IPv6 dióhéjban

Mohácsi János
IPv6 forum elnökhelyettes,
NIIF Intézet

Első Magyar IPv6 Fórum konferencia

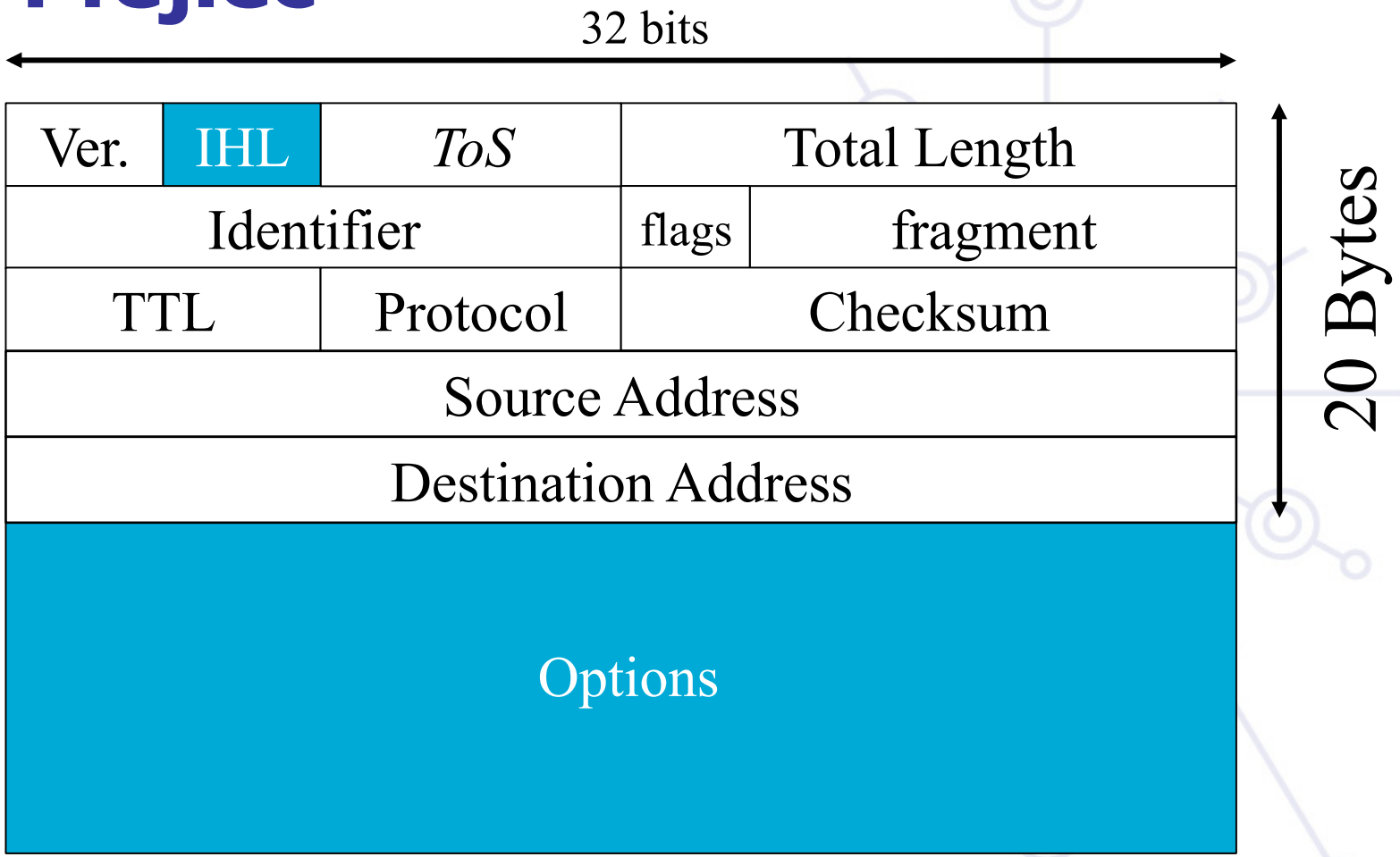
IPv6 protokoll (RFC 2460 DS)

IPv6 fejléc

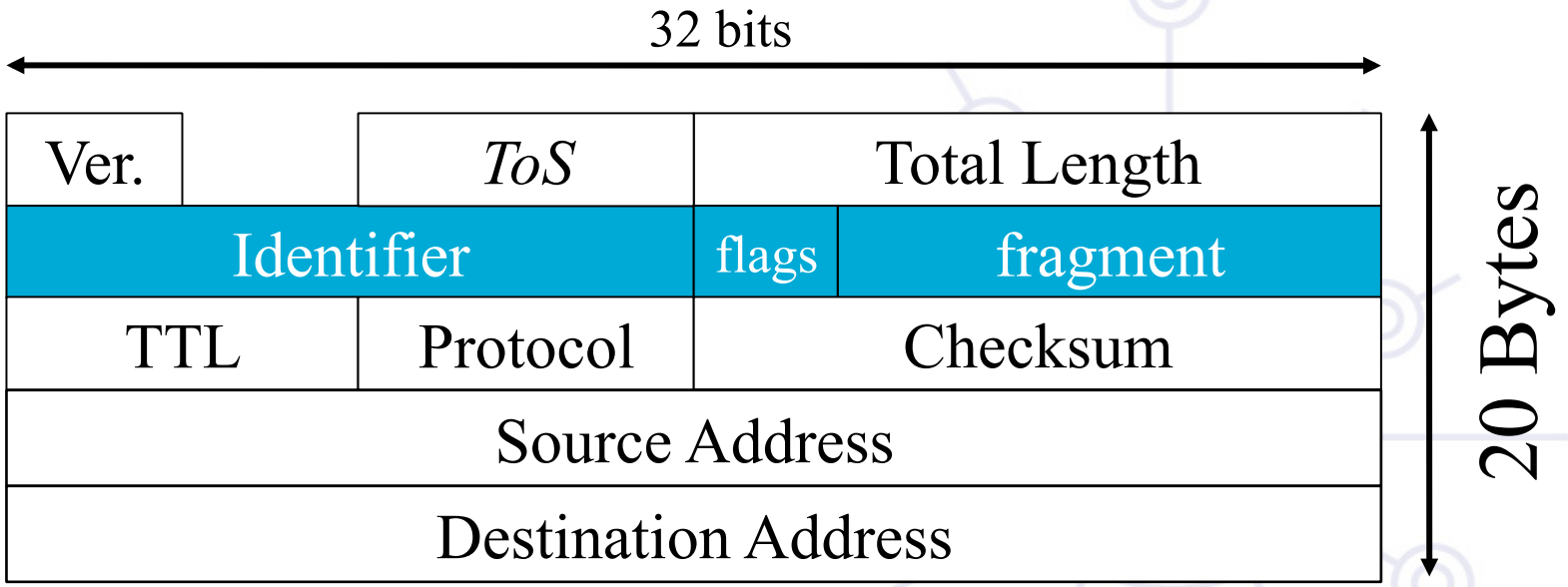
IPv6 címzés

IPv6-hoz kapcsolódó protokollok

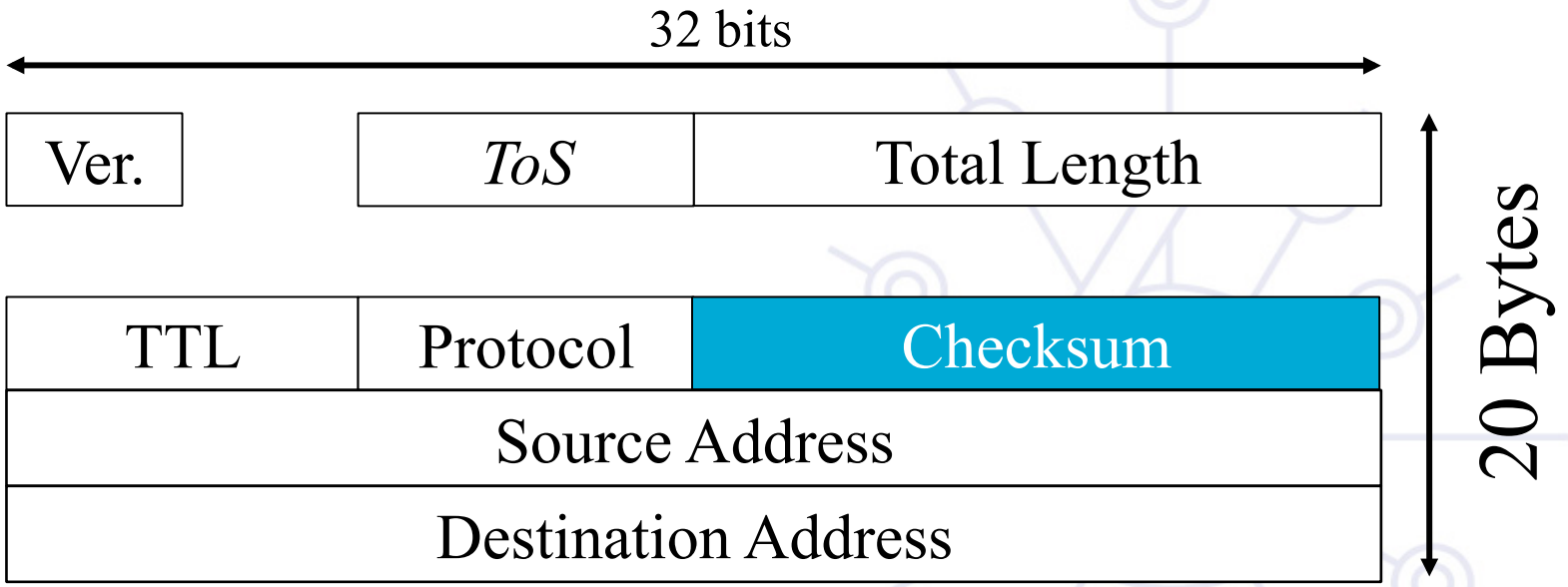
IPv4 fejléc


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

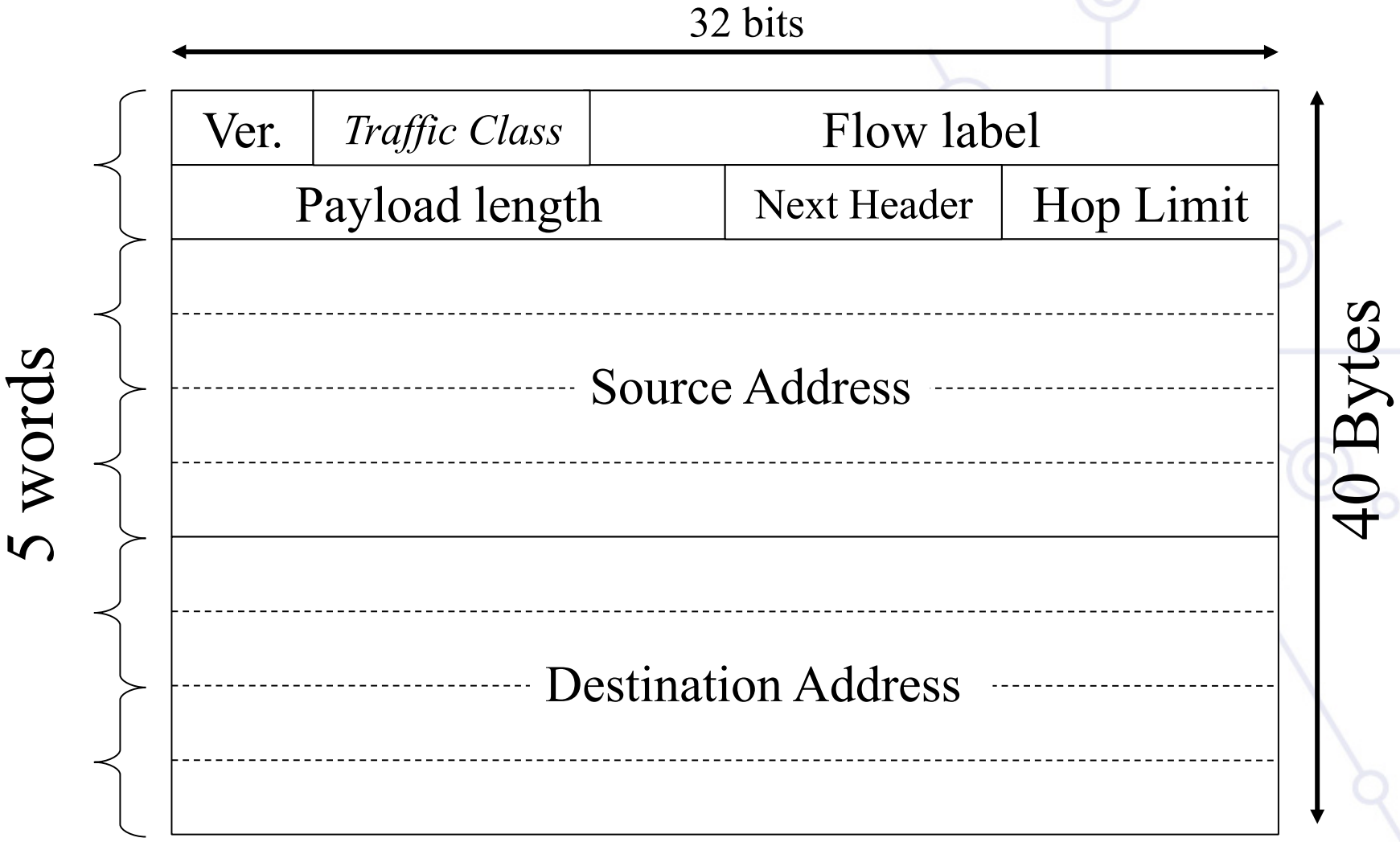
IPv4 fejléc


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

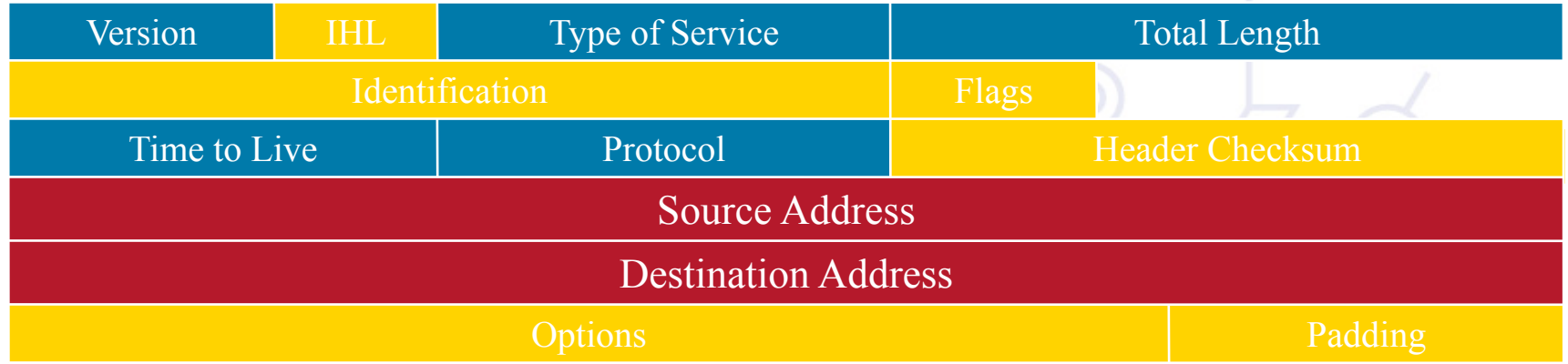
IPv4 fejléc

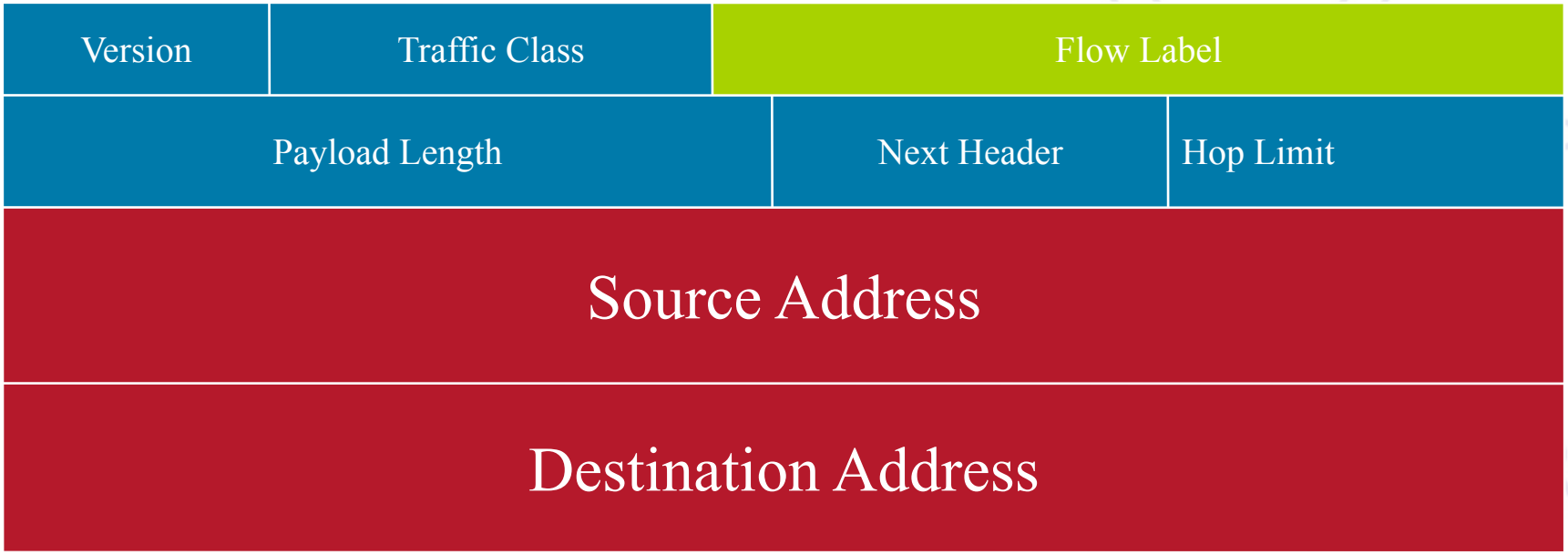

32 bits
Ver.
ToS
Total Length
TTL
Protocol
Checksum
Source Address
Destination Address
20 Bytes

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

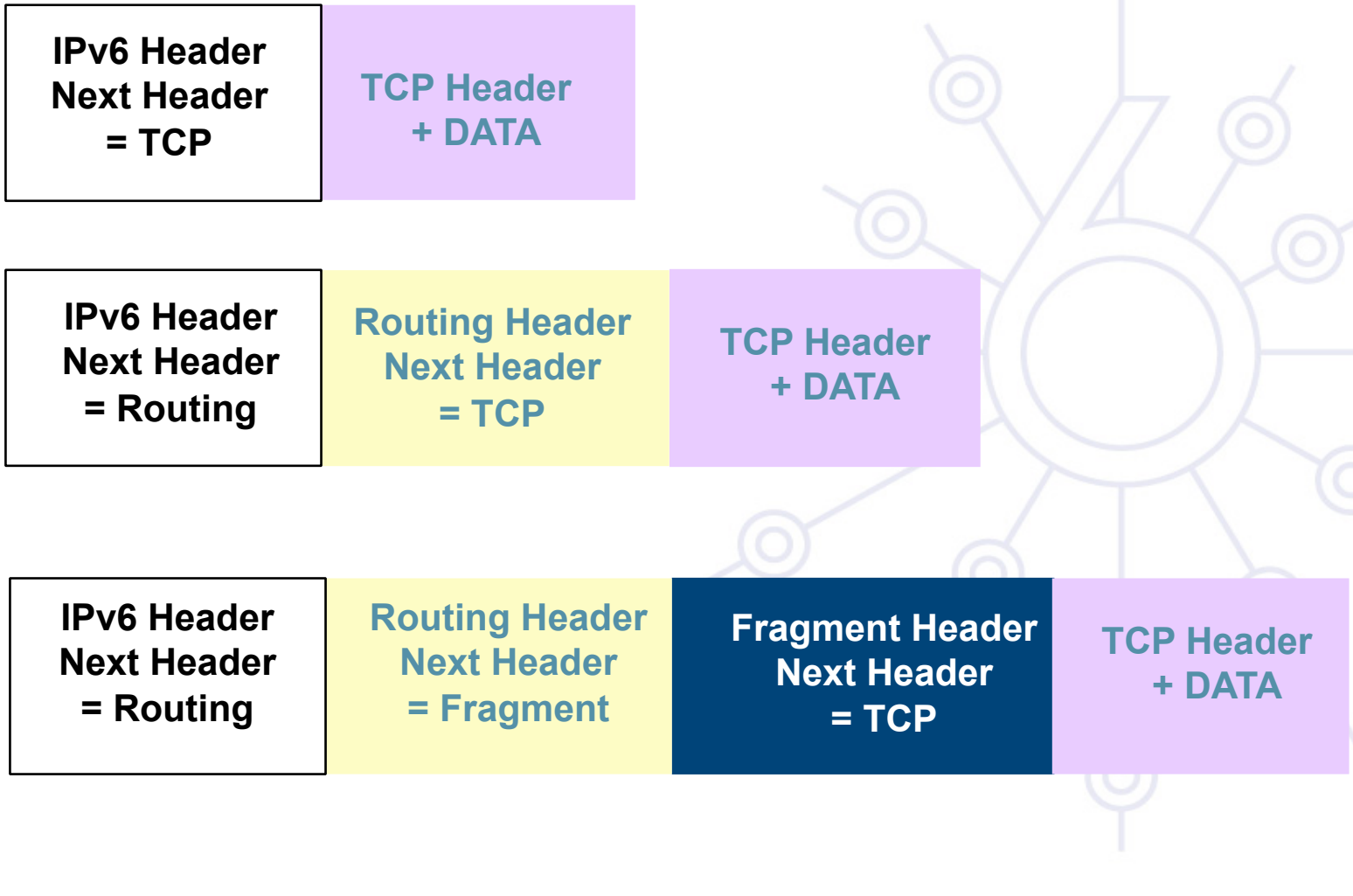
Hop Limit

- Nem jelenthet problémát

Payload hossz

- Egyes esetekben Jumbogram használata ajánlott

IPv6: Opcionális fejlécek



IPv6 Címzés

Első Magyar IPv6 Fórum konferencia

IPv6 Címzési séma

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

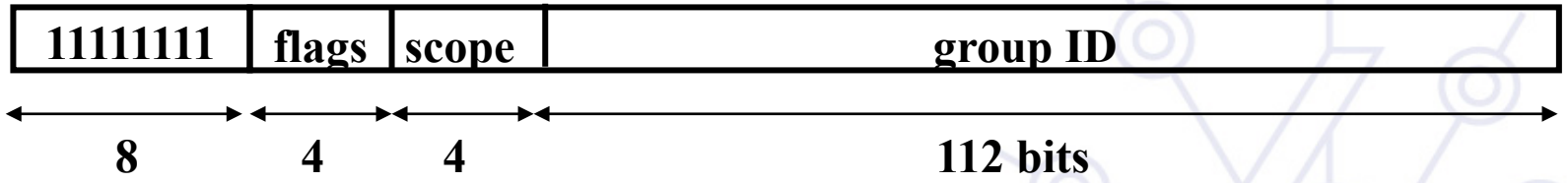
IPv6 cím típus prefixek

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

Multicast címek



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

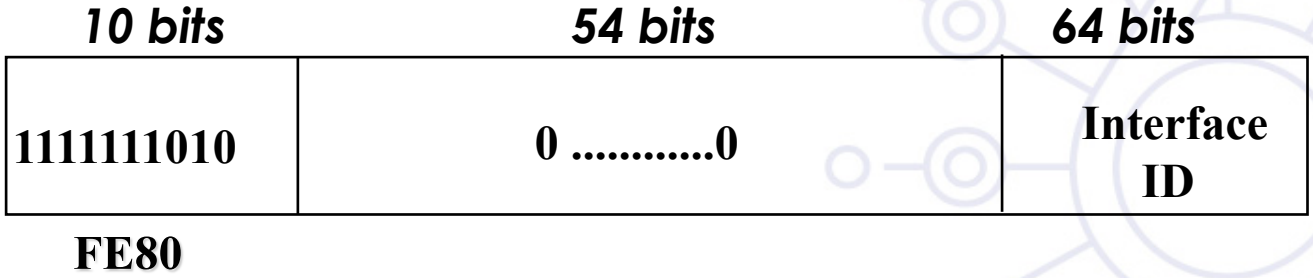
- **T**: Transient, vagy nem, dinamikusan osztott, vagy jólismert a cím
- **P**: Prefix alapján osztott vagy nem - hálózati prefix alapján
- **R**: Rendezvous Point cím belefoglalva, vagy nem

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)

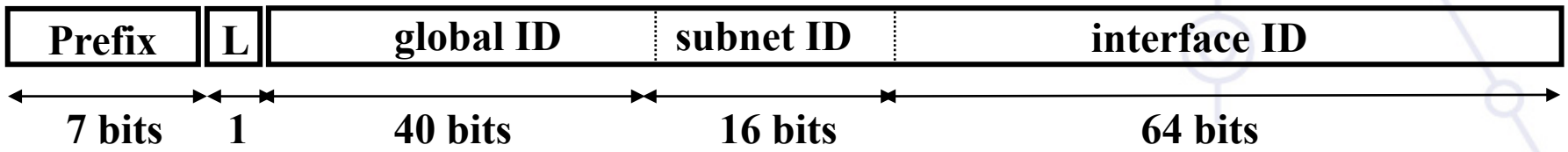
Link-Local & Unique-Local Unicast címek

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



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

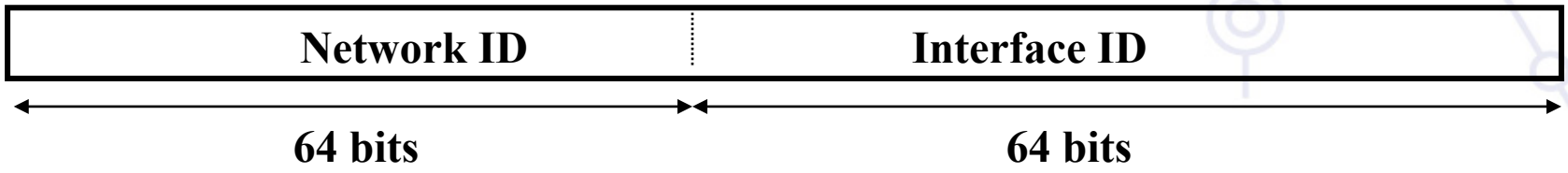
- L = 1 ha a cím helyileg kiosztott - ULA-k álvéletlen global ID-vel
- L = 0 még meghatározandó



Interface ID-k

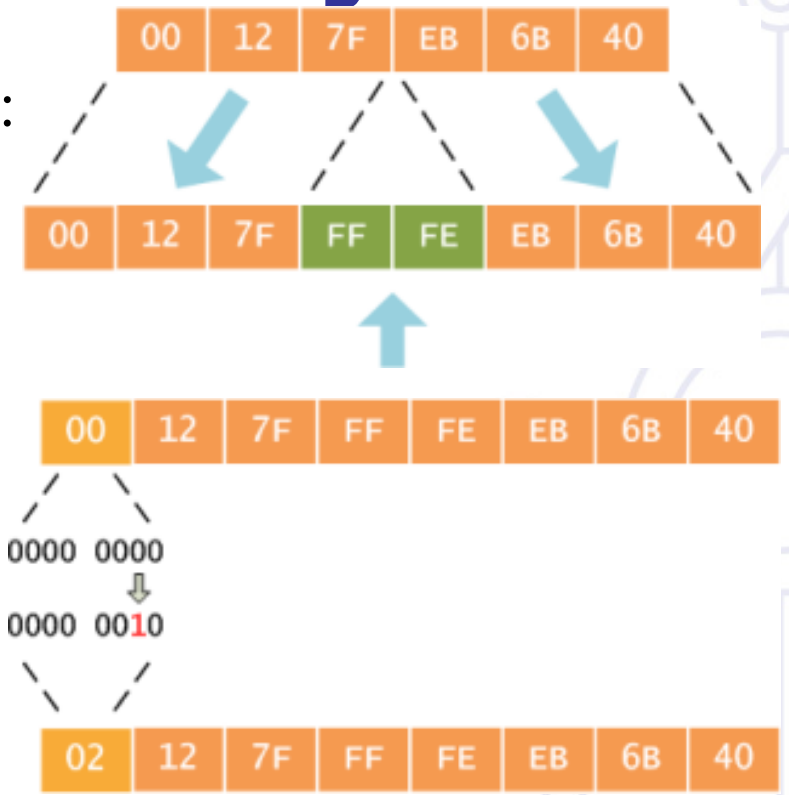
Az unicast címek legalacsonyabb helyiértékű 64-bitje a következő módszerekkel osztható:

- Automatikus konfigurációval a 64-bites MAC címből
- Automatikus konfigurációval a 48-bites MAC címből (pl. Ethernet) kiterjesztve a 64-bites EUI-64 formátumra
- DHCPv6-al
- Statikusan
- Álvéletlen szám automatikus generálásával (pl. adatvédelmi okokból)
- CGA (Cryptographically Generated Address)
- További eljárások várhatóak a jövőben



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.

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!

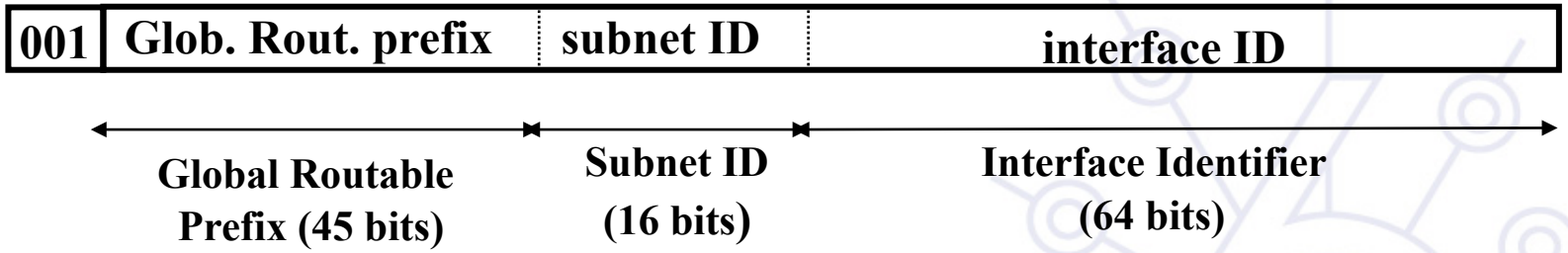
Privacy extensions (RFC 3041)

- 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

Globális IPv6 címzési séma (2)



LIR-ek alapértelmezetként /32 –t kapnak

- A production címek a 2001 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

IPv6 kapcsolódó protokolljai

Első Magyar IPv6 Fórum konferencia

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)

Címfeloldás - IPv6 Neighbor Discovery (1)

Minden IPv6 nodenak kötelező speciális multicast csoporthoz csatlakoznia minden hálózati interfészen

- 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)

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

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)

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

Stateless auto-configuration

IPv6 Stateless Address Auto-configuration

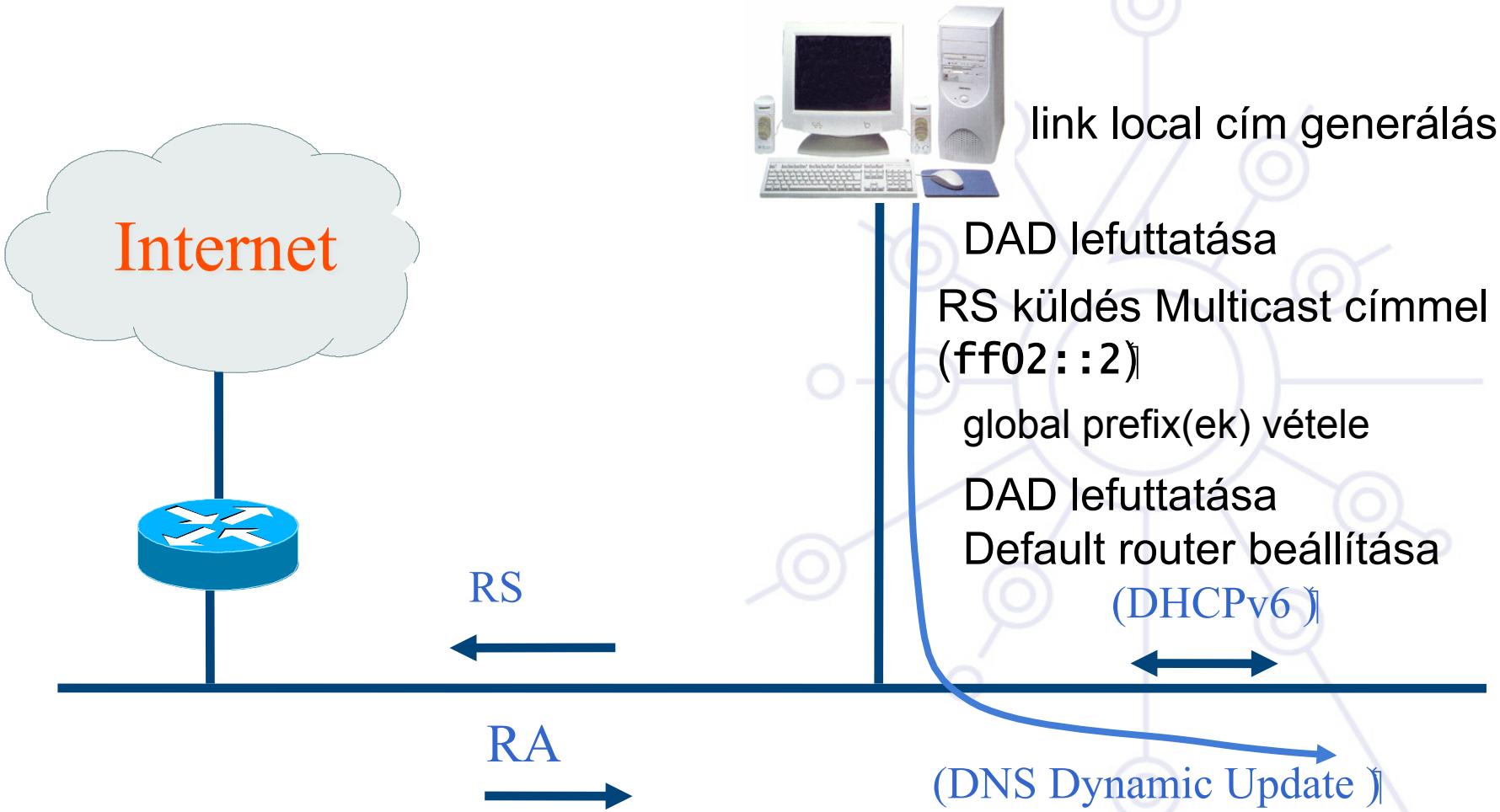
- RFC 2462 DS
- Nem vonatkozik a routerekre

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




deploy
IPv6 bevezetési stratégiák
vállalati és szolgáltató
környezetben

Áttekintés

Vállalati bevezetési stratégia

Vállalati IPv6 cím allokáció és menedzsment

Vállalati bevezetési topológia – lehetőségek

Vállalati szolgáltatások

Szolgáltatói bevezetési megfontolások

Áttekintés

Vállalati bevezetési stratégia

Vállalati IPv6 cím allokáció és menedzsment

Vállalati bevezetési topológia – lehetőségek

Vállalati szolgáltatások

Szolgáltatói bevezetési megfontolások

Különböző vállalati 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)

Vállalati bevezetési terv/1

1. **Menedzsment meggyőzése az IPv6 bevezetés szükségességéről**
2. **IPv6 címtartomány igénylése az ISP-től**
   - Az ISP-k általában egy /32 prefixet kapnak a RIPE NCC/RIR-ektől
   - Felhasználók egy /48 prefixet kapnak az LIR-ektől
3. **Külső IPv6 kapcsolat igénylésre**
   - Ha lehetséges akkor dual-stack kapcsolat
   - Sokan eleinte tunnelt fognak használni IPv6 szolgáltatás eléréshez
     - ebben az esetben biztosítani kell, hogy senki se tudja rosszindulatú célokra használni a tunnelt – pl. filtering használatával

Vállalati 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

Áttekintés

Vállalati bevezetési stratégia

Vállalati IPv6 cím allokáció és menedzsment

Vállalati bevezetési topológia – lehetőségek

Vállalati 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

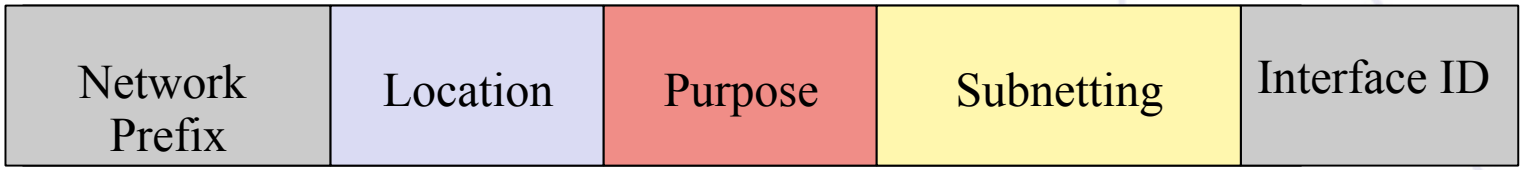
Vállalati subnetelés

A legtöbb site /48 –at fog kapni:

16 bit marad az alhálózatoknak–hogyan használjuk?

Módszerek:

- Szekvenciális
- Követve a meglévő IPv4 címzési stratégiát
- Hely-Felhasználási mód szerinti subnetelés



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

Vállalati bevezetési stratégia

Vállalati IPv6 cím allokáció és **menedzsment**

Vállalati bevezetési topológia – lehetőségek

Vállalati szolgáltatások

Szolgáltatói bevezetési megfontolások

vállalati 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

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 szerver információ 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. Layer 2 admission control – pl. 802.1X alkalmazása
3. 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/
4. DHCPv6 használata prefix és default gateway opcióval

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

A két fő megközelítés:

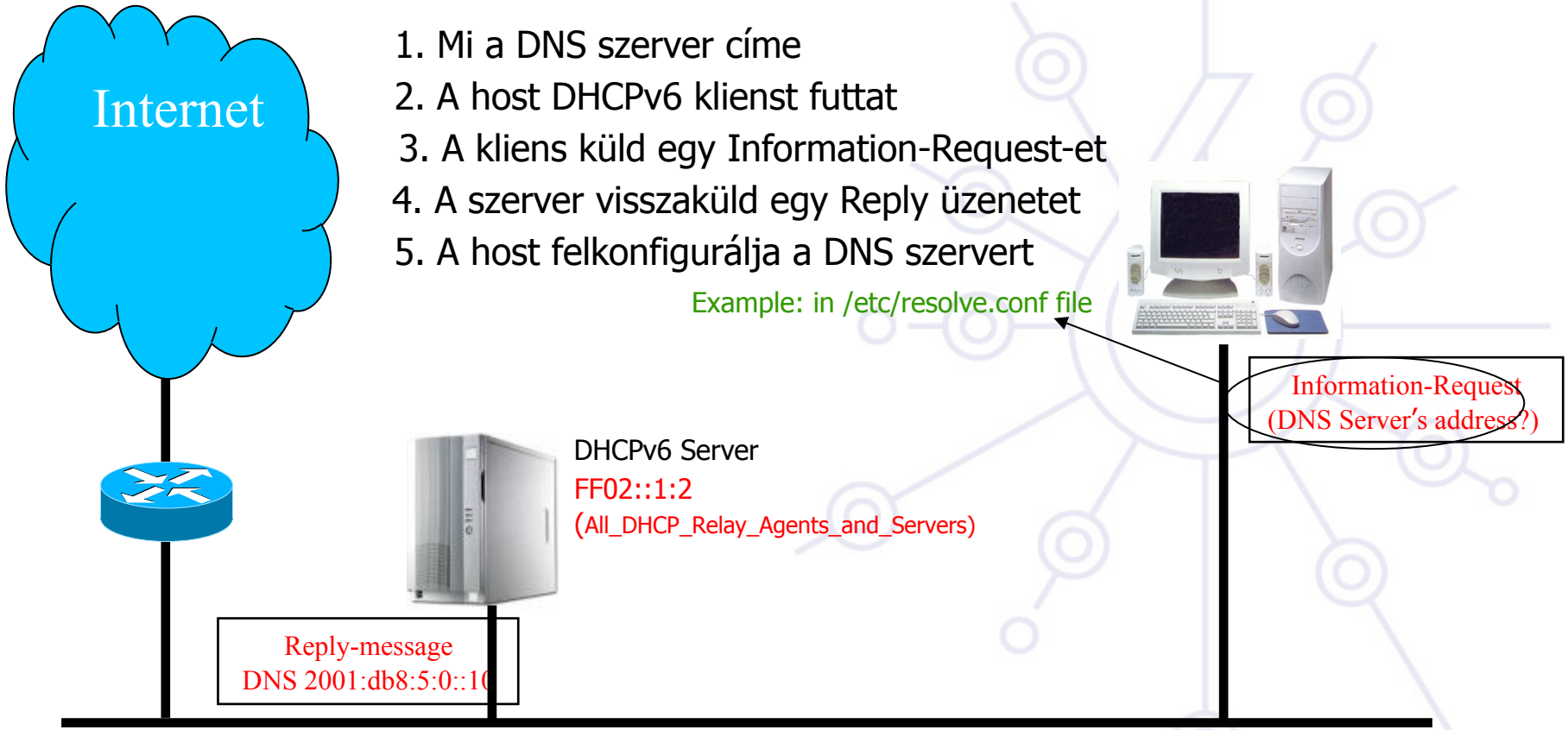
- Stateless address autoconfiguration stateless DHCPv6-tal a egyéb információkért.
- DHCPv6 használata a címekhez és egyéb információkhoz, hogy jobban ellenőrzött legyen a címek hozzárendelése.

DHCPv6 elemek [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 címen figyel:
    - All_DHCP_Relay_Agents_and_Servers (FF02::1:2).
  - Általában eltárolják a kliensek állapotát - Mint IPv4
- Kliens
  - Kéréseket kezdeményez a linken, hogy konfigurációs paramétereket kapjon
  - Link-local címet használ a szerverhez csatlakozáshoz
- Relay agent

Stateless Autoconfiguration DHCPv6



DHCPv6 további információk

Korábban: MAC , Client ID

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

- DUID is opaque in the communication

DUID típusok:

- DUID-LLT – Link-Layer cím + idő
- DUID-EN – gyártóhoz rendelt a gyártói azonosító alapján
- DUID-LL – Link-Layer cím

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

Áttekintés

Vállalati bevezetési stratégia

Vállalati IPv6 cím allokáció és menedzsment

Vállalati bevezetési topológia – lehetőségek

Vállalati 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 nem 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

Áttekintés

Vállalati bevezetési stratégia

Vállalati IPv6 cím allokáció és menedzsment

Vállalati bevezetési topológia – lehetőségek

Vállalati szolgáltatások (DNS, levelezés, web, VPN, security, felügyelet)

Szolgáltatói bevezetési megfontolások

Outline of ISP IPv6 deployment

1. Obtain IPv6 address space
2. Plan the addressing
3. Plan the routing
4. Test in a small case
5. Deploy IPv6 (incrementally – dual-stack/6PE)
6. Enable IPv6 services


deploy
IPv6 Biztonság

Milyen biztonsági 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

IPv6 címek biztonsága

Az alhálózat mérete sokkal nagyobb – scannelés?

- Sok év szükséges egy /64-es alhálózat teljes feltérképezéséhez
- `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

Kriptográfiailag generált címek (CGA) [RFC 3972]

- A cím Host-ID része egy kódolt hash
  - A nyilvános kulcs hitelesíti a CGA címekről küldött üzeneteket

A privát címek definiáltak [RFC 4941]

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

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

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. Layer 2 admission control – pl. 802.1X alkalmazása
3. 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/
4. DHCPv6 használata prefix és default gateway opcióval

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”
- Az IPv6 nem követel end-to-end kapcsolatot, de end-to-end címzést tesz lehetővé

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

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]

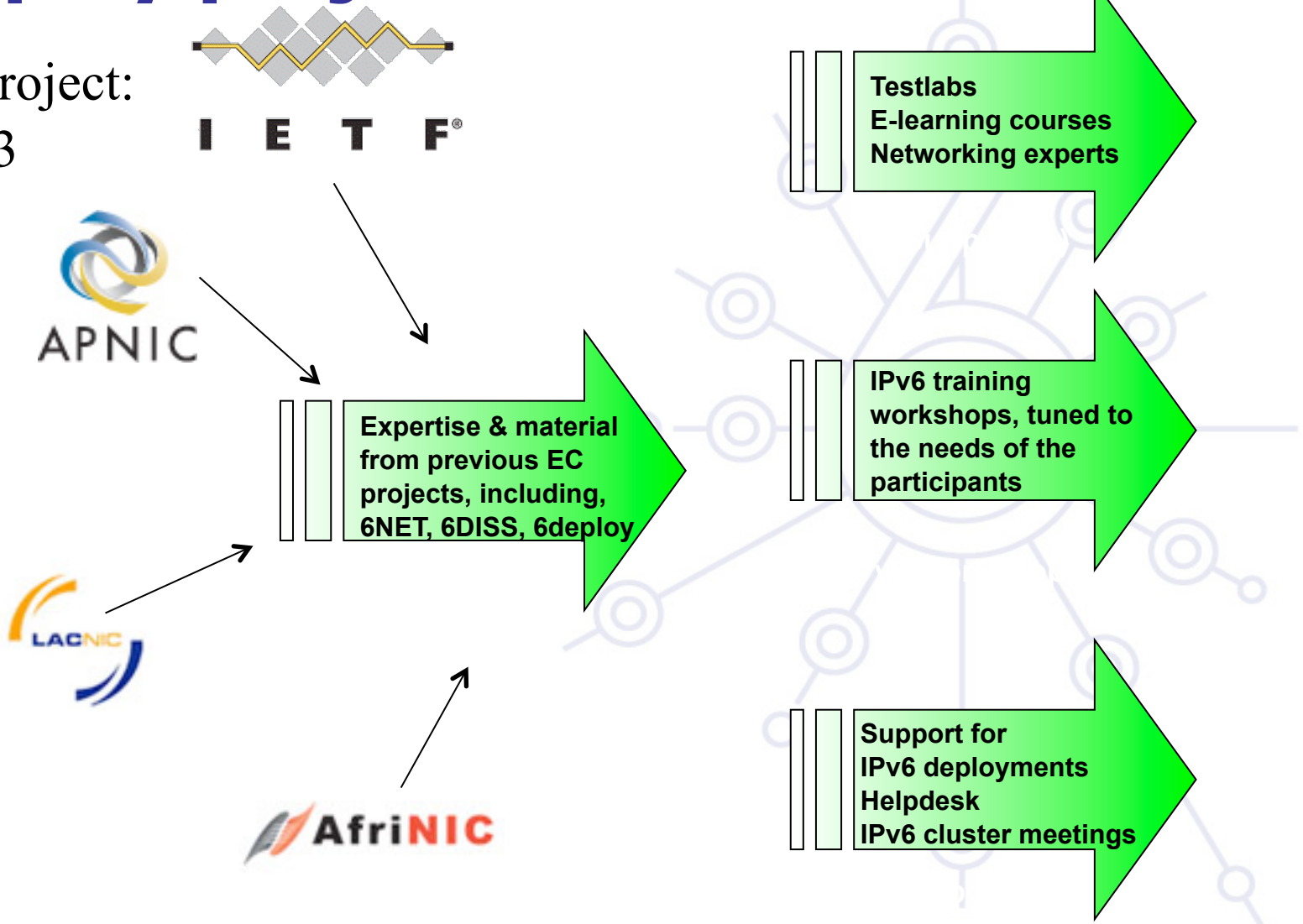
[szükséges]

További információk

Első Magyar IPv6 Fórum konferencia

6deploy projekt

EU FP7 project:
2010-2013



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

http://www.getipv6.info

https://ipv6forum.hu

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

Tutorialok:

- 6deploy workshop-ok http://www.6deploy.eu/


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