HOGYAN VEZESSÜK BE HÁLÓZATUNKON AZ IPV6-OT?

Mohácsi János
NIIF Intézet

Miért van szükség rá?

A jelenlegi Internet Protokoll (4. verzió) hatalmas méretű növekedést tett lehetővé

Új problémák merültek fel:

- 1. Az IP címtartomány szűkössé vált
- 2. Relatíve nehézkes konfiguráció és működtetés
- 3. Biztonság hiánya
- 4. Minőségi paraméterek kezelése (hang, videó)
- 5. Új, és nagyteljesítményű hálózati technológiák
- 6. Mobilitás szükségessége
- 7. Gazdaságtalan routing (címzés, BGP, stb.)

IP címek szűkössége

Internetes eszközök széleskörű elterjedése

- Okos mobil telefonok, tabletek
- Inteligens autók
- Inteligens grid-ek
- Fogyasztói elektronikai eszközök

Új növekvő populációk

- Kína, Dél-Korea, Japán, India, Oroszország, Afrika

Új "folyamatos" Internet hozzáférések

- Kábel, xDSL, Ethernet házig, WLAN, Smart Grid-ek

Új Internet alkalmazások - nehéz vagy lehetetlen NAT-al működtetni

- Hálózatos játékok, Internet telefónia/videokonferencia, Üzenetküldési szolgáltatások, peer-to-peer paradigmák

NAT kiváltása, hogy a hálózat robosztusabb, biztonságosabb, gyorsabb, menedzselhetőbb legyen

IP történelem

1983 : Kutatási hálózat ~ 100 számítógép

1992 : Kereskedelmi tevékenység

- Exponenciális növekedés

1993 : class B címek elfogytak

- Hálózat összeomlásának jóslatai 1994-re!

Szükség megoldások

B osztály méretű csak különleges esetekben

C osztály újraosztályozott használata

Classless Internet Domain Routing (CIDR)

- RFC 1519
- hálózati cím = [prefix/prefix hossza]
- Kisebb veszteség
- Lehetővé teszi az aggregációt

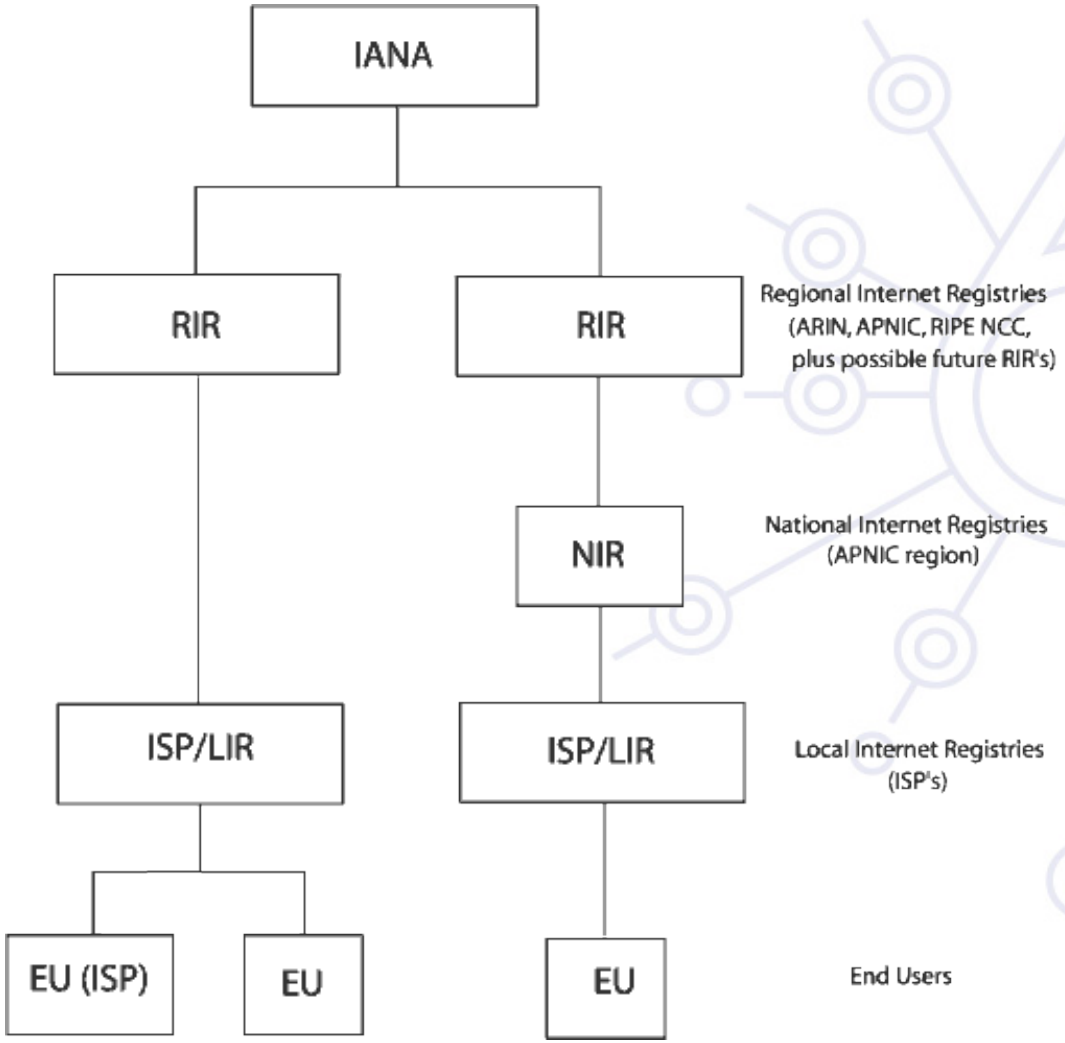
Privát címek

- RFC 1918 (BCP)
- 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

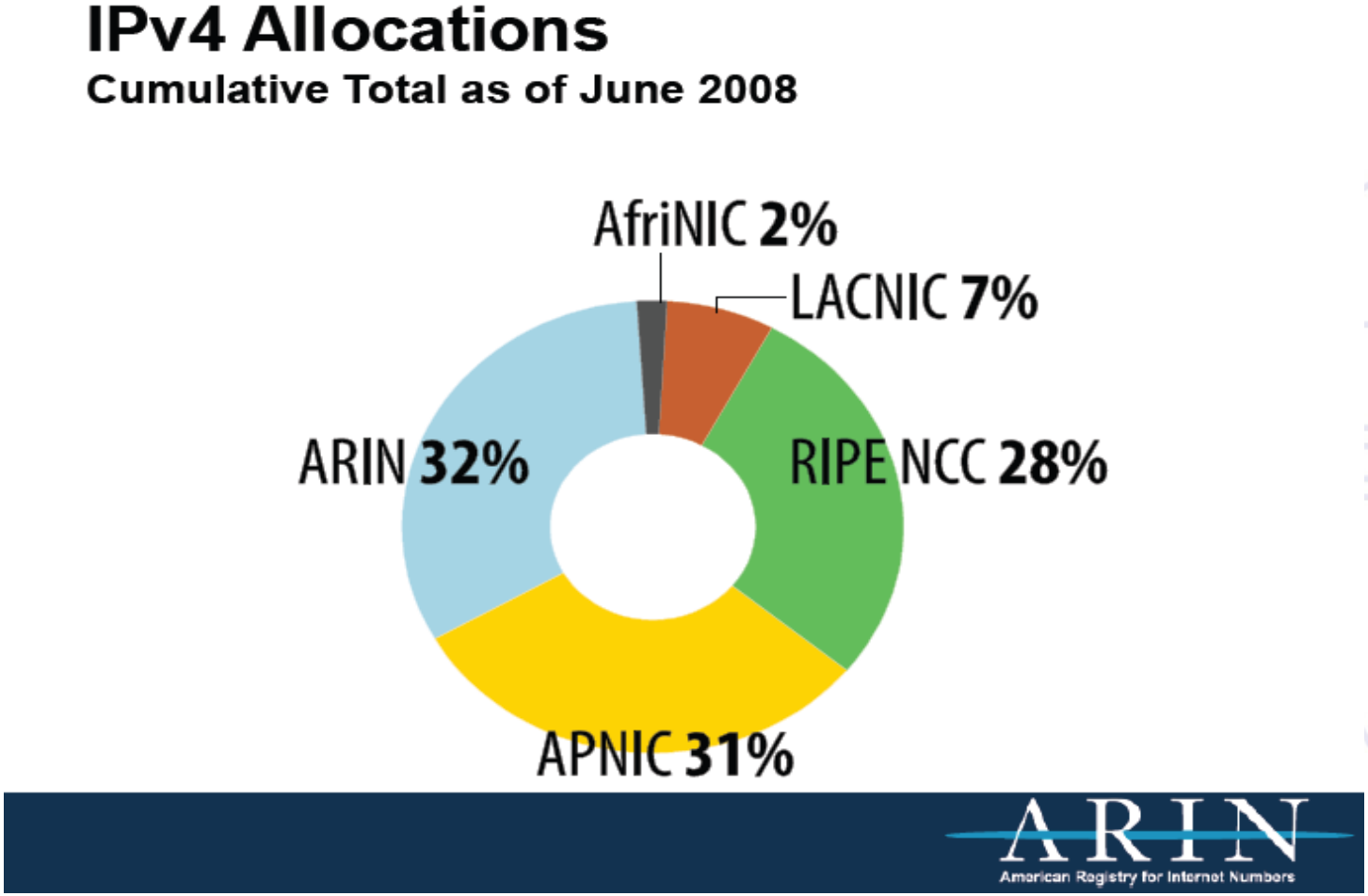
Network Address Translation

- RFC 1631, 2663 and 2993
- …de a NAT nem skálázható és elrontja a end-to-end címezhetőséget

Cím osztási séma



Kiosztott IPv4 címek régiók szerint



Címelfogyás

Címelfogyást mostanában gyakran emlegetik

- De most itt van!
- http://www.potaroo.net/tools/ipv4/

IANA kiosztotta az utolsó 5 /8-az 2011 Februárjában

- APNIC el kezdte kiosztani az utolsó /8-at 2011 Áprilisában

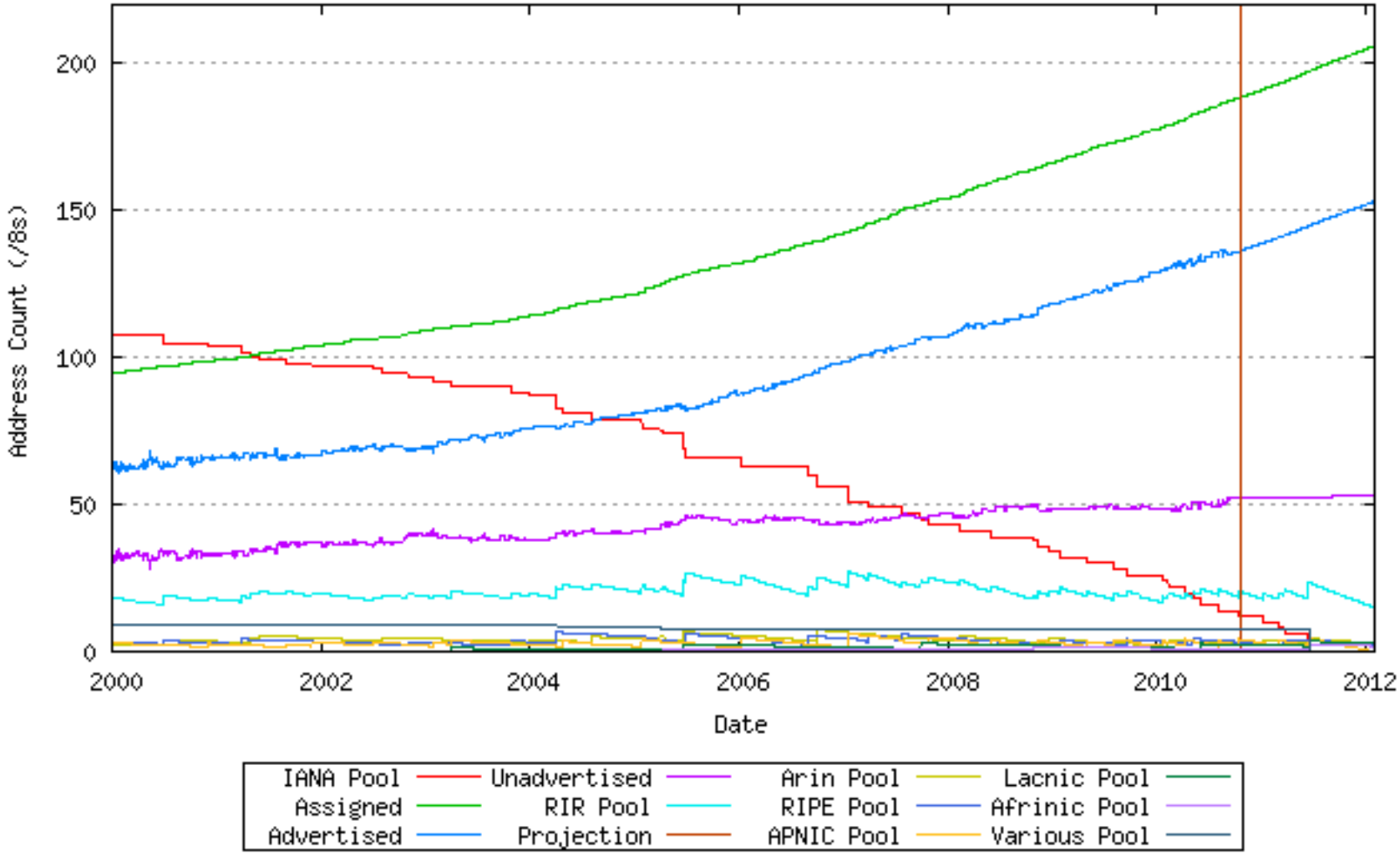
A címelfogyása új mechanizmusokat igényel, amely a címeket konzervatívabban osztja

- Kevesebb globális IPv4 címet lehet kapni
- Szigorúbb címosztási szabályok

Jelentős hatása lehet az új alkalmazásokra, amelyeknek globális IP címre van szükséges

- alkalmazások (különösen biztonsági alkalmazások) vagy p2p

IP címek fogyása – Geoff Huston



RIR címelfogyás - dátumok

Becsült címelfogyási dátumok (jelenlegi IP cím felhasználási ütem mellett)

- APNIC:19-Apr-2011
- RIPENCC:02-Aug-2012
- AFRINIC:21-Mar-2014
- ARIN:07-May-2014
- LACNIC:28-May-2014

Címelfogyás nem jelent világvégét, csak nagyon szigorú címosztást – pl. maximum 1024 cím kiadása

- Policy lehet különböző a különböző régióban

Lehetséges lépések

IPv6 bevezetése – IPv6 kész a használatra

- Kutatói hálózatok régóta elérhetővé tették

Nem használt IPv4 tartományok visszavétele

- Nem jelentős nyereség
- jogi konfliktusok

Kísérleti IPv4 tartomány "E" alkalmazása

- Szoftverek nem támogatják

Internet szolgáltatóknál NAT

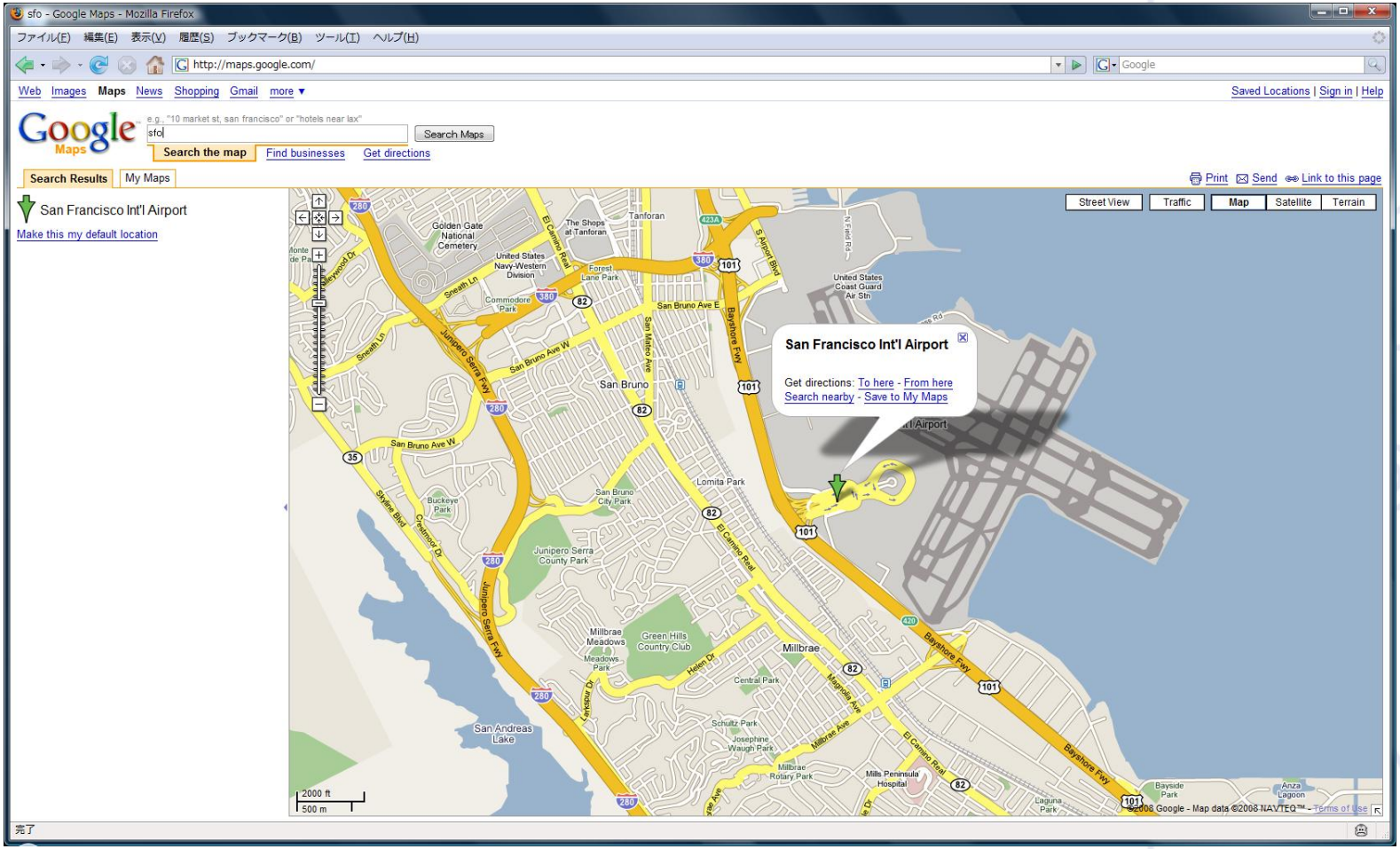
- Felhasználók osztályozása
- Szoftverek működési problámái

IPv4 cím piac kialakítása

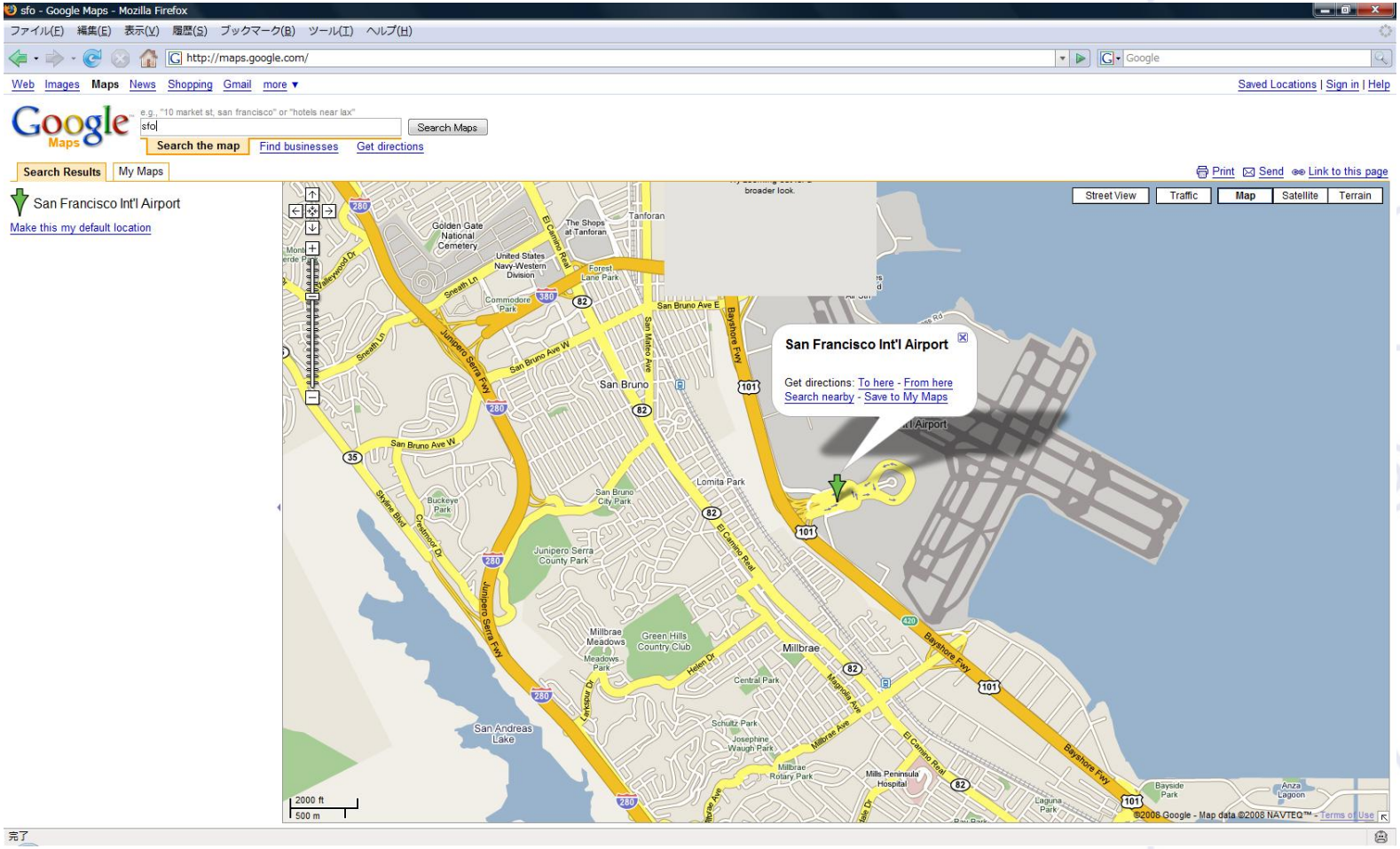
- IPv4 címek fragmentálódás - egyre több kevés címet tartalmazó hálózat jelenik meg a globális routing-táblában, és ez a jelenlegi útvonalválasztók képességeinek határát fogja feszegetni.

Limitation of NAT Solution

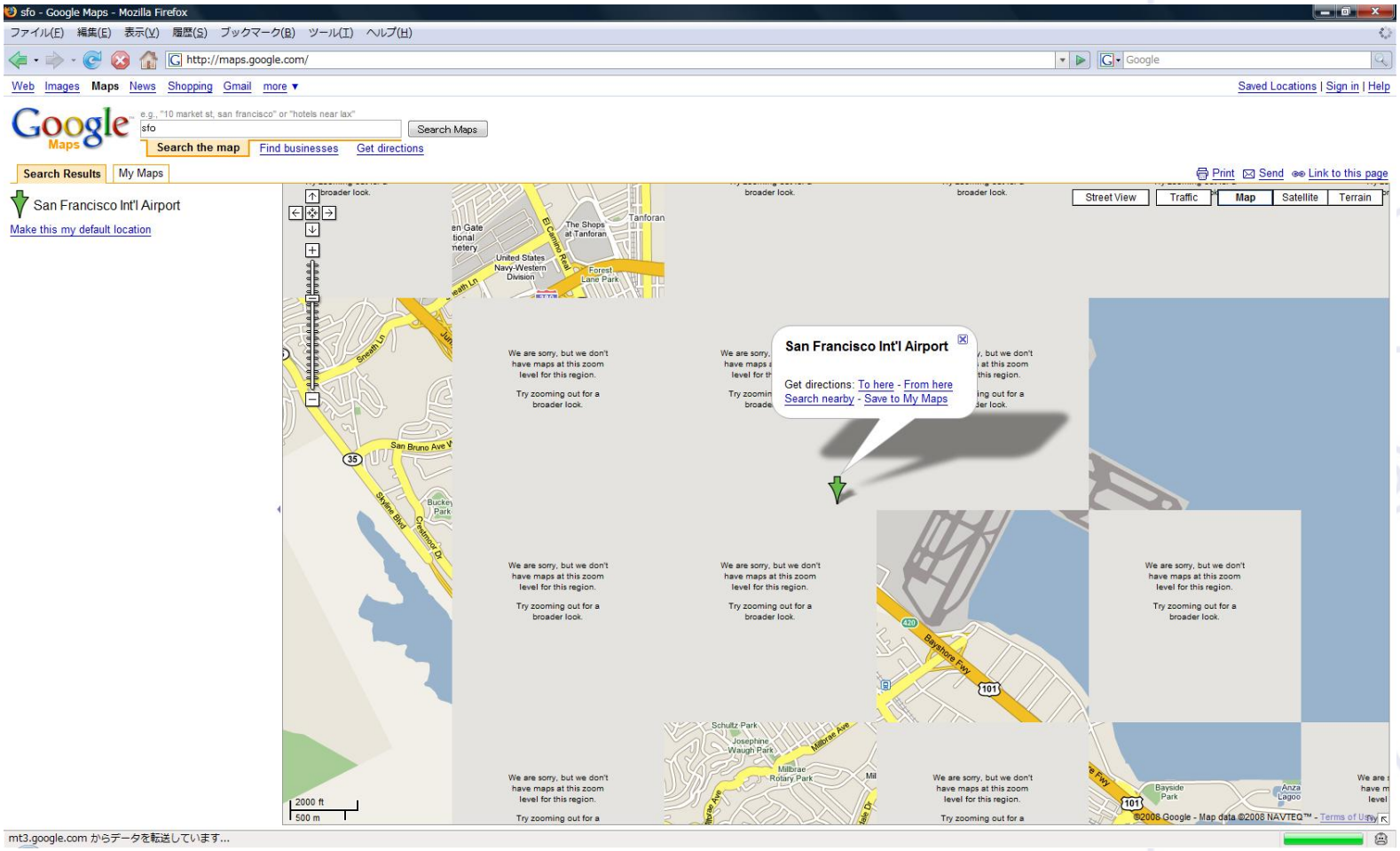
Max 30 Connections



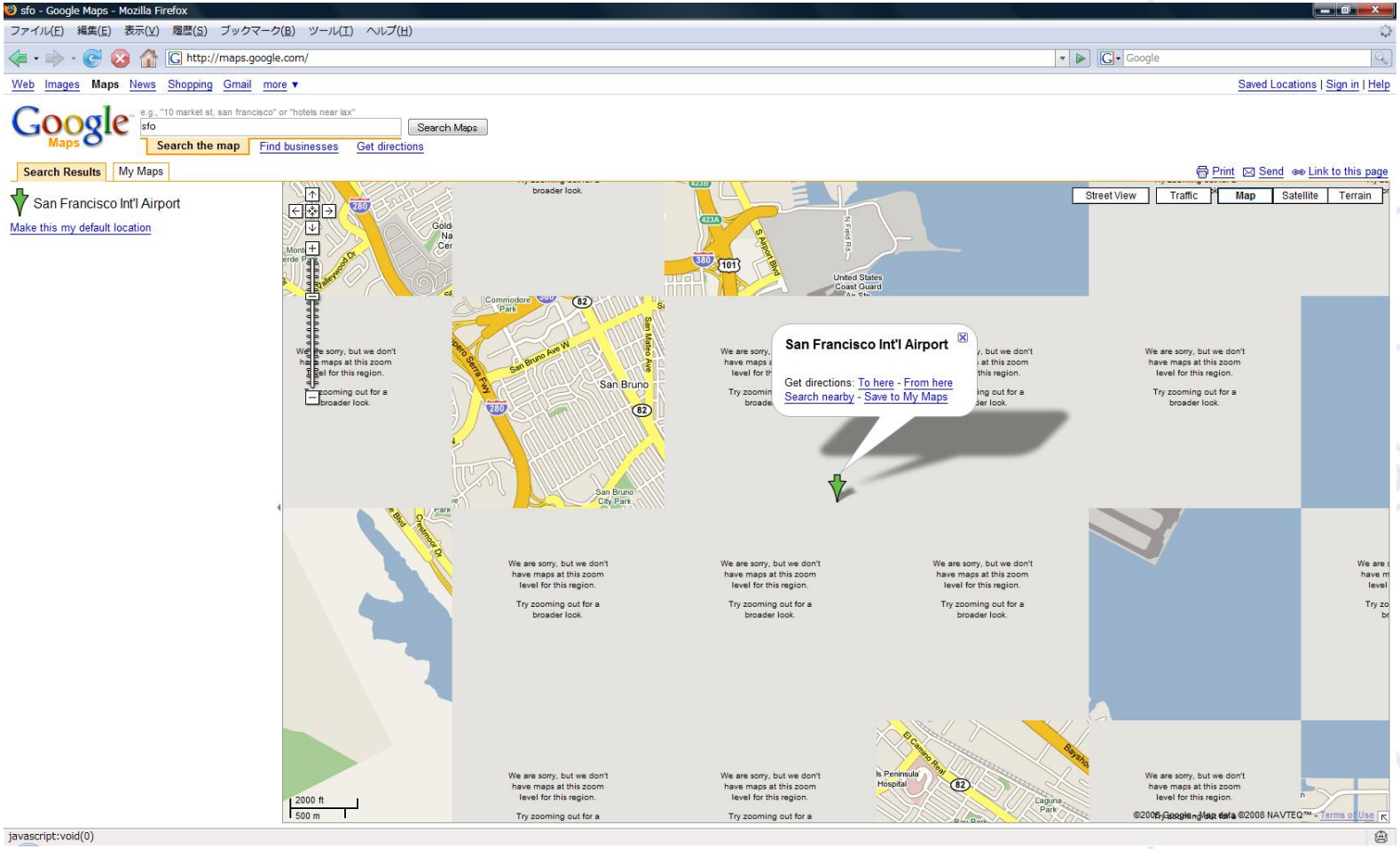
Max 20 Connections



Max 15 Connections



Max 10 Connections



Max 5 Connections

IPv6 protokoll (RFC 2460 DS)

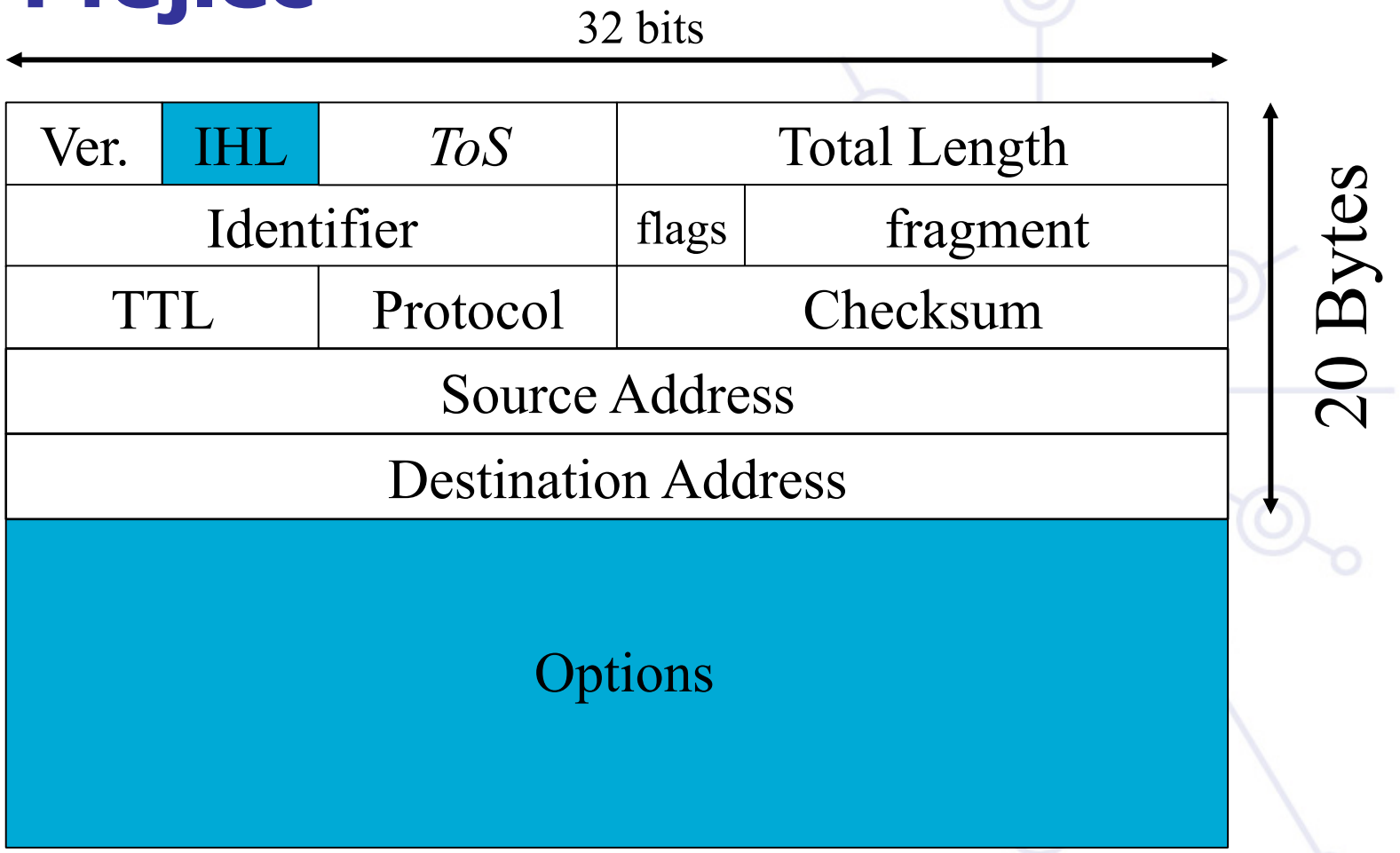
IPv6 fejléc

IPv6 címzés

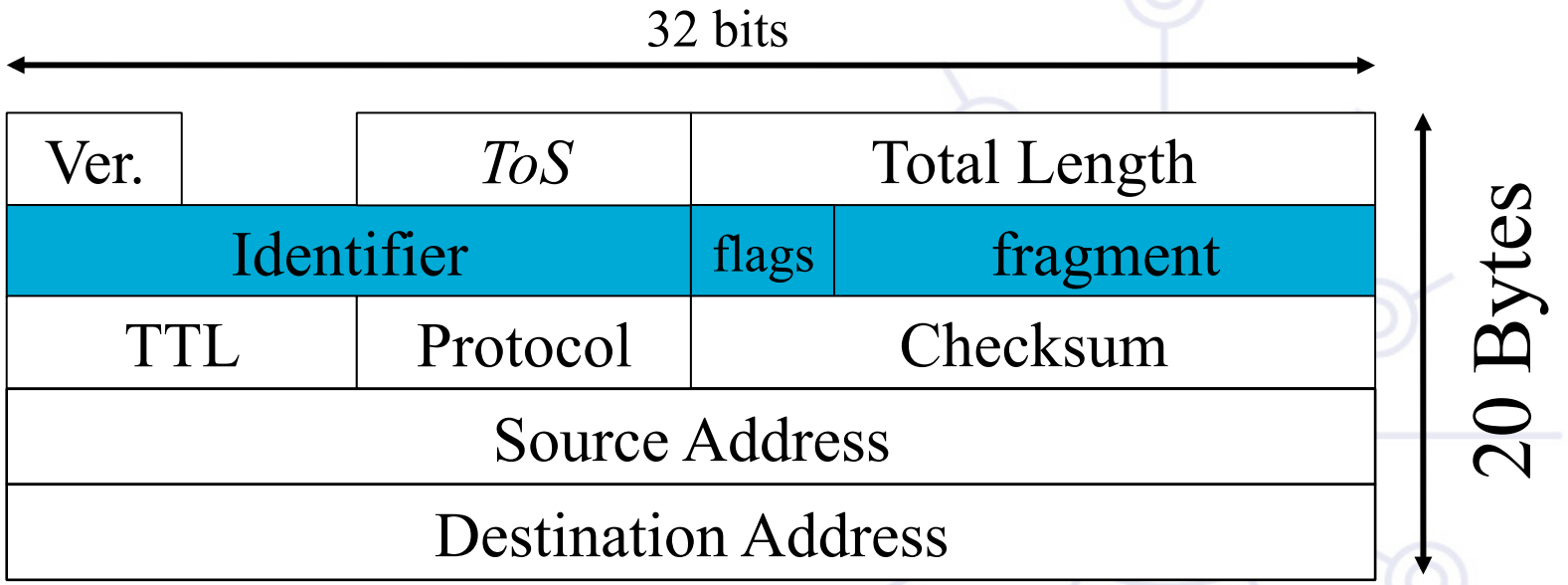
IPv6-hoz kapcsolódó protokollok

IPv6 fejléc

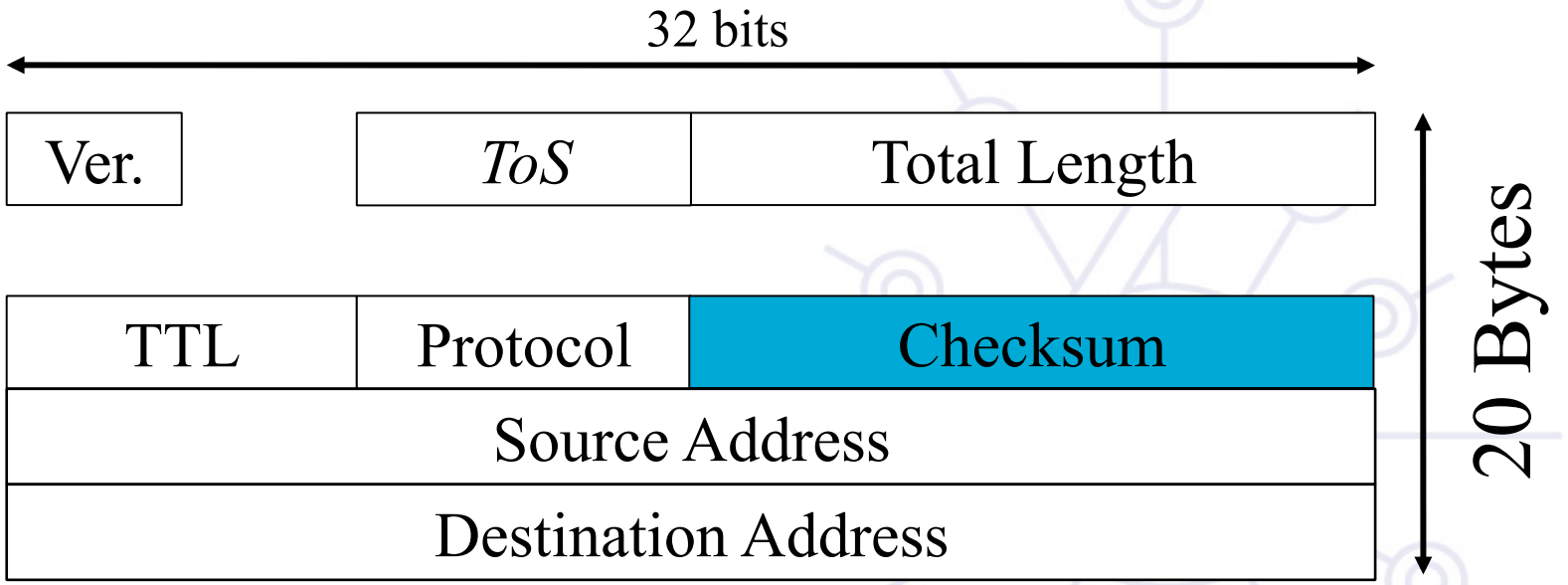
IPv4 fejléc


32 bits
Ver.
IHL
ToS
Total Length
Identifier
flags
fragment
TTL
Protocol
Checksum
Source Address
Destination Address
Options
20 Bytes

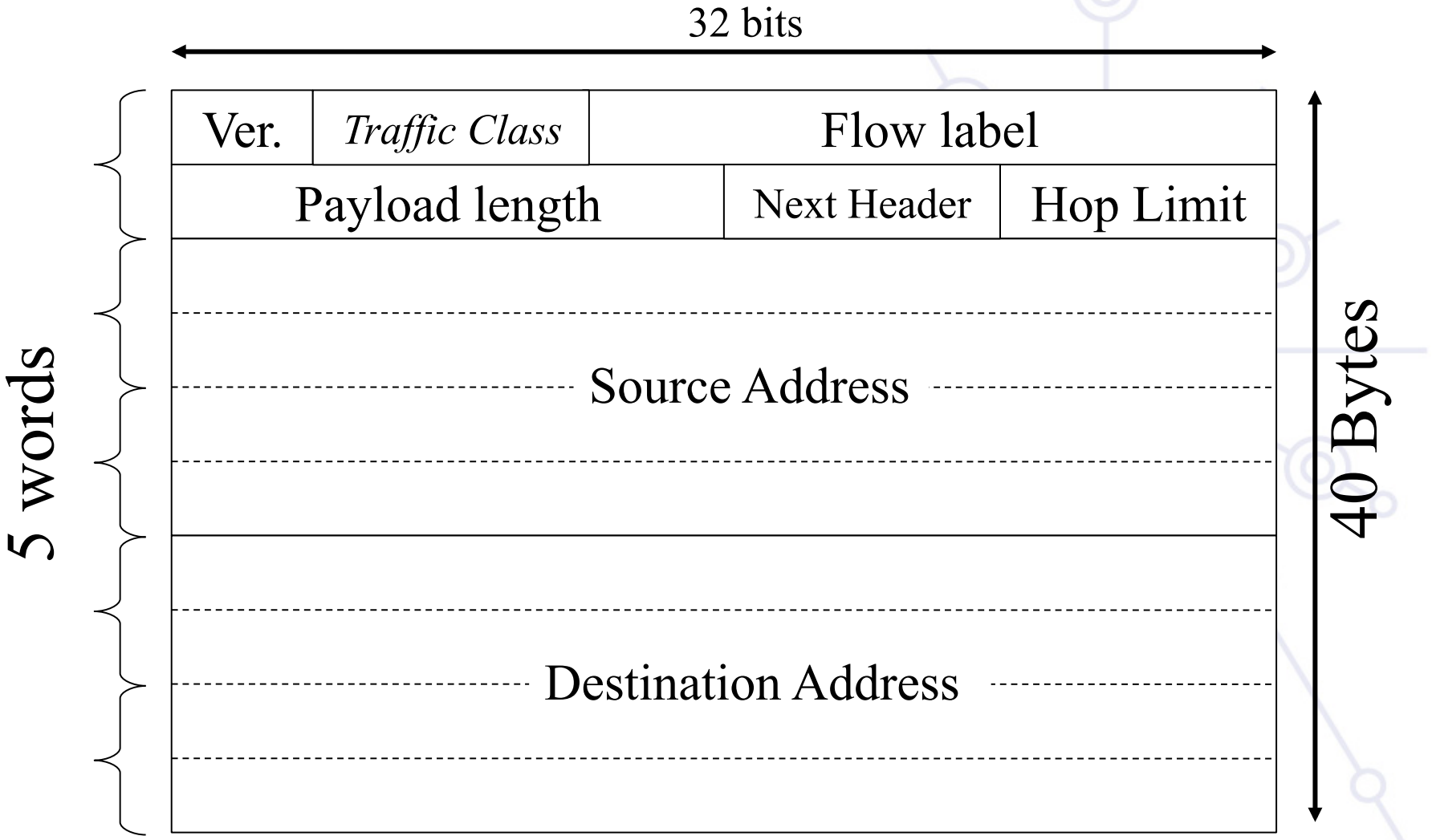
IPv4 fejléc


32 bits
Ver.
ToS
Total Length
Identifier
flags
fragment
TTL
Protocol
Checksum
Source Address
Destination Address
20 Bytes

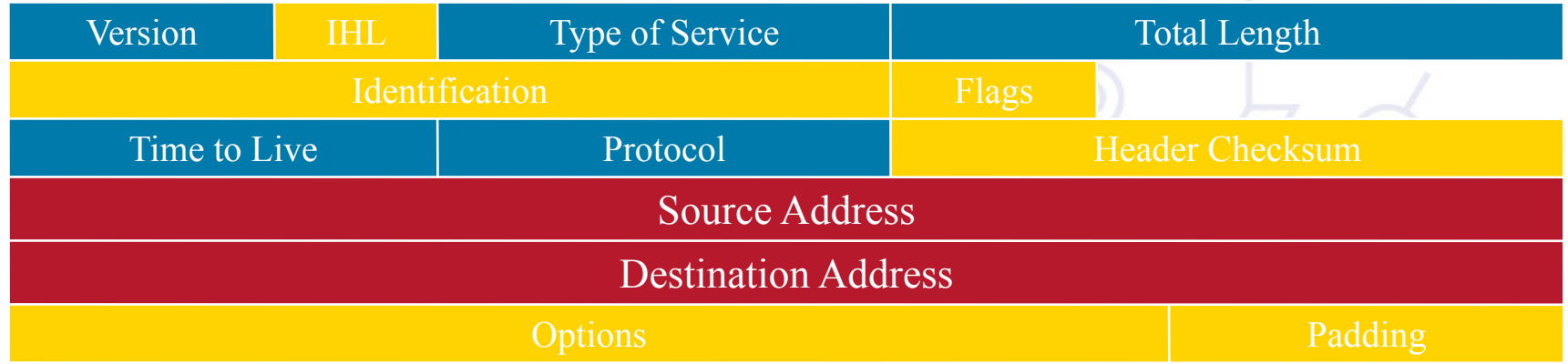
IPv4 fejléc

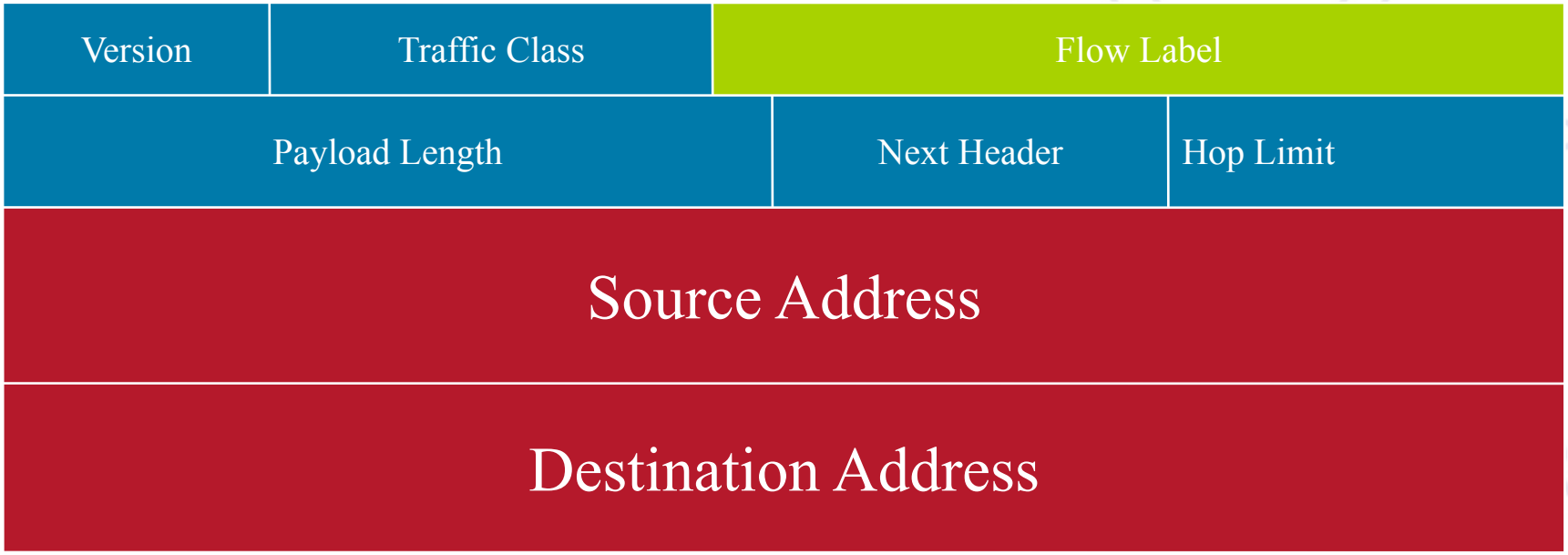

32 bits
Ver.
ToS
Total Length
TTL
Protocol
Checksum
Source Address
Destination Address
20 Bytes

IPv6: fejléc - egyszerűsítés



IPv4 & IPv6 fejléc összehasonlítás





Elegendő lesz a jövőben?

Cím hosszúság

- 1 564 és 3 911 873 538 269 506 102 közötti cím a Föld minden m^2 -re
- Szemléltesse egyetlen vízmolekula a teljes IPv4-es címteret. Akkor az IPv6 címzési kapacitásának kb. 2.38 tonna víz felel meg.
- Ok a fix címhosszúság alkalmazására

Hop Limit

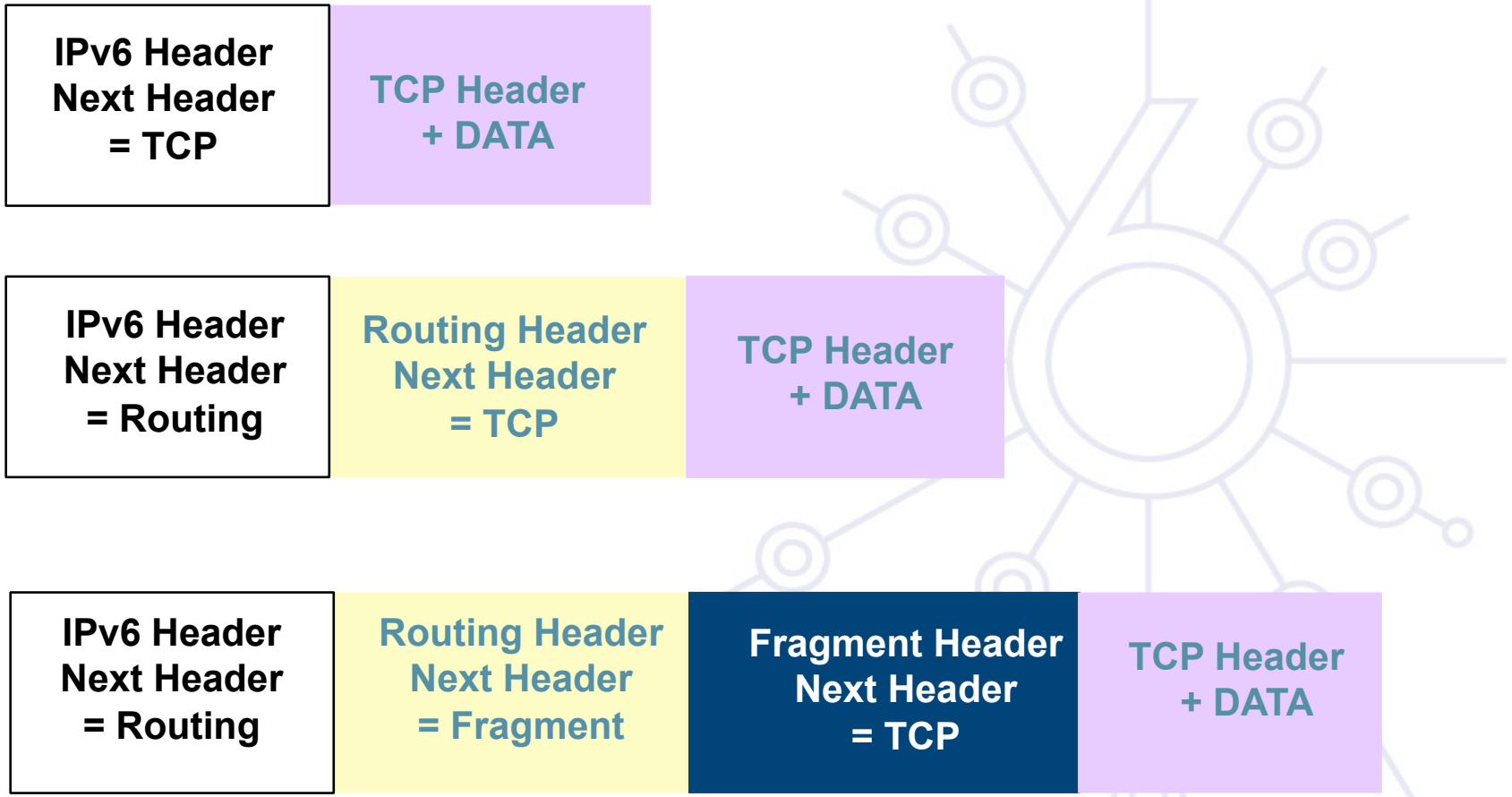
- Nem jelenthet problémát

Payload hossz

- Egyes esetekben Jumbogram használata ajánlott

IPv6 extensions

IPv6: Opcionális fejlécek



IPv6 Címzés

6DEPLOY. IPv6 bevezetés és támogatás

IPv6 Címzési séma

Az RFC4291 definiálja az IPv6 címzési sémát

Az RFC3587 határozza meg az IPv6 global unicast címek formátumát

128 bit hosszú címek

- Lehetővé teszi a hierarchiát
- Rugalmasan fejleszthető hálózat

CIDR elvek használata:

- Prefix / prefix hossz
  - 2001:db8:3003::/48
  - 2001:db8:3003:2:a00:20ff:fe18:964c/64
- Az aggregáció csökkenti a routing táblák méretét

Hexadecimális ábrázolás

Az interfészeknek több IPv6 címe van

IPv6 cím típusok

Unicast (one-to-one)

- global
- link-local
- site-local (érvénytelenített)
- Unique Local (ULA)
- IPv4-compatible (érvénytelenített)
- IPv4-mapped

Multicast (one-to-many)

Anycast (one-to-nearest)

Fenntartott

Szöveges címformátum

Preferált formátum (egy 16 byteos global IPv6 cím)

2001:0DB8:3003:0001:0000:0000:6543:210F

Kompakt formátum:

2001:DB8:3003:1::6543:210F

IPv4-mapped: ::FFFF:134.1.68.3

Szöveges forma:

- [2001:DB8:3003:2:a00:20ff:fe18:964c]
- http://[2001:DB8::43]:80/index.html

IPv6 cím típus prefixek

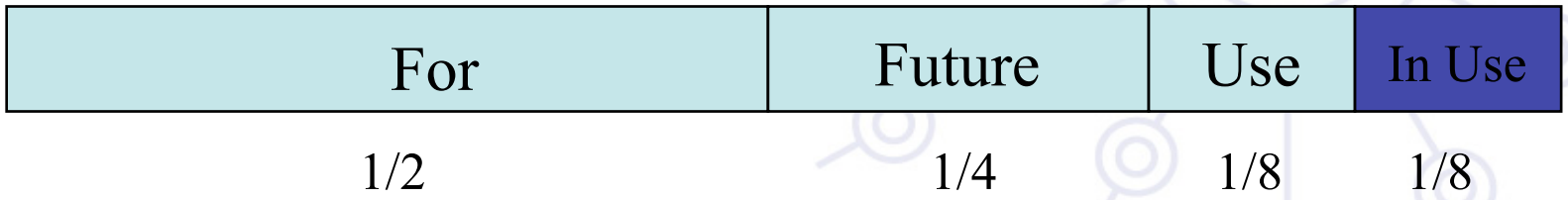
Address Type	Binary Prefix	IPv6 Notation
Unspecified	00…0 (128 bits)	::/128
Loopback	00…1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA	1111 110	FC00::/7
Global Unicast	(everything else)	
IPv4-mapped	0..0:1111 1111:1111 1111:IPv4	::FFFF:IPv4/128
Site-Local Unicast (deprecated)	1111 1110 11	FEC0::/10
IPv4-compatible (deprecated)	00…0 (96 bits)	::IPv4/128

Global Unicast hozzárendelés a 2000::/3-t (001 prefixet) használja

Anycast címek az unicast prefixekből kerülnek foglalásra

IPv6 címtér

Aggregatable Global Unicast címek (001): 1/8
Unique Local Unicast címek (1111 1110 00): 1/128
Link-Local Unicast címek (1111 1110 10): 1/1024
Multicast címek (1111 1111): 1/256



További információk:
http://www.iana.org/assignments/ipv6-address-space

Néhány speciális célú Unicast cím

Az RFC5156-ben leírtak szerint

Az **unspecified address,** helyörzőként szolgál, amennyiben nincs elérhető cím:

0:0:0:0:0:0:0:0 (::/128)

A **loopback address,** csomagok küldésére saját magának:

0:0:0:0:0:0:0:1 (::1/128)

A **documentation prefix [RFC3849]: 2001:db8::/32**

Link-Local & Site-Local Unicast címek

Link-local címek autokonfiguráció esetén, vagy ha nincs elérhető router **(FE80::/10):**

10 bits	*54 bits*	*64 bits*
1111111010	0 0	Interface ID
FE80		

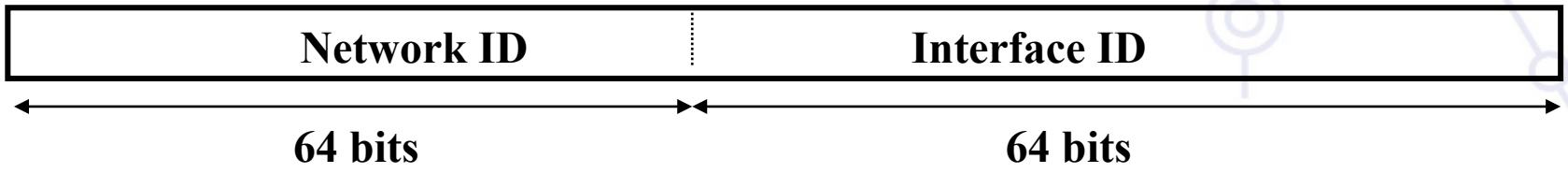
Site-local címek - független a TLA / NLA* változásoktól **(FEC0::/10):** (érvénytelenítve: RFC3879)

10 bits	*54 bits*	*64 bits*
1111111011	Subnet ID	Interface ID

Interface ID-k

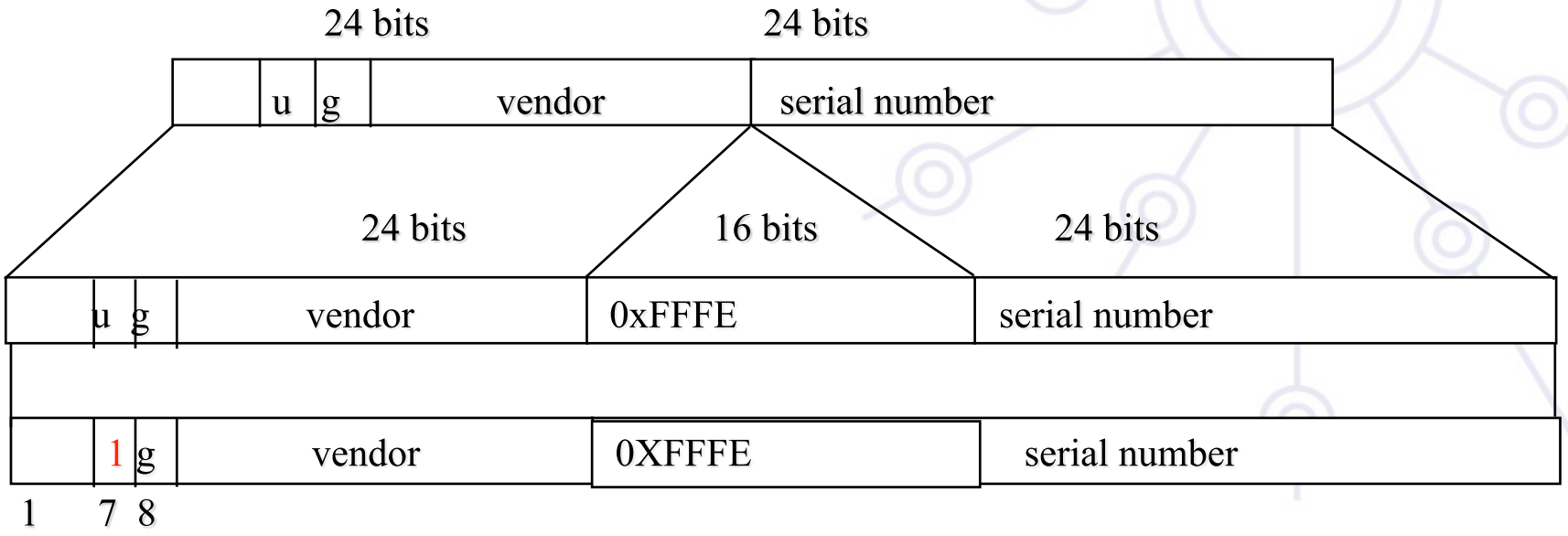
Az unicast címek legalacsonyabb helyiértékű 64-bitje a következő módszerekkel osztható:

- Automatikus konfigurációval a 64-bites MAC címből
- Automatikus konfigurációval a 48-bites MAC címből (pl. Ethernet) kiterjesztve a 64-bites EUI-64 formátumra
- DHCP-vel
- Kézzel beállítva
- Álvéletlen szám automatikus generálásával (pl. adatvédelmi okokból)
- CGA (Cryptographically Generated Address)
- További eljárások várhatóak a jövőben



Autokonfigurált Interface ID-k (1)

- 64 bit - kompatibilitás az IEEE 1394-el (FireWire)
- Megkönnyíti az automatikus konfigurációt
- Az IEEE definiál egy eljárást EUI-64 készítésére IEEE 802 MAC címből (Ethernet, FDDI)



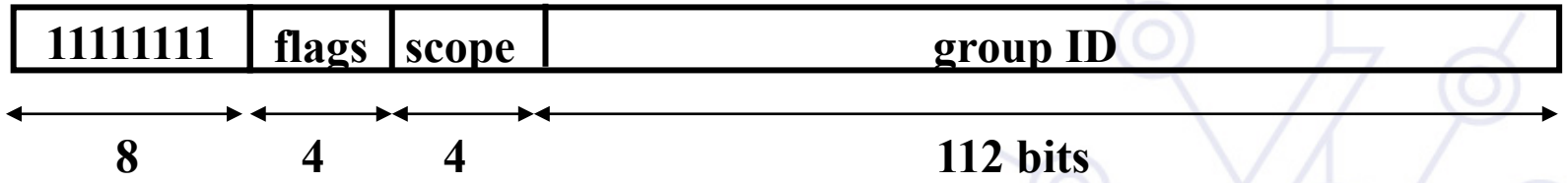
Autokonfigurált Interface ID-k (2)

Non global azonosítóval rendelkező linkek (pl. Localtalk 8 bit node identifier) → a balra eső biteket nullákkal kell feltölteni

Az azonosító nélküli linkek esetén több különböző út lehetséges (pl. tunnel-ek, PPP), hogy legyen subnet-prefix-unique azonosító

- Egy másik interfész univerzális azonosítójának használata
- Kézi beállítás
- Node szériaszáma
- Egyéb node-specifikus token

Multicast címek



Flag-ek: 0RPT: The legmagasabb helyiértékű flag fenn van tartva, és 0-val kell inicializálni.

- **T**: Transient, vagy nem, dinamikusan osztott, vagy jólismert a cím
- **P**: Prefix alapján osztott vagy nem - hálózati prefix alapján
- **R**: Rendezvous Point cím belefoglalva, vagy nem

Scope mező:
1 - Interface-Local
2 - link-local
4 - admin-local
5 - site-local
8 - organization-local
E - global

(3,F fenntartott)(6,7,9,A,B,C,D nincs kiosztva)

Unique Local IPv6 Unicast címek (1)

RFC4193 definiálja az ULA-t

- Globálisan egyedi prefix nagy valószínűségű egyediséggel
- Helyi kommunikációra tervezve, általában a siteon belül
- Nem elvárás velük szemben a globális Internet irányába történő route-olás
- Csak egy korlátozott körzetben routolhatóak, pl. csak néhány site között
- Locally-Assigned helyi címek vagy Centrally-Assigned helyi címek

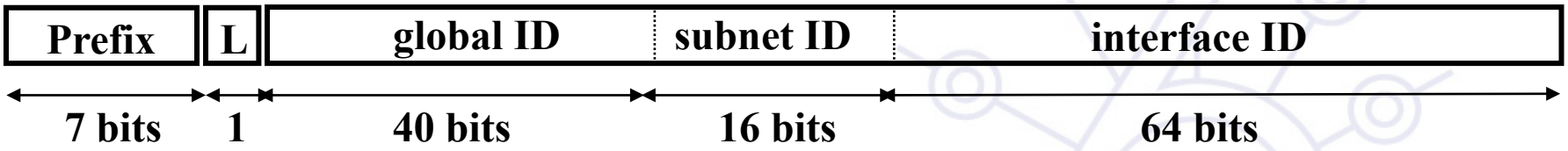
Unique Local IPv6 Unicast címek (2)

ULA tulajdonságok:

- Jólismert prefix - egyszerű szűrés a site határánál
- ISP független, és a siteon belüli kommunikációra használható akár állandó akár bizonytalan az Internet hozzáférés
- Ha véletlenül routingon, vagy DNS-en keresztül kiszivárog a siteon kívülre, nem ütközik más címekkel
- Az alkalmazások globális scope-ú címként használják

Unique Local IPv6 Unicast címek (3)

Formátum:



FC00::/7 Prefix azonosítja a Local IPv6 unicast címeket

L = 1 ha a cím **helyileg kiosztott**

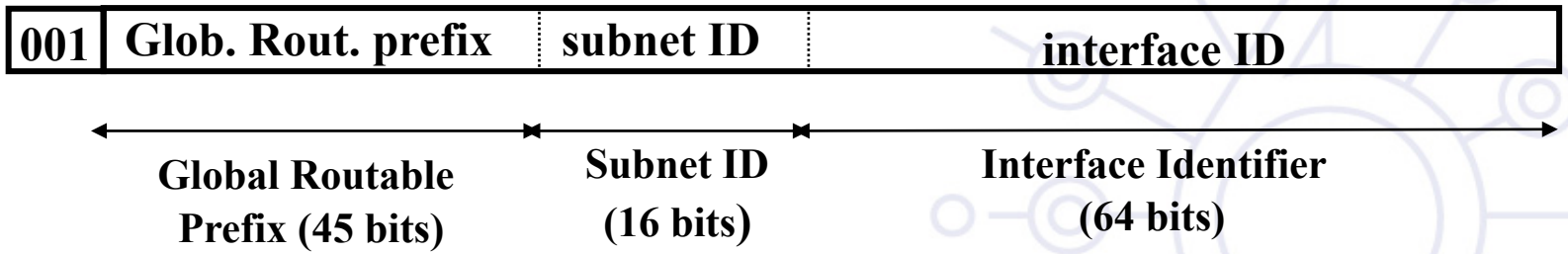
L = 0 még meghatározandó (a gyakorlatban a **központilag kiosztott** prefixek)

ULA-k álvéletlenül lefoglalt global ID-k alapján készülnek

- Ez biztosítja, hogy nincs semmilyen viszony a foglalások között, és egyértelműsíti, hogy a prefix-eket nem globális route-olásra szánja

Global Unicast címek

Az RFC3587 definiálja



A global routing prefix egy zónához (sitehoz, alhálózatok / linkek csoportjához) rendelt érték

- Hierarchikus struktúraként hozták létre a hatékonyabb globális routing érdekében

Az subnet ID azonosít egy alhálózatot a siteon

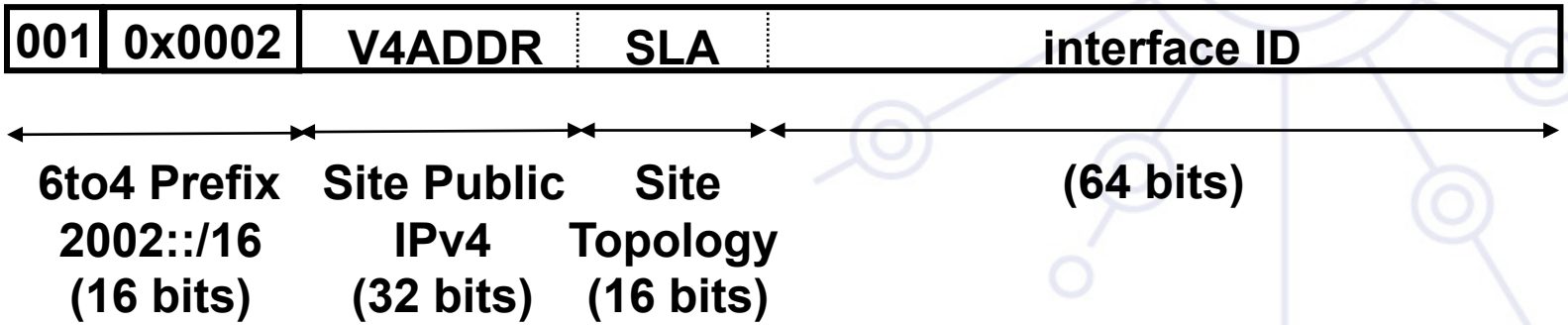
- Hierarchikus struktúra a site-adminisztrátor számára

6to4 címek

Az **RFC3056 definiálja: Connection of IPv6 Domains via IPv4 Clouds**

Hozzárendelt Prefix: 2002::/16

A 2002:V4ADDR::/48 siteokhoz rendeléshez



Miért fix hosszakat használunk?

A fix méret csökkenti a felhasználó problémáit, ha szolgáltatót kíván váltani.

A szabványos méret nem igényli azt, hogy a felhasználó indokolja az igényeit.

16 bites site méret elegendő a legtöbb felhasználónak a legnagyobbakat kivéve

Anycast címek

Az interfészek (általában különböző nodeok) csoportjának azonosítója. Az anycast címekre küldött csomag a „legközelebbi” interfészhez kerül (a routing protokoll távolsága alapján).

Az unicast címtérből (bármilyen scopeból) kerül kiosztásra. **Szintaktikailag nem megkülönböztethető az unicast címektől**

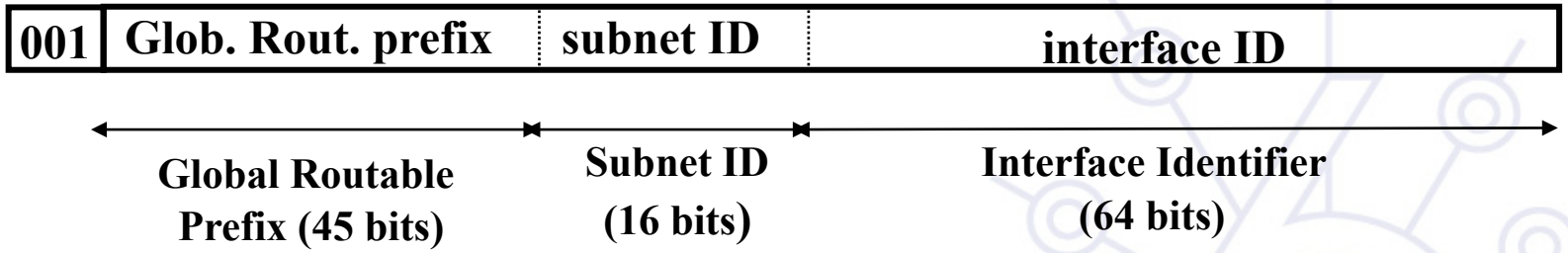
Ha egy unicast cím több mint egy interfészhez van társítva, anycast címmé változik, a címhez rendelt node-okat kifejezetten úgy kell konfigurálni, hogy tudjanak arról, hogy ez anycast cím

Egy anycast cím általában nem lehet egy csomag forrás-címe

A foglalt anycast címek az **RFC2526**-ben találhatóak:

Az alhálózati router anycast címe előre meghatározott (az összes routeren kötelezően):

Production címzési séma (2)



LIR-ek alapértelmezetként /32 –t kapnak

- A production címek a 2001, 2003, 2400, stb. prefixeket kapják ma
- Nagyobb igényelhető, ha indokolt

/48 néhány kritikus infrastuktúra használja

/48-tól /128-ig kaphatják a végfelhasználók

- Az RFC3177 és az aktuális szabályzat szerint
- Általában /48, ha nagyobb hálózatok számára indokolt, akkor /47
- A kisebb hálózatoknak /48-/60 között
- /64 ha egy és csak egy hálózat szükséges
- /128 ha biztos, hogy egy és csak egy eszköz csatlakozik


deploy
IPv6 kapcsolódó protokolljai

Új protokollok

Új lehetőségek kerültek bele az IPv6 protokoll specifikációjába (RFC 2460 DS)

Neighbor Discovery (ND) (RFC 2461 DS)

Automatikus konfiguráció :

- Stateless Address Auto-configuration (RFC 2462 DS)
- DHCPv6: Dynamic Host Configuration Protocol for IPv6 (RFC 3315 PS)
- Path MTU discovery (pMTU) (RFC 1981 PS)

Új protokollok (2)

MLD (Multicast Listener Discovery) (RFC 2710 PS)

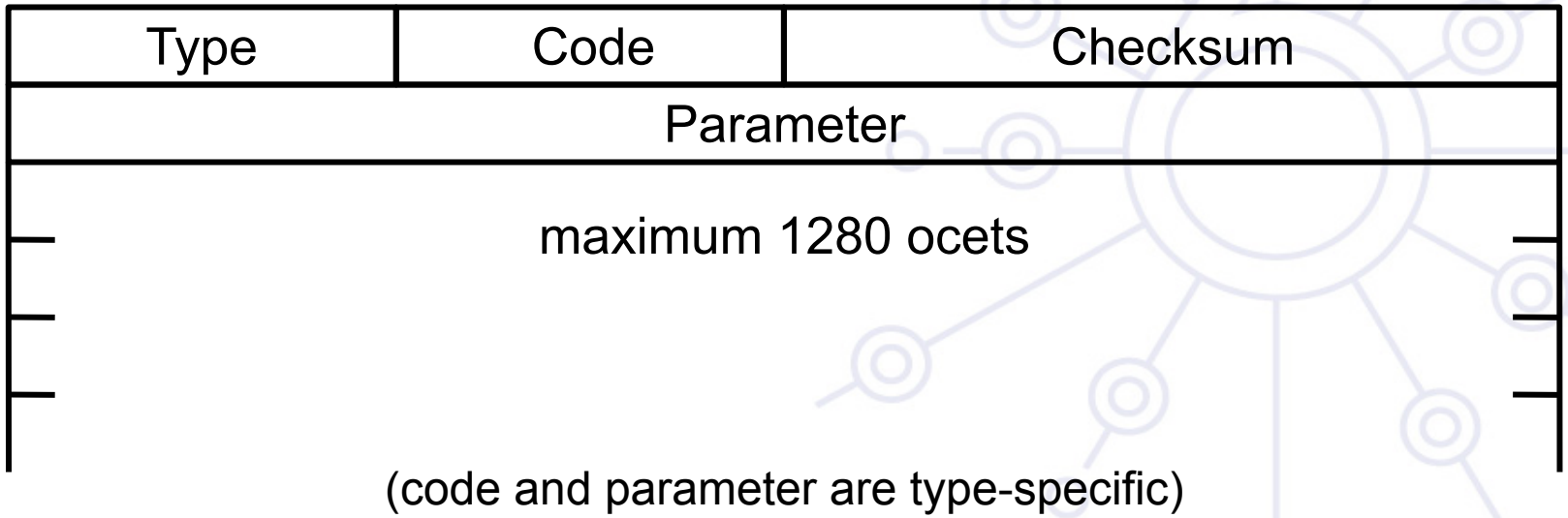
- Multicast csoport management IPv6 linken/subneten
- IGMPv2-n alapul
- MLDv2 (IPv4 IGMPv3-nek felel meg)

ICMPv6 (RFC 2463 DS) "Super" protokoll, ami:

- Az ICMPv4 által nyújtott szolgáltatásokra képes (Error control, administration, ...)
- ND üzeneteket továbbítja
- MLD üzeneteket továbbítja (Query, Reports, ...)

ICMP Hibaüzenetek

Közös formátum (mint az IPv4):



ICMP Hibaüzenet típusok

destination unreachable
- no route
- administratively prohibited
- address unreachable
- port unreachable

packet too big

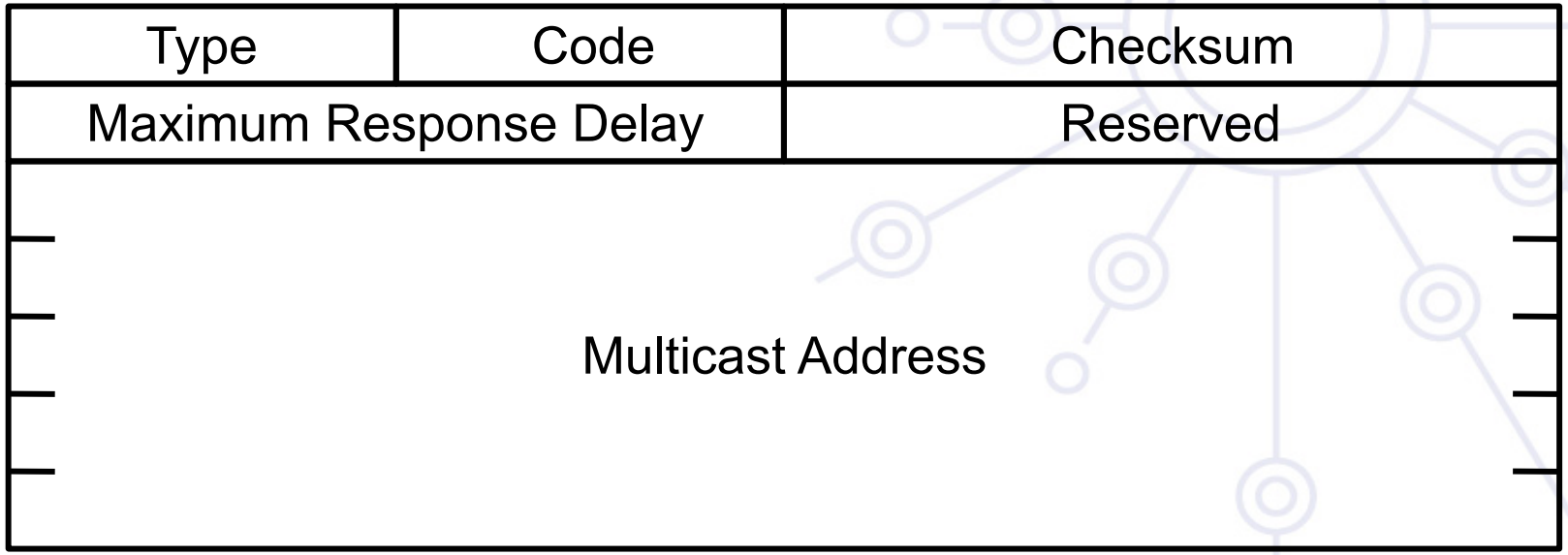
time exceeded

parameter problem
- erroneous header field
- unrecognized next header type
- unrecognized option

ICMP(v6) csomagok

Echo kérés & válasz (mint az IPv4)

Multicast Listener Discovery csomagok:
query, report, done (mint IGMP IPv4):



Neighbor Discovery

Az IPv6 nodeok, amelyek ugyanazt a fizikai médiumot (linket) használják, Neighbor Discovery-t (NDP) (Környezetfelmérő protokoll) használnak, hogy:

- felfedezzék egymást – létezésüket
- meghatározzák szomszédaik link-layer címét
- megtalálják a routereket
- Karbantartsák szomszédaik elérhetőségi információját (NUD)

nem alkalmazható közvetlenül NBMA (Non Broadcast Multi Access) hálózatokra, az ND multicast-ot használ bizonyos funkciókra

Neighbor Discovery (2)

Protokoll tulajdonságai:

- Routerek felfedezése
- Prefix(ek) felfedezése
- Paraméterek felfedezése (link MTU, Max Hop Limit, ...)
- Automatikus cím konfiguráció
- Cím feloldás
- Next Hop meghatározása
- Neighbor Unreachability Detection
- Duplicate Address Detection
- Redirect (Átirányítás)

Neighbor Discovery (3): összehasonlítás az IPv4-el

A következők egyesítése:

- ARP
- R-Disc
- ICMP redirect
- ...

Neighbor Discovery (4)

Az ND 5 különbböző ICMP csomagot definiál:

- Router Advertisement (RA) :
  - Ismétlődő hirdetés (a router elérhetőségéről), következőket tartalmazza:
    - » A linken használt prefixek listájából (autoconf)
    - » A Max Hop Limit lehetséges értékéből (TTL az IPv4-ban)
    - » Az MTU értékéből
    - » Néhány egyéb paraméterből
- Router Solicitation (RS) :
  - A host-oknak azonnal szüksége van RA-ra (bootoláskor)

Neighbor Discovery (5)

- Neighbor Solicitation (NS):
  - A szomszéd link-layer címének, vagy
  - elérhetőségének meghatározására, vagy
  - a duplikált címek (DAD) felderítésére
- Neighbor Advertisement (NA):
  - Egy NS csomagra adott válasz
  - A fizikai cím megváltozásának hirdetésére
- Redirect:
  - A router tájékoztatja ezzel a hostot, hogy van egy jobb út a megadott cél felé

ARP – emlékeztető

Összerendelés keresése:

Cél IP @ ➔ Link-Layer (MAC) @

IPv4 & ARP felidézése

- ARP kérés broadcast -olt
  - pl. `ethernet @: FF-FF-FF-FF-FF-FF`
  - Tartalmazza a forrás Link-layer címét
- ARP válasz a forrásnak unicast módon küldve
  - Tartalmazza a cél Link-layer címét

Címfeloldás - IPv6 Neighbor Discovery (1)

Minden IPv6 nodenak kötelező 2 speciális multicast csoporthoz csatlakoznia minden hálózati interfészen

- All-nodes multicast csoport: ff02::1
- Solicited-node multicast csoport

A FF02::1:FF00:0/104 prefix összefűzése az IPv6 cím utolsó 24 bitjével

```
Cél IPv6 @: 2001:0660:010a:4002:4421:21FF:FE24:87c1
                              ⬇
Sol. Mcast @: FF02:0000:0000:0000:0000:0001:FF24:87c1
                              ⬇
Ethernet: 33-33-FF-24-87-c1
```

Címfeloldás - IPv6 Neighbor Discovery (2)

- H1 ismeri H2 (IP2) IP címét, és a MAC címét (MAC2) is meg akarja tudni
- H1 felépíti IP2 solicited multicast címét: Multi (IP2)
- H1 egy « Neighbor solicitation » üzenetet küld erre a solicited multicast IPv6 címre
- **Link szinten**, az NS csomagot a **multicast címre** küldi a broadcast helyett

Címfeloldás - IPv6 Neighbor Discovery (3)

- Az ethernet kezeli a multicastot
- Az ethernet keret gyakran a linken broadcast-olódik
- Csak a H2 az ethernet keret célja, és csak az küldi a « Neighbor Solicitation » csomagot az IPv6 stack-re
- A H2 egy unicast « Neighbor Advertisement » üzenettel válaszol H1-nek. Ez az üzenet H2 link layer címét tartalmazza.

Path MTU discovery (RFC 1981)

RFC 1191-ből származik, (a protokoll IPv4 változatából)

Útvonal : linkek csoportja a forrás és a cél között, amelyet egy IPv6 csomag követ

link MTU : maximum csomag hossz (byte-ban), amit át lehet juttatni egy linken töredezettség nélkül

Path MTU (vagy pMTU) = min { link MTU-k } egy adott útvonalra

Path MTU Discovery = automatikus pMTU felfedezés egy adott útvonalra

Path MTU discovery (2)

A protokoll működése

- feltételezzük, hogy a pMTU = link MTU a szomszéd eléréséhez (first hop)
- ha van egy olyan köztes router, amelynél a link MTU < pMTU ➔ az küld egy ICMPv6 üzenetet: "Packet size Too Large"
- ennek hatására a forrás csökkenti pMTU-t az ICMPv6 üzenetben kapott információk alapján

=> Köztes eszközökben nem megengedett a csomag feldarabolása

Auto-configuration

A hostoknak plug & play módon kellene működniük

ICMPv6 üzenetek használatával (Neighbor Discovery)

Bootoláskor a host lekérdezi a hálózat paramétereit:

- IPv6 prefix(eket)
- default router cím(eket)
- hop limit
- (link local) MTU
- ...

Auto-configuration (folytatás)

Csak a routereket kell manuálisan konfigurálni

- de a **prefix delegáción** dolgoznak
  (draft-ietf-ipv6-prefix-delegation-requirement-01.txt)

A hostok automatikusan IPv6 címhez juthatnak

- DE ez nincs automatikusan regisztrálva a DNS-ben
- ha a cím mindig ugyanaz: manuálisan be lehet regisztrálni

Igény a DNS Dynamic Update-re

(RFC 2136 PS and RFC 3007 PS) for IPv6

- Biztonsági problémák…

Stateless auto-configuration

IPv6 Stateless Address Auto-configuration

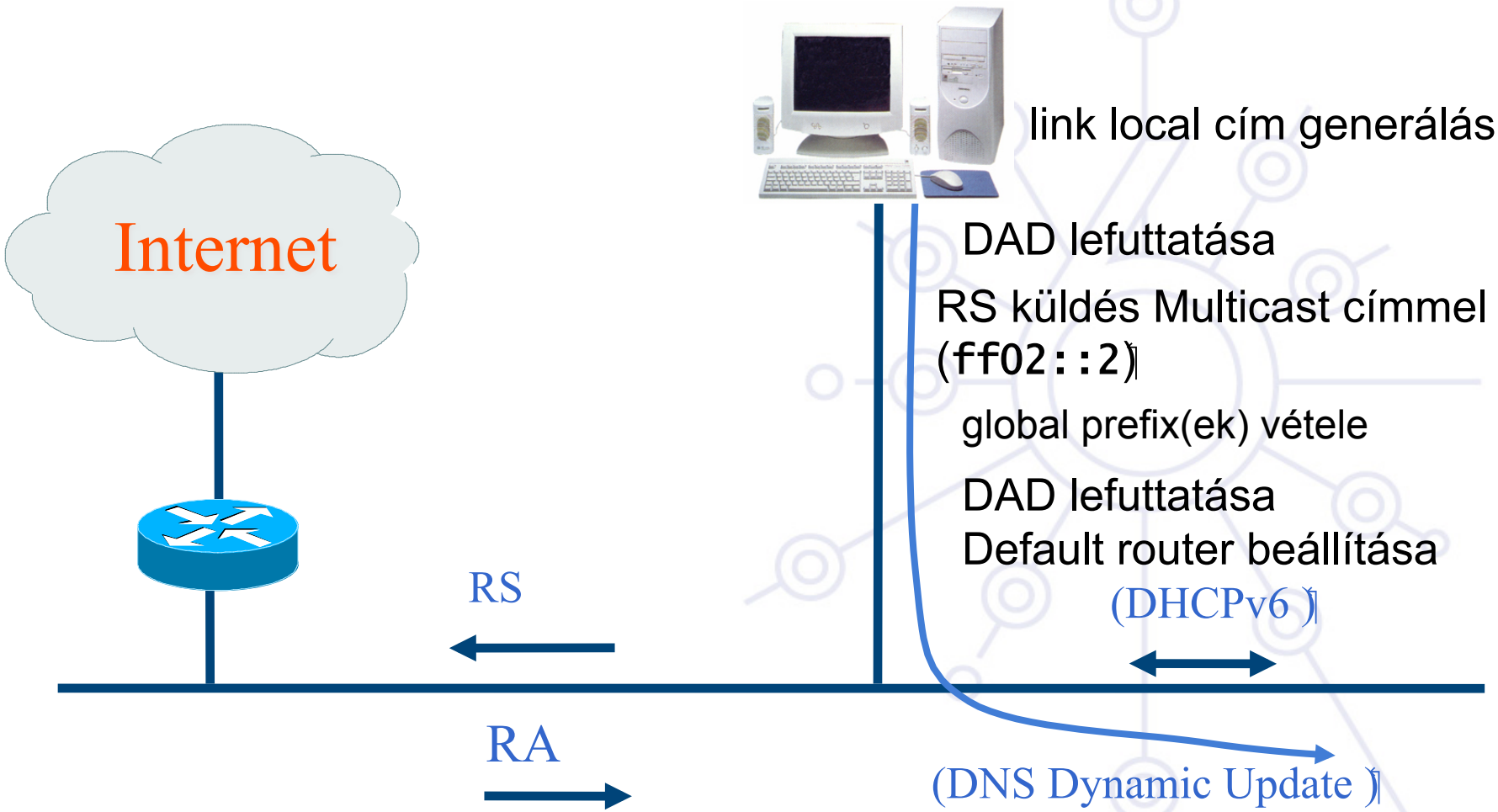
- RFC 2462 DS
- Nem vonatkozik a routerekre

Megengedi a hostnak globális IPv6 cím kialakítását:

- az interfész azonosító = EUI-64 (a MAC címből)
- router advertisement-ek jönnek a router(ek)től a linken

=> GA = concat (RA, EUI64)

Auto-configuration példa



Interface Identifier: probléma

IEEE 24 bit OUI azonosítja a hardvert

(http://standards.ieee.org/regauth/oui/oui.txt)

Interface ID alkalmazható a felhasználó követésére:

- A prefix megváltozik, de az interface ID ugyanaz marad!

Privacy extensions (RFC 3041)

- Interfész ID megváltoztatható
- MD5 algorithmus - véletlenszám/tároló
- Biztonsági probléma?

Privacy extension (RFC 4941)

- A privacy extension nincsen default bekapcsolva
- DAD minden később generált címre
- Per prefix engedélyezhető a privacy extension
- Nem csak MD5 hash algoritmus használható

Stateless Autoconfiguration: javaslatok

Csak routereket kell manuálisan konfigurálni

- prefix delegáció – hogy ezt is meglehessen spórolni

  (http://www.ietf.org/rfc/rfc3633.txt)

Hosztok automatikusan kapnak IPv6 címet

- DE nincsenek automatikusan DNS-be regisztrálva
  - Kivéve Windows Windows szerver DNS és MAC OS X Bonjour képes DNS esetén

Szervereket célszerű manuálisan konfigurálni

IPv6 támogatás a DNS-ben

DNS Extensions IPv6-ra

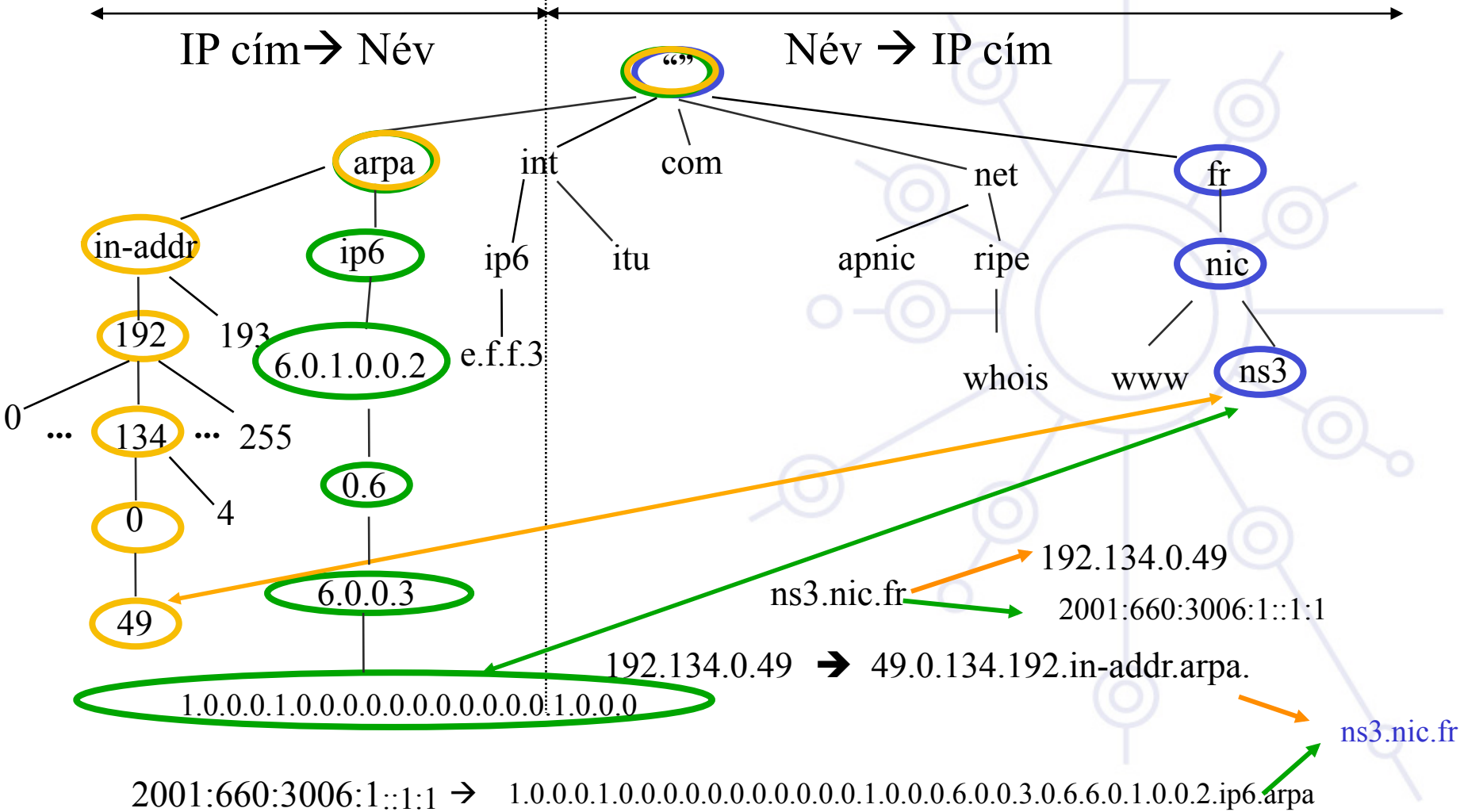
- RFC 1886 (PS) → RFC 3596 (DS) (sikeres együttműködési tesztek után)
- **AAAA** (RFC 3596): forward lookup (‘Név → IPv6 cím’):
  - Megfelel az **‘A’** recordnak
  - Példa:

```
ns3.nic.fr.        IN      A       192.134.0.49
                   IN      AAAA    2001:660:3006:1::1:1
```

- **PTR** : reverse lookup (‘IPv6 cím → Név’):
  - Reverse tree megfelelően az **in-addr.arpa** -nak
    - Nibble (4 bits) boundary
    - New tree: **ip6.arpa** (RFC 3596), használatban
    - Former tree: **ip6.int** (RFC 1886), elavult
  - Példa:

```
$ORIGIN 1.0.0.0.6.0.0.3.0.6.6.0.1.0.0.2.ip6.{int,arpa}.
1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0   PTR   ns3.nic.fr.
```

Lekérdezés egy IPv6-képes DNS fán




6deploy
IPv6 bevezetési stratégiák
campus és szolgáltató
környezetben

Figyelmeztetés ...

Ez a terület folyamatosan fejlődik

- ismeretek és ötletek tapasztalt szakemberektől

- nem akarjuk azt mondani, hogy mindenki ugyanezt csinálja, csak ötleteket adunk

- minden intézmény speciális, ezért muszáj előzőleg átgondolni, hogy mit kell tenni és hogyan

Áttekintés

Campus bevezetési stratégia

Campus IPv6 cím allokáció és menedzsment

Campus bevezetési topológia – lehetőségek

Campus szolgáltatások

Szolgáltatói bevezetési megfontolások

Áttekintés

Campus bevezetési stratégia

Campus IPv6 cím allokáció és menedzsment

Campus bevezetési topológia - lehetőségek

Campus szolgáltatások

Szolgáltatói bevezetési megfontolások

Különböző Campus átmenet megközelítések

Az IPv4 évekig használatban lesz miután az IPv6 kiépült.

Az IP protokoll mindkét verziójának jelen kell lennie.

Dual Stack

- szerverek/kliensek mindkét protokollt ismerik
- alkalmazások/szolgáltatások kiválasztják a kívánt verziót

Tunneling (“connecting IPv6 clouds”)

- IPv6 adatcsomagként az IPv4 csomagban vagy MPLS keretben

Transzlációs megoldások (“IPv4<->IPv6 services”)

- Layer 3: IP fejléc információk átírásával (NAT64)
- Layer 4: TCP fejléc átírásával (TRT)
- Layer 7: Application layer gateways (ALGs)

A dual-stack előnyei

A dual-stack bevezetésével tesztelhetők IPv6-only eszközök/szolgáltatások, anélkül hogy az IPv4 kapcsolatokat megszakítanánk.

Dual-stack IPv6 + IPv4 NAT: hagyományos IPv4 alkalmazások (email, www) használhatók az új IPv6 alkalmazások mellett (p2p, home networking, …)

- Az IPv6 új generációs alkalmazásokat kínál

Campus bevezetési terv/1

1. **IPv6 címtartomány igénylése az ISP-től**
   - Az ISP-k általában egy /32 prefixet kapnak a RIPE NCC/RIR-ektől
   - Egyetemek/felhasználók egy /48 prefixet kapnak az NREN/LIR-ektől
2. **Külső IPv6 kapcsolat igénylésre**
   - Ha lehetséges akkor dual-stack kapcsolat
   - Sok intézmény fog tunnelt használni IPv6 szolgáltatás eléréshez
     - ebben az esetben biztosítani kell, hogy senki se tudja rosszindulatú célokra használni a tunnelt – pl. filtering használatával

Campus bevezetési terv/2

3. **Belső bevezetés**
   - Meg kell határozni egy IPv6 tűzfal/biztonsági policy-t
     - Az IPv4 tűzfal/biztonsági policy jó kiindulópont
   - Ki kell fejleszteni egy IPv6 címzési tervet az adott site-ra
   - Meg kell határozni a cím kiosztási policy-t (RA/DHCPv6?)
   - Dual-stack infrastruktúrára átállás
     - Hálózati kapcsolatok IPv6 képessé válnak
   - IPv6 szolgáltatások és alkalmazások
     - Kezdve a DNS-sel
   - IPv6 engedélyezése a hosztokon (Linux, WinXP, Vista, Mac OS X…)
   - Menedzsment és monitoring eszközök használata

IPv6 kapcsolódás

- **Kapcsolat**
  - Dual Stack kapcsolat vagy dedikált kapcsolat?
  - Dedikált kapcsolat esetén – milyen útvonalon?
  - A teljes kapcsolaton van IPv6? – ha nem akkor melyek a nem IPv6 képes komponensek. Hogyan lehet őket IPv6 képessé tenni? Lehetséges-e a jelenlegi kapcsolaton egy másik VLAN-ban/VRF-ben átvinni az IPv6-ot?
  - SLA- mint IPv4 esetén?
- **Prefix**
  - Milyen prefix-et lehet használni – milyen prefixet fogad el?
- **Routing**
  - Milyen IPv6 kapcsolata van?
- **IPv6 szolgáltatások –** BGP, QoS, DNS, Webhosting

Áttekintés

Campus bevezetési stratégia

Campus IPv6 cím allokáció és menedzsment

Campus bevezetési topológia - lehetőségek

Campus szolgáltatások

Szolgáltatói bevezetési megfontolások

Az IPv6 címzési terv céljai

- Könnyebb biztonsági policy implementáció
- Könnyebben követhető cím használat – helyek szerint
- Jobb skálázhatóság - mint IPv4 esetén
- Jobb hálózat menedzsment kialakításának lehetősége

Campus címzés

A legtöbb site /48 –at fog kapni:

16 bit marad az alhálózatoknak–hogyan használjuk?

Két fő kérdést kell megválaszolni:

Topológiailag hány különböző „zónát” tudunk azonosítani ?

- Meglévőket, vagy újakat tudunk létrehozni bármilyen célból

Hány hálózat (alhálózat) szükséges ezekben a zónákban?

Példahálózat. «zónák»

Zóna leírás	Alhálózatok száma
Upstream interco and infrast	16
Administration services	4
Medical Sciences dept	32
Dept A	16
Dept B	16
…	

Campus címzés - site level subnetting – 1. módszer

1. Szekvenciálisan, pl.

- 0000
- 0001
- …
- FFFF

0020/60

0030/60

- 16 bit = 65536 alhálózat

Alhálózat ID	Zóna leírás
0000 / 60	BB Infrastructure
0010 / 60	Administration
0020 / 59	Medical Sciences dept
0040 / 60	Dept A
0050 / 60	Dept B
…	…

Prefixek fenntartása további alkalmazások számára

Campus címzés - site level subnetting – 2. módszer

2. Követve a meglévő IPv4 stratégiát:

- Alhálózatok, vagy hálózatok és alhálózatok kombinációja, vagy VLAN-ok, stb., e.g.
- IPv4 alhálózatok:
  - 152.66.**60**.0/24 0060 003c
  - 152.66.**91**.0/24 0091 005b
  - 152.66.**156**.0/24 0156 009c
- VLAN -ok:
  - VLAN id 100 0100 (w/o decimal/hex conversion)
    or 0064 (w dec/hex conversion)

Campus címzés - site level subnetting – 3. módszer

3. Topológiai/aggregációs kábelezésnek megfelelően, supernetek, nagy hálózati tartományok, stb.

- Fő könyvtár= 0010/60
  - Folyosó a könyvtárban = 001a/64
- Számítógép központ= 0200/56
  - Hallgatói szerverek = 02c0/64
- Egészségügyi fakultás= c000/52
- és így tovább. . .

Campus címzés - site level subnetting – 4. módszer

Hely-Felhasználási mód szerinti subnetelés

Hely: 4-8 bits
Felhasználás: 4-8 bits
Subnetting: 4-8 bits

Felhasználás és Hely felcserélhető

Location	Purpose	Subnetting	Description
0/52			Building A
	00/56		Servers
	01/56		Students
		0100/64	Students lab 1
		0101/64	Students lab 2
1/52			Building B
	10/56		Grid server
		1000/64	Frontends to Grid
		1001/64	Computational node set 1
		1002/64	Computational node set 2
3/52			Non-location based networks
	30/56		VPNs

Példahálózat – topológiai aggregáció + szekvenciális allokáció

Zóna leírás	Alhálózatok száma
Upstream interco and infrast	16
Administration services	4
Medical Sciences dept	32
Dept A	16
Dept B	16
…	

Érdemes elkezdeni gondolkodni róla

IPv6 alhálózat prefix allokáció (pl.)

alhálózat ID	alhálózat prefix allokáció	Leírás
0000 / 60		BB Infrastructure
	0000/64	Upstream interconnection
	0001/64	Campus architecture (DMZ)
	…	
	000B/64	Campus architecture
	…	
	000F	…
0010 / 60		Administration
	0010/64	Campus interco
	0011/64	Registration
	0012/64	Finance dept
	…	…

IPv6 alhálózat prefix allokáció pl. /2

alhálózat ID	alhálózat prefix allokáció	leírás
0020 / 60		Medical Sciences dept
	0020/64	Upstream interconnection
	0021/64	Nobel group
	…	
0030 / 60	***Reserved***	***Medical Sciences dept***
0040 / 60		Dept A
…		…

Új dolgok, amiken érdemes elgondolkodni

Használható “csupa 0” és “csupa 1”! (0000, ffff)

Nincs a szokásos 254 host/alhálózat korlát!

- LAN-ok sok L2 switch-csel, figyelembe véve a nagyobb broadcast tartományokat (kicsi ütközési tartományokkal), akár hosztok ezreit lehet 1 LAN-ba tenni

Nem szükséges a “secondary address” (habár, lehetséges több mint 1 cím/interface)

Nincsen szükség kicsi alhálózatokra (/30, /31, /32)

- meg kell tervezni, mire van szükség a backbone blokkoknál, loopback-eknél, stb.

/64 tartományt érdemes használni linkekre ha globális cím szükséges a linken

- Főleg, ha auto-konfigurációt tervezünk használni!
- Globális címek - nem minden esetben szükséges

Új dolgok, amiken érdemes elgondolkodni / 2

Minden /64 alhálózat messze több címet tartalmaz, mint amennyi szükséges a világ összes számítógépe számára

és egy /48 tartománnyal pedig 65536 ilyen alhálózatunk lehet

- ezt a hatalmat bölcsen kell használni!

Ennyi alhálózattal az IGP protokollnak akár route-ok ezreivel kell megbirkóznia

- figyelembe kell venni a belső topológiát és az aggregációt, hogy elkerüljük a későbbiekben felmerülő problémákat.

Új dolgok, amiken érdemes elgondolkodni / 3

Újraszámozásra szükség lesz szolgáltató váltás esetén. Bár az IPv6 ezt megkönnyíti, nem lesz egyszerű…

- Mindenáron kerüljük a numerikus címhasználatot
- Kerüljük az előre konfigurált címeket a hostokon, kivéve a szervereket (ez nagyon fontos a DNS szervereknél) - használjuk azt a lehetőséget, hogy hozzárendelhetünk egynél több IPv6 címet egy interfészhez (IPv6 alias címek szerverek számára)
- Számítsunk rá, hogy az ISP váltás újraszámozást jelent.
- Az ISP váltás hatással lesz az első 48 bitre, ennek ellenére a további 80 változatlan maradhat minden hoston/szerveren.

A címekkel való takarékoskodás nem elsődleges szempont

DHCPv6 segítségünkre lehet

Az alhálózat méretekről

/48 – intézmény/site (nagyon kicsi intézmény esetén: /56 esetleg /60)

/64 – alhálózat

/128 – host

Linkek subnet méretei:

Link local only: problémás lehet a traceroute6 – ipv6 unnumbered

/127: csupa 0 címet router anycast cím, bár ez nem implementált széles körben manapság. Bővebb információk: RFC 3627, RFC 6164

/126: működik annak ellenére, hogy néhány cím anycast célra van fenntartva

/120: jóval kisebb ütközés az anycast címekkel

/112: a címhatár éppen kettőspont határon van

/64: az RFC 3513 – on alapul, megengedi EUI-64 címek használatát

javasolt pont-multipont és broadcast linkek esetén

Áttekintés

Campus bevezetési stratégia

Campus IPv6 cím allokáció és **menedzsment**

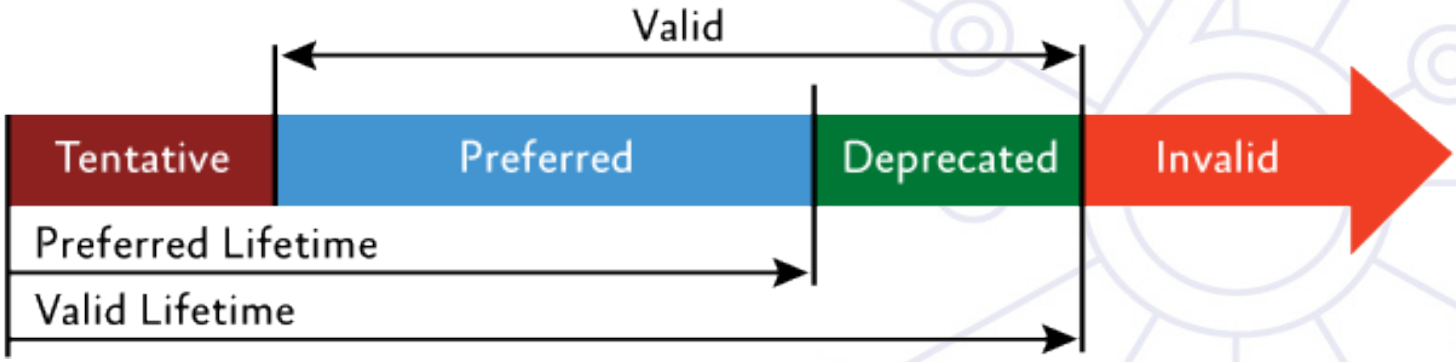
Campus bevezetési topológia - lehetőségek

Campus szolgáltatások

Szolgáltatói bevezetési megfontolások

Címek élettartama

Minden címnek van egy életciklusa:



Campus címzés – címek hozzárendelése

Milyen cím hozzárendelést használjunk?

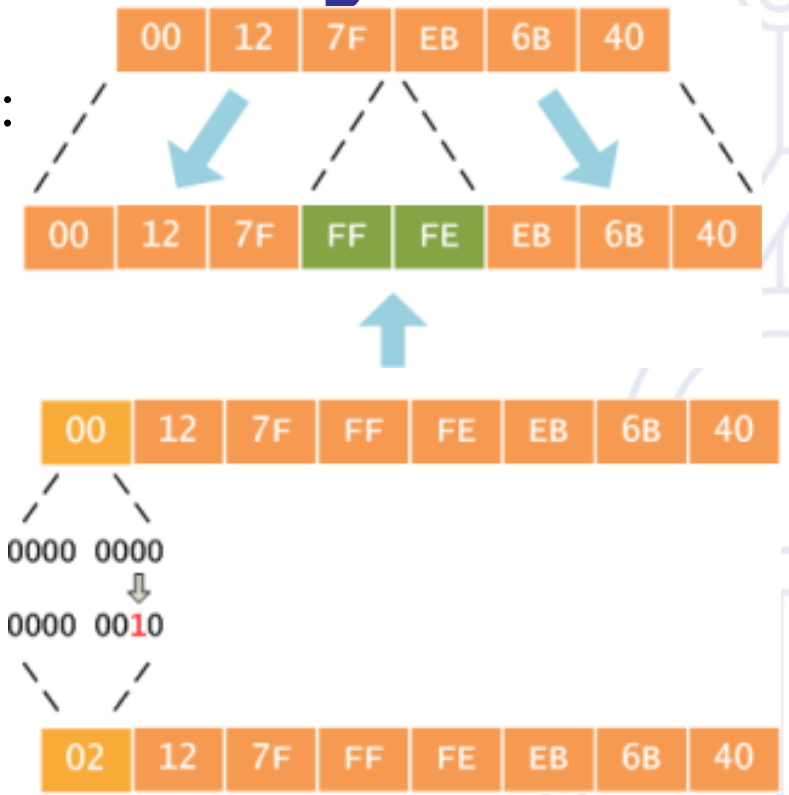
- Auto-konfiguráció – IEEE biztosítja az egyediséget
- DHCPv6 – központi menedzsment biztosítja az egyediséget
- Manuális – 7. bitnek az IID-ből 0-nak kell lennie

Melyiket használjuk host oldalon – RA üzenetekben definiált, hogy mit kell használni

- M – "Managed address configuration" flag – DHCPv6 használandó
- O – "Other configuration" flag – egyéb konfigurációs információ elérhető DHCPv6-on kereszül (DNS stb.) – stateless DHCPv6
- Mindkettő üres – SLAAC használandó

Statikus/Manuálisan konfigurált címek

Ismétlés EUI-64-ből:



Azért invertáljük az 'u' bitet, hogy amikor kézzel hozzuk létre az interfész ID-t, megkönnyítsük a rendszer adminisztrátorok számára a local scope azonosítók kézi konfigurációját. Ennek feltételezhetően soros linkeknél, tunnel végpontoknál és szervereknél stb. lesz jelentősége. pl ::1, ::2, stb.

Campus címzés – cím hozzárendelés

Melyik cím hozzárendelést használjuk?

- Autoconfiguration - IEEE biztosítja az egyediséget
- DHCPv6 - központi menedzsment biztosítja az egyediséget
- Manuális – 7. bitnek az IID-ből 0-nak kell lennie

Módszerek manuális cím hozzárendeléshez:

IID rész	Leírás
0000::<kicsiszám>	**Könnyű megjegyezni az allokációt – pl. ugyanazt a végződést használni, mint IPv4-ben**
0080:vvww:yyzz:XXXX/112	**Automatikusan hozzárendelve a vv.ww.yy.zz IPv4 cím: /112 tartozik az IPv4 host-hoz – szolgáltatás virtualizációhoz jól használható**

Stateless address autoconfiguration [RFC4862]

Plusz lehetőség a manuális konfigurácó és a DHCP mellett

Mindenütt működik

Ne használjunk auto-konfigurált címeket stabil szolgáltatásokhoz (pl. email, DNS, web) – a szerverek változhatnak idővel (hálózat kártya csere, teljes szerver csere stb.) -> az auto-konfigurált cím változhat.

DNS szervereket ki kell egészíteni DHCPv6-tal, vagy RDNSS [RFC 5006] opció használatával:

- Cisco router konfiguráció részlet:

```
ipv6 dhcp pool dhcp6dns
  dns-server 2001:db8:0::2
  domain-name example.hu
```

- és az interfészen konfiguráció:

```
ipv6 nd other-config-flag
ipv6 dhcp server dhcp6dns
```

Problémák a SLAAC-vel

Rogue RA-k [RFC 6104]

Lehetséges megoldások:

1. RA snooping - RA Guard [RFC 6105]
2. ACL a switch-eken
3. SEND használata
4. RA router preference használata – magasra állítani
5. Layer 2 admission control – pl. 802.1X alkalmazása
6. Host based filtering – nem kívánatos RA-k
7. Hibás RA üzenetek monitorozására, kezelésére eszközök:
    1. rafixd: http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/rafixd/
    2. ramond: http://ramond.sourceforge.net/
8. DHCPv6 használata prefix és default gateway opcióval

Privacy Enhanced SLAAC [RFC4949]

megakadályozza az eszköz/felhasználó követését harmadik fél számára

a felelősségre vonhatóság csökken

Szigorú környezetben le kell tiltani

Windows kliensek: `netsh interface ipv6 set privacy=disabled`

Kriptográfiailag generált IPv6 cím(CGA)

Alapötlet: Interface Id = hash (Nyilvános kulcs)

A nyilvános kulcs hitelesíti a CGA címekről küldött üzeneteket

Cím birtoklás bizonyítás biztonsági infrastruktúra nélkül

Nem széleskörben implementált és hozzáférhető

CGA: [RFC3972], HBA:[RFC5535]

DHCPv6

Az IPv6-ban létezik stateless address autoconfiguration, de működik a DHCPv6 is. (RFC 3315)

DHCPv6 használható címkiosztásra, továbbá egyéb információk szolgáltatására mint például name server, NTP server stb.

Ha a DHCPv6-ot nem használjuk címkiosztásra, nincs szükség állapotokra a szerver oldalon, és a protokollnak csak egy része szükséges. Ezt nevezzük *Stateless DHCPv6*-nak (RFC 3736)

Néhány szerver és kliens implementáció csak Stateless DHCPv6-ot használ, amíg mások a teljes DHCP protokollt.

- Néhány kliens nem implementálta még a DHCPv6 klienst. (Lion előtti Mac OS X, WinXP)

A két fő megközelítés:

- Stateless address autoconfiguration stateless DHCPv6-tal a egyéb információkért.
- DHCPv6 használata a címekhez és egyéb információkhoz, hogy jobban ellenőrzött legyen a címek hozzárendelése.

Stateful Autoconfiguration DHCPv6 [RFC3315]

A DHCPv6 kliens-szerver modellben működik

- Szerver
  - Megválaszolja a kliensek kéréseit
  - Opcionálisan szolgáltat a kliensnek:
    - IPv6 címeket
    - Egyéb konfigurációs paramétereket (DNS szerverek…)
  - A következő multicast címeken figyel:
    - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
    - All_DHCP_Servers (FF05::1:3)
  - A szolgáltatói eszközökhöz történő hozzáférésvezérlés biztosítását végzi.
  - Általában eltárolják a kliensek állapotát, annak ellenére, hogy állapotmentes működés is lehetséges (RFC 3736). (a szokásos módszer amit használnak IPv4-hez jelenleg)

Stateful Autoconfiguration DHCPv6 /2

- Kliens
  - Kéréseket kezdeményez a linken, hogy konfigurációs paramétereket kapjon
  - Link-local címet használ a szerverhez csatlakozáshoz
  - Request-eket küld a FF02::1:2 multicast címre (All_DHCP_Relay_Agents_and_Servers)
- Relay agent
  - Egy csomópont, amely közvetítőként továbbít DHCP üzeneteket a kliensek és szerverek között.
  - A klienssel azonos alhálózaton
  - Multicast címen figyel:
    - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)

Stateful Autoconfiguration DHCPv6 /3

1. Mi a DNS szerver címe
2. A host DHCPv6 klienst futtat
3. A kliens küld egy Information-Request-et
4. A szerver visszaküld egy Reply üzenetet
5. A host felkonfigurálja a DNS szervert

Example: in /etc/resolve.conf file

DHCPv6 bevezetési problémák

Egy lehetséges probléma a DHCP-nél, hogy a DHCPv4 csak IPv4 információkat (szerverek címei stb.) szolgáltat, a DHCPv6 pedig csak IPv6 információkat. Egy dual-stack host futtassa mindkettőt, vagy csak az egyiket (de melyiket)?

Különböző gyártók dolgoznak a DHCP integrációján – különböző implementációk elérhetők jelenleg:

- dibbler http://klub.com.pl/dhcpv6/
- KAME-WIDE DHCPv6 http://sourceforge.net/projects/wide-dhcpv6/
- ISC DHCPv6 https://www.isc.org/software/dhcp
- A Cisco routereknek van egy beépített stateless szerverük, amely tud küldeni alapvető információkat, mint névszerver és domain név (SIP szerver opciók is).
- Sok Linux disztribució és *BSD nem használja alap installáció esetén a DHCPv6-ot

DHCP-t használhatunk routerek között is prefix delegációra (RFC 3633). Számos implementáció létezik. Pl. a Cisco routerek kliens és szerverként is tudnak működni.

DHCPv6 további információk

Emlkéztető

BootP – kliens azonosítás MAC cím alapján

DHCP – kliens azonosítás MAC cím alapján vagy client ID-val

DHCPv6 – kliens azonosítás DUID-dal (DHCP unique ID)

- DUID is opaque in the communication

DUID típusok:

DUID-LLT – Link-Layer cím + idő

Type:1	Hardware Type: (Ethernet=6)
Time (time() since 1 Jan 2000)	
Link-Layer Address (variable)	

DHCPv6 további információk /2

DUID típusok:

DUID-EN – gyártóhoz rendelt a gyártói azonosító alapján

DUID-LL – Link-Layer cím

Type:3	Hardware Type: (Ethernet=6)
Link-Layer Address (variable)	

Néhány fontos terminológia:

IA – "identity-association" konstrukció, amely a szerver és a kliens képes azonosítani és menedzselni több IPv6 címet (klienshez rendelt címeket) – hasonló időzítés mint SLAAC esetén

IAID, IA_TA, IA_NA

DHCPv6 szoftverek képességei

Dibbler

Windows és Linux

Rugalmas – számos opció, RFC-k, és draft-ok (pl. DS-lite) is támogatott

Néha összetett konfiguráció

WIDE-DHCPv6

Linux, *BSD, UNIX

Nincs IA_TA támogatás, a kliensekben csak DUID_LLT támogatás

Képes szerverként és kliensként futni ugyanazon gépen

Windows (Vista, Win7)

Nincs IA_TA támogatás

WIDE kliens DUID LL

Miért?

- Az adminisztrátor nem tudja, mi az értéke az automatikusan generált DUID-nak -> új DUID generálás ismert értékekkel
- Az időbélyeg jó megoldás lehet az egyediség biztosítására, de a campus adminisztrátorok kiszámítható működést szeretnének

Új DUID létrehozás

- wide_mkduid.pl Perl script elérhető Jeffrey F. Blank-től a Michigan-i Műszaki Egyetemről:

http://www.ipv6.mtu.edu/wide_mkduid.pl

- Létre hozhatunk LLT-t és LL DUID-ot:

```
wide_mkduid.pl [ -t <time> ] { -m <macaddr> | <ifname> }
if specified, <macaddr> must be 6 colon-separated hex values
if specified, <time> must be an integer or 'now'
```

- Amiket azután a kliens konfigurációs fájl helyére kell másolni (`/var/lib/dhcpv6/dhcp6c_duid` or `/var/db/dhcp6c_duid`)

Problémák

1. **IPv6 címek – több adatbázisba konzisztensen**

   Szükséges a hostokat DNS-be regisztrálni – manuálisan fáradságos lenne a címek hossza miatt

   Szeretnénk DHCP-t is használni

2. **IPv6 cím és MAC cím összerendelése**

   Campus környezet monitorozására valós idejű információkkal kell rendelkezni – pl. későbbi incidens koordinációhoz

   Különösen fontos, ha valaki titkosítással kiegészített címeket használ

Probléma 1 – megoldás 1: L2D2 /1

Adatok tárolása adatbázisban

- LDAP

A user interface-nek platformsemlegesnek kell lennie, és könnyen hozzáférhetőnek

- HTTP és CGI

Rugalmasság

- Elosztott: HTTP, LDAP, DNS, DHCP (IPv4), DHCP (IPv6)

Robusztus

- a DNS és DHCP szerverek konfigurációs fájlokat használnak

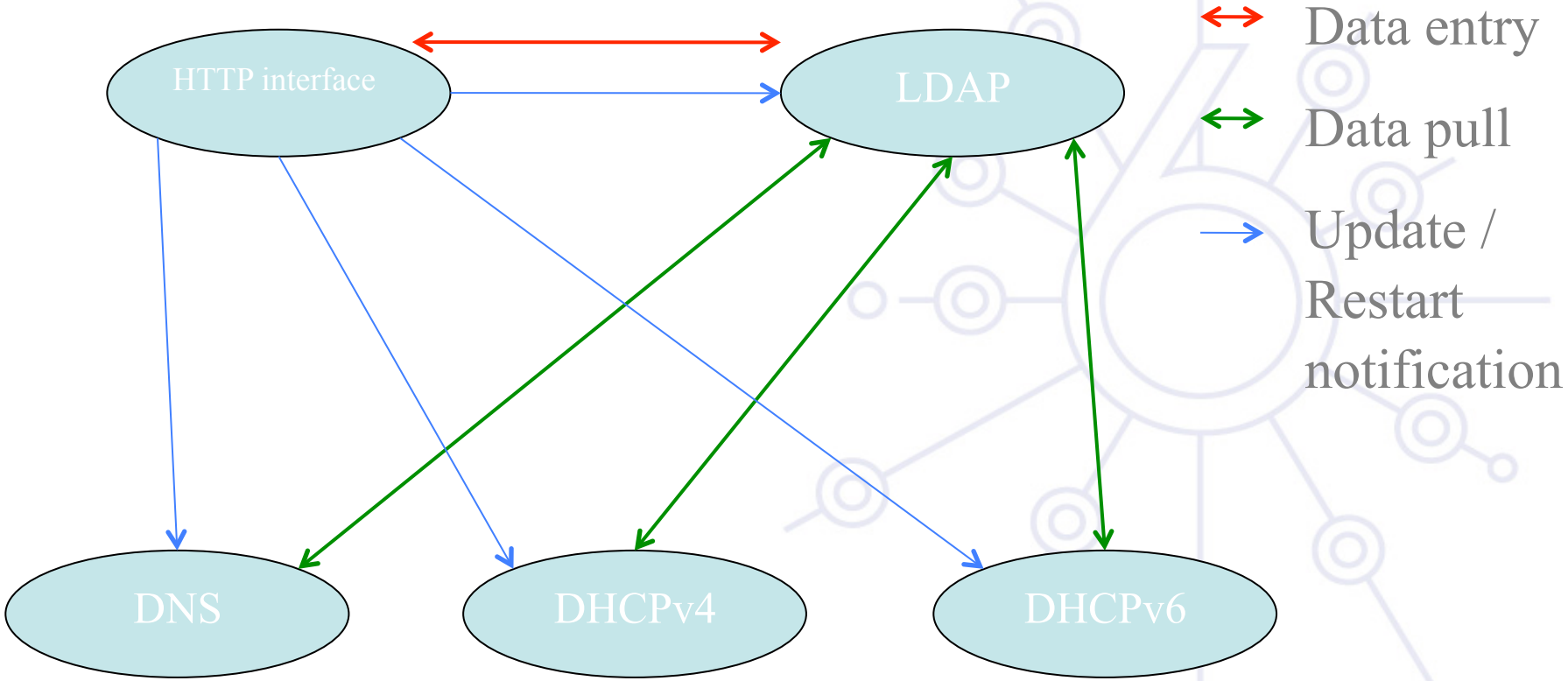
Biztonságos

- Többnyire ártalmatlan műveleteket érhetők el a szerveren

L2D2 elérhető:

- http://www.kfki.hu/cnc/projekt/l2d2

Probléma 1 – megoldás 1: L2D2 /2



Probléma 1 – megoldás 2: nsupdate használata

Scriptelhető

Néhány DHCP szerver támogatja:

- Dibbler
- ISC DHCP

Probléma 2 – megoldások

Naplózzuk az IPv6 neighbor cache-t!

1. **Gyűjtsünk IPv6 neighbor cache-t routereinkről**

   A netdisco béta verziója fel tudja fedezni a routerek ipv6 neighbor cache-ét (http://www.netdisco.org)

   Vigyázat! Ehhez a NET::SNMP::INFO::IPv6 perl module fejlesztői verziójára van szükség.

1. **Monitorozzuk a hálózati szegmensünket!**

   Sniff-eljük a szegmensünk ND és RA forgalmát: a LORIA-nál fejlesztett ndpmon segítségével (http://ndpmon.sourceforge.net/)

   Riportok: rossz MAC/IP párok, rossz router MAC, rossz router IP, rossz prefix, rossz router redirect, router flag a Neighbor Advertisment-ben, DAD DOS, flip flop, újra felhasznált régi ethernet címek

Áttekintés

Campus bevezetési stratégia

Campus IPv6 cím allokáció és menedzsment

Campus bevezetési topológia – lehetőségek

Campus szolgáltatások

Szolgáltatói bevezetési megfontolások

IPv6 bevezetési opciók

Legegyszerűbb

- dual stack hálózati környezet bevezetése

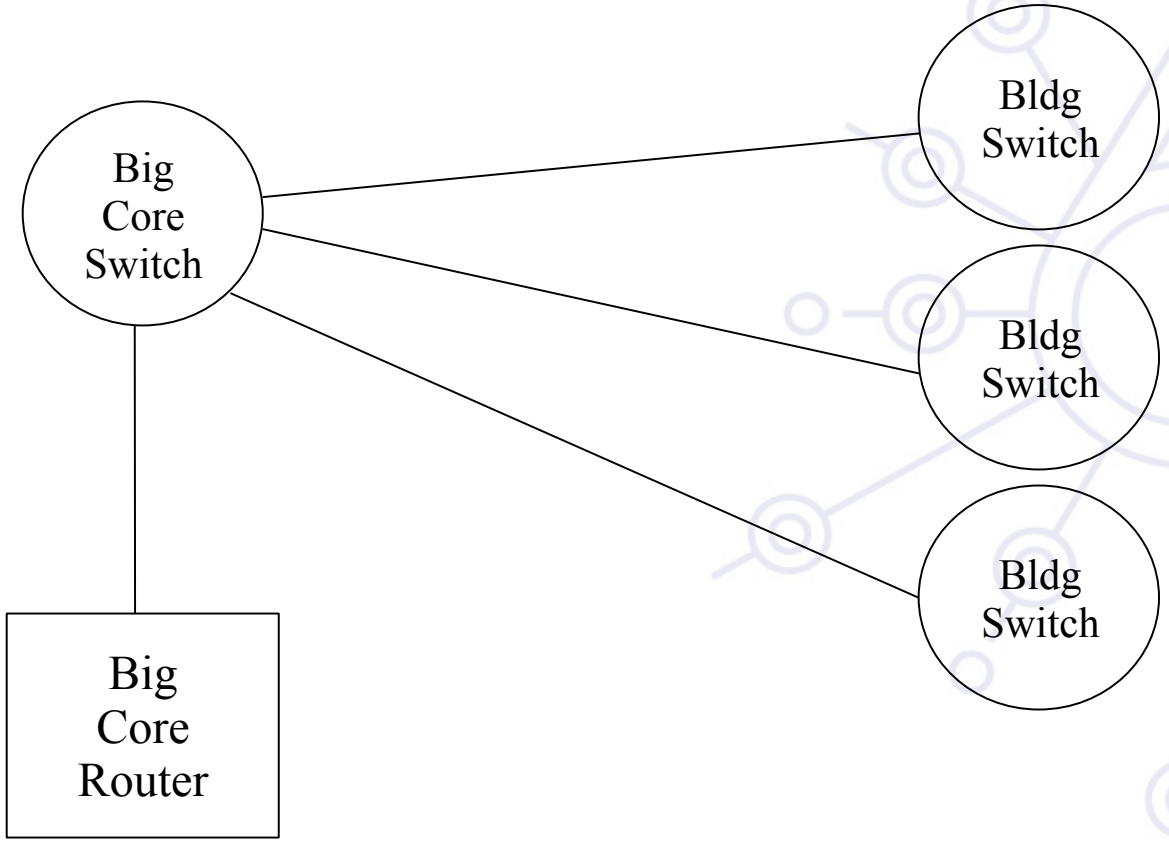
Ha a hostok/szolgáltatások nem dual stack képesek

- A dual-stack bekapcsolása enm ront el semmit
- hamis feltevésnek tűnik (Windows Vista, Mac OS X jelenlegi verzióit már IPv6 támogatással szállítják)

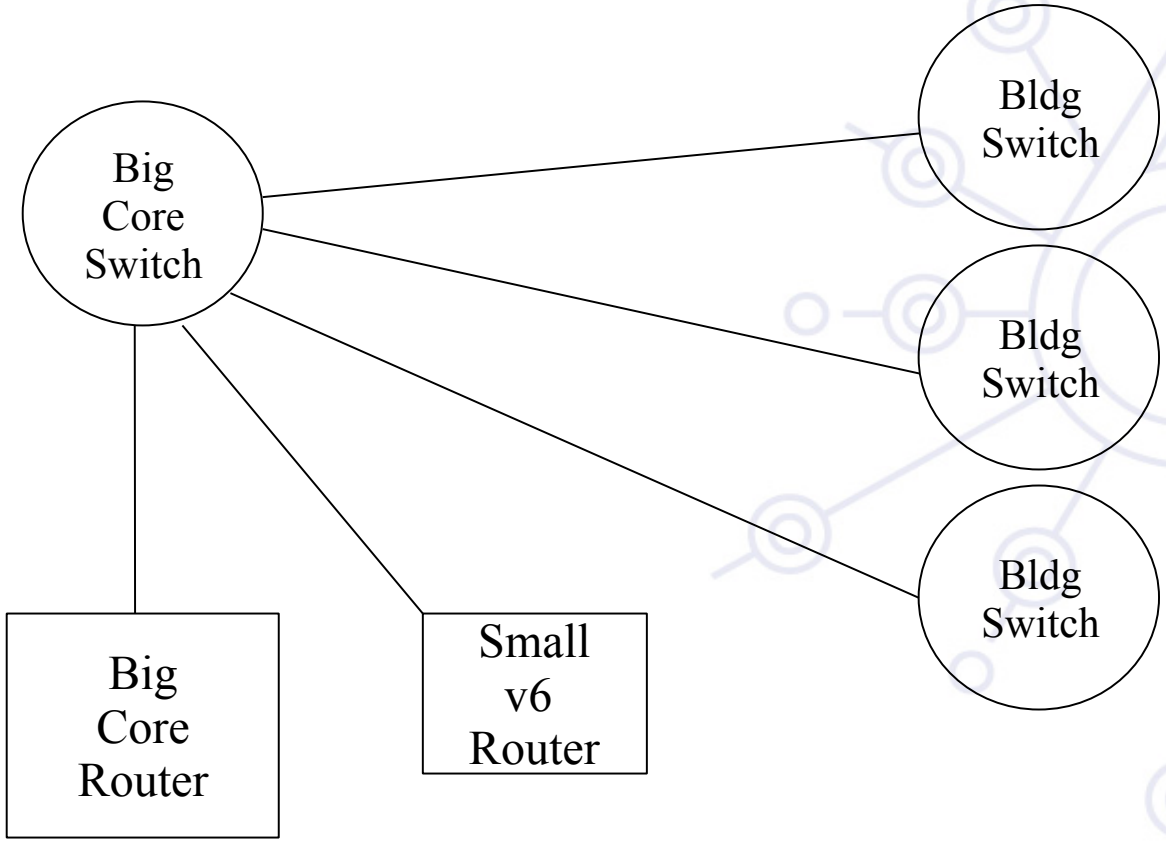
Ha a L3 eszközök nem támogatják az IPv6-ot vagy az adminisztrátorok nem szívesen upgrade-elik öket

- További IPv6 képes L3 eszköz(ök) beüzemelése
- CAPEX probléma esetén, némi plusz munkával egyszerű (olcsó) PC-ket is használhatunk

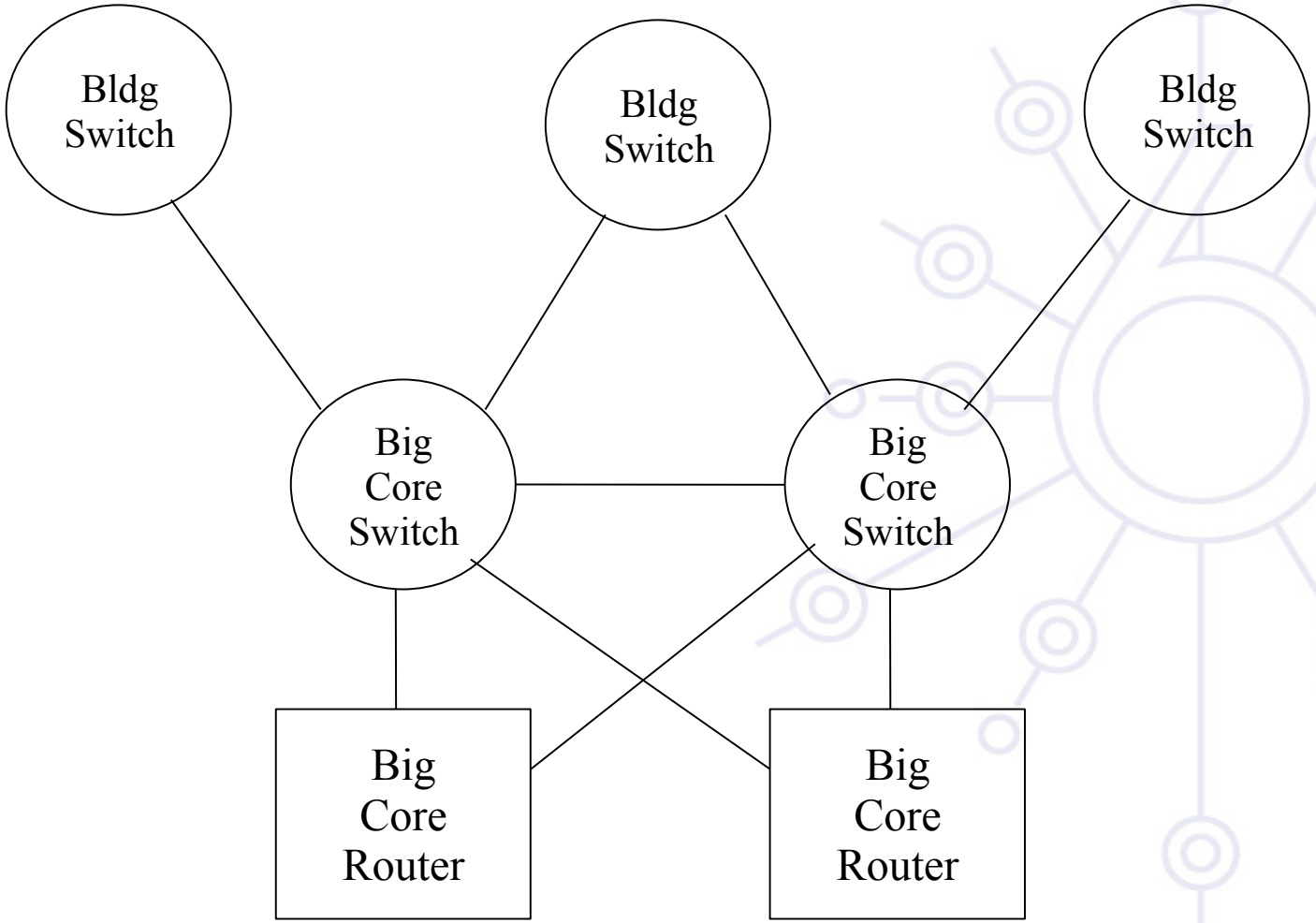
Layer-2 Campus - 1 Switch



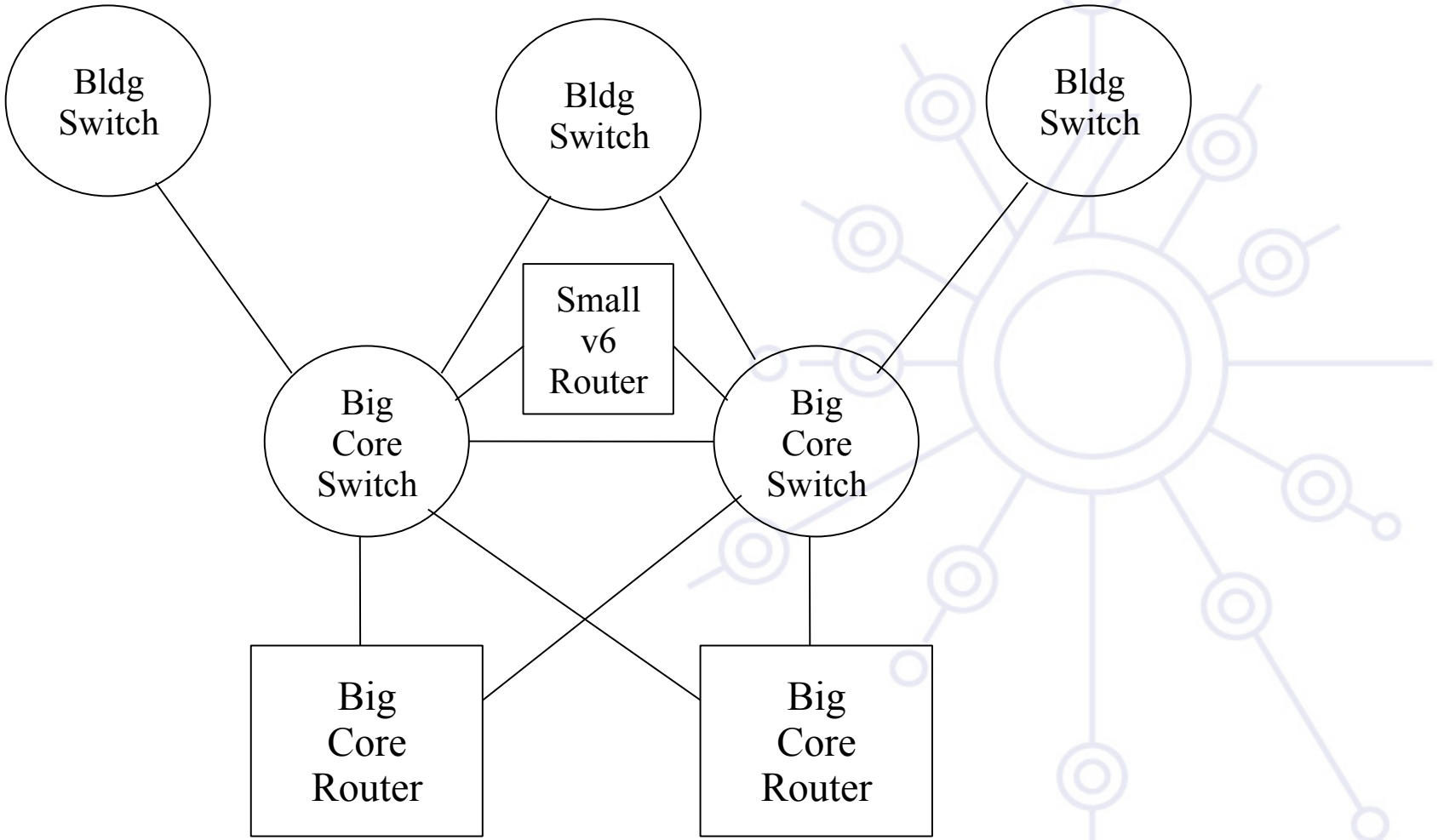
Layer-2 Campus - 1 Switch



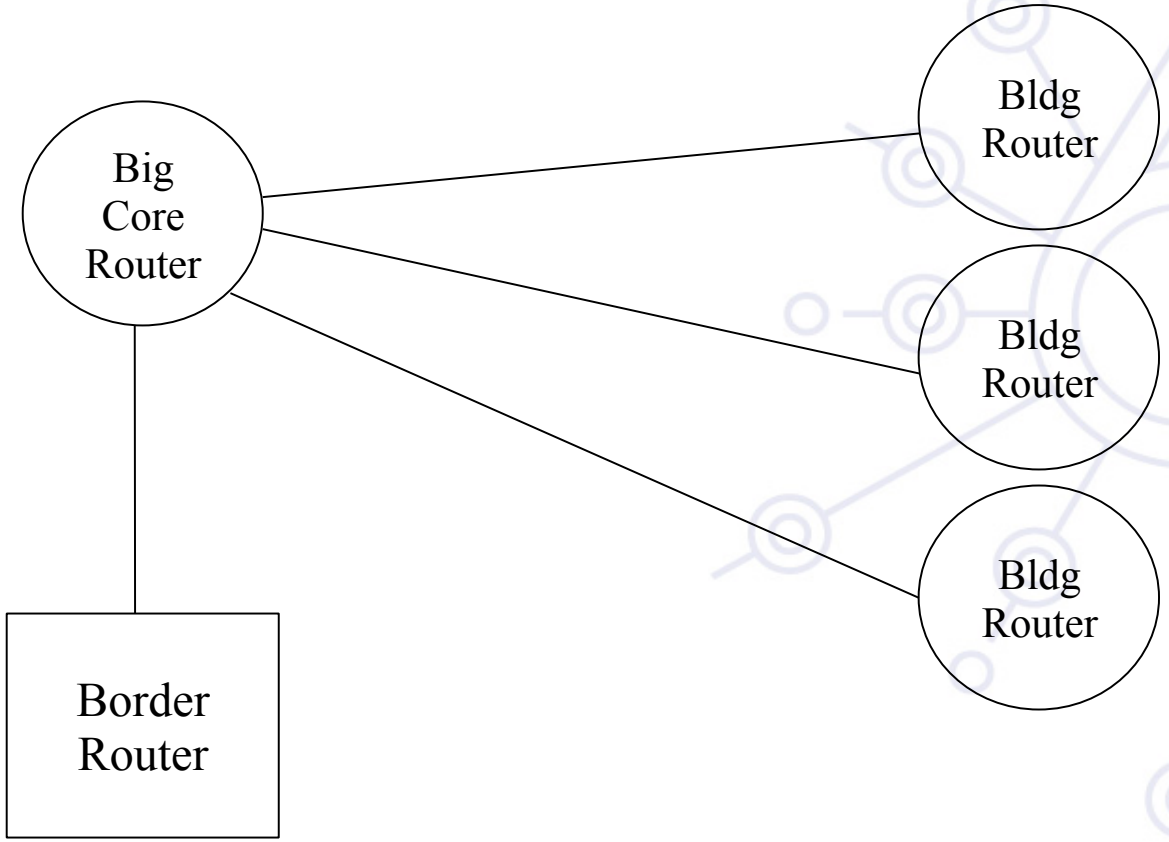
Layer-2 Campus - Redundáns switch



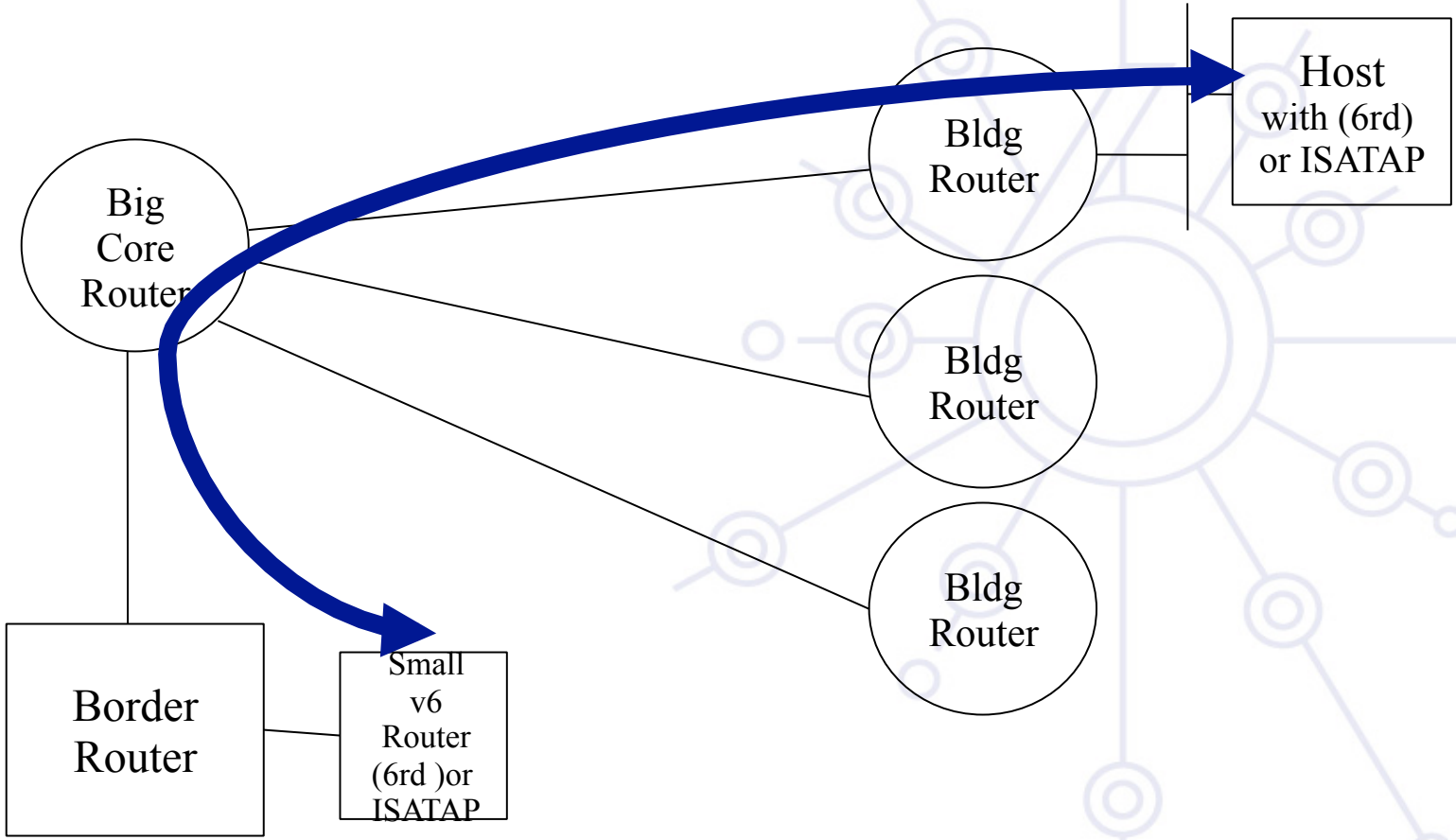
Layer-2 Campus – Redundáns switch



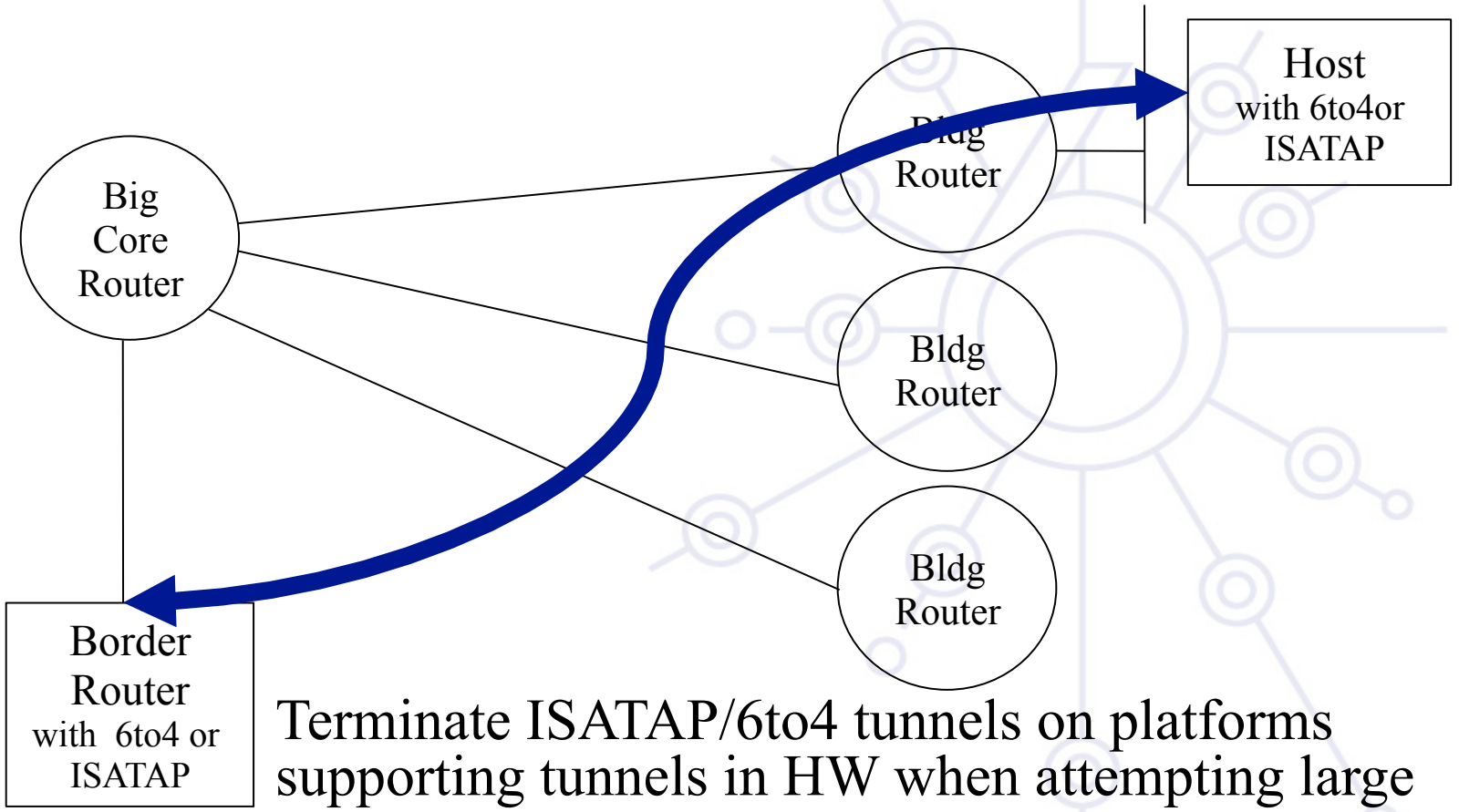
Layer-3 Campus



Layer-3 Campus – megoldás 1

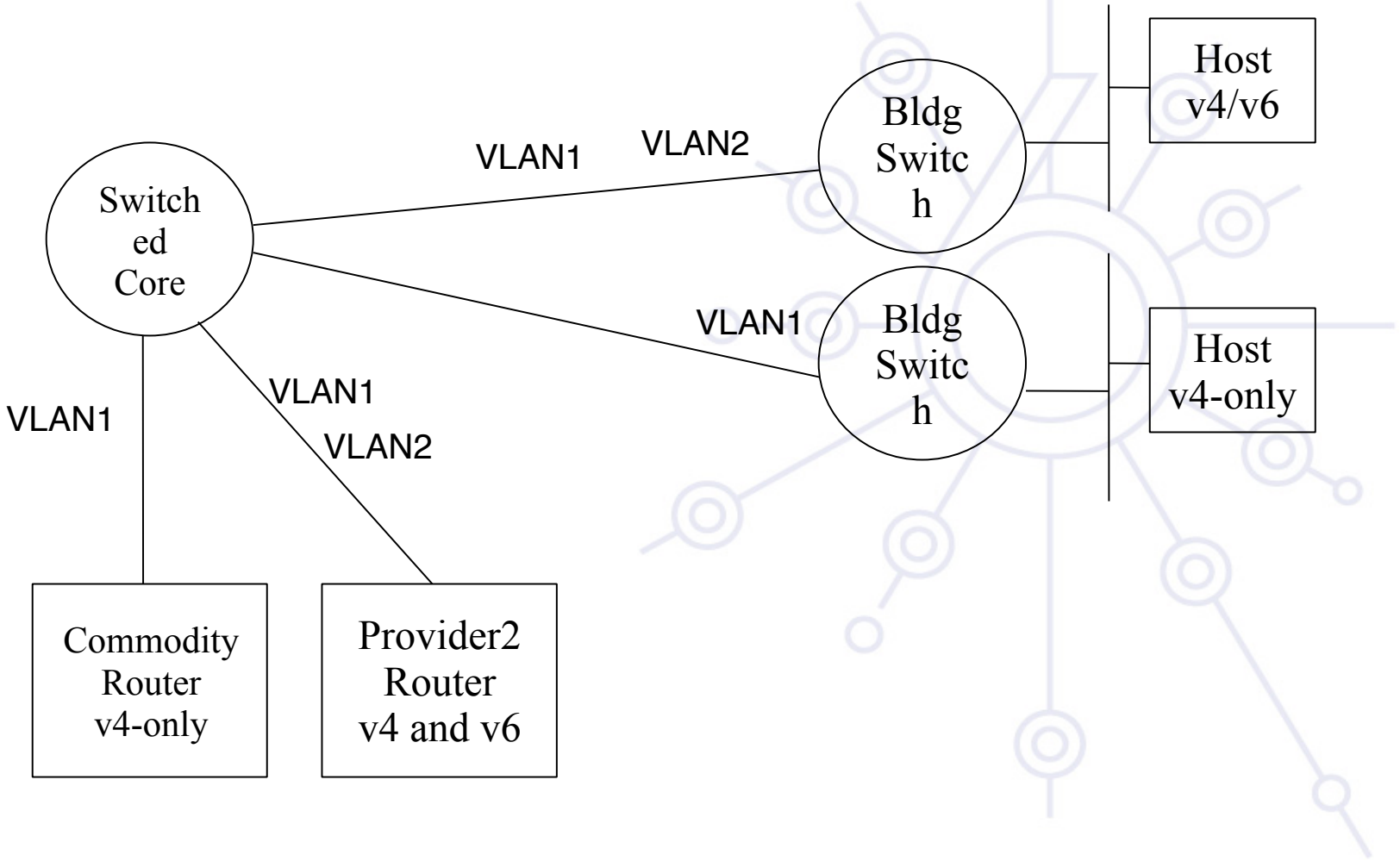


Layer-3 Campus – megoldás2



Terminate ISATAP/6to4 tunnels on platforms supporting tunnels in HW when attempting large scale (>100)deployments

Edge Router Options



Routing Protokollok

iBGP és IGP (IS-IS/OSPFv3)

- IPv6 – IPv4 iBGP session-ök
- 32 bit-es router-id szükséges az IPv6 BGP peering konfigurálásához

Statikus routing

- Az összes skálázási probléma fennáll, de kezdésnek nem rossz
- Különösen a trönkölt v6 VLAN-ban alkalmazható

OSPFv3

- Független az OSPFv2-től – egyik sem fog tudni a másikról.

Hasonló protokollokat érdemes használni, mint IPv4-ben.

Áttekintés

Campus bevezetési stratégia

Campus IPv6 cím allokáció és menedzsment

Campus bevezetési topológia – lehetőségek

Campus szolgáltatások

Szolgáltatói bevezetési megfontolások

Campus szolgáltatások

- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Távoli hozzáférés és VPN
- Biztonság politika- IPv6 Security
- Routing
- Hálózat és szolgáltatások monitorozása

Hogyan engedélyezzünk IPv6 szolgáltatást ?

v6 teszt szolgáltatás létrehozása más névvel:

- service.v6.fqdn vagy service6.fqdn AAAA-val + fordított PTR bejegyzés
- Teszteljük

v6 és v4 szolgáltatás azonos név alatt:

- service.fqdn with A +AAAA és két PTR bejegyzés.

Hogyan engedélyezzünk IPv6 szolgáltatást, ha nincs IPv6 képes szerverünk?

Használjunk proxy (pontosabban reverse-proxy) szervert

- Apache2.x proxy egy jó választás

Használjunk netcat-ot

- A hackelés egy fajtája ☺

Más proxy-k

Campus szolgáltatások

- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Hálózat és szolgáltatások monitorozása
- Távoli hozzáférés és VPN
- Nagyrendelkezésre állású megoldások
- Biztonság politika- IPv6 Security
- Routing

Dual-stack alkalmazások

Support both protocols on selected links (and nodes)

Requires support in:

- Host platforms
- Router platforms
- Applications and services
  - e.g. web, DNS, SMTP

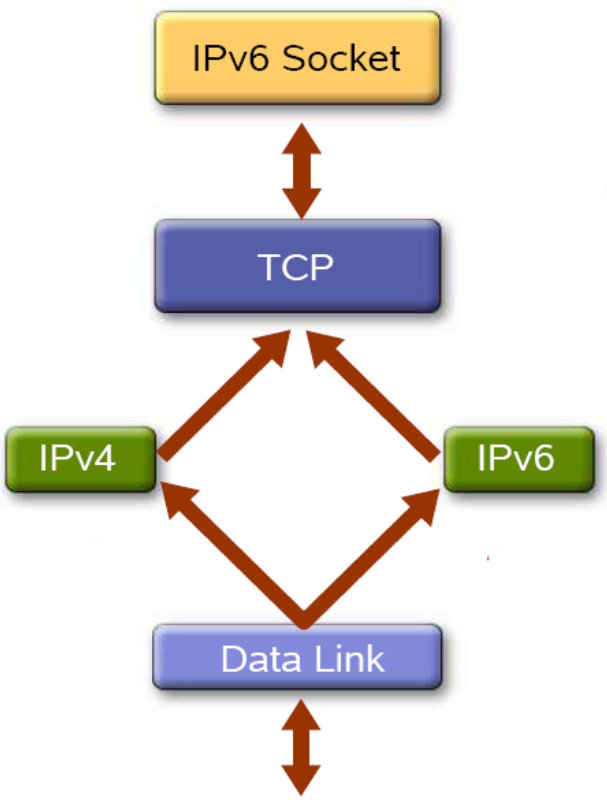
Adds considerations for

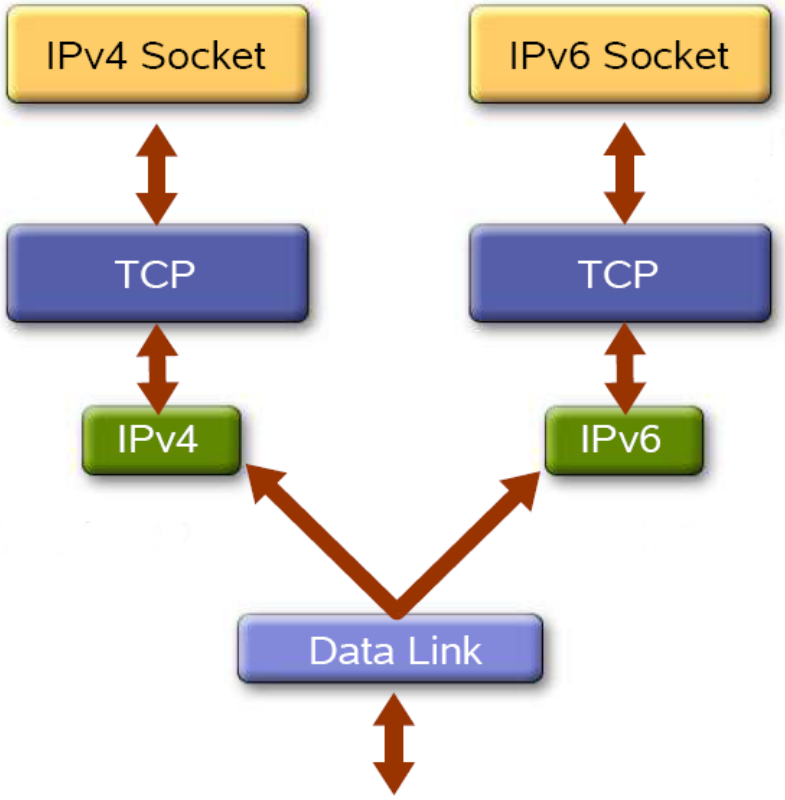
- Security in all components
- New policies dependent on IPv6-specific features

Can run global IPv6 alongside NAT-ed IPv4

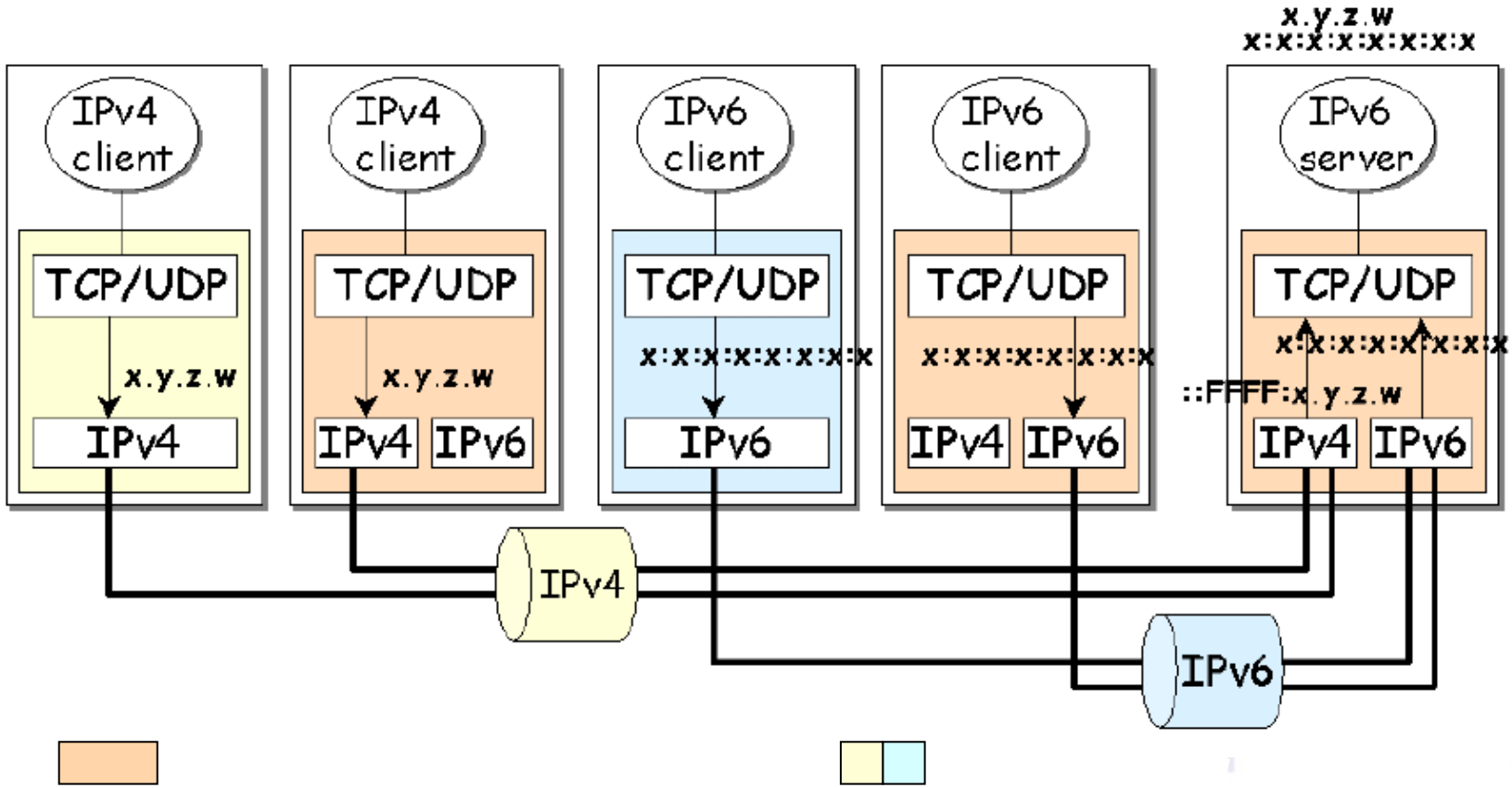
Dual stack

2 different implementations of network stack

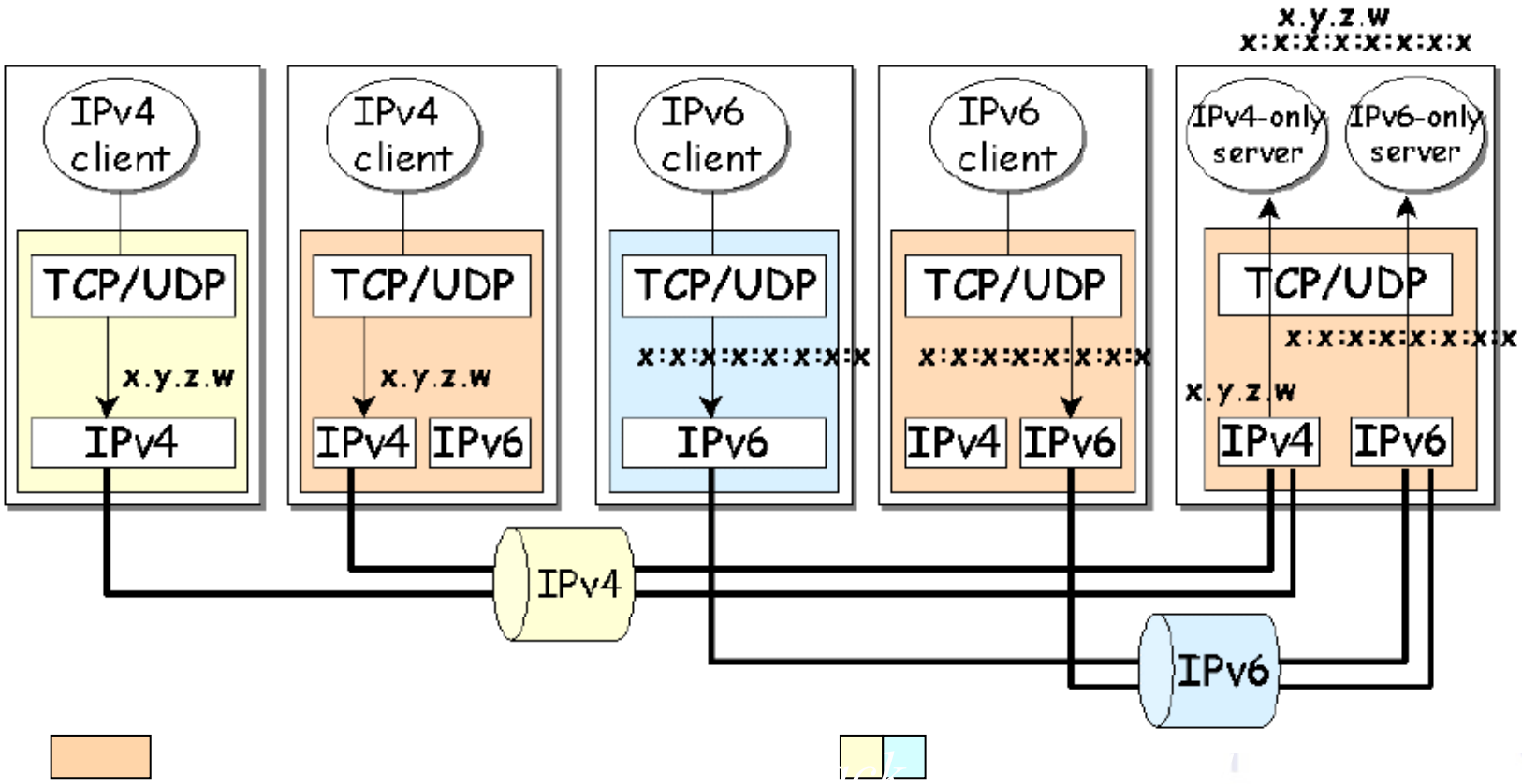




Mapping IPv4 address in IPv6



IPv4-only and IPv6-only



Campus szolgáltatások

- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Hálózat és szolgáltatások monitorozása
- Távoli hozzáférés és VPN
- Nagyrendelkezésre állású megoldások
- Biztonság politika- IPv6 Security
- Routing

IPv6 DNS támogatás

BIND8 (http://www.isc.org/products/BIND/)

- IPv6 RRs - csak AAAA
- IPv4 transzport
- IPv6 transport - patch-elve vagy v8.4.0 után, resolver v8.3.0 után

BIND9 (http://www.isc.org/products/BIND/)

- minden IPv6 RRs
- IPv4/IPv6 transzport

NSD

- Csak authoritative

PowerDNS – SQL backend

Djbdns - kerülendő!

- IPv6 RRs - csak AAAA
- csak IPv4 transzport (IPv6 transzporthoz patch-elni kell)

Unix disztribúció

- Resolver Library (+ (adaptált) BIND)

Microsoft Windows (Resolver & Server)

Bind 9 konfiguráció

named.conf bejegyzések

- Több mint egy *listen-on-v6* opció használható;

```
options {
        listen-on-v6 port   53 { any; };
        listen-on-v6 port 1234 { any; };
};
```

Zóna transzfer:

```
transfer-source-v6 1:2:3:4:5:6:7:8;
```

A lekérdezés IPv6 felett is működik:

```
query-source-v6 address * 53;
```

Ne felejtsük el frissíteni a hozzáférési listákat az IPv6 címek miatt!!

IPv6 DNS és root serverek

DNS root serverek kritikus infrastuktúra elemek

13 root – a Föld „körül” (#10 USA-ban)

Valóságban több – az anycast szerverek miatt

Nem mind a 13 szerver IPv6 képes és érhető el IPv6-on

- http://www.root-servers.org komplett és up-to-date lista.

Campus szolgáltatások

- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Hálózat és szolgáltatások monitorozása
- Távoli hozzáférés és VPN
- Nagyrendelkezésre állású megoldások
- Biztonság politika- IPv6 Security
- Routing

Alkalmazások/1

Apache

- 2.x+ verziók automatikusan támogatják az IPv6-ot
  - --enable-v4-mapped
- Listen ::
  - Listen [::]:80
- NameVirtualHost (IPv6 cím szintén)
- Access control működik – Ne felejtsük el az ACL IPv6 címmel kiegészíteni
- WebDAV szintén működik
- Apache 1.3.14-1.3.19- IPv6 patch elérhető

OpenSSH

- ListenAddress ::
- sshd -6 (-4)

Alkalmazások /2

Postfix

- **Postfix 2.2+ hivatalosan támogatja az IPv6-ot**
- **Postfix 2.1 - IPv6 patch és Ipv6+TLS patch elérhető: http://www.ipnet6.org/postfix/**
- **inet_interfaces = loopback-only" IP verzió független `/etc/postfix/main.cf`:**

```
inet_protocols = ipv4,ipv6,all
```

- **mynetworks [ipv6:addr:range]/plen**
- **smtp_bind_address6 forrás cím a kimenő SMTP kapcsolat esetén.**
- **lmtp_bind_address6 forrás cím a kimenő LMTP kapcsolat esetén**

Exim

- **HAVE_IPV6=YES Local/Makefile fileban**
- **dc_other_hostnames='…:host6.domain'**
- **dc_local_interfaces='ipv4address:2001::db8::ff47::1203::::5'**
- **dc_relay_nets='a.b.0.0/16:2001::db8::ff47::1203::::/64'**

Alkalmazások /3

Sendmail

- Az m4 konfigurációs file-ban definiálni kell az IPv6 transzportot
- DAEMON_OPTIONS('Name=MTA-v4, Family=inet')
- DAEMON_OPTIONS('Name=MTA-v6, Family=inet6')
- DBMs:
  - IPv6:2002:c0a8:51d2::23f4 REJECT
- Opció:
  - ResolverOptions=WorkAroundBrokenAAAA

Általában nincsen probléma, ha az MX-nek van IPv6 címe, de rossz MTA implementációk miatt célszerű, egy „utolsó esély" MX csak IPv4 címmel

- lásd RFC 3974

Alkalmazások /4

Microsoft Exchange

automatikus ha van IPv6 cím

Inetd

- tcp → tcp6 vagy tcp46
- udp → udp6 vagy udp46

INN

- --enable-ipv6 a configure parancshoz

Diablo news server – IPv6-ot támogatja

FTP

- vsftpd,moftpd, pure-ftpd, tnftpd, wzdftpd, lukemftpd – supports IPv6

Alkalmazások /5

Web proxy-k

- Több web-proxy támogatja az IPv6 kapcsolatokat: wwwoffle v2.7, squid v2.5 patch-el, privoxy v3.1.1, www6to4 v1.5, Prometeo v1.4, ffproxy v1.6-RC1 és polipo v0.9.x
- Privoxy:
  - listen-address [2001:db8:ff47:1203:2::5]:8118
  - permit-access [2001:db8:ff47:1203::]/64

Alkalmazások /6

Adatbázis-kezelők

- Postgresql támogatja az IPv6-ot
  - pg_hba.conf - fájlban
    - CIDR-address – IPv6 támogatott
- MySQL az 5-ös változattól

Windows filesharing

- Windows 2003 server Site-Local címekkel! – windows firewall letiltás (`netsh interface ipv6 set interface interface="Local*" firewall=disabled`) és IPv6 for Filesharing az Advanced settings fülben
- Windows Vista - OK
- Samba
  - patch-el: http://www.litech.org/samba/ vagy samba 3.3

Alkalmazások /7

NTP

- A 4.x támogatja az IPV6-ot
- /etc/ntp.conf konfigurálás – fallback nehéz az UDP miatt
- Néhány IPv6 képes NTP szerver
  - time1.niif.hu (IPv6 and IPv4)
  - ntp.rhrk.uni-kl.de (IPv4 and IPv6)
  - ntp6.remco.org (IPv6)
  - chime3.ipv6.surfnet.nl (IPv6)
  - ntp.ipv6.viagenie.qc.ca (IPv6)

CUPS

- Az IPv6 támogatott az 1.2b1 változat óta
  - /etc/cups/cupsd.conf fájlban:

    ```
    Listen [::1]:631
    ```
  - "/etc/cups/client.conf" fájlban:

    ```
    ServerName [2001:db8:ff47:1203::5]
    ```

Alkalmazások /8

TightVNC

- A helyes működéshez Windows szerveren engedélyezni az "Allow loopback connections" opciót

Telnet

- A megszokott módon (néha -4 és -6)
- Windows 2003 Telnet szerver még nem támogatja IPv6-ot , de:

  netsh interface portproxy add v6tov4 23

Alkalmazások /9

OpenLDAP

- AZ IPv6 támogatott az LDAP szerveren és kliensen is
  - Egyéb LDAP-ot használó alkalmazások is IPv6 képesek lesznek ha az OpenLDAP client library-t használják
- Sun ONE Directory szerver támogatja az IPv6-ot
- Fedora DS 1.0.3 szerver támogatja az IPv6-ot

GnomeMeeting/Ekiga + Polycom HDX

- H.323 VoIP és videokonferencia. IPv6 és *x támogatás. http://www.gnomemeeting.org/

Kphone

- IPv6 VoIP SIP alapú softphone

http://www.iptel.org/products/kphone/

Néhány programozási nyelv

Perl

- Speciális modulok mint Socket6 és IO::Socket::INET6

Python 2.3.4 és későbbi működik IPv6-al

- Habár, Windows binárisok a python.org-on nem támogatják.

PHP

- Részleges IPv6 támogatás
- Sok PHP szkript működik IPv6-on mindenféle változtatás nélkül

Java

- SUN Java SDK 1.4 és később IPv6 támogatás
- A legtöbb Java alkalmazás működik IPv6-al, mert a Java API magasabb szinten kezeli a kapcsolatokat

További alkalmazások

Nagy lista az IPv6 képes alklamazásokról

http://www.deepspace6.net/docs/ipv6_status_page_apps.html

IPv6 Application and Patch Database

- kereshető

http://ipv6.niif.hu/ipv6_apps/

- konfigurációs leírások

http://ipv6.niif.hu/faq/

Proxy megoldások

Proxy

- Squid (http://devel.squid-cache.org/projects.html)

Web Cache

- NetCache C1300, C2300, C3300. BlueCoat SG
- WCCP még nem támogatott IPv6 felett Cisco eszközöknél

Apache2 reverse proxy

Könnyű konfigurálás:

```
ProxyRequests Off
ProxyPass / http://ipv4address
ProxyPassReverse / http://ipv4address
ProxyPreserveHost On
```

Reverse proxy pro és kontra

Előnyök:

- Gyors implementálás, azonnali web szolgáltatást nyújt IPv6 felett
- Módosítás nem szükséges működő web szerver környezetben
- Lehetővé teszi a megfelelően időzített átállást
- Skálázható: egy központi proxy több weboldalt képes kiszolgálni

Hátrányok:

- Jelentős adminisztrációs többletmunka nagyméretű rendszereknél
- Elrontja a hitelesítési és hozzáférés sémákat
- Statisztikák: minden IPv6 kérés úgy tűnik egy helyről érkezik
  - Orvosolható: szűréssel és a logok elemzésével vagy egy speciális modullal a proxy-n
- Nem hosszú távú megoldás, natív IPv6 támogatás könnyen rendelkezésre áll hasonló alkalmazásokban és előnyben kell azt részesíteni, amint lehetséges

Campus szolgáltatások

- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Hálózat és szolgáltatások monitorozása
- Távoli hozzáférés és VPN
- Nagyrendelkezésre állású megoldások
- Biztonság politika- IPv6 Security
- Routing

Management és monitorozás

- Eszközök konfigurálása és monitorozása - SNMP
- Statisztikák - Cricket/MRTG/Cacti
- Szolgáltatás monitorozás - Nagios
- Behatolás érzékelés (IDS)

Campus szolgáltatások

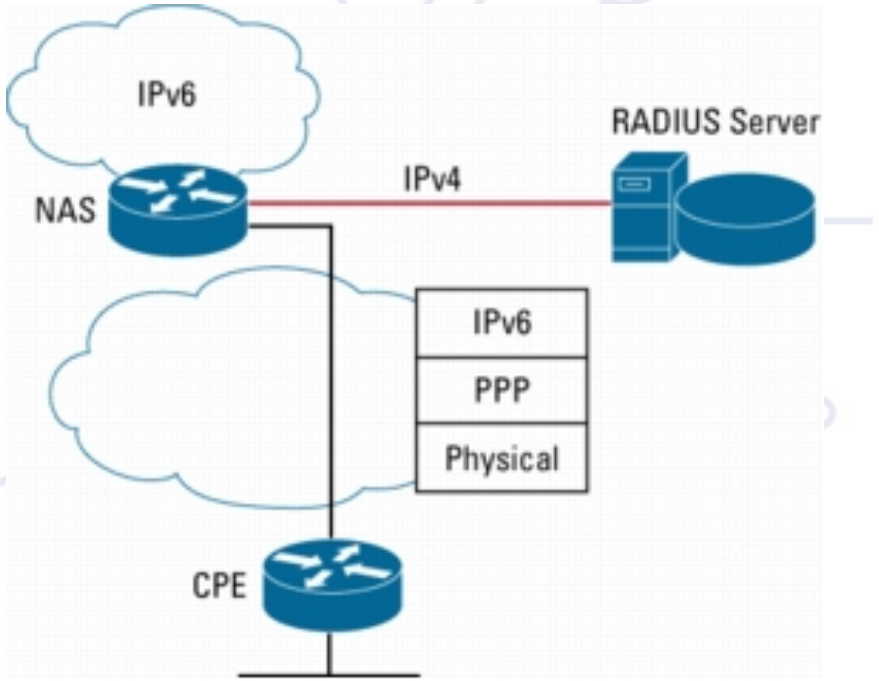
- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Hálózat és szolgáltatások monitorozása
- Távoli hozzáférés és VPN
- Nagyrendelkezésre állású megoldások
- Biztonság politika- IPv6 Security
- Routing

Távoli hozzáférés IPv6 felett

- **Használjunk natív kapcsolatot**, ha lehetséges
  - Viszonylag egyszerű, ha dial-up pool-t vagy ADSL szolgáltatást nyújtunk
- **(Open)VPN**
- **tunnel broker szolgáltatás –** Nem túl optimális
- **6to4, ha van IPv4 címünk**
  - jó 6to4 relay kapcsolat szükséges
- **Teredo/softwire** NAT-olt környezetben

Remote access via IPv6 - PPP

- **The dial-up connection uses a modem and the PSTN service in order to get connection to remote devices.**
  - Most cases use PPP (Point-to-Point Protocol), which gives a standard method to transport the datagrams of several protocols over point-to-point links (RFC1661, 2153, 5342) - PPP has been updated to support the transport of IPv6 datagrams (RFC5072)



PPP and IPv6

PPP protocol has three main parts

- Definition of the encapsulation method of the IPv6 datagrams over the point- to-point link (IP6CP)
- LCP (Link Control Protocol) used to establish, configure and test the connection at link layer
- NCP (Network Control Protocol) used to establish and configure the connection at network layer

IPv6 operation:

- negotiates one link local address (fe80::/64) between the end points or peers
- Could negotiate datagram compression via IP6CP (IPv6 Control Protocol)
- PPP does not give global IPv6 addresses but link local - The global IPv6 addresses must be configured by other means
  - Manual configuration
  - Autoconfiguration (RA)
  - DHCPv6

PPP and IPv6 - implementations

Routers:

- Cisco
- Juniper

Hosts:

- Windows Vista and Microsoft Windows Server 2008
  - Windows XP: Cfos IPv6 link http://www.cfos.de/ipv6_link/ipv6_link_e.htm
- Linux, *BSD (including Mac OS X), Solaris

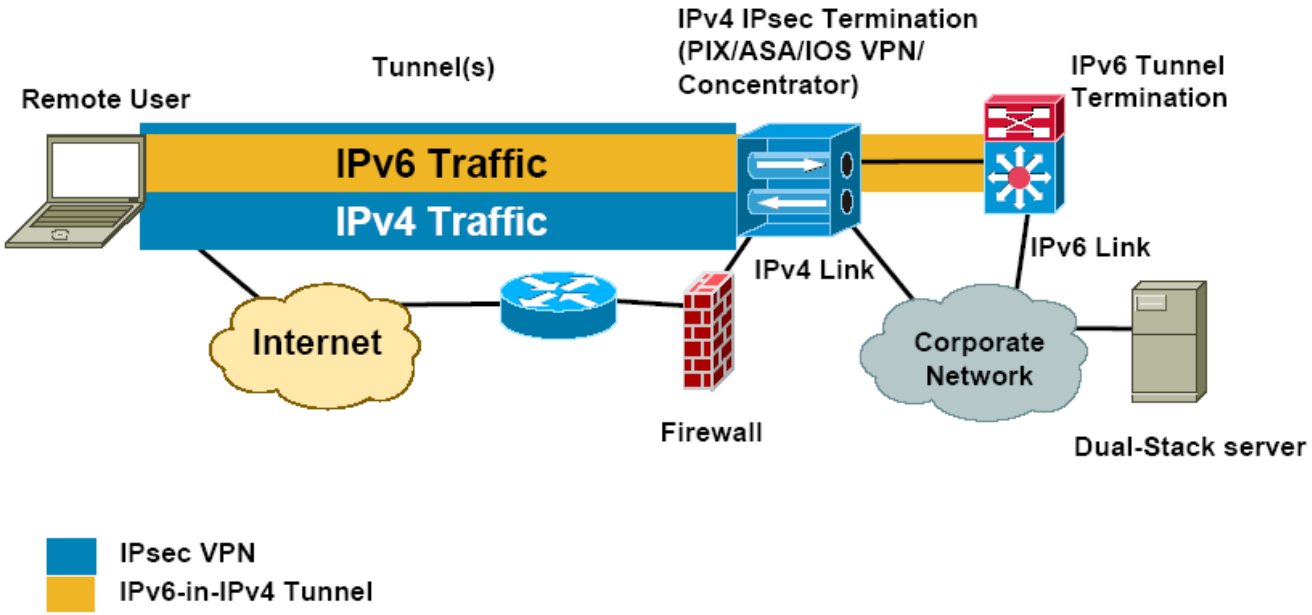
Opensource:

http://sourceforge.net/projects/pppcbcp

http://freshmeat.net/projects/pppd

Remote Access with IPSEC – or other VPNs

IPv6-in-IPv4 Tunnel Example



Cisco Anyconnect VPN

Támogatott

kliens: WinXP, Mac OS X, Linux

Campus szolgáltatások

- Névfeloldás szolgáltatás- DNS
- Alkalmazások
  - Levelezés
  - Web
    - Proxy-zás
- Hálózat és szolgáltatások monitorozása
- Távoli hozzáférés és VPN
- Nagyrendelkezésre állású megoldások
- Biztonság politika- IPv6 Security
- Routing

IPv6 terhelés elosztás – nagy rendelkezésre állás

- Server cluster-ek
  - Nyílt forrású megoldás: *BSD pf (http://www.openbsd.org/faq/pf/), Linux LVS 2.6.28 (http://kb.linuxvirtualserver.org/wiki/IPv6_load_balancing)
  - Üzleti megoldások: Veritas Cluster Server, BigIron F5, Windows Server 2008 - Network Load Balancer
- First-Hop redundancia:
  - HSRPv6 (Cisco)
  - VRRPv6 – IETF szabvány
  - NUD (Neighbor Unreachability Detection)- lásd köv. fólia
- Traffic loadbalancing
  - Multilink PPP – csak ha multilink PPP támogatott
  - Equal-Cost Multi-Path routing - ha IPv6 routing támogatott
  - Ethernet Link Aggregations - L2 megoldás

VRRP

IETF: Version 3

- RFC5798, March 2010
- Based on VRRPv2 for IPv4
- Election protocol

Usage of «virtual» addresses

- Which are used by/configured on hosts
- One of the existent VRRP routers is elected as «MASTER»

IPv6 Multicast Address

- Assigned by IANA = FF02::12

VRRP

Advantage of using VRRP on IPv4:

- Higher-availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

Advantage of using VRRP on IPv6:

- Quicker switchover to Backup routers than can be obtained with standard IPv6 Neighbor Discovery mechanisms.

Redundáns default gateway implementálása

Ha HSRP,GLBP vagy VRRP nem áll rendelkezésre

NUD alkalmazható egy elfogadható HA megoldásnak a gaterway redundancia implementálására (napjainkban csak Campus/Datacenter környezetre vonatkozik ... HSRP elérhető a routerekben)

- (config-if)#ipv6 nd reachable-time 5000

A hosztok a NUD "reachable time" változóját használják, hogy a következő ismert default gateway-t megtalálják (30 mp az alapérték)

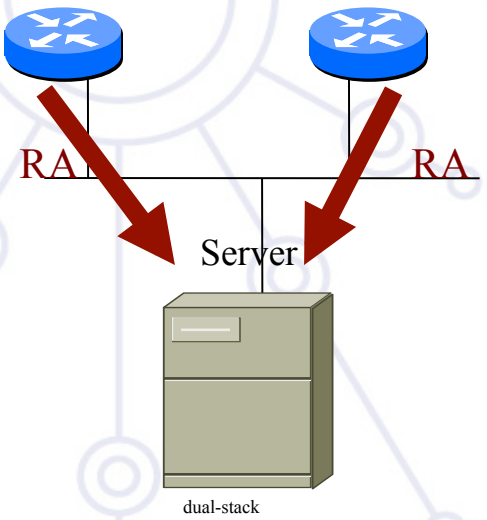
Default Gateway . . . . . : 10.121.10.1

fe80::211:bcff:fec0:d000%4

fe80::211:bcff:fec0:c800%4

Reachable Time : 6s

Base Reachable Time : 5s



Összegzés

Telepítési stratégia
- Együttélési mechanizmus?
- IPv6 prefix beszerzése
- … és külső IPv6 kapcsolat
- Biztonsági politika megtervezése

IPv6 cím allokáció és használat
- Dolgozzunk ki egy címzési tervet
- Döntsük el milyen címallokációs eljárást használunk

Telepítési topológia – opcionális
- IPv6 bevezetés megkezdése
- Hogyan oldjuk meg a távoli hozzáférést ?

Szolgáltatások
- Szolgáltatások elérésének engedélyezése IPv6-on
  - Kezdjük a DNS-sel
- Felügyeleti és monitoring eszközök IPv6-on
- IPv6 engedélyezése a hosztokon


deploy
IPv6 Biztonság

Milyen újdonságok vannak az IPv6-ban?

A biztonságot figyelembe vették az IPv6 tervezésétől kezdve

Néhány kulcsfontosságú fejlesztés:

- Az IPSEC használható mindenütt – kötelezően az implementációk része
- Kriptográfiailag generált címek (CGA)
- Secure Neighbor Discovery (SEND)
- Letapogatás/behatolás nehezebbé vált

Gateway és host szkennelés

Az alhálózat mérete sokkal nagyobb

- Kb. 28 év szükséges egy /64-es alhálózat teljes feltérképezéséhez (1 millió cím/mp)

De…

- NMAP NEM támogatja az IPv6-os hálózat szkennelést – de a host scannelést igen
- Az IPv6 szkennelés metodikája megváltozhat
  - DNS alapú, párhuzamosított, szokásos számozás
- Router feltörése egy fontos ponton
  - Aktuálisan használt címek jegyzéke

IPv6 címek biztonsága

Kriptográfiailag generált címek (CGA) [RFC 3972]

- A cím Host-ID része egy kódolt hash
  - A nyilvános kulcs hitelesíti a CGA címekről küldött üzeneteket
  - Securing Neighbor Discovery használja [RFC 3971]
  - További használat [RFC 4581]

A privát címek definiáltak [RFC 4941]

- Megakadályozza az eszköz/felhasználó követést – vannak ennél hatékonyabb eszközök
- Nehezebbé teszi elszámoltathatóságot

Host-ID, ha megfelel egy szabálynak, akkor engedélyezheti a hálózati hozzáférést

Auto konfiguráció/Neighbor Discovery

Neigbor Discovery

- Hasonló problémákkal küzd, mint az ARP cache poisoning

SEcure Neighbor Discovery (SEND) [RFC 3971]

- CGA-t használ
  - Linux/BSD implementáció: DoCoMo's Open Source SEND Project
  - Cisco implementáció

DHCPv6 + authentication lehetséges

ND + IPSec szintén

Neighbor Discovery - problémák

DoS - Duplicate Address Detection (DAD)

- Csomópontok SLAAC esetén saját maguk generálják a címüket (EUI 64, Privacy Extensions)
- Optimistic DAD – "Bocs ezt már foglalt, én használom, válassz másikat"

Neighbor Cache table overload

- Nagy címtér (64 bits – 1.8e+19 cím)
- Sok bejegyzés a szomszédségi táblában – nem létező csomópontokra

L2 switch támogatás szükséges a megakadályozásukhoz

Problémák a SLAAC-vel

Rogue RA-k [RFC 6104]

Lehetséges megoldások:

1. RA snooping - RA Guard [RFC 6105]
2. ACL a switch-eken
3. SEND használata
4. RA router preference használata – magasra állítani
5. Layer 2 admission control – pl. 802.1X alkalmazása
6. Host based filtering – nem kívánatos RA-k
7. Hibás RA üzenetek monitorozására, kezelésére eszközök:
    1. rafixd: http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/rafixd/
    2. ramond: http://ramond.sourceforge.net/
8. DHCPv6 használata prefix és default gateway opcióval

DHCPv6 problémák

Hamis DHCPv6 szerver

- Korlátozandó, hogy ki lehet DHCP szerver

DHCPv6 problems and solutions

SAVI (draft-ietf-savi-dhcp-07, November 2010)

- Komplex megoldás a következő problémákra: fake RA,DHCPv4 és DHCPv6

Szegény ember RA Guard-ja

ACL to filter RA and DHCPv6:

```
ipv6 access-list block-ra-dhcp
   10 deny icmp any any 134 0
   20 deny udp any eq 547 fe80::/64 eq 546
   30 permit ipv6 any any
exit
```

Apply for the interface:

```
interface 1-44
   ipv6 access-group block-ra-dhcp in
```

Jogosulatlan hozzáférés

A biztonsági politika implementációjának egyik legfontosabb eszköze IPv6 esetén is Layer 3,Layer 4 szintű tűzfal

Néhány tervezési szempont!

- Szűrjük ki a „site-scoped” multicast címeket a site határain
- Szűrjük ki az IPv4 mapped IPv6 címeket a „dróton”

Action	Src	Dst	Src port	Dst port
permit	a:b:c:d::e	x:y:z:w::v	any	ssh
deny	any	any		

Elárasztásos dDOS támadások

Az IPv6-ban nincsenek broadcast címek

- Ezzel kivédünk számos támadást, melyek ICMP csomagokat küldenek broadcast címre
- Globális multicast címek speciális eszköz csoportoknak

  Pl.: link-local címek, stb.

IPv6 szabvány megtiltja, hogy globális multicast címre érkező üzenetekre ICMPv6 csmag generálódjon

- Számos népszerű operációs rendszer követi ezt a specifikációt
- Még mindig kérdéses az ICMP csomagok veszélye, globális multicast forráscímmel

IPv6 erősítéses támadás megakadályozása

A hoszt implementációk kövessék az ICMPv6 specifikációját [RFC 4443]

Használjunk Ingress Filtering-et

- „Denial of Service Attacks” jellegű támadások ellen IP Source Address Spoofing [RFC 2827]

Használjunk ingress filtering-et IPv6 csomagoknál IPv6 multicast forrás címre

Tűzfalak

IPv6 architektúrák és tűzfalkövetelmények

- NAT nem szükséges – hasonló szintű biztonság érhető el IPv6-tal mint IPv4-gyel (biztonság és adatvédelem)
  - Még jobb: e2e biztonság IPSec-kel
- A csomagszűrés gyengeségeit nem tudjuk NAT-tal elrejteni
- Az IPv6 nem követel end-to-end kapcsolatot, de end-to-end címzést tesz lehetővé
- Támogassa IPv4/IPv6 átmenetet és együttes használatot
- Ne veszélyeztesse az IPv4 biztonságot

IPv6 képes tűzfalak

PL.: Cisco ACL/PIX, iptables, ipfw, pf, Juniper NetScreen

Tűzfalkövetelmények

Nem lehet vakon kiszűrni ICMPv6-t:

Echo request/reply	Debug
Destination unreachable	Debug – jobb hibajelzés mint ICMPv4 esetén
TTL exceeded	Hibajelentés
Parameter problem	Hibajelentés
NS/NA	Szükséges a helyes müködéshez – kivéve statikus ND bejegyzések esetén
RS/RA	SLAAC esetén szükséges
Packet too big	Path MTU discovery
MLD	Nem link-local multicast esetén követelmény

[IPv6 specifikus]

[szükséges]

Tűzfalkövetelmények 2

Nem lehet vakon kiszűrni az IP opciókat (→ extension Header):

Hop-by-hop header	Mit kell tenni jumbogramokkal és router alert opcióval? – multicast join üzenetekhez szükséges...
Routing header	Source routing – IPv4 esetén kártékonynak minősített, de szükséges IPv6 mobilitáshoz – csak a Home Agent-en szükséges engedélyezni a Type 2 típusú RH-t
ESP header	Biztonsági policy szerinti feldolgozás
AH header	Biztonsági policy szerinti feldolgozás
Fragment header	Minden fregmens kivéve az utolsót 1280 octetnél hoszabb kell, hogy legyen

IPv6 tűzfalak alkalmazástámogatása

FTP:

- Elég komplex: PORT, LPRT, EPRT, PSV, EPSV, LPSV (RFC 1639, RFC 2428)
- IPv6 tűzfalakban alig van támogatás
- A HTTP tűnik a következő generációs fájltranszfer protokollnak különösen WEBDAV és DELTA kiegészítéssel

Egyéb nem triviálisan proxy-zható protokoll pl. H. 323:

- Nincs támogatás

Eszközkonfigurálás: Hostok

6DEPLOY. IPv6 telepítés és támogatás

IPv6 Support – Hosts Operating Systems

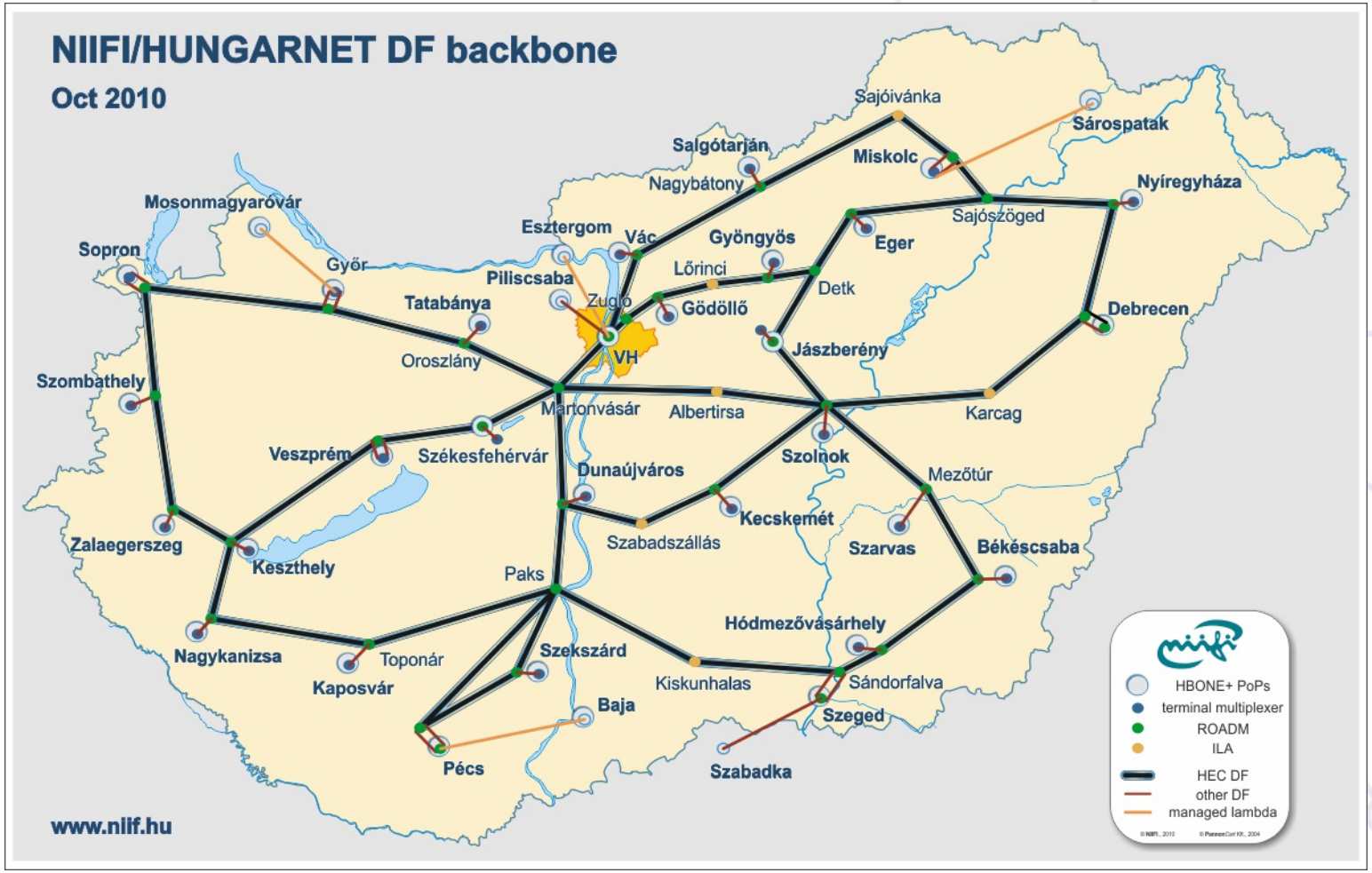
Vendor	First versions supporting IPv6	More Information
Apple	MAC OS X 10.2, iOS4	http://developer.apple.com/macosx/
BSD	FreeBSD 4.0 OpenBSD 2.7, NetBSD 1.5 BSD/OS 4.2	http://www.kame.net/
HP / Compaq	HP-UX 11i, Tru64 UNIX V5.1, OpenVMS V5.1	http://docs.hp.com/en/5990-7247/index.html
IBM	z/OS Rel. 1.4, AIX 4.3, OS/390 V2R6 eNCS	http://www-01.ibm.com/software/info/ipv6/compliance.jsp
Linux	Red Hat 6.2, Mandrake 8.0, SuSE 7.1, Debian 2.2, Android OS 2.2	http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-distributions.html
Microsoft	Windows Vista, XP, Server 2003, Server 2008, CE .NET, Mobile	http://www.microsoft.com/ipv6/
Novell	Netware 6.1	http://www.novell.com/documentation/oes2/ntwk_ipv6_nw/index.html?page=/documentation/oes2/ntwk_ipv6_nw/data/ai4x21f.html
Sun/ Oracle	Solaris 8, 9 and 10	http://docs.sun.com/app/docs/doc/817-0573?l=en
Nokia	Symbian 7.0	

General purpose and embedded OSs supporting IPv6 http://www.ipv6tf.org/index.php?page=guide/organizations/vendors/oss

Az IPv6 Magyarországon

6DEPLOY. IPv6 telepítés és támogatás

NIIF Hungarnet IPv6 topológia - 2011

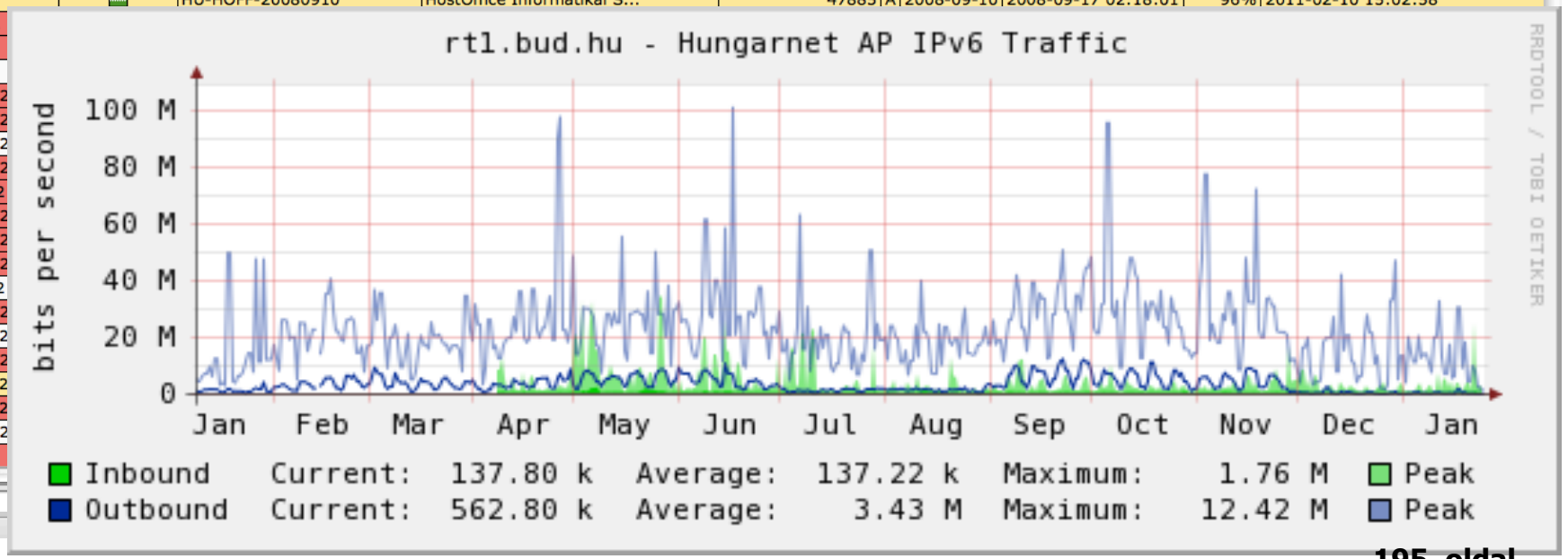


IPv6 elterjedtség - forgalom

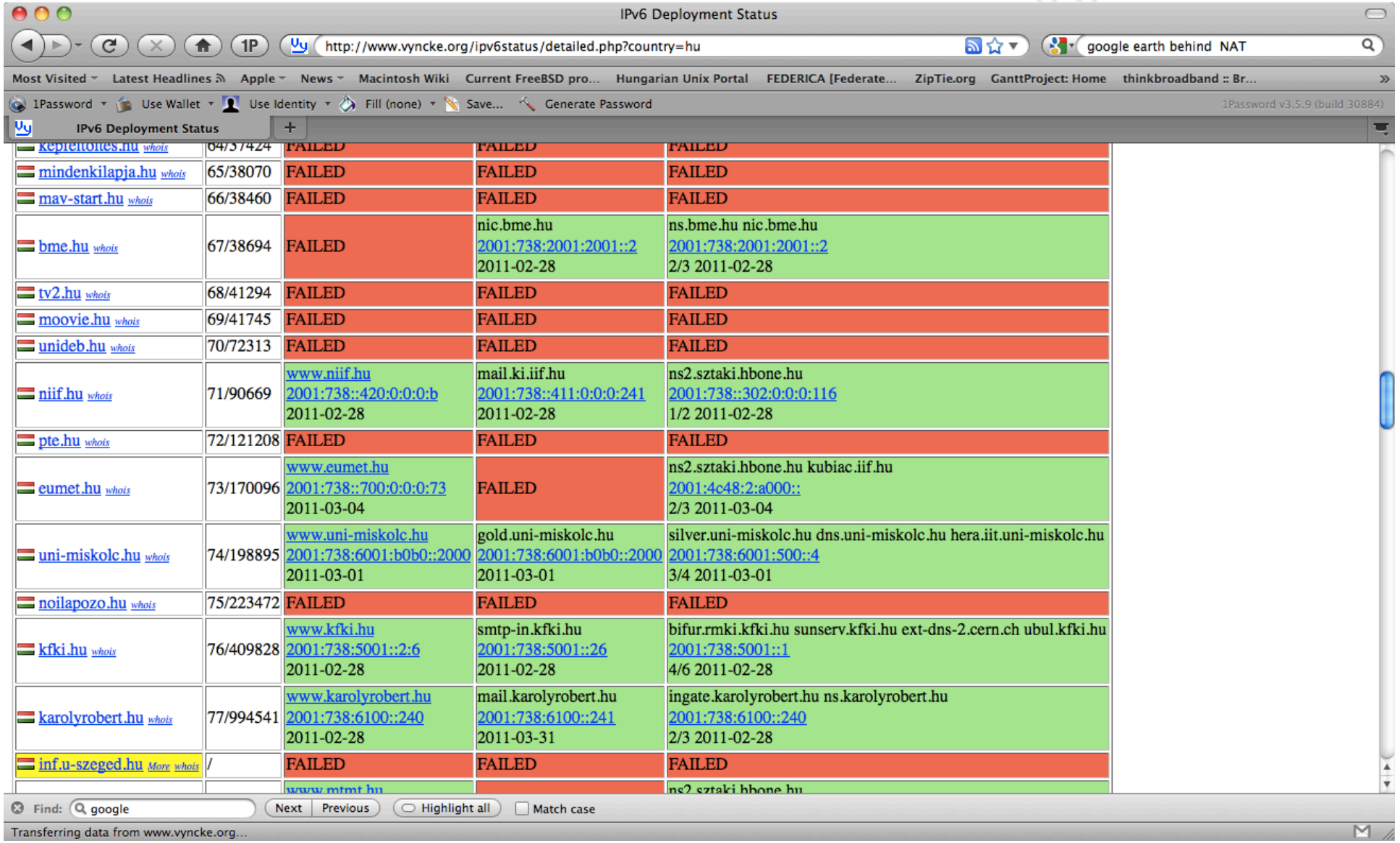
SixXS – IPv6 Deployment & Tunnel Broker :: Ghost Route Hunter : IPv6 DFP visibility : All

http://www.sixxs.net/tools/grh/dfp/all/?sort=country

LG	3ffe:2f00::/24		BME-FSZ/HU		2547	C	1998-09-08		0%	2006-06-21 09:02:20
LG	2001:738::/32		HU-HUNGARNET-2001071...	HungarNet	1955	A	2001-07-17		100%	2011-02-10 15:02:57
LG	3ffe:401c::/32		T-NET	T-NET IPv6 Project	29657	C	2001-11-24	2003-11-25 12:11:22	0%	2006-06-06 16:17:21
LG	2001:1aa0::/32		HU-PANTEL-20040317	PanTel Telecommunications...	12301	A	2004-03-17	2008-01-17 16:17:27	100%	2011-02-10 15:02:57
LG	2001:4c48::/32		HU-HTC-20050420	Hungarian Telecom MATAV	5483	A	2005-04-20	2009-02-11 21:02:27	100%	2011-02-10 15:02:57
LG	2001:7f8:35::/48		BIX-20050905	Council of Hungarian Inte...		A	2005-09-05	2008-04-23 18:17:28	0%	2011-02-10 15:02:57
LG	2a01:1f0::/32		HU-COVYSOFT-20060927	CovySoft Networks Co.		A	2006-09-27		0%	never
LG	2a01:270::/32		HU-ATW-20061219	ATW Internet Kft.	41075	A	2006-12-19	2006-12-21 11:32:22	100%	2011-02-10 15:02:58
LG	2a01:368::/32		HU-HDSNET-20070518	Egyesult Magyar Kabeltele...	20845	A	2007-05-18	2009-07-17 13:17:32	100%	2011-02-10 15:02:58
LG	2a01:5d0::/32		HU-TARR-20071108	Tarr Kft.	8462	A	2007-11-08	2009-09-24 03:47:31	100%	2011-02-10 15:02:58
LG	2a02:558::/32		HU-EXTERNET-20080626	Externet Kft.	12594	A	2008-06-26	2009-05-18 14:17:30	100%	2011-02-10 15:02:58
LG	2a02:738::/32		HU-INTERWARE-2008090...	InterWare Ltd.		A	2008-09-01	2008-11-06 14:02:37	0%	2010-08-17 02:47:43
LG	2a02:730::/32		HU-DENINET-20080901	Deninet KFT	29278	A	2008-09-01	2009-05-27 06:17:31	100%	2011-02-10 15:02:58
LG	2a02:780::/32		HU-HOFF-20080910	HostOffice Informatikai S...	47885	A	2008-09-10	2008-09-17 02:18:01	96%	2011-02-10 15:02:58
LG	2001:950::/32									
LG	2a02:808::/32									
LG	2a02:a50::/32									
LG	2a00:10b8::/32									
LG	2a00:10d0::/32									
LG	2a00:1110::/32									
LG	2a00:1530::/32									
LG	2a00:15f0::/32									
LG	2a00:1770::/32									
LG	2a00:1878::/32									
LG	2a00:1b90::/32									
LG	2a00:1f40::/32									
LG	2a02:2950::/32									
LG	2a02:2a98::/32									
LG	2a01:9200::/32									
LG	2a01:be00::/32									
LG	2a03:da00::/32									
LG	2001:1a98::/32									
LG	2a01:528::/32									



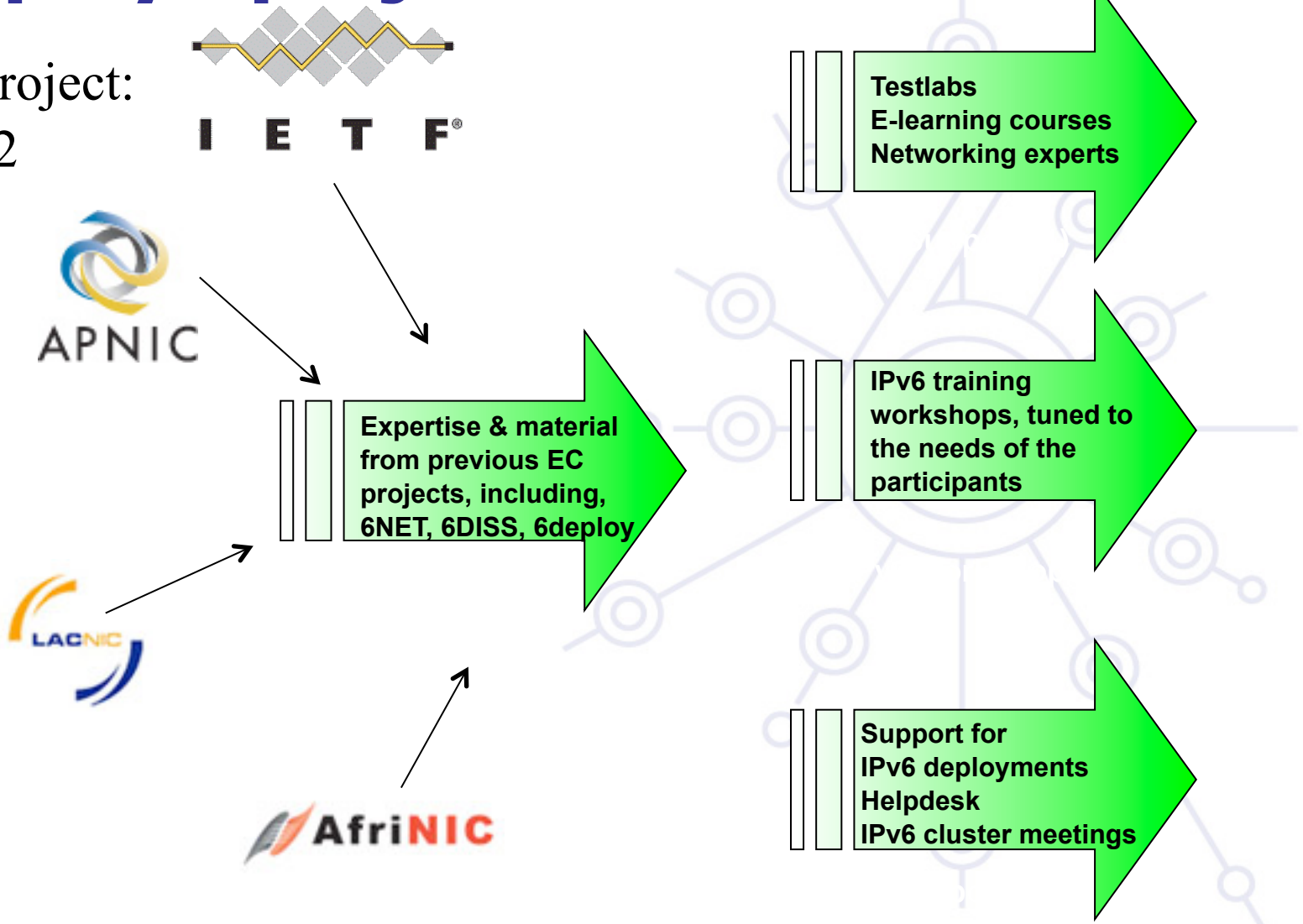
IPv6 elterjedtség /2



mindenkilapja.hu whois	65/38070	FAILED	FAILED	FAILED
mav-start.hu whois	66/38460	FAILED	FAILED	FAILED
bme.hu whois	67/38694	FAILED	nic.bme.hu 2001:738:2001:2001::2 2011-02-28	ns.bme.hu nic.bme.hu 2001:738:2001:2001::2 2/3 2011-02-28
tv2.hu whois	68/41294	FAILED	FAILED	FAILED
moovie.hu whois	69/41745	FAILED	FAILED	FAILED
unideb.hu whois	70/72313	FAILED	FAILED	FAILED
niif.hu whois	71/90669	www.niif.hu 2001:738::420:0:0:0:b 2011-02-28	mail.ki.iif.hu 2001:738::411:0:0:0:241 2011-02-28	ns2.sztaki.hbone.hu 2001:738::302:0:0:0:116 1/2 2011-02-28
pte.hu whois	72/121208	FAILED	FAILED	FAILED
eumet.hu whois	73/170096	www.eumet.hu 2001:738::700:0:0:0:73 2011-03-04	FAILED	ns2.sztaki.hbone.hu kubiac.iif.hu 2001:4c48:2:a000:: 2/3 2011-03-04
uni-miskolc.hu whois	74/198895	www.uni-miskolc.hu 2001:738:6001:b0b0::2000 2011-03-01	gold.uni-miskolc.hu 2001:738:6001:b0b0::2000 2011-03-01	silver.uni-miskolc.hu dns.uni-miskolc.hu hera.iit.uni-miskolc.hu 2001:738:6001:500::4 3/4 2011-03-01
noilapozo.hu whois	75/223472	FAILED	FAILED	FAILED
kfki.hu whois	76/409828	www.kfki.hu 2001:738:5001::2:6 2011-02-28	smtp-in.kfki.hu 2001:738:5001::26 2011-02-28	bifur.rmki.kfki.hu sunserv.kfki.hu ext-dns-2.cern.ch ubul.kfki.hu 2001:738:5001::1 4/6 2011-02-28
karolyrobert.hu whois	77/994541	www.karolyrobert.hu 2001:738:6100::240 2011-02-28	mail.karolyrobert.hu 2001:738:6100::241 2011-03-31	ingate.karolyrobert.hu ns.karolyrobert.hu 2001:738:6100::240 2/3 2011-02-28
inf.u-szeged.hu More whois	/	FAILED	FAILED	FAILED

6deploy2 projekt

EU FP7 project:
2010-2012



Mi a teendő az Internet továbbfejlődésért?

- Annak elfogadása, hogy a legkisebb kockázata az IPv6-nak van
- Együttműködés az IPv6 bevezetésében
- Másfajta ösztönzők
- Tagállamok példamutatása
- IPv6 támogatás megkövetelése beszerzéskor

European IPv6 day - 2008. május. 30

Ki korán kel, aranyat lel" – jelentette ki Vivane Reding, az Európai Unió információs társadalomért és a médiaügyekért felelős biztosa. „A vállalatok és közintézmények ugyan rövidtávon abba a kísértésbe eshetnek, hogy beérjék a régi rendszerrel, és igényeiket annak szűk lehetőségeihez alakítsák. Ez azonban azzal járna, hogy Európa nem tudna élni a legújabb internetes technológiák kínálta lehetőségekkel, és komoly problémával szembesülne, amikor a régi rendszer címtartománya kimerülne. … Ezért arra kérem a tagállamokat, gondoskodjanak arról, hogy 2010-ig az IPv6 protokollt a közintézmények és a vállalatok széles körben alkalmazzák".

World IPv6 day - ISOC

2011 június 8. – 24 órás teszt

http://isoc.org/wp/worldipv6day/

- IPv6 szolgáltatások nyújtása – koordinált!
- Tapasztalatok gyűjtése
- "…some of the major organisations that will offer their content over IPv6 for a 24-hour "test flight"….
- Sok résztvevő:
  - Google, Facebook, Yahoo!, Akamai Limelight Networks
  - Cisco, Meebo, Genius, W3C, Universidad Nacional Autonoma de Mexico, Rensselaer Polytechnic Institute, NYI NET, Host Europe, Xiphiastec, Tom's Hardware, NUST School of Electrical Engineering and Computer Science, Twenga, Plurk, Terra (Brazil), Jolokia Networks, Juniper Networks, Microsoft Bing, Gigatux, Voxel, LemonEntry, 2g2u, 2020Media, Vonage, sapo.pt, Tagadab.com, Mercury Z, Outpost10f, Public Interest Registry, Sesame Workshop, Arces

NIIF felkészülés

2006 év eleje óta támogatott az IPv6

Szolgáltatások IPv6 képesek régóta

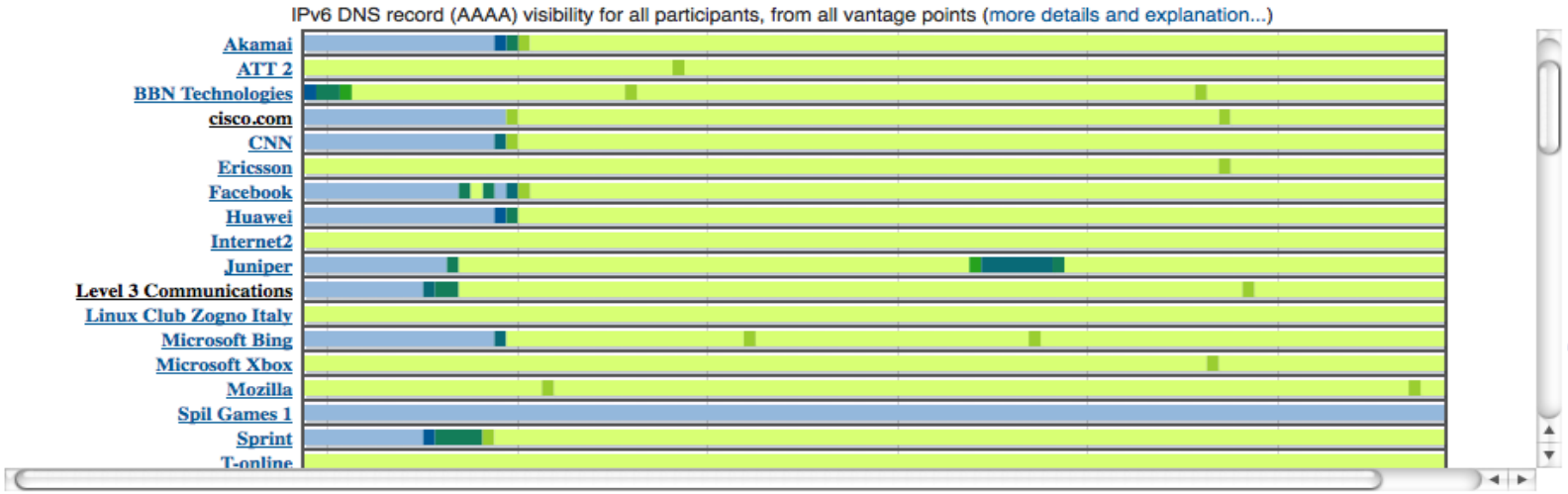
Operátorok felkészítése

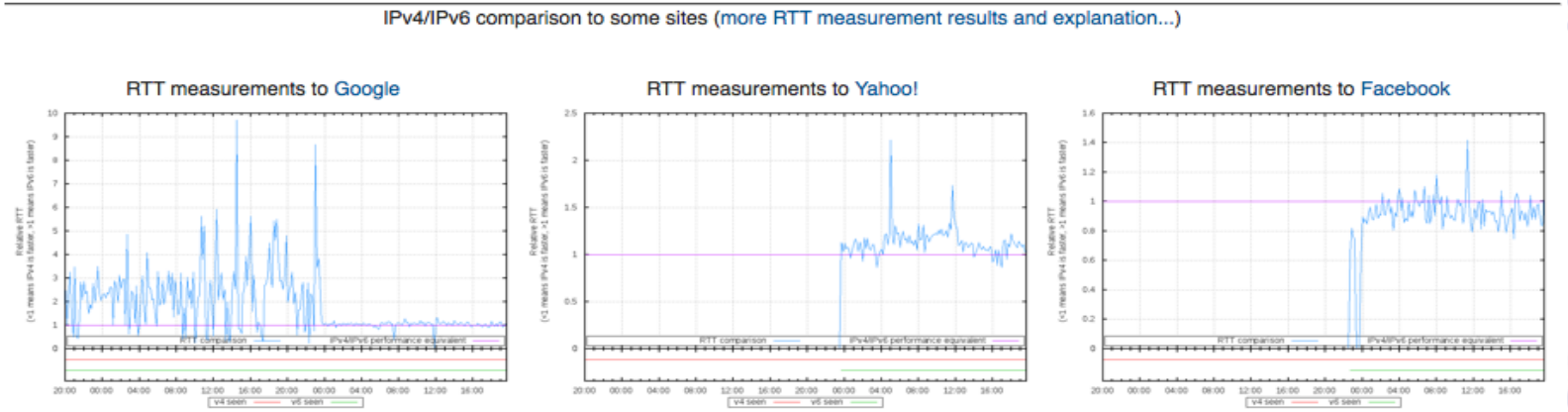
Felhasználók értesítése

IPv6 readiness check

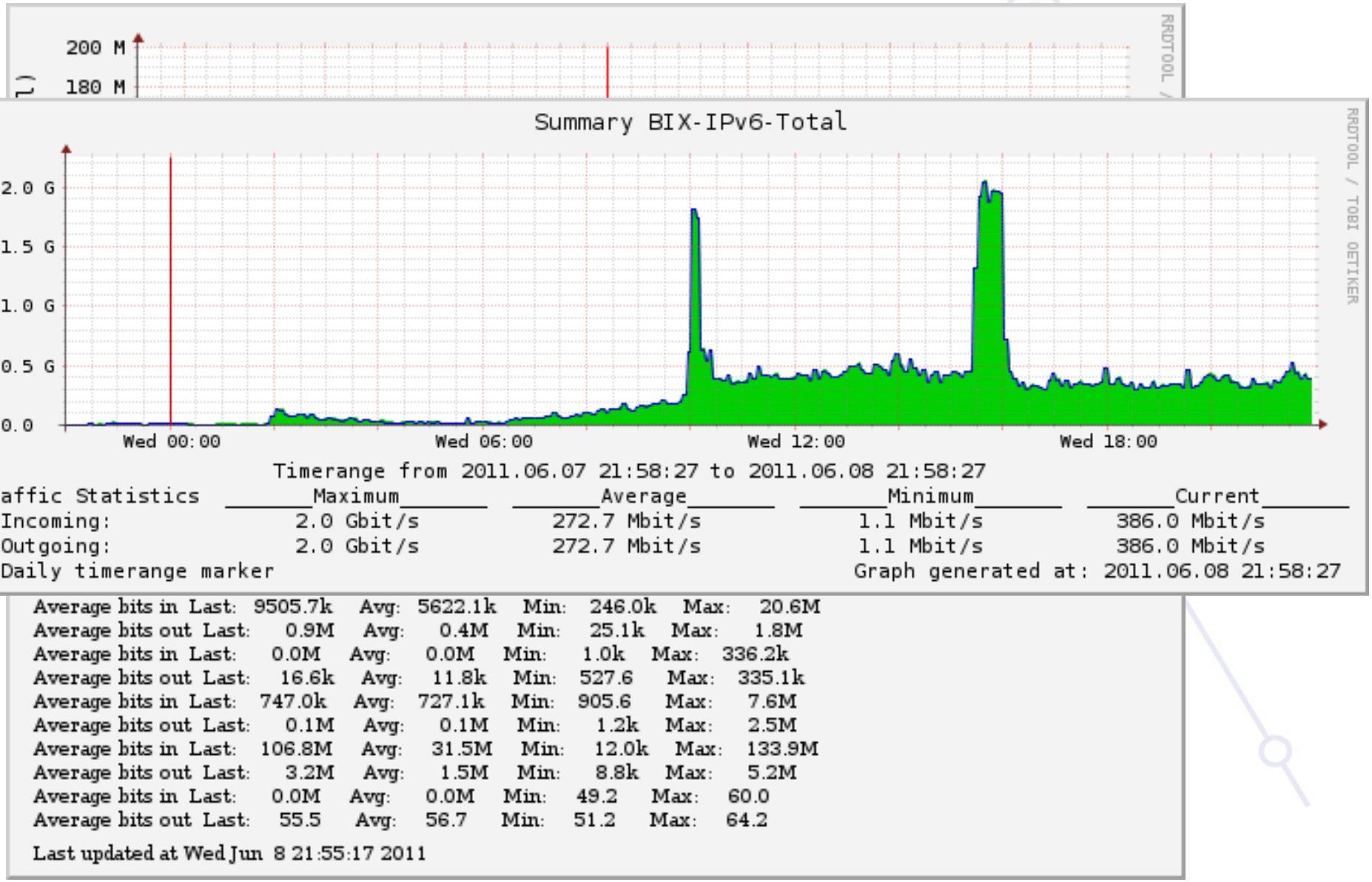
- http://go6.se/check
- http://test-ipv6.com/ és http://test-ipv6.sth.sze.hu/
- http://netalyzr.icsi.berkeley.edu/m=testv6

RIPE IPv6 dashboard





IPv6 forgalom - este



Problémák

freemail (T-com routing?) IPv6 elérési probléma
10:00 körül – 30 perc után megjavult

Mac OS X – AAAA nem cachelés

Érdekes routing – Level3:

```
traceroute to ipv6.test.Level3.com (2001:1900:2018:3000::105) from 2001:738:0:1:206:5bff:fef3:4366, port 33434, from port 42608, 30 hops max, 60 byte packet
s
 1  c6513-2-vlan150.vh.hbone.hu (2001:738:0:1::1)  0.456 ms  0.245 ms  0.398 ms
 2  be2.rtr1.vh.hbone.hu (::ffff:195.111.96.60)  0.694 ms  0.572 ms  0.567 ms
 3  2001:2000:3080:17::1 (2001:2000:3080:17::1)  0.228 ms  0.225 ms  0.230 ms
 4  ldn-b5-v6.telia.net (2001:2000:3018:b::1)  38.152 ms  36.232 ms  38.066 ms
 5  * * *
 6  vl-4086.car1.NewYork1.Level3.net (2001:1900:6:1::12)  106.838 ms  106.080 ms  106.225 ms
 7  vl-4083.car2.SanJose1.Level3.net (2001:1900:4:1::ee)  104.267 ms  165.523 ms  691.354 ms
 8  vl-4060.car2.NewYork2.Level3.net (2001:1900:4:1::fe)  115.120 ms  115.138 ms  115.773 ms
 9  vl-4061.car1.Chicago1.Level3.net (2001:1900:4:1::21)  136.240 ms  136.943 ms  136.156 ms
10  * * *
11  vl-4041.car2.Denver1.Level3.net (2001:1900:4:1::35)  212.448 ms  166.424 ms  166.655 ms
12  vl-4081.car1.Denver1.Level3.net (2001:1900:4:1::31)  173.636 ms  317.868 ms  162.589 ms
13  Level3-MOSS.vl-956.car1.Denver1.Level3.net (2001:1900:4:2::fa)  159.885 ms  160.297 ms  160.744 ms
```

Citrix Netscaler fragmentation crash bug

IPv6 világnap - konkluzió

IPv6 világnap – jól előkészített

A potencális hibák nagy része előre ismert volt

Részletes analízis szükséges a tartalom szolgáltatók részéről az ő tapasztalataikról

- mi működött, mi nem
- CDN?

Újabb IPv6 world day-re lenne szükség – a hibákból tanulva – várható 2012 Februárjában?

1 éven belül bevezethető lenne a IPv6 világnapon tesztelő tartalom tulajdonosoknál az IPv6…

Facebook a fejlesztői weboldalát dual-stack-re konfigurálva hagyta….. – mert jók voltak a tapasztalatok

World IPv6 launch - ISOC

2012 június 6. – IPv6 bekapcsolása:

http://www.worldipv6launch.org/

IPv6 szolgáltatások elindítása

Fókusz:

- Internet Szolgáltatók – ISP
- Tartalom szolgáltatók – CP
- CPE gyártók

Nem késő még csatlakozni

További információk

http://tools.ietf.org/wg/6man/charters

http://tools.ietf.org/wg/v6ops/charters

http://ipv6.niif.hu

http://www.6deploy.eu

További információk

Könyvek

- IPv6, The New Internet Protocol
  by Christian Huitema (Prentice Hall)
- IPv6 Essentials by Silvia Hagen (Oreilly)
- Running IPv6 by Iljitsch van Beijnum (APress)
- http://www.6diss.org/publications/info/deployment-guide.pdf -
  by 6NET project


deploy
Kérdések?
6DEPLOY Projekt Web oldal:
http://www.6deploy.org
mohacsi@niif.hu