5. Nagyobb figyelem szentelése a szolgáltatás típusának, különösen a valós idejű adatoknál.
6. A többesküldés segítése, hatósugarak megadásának lehetővé tételével.
7. Lehetőség arra, hogy egy hoszt a címének megváltoztatása nélkül barangoljon (ezt is később a NAT technológiánál fogjuk venni)
8. A protokoll fejlődésének lehetővé tétele.
9. Az új és régi protokoll még évekig egymás mellett létezhessen.

A protokollt az RFC 1883 szabvány specifikálja. Az alábbi ábrán az IPv6 fejrészét láthatjuk:

<table>
<tr><th colspan="2">0-7 bitek</th><th colspan="2">8-15 bitek</th><th colspan="2">16-23 bitek</th><th>24-31 bitek</th></tr>
<tr><td>Verzió</td><td colspan="2">Forgalmi osztály</td><td colspan="4">Folyamcímke</td></tr>
<tr><td colspan="4">Adatmező hossza</td><td colspan="2">Következő fejrész</td><td>Átugrás korlát</td></tr>
<tr><td colspan="7">Forráscím
(16 bájt)</td></tr>
<tr><td colspan="7">Célcím
(16 bájt)</td></tr>
</table>

Az első mező, a **Verzió** (Version), amely megegyezik az IPv4 Verzió mezőjével, csak itt a 6-os konstans szerepel.
A **Forgalmi osztály** (Traffic Class) mezőt arra használják, hogy a különböző valós idejű szállítási követelményekkel rendelkező csomagok között különbséget tegyenek. Az IP-ben kezdettől fogva volt már ilyen mező – ld. *Szolgáltatás típusa*, de a routerek nem nagyon használták ki.
A **Folyamcímke** (Flow Label) mezőt majd arra lehet használni, hogy egy forrás és egy cél között felállíthasson egy álösszeköttetést bizonyos tulajdonságokkal és igényekkel. Például egy bizonyos hoszt bizonyos folyamatától egy bizonyos célhoszt bizonyos folyamataíg tartó csomagfolyamnak szigorú késleltetési igényei lehetnek, és ezért fenntartott sávszélességre van szüksége. A folyamot előre fel lehet állítani, és egy azonosítót adni neki. Tulajdonképpen ez egy kísérlet arra, hogy mind a datagram alapú hálózatok rugalmassága, mind a virtuális áramkör alapú hálózat adta garanciák együtt legyenek.
Az **Adatmező hossza** (Payload Length) mező megmondja, hogy mennyi bájt következik ezután a mező után. A jelentése megváltozott az IPv4 *Teljes hossz* mezőjéhez képest, hiszen itt az első 40 bájtot már nem számolják bele a mező értékébe.
Lehetnek opcionális fejrészek. A **Következő fejrész** (Next Header) mező mondja meg, hogy a hat kiegészítő fejrész közül melyik következik. Ha a fejrész az utolsó IP-fejrész, akkor a mező azt mondja meg, hogy melyik szállítási protokoll kezelőjének (TCP, UDP, stb.) kell a csomagot továbbítani.
Az **Átugráskorlát** (Hop Limit) gátolja meg a csomagokat abban, hogy örökké élhessenek. Ez gyakorlatilag ugyan az, mint az *Élettartam* volt az IPv4-ben.
Ezek után következnek a **Forrás címe** (Source Address) és a **Cél címe** (Destination Address) mezők, amelyek egy-egy 16 bájtos (128 bites) címet takarnak. Az IPv6 címeket nyolc darab, 4 hexadecimális számjegyből álló, kettősponttal elválasztott sorozatként jelöljük:
8000:0000:0000:0123:4567:89AB:CDEF
A címek jelölése megengedi, hogy a nullákat elhagyjuk belőle, így egyes helyeken például 8:::123:4567:89AB:CDEF alakban is találkozhatunk velük, illetve a kettőspontok helyett sima pontok is szerepelhetnek.

DHCP

Az eddigi órákon mindig kézzel osztottuk ki az IP címeket. Viszont az könnyen beismerhető, hogy nagyobb méretekben ez a helyzet tarthatatlan, hiszen több szár vagy ezer gépet nem lehet bekonfigurálni úgy, hogy biztosan minden gépnek egyedi címet adjunk. Ezek után ott van az is, hogy ha a gépek egy része inaktív, akkor az ő címüket addig más is használhatná, valamennyivel megnövelve így a hálózat kapacitását.
Ezt a DHCP protokoll (Dynamic Host Configuration Protocol) képes nekünk megtenni. A protokoll képes kezelni, hogy az inaktív címeket újra kiossza, illetve azt is, hogy csak egy bizonyos tartományt használjon fel a dinamikus címek használatára. Ez nagy mértékben leveszi a terhet a vállunkról.
Az órán nem fogunk a továbbiakban foglalkozni ezzel a protokollal (talán egy későbbi órán megnézzük, hogyan kell Packet Tracerben konfigurálni).

Hálózat tervezés Packet Tracerben

A lenti ábrán adott egy hálózat, amely demonstrálja az IP címkiosztást. Segíthet a címek tervezésében az ezen a linken található kalkulátor. Továbbá, az alábbi hálózat az itt található videók alapján készült egy pár kisebb módosítással:

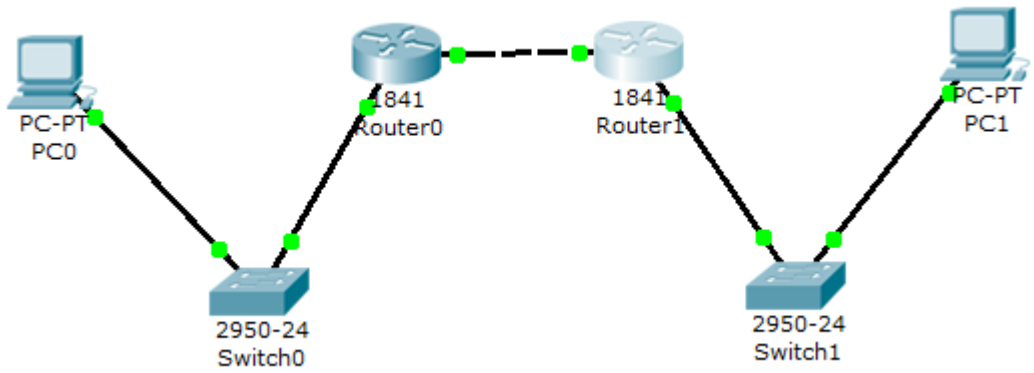
1. rész: http://www.youtube.com/watch?v=ta7130b_oA0
2. rész: http://www.youtube.com/watch?v=iGTMbUGgaKU
3. rész: http://www.youtube.com/watch?v=GLM8IayZ5P8

Szükséges lépések

1. Tervezzük meg a hálózatunk vázlatát akár papíron, akár Packet Tracerben, és döntsük el, hogy hány alhálózatra van szükségünk.
2. Írjuk le, hogy hogyan fognak kinézni az IP címek, mi lesz az alhálózati maszk, illetve milyen részekre darabolják a hostok címtartományát.
3. Tervezzük meg a hálózaton az egyes interfészek portjainak kiosztását.
4. Építsük meg, és konfiguráljuk a hálózatot. Ha nagy hálózattal találkozunk, azt is bontsuk részekre, és úgy implementáljuk.

A hálózat tervezett felépítése

A mostani példánkban két router lesz statikus routolással összekötve, és mindkét routerhez a másik portján egy-egy switchen keresztül gépek csatlakoznak. A hálózat tervezett felépítése az alábbi ábrán látható.



Ahhoz, hogy a hálózatunk megfelelően, statikus routolást is majd be kell állítani. Itt effektíve három alhálózatra lesz szükségünk:

- PC0 és Router0 között
- Router0 és Router1 között
- Router1 és PC1 között

Ezért két bitet fogunk felhasználni az alhálózatok számára, mivel két biten négy alhálózatot meg tudunk címezni, ezek pedig: 00, 01, 10, 11.

Az alhálózatok kiosztása

A hálózatunk legyen C osztályú, ami azt jelenti, hogy összesen 8 bit használható fel az egyes állomások címzésére. Ebből kettő bit lesz az alhálózat azonosítója. Végső soron egy általános IP címünk a következő lesz:

192.168.1.2/26

Amely tehát azt jelenti, hogy egy C osztályos IP cím, amely két extra bitet foglal el az alhálózatok címzésére, így összesen 26 bit jut a hálózatunk jelölésére.
Az ehhez tartozó alhálózati maszk (255.255.255.192) bináris ábrázolása:

11111111 11111111 11111111 11000000

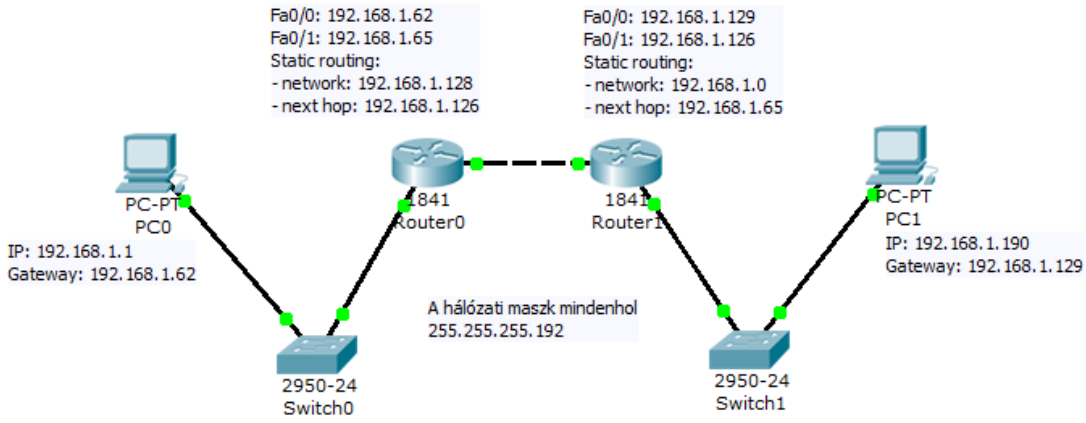
Ebből következően, mivel a legkisebb helyi értékű egyes értéke 64, így az egyes alhálózatok 64 gépet engednek meg. Más szavakkal a 0-255 tartományt 4 egyenlő részre osztjuk fel a négy alhálózat számára, így a következő intervallumokra bomlanak az alhálózatok hostjainak IP címei:

Alhálózat jelölő bitek	A meghatározott intervallum	Szórási cím	A hálózatot jelölő címek
00	0-63	63	0
01	64-127	127	64
10	128-191	191	128
11	192-255	255	192

Ahogy korábban is említettük, a különleges címeknél figyelembe kell venni az alhálózatokat. Tehát például a 64 azért lesz hálózatot jelölő cím, mert a bináris ábrázolása 01000000, ahol az első két számjegy az alhálózaté, amit ilyenkor nem veszünk figyelembe, viszont a hostoknál csupa nulla szerepel. Analóg módon, ha a 191-et ábrázoljuk, 10111111 jön ki, és itt is csak a hostokra eső helyi értékeket kell figyelembe venni.

A portok kiosztása és a megtervezett hálózat

Már csak az maradt hátra, hogy alkalmazzuk ezt a felépített hálózatunkra, illetve a statikus routolást beállítsuk. Az alábbi ábrán látható, hogyan kerültek kiosztásra az IP címek.



Az elején érdemes azt a megállapítást tennünk, hogy minden maszk, ahol ezt be kell állítani, 255.255.255.192. A routerek egymással az Fa0/1-es porton kapcsolódnak, a PC-k felé pedig a Fa0/0 úton mennek. A routerek statikus útvonalának beállításához szükséges parancsok:

- Router0-n:
  ```
  ip route 192.168.1.128 255.255.255.192 192.168.1.126
  ```
- Router1-en:
  ```
  ip route 192.168.1.0 255.255.255.192 192.168.1.65
  ```

Kérdések

1. Mire szolgál az IPv4 fejlécben a „Szolgáltatás típusa” mező?
2. Mi a szerepe a multicastnak?
3. Miket mondhatunk el a 10.0.0.1-es IP címről?
4. A 192.168.1.63/25 IP cím esetén hány alhálózat van?
5. Mit jelöl a 192.168.1.127/25 IP cím?
6. Mit jelöl a 192.168.1.63/25 IP cím?
7. Ha a hálózati maszk 255.255.224.0, akkor hány bitre terjed ki az alhálózat?
8. Melyik a helyes alhálózati maszk egy A osztályos cím esetén, ahol 5 alhálózati bitünk van?
9. Mit jelent a DHCP?
10. Mit jelent az IPv6 „Átugráskorlát” mezője?

Források

1. CISCO CCNA első és második szemeszterének tananyaga
2. Andrew S. Tanenbaum: Számítógép-Hálózatok