8. Síťová vrstva

# Protokol IP (nespojovanost, best effort)

* IP (Internet Protocol) je jedním z nejdůležitějších protokolů v internetové síti.
* Je to síťový protokol vrstvy 3 (OSI Layer 3) a slouží k přenosu datových paketů mezi počítači v rámci internetu.

## Nespojovanost

* IP protokol je nespojovaný, což znamená, že při přenosu dat neprovádí žádnou kontrolu kvality služby ani nezajišťuje spojení mezi zdrojem a cílem.
* To znamená, že při přenosu dat se nezaručuje, že pakety budou dodány v pořadí, v jakém byly odeslány, nebo že všechny pakety dojdou k cíli.

## Best Effort

* IP protokol pracuje s principem "best effort" (nejlepšího úsilí), což znamená, že se snaží dodat pakety k cíli, ale nezaručuje to.
* Pokud dojde k chybě při přenosu, pakety mohou být ztraceny nebo se mohou dostat do špatného pořadí. Tyto chyby se pak řeší na vyšších vrstvách síťových protokolů, například pomocí protokolů TCP nebo UDP.

# Směrování paketů, princip činnosti směrovače (router), směrovací tabulka

## Směrování paketů

* Směrování paketů je proces, kdy se určuje cesta pro přenos paketů z jedné sítě do jiné
* Toto se provádí pomocí směrovačů (routerů).
* Směrovač je zařízení, které slouží k přenosu datových paketů mezi různými sítěmi.
* Každý paket přicházející na směrovač se analyzuje a určuje se, jakým směrem má být odeslán dál.
* Tento proces se provádí na základě informací uložených v směrovací tabulce.

## Princip činnosti směrovače

* Pokud router přijme paket na rozhraní, koukne se na MAC adresu v rámci, zda je zpráva opravdu určena pro něj.
* Pokud MAC adresy souhlasí, otevře IP paket a podívá se na IP adresu příjemce.
* Poté prohledá svojí routovací tabulku; pokud má onu IP adresu uloženou, poté paket pošle na aktivní port, u které má danou MAC adresu přiřazenou.
* Pokud IP adresu v routovací tabulce nemá, a nemá nastavenou defaultní routu - “vše co neznáš, posílej tudy”; pak paket zahodí.

## Směrovací tabulka

* Do routovací tabulky se vytváří několik typů záznamů cest (route), záleží na tom, jakým způsobem vznikly.
* Pakety jsou podle toho směrovány jedním ze základních způsobů routování
* Statické routování
  + Ručně zadané cesty (záznamy v routovací tabulce), bezpečné a dobré, ale nereflektuje změny v topologii sítě
* Dynamické routování
  + Síť se automaticky přizpůsobuje změnám v topologii a dopravě, automaticky se vypočítávají cesty pomocí routovacího protokolu. Routery si mezi sebou vyměňují informace
* Defaultní routování
  + dochází k němu, pokud neexistuje žádná jiná odpovídající cesta
  + pokud není nastavena defaultní routa, paket je zahozen

# IPv4 adresa, maska podsítě a výchozí brána, statické a dynamické přiřazování IP adres

## IPv4

* Jedná se o adresu, kam se mají data zasílat
* Má 32 bitů
* Příklad: 192.0.2.126
* Maximální možnost 255
* Je jednoduchá oproti IPv6

## Maska podsítě

* Slouží k rozdělení sítě
* Vymezí rozmezí adres, které k sítí patří
* Příklad 192.168.0.0/24 má rozsah 192.168.0.0-192.168.0.255 maska 24 se napíše 255.255.255.0

## Výchozí brána

* Vyhrazuje se pro bránu většinou první adresa (192.168.0.1)
* Cesta používaná k předávání informací, když zařízení neví, kde je cíl.
* Data se potom popřípadě pošlou do jiné sítě

## Statické přiřazování

* Je určená ip adresa pro dané zařízení
* Zařízení tak bude mít vždycky stejnou adresu
* Dá se nastavit ve Windows přímo na zařízení, ale často se nastavuje na routeru samotném
* Používá se třeba pro servery, který potřebují mít stejnou adresu

## Dynamické přiřazování

* Když se připojí zařízení je mu přidělena nějaká adresa
* Tato akce je hlavně prováděna pomocí DHCP
* Adresy jsou propůjčeny z poolu uživatelům pomocí DHCP
* Počítače si musí obnovovat propůjčenou adresu, protože ji mají časově omezenou, aby se, popřípadě uvolnily adresy,
* Lease time je nastavitelný většinou je nastavený na pár hodin

# Typy IPv4 adres, třídy IPv4 adres, řešení nedostatku IPv4 adres – podsítě (VLSM), privátní adresy (NAT)

## Typy, Třídy

### Veřejné

* Viditelné ostatními v internetu
* Je možné se na ně připojit apod.

### Privátní

* Vyhrazené adresy pro privatní použítí
* Class A: 10.0.0.0 to 10.255.255.255
* Class B: 172.16.0.0 to 172.31.255.255
* Class C: 192.168.0.0 to 192.168.255.255

### Unicast address

* Posílání pouze jednomu cílu

### Multicast address

* Poslání jedněch dat více zařízení

### Broadcast address

* Zpráva poslána všem

## VLSM

* Je technika, která umožňuje efektivně využívat adresy v síti tím, že umožňuje stanovit různou délku masky podsítě pro různé podsítě v síti.
* To znamená, že můžete vytvořit větší podsítě s větším počtem adres a menší podsítě s menším počtem adres, což je užitečné například v případě, že některé podsítě potřebují více adres než jiné.
* Tím se dá efektivněji využít celý rozsah adres v síti.
* Příklad Síť LAN A potřebuje 60 adres připadímě mu teda subnet /26 která podporuje 64 uživatelů a Síť LAN B, která potřebuje pouze 2 uživatele tak mu přiřadíme subnet /31 který podporuje 2 uživatele

## NAT

* Způsob, jak mít víc privátních adres přidělené jedné veřejné
* Řeší nedostatek IPv4 adres

### Typy NAT

### Statický NAT

* Jedna privátní adresa převedena na jednu veřejnou.

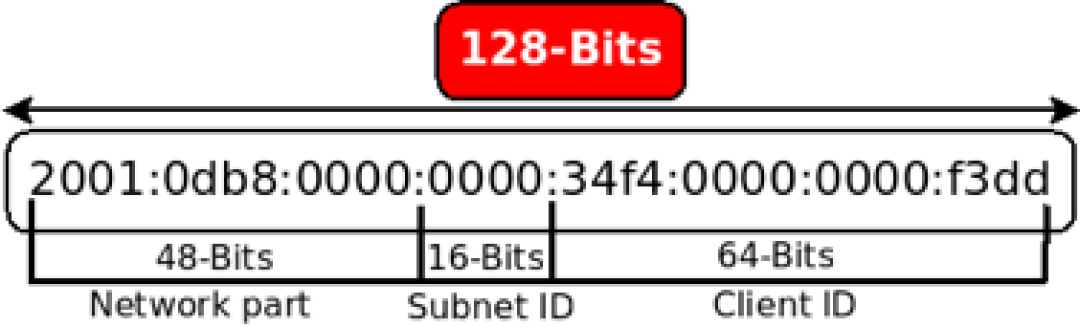
### Dynamická NAT

* Zařízení z privátní sítě čerpají z poolu veřejných adres. Přiděluje se jim veřejná ip adresa podle potřeby.

### PAT

* Jedná se o typ dynamického NAT, který však spojuje několik privátních IP adres do jediné veřejné.
* Uživateli se v privátní síti se přidělí port který funguje jako identifikátor v lokální sítí o koho se jedná a díky tomu může router předat informace správnému uživateli

# Reprezentace a struktura IPv6 adresy, typy IPv6 adres

* Má 128bitů
* Jedna část má 16bitů
* Rozděluje se na 2 části po 64bit
* V první části se nachází údaje o networku a subnetu
* V druhé je Client ID 

## Typy

### Unicast

* Posílání pouze jednomu cílu

### Multicast

* Poslání jedněch dat více zařízení

### Loopback

* Packet se pošle zpět

### Link local

* Slouží ke komunikaci v lokální síti
* Začínají fe80::
* Nepoužívají se na internetu

### Globalní adresy

* Slouží ke komunikaci na internetu

# Způsoby koexistence IPv4 a IPv6

## Dual Stack

* Tato metoda umožňuje zařízením používat jak IPv4, tak IPv6 adresy současně. Toto je nejběžnější způsob pro přechod na IPv6, kdy se udržuje kompatibilita s existujícími IPv4 sítěmi.

## Tunneling

* Tato metoda umožňuje přenos IPv6 paketů přes IPv4 sítě, kdy se IPv6 pakety zabalí do IPv4 paketů. ¨
* Tyto pakety se poté přenášejí přes IPv4 síť a jsou dekomprimovány na druhé straně zpět do IPv6 paketů.

## Translation

* Tato metoda umožňuje komunikaci mezi IPv4 a IPv6 sítěmi prostřednictvím technologie pro překlad mezi těmito protokoly.
* Tyto technologie překládají pakety mezi IPv4 a IPv6 formáty, umožňujíc tak komunikaci mezi zařízeními, která podporují jen jeden z těchto protokolů.

# Protokoly ICMPv4 a ICMPv6

* Slouží hlavně k diagnostice v síti
* Tyto zprávy se používají k řešení problémů, jako je například neuspokojivý stav spojení, ztráta paketů, nedostatek volných zdrojů a další. (Errory)
* Pomocí tohoto protokolu funguje i třeba traceroute nebo ping
* ICMPv4 pro IPv4
* ICMPv6 pro iPv6

### Traceroute

* Slouží k zobrazení cesty z jednoho internetového zařízení do jiného

### Ping

* Je zjednodušená verze traceroute. Testuje jak rychle se tam dostal a jestli dostal odpověď