10. Protokoly síťové vrstvy – IPv4, IPv6, ICMP, IGMP.

POČÍTAČOVÉ SÍTĚ A PROGRAMOVÁNÍ

IPv4

- Internet Protokol verze 4
- Datově orientovaný protokol používaný v sítích s přepojováním paketů (např. Ethernet).
- Pracuje nad různými technologiemi díky abstrakci pomocí enkapsulace.
- Je bezestavový, nespojovaný (před odesláním nesestavuje cestu).
- Nezaručuje doručení, zachování pořadí ani vyloučení duplicity.
- Pakety putují v síti nezávisle.
- Tyto záruky jsou ponechány na vyšší vrstvě, kterou představuje protokol TCP.
- Z toho plyne nižší režie → vyšší rychlost.
- Kontrola integrity také na vyšší vrstvě, IPv4 obsahuje pouze kontrolní součet hlavičky datagramu se služebními údaji.
- Teoreticky poskytuje adresní prostor 2^{32} (4 294 967 296), prakticky však méně, protože jsou adresy sdružovány, kvůli snadnějšímu směrování do podsítí (masky sítě).
- Všechny bloky jsou již vyčerpány tzn. Všechny IP adresy již někdo vlastní.
- Formát IPv4 adresy je xxx.xxx.xxx.xxx
    - „xxx“ je v rozmezí 0-255

Hlavička IPv4 paketu

bits	0-3	4-7	8-15	16-18	19-31
0	4	header length	Type of Service	total length (header + data)	
32	identification			flags	fragment offset
64	TTL		protocol	header checksum	
96	source IP				
128	destination IP				
160	options (if any)				
160/192+	DATA				

- **Verze:** verze protokolu („4“ v obrázku)
- **IHL:** délka hlavičky udávaná v počtu 32bitových čísel
- **TOS:** typ služby, mělo umožňovat odesílateli nastavit parametry preferované cesty (požadavek nejnižšího zpoždění, největší šířka pásma, …), v praxi nevyužito
- **Celková délka:** délka datagramu v bajtech
- **Identifikace:** využívá se při fragmentaci
- **Příznaky:** slouží pro řízení fragmentace. První je vždy nulový, druhý je Don’t fragment zakazující tento datagram fragmentovat, a třetí More fragments nastavuje, zdali není fragmentem posledním.
- **TTL:** ochrana proti zacyklení
- **Protokol:** určuje, kterému protokolu vyšší vrstvy se mají data předat při doručení.
- **Kontrolní součet hlavičky:** slouží k ověření, zda nedošlo k poškození. Počítá se pouze z hlavičky a pokud nesouhlasí, datagram bude zahozen.

- **Volby:** různé rozšiřující informace či požadavky. Například lze předepsat sérii adres, kterými má datagram projít. Volby obvykle nejsou v datagramu použity.

IP adresy

- Dělíme je do tříd (A-E)
    - Třída E slouží pro experimentální účely
    - Existují rezervované IP adresy:

třída	rozsah	minimální adresa	maximální adresa	maska rozsahu [10]	maska rozsahu [prefix]
A	10	10.0.0.0	10.255.255.255	255.0.0.0	/8
B	172.16 až 32	172.16.0.0	172.31.255.255	255.240.0.0	/12
C	192.168	192.168.0.0	192.168.255.255	255.255.0.0	/16
D	nic	–	–	–	–
E	nic	–	–	–	–

IPv6

- Internet Protokol verze 6
- Nástupce IPv4
- Hlavní plus oproti IPv4 je masivně větší adresní prostor 2^{128}
- Formát IPv6 adresy je xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
- X je z rozsahu hexadecimálních znaků (0-9, A-F)
- Nuly mohou být vynechány nebo nahrazeny dvěma dvojtečkami
- V případech, kdy síť LAN a WAN není na IPv6 připravena je možno využít tzv. Mechanismů přechodu založených na enkapsulaci IPv6 packetů do IPv4.
- Na rozdíl od IPv4 nemá v hlavičce vůbec kontrolní součet, protože chybovost je nízká a v nejhorším případě dojde k zaslání packetu na špatný počítač.
- Používá end-to-end fragmentaci na rozdíl od IPv4, u které velké datagramy fragmentoval router.
- Poskytuje ověřování a šifrování.

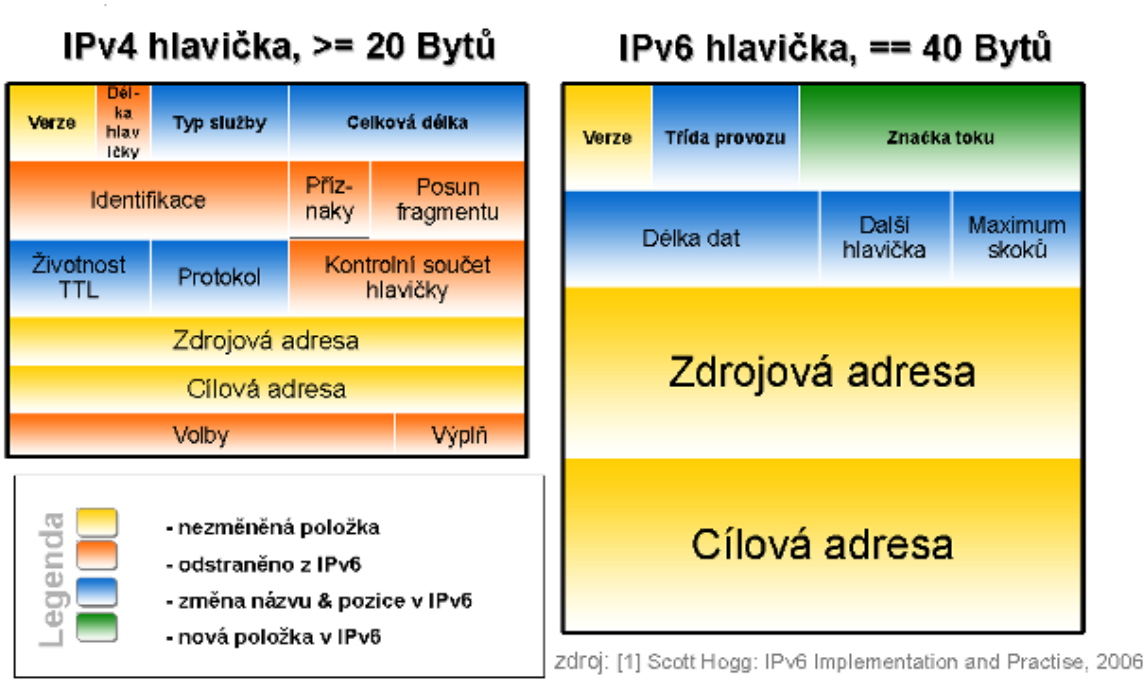
Hlavička IPv6 paketu

Hlavička IPv6[30]

Byty	0	1	2	3
0–3	Verze	Třída provozu	Značka toku	
4–7	Délka dat		Další hlavička	Max. skoků
8–11	Zdrojová adresa			
12–15				
16–19				
20–23				
24–27	Cílová adresa			
28–31				
32–35				
36–39				

- **Verze:** 4 bity, verze 6
- **Třída provozu**: 8 bitů na prioritu paketu. Úroveň priority se dělí na rozsahy: kde zdroj podporuje kontrolu přetížení a bez podpory kontroly přetížení.
- **Značka toku**: 20 bitů pro správu QoS. Původně určeno pro speciální obsluhu aplikací reálného času, nyní se nepoužívá.
- **Délka dat**: 16 bitů pro délku těla paketu. Při vynulování se nastaví „jumbo“ tělo (skok za skokem)
- **Další hlavička**: 8 bitů, určuje další vnořený protokol. Hodnoty se shodují s hodnotami definovanými pro IPv4.
- **Zdrojová a cílová adresa**: 128 bitů na každou adresu.
- **Hop limit**: 8 bitů, číselně definuje počet povolených přechodů síťovými prvky. Každý přechod znamená snížení čísla o 1.

Srovnání IPv4 a IPv6



zdroj: [1] Scott Hogg: IPv6 Implementation and Practise, 2006

ICMP

- Internet Control Message Protocol
- Protokol používají opravné systémy v síti pro odeslání služebních informací, například chybových zpráv.
- ICMP od TCP a UDP se liší tím, že obvykle není používán přímo, ale je vygenerován na základě nějaké události. Výjimkou je nástroj ping, který posílá ICMP zprávu „Echo request“, který zjišťuje, za jakou dobu dostane odpověď.
- Existuje verze ICMPv4 a ICMPv6 pro IPv4 a IPv6.
- Každá ICMP zpráva je zapouzdřena v jednom IP datagramu, a tak ICMP nezaručuje doručení.
- Typické použití je třeba, když dostanete nějaký packet, kterému vypršel TTL, tak pošlete ICMP zprávu „Time to live exceeded in transit“ odesilateli packetu.

ICMP header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Type								Code								Checksum															
4	32	Rest of header																															

IGMP

- Internet Group Management Protocol
- Protokol, který rozšiřuje požadavky na implementaci protokolu IPv4 o podporu multicastu.
- multicast management se u IPv6 stará Multicast Listener Discovery.
- Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru lokální síti.
- Routery pracují ve dvou stavech:
- **Dotazovač:**
    - Zasílá dotazy na členství.
- **Poslouchač:**
    - Naslouchá a je neaktivní.
- Aby se stanice připojila do skupiny, musí zaslat IGMP zprávu „Membership report“ s IP adresou třídy D (multicast).
- Tato zpráva dorazí k lokálnímu routeru.
- K odhlášení použije „Leave groupe“.