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

**Účel a funkce IP adres**

IPv4 (Internet Protocol verze 4) je klíčovým protokolem, který slouží k identifikaci a adresaci zařízení v počítačových sítích, včetně internetu. Je součástí sady protokolů TCP/IP který je orientován na rychlost efektivnost přenosu a hraje zásadní roli v tom, jak jsou data přenášena mezi různými zařízeními.

Hlavním účelem IPv4 je poskytovat jedinečné adresy pro každé zařízení připojené k síti což dělá např. pomocí DHCP. Protokol IPv4 využívá 32bitové adresy, což umožňuje přidělení přibližně 4 miliard unikátních IP adres. Tímto způsobem zajišťuje, že každé zařízení má svůj vlastní identifikátor, což je nezbytné pro správnou komunikaci.

Každá IP adresa je tvořena čtyřmi osmibitovými čísly (tzv. oktety), oddělenými tečkami a jejich hodnota se pohybuje od 0 do 255. Funkcí IP adresy je umožnit směrování paketů z jednoho zařízení na druhé. Každá adresa má dvě složky:

* Síťová část: Identifikuje konkrétní síť.
* Hostitelská část: Identifikuje konkrétní zařízení (hosta) v síti.

Další důležitou funkcí IPv4 je routing, tedy směrování dat. Směrovače využívají informace obsažené v IPv4 adresách, aby se rozhodly, kam mají data směřovat. Kromě toho IPv4 podporuje fragmentaci datových paketů, což znamená, že větší zprávy mohou být rozděleny na menší části pro efektivnější přenos.

Protokol také zahrnuje mechanismy pro kontrolu chyb, čímž zvyšuje spolehlivost komunikace. Umožňuje různé typy přenosových služeb, jako jsou unicast (přenášení dat z jednoho zařízení na jiné), multicast (přenášení dat z jednoho zařízení na více zařízení) a broadcast (přenášení dat ze zařízení na všechna připojená zařízení).

IPv4 je široce podporován a interoperabilní s mnoha různými protokoly a zařízeními, což usnadňuje integraci různých technologií. Přestože je IPv4 stále nejpoužívanějším protokolem, jeho omezený počet adres vedl k přechodu na IPv6, který nabízí mnohem větší adresní prostor a další vylepšení, aby vyhověl rostoucím potřebám moderního internetu.

Složení IPv4 paketu

### 1. **Header (hlavička)**

Hlavní části datagramu se nacházejí v hlavičce, která je obvykle 20 až 60 bytů dlouhá. Hlavička obsahuje následující pole:

* **Verze**: Určuje verzi protokolu (pro IPv4 je to hodnota 4).
* **IHL (Internet Header Length)**: Velikost hlavičky v 32bitových slovech.
* **Typ služby (Type of Service)**: Slouží k určení priority a zpracování paketu.
* **Délka (Total Length)**: Celková délka datagramu v bajtech, včetně hlavičky a dat.
* **Identifikace**: Slouží k identifikaci fragmentů datagramu.
* **Flagy**: Ovládají fragmentaci, například zda je paket fragmentován.
* **Fragment Offset**: Určuje pozici fragmentu v původním datagramu.
* **TTL (Time to Live)**: Počet skoků, které paket může vykonat, než je zahozen. Pomáhá zabránit nekonečným smyčkám.
* **Protokol**: Určuje protokol na transportní vrstvě (např. TCP, UDP).
* **Kontrolní součet (Header Checksum)**: Kontroluje chyby v hlavičce.
* **Zdrojová IP adresa**: IP adresa odesílatele.
* **Cílová IP adresa**: IP adresa příjemce.

### 2. **Payload (nosič)**

Za hlavičkou následuje část dat, která je přenášena, nazývaná payload. Tato část může obsahovat různé typy dat, jako jsou TCP segmenty, UDP datagramy nebo jiná aplikační data.

### 3. **Fragmentace**

Pokud je datagram příliš velký na to, aby byl přenesen v jednom kuse, může být fragmentován na menší části. Každý fragment obsahuje svou vlastní hlavičku a fragment offset, což umožňuje příjemci správně zrekonstruovat původní datagram.

### 4. **Délka datagramu**

Celková délka IPv4 datagramu se měří v bajtech a zahrnuje jak hlavičku, tak payload. Maximální velikost IPv4 datagramu je obvykle 65,535 bytů, což zahrnuje hlavičku a data.

IPv4 datagram je tedy klíčovým prvkem v komunikaci v rámci protokolu IPv4, umožňuje efektivní a spolehlivý přenos dat mezi různými zařízeními v síti.

**Třídy IP adres**

IPv4 adresy jsou rozděleny do pěti tříd (A, B, C, D, E), přičemž třídy A, B a C jsou nejvíce používané pro veřejné a soukromé adresování:

* Třída A: Rozsah 1.0.0.0 až 126.0.0.0 (síťová část je prvních 8 bitů, zbytek je pro hosty). Podporuje velké sítě s až 16 miliony hostů.
* Třída B: Rozsah 128.0.0.0 až 191.255.0.0 (síťová část je prvních 16 bitů). Podporuje středně velké sítě, až 65 000 hostů.
* Třída C: Rozsah 192.0.0.0 až 223.255.255.0 (síťová část je prvních 24 bitů). Podporuje malé sítě do 254 hostů.
* Třída D: Používá se pro multicast (rozsah 224.0.0.0 až 239.255.255.255).
* Třída E: Rezervována pro budoucí použití (rozsah 240.0.0.0 až 255.255.255.255).

**Rezervované IP adresy**

Některé IP adresy nelze použít pro veřejné adresování, protože jsou rezervované pro specifické účely:

- Loopback adresy: Rozsah 127.0.0.0 až 127.255.255.255 slouží pro testování síťových - - rozhraní na samotném zařízení (typicky 127.0.0.1).

- Privátní IP adresy: Tyto adresy nejsou routovány na veřejném internetu a slouží k internímu použití v privátních sítích. Privátní rozsahy jsou:

- Třída A: 10.0.0.0 až 10.255.255.255

- Třída B: 172.16.0.0 až 172.31.255.255

- Třída C: 192.168.0.0 až 192.168.255.255

- Broadcast adresy: Adresa s hostitelskou částí složenou pouze z jedniček (255) slouží k odeslání paketů všem zařízením v síti.

**Veřejné a soukromé IP adresy**

#### Veřejné IP adresy

Veřejné IP adresy jsou adresy, které jsou směrovány na internetu a jsou jedinečné po celém světě. Tyto adresy umožňují zařízení, jako jsou servery a směrovače, komunikovat s jinými zařízeními v rámci globální sítě. Každá veřejná IP adresa je přidělována jedinečně a zajišťuje, že zařízení mohou být přesně identifikována v rámci internetu.

**Vlastnosti veřejných IP adres:**

* **Jedinečnost**: Každá veřejná IP adresa musí být jedinečná v rámci internetu, což zajišťuje, že nedochází k žádným konfliktům.
* **Směrování**: Veřejné IP adresy mohou být směrovány na internetu, což umožňuje uživatelům přístup k webovým stránkám a online službám.
* **Přidělování**: Veřejné IP adresy jsou spravovány organizacemi, jako je Internet Assigned Numbers Authority (IANA) a regionální internetové registry (RIR), které přidělují adresy poskytovatelům internetových služeb.

#### Soukromé IP adresy

Soukromé IP adresy jsou adresy určené pro použití v lokálních sítích a nejsou směrovány na internetu. Tyto adresy umožňují zařízení v rámci jedné sítě komunikovat mezi sebou, aniž by byly viditelné na veřejném internetu. Soukromé IP adresy se používají v domácnostech, kancelářích a jiných organizacích.

**Vlastnosti soukromých IP adres:**

* **Několik sítí s obdobnými adresami**: Různé sítě mohou používat stejné soukromé IP adresy, protože tyto adresy nejsou viditelné z internetu díky překladu NAT. Například adresa 192.168.1.1 může existovat v několika různých domácnostech.
* **Rezervované rozsahy**: Existují specifické rozsahy IP adres, které jsou vyhrazeny pro soukromé použití:

- Třída A: 10.0.0.0 – 10.255.255.255

- Třída B: 172.16.0.0 – 172.31.255.255

- Třída C: 192.168.0.0 – 192.168.255.255

* **Nesměrování na internetu**: Soukromé IP adresy nelze přímo směrovat na veřejném internetu, což zvyšuje bezpečnost a chrání vnitřní síť před vnějšími hrozbami.

#### Použití veřejných a soukromých IP adres

Veřejné a soukromé IP adresy mají různá použití v rámci různých scénářů:

* **Domácí sítě**: V domácnostech se obvykle používají soukromé IP adresy. Router přiděluje soukromé adresy jednotlivým zařízením (např. počítačům, chytrým telefonům) a používá jednu veřejnou IP adresu pro připojení k internetu.
* **Podnikové sítě**: Firmy často používají kombinaci veřejných a soukromých IP adres. Soukromé adresy jsou použity pro interní komunikaci mezi zařízeními, zatímco veřejné adresy jsou potřebné pro přístup k veřejným službám a webovým aplikacím.
* **Serverové farmy**: Servery, které poskytují služby na internetu, používají veřejné IP adresy, aby byly dostupné pro uživatele. Na druhou stranu, servery v rámci interních aplikací nebo databází mohou používat soukromé adresy.

### **Subnetting**

Subnetting je klíčová technika v oblasti správy IP adres, která umožňuje rozdělení větší sítě na menší podsítě. Tento proces nejenže zvyšuje efektivitu využití IP adres, ale také zlepšuje správu a bezpečnost sítí. V tomto textu se podíváme na principy subnettingu, jeho výhody a praktické aplikace.

#### Co je Subnetting?

Subnetting je proces, při kterém se hlavní síť dělí na menší logické části, zvané podsítě. Každá podsíť má svou vlastní subnetovou masku, která určuje, jaká část IP adresy je určena pro identifikaci sítě a jaká část je vyhrazena pro jednotlivé hostitele. Například, pokud máme IP adresu 192.168.1.0 s maskou 255.255.255.0, znamená to, že první tři octety (192.168.1) představují síť a poslední octet je vyhrazen pro hostitele.

#### Jak funguje Subnetting?

Při subnettingu se používá subnetová maska, která určuje, jaká část IP adresy slouží jako identifikátor sítě.

Tímto způsobem se můžeme zaměřit na specifické potřeby různých částí sítě a efektivně využít dostupné IP adresy.

#### Výhody Subnettingu

* **Efektivní využití IP adres**: Subnetting umožňuje lépe využívat omezený adresní prostor. Tím, že se síť rozdělí na menší podsítě, mohou organizace přesněji přizpůsobit počet potřebných adres.
* **Zlepšení bezpečnosti**: Rozdělením sítě na menší podsítě lze implementovat specifická bezpečnostní opatření pro každou část sítě. Například, citlivé informace mohou být umístěny v oddělené podsíti, což zvyšuje ochranu před neoprávněným přístupem.
* **Zjednodušení správy sítě**: Správci sítí mohou lépe organizovat a spravovat různé části sítě. Subnetting umožňuje efektivnější monitoring a diagnostiku problémů v jednotlivých podsítích.
* **Snížení provozu**: Subnetting může snížit množství broadcastového provozu, protože broadcastové zprávy jsou omezeny na jednotlivé podsítě, což zvyšuje výkon sítě.

Správce sítě by mohl provést subnetting hlavní sítě (např. 192.168.0.0/24) na menší podsítě, čímž by efektivně pokryl potřeby každého oddělení a minimalizoval plýtvání IP adresami.

### **Supernetting**

Jedná se o techniku, která spojuje několik menších sítí do jedné větší sítě, čímž se zjednodušuje směrování a správa IP adres. Tato metoda je obzvlášť užitečná pro poskytovatele internetových služeb (ISP) a organizace, které chtějí zefektivnit správu svých adresních prostorů.

#### Co je Supernetting?

Supernetting, také známé jako Classless Inter-Domain Routing (CIDR), umožňuje sloučení několika IP adres do jednoho většího bloku. Místo toho, aby jednotlivé sítě měly své vlastní třídy a masky, supernetting umožňuje použít širší masku, což redukuje počet záznamů v směrovacích tabulkách a zjednodušuje proces směrování.

#### Jak funguje Supernetting?

Supernetting se provádí spojením sousedních IP adres a jejich zařazením pod jednu společnou síť. Tímto způsobem se sníží počet záznamů v směrovacích tabulkách a zjednoduší se správa adresního prostoru.

#### Výhody Supernettingu

* **Redukce směrovacích záznamů**: Supernetting umožňuje snížit množství záznamů v směrovacích tabulkách, což zefektivňuje proces směrování. Menší tabulky znamenají rychlejší rozhodování o směrování a méně zátěže pro směrovače.
* **Efektivní využití IP adres**: Tato technika pomáhá lépe využívat dostupné IP adresy tím, že sloučí menší sítě, které by jinak mohly zůstat nevyužité.
* **Zjednodušení správy**: Správa jedné větší sítě je často jednodušší než správa několika menších. Supernetting umožňuje centrálnější přístup ke správě IP adres.

**VLSM**

Variable Length Subnet Masking (VLSM) je pokročilá technika správy IP adres, která umožňuje používat různé délky subnetových masek v rámci jedné sítě. Tento přístup přináší flexibilitu a efektivitu, zejména v situacích, kdy organizace potřebují optimalizovat využití dostupných IP adres.

#### Co je VLSM?

VLSM umožňuje rozdělění sítě na sub-nety, které mohou mít různé velikosti podle aktuálních potřeb. Zatímco tradiční subnetting obvykle používá stejnou subnetovou masku pro všechny sub-nety, VLSM umožňuje kombinaci různých délek masky, což znamená, že jednotlivé podsítě mohou mít různý počet hostitelů.

#### Jak funguje VLSM?

Při použití VLSM se nejprve definuje hlavní síť a poté se rozdělí na menší podsítě. Při tomto procesu se přiřazují subnetové masky podle potřeby jednotlivých podsítí. Tímto způsobem se efektivně využívají dostupné adresy, a přitom se minimalizuje plýtvání adresním prostorem.