INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK ÉS ALKALMAZÁSOK

IPv6 alapok

Szabó Sándor
Bokor László
BME Híradástechnikai Tanszék
szabos@hit.bme.hu

2011. május 11.,
Budapest

Kivonat

- Miért nem elég az IPv4?
- Az IPv6-os fejléc
  - kiegészítő fejlécek
- IPv6 címzés
  - címzési típusok
  - ICMPv6
- Együttélés IPv4 vs. IPv6
  - dual stack
  - tunneling / encapsulation és NAT

Az IPv6 története

- Jelenleg IPv4 (1970-es évek elejéről)
  - Nagy tapasztalat (30++ év)
  - 1983 óta az Internet alapja
  - Folyamatos fejlesztés
- IPv6?
  - 1990-es évek elejétől szabványosítják
  - 1995 óta szabványos (draft)
  - Rengeteg hiányzó komponens
  - Kevés tapasztalat
  - Folyamatos fejlesztés

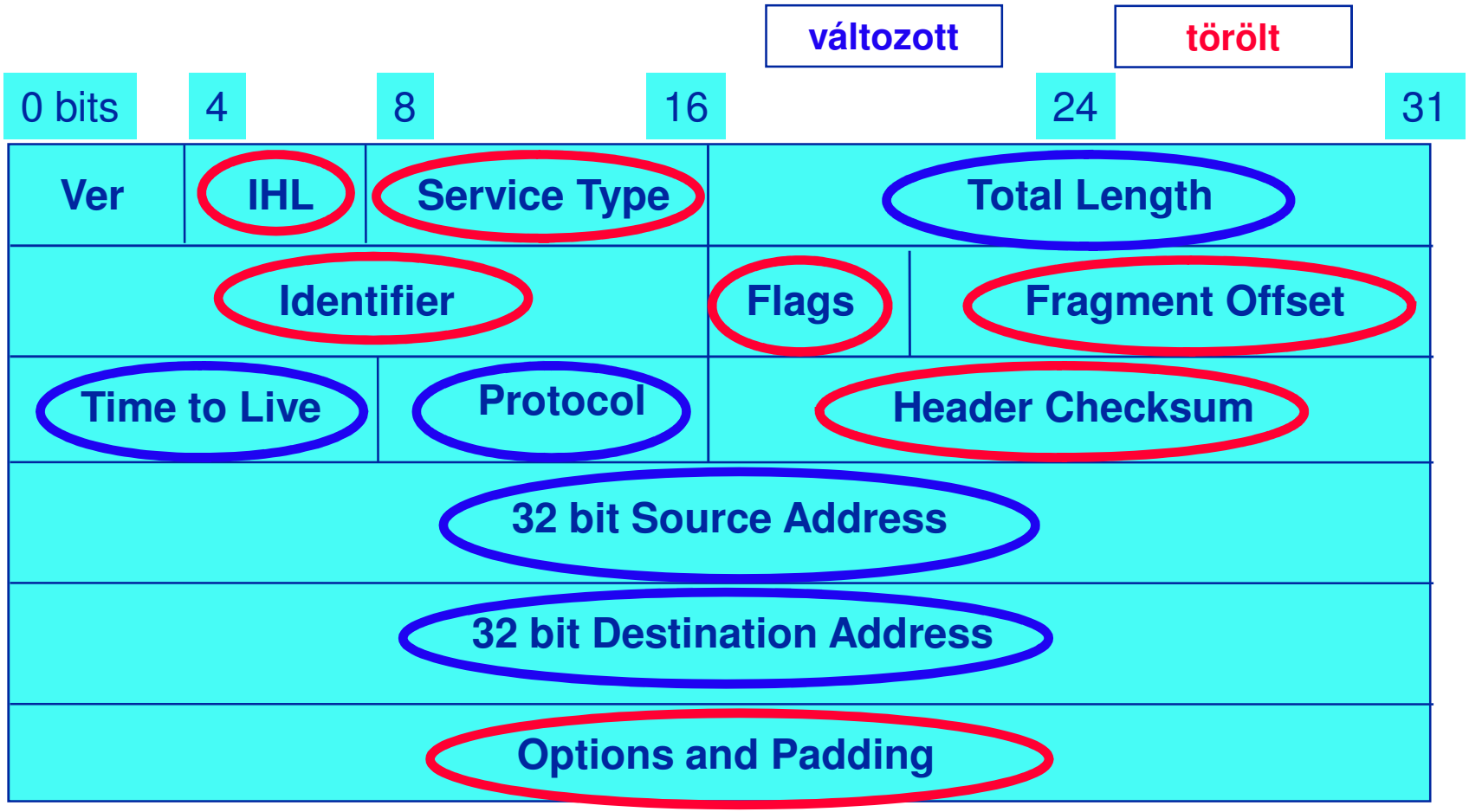
Az IPv6 újdonságai

- Kiterjesztett címtér
  - 128 bit, szemben az IPv4 32 bitjével
  - 6,65 10^{23} cím/m^2
- Állapotmentes auto-konfiguráció
- Egyszerűsített fejléc
  - összesen 40 byte (16+16+8)
  - gyorsabb feldolgozás
- Az opciók és kiterjesztések jobb kezelése
  - kiterjesztés fejlécek

Miért kell az IPv6?

- Az IPv4 korlátozott
  - 4,3 milliárd cím, 60% az USA-ban
  - egyre növekvő felhasználói populáció (pl. ADSL, mobil készülékek, játék konzolok)
  - KEVÉS CÍM (a NAT nem megoldás)
- Az IPv6 teret hódít
  - Japán, Korea, Kína, EU, India
  - Ausztrália, Taiwan, Szingapúr, Egyiptom
- Új szolgáltatások IPv6 felett
  - pl. mobilitás támogatás

IPv6 vs. IPv4 fejléc



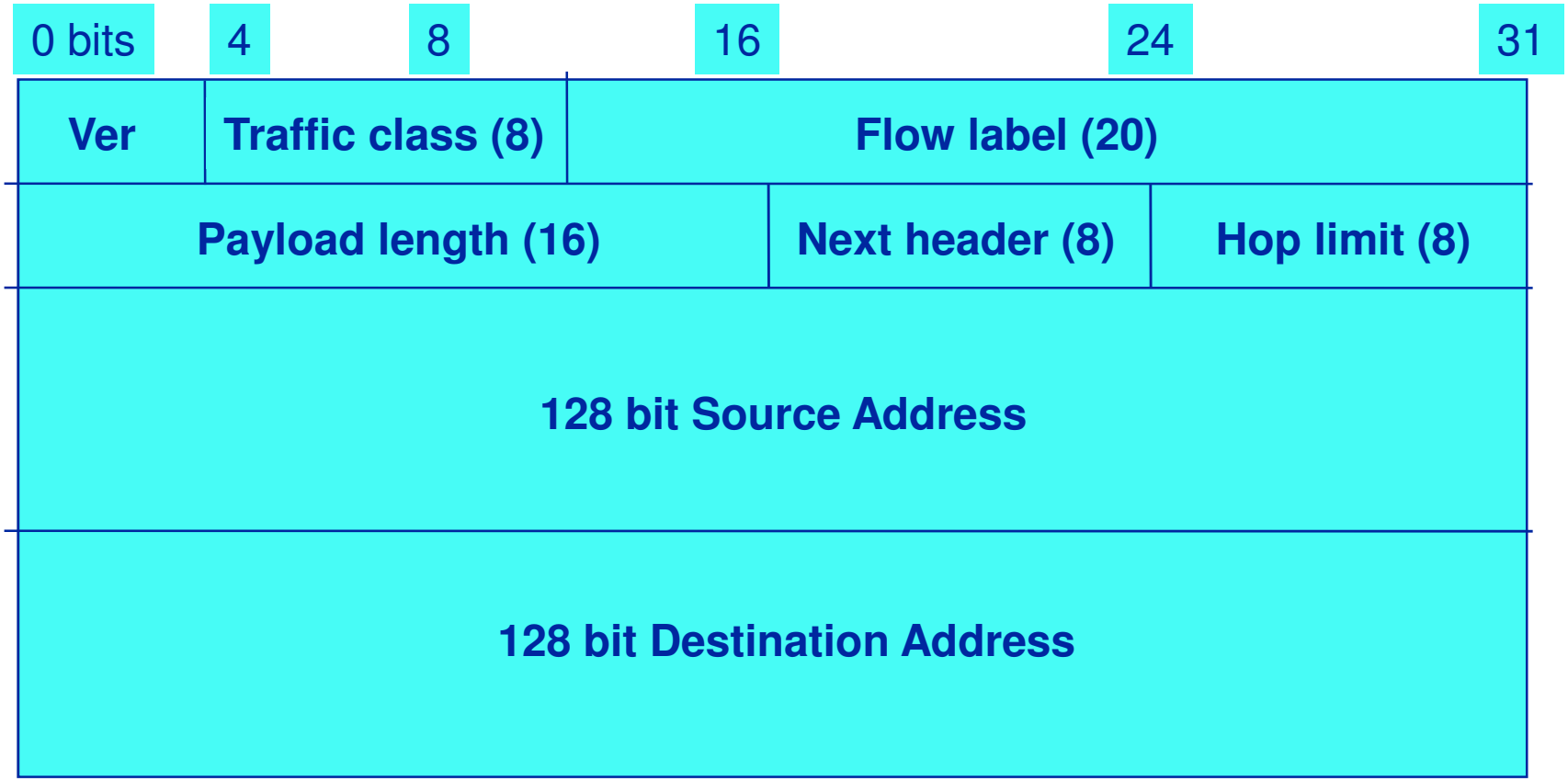
Az IPv6-os fejléc – ami eltűnt

- Az alábbi IPv4-es mezők tűntek el
  - Fejléc hossz (fix 40 byte)
  - Azonosító
  - Flags
  - Fragment offset
  - Fejléc ellenőrzőösszeg
- A középső három a töredezés kezeléshez volt szükséges, ami az IPv6-ban nem létezik
- Ellenőrzőösszeg = lassúság

Az IPv6-os fejléc – ami átalakult

- Type-of-Service =>
  forgalmi osztály (traffic class)
  - prioritások kezelése
- Protocol Type => Next header
  - TCP, UDP, de kiegészítő fejlécek is, lásd később
- Time To Live (TTL) => Hop Limit
- Címzett és feladó címe (hosszabb)
- Új mező: Folyam azonosító (flow label)
  - hatékonyabb csomagtovábbítás

Az IPv6-os fejléc



Az IPv6 kiegészítő fejlécei

- Ebben a sorrendben
  - Hop-by-Hop Options header (jumbogram)
  - Destination Options header (köztes célnál)
  - Routing header (routing type)
  - Fragment header
  - Authentication header
  - Encrypted Security Payload header
  - Destination Options header (végső célnál)
  - (Upper layer header)
- A “Next header” jelzi mi következik

Hop-by-hop options fejléc

- Minden opciós fejlécben:
  - Köv. fejléc, fejléc hossza, opciók
- Minden érintett node-nak fel kell dolgozza
  - Hop-by-hop = lépésről lépésre
- A jelenlegi egyetlen hop-by-hop: jumbogram
  - Jumbogram = nagyon nagy csomag
  - Alapból Payload length = 16 bit (max. 64 kbyte)
  - Így: 32 bit (max. 4 Gbyte)

Destination options fejléc

- Ez is egy opciós kiegészítő fejléc
  - Formátuma az opciós fejlécé
- A végállomásnak kell feldolgoznia
- Kétszer is előfordulhat
  - Ha a routing fejlécet is használjuk
  - Első (routing header előtti)
    - A routing headerben előírt állomások dolgozzák fel
  - Az utolsó (routing header utáni)
    - A célállomás dolgozza fel

Routing kiegészítő fejléc

- (IPv4-ben ez volt a Source routing option)
- Laza/szigorú útvonalmegjelölés
- A fejlécben:
  - Következő fejléc
  - Node-ok (címek) száma
  - Routing típus (laza/szigorú)
  - Hátralévő szegmensek száma (következő cím)
  - (Reserved)
  - Az érintendő állomások címei

Fragment kiegészítő fejléc

- Router nem töredezhet, csak a forrás
  - Ha jumbogram, akkor nem
- A fejlécben:
  - Következő fejléc
  - Reserved
  - Fragment offset (honnantól fragmentálunk)
    - pl. az IPv6-os fejléc nem darabolható
  - Azonosító (identification)
    - Hanyadik darabka

Authentication kiegészítő fejléc

- Autentikációs céllal (eredetiség)
  - Valóban a küldő küldte
  - Nem történt benne változás
- A fejlécben:
  - Köv. fejléc, payload length, reserved
  - SPI (Security Parameter Index)
  - Sorszám (Sequence number) – UDP esetén is!
  - Autentikációs adatok (Authentication data)

ESP kiegészítő fejléc

- Célja: titkosítás (bizalmasság)
  - csak az arra feljogosított tudja olvasni
- Fejlécben:
  - SPI
  - Sorszám (Sequence number)
  - Titkosított adatok (Encrypted data)
    (payload, padding, padding hossza, köv. fejléc)
  - Autentikációs adatok (Authentication data)
- Kétféle: szállító (transport) és alagút (tunnel)

IPv6 címzés – néhány számadat

- IPv4 – 32 bit
  - $2^{32} = 4{,}29\ 10^{9}$ darab cím (elvileg)
    - már több, mint 6,5 milliárd ember a Földön
  - összesen 2 113 389 darab hálózat
- IPv6 – 128 bit
  - $2^{128} = 3{,}4\ 10^{38}$ darab cím (elvileg)
    - $6{,}65\ 10^{23}$ darab cím/m^2
  - 2^{45} darab /48-as hálózat (global unicast 001)
    - $3{,}5\ 10^{15}$ darab hálózat
    - mindegyikből további 65 535 /64-es alhálózat

IPv6 cím típusok

- Címzett alapján
  - Unicast (egyes küldéses)
  - Multicast (többes küldéses)
  - Anycast
- Route-olhatóság alapján
  - globális (global)
  - nem globális (non-global)
    - link-local
    - egyedi lokális IPv6 cím (régen site-local)

IPv6 cím

- 128 bit = 8 x 16 bit hexadecimális formában
  pl. 2001:00B8:0000:0000:0002:B3FF:FE1E:8329
- Egyszerűsítési lehetőségek
  - Bevezető nullák elhagyása
    2001:B8:0:0:2:B3FF:FE1E:8329
  - Dupla kettőspont: csupa nullák helyettesítésére
    2001:B8::2:B3FF:FE1E:8329
    Csak egyszer lehet!
- Prefixek jelölése: IPv6 cím/prefix alakban
  - 2001:B8:0:56::/64

Nevezetes IPv6 címtartományok

- Kioszthatóó
  - 2000::/3 global unicast
  - FE80::/10 link-local unicast
  - FEC0::/10 korábbi site-local
    - már nem használatos
  - FC00::/7 lokális egyedi IPv6 címek
  - FF00::/8 multicast
- Speciális
  - :: unspecified address (mint 0.0.0.0 az IPv4-ben)
  - ::1 loopback

IPv4 és IPv6 keveréke – címzés

- IPv6-ba ágyazott IPv4 cím (elavult)
  - IPv4 kompatibilis IPv6 cím ::ipv4_cím
    pl. 62.2.84.115-ből: ::3e02:5473
- IPv6-ra leképzett IPv4 cím ::FFFF:ipv4_cím
  - manapság ez az általánosan elterjedt és használt
    pl. 62.2.84.115-ből: ::ffff:3e02:5473
- 6to4 cím 2002:public_ipv4_cím::/48
- ISATAP címek
  - dual stack node-ok között IPv4 felett
- Teredo címek (NAT mögött)

Globális unicast címek

- Bináris 001-gyel kezdődnek (2000::/3)
- *n* bit a globális route-olhatósági prefix (pl. földrajzi pozíció alapján)
- 64-*n* bit alhálózati azonosító
- 64 bit interfész azonosító
- Pl. Műegyetem:
  - Egyetemi szinten: 2001:738::/32
  - pl. Híradástechnikai Tanszék:

Lokális IPv6 címek

- Link-local: soha nem szabad route-olni
  - nem kell hozzá semmilyen beállítás
  - ad-hoc hálózatok, router nélküli hálózatok esetén ideális, vagy szomszéd felderítéshez
- Alakja: FE80::[64_bitnyi_Interface_ID]
  - Pl. ha az Ethernet kártya hardver címe 00:1A:6B:3A:9F:BC, akkor a link-local cím FE80::21A:6BFF:FE3A:9FBC lesz
- Egyedi lokális IPv6 címek:
  - FC[40_bit_global_ID]:[16_bit_subnet_ID]:[64_bitnyi_Interface_ID]

Anycast címek

- A nagy terhelésű eszközökhöz találták ki
  - számítógépek egy csoportjából egyetlen (tipikusan a legközelebbi) állomást címzi
- Az unicast tartományból szabadon
- Subnet-router anycast
  - [n_bitnyi_subnet_prefix]:[128-n_bitnyi_0]
  - az első router fogja feldolgozni a linken
- Reserved address anycast cím
  - Az utolsó 7 biten, pl. 126 (7E): mobil IPv6 Home-Agent anycast

Multicast címek

- FF[0RPT][4_bitnyi_scope][Csoport_ID]
  - 0RPT flagek (bitek)
    - R=0 Randevú pont nincs beágyazva
    - P=0 Multicast cím prefix infó nélkül
    - T=0 Jól ismert multicast cím (1: ideiglenes)
  - Scope példák
    - 1: Interface-local scope
    - 2: Link-local scope
    - 5: Site-local scope
    - E: Global scope

Multicast cím példák

- Minden node
  - a küldővel azonos linken FF02::1
  - a küldővel azonos site-on FF05::1
- Minden router
  - a küldővel azonos linken FF02::2
  - a küldővel azonos site-on FF05::2
- Minden DHCP ügyfél FF02::1:2
- Minden DHCP szerver FF05::1:3
- Minden NTP szerver
  - a küldővel azonos site-on FF05::101
  - az Interneten FF0E::101

Cím választás

- Az IPv6 természeténél fogva több cím létét is lehetővé teszi, melyek különbözhetnek
  - scope-jukban (link-local, global)
  - állapotukban (elsőbbségi, érvénytelenített)
- Melyiket használjuk?
  - létezik ajánlás erre nézve (RFC 3484)
  - azonos scope, vagy a kisebb scope
  - elsőbbségi
  - 6to4, vagy ISATAP helyett natív, ha van
  - a leghosszabb prefix egyezésű

Internet Control Message Protocol 6-os verzió (ICMPv6)

- Sokkal fejlettebb, mint az ICMPv4
  - Multicast management (IGMP helyett)
  - Neighbor Discovery (ARP, RARP helyett)
    - a szomszéd állomások, routerek, elérhető szomszédok és változó adatkapcsolati címek feltérképezésére
  - Echo request/echo reply (ping)
  - Packet too big (fragment fejlécek helyett)
- Két típusú üzenet
  - hiba
  - információs

ICMPv6 hibaüzenetek

- Címzett elérhetetlen (destination unreachable)
  - ha az IP datagram nem továbbítható
    - Nincs route a célhoz, cím/port elérhetetlen, adminisztratíve tiltott
- Túl nagy csomag (Packet Too Big)
  - az MTU a köv. linken kisebb a csomagméretnél
- Lejárt az idő (Time Exceeded)
  - ha a hop számláló nullára csökkent
- Paraméter probléma (Parameter problem)
  - ha valamelyik paraméter nem értelmezhető

ICMPv6 információs üzenetek

- Echo request / echo reply
- multicast felderítő üzenetek
  - router
  - listener
- router felderítő (router discovery)
- szomszéd felderítő (neighbor discovery)
- hálózat újraszámozás (router renumbering)
- mobilitás támogatáshoz kapcsolódó üzenetek
  - Részletesen lásd a későbbi előadásokon

ICMPv6: echo request és reply

- Ugyanúgy, mint az ICMPv4-nél
- Az „echo request” üzenet adatát az „echo reply” üzenetbe kell másolni
- A ping6 alkalmazás is ezt használja

ICMPv6 – Neighbor Discovery

- Feladatai
  - Cím automatikus konfigurálása (autoconf.)
  - network prefix, router automatikus felderítése
  - duplikált IP cím érzékelés
  - MAC cím felderítés
  - Szomszédos routerek felderítése
  - A nem elérhető szomszédok azonosítása (NUD)
  - MAC cím váltások érzékelése
- Router solicitation és router advertisement

ICMPv6: Router felderítés

- Két üzenet
  - Router advertisement (router információk)
  - Router solicitation (az előbbi kikényszerítése)
- Ami a router advertisement üzenetben jön:
  - Current Hop limit (ajánlás a hop limitre)
  - Autoconfig flags (DHCP, vagy más stateful)
  - Router lifetime (meddig elérhető a router, s)
  - Reachable time (szomszédok vonatkozásában)
  - Retransmission timer (szomszéd üdvözlésre)
  - Options (MAC cím, MTU, network prefix)

ICMPv6: Neighbor Discovery

- Neighbor solicitation és advertisement
  - MAC cím feloldás (IPv4-ben ARP volt)
  - A szomszédok elérhetőségének azonosítása
  - Duplikált IP címek azonosítása
- ICMP redirect
- Inverse Neighbor Discovery (IND)
  - IPv4-ben ez volt a RARP
- Sebezhetőség, biztonság
  - SEcure ND (SEND)

ICMPv6 példa: Szomszéd kérelmezés

- A neighbor solicitation üzenetben jön:
  - Típus: 135
  - Kód (code): nem használjuk
  - Checksum
  - Reserved
  - Célcím (target address): aminek a MAC címét fel akarjuk oldani
  - Options: pl. source link-layer address: a küldő MAC címe

ICMPv6 – Autoconfiguration

- Két típus: stateless és stateful
  - Stateful = DHCP az IPv4-ben
    hívják: ~ autoconfiguration, ~ DHCP
  - Stateless: hálózati prefix alapján
    - vagy MAC cím, vagy random ID
    - duplikált címek szűrése DAD-del
- A kettő kombinálható
  - pl. stateless a címhez
  - stateful a DNS-ek címéért

Az autokonfiguráció lépései

- Stateless = semmiből indul,
- Lépések:
  - Link-local cím generálása (MAC cím alapján)
  - Link-local cím egyediség tesztje (ND-vel)
    - Ha OK, akkor tovább, ha nem OK, akkor vissza
  - Link-local cím beállítása az interfészen
  - Kapcsolatba lépés a routerrel (R.Sol., R.Adv.)
  - Router direction (ha stateful: DHCP server címe)
  - Globális cím konfiguráció (DHCP, vagy R.adv.)

ICMPv6: Router renumbering

- Alhálózatok prefixeinek átírására szolgál
  - A hálózati adminisztrációt könnyíti
  - Természetesen követelmény az autentikáció
  - Sorszámozás a régebbi, keringő üzenetek ellen
- Két üzenet:
  - Router renumbering command
  - Router renumbering result
- Match prefix part => use prefix part
  - A régi prefixből így lesz új

ICMPv6 – Path MTU discovery

- Az IPv6-nál nincs fragmentálás
- Ha a csomag nagy (> MTU):
  - eldobja a router
  - küld egy ICMPv6 üzenetet a forrásnak (PTB)
    - A PTB tartalmazza a következő link MTU-ját
- Módszer:
  - küldjünk echo requestet a címre
  - kezdjünk nagy MTU-val, majd lépdeljünk lefelé
  - az új MTU-val próbálkozik
    - soha nem megy 1280 byte alá
  - GOTO eleje

ICMPv6 – Multicasting

- Multicast Listener Discovery
- Multicast Router Discovery

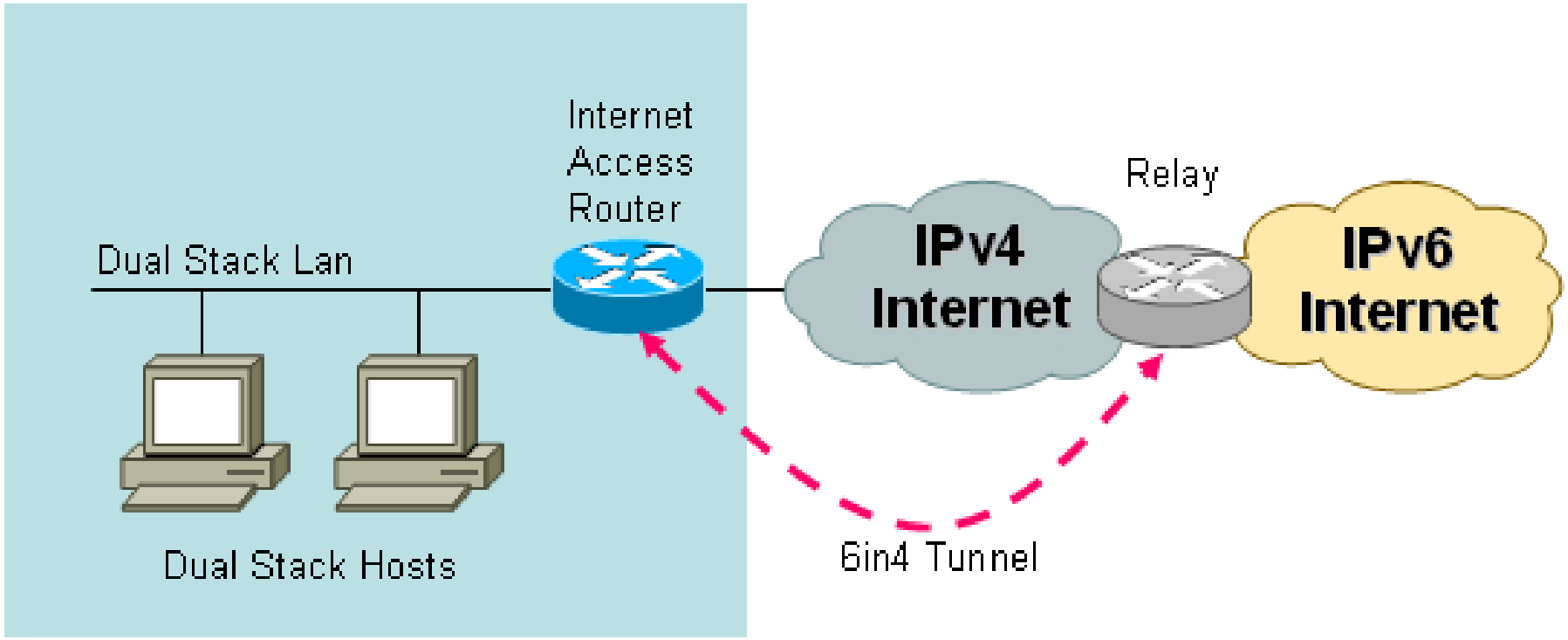
Együttműködés, migráció

- Az IPv4 és az IPv6 sokáig együtt fog élni egymás mellett
  - IPv4 világ kész, az IPv6 világ most épül
- Három módszer
  - kettős protokoll stack (dual stack)
  - alagút (tunneling, vagy encapsulation)
    - IPv6 szigetek összekötése IPv4 felett
  - fordítás (translation)
    - IPv6 hosztok kommunikációja IPv4 hosztokkal
- A fentiek kombinálhatóak is

Dual stack

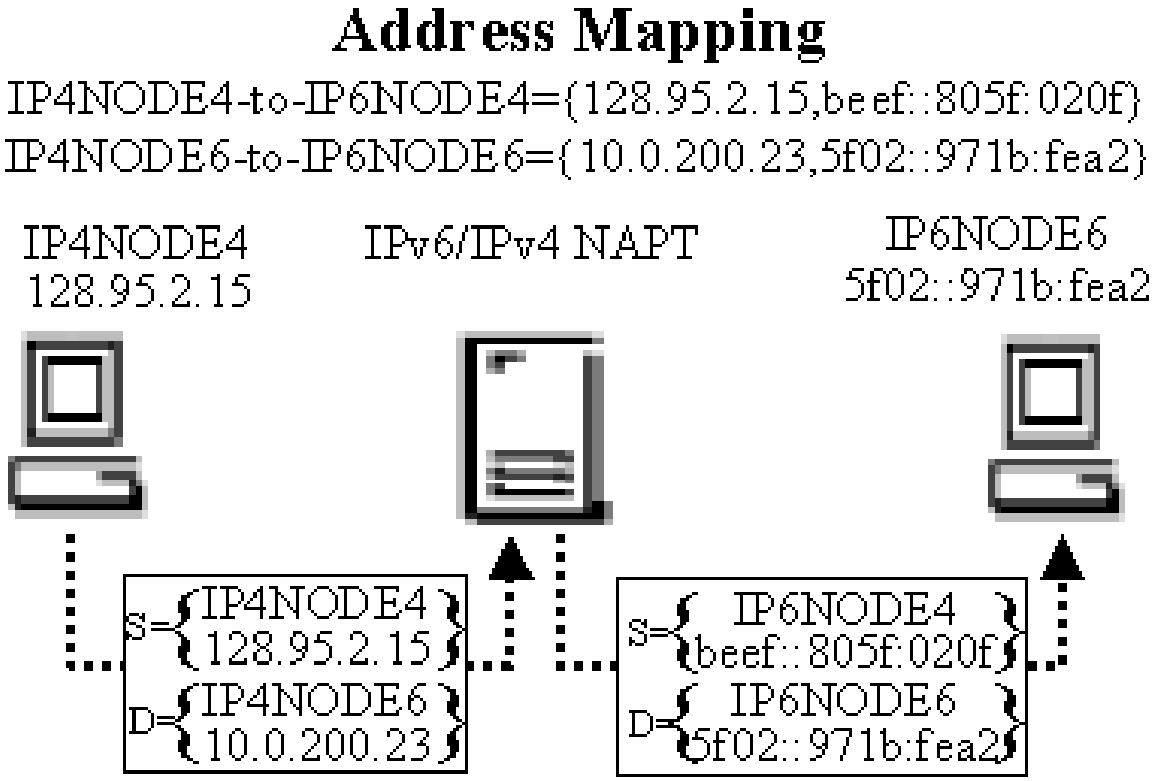
- A legáltalánosabb megoldás manapság
  - mind IPv4, mind IPv6 felett működni képes
  - routereken és hosztokon
- DNS
  - A rekord az IPv4-es címre
  - AAAA rekord az IPv6-os címre
- Automatikusan azt használja, ami elérhető
  - IPv4-es hosztokkal IPv4 felett, 6-ossal 6 felett
  - pl. a Linux, ha lehet, az IPv6-ot preferálja

Tunneling/encapsulation



Hálózati cím és protokoll fordítás

- A már korábban tárgyalt NAT kiterjesztése
  - IPv6-os címeket IPv4-esre fordítunk és fordítva



Hivatkozások

- RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture, http://www.ietf.org/rfc/rfc3513.txt
- RFC 2894: Router Renumbering for IPv6, http://www.ietf.org/rfc/rfc2894.txt
- RFC 2461: Neighbor Discovery for IP Version 6 (IPv6), http://www.ietf.org/rfc/rfc2461.txt
- RFC 2462:IPv6 Stateless Address Autoconfiguration, http://www.ietf.org/rfc/rfc2462.txt
- RFC 1897: IPv6 Testing Address Allocation, http://www.ietf.org/rfc/rfc1897.txt
- RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, http://www.ietf.org/rfc/rfc3041.txt

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Híradástechnikai Tanszék

Szabó Sándor
Bokor László
BME Híradástechnikai Tanszék
szabos@hit.bme.hu