Protokoly síťové vrstvy – IPv4,IPv6,ICMP,IGMP

IPv4

- Internet Protokol verze 4
- datově orientovaný protokol používáný v sítích s přepojováním paketů
- nezaručuje doručení, zachování pořadí ani vyloučení duplicity
    - tyto záruky jsou ponechány na vyšší vrstvě, kterou představuje protokol TCP
- 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), praktickyk však méně, protože jsou adresy sdružovány, kvůli snadnějšímu směrování do podsítí (maska sítě)
- všechny bloky jsou již vyčerpány tzn. všechny ip adresy již někdo vlastní

Formát IP datagramu

Bajty	0		1	2	3
Bajt 0 až 3	verze	IHL	typ služby	celková délka	
Bajt 4 až 7	identifikace			příznaky (3 bity)	offset fragmentu (13 bitů)
Bajt 8 až 11	TTL		číslo protokolu	kontrolní součet hlavičky	
Bajt 12 až 15	zdrojová adresa				
Bajt 16 až 19	cílová adresa				
Bajt 20 až ((IHL × 4) - 1)	rozšířená nepovinná nastavení				
...	data				

- Formát IPv4 adresy je xxx.xxx.xxx.xxx
    - "xxx" je v rozmezí 0-255

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

- narozdíl od ipv4 nemá v hlavičce vůbec kontrolní součet protože chybovost je nízká a v nejhorší případě dojde k zaslání packety na špatnému počítač
- používá end-to-end fragmentaci narozdil od IPv4, u které velké datagramy fragmentoval router
- poskytuje ověřování a šifrování

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																																

ICMP

- Internet Control Message Protocol
- protokol používají opračních 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. Výjmkou je nástroj ping, který posílá ICMP zprávy “Echo requst” který zjišťuje za jakou dobu dostane odpověď
- existuje verze ICMPv4 a ICMPv6 pro IPv4 a IPv6
- každá ICMP zpráva je zapozdřena v jednom ip datagramu, a tak ICMP nezaručuje doručení
- typické použití je třeba když dostanete nějakou packet kterému vypršel TTL tak pošlete ICMP zprávu „*Time to live exceeded in transit*“ odesílateli 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 protokoli IPv4 o podporu multicastu
    - o multicast management se u IPv6 stará Multicast Listener Discvery
- využívá se pro dynamické přihlašování a odhlašování ze skupinu u multicastového routeru lokální síti
- Routery pracují ve dvou stavech
    - dotazovač
        - zasílá dotazy na členství
    - polouchač
        - nashlouchá a je neaktivní
- aby se stanice připojila do skupiny musí zalsat IGMP zpráv “Membership report” s ip adresou třídy D. Tato zpráva dorazí k lokálnímu routeru
- K odhlášení použije “Leave group”