# IPv6 gyakorlatban

## HUNOG konferencia 2023.10.12

János Mohácsi, Nemzetközi K+F vezető , KIFÜ

# Napirend

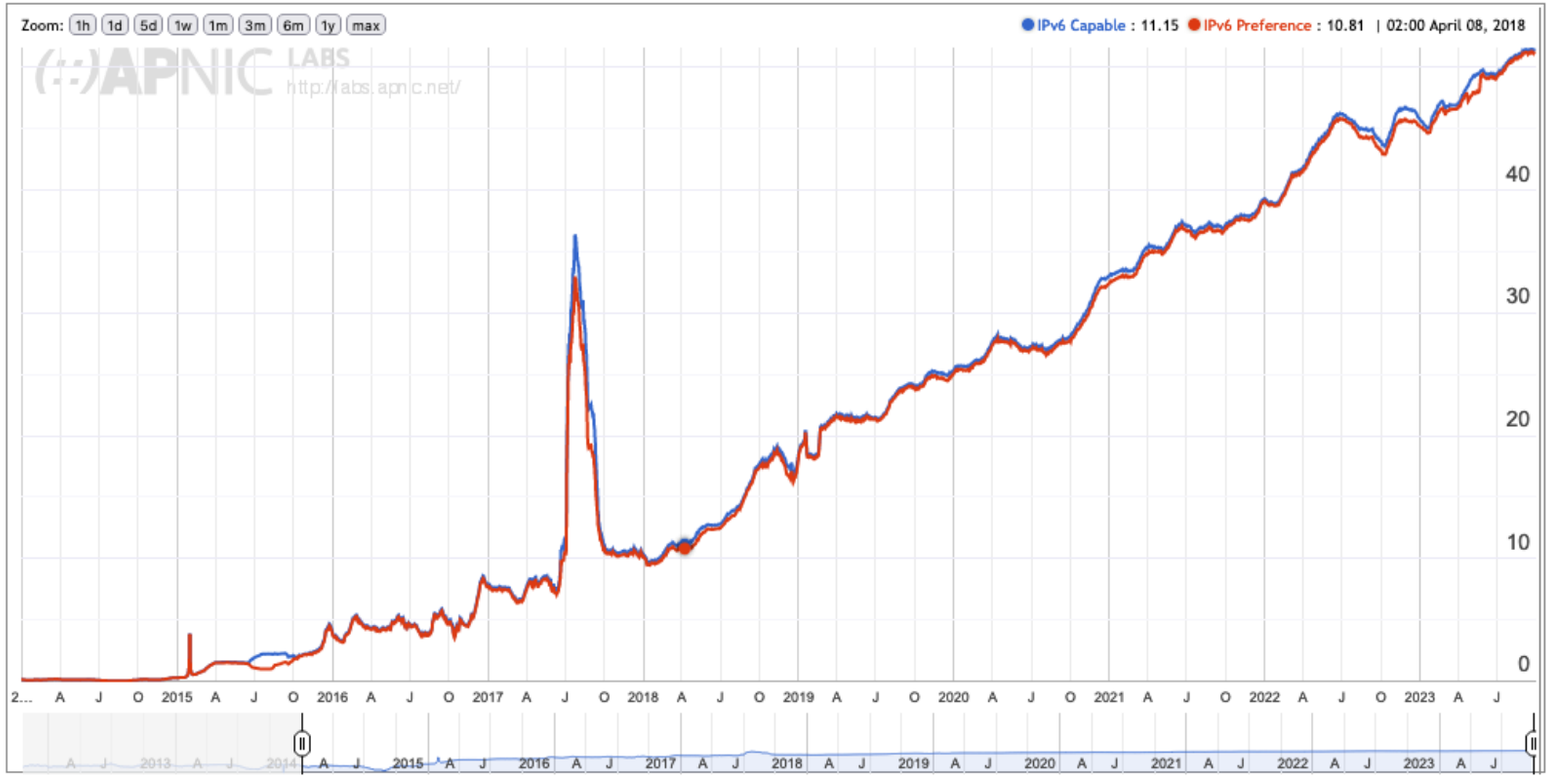
1. IPv6 trendek
2. IPv6 gyakorlati kérdései
3. Kérdések

Slido

Slido.com #2032 745

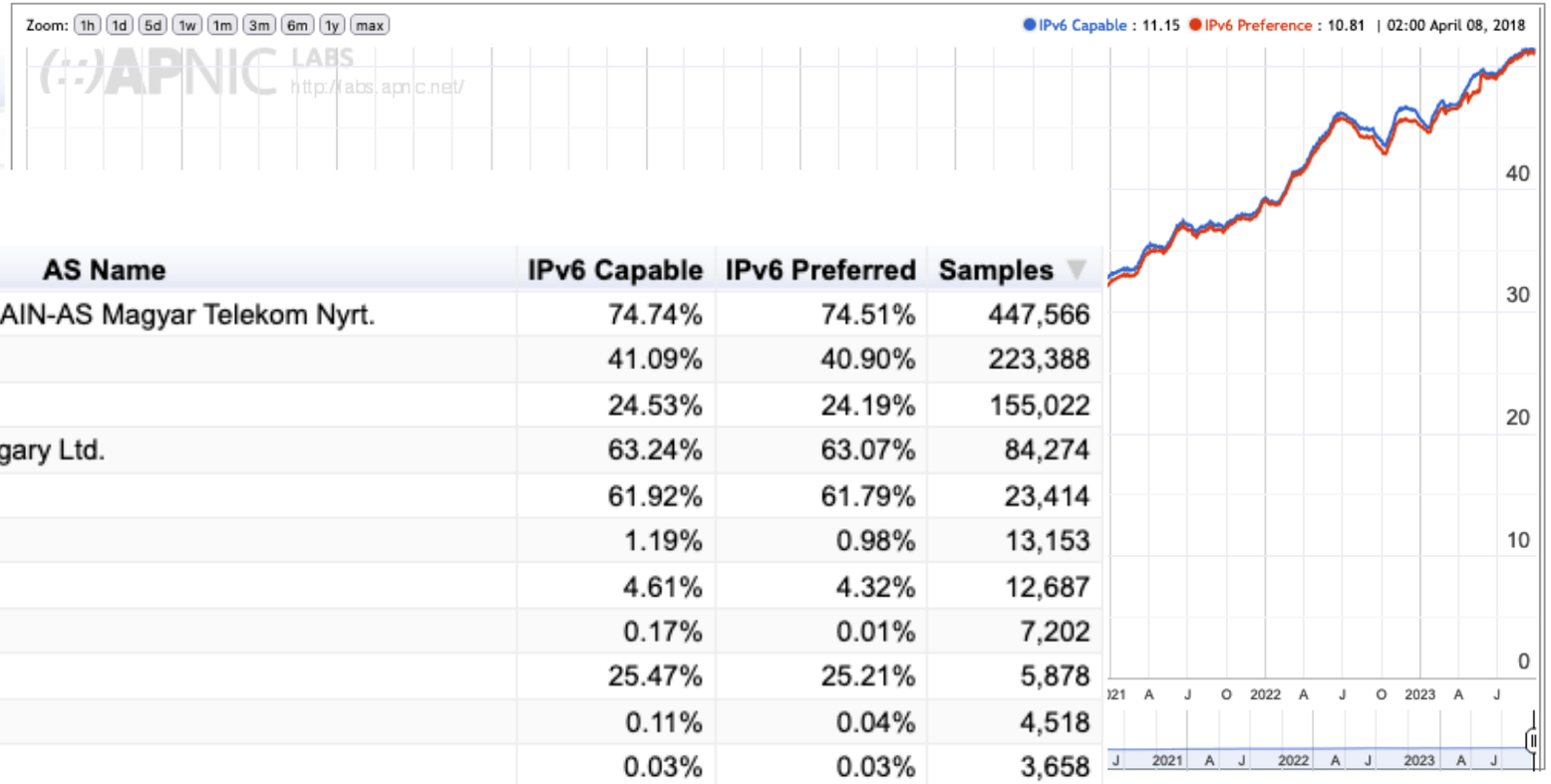
# IPv6 – hogy állunk? – APNIC lab mérései alapján

| Code | Region | IPv6 Capable | IPv6 Preferred |
|---|---|---|---|
| XA | World | 35.27% | 34.25% |
| XC | Americas | 42.65% | 41.01% |
| XD | Asia | 39.93% | 38.86% |
| XF | Oceania | 34.97% | 32.90% |
| XE | Europe | 31.69% | 30.96% |
| XG | Unclassified | 26.25% | 26.21% |
| XB | Africa | 2.04% | 2.00% |



# IPv6 – hogy állunk? – APNIC lab mérései alapján

| Code | Region | IPv6 Capable | IPv6 Preferred |
|---|---|---|---|
| XA | World | 35.27% | 34.25% |
| XC | Americas | | |
| XD | Asia | | |
| XF | Oceania | | |
| XE | Europe | | |
| XG | Unclassified | | |
| XB | Africa | | |




| ASN | AS Name | IPv6 Capable | IPv6 Preferred | Samples |
|---|---|---|---|---|
| AS5483 | MAGYAR-TELEKOM-MAIN-AS Magyar Telekom Nyrt. | 74.74% | 74.51% | 447,566 |
| AS21334 | ASN-VODAFONE- | 41.09% | 40.90% | 223,388 |
| AS20845 | DIGICABLE | 24.53% | 24.19% | 155,022 |
| AS213155 | YETTEL-HU Yettel Hungary Ltd. | 63.24% | 63.07% | 84,274 |
| AS8462 | TARR1 | 61.92% | 61.79% | 23,414 |
| AS12301 | INVITECH | 1.19% | 0.98% | 13,153 |
| AS43529 | VIDANET-AS | 4.61% | 4.32% | 12,687 |
| AS35311 | PR-TELECOM-AS | 0.17% | 0.01% | 7,202 |
| AS1955 | HBONE-AS KIFU | 25.47% | 25.21% | 5,878 |
| AS57389 | ZT- | 0.11% | 0.04% | 4,518 |
| AS212910 | OROS | 0.03% | 0.03% | 3,658 |
| AS47169 | HPC-MVM-AS | 0.47% | 0.09% | 3,417 |
| AS25274 | NARACOM- | 0.18% | 0.09% | 3,350 |
| AS50181 | GAX-KABELSZAT | 0.17% | 0.10% | 2,977 |
| AS42232 | PARISAT | 0.10% | 0.07% | 2,913 |
| AS24822 | OPCNET-HU-AS | 0.15% | 0.04% | 2,643 |
| AS8990 | AHRT-AS | 0.92% | 0.50% | 2,599 |
| AS42864 | GIGANET-HU GigaNet Internet Service Provider Co | 0.26% | 0.17% | 2,306 |
| AS47159 | CELLKABEL | 0.04% | 0.04% | 2,304 |
| AS197248 | DRAVANET-AS | 1.20% | 0.93% | 2,248 |

# Bevezetési szempontok

- IPv6  bevezetési stratégia
- IPv6 cím allokáció és menedzsment
- Campus/Enterprise bevezetési szempontok
- Otthoni/szélessávú hálózat kiszolgálási szempontok
- IPv6 biztonság

# Különböző 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
    - 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, …)
- 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)

# IPv6 cím típusok

- Unicast (one-to-one)
  - global – 2001::/3
  - link-local – fe80::/10
  - Unique Local (ULA) – fc00::7
  - IPv4-mapped – csak hoston belül/alkalmazásban lehet vele találkozni
- Multicast (one-to-many)
- Anycast (one-to-nearest)
- Fenntartott

# IPv6 címzés és allokáció

- LIR Szolgáltató – RIR-től kap /32-őt
- A legtöbb felhasználó /48- /60 –at fog kapni:


- /48 esetén 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?

# IPv6 címzés

1. Szekvenciális
2. Topológiai/aggregációs
3. Követve IPv4 címosztást
4. 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 | | Labs |

Cím menedzsment: SLAAC, DHPCv6, manual, privacy addresses (F(Prefix, secret)

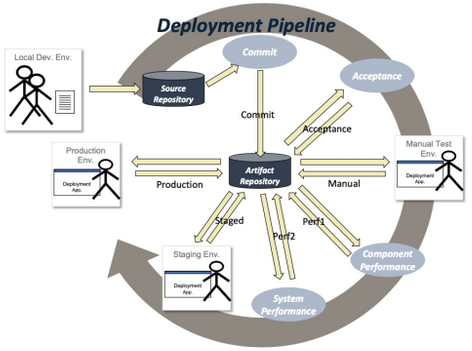
További információk: APNIC, RIPE, Ciscolive, RFC6177

# IPv6 címek - 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 subnetekre auto-konfiguráció esetén ha globális
- /127 vagy linklocal a p2p linkre
- Globális címek - nem minden esetben szükséges
- Minden /64 alhálózat messze több címet tartalmaz, mint amennyi szükséges a világ összes számítógépe számára
- egy /48 tartománnyal pedig 65536 ilyen alhálózatunk lehet
- figyelembe kell venni a belső topológiát és az aggregációt, hogy elkerüljük a későbbiekben felmerülő problémákat.

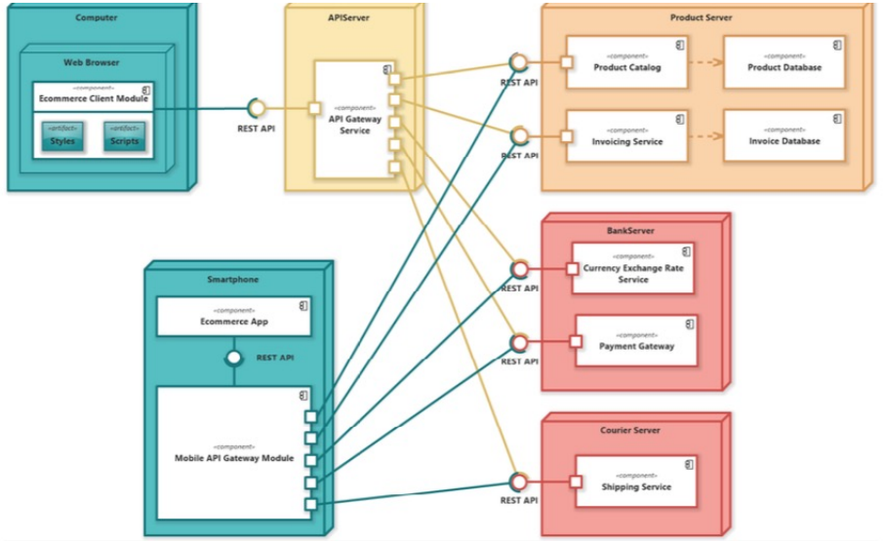
# Vállalati bevezetés – fázisok – RFC 7381

1. Előkészületi és értékelési szakasz
   1. Tervezés
   2. Leltári fázis.
      1. A hálózati infrastruktúra készenléte
      2. Alkalmazások készültségének értékelése
      3. A készültség validálása és tesztelés
   3. Képzés
   4. Biztonsági politika.
      1. Az IPv6 nem biztonságosabb, mint az IPv4.
      2. IPv6 és az IPv4 biztonsági hasonlóságok
      3. Az IPv6 speciális biztonsági problémái
   5. Útvonalválasztás
   6. Címzési terv
   7. Eszközök értékelése
2. Külső/kapcsolódási fázis
   1. Kapcsolódás
   2. Biztonság
   3. Monitoring
   4. Szerverek és alkalmazások
   5. IPv6 Network Prefix Translation
3. Belső fázis
   1. Biztonság
   2. Hálózati infrastruktúra
   3. Végfelhasználói eszközök
   4. Vállalati rendszerek
4. Csak IPv6



# Vállalati rendszerek – mikro szolgáltatás architektúra

- Minden komponens önálló
  - funkcionális és működési összetettséget teremt
  - Vannak kapcsolatok a háttér-összetevők között
  - REST API-k – mind terheléselosztott – DC-ben vagy a felhőben helyezkednek el.
  - Az IoT esetében nem védett helyekre költöznek
    - gyárak, radiológiai osztályok, osztályok stb.
  - végpontok a hálózati szolgáltatók között mozoghatnak
- STUN/ICE nagyon lassú lehet és drága
- **„elsőként IPv6” tervezési modell!**
- Felelősség a jövőbeni problémákért?
- A CGNAT már probléma az ilyen rendszerekben
- A működési támogatás teljesen új kihívás
- Az alkalmazások architektúrájában bekövetkezett változások hatással lesznek a hálózat tervezésére és működtetésére



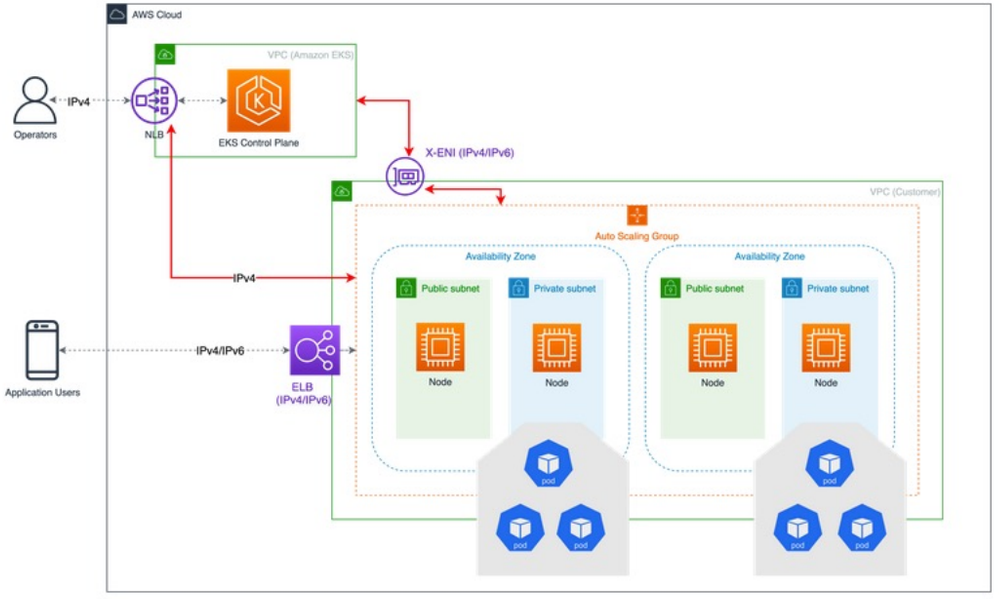
# IPv6 felhőben - ?

- Az IPv4/v6 szolgáltatásparitás gyakran nincs meg
- Egyes (sok?) szolgáltatásokból hiányzik az IPv6 támogatás
- Olvasd el az apró betűs részt és a release notes-ot:

AWS Google Microsoft Azure VNET OpenStack

Eyal Estrin: Is the public cloud ready for IPv6?

- Mire kell figyelni:
  - Geolocation (szolgáltatás paritás)
  - Külső tiltó listák
  - Belső/külső tűzfalszabályok
  - Dual stack alkalmazások támogatása
  - Fejlesztők képzése
  - IPv6 hálózat a fejlesztőknek.
  - IPv6-kompatibilis alkalmazásokat
  - Tesztelés csak IPv6-alapú fejlesztői környezetben

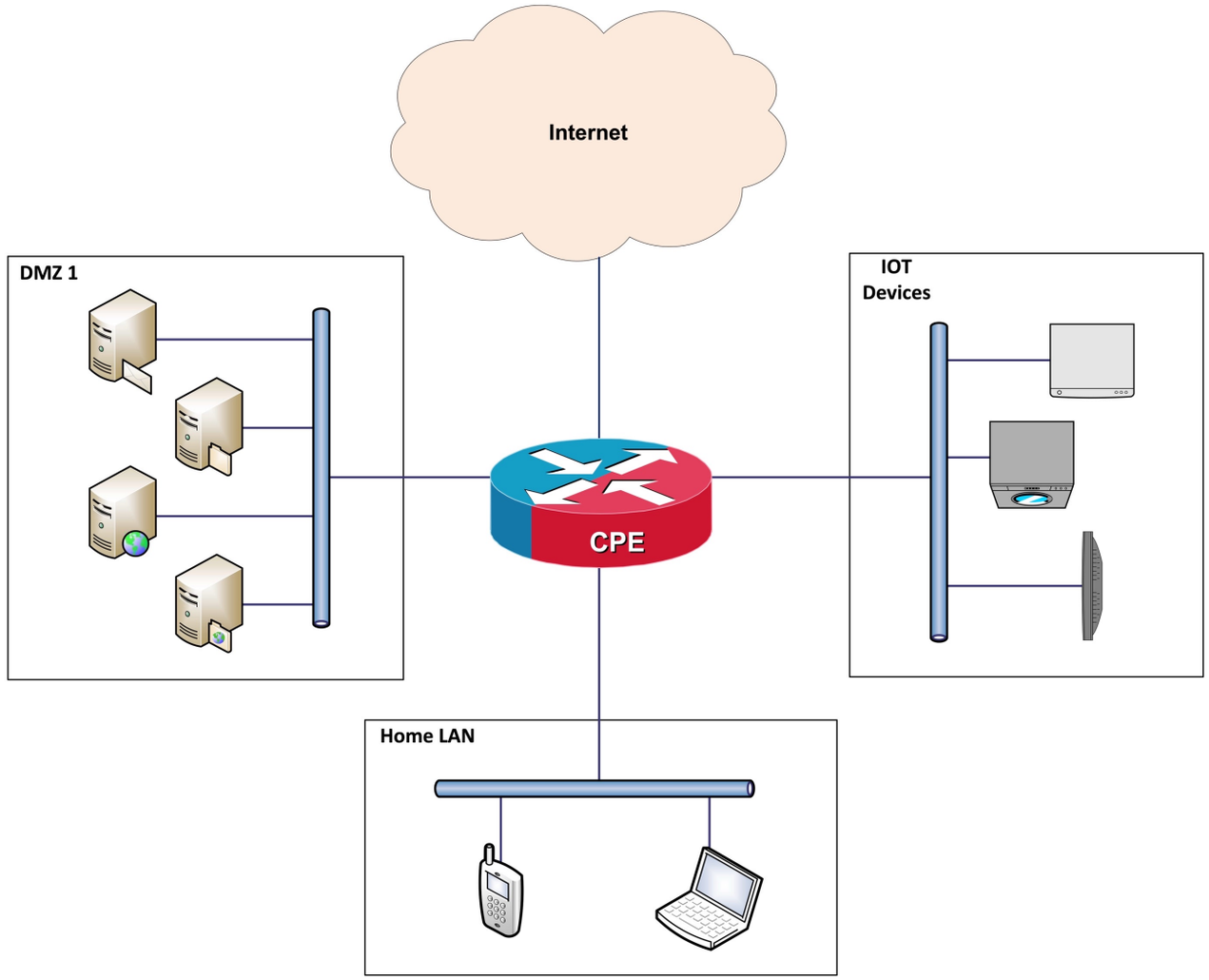


# K8S – IPv6

- Dual stack támogatott 1.21 (2021) óta – GA (1.23)
  - Egyes alkalmazásokat külön konfigurálni szükséges (pl. nginx, ceph)
- Csak IPv6 támogatott 1.18 óta de nem lehetett migrálni ipv4 clusterre (single stack a K8S koncepció része!)
- Kubernetes CNI – Container Network Interface – CNI IPv6 támogatás? – általában ok (Calico, cilium)
- Kubernetes koncepció - pod-ok priváthálózaton működnek
  - Ha azonban GUA-t használunk, a podok teljesen nyilvánosak
  - Ha szolgáltatások belül titkosítatlanul kommunikálnak http vagy hasonló használatával, akkor szolgáltatások titkosítás nélkül is elérhetők a világból
  - Network policy helyes beállítása szükséges!
- A szolgáltatási IP-címek egy külön készletből származnak
  - Legfeljebb /108
  - A /64 nem támogatott – bug
- kube-proxy
  - Az útválasztás helyett a k8s alapértelmezés szerint proxyt használ - az eredeti kérés IP-címének elvesztése

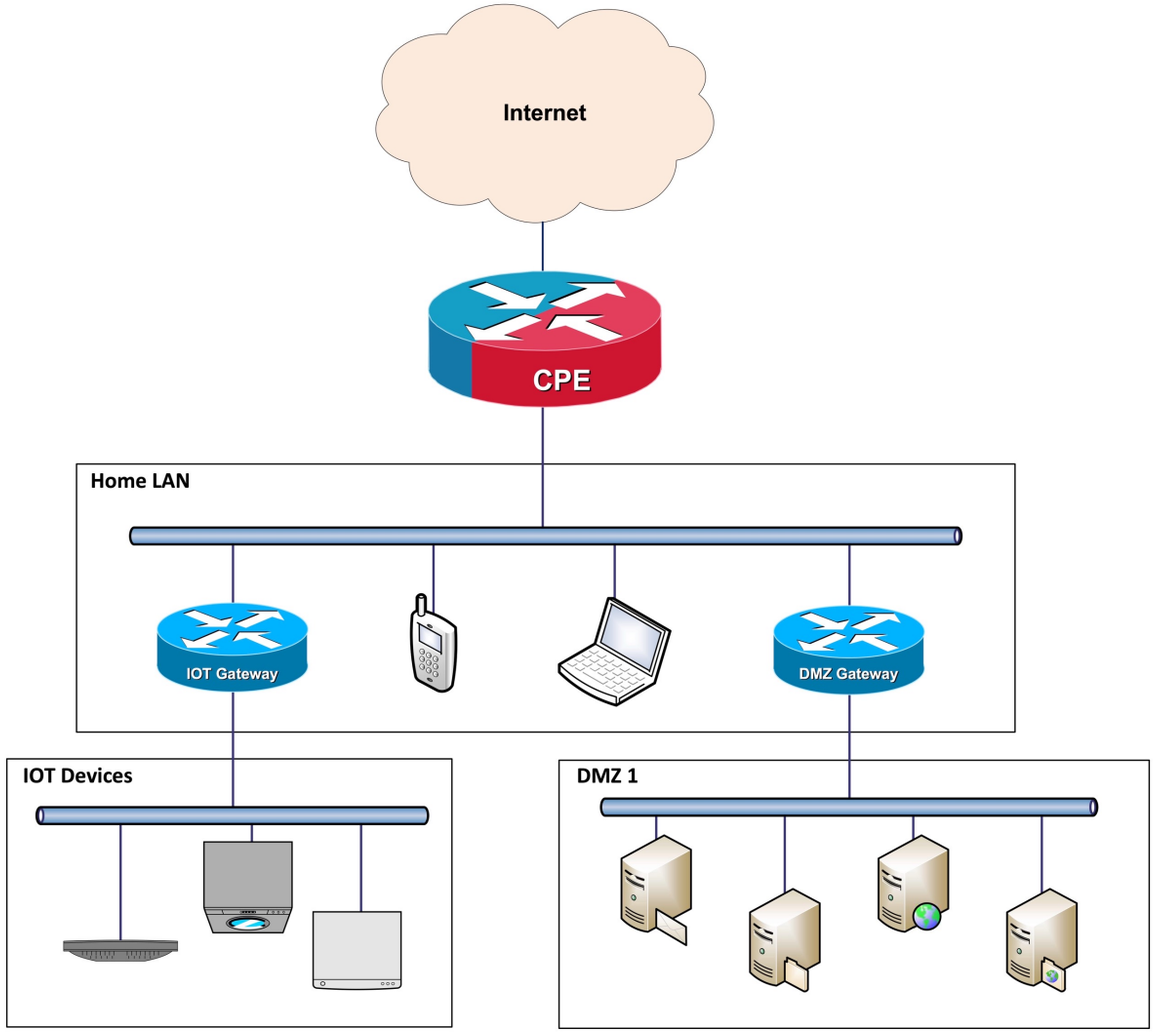
# Otthoni hálózat IPv6-al

- RFC 7084 - Basic Requirements for IPv6 Customer Edge Routers
- RFC 6092 - Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
- RFC 8585 - Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service



# Otthoni hálózat IPv6-al /2

- RFC 7368 - IPv6 Home Networking Architecture Principles
- /48-/60 közötti tartományt kell delegálni felhasználóknak DHCPv6-PD-vel
  - „állandó”, amíg ügyfél nem küld RELEASE-t vagy módosítja a DUID-t
- Otthoni routereknek kell támogatniuk az UPNP-t és PCP-t
- Megcímezhetőség vs. elérhetőség!
- Több szolgáltató esete?

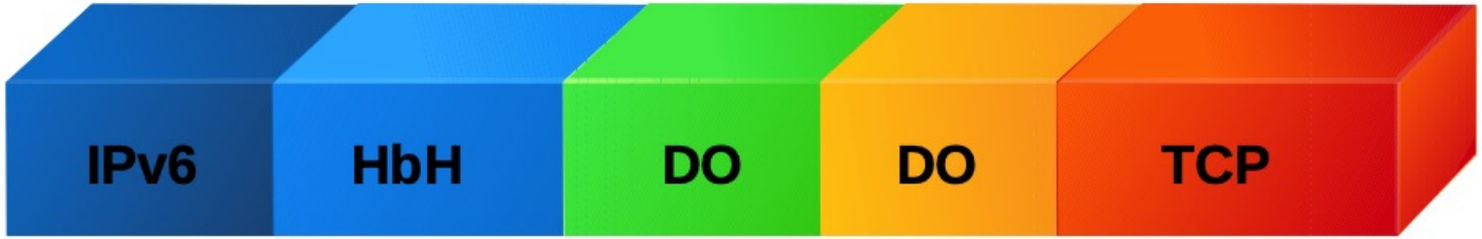


# IPv6 Security – különbségek /1

- Sokkal kevesebb tapasztalatunk van az IPv6-al mint az IPv4-al
- Az IPv6-megvalósítások sokkal kevésbé fejlettek, mint IPv4-es társaik A biztonsági termékek (tűzfalak, NIDS stb.) kevésbé támogatják az IPv6-ot, mint az IPv4-et.
- Internet megnövekedett bonyolultsága:
  - Két protokoll (IPv4 és IPv6)
  - NAT-ok fokozott használata
- Képzett emberi erőforrások hiánya
- IPSEC? - nem igen
- De IPv6 az egyetlen lehetőség, amely lehetővé a hálózati szolgáltatások nyújtását

# IPv6 Security – különbségek /2

1. Extended Headers – komplex feldolgozás

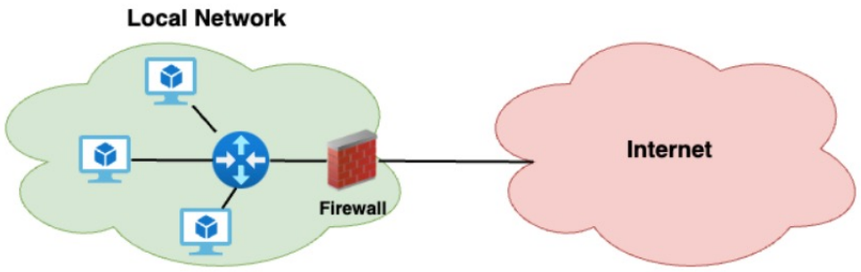



- EH követelmények elemzése
- Nem szükséges EH-k blokkolása
- A tűzfalnak ki kell szűrnie az összes olyan csomagot, amelyben nincs teljes fejléclánc az első töredékben.

2. Szkennelés
   - Munkaállomások és mobilok: SLAAC → véletlenszerű címek → nem megvalósítható DHCPv6 → minta alapú címek → megvalósítható
   - Szerverek (hw, virtuális): Kézi konfiguráció → minta alapú címek → megvalósítható DHCPv6 → minta alapú címek → megvalósítható, SLAAC → kivitelezhetetlen
   - Megfelelő választás és konfiguráció

# IPv6 Security – különbségek /3

3. Tűzfal




- NAT nem szükséges – hasonló szintű biztonság érhető el IPv6-tal mint IPv4-gyel
- A csomagszűrés és alkalmazás gyengeségeit nem tudjuk NAT-tal elrejteni
- Az IPv6 nem követel end-to-end kapcsolatot, de end-to-end címzést tesz lehetővé
- Ne veszélyeztessük az IPv4 biztonságot
- Csak a kimenő kommunikáció engedélyezése (és a visszatérő forgalom)
- Használjunk ideiglenes címeket a stabil címekkel együtt
- Csak meghatározott stabil címekre engedélyezzük a bejövő kapcsolatokat
- Nem lehet vakon kiszűrni ICMPv6-t: PMTUD – packet too big, NS/NA, RS/RA
- Automatikus Block list kezelés komplex lehet - /128 – milyen gyakran változik az ideiglenes cím? - aggregáció? – prefix méret függő blokkolási idő?

# IPv6 Security – különbségek /4

4. Címkonfiguráció
- Az IPv6 biztonsági beállításoknak meg kell egyeznie az IPv4 megfelelőivel
- Van ARP és DHCPv4 biztonsági ellenőrzés a hálózaton?
  - Nincs → Nincs szükség az IPv6-os megfelelőikre sem
  - Van → RA-Guard, DHCPv6-{Snooping, Shield}, FHS és hasonlók telepítése

5. VPN
   - IPv6 hálózaton IPv6-ot nem támogató VPN az IPv6 forgalmat VPN nélkül kiengedi…..

6. Csak IPv4 hálózat?
   - Az IPv6 támogatása általában alapértelmezés szerint engedélyezve van az összes operációs rendszerben

# IPv6 a világban

## RFC 9386 - IPv6 Deployment Status

| Internet access changing to IPv6-only | Reports of speed benefit of IPv6 = $$$ | (Renewed) Government requirements | Industry pressure | Public Cloud IPv6 support |
|---|---|---|---|---|
| comcast xfinity (USA) | amazon | (USA) OMB-21-07 | | aws |
| T-Mobile (USA) | Meta | (USA) | | Azure |
| sky (UK & Italy) | Google | (China) | | Google Cloud |
| free (France) | Akamai | (Vietnam) | | |
| Jio (India) | Bing | | | |
| orange (France, Poland) | | | | |

# KIFÜ – magyar oktatási-kutatás digitalis infrastruktúra

# KIFÜ – magyar oktatási-kutatás digitalis infrastruktúra

## NIIF Program 1986 óta

**1992 tagja a nemzetközi NRENeknek**

NIIFI + KIFU összeolvadás 2016

## Hálózati technológiák

MPLS (2002), IPv6(2003), Segment routing (2013), 100 Gbps (2012)

**Hibrid hálózat (** IP/MPLS +DWDM) – nx100+ Gbps sebesség

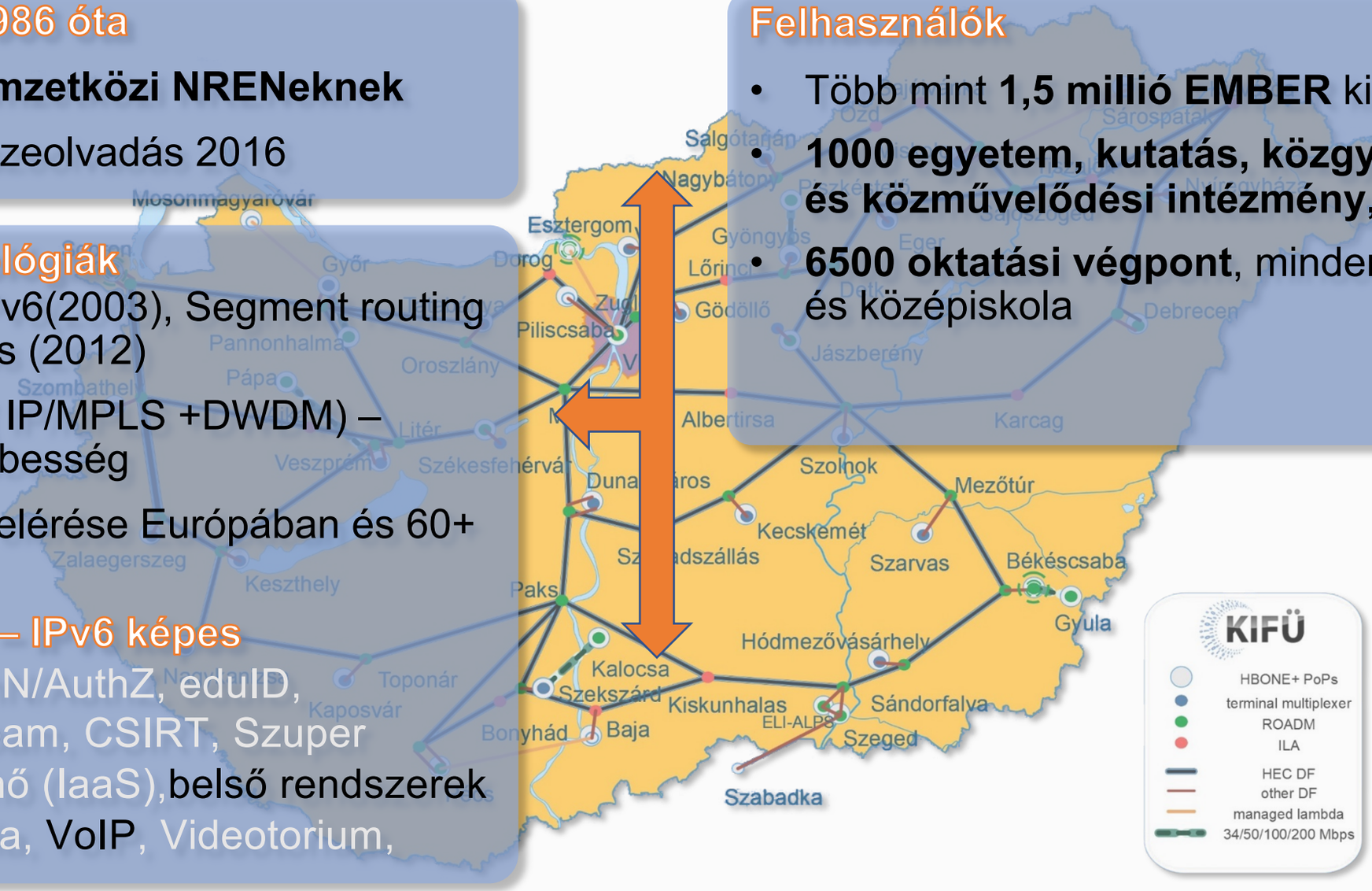
44 R&E hálózat elérése Európában és 60+ világszerte

## Szolgáltatások – IPv6 képes

Szövetségi AuthN/AuthZ, eduID, eduGAIN, eduroam, CSIRT, Szuper számítógép, felhő (IaaS),belső rendszerek Videokonferencia, VoIP, Videotorium,

## Felhasználók

- Több mint **1,5 millió EMBER** kiszolgálása
- **1000 egyetem, kutatás, közgyűjtemény és közművelődési intézmény, kórház**
- **6500 oktatási végpont**, minden általános és középiskola



# Kérdések?

- mohacsi.janos@kifu.gov.hu

Slido

Slido.com #2032 745