# **5. Síťová vrstva referenčního modelu OSI**

**Osnova:**

* třetí vrstva ISO/OSI modelu
* v Internetu poskytuje spojení mezi LAN sítěmi
* na této vrstvě pracují routery

**(1.) Účel, funkce síťové vrstvy**

Třetí vrstva modelu OSI poskytuje služby pro výměnu dat mezi koncovými zařízeními pomocí logického adresování a směrování. **Její účel je zajistit doručení paketů do vzdálené sítě.**

Pro docílení end-to-end komunikace, **protokoly síťové vrstvy vykonávají 4 základní funkce**

1. **Adresování koncových zařízení** – pro komunikaci musí být koncová zařízení adresována jedinečnou IP adresou
2. **Zapouzdření** – síťová vrstva zapouzdřuje datové jednotky protokolů (PDU) do **paketů**. Zapouzdření přidává do záhlaví informace o zařízeních
3. **Směrování** – síťová vrstva poskytuje služby pro směrování paketů k cílovým hostitelům na jiných sítích. Role routeru je směrovat pakety nejlepší cestou k cíli. Každý router, kterým paket projde k dosažení cíle se nazývá hop
4. **Rozbalení** – když se paket dostane k síťové vrstvě hostitele, hostitel zkontroluje IP adresu, pokud odpovídá jeho vlastní IP adrese, paketu záhlaví odstraní a výsledné PDU 4. vrstvy pošle příslušné službě na transportní vrstvě

**(2.) Protokoly síťové vrstvy a jejich datové jednotky**

Síťová vrstva využívá různé protokoly pro logické adresování, směrování a jiné služby pro end to end komunikaci. Příklady protokolů jsou:

1. **Internet Protocol (IP):** 
   * Hlavní protokol používaný pro adresování a směrování paketů\*\*
   * Zodpovědný za dělení dat a jejich následné zapouzdření do paketů
   * 2 nejrozšířenější verze
     1. **IPv4** – **používá 32bitouvou adresu** => **méně adres, než zařízení na internetu tento problém řeší NAT** protokol, který dovoluje více zařízením sdílet jednu IP adresu
     2. **IPv6** – vznikla jako **řešení na nedostatek IPv4 adres**, používá **128bitovou adresu**
        1. Ke komunikaci se využívají multicast adresy, např. na RS, RA, atd.
           1. RS = Router Solicitation

Snaží se najít IPv6 default gateway

* + - * 1. RA = Router Advertisment

Odpověď na RS

“Hej zmrde, mojí adresu můžeš použít pokud se chceš dostat do jiných sít”

* + - * 1. NS = Neighbor Solicitation

Zjišťování souseda

Zjišťování zda soused je stále up

Využíváno v DAD

* + - * 1. NA = Neighbor Advertisement

Odpověď na NS

NA je zaslán taky, když si uzel změní link-local adresu

* + **Základní jednotka IP protokolu se nazývá paket (datagram)**

## Vlastnosti IP protokolu

* Přenos dat pomocí IP protokolu je:
  1. **Nespojovaný** — Connectionless communication
     + Před odesláním dat se nenavazuje spojení mezi odesílatelem a příjemcem
     + Odesílatel neví, zda příjemce existuje a jestli je schopen data přijmout
     + Jednotlivé pakety z jednoho přenosu mohou putovat k cíli různými cestami
       - Tím můžou dorazit v různém pořadí
  2. **Nespolehlivý** — Best effor
     + Odesílatel odesílá odeslat data co nejrychleji
     + Není zaručeno, že všechna data se doručí
     + Odesílatel nezjistí, zda data byla úspěšně doručena
  3. **Nezávislý na typu přenosového média**
     + IP pakety putují po jakémkoliv přenosovém médiu, díky linkové vrstvě

1. **Address Resolution Protocol (ARP):** 
   * Zařízení na ethernetové síti musí znát IP adresu i MAC adresu
   * ARP umožňuje zjistit MAC adresu pomocí IP adresy
   * Každé zařízení má ARP tabulku, ve které má MAC a IP adresy známých nařízení
   * PDU ARP je ARP paket, ten obsahuje ARP záznam, který obsahuje:
     1. IP adresu
     2. MAC adresu
     3. Typ hardwarové adresy
     4. Typ protokolu – protokol použitý pro přenos dat
     5. Délka hardwarové adresy
     6. Délka protokolu – délka použité IP adresy
2. **Internet Control Message Protocol (ICMP):** 
   * Používá se pro řešení problémů v síti (př. Zjišťování, zda jsou zařízení dostupná)
   * Umožňuje přenos chybových zpráv mezi zařízeními
   * Vysílání zpráv pro ověření připojení
     1. Ping – informuje uživatele o stavu připojení
     2. Traceroute – ukazuje uživateli všechny hopy mezi zařízeními
   * PDU ICMP je ICMP paket
   * Error zprávy:
     1. Destination nebo service unreachable
     2. Time exceeded – TTL v paketu klesne na 0 u IPV4, u IPV6 je to Hop limit
3. **Open Shortest Path First (OSPF):** 
   * Protokol pro dynamické směrování paketů po síti
   * Po konfiguraci namapuje automaticky celou síť a reaguje i na změny v síti
   * Pakety směruje po nejoptimálnější cestě, kterou vypočítá pomocí ceny (path cost) – každá cesta má cenu která se odvozuje od rychlosti přenosu
   * Základní **PDU OSPF je Hello Paket**, který kontroluje dostupnost ostatních zařízení v síti, další PDU jsou
     1. **DBD** – shrnutí rout
     2. **LSR** (link state request) PDU pomocí kterého žádá o informace o síti
     3. **LSU** (link state update) PDU pomocí kterého přenáší informace o síti
     4. **LSA** (link state advertisment) PDU pomocí kterého potvrzuje úspěšný příjem informací

**(3.) Princip paketového přenosu dat**

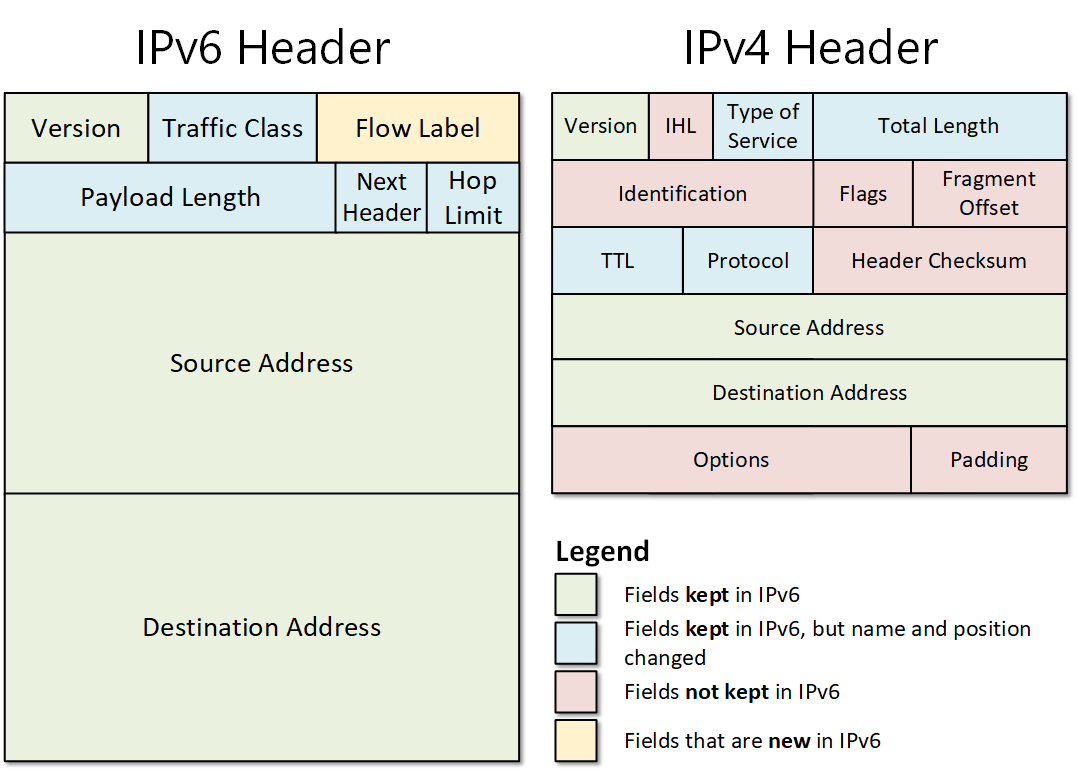
Princip přenosu dat v paketu spočívá v rozdělení dat na menší části a vložení do paketu který obsahuje informace o odesílateli a cíli.

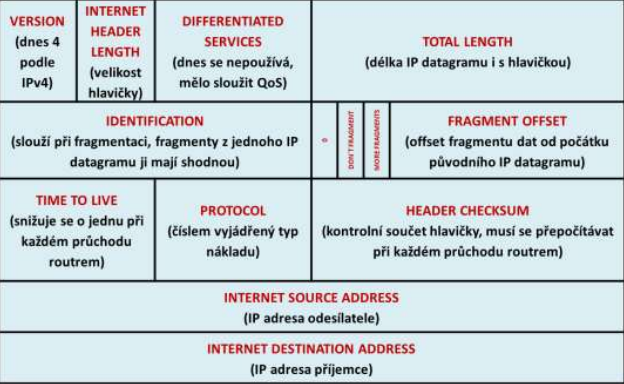
1. V **záhlaví paketu IPv4** se nachází tyto informace:
   * **Version** – IP verze paketu
   * **Differential services** (DS) – určují prioritu paketu
   * **Protocol** – toto pole obsahuje jakému protokolu paket patří, to umožňuje síťové vrstvě poslat data vhodnému protokolu vyšší vrstvy (TCP, UDP, ICMP…)
   * **Time To Live** (TTL) – Hodnota, která **určuje délku životnosti** paketu, zdrojové zařízení nastaví hodnotu, která se zmenší o 1 po každém zpracování routerem, když tato hodnota dosáhne 0, paket je odhozen a router pošle zdrojové adrese ICMP „Time Exceeded“ zprávu
   * **Header checksum** – detekuje korupci záhlaví
   * **Source IPv4 address** – zdrojová adresa
   * **Destination IPv4 address** – cílová adresa
2. V záhlaví paketu IPv6 se nachází tyto informace:
   * Traffic Class – ekvivalent DS
   * Flow Label – se všemi pakety se stejnou flow label je zacházeno stejně
   * Payload Length – obsahuje informace o velikosti dat v paketu bez velikosti záhlaví
   * Next Header – ekvivalent pole Protocol
   * Hop Limit – ekvivalent pole TTL, pro pole checksum není potřeba jelikož jeho funkce je vykonávána na vyšších i nižších vrstvách, takže nepotřebuje být kontrolováno při každém snížení TTL
   * Source IPv6 address
   * Destination IPv6 address

Po vytvoření jsou pakety směrovány pomocí různých protokolů. Pakety jsou směrovány pomocí informací v záhlaví. V cíli jsou pakety seřazeny do správného pořadí za použití sequence number a následně jsou sestaveny do původní podoby.

**Routing**

* Proces volby dalšího směru v cestě paketu k cílové síti
  + Výpočet optimální cesty k cíli (routovací tabulka)
  + Výběr optimální cesty pro odesílání paketů podle údajů v routovací tabulce
  + Zapozdření paketu a odeslání paketu na výstupní rozhraní
  + Routovací tabulka je soubor uložený v RAM
    - Obsahuje informace o známých sítí
  + O tom, kam bude paket odeslán se rozhoduje porovnáváním cílové Ip adresy z hlavičky paketu se záznamy v routovací tabulce
  + Po tom, co na router přijde paket:
    - Vezme si z paketu vypočtenou cílovou síť + routovací tabulku
    - Provede logický AND obou hodnot
      * Pokud výsledkem je shodná cílová síť se sítí z routovací tabulky
        + Pošle to na tu routu
    - Pokud nenajde žádný výsledek, pošle paket default gatewayi
    - Pokud nemá default gateway, **paket zahodí**





**IP paket**

IP protokol přidá k datům z vyšší vrstvy hlavičku s potřebnými informacemi pro doručení paketu přes mnoho sítí k cíli

**IPv4 paket**

* Minimální velikost je 20 B
* Maximální velikost 65535 B
* Fragmentace paketů
  + IPv4 pakety mohou být na routrech fragmentovány
  + K nutnosti fragmentace může dojít na routrech, které spojují linkové segmenty, které používají na linkové vrstvě různé protokoly → při předání z většího rámce (FDDI) do menšího rámce (Ethernet)
* Typy:
  + Unicast — Pro jeden uzel
  + Multicast — Pro jeden typ uzlů, např. OSPF routery
  + Broadcast — Poslední IP v subnetu — pro všechny uzly (v lokální síti)

<aside> 💡 Přidat APIPA adresy

</aside>

**IPv6 paket**

* Jednoduší narozdíl od IPv4 hlavičky
* Může mít více různých hlaviček, bez možnosti rozšíření
* Povinná hlavičká má 40 B (base header)
* Rozšiřující hlavičky jsou nepovinné (extension headers)
* Nemá kontrolní součet (jelikož prakticky již ji dělá linková vrstva — Ethernet)
* Minimální velikost je 1280 B
* Version — Verze protokolu (zde 6)
* Traffic class — Nastavení priority
* Flow label — značka toku, označující příslušnost datagramu do určitého toku, tok => proud datagramů se společnými vlastnostmi (odesílatel, adresát, cesta)
* Payload length — Počet bajtů následujících za standardní hlavičkou
  + Započítává rozšiřující hlavičky
  + Maximální délka je 64 KB
  + Pro větší datagramy se používá rozšiřující hlavička pro **JUMBO OBSAH (4000 MB max)**
  + Next Header — Identifikace dalšího obsahu
    - Jaká je následující rozšiřující hlavička
    - Nebo jaký je zapozdřený protokol
  + Hop Limit — TTL, ale IPv6

S porovnáním s IPv4 paketem chybí:

* Kontrolní součet
* Fragmentace
* Rozšířující volby

Typy IPv6 adres:

* Unicast
* Multicast
* Anycast
* Vícero serverů může mít stejnou IPv6 - IPv6 enabled routery ho doručí k nejblížší

**Link-local adresy**

* **fe80::/10**
* První adresa, kterou si uzel s IPv6 nastaví samo
  + Vezme prefix
  + Vygeneruje identifikátor
    - Vícero možností, EUI 64, Random, atd.
* Super handy, zajistí nám IPv6 komunikaci v síti bez jakékoliv konfigurace
* Ke komunikaci se využívají multicast adresy, např. na RS, RA, atd.
  + RS = **Router Solicitation**
    - Snaží se najít IPv6 default gateway
  + RA = **Router Advertisment**
    - Odpověď na RS
    - “Hej zmrde, mojí adresu můžeš použít pokud se chceš dostat do jiných sít”
  + NS = **Neighbor Solicitation**
    - Zjišťování souseda
    - Zjišťování zda soused je stále up
    - Využíváno v DAD
  + NA = **Neighbor Advertisement**
    - Odpověď na NS
    - NA je zaslán taky, když si uzel změní link-local adresu