#### 27. IP adresa a způsoby řešení nedostatku IP adres

**složení, syntaxe zápisu (IPv4, IPv6), rozdělení do tříd**

• **způsob zápisu –**

IPv4 = čtyři desítková čísla -> např. 192.168.48.36, IPv6 = osm skupin po čtyřech [hexadecimálních](https://cs.wikipedia.org/wiki/%C5%A0estn%C3%A1ctkov%C3%A1_soustava) číslicích, např. 2001: 0718: 1c01: 0016: 0214: 22ff: fec9: 0ca5

**• třídy IPv4 adres –**

A (10.0.0.0 až 10.255.255.255),

B (172.16.0.0 až 172.31.255.255),   
C (192.168.0.0 až 192.168.255.255),

100.64.0.0/10 - IPv4 Prefix for Shared Address Space podle specifikace [RFC 6598](https://tools.ietf.org/html/rfc6598)

**• max. hodnoty jednotlivých čísel u IPv4 + důvod**

**• zkracování zápisu IPv6 adres –**

Klasický tvar: 2001: 0718: 1c01: 0016: 0214: 22ff: fec9: 0ca5

Úvodní nuly v každé skupině lze ze zápisu vynechat. Výše uvedenou adresu tedy lze psát ve tvaru: 2001: 718: 1c01: 16: 0214: 22ff: fec9: ca5

**rozdíly mezi IPv4 a IPv6**

**• délka adresy –**

IPv4 = čtyři desítková čísla

IPv6 = osm skupin po čtyřech [hexadecimálních](https://cs.wikipedia.org/wiki/%C5%A0estn%C3%A1ctkov%C3%A1_soustava) číslicích

**• velikosti adresního prostoru u IPv4 a IPv6**

IPv4 = 232

IPv6 = 2128

**• min. přidělovaná velikost IPv6 sítě**

Minimální délka prefixu je 64

**• broadcast a multicast na IPv4 a IPv6**

IPv4 broadcast – broadcast adresa se získává z masky sítě. Změnou všech nul v masce sítě na jedničku dostaneme broadcast adresu.

IPv6 broadcast – Ipv6 nepoužívá metodu broadcast. Místo toho využívá Multicast.

IPv4 multicast – pro multicast je rezervováno místo s tímto rozsahem:   
232.0.0.0-232.255.255.255

IPv6 multicast – používá se pro optimalizaci dodatkových služeb, přenosu zařízení, bezpečnost a konfiguraci

**• veřejné, privátní a link-local adresy**

Privátní adresy se používají pro adresování vnitřních (lokálních) sítí.

IPv4 – používá 24bitové, 20bitové a 16bitové bloky pro jejich udělení

IPv6 – používá náhodné 40bitové číslo v prefixu -> předchází tím kolizím.

Veřejné adresy využívají ostatní bloky pro jejich adresaci.

**• ARP a NDP**

Protokol ARP je používán protokolem IPv4 k vyhledání fyzické adresy (například adresy MAC nebo adresy linky) přidružené k adrese IPv4.

IPv6 vkládá tyto funkce do samotného protokolu IP jako součást algoritmu automatické bezstavové konfigurace a zjišťování sousedních uzlů pomocí protokolu ICMPv6 (Internet Control Message Protocol, verze 6). Něco jako ARP6 proto neexistuje.

**způsoby získání adresy (DHCP, RA)**

**• DHCP**

IPv4 - Tento protokol se používá k dynamickému získávání adres IP a jiných informací o konfiguraci. IBM i podporuje server DHCP pro IPv4.

IPv6 - Implementace IBM i protokolu DHCP nepodporuje IPv6. Je však možné použít implementaci [serveru ISC DHCP](https://www.ibm.com/support/knowledgecenter/cs/ssw_ibm_i_72/rzakg/rzakguseiscdhcp4.htm?view=kc).

**◦ základní předávané parametry**

Používá sadu protokolů TCP/IP

**◦ identifikace koncového zařízení**

K ověřování dochází pomocí vlastní části síťové a cílové IP adresy.

**◦ komunikace s DHCP serverem (vrstva, cílové adresy)**

Aplikační vrstva, prezentační vrstva, relační vrstva, transportní vrstva, síťová vrstva, linková vrstva, fyzická vrstva,

**◦ obnova IP adresy**

- Klient dostane tzv. DHCPACK kdy může používat ip adresu a její zbylá nastavení. Pokud jí v době zapůjčení neobnoví musí ji přestat používat.

**◦ příklad DHCP serveru**

**◦ dynamická a statická alokace**

Statická:

DHCP server obsahuje seznam [MAC adres](https://cs.wikipedia.org/wiki/MAC_adresa) a k nim příslušným IP adres. Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu.

Dynamická:

Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány stanicím, které nejsou registrovány. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu.

**• SLAAC (RA)**

Host v IPv6 může být konfigurován automaticky, pokud je připojen na směrovanou IPv6 síť, za použití zpráv směrem k [ICMP](https://cs.wikipedia.org/wiki/ICMP) v6 směrovači. Při prvním připojení k síti host vyšle 'router solicitation' [multicast](https://cs.wikipedia.org/wiki/IP_multicast" \o "IP multicast) žádost o konfigurační parametry na místní linku. Odpovídajícím způsobem nastavený ICMPv6 směrovač odpoví na tuto žádost paketem 'router advertisement', který obsahuje konfigurační parametry síťové vrstvy.[[10]](https://cs.wikipedia.org/wiki/IPv6#cite_note-rfc2462-10) Pokud není IPv6 autokonfigurace použitelná, host může využít stavové konfigurace ([DHCPv6](https://cs.wikipedia.org/wiki/DHCPv6)) nebo být nastaven ručně či jiným způsobem.

SLAAC počítá s 64bitovým prefixem sítě, pro jinou velikost síťového prefixu není chování implementací IPv6 definováno.

**◦ předávané parametry**

[DNS](https://cs.wikipedia.org/wiki/Domain_Name_System) – systém doménových jmen

[DHCP](https://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) – dynamické přidělování síťových informací jako například: výchozí brána, maska sítě, IP adresa

[FTP](https://cs.wikipedia.org/wiki/File_Transfer_Protocol) – přenos souborů po síti

[TFTP](https://cs.wikipedia.org/wiki/Trivial_File_Transfer_Protocol) - jednoduchý protokol pro přenos souborů

[HTTP](https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol) – přenos hypertextových dokumentů ([WWW](https://cs.wikipedia.org/wiki/World_Wide_Web))

[WebDAV](https://cs.wikipedia.org/wiki/WebDAV) – rozšíření HTTP o práci se soubory

[IMAP](https://cs.wikipedia.org/wiki/Internet_Message_Access_Protocol) (Internet Message Access Protocol) umožňuje manipulovat s jednotlivými [e-mail](https://cs.wikipedia.org/wiki/E-mail) zprávami na poštovním serveru.

[IRC](https://cs.wikipedia.org/wiki/IRC) (Internet Relay Chat) – jednoduchý chat po internetu.

[NNTP](https://cs.wikipedia.org/wiki/NNTP) (Network News Transfer Protocol) umožňuje číst a umísťovat do sítě zprávy typu news.

[NFS](https://cs.wikipedia.org/wiki/Network_File_System) (Network File System) – síťový systém souborů, který umožňuje transparentní sdílení vzdálených souborů jakoby byly lokální.

[NTLM](https://cs.wikipedia.org/wiki/NTLM) Autentizační protokol Windows

[NTP](https://cs.wikipedia.org/wiki/Network_Time_Protocol) – synchronizace času (šíření přesného času)

[POP3](https://cs.wikipedia.org/wiki/Post_Office_Protocol) (Post Office Protocol) – protokol pro získání pošty z poštovního serveru.

[SMB](https://cs.wikipedia.org/wiki/Server_Message_Block) (Server Message Block) - [sdílení souborů a tiskáren](https://cs.wikipedia.org/wiki/Sd%C3%ADlen%C3%BD_prost%C5%99edek) v sítích Windows

[SMTP](https://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) – zasílání elektronické pošty

[SNMP](https://cs.wikipedia.org/wiki/Simple_Network_Management_Protocol) Simple Network Management Protokol je určen pro správu [síťových uzlů](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_uzel).

[Telnet](https://cs.wikipedia.org/wiki/Telnet) – protokol virtuálního terminálu.

[SSH](https://cs.wikipedia.org/wiki/Secure_Shell) – bezpečný shell

[X11](https://cs.wikipedia.org/wiki/X11) – zobrazování oken grafických programů v Unixových systémech

[XMPP](https://cs.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol) – rozšiřitelný protokol pro zasílání zpráv a sledování přítomnosti (protokol [Jabber](https://cs.wikipedia.org/wiki/Jabber" \o "Jabber))

**◦ předávání adres DNS serverů**

1. Uživatel zadal do svého [WWW klienta](https://cs.wikipedia.org/wiki/Webov%C3%BD_prohl%C3%AD%C5%BEe%C4%8D) doménové jméno www.wikipedia.org. Resolver v počítači se obrátil na lokální DNS server s dotazem na IP adresu pro www.wikipedia.org.
2. Lokální DNS server tuto informaci nezná. Má však k dispozici adresy kořenových serverů. Na jeden z nich se obrátí (řekněme na 193.0.14.129) a dotaz mu přepošle.
3. Kořenový server také nezná odpověď. Ví však, že existuje doména nejvyšší úrovně org a jaké jsou její autoritativní servery, jejichž adresy tazateli poskytne.
4. Lokální server jeden z nich vybere (řekněme, že zvolí tld1.ultradns.net s IP adresou 204.74.112.1) a pošle mu dotaz na IP adresu ke jménu www.wikipedia.org.
5. Oslovený server informaci opět nezná, ale poskytne IP adresy autoritativních serverů pro doménu wikipedia.org. Jsou to ns0.wikimedia.org (207.142.131.207), ns1.wikimedia.org (211.115.107.190) a ns2.wikimedia.org (145.97.39.158).
6. Lokální server opět jeden z nich vybere a pošle mu dotaz na IP adresu ke jménu www.wikipedia.org.
7. Jelikož toto jméno se již nachází v doméně wikipedia.org, dostane od jejího serveru nepochybně autoritativní odpověď, že hledaná IP adresa zní 145.97.39.155
8. Lokální DNS server tuto odpověď předá uživatelskému počítači, který se na ni ptal. 666

**◦ komunikace routeru s koncovými zařízeními a opačně (vrstva, cílové adresy)**

Routování probíhá pomocí referenčního modelu ISO/OSI

Cílové adresy se zde překládají pomocí techniky NAT

**• DHCPv6**

DHCPv6 je [síťový protokol](https://cs.wikipedia.org/wiki/TCP/IP), který umožňuje počítačům získat [IPv6 adresu](https://cs.wikipedia.org/wiki/IP_adresa#Adresy_v_IPv6), případně jiné parametry sítě jako adresy [DNS](https://cs.wikipedia.org/wiki/DNS) serverů. Princip je podobný [DHCP](https://cs.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol), existuje ale několik zásadních rozdílů, např. DHCPv6:

* umí spravovat více IP adres pro jedno rozhraní
* je jednodušší, protože klient využívá automatické konfigurace [lokální linkové](https://cs.wikipedia.org/wiki/IPv6#Adresy_m%C3%ADstn%C3%AD_linky) IPv6 adresy
* klient posílá zprávy na [skupinové adresy](https://cs.wikipedia.org/wiki/IP_multicast), nikoliv [všesměrovým vysíláním](https://cs.wikipedia.org/wiki/Broadcast)
* klient je identifikován prostřednictvím jedinečného identifikátoru DUID (DHCP unique identifier)
* zprávy pro počáteční přidělení adresy se jmenují: Solicit, Advertise, Request, Reply
* nedokáže poskytnout informaci o [výchozí bráně](https://cs.wikipedia.org/wiki/Implicitn%C3%AD_br%C3%A1na) (default route, default gateway) – tu klient obdrží pomocí oznámení směrovače (Router Advertisment).

**◦ předávané parametry**

**◦ identifikace koncového zařízení**

K ověřování dochází pomocí vlastní části síťové a cílové IP adresy.

**◦ spolupráce s RA**

**• statická konfigurace IP adres**

neboli pevná IP adresa. Pevnou IP adresu můžeme od poskytovatele připojení získat většinou za příplatek, ale dostáváme tím garanci, že IP adresa koncového zařízení, které se připojuje do internetu zůstane stále stejná.

**základní údaje nutné pro směrování, maska a její použití**

**• určení adresy sítě a broadcastu (IPv4)**

broadcast adresa se získává z masky sítě. Změnou všech nul v masce sítě na jedničku dostaneme broadcast adresu.

**• vliv masky, resp. délky prefixu na velikost sítě**

**• rozpoznání rozdílných sítí**

**řešení nedostatku IPv4 adres (CIDR, subnetting, privátní adresy, NAT,**

**proxy)**

**• CIDR**

Classless Inter-Domain Routing (CIDR, tj. „beztřídní směrování“) je v [počítačových sítích](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) metoda směrování, která v roce [1993](https://cs.wikipedia.org/wiki/1993) umožnila v [IPv4](https://cs.wikipedia.org/wiki/IPv4) používat jemnější dělení větších sítí na [podsítě](https://cs.wikipedia.org/wiki/Pods%C3%AD%C5%A5) tím, že [maska sítě](https://cs.wikipedia.org/wiki/Maska_s%C3%ADt%C4%9B) byla určena počtem [bitů](https://cs.wikipedia.org/wiki/Bit) a nikoliv příslušností IP adresy ke [třídě IP adres](https://cs.wikipedia.org/wiki/T%C5%99%C3%ADdy_IP_adres). CIDR byl zaveden [IETF](https://cs.wikipedia.org/wiki/Internet_Engineering_Task_Force) a jeho cílem bylo zpomalit [vyčerpání IPv4 adres](https://cs.wikipedia.org/wiki/Vy%C4%8Derp%C3%A1n%C3%AD_IPv4_adres) a též omezit růst [směrovacích tabulek](https://cs.wikipedia.org/wiki/Sm%C4%9Brovac%C3%AD_tabulka) na [směrovačích](https://cs.wikipedia.org/wiki/Router) v [Internetu](https://cs.wikipedia.org/wiki/Internet).

**◦ důvod zavedení**

Před zavedením CIDR byly adresy rozděleny do [tříd](https://cs.wikipedia.org/wiki/T%C5%99%C3%ADdy_IP_adres) a koncovým sítím připojeným k Internetu se v závislosti na jejich velikosti přidělovala adresa sítě třídy A, B nebo C. To způsobovalo dva problémy, jejichž závažnost postupně narůstala:

* Špatnou efektivitu využití adresního prostoru a v jejím důsledku rychle ubývající zásobu volných adres. Jako první začaly docházet adresy třídy B, protože sítí příliš velkých pro třídu C (256 místních adres) bylo mnoho a adres třídy B jen 16 tisíc (16384).
* Velké směrovací tabulky. Adresy sítí se přidělovaly tak, jak byly postupně vyžadovány, bez respektování jejich geografické či jiné souvstažnosti. To znamenalo, že v páteřních částech Internetu musely [směrovače](https://cs.wikipedia.org/wiki/Sm%C4%9Brova%C4%8D) uchovávat ve svých směrovacích tabulkách pro každou koncovou síť samostatný záznam. Tím směrovací tabulky nabývaly značné velikosti, takže jejich procházení bylo pomalé a mohlo nastat až vyčerpání dostupné kapacity operační paměti směrovačů.

**◦ způsob použití**

Zavedením CIDR bylo možné určit masku na hranici jednotlivých bitů IP adresy, místo po výše zmíněných osmicích bitů (resp. po jednotlivých [bajtech](https://cs.wikipedia.org/wiki/Bajt)).

**• dělení sítě na podsítě (subnetting)**

Podsíť ([anglicky](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina) subnet, subnetwork) je v [informatice](https://cs.wikipedia.org/wiki/Informatika) označení pro samostatnou část [počítačové sítě](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5). Označením podsíť je obvykle míněna konkrétní (menší) vyčleněná část větší [IP sítě](https://cs.wikipedia.org/wiki/TCP/IP). Pro určení rozsahu [IP adres](https://cs.wikipedia.org/wiki/IP_adresa) v dané podsíti slouží [maska sítě](https://cs.wikipedia.org/wiki/Maska_s%C3%ADt%C4%9B).

**◦ způsob rozdělení**

[Počítače](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D), které jsou umístěny v jedné síti (resp. podsíti), mají ve svých [IP adresách](https://cs.wikipedia.org/wiki/IP_adresa) shodné nejvýznamnější bity této IP adresy. Tím je IP adresa rozdělena na dvě části, které označujeme jako „číslo sítě“ a „číslo počítače“. Místo označení „číslo počítače“ by mělo být uvedeno „číslo síťového rozhraní“, protože některé počítače mohou mít více [síťových karet](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A1_karta) a tím i více síťových rozhraní s více IP adresami.

Velikost významnější části IP adresy (tj. velikost části, která vyjadřuje „číslo sítě“) je definována pomocí [CIDR](https://cs.wikipedia.org/wiki/Classless_Inter-Domain_Routing) notace počtem bitů zleva (tzv. prefix) nebo pomocí [masky sítě](https://cs.wikipedia.org/wiki/Maska_s%C3%ADt%C4%9B).

**◦ VLSM**

VLSM umožňuje síťovým inženýrům rozdělit prostor adres IP do hierarchie podsítí různých velikostí, což umožňuje vytvářet podsítě s velmi odlišnými počty hostitelů, aniž by došlo ke ztrátě velkého počtu adres.

**• privátní adresy**

Privátní adresy se používají pro adresování vnitřních (lokálních) sítí.

IPv4 – používá 24bitové, 20bitové a 16bitové bloky pro jejich udělení

**◦ důvod použití a vlastnosti**

Privátní adresy se používají pro adresování vnitřních (lokálních) sítí.

**◦ příklady privátních rozsahů**

* ve třídě A: 10.0.0.0 až 10.255.255.255 (celkem 1× 16 777 216 adres; tj. 16 777 216 adres, z nichž je použitelných jen 16 777 214)
* ve třídě B: 172.16.0.0 až 172.31.255.255 (celkem 16× 65 536 adres; tj. 1 048 576 adres, z nichž je použitelných jen 1 048 544)
* ve třídě C: 192.168.0.0 až 192.168.255.255 (celkem 256× 256 adres; tj. 65 536 adres, z nichž je použitelných jen 65 024)

**• NAT**

**◦ účel použití, princip, vrstva**

NAT se většinou používá pro přístup více počítačů z [lokální sítě](https://cs.wikipedia.org/wiki/Local_Area_Network) do [Internetu](https://cs.wikipedia.org/wiki/Internet) prostřednictvím jediné veřejné IP adresy (viz [gateway](https://cs.wikipedia.org/wiki/Gateway" \o "Gateway)).

**◦ omezení komunikace do vnitřní sítě**

 NAT však znemožňuje přímou komunikaci mezi klienty ([end–to–end spojení](https://cs.wikipedia.org/wiki/Princip_konec-konec)) a může snížit rychlost přenosu.

**◦ přesměrování portů**

Pro obcházení problémů, které NAT způsobuje, jsou k dispozici různé techniky umožňující (přímou) komunikaci mezi zařízeními za NAT – viz [NAT traversal](https://cs.wikipedia.org/wiki/NAT_traversal)[[16]](https://cs.wikipedia.org/wiki/Network_address_translation#cite_note-16) nebo [Hole punching](https://cs.wikipedia.org/wiki/Hole_punching). Protokol [UPnP](https://cs.wikipedia.org/wiki/UPnP" \o "UPnP) ([anglicky](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina) Universal Plug and Play) umožňuje automatickou konfiguraci přesměrování portů na routeru, avšak vyžaduje vysokou úroveň důvěry mezi ovládající stanicí a routerem, což například v případě [Carrier-grade NAT](https://cs.wikipedia.org/wiki/Carrier-grade_NAT" \o "Carrier-grade NAT) není možné.

**• proxy**

**◦ účel použití, princip, vrstva**

Proxy server funguje jako prostředník mezi [klientem](https://cs.wikipedia.org/wiki/Klient_(po%C4%8D%C3%ADta%C4%8De)) a cílovým [počítačem](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D) ([serverem](https://cs.wikipedia.org/wiki/Server)), překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient. Přijatou odpověď následně odesílá zpět na klienta. Může se jednat jak o specializovaný [hardware](https://cs.wikipedia.org/wiki/Hardware), tak o [software](https://cs.wikipedia.org/wiki/Software) provozovaný na běžném [počítači](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D). Proxy server odděluje [lokální počítačovou síť](https://cs.wikipedia.org/wiki/Local_Area_Network) ([intranet](https://cs.wikipedia.org/wiki/Intranet)) od [Internetu](https://cs.wikipedia.org/wiki/Internet).

Linková vrstva

**◦ porovnání s NAT**

NAT-device změní adresu počítače, který vysílá paket do Internetu, aby vaše (nebo registrovány v nastavení), aniž by se změnila strukturu dotazu a poté, co obdrží balíček z online serveru, který ji doručí na místo určení i nezměněné

proxy- Server obdrží žádost od počítače, který vysílá paket do Internetu, předá jej on-line serveru prostřednictvím zavedené IP adresy, a poté, co obdrží balíček, dodává, že na místo určení bez úprav nebo opraveny filtrem (je-li to nutné - zkontrolujte antivirový modul) Technologie nevyžaduje předpis dalších síťových nastavení na jednotlivých počítačích v síti LAN

**◦ reverzní proxy**

Reverzní proxy je proxy server, který se zobrazí klientům jako obyčejný server. Žádosti jsou přesměrovány na jeden nebo více serverů, které je zpracují. Odpovědi jsou navráceny, jakoby přišly přímo z webového serveru.

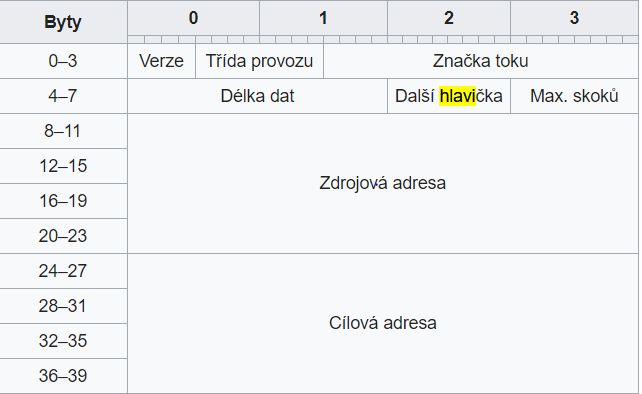
**IP datagram (hlavička, TTL...) , fragmentace**

**• popis základních částí IPv4 a IPv6 hlavičky, velikost hlavičky**

IPv4 - Datagram IPv4 obsahuje hlavičku se služebními údaji nutnými pro přepravu a za ní následují data. Konec hlavičky je zarovnán na násobek čtveřice bajtů pomocí výplně ([anglicky](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina) padding). Strukturu IP datagramu vystihuje tabulka uvedená nahoře.

délka hlavičky jako počet 32bitových slov (pro získání délky v bajtech je potřeba vynásobit čtyřmi, tzn. typická a minimální délka (0x5 × 4) = 20 bajtů, a maximální (0xF ×\* 4) = 60 bajtů.

IPv6 –



**◦ verze**

Verze protokolu, zde 6.

**◦ adresy**

Adresa odesílatele, cílová adresa

**◦ TTL, hop limit**

Životnost datagramu. Stejně jako u TTL v IPv4 zde každý směrovač zmenší hodnotu o jedničku a dojde-li do nuly, datagram zahodí.

**◦ délka**

Délka datagramu, ovšem nepočítá se do ní úvodní 20B hlavička.

**◦ protokol, next header**

Rozšiřující prvky jsou v IPv6 přesunuty do rozšiřujících hlaviček, které se v případě potřeby připojují za základní hlavičku. Jsou zřetězeny položkami Další hlavička, které vždy identifikují typ následující hlavičky. Poslední hlavička pak v této položce nese informaci o protokolu vyšší vrstvy, kterému mají být data předána při doručení. Pokud tedy datagram žádné rozšiřující hlavičky nemá, hned základní hlavička v této položce stanoví protokol vyšší vrstvy.

**• fragmentace**

**◦ důvod**

IP datagram je rozdělen na menší části, aby mohly být přeneseny další části počítačové sítě

**◦ parametr fragment offset**

pozice fragmentu v originálním paketu (počet osmic bytů dat od počátku původního datagramu k počátku tohoto fragmentu)