

IPv6: Proč IoT potřebuje více IP adres

Každé zařízení připojené k internetu – ať už je to notebook, mobilní telefon nebo chytrý termostat – potřebuje svou unikátní identifikační značku, aby mohlo odesílat a přijímat data. Tato značka se nazývá **IP adresa**. Rozmach Internetu věcí (IoT) však přivedl původní adresovací systém na pokraj jeho kapacity.

Problém jménem IPv4

Současný internet byl z velké části vybudován na protokolu **IPv4** (Internet Protocol verze 4).

- Tento protokol používá 32bitové adresy, což umožňuje vytvořit zhruba **4,3 miliardy** unikátních IP adres.
- V 80. letech se to zdálo jako nevyčerpatelné množství. Dnes, kdy má průměrný člověk počítač, smartphone, chytré hodinky a další elektroniku, jsou tyto adresy globálně prakticky vyčerpány.

Aby internet vůbec mohl dál fungovat, masivně se využívá technologie zvaná **NAT (Network Address Translation)**. Díky NATu sdílí všechna zařízení ve tvé domácí síti jedinou veřejnou IPv4 adresu. Domácí router pak funguje jako překladatel a vnitřně rozděljuje provoz.

Pro síť IoT je ale NAT velkou překážkou. Komplikuje přímou komunikaci mezi zařízeními a vyžaduje složité obezličky, aby se vnější systémy dokázaly spojit se senzorem schovaným za routerem.

Řešení: Protokol IPv6

Protokol **IPv6** je nová generace internetového protokolu, která byla navržena tak, aby problém s nedostatkem adres jednou provždy vyřešila.

Zatímco IPv4 používá 32 bitů, IPv6 využívá **128bitové adresy**. Výsledný počet dostupných adres je astronomický: přibližně 340 sextilionů (číslo s 36 nulami). V praxi to znamená, že bychom mohli přidělit IP adresu doslova každému zrnku písku na Zemi, a stále by jich obrovské množství zbylo.

Proč je IPv6 pro IoT naprosto klíčové?

Přechod na IPv6 není jen o větším množství čísel. Pro Internet věcí přináší několik nenahraditelných výhod:

1. Konec NATu a návrat k "End-to-End" komunikaci

Díky nevyčerpatelnému množství adres může dostat každé IoT zařízení – každý senzor na poli nebo stroj v továrně – svou **vlastní unikátní veřejnou IP adresu**. Zařízení mohou komunikovat napřímo přes internet (end-to-end) bez nutnosti složitého nastavování routerů nebo přesměrovávání portů.

2. Autokonfigurace (SLAAC)

Protokol IPv6 obsahuje funkci zvanou **Stateless Address Autoconfiguration (SLAAC)**. Zařízení, které se připojí k síti, si dokáže samo vygenerovat platnou IP adresu bez nutnosti centrálního serveru (jako je DHCP u IPv4). To je naprosto ideální pro tisíce drobných, nízkoenergetických senzorů, které se potřebují jen rychle připojit, odeslat data a zase se uspat.

3. Menší režie a efektivnější směrování

Hlavičky datových paketů v IPv6 jsou navrženy tak, aby byly jednodušší a strukturovanější. Síťové prvky je díky tomu dokážou zpracovávat rychleji, což snižuje zátěž sítě a šetří výpočetní výkon. Pro IoT zařízení s minimálním výkonem a bateriovým napájením je každý ušetřený cyklus procesoru velkou výhodou.

4. Nativní podpora bezpečnosti

Ačkoliv bezpečnostní protokol **IPsec** (zajišťující šifrování a autentizaci síťové komunikace) lze používat i u IPv4, u IPv6 byl od začátku navržen jako jeho integrální součást. Jelikož jsou IoT zařízení často terčem hackerů kvůli slabému zabezpečení, přímá integrace pokročilých bezpečnostních mechanismů přímo do síťové vrstvy představuje velký posun vpřed.

Související články:

- [OSI model a síťové vrstvy](#)
- [Zabezpečení sítě a NAT](#)
- [Základní komunikační protokoly IoT](#)

From:

<https://serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:

<https://serviceit.cz/doku.php?id=it:siete:ipv6>

Last update: **2026/05/30 18:08**

