

PSI – BI-WSI-SI-17

Adresace IPv4, rozdělení adresního prostoru. Rozdíly mezi IPv4 a IPv6.

Obsah

1	Adresace	2
2	IPv4	2
2.1	Adresace pomocí IPv4	2
2.2	Struktura hlavičky IPv4	3
2.3	Fragmentace v IPv4	3
3	Služby spojené se síťovou vrstvou	3
4	IPv6	3
4.1	IPv4 vs IPv6	4

1 Adresace

Abychom mohli komunikovat mezi jednotlivými uzly v síti je nutné nějdříve každému uzlu přidělit nějakou adresu, díky které jej bude možné identifikovat. Každá síť má definovanou vlastní množinu adresu, která je disjunkt ní s ostatními sítěmi (lze tedy narazit na 2 sítě s totožnou adresací). V každé síti je poté potřeba rozdělit její adresní prostor případně celou síť navenek zapouzdřit jednou adresou (NAT) a tím vytvořit podsítě (víceúrovňové uspořádání).

2 IPv4

Hlavní význam IPv4 v počítačových sítích je adresace jednotlivých uzlů v síti. Díky této adresaci je poté možné předat data správnému adresátovi. IPv4 je 32 bitová adresa, která slouží k indentifikaci síťových zařízení na 3. úrovni modelu ISO-OSI (síťová vrstva). IPv4 je rozdělena do 4 oktetů (bytů), adresy se dají zapsat také dekadicky, kde každý oktet je od dalšího oddělen tečkou.

2.1 Adresace pomocí IPv4

Původní rozdělení IPv4 bylo pomocí tříd

- A, B, C - normální adresy (unicast)
- D - multicast
- E - rezervováno

Třída	Úvodní bity	síťových adres (bitů)	počet sítí	počet adres v síti	první adresa
A	0	8	128	2^{24}	0.0.0.0
B	10	16	16384	2^{16}	128.0.0.0
C	110	24	2097152	2^8	192.0.0.0
D	1110				224.0.0.0
E	1111				240.0.0.0

S tímto rozdělením adres přišel ovšem rychle problém jejich neefektivnosti, v některých případech bylo nutné jít o třídu víc i kvůli „pár adresám“. Tuto situaci ovšem pomohlo vyřešit schéma CIDR (Classless Inter-Domain Routing). Toto schéma dovoluje libovolnou délku síťového prefixu (narozdíl od IPv4 class). Velikost sítě je poté dána její maskou. Například pro síť o velikosti 2^{18} adres je její maska ve formátu 255.255.192.0 (CIDR formát - /18). Na posledních 18 bitech, které představují adresní prostor jsou v masce 0 a na ostatních se nachází 1.

V rámci privátních sítí je možné použít tyto volně dostupné adresní prostory. Tyto privátní adresy neroutují do internetu, ale slouží pro routování v rámci NAT. Toto bylo jedno z řešení problému s nedostatkem veřejných IP adres a také pomáhá izolovat privátní síť.

10.0.0.0/8	16777216 adres	1x class A
172.16.0.0/12	1048576 adres	16x class B
182.168.0.0/16	65537 adres	256x class C

2.2 Struktura hlavičky IPv4

- Version: 4 (IPv4)
- Header length: délka hlavičky v 32-bit slovech
- Type of Service: má různá využití, například pro QoS
- Total length: celková délka packetu v bytech
- Identification: identifikátor packetu (pro přiřazení fragmentů)
- Flags: příznaky, stavové flagy
- Fragment offset: relativní pozice fragmentu (jednotka: 8 bytů)
- Time to Live: prevence pro „nekonečný packet“, jedná se o počet průchodů skrz routery, snižuje se 1, pokud klesne na 0, packet se zahodí
- Protocol: typ protokolu vyšší vrstvy (ssh, telnet, smtp)
- Header checksum: kontrolní součet hlavičky (slouží ke kontrole integrity)
- Source address: zdrojová adresa
- Destination address: cílová adresa
- Options: nepovinné položky
- Padding: Zarovnání hlavičky na hranici 32 bitů

2.3 Fragmentace v IPv4

Paket nemůže být libovolně velký, je omezený délkou rámce (MTU - Maximum Transmission Unit), která je typicky 1500 bytů. Vyšší MTU redukuje overhead, nižší ovšem snižuje transportní zpoždění. Pokud je ovšem paket větší, než je MTU, je nutné jej rozdělit na části. O toto se postará síťová vrstva a každý router může fragmentovat (rozdělovat) IPv4 pakety. Pakety jsou poté doručeny nezávisle na sobě a jsou složeny až na cílovém zařízení.

3 Služby spojené se síťovou vrstvou

- ICMP (internet Control Message Protocol) Chybové zprávy sítě, které se odesílají původnímu odesílateli. Odesílá protokol č. 1 v IP headeru, typ a kód (oba jsou 4 bity). Například: 0 - echo reply (ping), 3 - nedosažitelná adresa, 11 - TTL expired
- ARP - Address resolution Protocol (RFC826) Jedná se o protokol linkové vrstvy (2. úroveň ISO-OSI). Jedná se o mapování mezi síťovou a hardwarovou adresou (IP a MAC). To pomáhá zrychlovat komunikaci vytvořením rezoluční tabulky, každému záznamu je také přiřazena automaticky expirace záznamu.

4 IPv6

Důvody k přechodu do nového adresového standardu je několik. V roce 2011 byly rozděleny poslední bloky IPv4 veřejných adres a již přidělené adresy nelze odebrat. Nový standard pro IP tedy musí mít větší adresní prostor, také jsou tu určité možnosti pro zautomatizování konfigurace (zbavení se DHCP) a lepší bezpečnosti. Toto vše by mělo řešit IPv6.

4.1 IPv4 vs IPv6

IPv6 má o 2^96 více adres než IPv4, stejně jako IPv4 používá hop limit, což je obdoba TTL. IPv6 má i rozdíly v hlavičce, nenachází se zde délka hlavičky, která je vždy stejná. Také zde není fragmentace ani options. Chybí zde i kontrolní součet, který je vypočítáván na každém routeru. Oproti IPv4 je zde nová položka: Flow label (20b) - jedná se identifikaci datového toku a slouží k usnadnění směrování, není zatím specifikováno. Hlavičku je možné rozšířit, za hlavičkou můžou následovat rozšiřující hlavičky, jejich pořadí je pevné.

V důsledku ztráty fragmentace na jednotlivých routerech, je nutné aby jí provedl již odesílatel. Pro IPv6 je minimální MTU 1280 bytů a pokud odesílatel odesílá větší balík, než je možné poslat je mu odeslána zpráva pomocí ICMP.