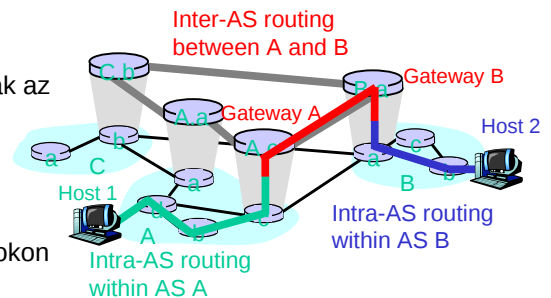


Számítógépes Hálózatok ősz 2006

10. Hálózati réteg – IP címzés, ARP, Circuit Switching, Packet Switching

Inter-AS-Routing

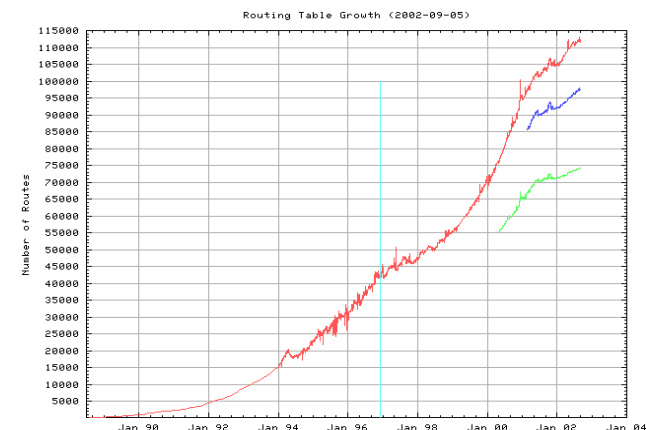
- Inter-AS-Routing nehéz...
 - Szervezetek megtagadhatják az üzenetek továbbítását (pl. csak fizető ügyfelek csomagjait továbbítja)
 - Politikai követelmények
 - Továbbítás más országokon keresztül?
 - Különböző AS-ek routing-metrikái sokszor nem összehasonlíthatók
 - Útvonal optimalizálás lehetetlen!
 - Inter-AS-Routing megpróbálja legalább a csomópontok elérhetőségét lehetővé tenni
 - Méret: inter-domain routereknek ma kb. 140.000 hálózatról kell tudni



Inter-AS routing: BGP (Border Gateway Protocol)

- Az inter-AS routing standard BGPv4
- Path Vector protokoll
 - Hasonló a Distance Vector protokollhoz
 - Minden Border Gateway meghirdeti minden szomszédjának (peers) az egész utat (AS-ek sorozata) a célig (advertisement)
 - TCP-t használ
- Amikor Gateway X az utat Z-hez Peer-Gateway W-nek küldi
 - akkor W választhatja ezt az utat, vagy éppen nem
 - Optimalizálási kritériumok:
 - költségek, politika, etc...
 - Ha W az X által meghirdetett utat választja, akkor meghirdeti
 - $\text{Path}(W,Z) = (W, \text{Path}(X,Z))$
- Megjegyzés
 - X tudja szabályozni a hozzá érkező forgalmat a meghirdetések által.
 - Komplikált protokoll

BGP routing tábla méret 1990-2002



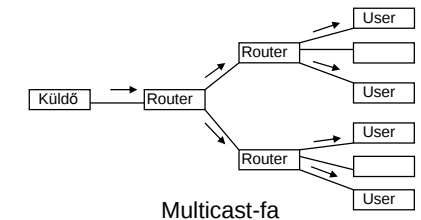
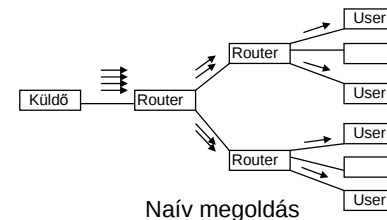
<http://www.mcvax.org/~jhma/routing/bgp-hist.html>

Broadcast és Multicast

- Broadcast routing
 - Egy csomagot (másolatot) minden más csomópontnak el kell küldeni
 - Megoldások:
 - A hálózat elárasztása (flooding)
 - Jobb: Konstruáljunk egy minimális feszítőfát
- Multicast routing
 - Az adatokat egy küldőtől egyidejűleg több fogadóhoz kell eljuttatni
 - Real time Streaming, Video-On-Demand,
 - Telefon-, Videokonferencia (all-to-all multicast),...
 - IP D címosztály:
 - Egy multicast-csoport (group) minden tagja ugyanazt a címet használja
 - Megoldások:
 - Optimális: Minimális Steiner Fa Probléma
 - NP-teljes (2-approximáció $O(n \log n)$ idő alatt kiszámítható!)
 - Más (nem-optimális) fát konstruálni

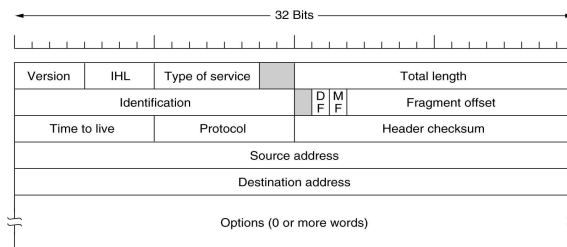
Multicasting

- Naív megoldás: Multicast-via-Unicast:
 - A küldő egy külön másolatot küld az adatokról minden fogadónak.
 - Nagyon inefficiens: A küldött csomagok száma sokkal nagyobb, mint ami szükséges lenne (különösen rossz all-to-all multicast esetén).
- Egy multicast-fa telepítése segítségével:
 - Minden linken csak egyszer továbbítódik egy csomag.
 - A routerek döntenek el, hogy egy csomagot több linken is továbbítanak-e.



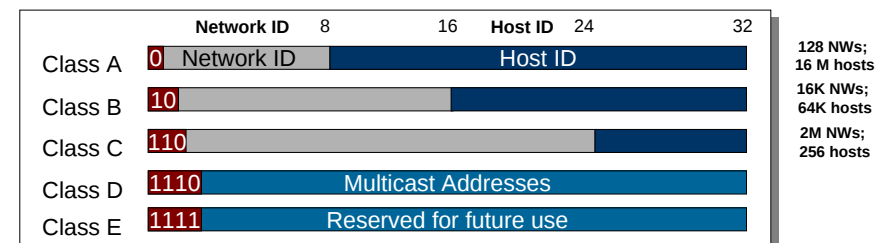
IPv4-Header (RFC 791)

- Version: 4 = IPv4
- IHL: fejléc hossz
 - 32 bites szavakban (>5)
- Type of Service
 - Optimalizálás „delay”, „throughput”, „reliability”, „monetary cost” szerint
- Checksum (csak a fejlécnek)
- Source és destination IP cím
- Protocol: azonosítja a megfelelő protokollt
 - pl. TCP, UDP, ICMP, IGMP
- Time to Live (TTL):
 - maximális hop szám



IPv4 címek

- Osztály alapú címzés (1993-ig)
 - 5 fix osztály, melyek mindegyikét egy prefix azonosítja
 - A, B, C osztály: fix hosszúságú hálózat prefix és host-ID
 - D a multicast osztály; E: lefoglalt



IPv4 címek

- Problémák:
 - A és B osztályú hálózatok sok állomást tartalmazhatnak, ami
 - a routerek számára nehezen kezelhető → **subnetting**
 - Elfogynak a címek: a címosztályok sok címet pazarolnak el
 - pl. egy szervezetnek 1000 állomással már B címosztályra lenne szüksége, ami elpazarol $64K - 2K = 62K$ címet → **classless addressing**

IPv4 címek -- Subnetting

- Képzeliünk el egy szervezetet, amely B címosztállyal rendelkezik és a szervezetben belül több LAN van (pl. Egyetem különböző Karai,...)
 - A központi routernek nem kell tudni minden állomásról, csak az egyes LAN-ok egy routeréről → új hierarchiaszint
- Subnetting
 - Bevezetünk alhálózatokat (subnet), melyeket az IP host-részéről leválasztott bitek azonosítanak (a hálózaton kívülről nem látható!)
 - A lokális routereknek tudni kell, hol van ez a leválasztás: ez a **subnet mask** által adható meg

Network		Host	
Network	Subnet	Host	
1111..	..1111	00000000	Mask

- Pl.: a subnet mask 11111111.11111111.11111111.00000000 azt jelenti, hogy
 - az IP cím 10000100.11100110.10010110.11110011
 - a 10000100.11100110 hálózatban a 10010110 alhálózatban
 - a 11110011 host-ot azonosítja

IPv4 címek -- Classless Inter Domain Routing (CIDR) (RFC 1519)

- A címosztályok nagyon sok IP címet pazarolnak
- 1993 óta: Classless Inter Domain Routing (CIDR)
 - A hálózat cím és a host-ID hossza szabadon adható meg hálózati maszk által.
 - Pl.: hálózati maszk 11111111.11111111.11111111.00000000
 - az IP cím 10000100.11100110.10010110.11110011
 - a 10000100.11100110.10010110 hálózatban
 - a 11110011 host-ot azonosítja
 - Ezek valódi hálózatokat jelentenek amit a többi router is lát – a subnetting-gel ellentétben
 - az IP csomagokba nem kell kiegészítés
 - többi routernek a kezelni kell ezeket a változó hosszúságú hálózati címeket (forwarding és a routing algoritmus)

IPv4 címek -- CIDR

- Route aggregation
 - A BGP, RIP v2 és OSPF routing protokollok különböző hálózatokat egy prefix által kezelhetnek
 - Pl. minden hálózat, melynek a prefixe 10010101010* az X szomszédos routeren keresztül érhető el

IP cím lefordítása MAC címre: ARP (RFC 826)

- Address Resolution Protocol (ARP)
- IP cím MAC címre fordítása
 - Broadcast a LAN-ban, lekérdezni azt, hogy melyik állomáshoz tartozik az adott IP cím
 - Csak az a csomópont válaszol, amelyhez az IP tartozik, a MAC címmel
 - A router akkor a csomagot oda ki tudja szállítani

IPv6

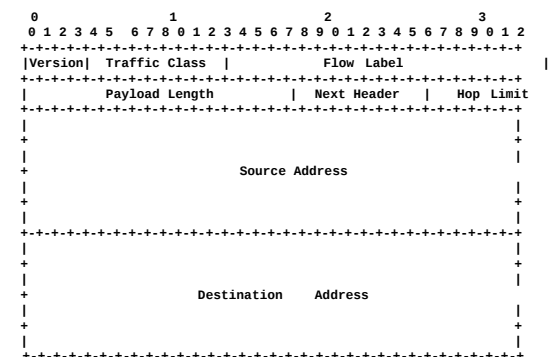
- 32 bites IP címek egyre szűkösebben állnak rendelkezésre
 - 4 milliárd ilyen IPv4 cím van (32 Bit) de
 - ezek statikusan hálózati és host-részre vannak osztva
 - címek mobil telefonoknak, hűtőszekrényeknek, autóknak, stb...
- Autokonfiguráció
 - DHCP, Mobile IP, átszámozás
- Új szolgáltatások
 - Biztonság (IPSec)
 - Quality of Service (QoS)
 - Multicast
- Egyszerűsítés a routernek
 - Nincs IP checksum
 - Nem partícionálja az IP csomagokat

A címek: DHCP

- DHCP (Dynamic Host Configuration Protocol)
 - Kézi hozzárendelés (hozzákötni a MAC címhez, pl. szervereknél)
 - Automatikus hozzárendelés (fix hozzárendelés, de nem előre beállított)
 - Dinamikus hozzárendelés (újrakiosztás lehetséges)
- Új számítógép kapcsolódása konfiguráció nélkül
 - A számítógép kér egy IP címet a DHCP szervertől
 - Az dinamikusan hozzárendel egy IP címet a számítógéphez
 - Miután a számítógép elhagyja a hálózatot, az IP cím újra kiosztható
 - Dinamikus hozzárendelés esetén az IP címeket „frissíteni” kell
 - Ha egy számítógép egy régi IP címet akar felhasználni, ami lejárt, vagy már újra ki van osztva
 - akkor a kéréseket vissza kell utasítani
- Probléma: IP címek lopása

IPv6-Header (RFC 2460)

- Version: 6 = IPv6
- Traffic Class
 - QoS-hez (prioritásokhoz)
- Flow Label
 - QoS-hez, valós idejű alkalmazásokhoz
- Payload Length
 - Az IP csomag fennmaradó részének (a datagramnak) a hossza
- Next Header (mint IPv4-ben):
 - pl. ICMP, IGMP, TCP, EGP, UDP, Multiplexing, ...
- Hop Limit (Time to Live)
 - Hop-ok max. száma
- Source Address
- Destination Address
 - 128 Bit IPv6-Adresse



IPsec – Security Architecture for the IP (RFC 2401)

- Biztonsági protokollok
 - Authentication Header (AH)
 - Biztosítja az adat küldőjének autentifikációját,
 - kapcsolat mentes adat integritást,
 - védelemet Replay-támadásokkal szemben
 - Encapsulating Security Payload (ESP)
 - IP fejléc titkosítás nélkül, adatok titkosítva, autentifikálással
- Kulcs management:
 - IKE (Internet Key Exchange) Protokoll
 - Egy Security Association létrehozása
 - Security szolgáltatásokkal védett simplex kapcsolat két állomás, vagy egy állomás és egy security gateway (router, amely támogatja IPsec-et), vagy két security gateway között
 - Identifikáció, kulcsok, hálózatok, megújítási időközök az autentifikációhoz és IPsec kulcsok rögzítése

IPsec

- IPsec transport üzemmódban (direkt kapcsolatokhoz)
 - IPsec fejléc az IP fejléc és az adatok között van
 - Megvizsgálják az IP routerek (azokban jelen kell lenni IPsec-nek)
- IPsec tunnel üzemmódban (ha legalább egy IPsec nélküli router között)
 - Az egész IP csomagot titkosítja és a IPsec fejléccel együtt egy új IP csomagba teszi
 - Csak a kapcsolat két végén kell hogy jelen legyen IPsec
- IPsec része az IPv6-nak
- porting IPv4-re létezik

Circuit Switching vagy Packet Switching

- Circuit Switching (vonali kapcsolás)
 - Egy kapcsolat létrehozása felhasználók között kapcsoló állomások által
 - vonalak explicit hozzárendelésével
 - vagy erőforrások explicit hozzárendelésével, pl. idő slots
 - Quality of Service egyszerű, kivéve a
 - kapcsolatfelépítés
 - Probléma
 - statikus hozzárendelés
 - a kommunikációs médium inefficiens kihasználása dinamikus terhelés esetén
 - Felhasználás
 - Telefon, telegráf, mobil telefon

Circuit Switching vagy Packet Switching

- Packet Switching (csomag kapcsolás)
 - Az IP alapelve
 - Az adatokat csomagokra osztja és a csomagokat küldő/fogadó információval ellátva egymástól függetlenül küldi
 - Probléma: Quality of Service
 - A kapcsolat minősége az egyes csomagoktól függ
 - A csomagok puffereződnek vagy el is veszhetnek
 - Előny:
 - A médium hatékony kihasználása dinamikus terhelés esetén
 - Összefoglalva
 - Packet Switching gyakorlatilag minden felhasználási területen felváltotta a Circuit Switching-et
 - Ok: a médium hatékony kihasználása