IPv4 adresace – třídní a beztřídní adresace (I. a II. epocha), speciální adresy, maska, číslo sítě/podsítě; IPv6 adresace – srovnání s IPv4

IP a IPv4 obecně

IP protokol je v architektuře TCP/IP protokol síťové vrstvy. Slouží k přenosu dat nespojovaným a nespolehlivým způsobem (mezi zdrojem a příjemcem). Protokol je implementován v koncových uzlech i ve směrovačích. V současnosti jsou paralelně používány dvě verze – IPv4 a novější IPv6.

IP adresa je číslo, které v síti jednoznačně identifikuje komunikující zařízení. Verze IPv4 je tvořena čtyřmi osmibitovými čísly oddělenými tečkou (celkem tedy má IPv4 adresa 32 bitů). Adresa může být zapsána v desítkové nebo ve dvojkové soustavě.

Tvar IPv4 adresy ve dvojkové soustavě: 11011100.11110000.11000010.10000001
Tvar IPv4 adresy v desítkové soustavě: 220.240.194.129

IPv4 adresa sestává z adresy sítě a z adresy uzlu.

Třídní adresace (I. epocha)

Původní návrh IPv4 předpokládal rozdělení adresy na síťovou a lokální část fixně – například by prvních osm bitů adresy určovalo síť, zbytek pak zařízení v síti. Sítí by mohlo při takovém dělení tedy být nejvýše 256 a v každé z nich by se pak mohlo nacházet přes 16 milionů stanic. Toto dělení se ukázalo jako nedostatečné (zejména po příchodu lokálních sítí) a proto se zavedlo dělení na třídy (I. epocha IP adresace).

Jednotlivé třídy adres se liší počtem bitů vyhrazených pro síťovou část adresy. Bylo tím umožněno přidělování adres podle potřeb dané organizace.

Přehled tříd

třída	bin. zač.	1. bajt	stand. maska	b. síť.	b. stan.	sítí	stanic v síti
A	0	0–127	255.0.0.0 prefix /8	8	24	2^7 = 128	2^{24}-2 = 16 777 214
B	10	128–191	255.255.0.0 prefix /16	16	16	2^{14} = 16 384	2^{16}-2 = 65 534
C	110	192–223	255.255.255.0 prefix /32	24	8	2^{21} = 2 097 152	2^8-2 = 254
D	1110	224–239	*multicast*				
E	1111	240–255	*vyhrazeno jako rezerva*				

Úspěšnému žadateli o adresu sítě se přidělovala vždy adresa sítě požadované třídy, takže pro sebe žadatel měl vždy celý adresní prostor v dané podsíti. Toto se nazývá *třídní (classful) mechanismus hospodaření s adresním prostorem*.

Třída A

Pro síťovou část je vyhrazený první bajt (resp. 7 bitů, první bit slouží k identifikaci, že jde o adresu třídy A – první bit má vždy hodnotu 0). Ve třídě může existovat až 2^7 velkých sítí, každá z nich může mít až 2^{24}-2 koncových uzlů. Maska sítě třída A je dekadicky 255.0.0.0 (tedy prefix /8).

0XXXXXXX.YYYYYYYY.YYYYYYYY.YYYYYYYY

Třída B

Pro síťovou část jsou vyhrazeny první dva bajty (resp. 14 bitů, první dva bity identifikují třídu adres B – vždy mají hodnotu 10). Ve třídě může existovat 2^{14} sítí a každá z nich může obsahovat až 2^{16}-2 koncových uzlů. Maska třídy B je dekadicky 255.255.0.0 (tedy prefix /16).

10XXXXXX.XXXXXXXX.YYYYYYYY.YYYYYYYY

Třída C

Pro síťovou část jsou vyhrazeny první tři bajty (resp. 21 bitů, první tři bity identifikují třídu adres C – vždy mají hodnotu 110). Pro adresování uzlů zbývá pak jediný bajt. Ve třídě může existovat až 2^{21}-2 sítí, každá z nich může mít maximálně 256 koncových uzlů.

110XXXXX.XXXXXXXX.XXXXXXXX.YYYYYYYY

Třída D

Používá se jako *multicast*. Její adresy začínají 1110. Multicast je skupinová adresa – identifikuje skupinu síťových zařízení v síti, jimž se má zpráva doručit.

Třída E

Adresy v třídě E jsou rezervou pro budoucí použití. Aktuálně se adresy z třídy E používají pro experimentální účely.

Vyhrazené adresy

Ne všechny z výše uvedených adres tříd A–C je možné použit pro identifikaci síťového rozhraní (zařízení). V každé třídě existuje vždy skupina tzv. *vyhrazených adres*, které mají speciální účel, pro adresaci nelze použít např. adresy tvořené samými nulami nebo samými jedničkami.

IP adresa tvořená v lokální síti samými jedničkami vyjadřuje *broadcastovou adresu* pro všesměrové vysílání v dané síti (vysílání je doručeno všem uzlům sítě).

Adresa tvořená samými nulami identifikuje pak síť jako celek.

Privátní adresy

Kromě vyhrazených adres je v každé třídě vyhrazena skupina tzv. *privátních adres*, které jsou používány k adresování uvnitř lokálních sítí (*neveřejné adresy*).

Ve třídě A jsou to adresy 10.0.0.0 až 10.255.255.255.
Ve třídě B jsou to adresy 172.16.0.0 až 172.31.255.255.
Ve třídě C jsou to adresy 192.168.0.0 až 192.168.255.255.

Adresa 127.x.x.x je pak vyhrazena pro localhost (*loopback*) – umožňuje posílat pakety sám sobě, používá se např. pro různé účely testování.

Beztřídní adresace (II. epocha)

Beztřídní doménové směrování (CIDR – Classless Inter-Domain Routing) bylo zavedeno v roce 1993 pro zvýšení úspornosti přidělování IP adres.

Počalo dělení sítí na podsítě (subnetting), příp. řazení sítí do nadsítí (supernetting). Tento způsob se používá dodnes.

Subnetting

Umožňuje rozdělit jednu síťovou adresu na více menších síťových adres. Používá se zejména v oddělených oblastech, ve kterých je potřeba lépe využít přidělený adresní prostor. Typicky toto řešení používají firmy, které mají několik menších oddělených sítí s relativně malým počtem uzlů v každé síti.

Taková firma pak místo více adres[1] třídy C má přidělenu jen jednu, se kterou si vystačí. Několik bitů z lokální části adresy je totiž použito pro adresaci podsítě.

Př.: Chceme-li rozdělit síť 86.87.88.0/24 na dvě podsítě, budeme pro adresaci podsítí potřebovat jeden bit z lokální části IP adresy (1 bit může mít dva stavy = dvě podsítě). Z posledního bajtu z IP adresy nám tedy zbude 7 bitů pro koncové stanice (maximum bude 2^7-2 stanic). První ze sítí bude mít adresu 86.87.88.0/25 (… .0000000) a druhá síť 86.87.88.128/25 (… .10000000).

Toto posunutí hranice mezi síťovou a lokální částí adresy definuje tzv. *maska sítě*.

Maska sítě

Označuje, kolik bitů z IP adresy značí síť a kolik bitů značí koncové zařízení. Má stejnou velikost i tvar jako IP adresa samotná.

Má-li maska tvar např. 11111111.00000000.00000000.00000000 (tj. 255.0.0.0), znamená to, že celý první bajt IP adresy představuje číslo sítě a zbylé tři bajty jsou použity pro značení koncových stanic.

Protože má maska tvar souvislého sledu logických 1 zleva následovaným souvislým sledem logických 0, používá se také zápis masky formou *prefixu*. Ve výše uvedeném případě by prefixem byl /8. U masky např. 11111111.11110000.00000000.00000000 (255.240.0.0) pak /12.

Číslo sítě/podsítě

Jde o adresu, která je používána směrovači ke směrování paketů. Zjednodušeně řečeno jde o IP adresu celé sítě/podsítě jako takové. Výše byla v příkladu subnettingu uvedena adresa (číslo) sítě 86.87.88.0 s maskou /24, která byla následně rozdělena na dvě podsítě. Čísla podsítí pak byla 86.87.88.0 s maskou /25 a 86.87.88.128 také s maskou /25.

Číslo sítě lze spočítat logickým součinem (AND) IP adresy a masky sítě (v binárním tvaru). Má-li stanice IP adresu 86.87.88.133 (binárně 01010110.01010111.01011000.10000101) a maskou sítě je /25 (dekadicky 255.255.255.128 → binárně pak 11111111.11111111.11111111.10000000) a proběhne

[1] než nastala II. epocha, uvažovalo se nad různými způsoby, jak IP adresy přidělovat – jednou z možností bylo přidělení několika menších sítí (např. třídy C) namísto jedné sítě třídy B, která by nebyla celá využita a IP adresami by se tak zbytečně plýtvalo

logický součin, dojdeme k závěru, že číslo sítě je 86.87.88.128 (jde opět o podsít zmiňovanou v části subnetting). Samotný logický součin je znázorněn na následujícím řádku:

IP stanice	01010110.01010111.01011000.10000101
Maska sítě	11111111.11111111.11111111.10000000
Logický součin	01010110.01010111.01011000.10000000
Číslo sítě dekadicky	86.87.88.128

IPv6 adresace – srovnání s IPv4

Nová verze protokolu, která počítá s větší velikostí síťové adresy. Odvrací problém vyčerpání IP adres. Kromě zvětšení velikosti řeší také další problémy, které se během doby fungování protokolu IP nashromáždily – zejména má minimalizovat zátěž směrovačů, minimalizovat plýtvání adresním prostorem a umožnit přenos multimediálních dat.

Cíle (požadavky) IPv6

a) **adresní prostor navždy** – zajistit dostatečný počet adres pro budoucí použití (předpokládá se, že v síti budou v budoucnu zapojena i jiná elektronická zařízení, např. lednička, pračka, televizor apod. – IoT)
b) **skupinová komunikace** – umožnit vysílání dat určité skupině adresátů, např. pro rádiové vysílání, konference apod.
c) **zefektivnit překlad IP adres na MAC adresy** – v IPv4 se používal protokol ARP, který používal všesměrové vysílání, IPv6 přichází s efektivnější metodou: *objevování sousedů*
d) **bezpečnost** – doplnit protokol o šifrovací a autentizační procedury
e) **zefektivnit směrování** – přidělování adres pomocí autokonfiguračních mechanismů dynamicky – podporuje mobilitu – každému mobilnímu zařízení jsou přiřazeny dvě adresy, jedna v mateřské síti, druhá dynamická v hostující síti, firewall na domácí síti pak vytvoří tunel k danému zařízení
f) **lépe využít přenosové rychlosti** – pomocí toků (posloupností paketů), které mají stejnou zdrojovou i cílovou adresu, autentizaci, bezpečnost
g) **podpora priorit** – různé priority pro různé požadavky na přenos, např. pro přenos v reálném čase
h) **snadný přechod od IPv4 k IPv6** – po několik let je nutná koexistence a paralelní fungování obou verzí protokolů, přitom oba protokoly musí využívat vzájemně nezávislé zásobníky

IPv6 počítá se 128bitovou velikostí adresy, ta je složena ze dvou částí (prvních 64 bitů – prefix – je vyhrazeno pro identifikaci sítě, druhých 64 bitů pak pro identifikaci zařízení. Části pro identifikaci je buď vytvořena automaticky z MAC adresy rozhraní nebo je přiřazena následně. IPv6 adresy se s časem mění, aby byla zajištěna anonymita uživatele (MAC adresy jsou celosvětově unikátní).

IPv6 adresa se zapisuje jako osm skupin čtyř hexadecimálních číslic. Pokud je některá ze skupin 0000, je možné nuly vynechat a nahradit skupinu zápisem „::“. Je-li více skupin za sebou složeno ze samých nul, je možné všechny tyto skupiny vynechat a použít pouze zápis „::“.

Např. adresa fe80:0000:0000:0000:211:d8ff:fe50:f8cd je identická s fe80::211:d8ff:fe50:f8cd.

V praxi je možné se setkat i se smíšeným zápisem, kdy poslední 4 byty jsou zapisovány dekadicky a odděleny tečkou. Tato forma zápisu není však schválena RFC a aplikace ji v zásadě nepodporují.

Prefix adresy se může podobně jako v mechanismu CIDR IPv4 zapsat za lomítko na konec adresy, například tedy 1080:0:0:0:8::/80.

Typy adres IPv6

a) unicast
b) multicast
c) anycast[2]

IPv6 neobsahuje broadcast adresy – ty byly nahrazeny multicastem. Pro potřeby odeslání zprávy všem uzlům dané lokální sítě je v každé lokální síti vyhrazena speciální skupinová adresa.

Speciální adresy v IPv6

a) **globální individuální adresy** – prefix 001
b) **linkové adresy** – používají se pro automatickou konfiguraci síťového zařízení a pro objevování sousedů, prefix 1111:1110:10
c) **nespecifikované adresy**
    a. **::** – nesmí být přiřazena žádnému rozhraní, lze ji použít jako zdrojovou adresu při konfiguraci zařízení snažícího se získat IPv6 adresu
    b. **::1** (loopback) – používá se k posílání paketů sama sobě, nesmí být přiřazena žádnému rozhraní (obdoba 127.0.0.1 u IPv4)

Speciálním případem IPv6 je pak *IPv4 kompatibilní adresa* (IPv6 s vloženou IPv4 adresou). Přechodový mechanismus mezi IPv4 a IPv6 obsahuje metodu dynamického tunelování IPv6 paketů přes IPv4 oblasti. Uzlům používajícím tuto metodu jsou přiřazeny speciální IPv6 adresy, které obsahují na nejnižších 32 bitech IPv4 adresu. Prvních 12 B nabývá nulových hodnot (např. ::130.170.234.24).

Dalším speciálním typem IPv6 obsahujícím IPv4 adresu je *IPv4 překládaná adresa*. Tyto adresy se používají pro zařízení podporující pouze IPv4. Na prvních 10 B mají nulové hodnoty, další 2 B pak obsahují binární jedničky a posledních 32 bitů je opět IPv4 adresa (např. ::ffff:130.170.234.24).

ICMPv6

ICMP protokol je nahrazenou protokolem ICMPv6. Ten v sobě kombinuje dříve používané protokoly ICMP, IGMP a ARP. Používá se pro diagnostiku a ohlašování chyb vzniklých při přenosu paketů a při objevování sousedů. Jeho funkce jsou rozděleny do dvou oblastí:

a) **oblast chybová** – nedosažitelný cíl; příliš velký paket; vypršela životnost paketu; problémy s parametry
b) **oblast informační** – diagnostické zprávy; zprávy objevování sousedů; zprávy o zacházení se skupinovými adresami

[2] **anycast** – identifikuje skupinu síťových zařízení; zpráva se doručí nejbližšímu zařízení z dané skupiny (měřeno počtem hopů)