

8. IP adresy IPv4 – účel a funkce IP adres, třídy adres, rezervované IP adresy, veřejné a soukromé IP adresy, subnetting, supernetting, VLSM

Obsah

Úvod	1
IPv4 adresa	2
Formát IPv4 adresy	2
Masky	2
CIDR notace	3
Třídy adres	3
Funkce síťové masky.....	3
Třídy IP adres	4
Rezervované IP adresy.....	5
Veřejné IP adresy	6
Soukromé IP adresy	6
NAT (Network Address Translation).....	6
Subnetting (Podsítování).....	7
VLSM (Variable Length Subnet Mask).....	7
Supernetting.....	8
Závěr	8
Zdroje.....	8

Úvod

IP adresa (Internet Protocol Address) je jedinečný identifikátor, který se používá k identifikaci zařízení v síti, například na internetu nebo v lokální síti. Je to logická (softwarová) adresa. IP adresa umožňuje zařízením komunikovat mezi sebou tím, že poskytuje informaci o tom, kam mají být data odeslána a odkud přišla.

IPv4 adresa

IPv4 (Internet Protocol version 4) je čtvrtá verze internetového protokolu, která byla poprvé zavedena v roce 1983. Jedná se o protokol, který funguje na úrovni síťové vrstvy v modelu OSI (Open Systems Interconnection) a je zodpovědný za adresaci zařízení a směrování datových paketů mezi nimi. IP adresy verze IPv4 jsou stále dominantní i přes to, že se již několik let postupně zavádí modernější verze IPv6, která má řešit některé nedostatky IPv4, zejména nedostatečný počet dostupných IP adres.

Formát IPv4 adresy

IPv4 adresa je 32bitové číslo, které se běžně zapisuje jako čtyři oddělené desítkové bloky (tzv. oktety), přičemž každý blok obsahuje 8 bitů. Každý oktet má hodnotu v rozmezí 0 a 255.

Např.: 172.16.2.160

Adresa stanice
172.16.2.160 → 10101100 00010000 00000010 10100000

sít' stanice

Každý oktet reprezentuje binární číslo a celé IP adrese pak odpovídá binární hodnota, kterou zařízení používají pro identifikaci. IP adresy jsou v binárním tvaru zpracovávány směrovači a dalšími síťovými zařízeními, která zajišťují komunikaci mezi různými zařízeními v síti.

Masky

Síťová maska (anglicky *subnet mask*) je klíčový prvek v adresování. Pomáhá určit, jaká část IP adresy identifikuje síť a jaká část identifikuje konkrétní zařízení (host) v této síti. Síťová maska tedy odděluje síťovou (network) část IP adresy od části, která označuje jednotlivé zařízení v rámci této sítě (host). Maska je stejně jako IPv4 adresa 32bitová.

Skládá z dvou částí:

- **Síťová část:** Zapsaná jako posloupnost bitů „1“ (tyto bity označují síť).
- **Hostitelská část:** Zapsaná jako posloupnost bitů „0“ (tyto bity označují konkrétní zařízení, tzv. hosta, v síti).

Obvykle se zapisuje ve stejném formátu jako IP adresa, tedy jako čtyři desítková čísla oddělená tečkami. Například běžná síťová maska může vypadat takto: **255.255.255.0**

CIDR notace

Vedle tradičního zápisu síťové masky se často používá také CIDR notace (Classless Inter-Domain Routing), která zjednodušuje vyjádření masky a sítě. CIDR notace přidává k IP adrese lomítko / a číslo, které udává, kolik bitů v adrese tvoří síťovou část. Například:

- IP adresa 192.168.1.10/**24** znamená, že první 24 bitů je síťová část (což odpovídá síťové masce 255.255.255.0).

Třídy adres

třídy A:

- Masky: **255.0.0.0 (/8)**
- První oktet identifikuje síť, zbylé tři oktety jsou pro zařízení (hosty).
- Síť může obsahovat až 16 777 214 zařízení.

třídy B:

- Masky: **255.255.0.0 (/16)**
- První dva oktety identifikují síť, zbylé dva jsou pro hosty.
- Síť může obsahovat až 65 534 zařízení.

třídy C:

- Masky: **255.255.255.0 (/24)**
- První tři oktety identifikují síť, poslední oktet je pro zařízení.
- Síť může obsahovat až 254 zařízení.

Funkce síťové masky

Síťová maska umožňuje následující klíčové funkce:

- **Identifikace sítě a hostů**
- **Směrování dat:** Když zařízení v síti komunikuje, směrovače (routery) využívají síťovou masku k tomu, aby určili, zda se cílová adresa nachází ve stejné síti, nebo zda je potřeba odeslat data do jiné sítě. Směrovač porovnává síťovou část IP adresy odesílatele s cílovou adresou, aby zjistil, kam data poslat.
- **Subnetting** (rozdělení sítě na podsítě)
- **Supernetting** (sloučení podsítí)

Třídy IP adres

IPv4 adresa je rozdělena do několika tříd, které určují, jakým způsobem je síťová adresa rozdělena mezi síť a jednotlivé zařízení (tzv. hosty) v síti. Existuje pět základních tříd IPv4 adres: A, B, C, D a E. Třídy A, B a C jsou běžně používané pro standardní adresaci, zatímco třída D je určena pro multicast a třída E je rezervovaná pro budoucí použití.

- **Třída A:** IP adresy v této třídě mají první oktet mezi 1 a 126. Tato třída byla navržena pro velmi velké sítě, protože umožňuje až 16 milionů hostů na jednu síťovou adresu. Příklad: 10.0.0.1.
- **Třída B:** Tato třída zahrnuje IP adresy s prvním oktetem v rozmezí od 128 do 191. Síť může mít až 65 534 hostů. Příklad: 172.16.0.1.
- **Třída C:** Nejčastěji používaná třída pro menší sítě, IP adresy mají první oktet mezi 192 a 223. Umožňuje až 254 hostů na síť. Příklad: 192.168.1.1.
- **Třída D:** IP adresy od 224 do 239 jsou používány pro multicast, což umožňuje jedné adrese odeslat data více příjemcům zároveň.
- **Třída E:** Adresy od 240 do 255 jsou rezervovány pro experimentální účely a nejsou veřejně dostupné.

Struktura adresy se skládá se ze dvou částí:

- **síťová** (network - N), jedná se o neměnnou část adresy, která identifikuje konkrétní síť
- **uzlová** (host - H), jedná se o proměnnou část adresy, která identifikuje konkrétní zařízení (uzel) v rámci dané sítě.

Třída	Struktura adresy	První bajt adresy (binárně)	Platné hodnoty prvního oktetu (dekadicky)	Adresy sítí
A	N.H.H.H	0xxxxxxx	1-126	1.0.0.0 – 126.0.0.0
B	N.N.H.H	10xxxxxx	128-191	128.0.0.0 – 191.255.0.0
C	N.N.N.H	110xxxxx	192-223	192.0.0.0 – 239.255.255.0
D	skupinová	1110xxxx	224-239	224.0.0.0 – 239.255.255.255
E	experimentální	1111xxxx	240-254	240.0.0.0 – 255.255.255.254

Každá třída má specifickou velikost a použití, což umožňuje efektivní správu a rozdělení adresního prostoru. Tento systém rozdělení byl nezbytný pro to, aby bylo možné rozdělit adresy mezi různé sítě po celém světě a zároveň udržet logickou a funkční strukturu adresace.

Rezervované IP adresy

Některé IP adresy v rámci těchto tříd jsou rezervovány pro specifické účely a nelze je použít pro běžnou komunikaci na internetu.

Např:

0.0.0.0

Tato adresa se používá pro specifikaci „toto zařízení na této síti“. Obvykle se používá v situacích, kdy počítač nemá přiřazenou žádnou konkrétní IP adresu, ale potřebuje komunikovat v rámci místní sítě. Tato adresa může být také použita jako výchozí brána nebo v konfiguracích DHCP, kdy zařízení vyžaduje IP adresu.

127.x.x.x (Adresa smyčky)

Tento rozsah adres je známý jako adresa smyčky (Loopback Address) a slouží pro testování a diagnostiku. Nejčastěji používaná adresa v tomto rozsahu je 127.0.0.1, která odkazuje na místní počítač.

255.255.255.255 (Lokální všeobecná adresa)

Tato adresa se používá pro broadcast zprávy, což znamená, že je určena pro všechny zařízení v lokální síti.

122.0.0.0 (Adresa sítě)

Tato adresa slouží k identifikaci sítě a vyjadřuje celou síť bez specifikace konkrétního zařízení. V rámci logického operací je obvykle získána logickým součinem unicast adresy a implicitní masky.

0.0.0.5 (Adresa stanice)

Podobně jako u předchozí adresy, adresa 0.0.0.5 může být také výsledkem logického součinu unicast adresy a wildcard masky. Tato adresa ukazuje na specifické zařízení v rámci sítě.

122.255.255.255 (Všeobecná adresa v síti)

Tato adresa se používá jako directed (cílený) broadcast pro specifikovanou síť. Mohou být použity pouze jako cílové adresy, což znamená, že žádné zařízení nemůže být přímo přiřazeno k této adrese.

Veřejné IP adresy

Veřejné IP adresy jsou IP adresy, které jsou globálně jedinečné a používají se pro komunikaci na internetu. Tyto adresy jsou přiřazeny organizacemi spravujícími IP prostor, jako je IANA (Internet Assigned Numbers Authority), a jsou přidělovány jednotlivým uživatelům a organizacím poskytovateli internetových služeb (ISP).

Soukromé IP adresy

Soukromé IP adresy jsou IP adresy, které jsou používány pouze uvnitř lokálních sítí (LAN – Local Area Network) a **nejsou viditelné na internetu**. Tyto adresy jsou zdarma k použití a jsou definovány podle standardu RFC 1918. Zařízení v lokální síti mohou mezi sebou komunikovat pomocí těchto soukromých IP adres, ale ke komunikaci s internetem používají překlad adres (NAT – Network Address Translation).

- **Příklad soukromé IP adresy:** 192.168.1.1 (běžná adresa routerů v domácí síti)

Soukromé IP adresy jsou rozděleny do následujících rozsahů:

- **Třída A:** 10.0.0.0 – 10.255.255.255 (/8)
- **Třída B:** 172.16.0.0 – 172.31.255.255 (/12)
- **Třída C:** 192.168.0.0 – 192.168.255.255 (/16)

Třída	Rozsah adres	CIDR Prefix
A	10.0.0.0 až 10.255.255.255	10.0.0.0 / 8
B	172.16.0.0 až 172.31.255.255	172.16.0.0 / 12
C	192.168.0.0 až 192.168.255.255	192.168.0.0 / 16

NAT (Network Address Translation)

NAT je technologie používaná pro překlad mezi soukromými a veřejnými IP adresami. Typicky se NAT implementuje na routeru, kde zařízení uvnitř soukromé sítě mají přiřazené soukromé IP adresy, a když komunikují s internetem, jejich adresy jsou přeloženy na veřejnou IP adresu routeru. Tento proces umožňuje efektivní využití omezeného počtu veřejných IP adres.

Subnetting (Podsítování)

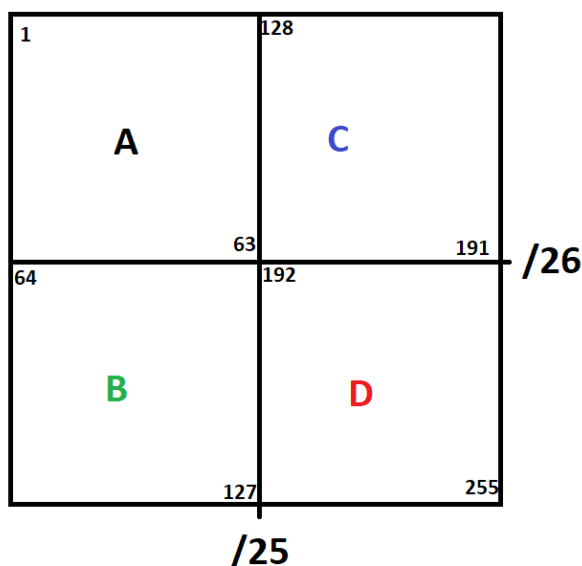
Subnetting je proces rozdělení větší sítě na menší logické podsítě (subnets). Cílem je efektivněji spravovat IP adresní prostor a zlepšit výkonnost a bezpečnost sítě. Pomocí podsítování můžeme lépe kontrolovat provoz mezi jednotlivými segmenty sítě a zlepšit organizaci adres v rámci velké sítě.

Subnetting využívá změnu "masky sítě" (subnet mask), která určuje, kolik bitů z IP adresy tvoří síťovou část a kolik bitů tvoří část hostitelskou.

Příklady:

Představme si, že máte síť s IP adresou **192.168.1.0/24**, což znamená, že máme 256 adres (od 192.168.1.0 do 192.168.1.255). Pokud však tuto síť potřebujeme rozdělit na menší části, můžeme použít subnetting. Tedy:

- Pokud síť rozdělíme na čtyři podsítě, použijeme masku **255.255.255.192 (/26)**, což nám poskytne čtyři podsítě, každou s 64 adresami.
 - Podsíť A: 192.168.1.0/26 (adresy od 192.168.1.0 do 192.168.1.63)
 - Podsíť B: 192.168.1.64/26 (adresy od 192.168.1.64 do 192.168.1.127)
 - Podsíť C: 192.168.1.128/26 (adresy od 192.168.1.128 do 192.168.1.191)
 - Podsíť D: 192.168.1.192/26 (adresy od 192.168.1.192 do 192.168.1.255)



VLSM (Variable Length Subnet Mask)

VLSM (Variable Length Subnet Mask) (podsíťové masky různé délky) je metoda podsítování, která umožňuje použít různé délky masky sítě pro různé podsítě. Tento

koncept přináší větší flexibilitu při alokaci IP adres, protože umožňuje přizpůsobit velikost podsítí přesně podle jejich potřeb.

Supernetting

Supernetting je opakem subnettingu. Zatímco subnetting dělí větší síť na menší části, supernetting spojuje několik malých sítí do jedné větší. Tento koncept se využívá zejména v situacích, kdy je třeba snížit počet záznamů ve směrovací tabulce směrovačů, což usnadňuje správu velkých sítí a zlepšuje jejich výkon.

Příklad:

Představme si, že máme čtyři sítě s následujícími IP adresami:

- 192.168.0.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

Namísto vedení čtyř záznamů pro každou síť můžeme tyto sítě spojit do jedné supernetové adresy: **192.168.0.0/22**. Tím získáme jednu síť, která zahrnuje všechny adresy od 192.168.0.0 do 192.168.3.255.

Závěr

IPv4 adresy, jejich třídění, veřejné a soukromé adresy, subnetting, supernetting a VLSM jsou klíčové koncepty pro efektivní správu moderních sítí. Přestože IPv6 nabízí prakticky neomezený adresní prostor, IPv4 je stále velmi rozšířené, a proto porozumění těmto principům zůstává nezbytné pro správu a zabezpečení sítí.

Zdroje

N:\DokumentyUčitelé\Peckova\