**8**

**IP adresy IPv4**

**Účel a funkce IP adres**

* IP adresa (Internetová protokolová adresa) = číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti
* IP adresa může být zapsána v desítkové soustavě nebo ve dvojkové soustavě
* každý počítač má svoje jedinečné číslo a slouží jako identifikátor mezi ostatními počítači a veškerými zařízeními na internetu
* toto číslo je automaticky generováno počítačem a musí být pro přehlednost jednoznačné
* v současnosti se nejvíce používá generování podle protokolu IPv4 a to v podobě například: 192.168.1.1, toto protokolové číslo je zapsané ve 32-bitovém čísle

[4 decimální čísla (oktety = 4 osmice bitů) -> 0 – 255], což znamená, že máme přibližně 4 miliardy možností, ale protože spousta adres je zabrána pro jiné účely, není jich doopravdy tolik

* jelikož IP adres verze 4 je pouze omezené množství, nové počítače mají IP adresu verze 6, která nabízí více variant, je zapsaná ve 128-bitovém čísle a má tedy 4x více kombinací než 32-bitové číslo
* IP adresa se dělí na 3 hlavní části: 1) číslo sítě 2) číslo podsítě 3) číslo síťového rozhraní
* tyto hlavní části umožňují co nejpřesnější lokalizaci počítače v síti kdekoliv na světě, můžeme si to představit jako poštovní adresu, akorát pro počítače
* podle tohoto čísla lze určit na které síti se uživatel s počítačem nachází a potom už ho můžeme snadno vystopovat
* jelikož jsou tyto čísla pro obyčejné uživatele příliš složitá, existuje systém DNS

(Domain Name System = systém jmenování domén), který umožňuje používat jména počítačů, která jsou dobře zapamatovatelná a automaticky je potom převede na číselnou IP adresu pro identifikaci

**Třídy adres**

Table

Description automatically generated

Table

Description automatically generated

<- (zkrácená podoba) ->

* původně sloužila v IPv4 k určení podsítě první osmice bitů (první číslo v zápisu IP adresy), když se to ukázalo jako nedostatečné, byly zavedeny tzv. třídy IP adres (A, B, C, D a E), kde bylo rozdělení na podsítě určeno tzv. maskou sítě a ta byla určena prvními několika bity samotné IP adresy, tento způsob se však po čase ukázal také jako nedostatečný, protože poskytoval relativně hodně velkých podsítí (třída A) a málo malých podsítí (třída C)

***Třída A***

* rozsah 0 – 127
* první 1 bit je adresa sítě, další 3 jsou adresy PC

***Třída B***

* rozsah 128 – 191
* první 2 bity jsou adresa sítě, další 2 bity jsou adresy PC

***Třída C***

* rozsah 192 – 233
* první 3 bity jsou adresa sítě, další 1 bit je adresa PC

***Třída D***

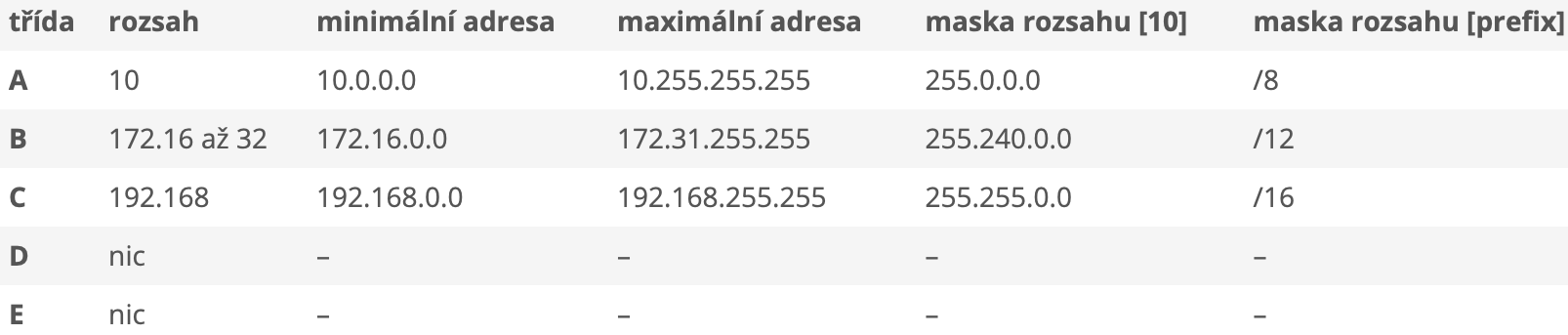
* slouží pro skupinovou adresaci (multicast)

***Třída E***

* slouží pro experimentální účely

**Rezervované IP adresy**

* nelze využívat všechny IP adresy, protože nějaké mají speciální určení
* nejnižší adresa v síti (s nulovou adresou stanice) slouží v IPv4 jako označení celé podsítě
* nejvyšší adresa v síti (adresa stanice obsahuje samé binární jedničky) slouží jako adresa pro všesměrové vysílání (broadcast), takové adresy tedy nelze použít pro normální účely
* adresy 127.x.x.x (tzv. localhost, nejčastěji se používá adresa 127.0.0.1) jsou rezervovány pro tzv. loopback, logickou smyčku umožňující posílat pakety sám sobě



* toto jsou rozsahy IP adres pro použití v domácí, firemní či podnikové síti jakéhokoliv typu, tyto rozsahy se na Internetu nikdy nemohou objevit
* vyhrazené adresy z třídy A jsou pro velké a rozlehlé sítě, adresy ze sítě B jsou pro menší, ale i tak rozlehlé sítě, adresy ze sítě C jsou pro domácí využití

**Veřejné a soukromé IP adresy**

**Veřejné**

* veřejná IP adresa je viditelná v síti Internet
* je-li IP adresa PC viditelná, je možno se k takovémuto PC odkudkoli z internetu připojit a komunikace s ním je velmi rychlá, a tudíž pohodlná
* k nevýhodám veřejné IP adresy patří menší anonymita, se kterou je spojeno riziko útoků na počítač dané adresy, je proto nezbytné, aby takového PC bylo zabezpečeno antivirovou ochranou a firewallem

**Neveřejné**

* neveřejná IP adresa je z hlediska bezpečnosti vhodnější, neboť je takovýto počítač v internetu neviditelný
* ve většině případů je takovéto PC skryto za proxyserverem, který přiděluje adresu pouze vnitřní sítě, je tedy možno sdílet data pouze v intranetu neboli interní síti
* naprostá většina poskytovatelů internetového připojení svým klientům poskytuje právě tento typ adresy

**Subnetting**

* proces rozdělení IP sítí do menších podsítí nazývaných „podsítě“
* používá se zejména v oddělených oblastech, ve kterých je potřeba lépe využít přidělený adresní prostor
* typicky toto řešení využívají firmy, které mají několik menších oddělených sítí s relativně malým počtem uzlů v každé síti, tato firma pak místo více adres třídy C (pro každou lokální síť jedna) vystačí s jedinou adresou třídy C, kde prvních několik bitů z lokální části adresy použije pro adresaci podsítě

****

* př. adresu 192.44.118.192 třídy C firma použije pro vytvoření 4 lokálních foremních podsítí takto:

Původní IP adresa:



Pro adresaci podsítí budou použity první 2 bity lokální části adresy, mohou vzniknout 4 podsítě s různými adresami:

Table

Description automatically generated

* rozdělení jedné síťové adresy na několik adres se děje posunutím hranice mezi oběma logickými složkami adresy směrem k nižším bitům (doprava)
* posunutí je definováno maskou sítě (podsítě)
* důležitý je fakt, že toto rozdělení na několik podsítí je záležitost lokální, nikoli globální, navenek se tedy všechny adresy podsítí jeví stále jako jediná síťová adresa
* z tohoto důvodu je nutné, aby sítě, které subnetting využívají měly jediný společný vstupní bod

**Supernetting**

* princip supernettingu je opačný než u subnettingu
* původně samostatné síťové adresy spojuje do jedné společné adresy
* pro použití supernettingu nejsou vhodné libovolné adresy, musí jít o adresy „sousední“, to jsou adresy, které se shodují v určitém počtu vyšších bitů své síťové části a vyčerpávají všechny bitové kombinace v příslušném počtu nižších bitů své síťové části
* supernetting se používá pro zjednodušení směrovacích tabulek
* informace o „splynutí“ více adres v jednu musí mít na rozdíl od subnettingu globální charakter, aby ji pro směrování bylo možné použít

**VLSM (Variable Length Subnet Masking)**

* aby nedocházelo k blokování IP adres u menších sítí, byl zaveden koncept IP adresace s možností měnit délku HOST ID (nebo SUBNET ID) podle velikosti uvažované IP subsítě
* aby mohl VLSM systém správně fungovat, bylo nutné upravit směrovací protokoly v IP sítích tak, aby si směrovače vyměňovaly mezi sebou nejen IP adresy sítí, ale i jejich přidružené síťové masky
* výsledkem použití VLSM systému je to, že menším subsítím je přiřazena delší IP maska a tím i kratší pole HOST ID, tak aby co nejlépe korespondovalo s požadavky dané sítě
* VLSM adresace tedy významně přispívá k efektivnějšímu využití přiděleného adresového prostoru s minimální blokací IP adres
* na druhou stranu VLSM je náročnější na pochopení a v některých případech může komplikovat správu sítě
* VLSM má smysl používat jen v těch případech, kdy je třeba efektivně využít IP adresový prostor, typicky toto hlavně platí pro veřejné IP adresy, které musíme šetřit

**Diagram

Description automatically generated**

**ZDROJE:**

<https://docplayer.cz/26775120-Adresace-ipv4-vlsm-cidr-priklady-a-principy.html>

<https://wiki.knihovna.cz/index.php/IP_adresa#Protokol_IPv4>

<http://dousa.blogujem.eu/2014/04/zakladni-zarikadla-v-ipv4-siti-ip-adresy/>

<https://www.earchiv.cz/anovinky/ai1646.php3>

<https://www.anetliberec.cz/clanky/detail-verejna-vs-neverejna-ip-adresa-54/>

<https://cs.wikipedia.org/wiki/IP_adresa>

<https://moodle.sspbrno.cz/pluginfile.php/6391/mod_resource/content/1/ip_adresy1.pdf>