

# Počítačové sítě 2

Jan Outrata



KATEDRA INFORMATIKY  
UNIVERZITA PALACKÉHO V OLMOUCI

přednášky



# Internet Protocol verze 6 (IPv6)

- 90. léta **rozmach Internetu** (komercializace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání  $\Rightarrow$  potřeba mnoha (unikátních) IP adres

- 90. léta **rozmach Internetu** (komercializace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání  $\Rightarrow$  potřeba mnoha (unikátních) IP adres
- ↪ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]

- 90. léta **rozmach Internetu** (komercializace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres
- ↪ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]
- setřeni (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpány** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ↪ černý trh s (globálními, veřejnými) IPv4 adresami

- 90. léta **rozmach Internetu** (komercializace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres
- ↪ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]
- setření (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpáný** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ↪ černý trh s (globálními, veřejnými) IPv4 adresami
- = **následovník IPv4**, IPng: otevřený vývoj IETF od 1991, základ **RFC 1883** (1995), **2460** (1998), 8200 (2017), neustálý vývoj, mnoho dalších RFC
  - příležitost řešení více nedostatků IPv4 – např. nejednotné adresní schéma pro Internet a LAN (NAT)
  - jediné dlouhodobé řešení problémů Internetu

- 90. léta **rozmach Internetu** (komercializace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres
- ↔ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]
- setřetí (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpány** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ↔ černý trh s (globálními, veřejnými) IPv4 adresami
- = **následovník IPv4**, IPng: otevřený vývoj IETF od 1991, základ **RFC 1883** (1995), **2460** (1998), 8200 (2017), neustálý vývoj, mnoho dalších RFC
  - příležitost řešení více nedostatků IPv4 – např. nejednotné adresní schéma pro Internet a LAN (NAT)
  - jediné dlouhodobé řešení problémů Internetu
- nejen **větší adresní prostor** (delší adresy), **nový pohled** na síťový paket, adresy a protokol:
  - zjednodušení záhlaví paketu, volitelná další záhlaví
  - **automatická konfigurace zařízení** a objevování sousedů – lokální adresy, SLAAC, ND
  - podpora QoS, real-time přenosů – tok/flow paketů
  - **zabezpečení** (autentizace a šifrování) – IPsec
  - **mobilita** – s využitím tzv. domácích agentů („zastupující“ směrovač v domácí síti)

- 90. léta **rozmach Internetu** (komercializace) + mobilní sítě a WiFi + IoT – změna rozsahu a způsobu využívání ⇒ potřeba mnoha (unikátních) IP adres
- ↪ **vyčerpávání adresního prostoru IPv4** – nedostatečný [PS-1.1]
- setřeni (CIDR, NAT), ale na (nejvyšší) úrovni IANA-RIR **vyčerpány** 2/2011, na úrovni RIR-LIR 11/2019 [PS-1.2] ↪ černý trh s (globálními, veřejnými) IPv4 adresami
- = **následovník IPv4**, IPng: otevřený vývoj IETF od 1991, základ **RFC 1883** (1995), **2460** (1998), 8200 (2017), neustálý vývoj, mnoho dalších RFC
  - příležitost řešení více nedostatků IPv4 – např. nejednotné adresní schéma pro Internet a LAN (NAT)
  - jediné dlouhodobé řešení problémů Internetu
- nejen **větší adresní prostor** (delší adresy), **nový pohled** na síťový paket, adresy a protokol:
  - zjednodušení záhlaví paketu, volitelná další záhlaví
  - **automatická konfigurace zařízení** a objevování sousedů – lokální adresy, SLAAC, ND
  - podpora QoS, real-time přenosů – tok/flow paketů
  - **zabezpečení** (autentizace a šifrování) – IPsec
  - **mobilita** – s využitím tzv. domácích agentů („zastupující“ směrovač v domácí síti)
  - ! při zachování podstaty IP (end-to-end komunikace, nespojovost, hop-by-hop doručování) a kompatibility s dalšími protokoly (TCP/UDP, ICMP, IGMP → MLD, OSPF, BGP, DNS aj.)



- před daty až 64 kB záhlaví 40 B:
- verze 4 b – hodnota 6
- traffic class 8 b  $\sim$  TOS z IPv4 – priorita doručení/QoS (pro aplikaci nebo v rámci toku, v praxi differentiated services) a signalizace zahlcení (ECN, 2 b)
- **flow label** 20 b – ID **toku/flow paketů** = označení „souvisejících“ paketů mezi odesílatelem a příjemcem pro stejné zacházení  $\sim$  **pseudospojení**, využití např. pro:
  - směrování – rozhodnutí jen u prvního paketu toku, rozkládání zátěže do více cest apod.
  - rezervaci přenosové kapacity (QoS, real-time, protokol RSVP) – např. pro streamovaný A/V přenos
  - prioritní uživatel aj.
- **délka dat** 16 b (v B)  $\neq$  délka paketu z IPv4 – včetně volitelných záhlaví
- **další záhlaví** 8 b = číslo protokolu z IPv4 v datech (např. TCP 6, UDP 17, ICMP 58) nebo typ následujícího volitelného záhlaví
- hop limit 8 b  $\sim$  TTL z IPv4 – snižování směrovačem o 1
- **adresy odesílatele a příjemce** 128 b – „aby už nikdy nedošly“

# Síťový paket

Obrázek z knihy  
zdroj: KR 4.16



Obrázek z knihy  
zdroj: KR 4.26

Z IPv4 záhlaví zrušeny:

- délka záhlaví – pevná (20 B)
- ID paketu, bity a offset pro **fragmentaci** paketu – směrovači náročná, pouze odesílatelem – volitelné záhlaví, udržování info o minimální MTU k příjemcům
- kontrolní součet záhlaví – jsou na transportní a linkové (CRC) vrstvě

Z IPv4 záhlaví zrušeny:

- délka záhlaví – pevná (20 B)
- ID paketu, bity a offset pro **fragmentaci** paketu – směrovači náročná, pouze odesílatelem – volitelné záhlaví, udržování info o minimální MTU k příjemcům
- kontrolní součet záhlaví – jsou na transportní a linkové (CRC) vrstvě

**Volitelná záhlaví** (rozšíření ~ volby z IPv4):

- posloupnost více, řetěz: v každém první položka typ následujícího 8 b [PS-2.3], druhá délka 8 b (v 8B, mimo 8 B), další proměnlivé [PS-2.4] – typy v pořadí:
- volby pro všechny (hop-by-hop) 0 – pro směrovače na cestě, položky typ 8 b, délka 8 b (mimo 2 B), hodnota [PS-2.5], např. výplně 1 (jen typ) a více B, upozornění směrovače, rychlý start (přenosová rychlost např. u 1. segmentu TCP), jumbogram (64 kB < velikost paketu < 4 GB) aj.
- volby pro cíl (destination) 60 – i za ESP (pro příjemce), např. výplně, PDM (měření zpoždění), domácí adresa aj.



## Volitelná záhlaví (rozšíření ~ volby z IPv4):

- směrování 43 – typ 0 ~ explicitní směrování z IPv4 2007 zrušen, typ 2 pro mobilitu (domácí adresa po doručení)
- fragmentace 44 ~ z IPv4 – délka 8 B, jen bit více fragmentů, ID 32 b [PS-2.7], všechna záhlaví (i transportní) v prvním, ve všech záhlaví před fragmentačním [PS-2.9]
- **autentizace AH** 51 – odesílatele, i integrita paketu
- **šifrování ESP** 50 – dat, odesílatelem nebo směrovačem, poslední záhlaví, + AH = **IPsec**
- další volitelné, např. mobilita 135 aj.
- problém firewally – neznají záhlaví, paket zahodí

- RFC 4291
- pro síťové rozhraní více (povinně), všichni v LAN stejná (pod)sít
- typy: unicast (individuální), multicast (skupinové, paket doručen všem členům skupiny) – broadcast speciální skupiny, např. všichni v LAN
  - **anycast (výběrové)** = skupinové, paket doručen jednomu „nejbližšímu“ (v počtu směrovačů na cestě) členu skupiny, např. routery v síti, (kořenové) DNS servery nebo webové servery – duplikace služby (rozložení zátěže, zrychlení, zálohy), i pro IPv4
- notace např. 2001:0718:1401:0050:0000:0000:0000:000d, zkrácený (kanonický) zápis 2001:718:1401:50::d, v URL v [] (RFC 3986)
- **síťový prefix** ~ adresa sítě/maska z IPv4 – maska = počet bitů 1 (CIDR) = délka prefixu, např. 2001:718:1401:50::/64
- ::/128 (0) nedefinovaná (nepřidělená), ::1/128 **lokální smyčka (loopback)**

## Unicast (individuální)

- až 64 b síť (síťový prefix), 64 b ID (síťového) rozhraní [PS-3.1]
- **globální** zatím 2000::/3 (RFC 3587) – jednoznačné v rámci celého Internetu, dalších 45 b globální (směrovací) prefix sítě [PS-3.22]:
  - RIR: 32 b (má /12, přiděluje /29 až /32)
  - LIR: 16/24/32 b (přiděluje /48, /56 nebo /64)
  - pak ID podsítě zákazníků LIR: 16/8/0 b
  - pro dokumentace 2001:db8::/32 – u IPv4 tři /24
- **link local** fe80::/10 – jednoznačné v rámci LAN (propojení na linkové vrstvě), nesměřují se, dalších 54 b nulových
- **unique local (ULA)** fc00::/7 (fd00::/8 lokální přidělení, RFC 4193) – jednoznačné v rámci organizace (intranetu), nesměřují se, dalších 40 b náhodné globální ID, 16 b ID podsítě
  - dříve site local fec0::/10 – jednoznačné v rámci „místní“ sítě, 54 b ID podsítě, problém více „míst“ jedné organizace
  - obdoba vyhrazených rozsahů adres pro privátní sítě z IPv4 – link a unique local jejich rozšíření
  - NAT netřeba (dostatek globálních adres), ale existuje NPTv6 (RFC 6296, bezstavový obousměrný překlad síťových prefixů)

## ID rozhraní (unicast)

- pevně 64 b, vlastní (přidělené) – jako u IPv4, nebo generované:
- původně **modifikované IEEE EUI-64** = MAC adresa rozhraní dle IEEE 802.x s 0xffffe „uprostřed“ a druhý bit prvního byte 1 (lokalita), např. pro 00:02:b3:bf:30:ea je 202:b3ff:febf:30ea – problém globálního ID = MAC a ne-bezpečnosti (zneužití)
- **kryptografické** (CGA, RFC 3972) – na základě veřejného klíče „vlastníka“ rozhraní, problém komplikovanosti určení
- **náhodné krátkodobé** (Privacy Extensions, RFC 4941) pro odchozí komunikaci – náhodné, problém dočasnosti, návrh polovina stálá
- **náhodné stálé** (RFC 7217) = posledních 64 b RID = hash síťového prefixu, (jiného) ID rozhraní a LAN, čítače a tajného klíče



## Multicast (skupinové)

- $ff00::/8$  – trvalé a dočasné, první 4 b druhého byte **dosah skupiny** [PS-3.15] ~ jednoznačnost adresy v zóně, např. 1 rozhraní, 2 linka (LAN), 5 místo, 8 organizace, E globální, ostatní např. ISP, A CESNET2, 112 b ID skupiny
- ID skupiny: definované IANA (trvalé) a vlastní (dočasné) – typy: obsahující globální unicast prefix sítě, od jediného odesílatele (SSM), obsahující ID rozhraní aj., 32 b ID
- speciální např.  $ff0x::1$  **broadcast** rozhraní/LAN,  $ff0x::2$  všechny směrovače,  $ff02::1:ff00:0/104$  **vyzývaný uzel (solicited node)** (poslední 3 B ID rozhraní, pro objevování sousedů), pro další typy uzlů a služeb (definované IANA, RFC 2375)

## Multicast (skupinové)

- $ff00::/8$  – trvalé a dočasné, první 4 b druhého byte **dosah skupiny** [PS-3.15] ~ jednoznačnost adresy v zóně, např. 1 rozhraní, 2 linka (LAN), 5 místo, 8 organizace, E globální, ostatní např. ISP, A CESNET2, 112 b ID skupiny
- ID skupiny: definované IANA (trvalé) a vlastní (dočasné) – typy: obsahující globální unicast prefix sítě, od jediného odesílatele (SSM), obsahující ID rozhraní aj., 32 b ID
- speciální např.  $ff0x::1$  **broadcast** rozhraní/LAN,  $ff0x::2$  všechny směrovače,  $ff02::1:ff00:0/104$  **vyzývaný uzel (solicited node)** (poslední 3 B ID rozhraní, pro objevování sousedů), pro další typy uzlů a služeb (definované IANA, RFC 2375)

## Anycast (výběrové)

- ze stejné části adresního prostoru jako globální unicast (individuální)
- směrování v rámci nejdelšího společného síťového prefixu (udržování skupin na směrovačích)  $\Rightarrow$  téměř výhradně v rámci sítě/AS, globálně výjimečně
- problém různých „nejbližších“ příjemců (dynamičnost směrování)  $\rightarrow$  zjištění unicast adresy nebo nastavová komunikace, např. DNS
- (pod)síť (~ „obecná“ adresa): pevné ID rozhraní, např. 0 směrovače pro každý prefix

# Nedokončené – přehledově



- **zjišťování a aktualizace linkové adresy** (MAC) rozhraní uzlu v LAN pro IPv6 adresu a opačně ~ ARP a RARP u IPv4
  - ověřování dosažitelnosti sousedů a detekce duplicitních adres v LAN
- žádost o a oznámení o linkové adrese – zprávy **neighbor solicitation (NS)** a **neighbor advertisement (NA)**
- používání link local adres, NS na (multicast) adresu vyzývaného uzlu
  - součást **ICMPv6** (RFC 4443): formát paketu a zprávy jako u ICMPv4, nové zprávy

## Bezstavová (StateLess Address AutoConfiguration, SLAAC)

- součást ND: **zjišťování směrovačů v LAN a dalších údajů sítě** (prefix, DNS aj.)
  - žádost o a oznámení směrovače – zprávy **router solicitation (RS)** a **router advertisement (RA)** – směrovače rozesílají (náhodně) periodicky, obě na (multicast) adresu všech směrovačů v LAN
- „**samopřidělení**“ unicast (individuální) **adresy**:
  - 1 pro globální z RA, popř. s předchozí RS, získány údaje sítě
  - 2 vytvoření ID rozhraní – generované
  - 3 kontrola jedinečnosti v LAN – detekce duplicitní (ND)
    - pro globální (prefix) může být v RA „zakázáno“, link local vždy

## Bezstavová (StateLess Address AutoConfiguration, SLAAC)

- součást ND: **zjišťování směrovačů v LAN a dalších údajů sítě** (prefix, DNS aj.)
- žádost o a oznámení směrovače – zprávy **router solicitation (RS)** a **router advertisement (RA)** – směrovače rozesílají (náhodně) periodicky, obě na (multicast) adresu všech směrovačů v LAN
- „**samopřidělení**“ unicast (individuální) **adresy**:
  - 1 pro globální z RA, popř. s předchozí RS, získány údaje sítě
  - 2 vytvoření ID rozhraní – generované
  - 3 kontrola jedinečnosti v LAN – detekce duplicitní (ND)
    - pro globální (prefix) může být v RA „zakázáno“, link local vždy

## DHCPv6

- zprávy jako u DHCPv4, používání link local adres (a speciálních multicast)
- **stavové** = údaje sítě kromě směrovače – z RA, přidělení adresy
- **bezstavové** = údaje sítě kromě směrovače a prefixu – nepřidělení adresy → SLAAC
- identifikace uzlu (ne rozhraní!) **DUID** – 3 typy

- = **postupný přechod**, ne „přepnutí Internetu“ z IPv4 na IPv6
  - zpočátku (1996–2006) lokální IPv6 sítě propojené IPv4 tunely = síť 6bone, dnes přímo
  - ? uživatelé a organizace (i menší ISP) „váhají“ – problém „slepice vs. vejce“
- velcí poskytovatelé obsahu a ISP – potřeba mnoha adres, World IPv6 Launch Day 6. 6. 2012
  - politická podpora – EU 2002, 2008, 2013, . . . , např. projekty 6NET, GEN6 aj., ČR 2009, 2015 výzva ministerstva/eGovernment po IPv6 . . .
  - 2023 cca 40+ % (Internet Society, Google) koncových zařízení/sítí celosvětově, ČR cca 20+ %

- = **postupný přechod**, ne „přepnutí Internetu“ z IPv4 na IPv6
  - zpočátku (1996–2006) lokální IPv6 sítě propojené IPv4 tunely = síť 6bone, dnes přímo
  - ? uživatelé a organizace (i menší ISP) „váhají“ – problém „slepice vs. vejce“
- velcí poskytovatelé obsahu a ISP – potřeba mnoha adres, World IPv6 Launch Day 6. 6. 2012
  - politická podpora – EU 2002, 2008, 2013, . . . , např. projekty 6NET, GEN6 aj., ČR 2009, 2015 výzva ministerstva/eGovernment po IPv6 . . .
  - 2023 cca 40+ % (Internet Society, Google) koncových zařízení/sítí celosvětově, ČR cca 20+ %

## Implementace

- i přes podobnost **nekompatibilní s IPv4**, nové protokoly nezávislé na IPv4
- 1996–2000 experimentální (Linux), 2000+ vlna „podporujeme IPv6“, 2005+ podpora výrobci HW a SW
- certifikace **IPv6 Forum** programy Ready pro hardware a systémy a Enabled pro služby (web a ISP) [PS-1.3]





- **dual stack** = podpora současně IPv4 i IPv6
- **tunelování IPv6 v IPv4 a opačně**
  - manuální – tunel server (IPv4 do IPv6 sítě) a tunel broker (registrace na tunel serveru), např. Freenet6, SixXS aj.
  - automatické: dříve 6to4, Teredo, 6over4, ISATAP, dnes **6rd** (IPv6 Rapid Deployment), **DS** (Dual-Stack) **Lite**, **lw4o6** (Lightweight 4over6), MAP-E
- **překlad (adres a DNS) mezi IPv6 a IPv4**: základ **SIIT** (Stateless IP/ICMP Translation), starší NAT-PT (NAT – Protocol Translation), novější **NAT64 a DNS64**, **464XLAT**, MAP-T, TRT (Transport Relay Translator), BIH (Bump-in-the-Host), SOCKS64