

- TÉMA č. 1 Komunikačné modely
- TÉMA č. 2 Porovnanie sietí PAN, LAN, WLAN, MAN, WAN
- TÉMA č. 3 Adaptéry počítačových sietí
- TÉMA č. 4 Bezdrôtová dátová komunikácia wifi
- TÉMA č. 5 IP adresný plán IPv4
- TÉMA č. 6 Smerovanie a smerovacie protokoly
- TÉMA č. 7 Prepínače a aplikácia VLAN
- TÉMA č. 8 Diagnostické nástroje pre správu počítačovej siete

## KOMUNIKAČNÉ MODELY

- **definujte vrstvomý komunikačný model OSI a model TCP/IP**
- Vrstvomý komunikačný model OSI (Open Systems Interconnection):  
OSI model je teoretický rámec, ktorý popisuje, ako by mala fungovať komunikácia medzi rôznymi počítačmi v sieti. Skladá sa z 7 vrstiev, ktoré sú:
  - o Fyzická vrstva (Physical Layer): Zodpovedná za prenos bitov medzi zariadeniami cez fyzický médiá, ako je napríklad kábel alebo bezdrôtový signál.
  - o Linková vrstva (Data Link Layer): Zabezpečuje spoľahlivý prenos dát medzi susednými uzlami v sieti. Riadi prístup k médiu a detekciu chýb.
  - o Sietová vrstva (Network Layer): Zodpovedná za doručovanie paketov cez rôzne siete. Vykonáva routovanie a presmerovanie.
  - o Transportná vrstva (Transport Layer): Poskytuje spoľahlivú komunikáciu medzi koncovými aplikáciami. Riadi tok dát a zabezpečuje spoľahlivosť a kontrolu chýb.
  - o Relačná vrstva (Session Layer): Riadi komunikáciu medzi aplikáciami na koncových zariadeniach. Umožňuje vytvorenie, udržiavanie a ukončovanie spojenia.
  - o Prezentačná vrstva (Presentation Layer): Zodpovedná za šifrovanie, kompresiu a formátovanie dát pre prenos medzi rôznymi systémami.
  - o Aplikačná vrstva (Application Layer): Poskytuje rozhranie pre používateľské aplikácie na prístup k sieťovým službám.
- Model TCP/IP (Transmission Control Protocol/Internet Protocol):  
Model TCP/IP, na rozdiel od modelu OSI, je skôr implementačným modelom, ktorý popisuje, ako skutočne funguje internetová komunikácia. Skladá sa z 4 vrstiev:
  - o Sietová vrstva (Network Layer): Zodpovedná za doručovanie paketov cez rôzne siete. Zahrňuje protokoly ako IP (Internet Protocol), ICMP (Internet Control Message Protocol) a ARP (Address Resolution Protocol).
  - o Transportná vrstva (Transport Layer): Poskytuje spoľahlivú komunikáciu medzi aplikáciami. Zahrňuje protokoly ako TCP (Transmission Control Protocol) a UDP (User Datagram Protocol).
  - o Aplikačná vrstva (Application Layer): Poskytuje služby pre koncové aplikácie. Zahrňuje protokoly ako HTTP, FTP, SMTP a DNS.
  - o Rozhranie siete (Network Interface Layer): Tiež nazývaná Linková vrstva alebo Fyzická vrstva v modeli OSI, zabezpečuje prenos dát medzi fyzickými vrstvami siete. Zahrňuje rôzne protokoly na správu prístupu k médiu a rámce dát pre prenos cez fyzické médiá.
- **popíšte spôsob komunikácie medzi jednotlivými vrstvami modelu**
- Komunikácia medzi vrstvami modelu OSI:

- Aplikačná vrstva <-> Prezentačná vrstva <-> Relačná vrstva: Komunikácia medzi týmito vrstvami sa zameriava na transformáciu dát do formátu, ktorý môže byť použitý v sieťovej komunikácii. Napríklad, kompresia alebo šifrovanie dát môže byť vykonaná v prezentačnej vrstve, zatiaľ čo relačná vrstva zodpovedá za riadenie a udržiavanie spojenia medzi aplikáciami.
- Aplikačná vrstva <-> Transportná vrstva: Aplikačná vrstva poskytuje dáta na prenos transportnej vrstve. Transportná vrstva potom rozdeľuje tieto dáta na menšie segmenty a pridáva k nim hlavičku s informáciami, ako je zdrojový a cieľový port, aby bola správa správne doručená.
- Transportná vrstva <-> Sietová vrstva: Transportná vrstva odosiela segmenty dát sietovej vrstve. Sietová vrstva pridáva ďalšie informácie, ako sú IP adresy zdroja a cieľa a kontrolné súčty, ktoré umožnia doručiť dáta cez rôzne siete.
- Sietová vrstva <-> Linková vrstva: Sietová vrstva prenáša dáta linkovej vrstve, ktorá ich zapúzdruje do rámca a pridáva fyzické adresy zariadení na zabezpečenie správnej lokálnej dodávky dát.
- Linková vrstva <-> Fyzická vrstva: Linková vrstva odosiela rámce fyzickej vrstve, ktorá ich konvertuje na signály pre prenos po fyzickom médiu, ako sú napríklad elektrické impulzy cez kábel alebo rádiové vlny cez bezdrôtové spojenie.

Takto sa dá postupovať cez jednotlivé vrstvy modelu OSI, pričom každá vrstva pridáva svoje vlastné hlavičky alebo informácie a prenáša dáta dole a nahor v sieti. Tento proces umožňuje efektívnu komunikáciu medzi rôznymi zariadeniami v sieti.

#### - **popíšte proces encapsulácie a deencapsulácie**

##### - Encapsulácia:

- Na odosielateľskom konci: Keď dáta opúšťajú aplikačnú vrstvu, sú postupne prenášané cez vrstvy modelu OSI. Každá vrstva pridáva svoju vlastnú hlavičku alebo záhlavie (header) k existujúcim dátam. Tento proces obalenia dát vrstvami modelu OSI sa nazýva encapsulation.
- Príklad: Keď aplikácia na odosielateľskom konci pošle dáta, tieto dáta sú najskôr prijaté aplikačnou vrstvou. Aplikačná vrstva pridá hlavičku, ktorá obsahuje informácie o typu aplikácie alebo služby. Potom tieto dáta prejdú do transportnej vrstvy, kde sa pridávajú informácie ako zdrojový a cieľový port. Tento proces pokračuje až kým dáta neprejdú cez všetky vrstvy a sú pripravené na odoslanie na sieť.

##### - Deencapsulácia:

- Na prijímajúcom konci: Keď obalené dáta prídu na prijímajúcom konci, prechádzajú opačným procesom. Každá vrstva odstraňuje svoju vlastnú hlavičku a odovzdáva dáta vrstve vyššie. Tento proces sa nazýva deencapsulation.
- Príklad: Keď obalené dáta prídu na sieťovú kartu na prijímajúcom konci, fyzická vrstva odstráni fyzickú adresu a odovzdá rámec linkovej vrstve. Linková vrstva potom odstráni linkovú adresu a odovzdá dáta sietovej vrstve. Sietová vrstva potom odstráni adresu IP a odovzdá dáta

transportnej vrstve a tento proces pokračuje, kým dáta nedosiahnu aplikačnú vrstvu na prijímajúcom konci.

Takto encapsulácia a deencapsulácia umožňujú dátam prechádzať cez rôzne vrstvy modelu OSI a zachovať integritu a správnu štruktúru dát počas komunikácie v počítačových sieťach.

- **vysvetlite pojem PDU**

PDU (Protocol Data Unit) je základná jednotka dát, ktorá sa prenáša cez počítačovú sieť v rámci určitého protokolu. Každá vrstva modelu sieťovej architektúry (ako napríklad model OSI alebo TCP/IP) používa svoju vlastnú PDU na prenos údajov, pričom každá PDU obsahuje určité informácie potrebné pre túto vrstvu.

Tu je vysvetlenie toho, čo PDU predstavuje v jednotlivých vrstvách modelu OSI:

Fyzická vrstva:

- V PDU fyzickej vrstvy sa nachádzajú jednoducho fyzické bity, ktoré sa prenášajú cez fyzický médium, ako sú napríklad elektrické signály alebo svetelné pulzy.

Linková vrstva:

- PDU linkovej vrstvy sa nazýva rámec (frame). Rámec zahŕňa dáta a riadiace informácie ako zdrojovú a cieľovú fyzickú adresu MAC (Media Access Control) a kontrolné súčty pre detekciu chýb v prenose dát.

Sietová vrstva:

- PDU sieťovej vrstvy sa nazýva paket (packet). Paket obsahuje dáta (často v podobe segmentov alebo datagramov) a informácie o zdrojovej a cieľovej logickú adresu IP, ako aj ďalšie informácie potrebné pre doručenie paketu cez sieť.

Transportná vrstva:

- PDU transportnej vrstvy sa nazýva segment (segment). Segment zahŕňa dáta z aplikačnej vrstvy a informácie o portoch zdroja a cieľa, ako aj kontrolné súčty pre spoľahlivý prenos dát.

Aplikačná vrstva:

- V aplikačnej vrstve sa PDU nazýva správa alebo jednoducho dáta. Tieto dáta sú určené na spracovanie koncovými aplikáciami a zvyčajne obsahujú užitočné informácie, ako sú textové alebo multimediálne dáta.

PDU je teda základnou jednotkou dát, ktorá sa používa v každej vrstve sieťovej architektúry na správne doručenie a spracovanie údajov v sieti. Každá vrstva pridáva svoje vlastné riadiace informácie k existujúcim dátam, aby sa zabezpečila správna komunikácia medzi zariadeniami v sieti.

- **porovnajte hlavičky PDU Frame a Packet**

Hlavičky PDU (Protocol Data Unit) pre rámec (Frame) a paket (Packet) sa líšia v závislosti na vrstve modelu sieťovej architektúry, ktorou prechádzajú. Tu je porovnanie hlavičiek pre rámec a paket vo vrstvách modelu OSI:

Hlavička PDU rámca (Frame):

- Fyzická vrstva (Layer 1): V závislosti od použitého typu fyzického média môžu obsahovať rôzne informácie, ako napríklad synchronizačné bity, adresu zdroja a adresu cieľa, kontrolné bity na detekciu chýb, dĺžku rámca atď. Napríklad v Ethernet rámcach je typická dĺžka rámca 64 až 1518 bytov.
- Linková vrstva (Layer 2): Hlavička rámca linkovej vrstvy obsahuje MAC adresu zdroja a cieľa (6 bytov každá), typ rámca (napríklad Ethernet II, IEEE 802.3) a prípadne ďalšie riadiace informácie, ako napríklad kontrolný súčet (FCS - Frame Check Sequence).

Hlavička PDU paketu (Packet):

- Sietová vrstva (Layer 3): Hlavička paketu sietovej vrstvy obsahuje IP adresu zdroja a cieľa (typicky 4 byty každá), informácie o verzii IP protokolu, dĺžka paketu, číslo fragmentu (ak je paket fragmentovaný), identifikátor protokolu a kontrolný súčet pre verifikáciu správnosti paketu.
- Transportná vrstva (Layer 4): Nie je priamo súčasťou hlavičky PDU paketu, ale dôležité informácie sa nachádzajú v hlavičkách segmentov transportnej vrstvy (napríklad v prípade TCP hlavička obsahuje porty zdroja a cieľa, sekvenčné a potvrdzovacie čísla a kontrolný súčet).

Porovnanie:

- Adresy: V hlavičke PDU rámca sú MAC adresy, zatiaľ čo v hlavičke PDU paketu sú IP adresy.
- Vrstvy: Hlavička rámca je vytvorená na linkovej vrstve, zatiaľ čo hlavička paketu je vytvorená na sietovej vrstve.
- Kontrola chýb: Hlavička rámca obsahuje kontrolný súčet (FCS) pre detekciu chýb na fyzickom médiu, zatiaľ čo hlavička paketu obsahuje kontrolný súčet IP pre overenie integrity dát paketu.
- Veľkosť: Hlavička rámca má fixnú veľkosť, zatiaľ čo veľkosť hlavičky paketu môže byť rôzna v závislosti od verzie IP protokolu a ďalších parametrov.

Takéto rozdiely v hlavičkách PDU rámca a paketu sú dôležité pre správne doručenie dát v počítačových sieťach.

- **zdôvodnite potrebu použitia verejných a privátnych IP adries v IPv4 a úlohu NAT**

Použitie verejných a privátnych IP adries v IPv4 súvisí s efektívnym spravovaním a alokáciou IP adries v rámci globálnej siete. Tu je zdôvodnenie pre ich použitie a úlohu sieťovej adresácie s použitím NAT (Network Address Translation):

Verejné IP adresy:

- Verejné IP adresy sú jedinečné adresy priradené organizáciám alebo zariadeniam a sú určené na použitie na internete. Tieto adresy musia byť jedinečné a globálne unikátne, aby bolo možné zabezpečiť jednoznačnú identifikáciu zariadení na celom internete.

Privátne IP adresy:

- Privátne IP adresy sú adresy priradené zariadeniam vo vnútorných súkromných sieťach, ako sú domáce siete alebo podnikové intranety. Tieto adresy sú zvyčajne priradené z rozsahu adries určeného pre privátne použitie (napríklad rozsahy 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12).
- Privátne IP adresy nie sú jedinečné globálne a môžu byť opakovane použité v rôznych súkromných sieťach, pretože sú izolované od internetu. To umožňuje efektívne využitie adresného priestoru a umožňuje zariadeniam vo vnútri siete komunikovať medzi sebou bez potreby verejných IP adries.

NAT (Network Address Translation):

- NAT je sieťová technika, ktorá umožňuje preklad IP adries medzi verejnými a privátnymi adresami. NAT sa používa na prekladanie súkromných adries na verejné adresy, keď zariadenia v súkromnej sieti komunikujú s internetom a naopak.
- Keď zariadenie vo vnútri súkromnej siete odosiela požiadavku na internet, NAT preloží zdrojovú privátnu adresu na verejnú adresu, ktorá je schopná komunikovať cez internet. Tým sa umožní, aby viacero zariadení vo vnútri siete používalo jedinou verejnú IP adresu na prístup na internet.
- NAT tiež zabezpečuje bezpečnosť súkromných sietí tým, že skrýva skutočné adresy zariadení vo vnútri siete pred vonkajším svetom, čím sa znižuje riziko útokov alebo neoprávneného prístupu.

Celkovo použitie verejných a privátnych IP adries spolu s NAT umožňuje efektívne využívať adresný priestor IPv4 a zabezpečuje, že súkromné siete môžu komunikovať s internetom, pričom zároveň chránia súkromie a bezpečnosť interných zariadení.

- **uved'te aspoň dve organizácie zodpovedné za otvorené štandardy v sieťach**

Dve z organizácií zodpovedných za otvorené štandardy v oblasti počítačových sietí sú:

Internet Engineering Task Force (IETF):

- IETF je organizačný zbor, ktorý sa zaoberá vývojom a štandardizáciou internetových protokolov a technológií. Jeho cieľom je zabezpečiť interoperabilitu a efektívnosť internetových sietí. IETF vytvára a udržiava mnoho štandardov, vrátane protokolov ako TCP/IP, HTTP, SMTP, DNS a mnohých ďalších.

Institute of Electrical and Electronics Engineers (IEEE):

- IEEE je celosvetová profesijná organizácia zameraná na vývoj a štandardizáciu technológií v oblasti elektroniky a informačných

technológií. V rámci svojich pracovných skupín a technických výborov IEEE vypracúva štandardy v mnohých oblastiach, vrátane počítačových sietí. Medzi známe sieťové štandardy IEEE patria napríklad štandardy Ethernet (napr. IEEE 802.3) a bezdrôtové siete Wi-Fi (napr. IEEE 802.11).

Tieto organizácie hrajú kľúčovú úlohu pri vytváraní a udržiavaní otvorených štandardov, ktoré umožňujú interoperabilitu a rozvoj počítačových sietí a internetu po celom svete.

- **porovnajzte halfduplex a fullduplexz pohľadu použitého média**

Half-duplex a full-duplex sú dva režimy prenosu dát v počítačových sieťach, ktoré ovplyvňujú spôsob, ako zariadenia komunikujú medzi sebou. Ich hlavný rozdiel spočíva v tom, ako je médium (napríklad kábel alebo bezdrôtové spojenie) využívané pre komunikáciu. Tu je porovnanie týchto dvoch režimov pohľadom na použité médium:

Half-duplex:

- V half-duplex režime môže zariadenie posilať alebo prijímať dáta, ale nie sú schopné robiť oboje súčasne. To znamená, že médium môže byť použité len na jednosmernú komunikáciu v každom okamihu.
- V typickom prípade sa half-duplex často využíva v sieťových prostrediach, kde sa používajú kolízne domény, ako napríklad v starších Ethernetových sieťach na odpojenie dobových hubov (koncentrátorov), ktoré zdieľajú spoločné médium.
- Príkladom half-duplex zariadenia je staršie Ethernetové rozhranie na káblovom pripojení, kde nie je možné súčasne posilať a prijímať dáta na jednom vodiči.

Full-duplex:

- V full-duplex režime sú zariadenia schopné posilať a prijímať dáta súčasne, čo znamená, že médium je využívané v oboch smeroch naraz.
- Full-duplex sa často využíva v moderných sieťových technológiách, ako sú switche a moderné Ethernetové rozhrania. Tento režim umožňuje výrazné zvýšenie priepustnosti a efektivity siete, pretože zariadenia môžu komunikovať nezávisle od seba.
- Príkladom full-duplex zariadenia je moderný switch s plnou duplexnou komunikáciou medzi jeho portami, ktoré umožňuje súčasné posielanie a prijímanie dát bez kolízií.

Celkovo, half-duplex a full-duplex režimy poskytujú rôzne možnosti pre komunikáciu v počítačových sieťach v závislosti od použitého média a zariadení. Full-duplex je často preferovaný v moderných sieťových prostrediach kvôli jeho výhodám v rýchlosti a efektívite komunikácie.

- **vysvetlite využitie protokolov pre IPTV a HTTP**

IPTV (Internet Protocol Television) a HTTP (Hypertext Transfer Protocol) sú dva rôzne protokoly, ktoré sa používajú na poskytovanie a prenos obsahu cez internet. Tu je vysvetlenie ich využitia:

Protokoly pre IPTV:

- IPTV je služba, ktorá umožňuje distribúciu televíznych programov a videí pomocou internetového protokolu IP. Pre prenos a správu týchto médií sú využívané rôzne protokoly v rámci IPTV technológie.
- Multicastové protokoly: IPTV často využíva multicastové protokoly, ktoré umožňujú distribúciu obsahu zo servera na viacero príjemcov súčasne. Tento prístup znižuje sieťovú prevádzku a záťaž na serveri. Typické multicastové protokoly používané v IPTV sú napríklad IGMP (Internet Group Management Protocol) pre riadenie multicastového toku a UDP (User Datagram Protocol) pre prenos datagramov.
- Protokol IPTV: Existujú špecifické protokoly navrhnuté pre IPTV, ako napríklad RTP (Real-time Transport Protocol) na prenos audiovizuálneho obsahu v reálnom čase. RTP zabezpečuje správne doručenie multimediálnych dát bez straty a oneskorenia, čo je kritické pre sledovanie televíznych programov v reálnom čase.

HTTP (Hypertext Transfer Protocol):

- HTTP je základný protokol používaný na prenos hypertextových dokumentov na internete. Napriek tomu, že je primárne určený pre prenos webových stránok, HTTP sa v dnešnej dobe používa na prenos rôznych typov dát, vrátane médií a streamovaného obsahu.
- Streamovanie médií: HTTP streamovanie je technika, ktorá umožňuje prenos audiovizuálneho obsahu pomocou HTTP protokolu. Tento prístup je často nazývaný aj "HTTP Live Streaming" (HLS) alebo "HTTP Adaptive Streaming" (HAS). V tomto prípade je obsah rozdelený na malé segmenty, ktoré sú požadované klientom pomocou štandardných HTTP požiadaviek. Tento spôsob streamovania umožňuje adaptáciu na meniacu sa sieťovú kapacitu a rôzne rýchlosti pripojenia klienta.

Celkovo, protokoly pre IPTV a HTTP sa využívajú na poskytovanie a prenos rôznych typov obsahu cez internet, pričom každý z nich má svoje vlastné vlastnosti a využitie v závislosti od konkrétnej aplikácie a požiadaviek na službu. IPTV sa často používa na distribúciu televíznych programov a videí v reálnom čase, zatiaľ čo HTTP sa používa na streamovanie médií a ďalší obsah na internete.

- **uved'te výhody a nevýhody jednotlivých zdrojov a metód získavania nových zamestnancov v podniku**

Získavanie nových zamestnancov je kľúčovým procesom pre každý podnik. Existuje niekoľko zdrojov a metód, ako podniky môžu získať nových zamestnancov, pričom každá má svoje výhody a nevýhody:

Interné zdroje a metódy:

- *Referencie od súčasných zamestnancov:*
  - *Výhody:* Tento spôsob získavania zamestnancov môže byť efektívny, pretože súčasní zamestnanci môžu odporúčať



kvalifikovaných kandidátov a môžu mať lepšiu predstavu o kultúre a požiadavkách firmy.

- *Nevýhody:* Existuje riziko zvýhodňovania známych pred inými kvalifikovanými kandidátmi a riziko vzniku homogénnej pracovnej sily.
- *Interné presuny a povýšenia:*
  - *Výhody:* Presuny a povýšenia interných zamestnancov môžu motivovať a udržať zamestnancov, pretože zvyšujú vnútornú mobilitu a dávajú zamestnancom cestu na rozvoj v rámci spoločnosti.
  - *Nevýhody:* Môže sa vyskytnúť nedostatok nových myšlienok a perspektív, ak sa spoločnosť príliš veľmi spolieha na existujúcu pracovnú silu.

Externé zdroje a metódy:

- *Inzeráty na pracovné pozície:*
  - *Výhody:* Inzeráty môžu prilákať širokú škálu záujemcov a umožniť podniku vybrať najlepších kandidátov.
  - *Nevýhody:* Inzeráty môžu byť nákladné a neefektívne, ak neposkytujú dostatočný vzhľad do kultúry a požiadaviek spoločnosti.
- *Spolupráca so zamestnaneckými agentúrami a headhuntermi:*
  - *Výhody:* Agentúry a headhunteri môžu mať prístup k širšiemu bazénu talentov a môžu poskytnúť vyššiu kvalitu kandidátov.
  - *Nevýhody:* Tieto služby môžu byť veľmi drahé a môžu mať tendenciu zameriavať sa len na určité profily kandidátov.
- *Práca na univerzitách a job mesece:*
  - *Výhody:* Tieto udalosti poskytujú možnosť priameho kontaktu so študentmi a mladými profesionálmi, ktorí hľadajú príležitosti na začiatok kariéry.
  - *Nevýhody:* Výber môže byť obmedzený na študentov alebo absolventov určitých škôl alebo programov.

Každá z týchto metód má svoje miesto a môže byť účinná v určitých situáciách. Pre úspešné získavanie nových zamestnancov je dôležité, aby podniky zvážili svoje potreby a možnosti a zvolili najvhodnejšie stratégie pre svoju situáciu.

## **POROVNANIE SIETÍ PAN, LAN, WLAN, MAN, WAN**

### **- definujte siete PAN, LAN, WLAN, MAN, WAN**

Tu sú definície pre jednotlivé typy sietí:

- PAN (Personal Area Network):
  - PAN je sieť, ktorá zahŕňa zariadenia nachádzajúce sa v blízkom okolí jedného používateľa. Tieto siete majú malý dosah a slúžia na komunikáciu medzi osobnými zariadeniami, ako sú napríklad počítače, mobilné telefóny, tlačiarne, osobné digitálne asistenty (PDA) a ďalšie. Príklady technológií PAN zahŕňajú Bluetooth a infraport.

- LAN (Local Area Network):
  - o LAN je sieť, ktorá sa rozprestiera na relatívne malom území, ako je budova, kancelária, škola alebo domácnosť. LAN umožňuje zdieľanie zdrojov a komunikáciu medzi zariadeniami nachádzajúcimi sa v rovnakej geografickej oblasti. Príklady zariadení v LAN zahŕňajú počítače, tlačiarne, servery, switche a routery.
- WLAN (Wireless Local Area Network):
  - o WLAN je bezdrôtová verzia LAN, ktorá umožňuje pripojenie zariadení k sieti bez použitia káblov. Tieto siete sú často využívané v domácnostiach, kanceláriách, verejných priestoroch a podobne. Príklady technológií WLAN zahŕňajú Wi-Fi a IEEE 802.11 štandardy.
- MAN (Metropolitan Area Network):
  - o MAN je sieť, ktorá sa rozprestiera na väčšom geografickom území, ako je mesto alebo metropolitná oblasť. MAN zvyčajne poskytuje vysokú rýchlosť pre prenos dát a je používaná na pripojenie viacerých lokálnych sietí (LAN) v rozsiahlej geografickej oblasti. Príkladom MAN môže byť káblová televízia alebo optické vlákna používané poskytovateľmi internetových služieb.
- WAN (Wide Area Network):
  - o WAN je sieť, ktorá sa rozprestiera na veľkom geografickom území, často cez štátne hranice alebo dokonca globálne. WAN umožňuje komunikáciu medzi vzdialenými lokálnymi sieťami (LAN) alebo medzi zariadeniami nachádzajúcimi sa na veľkých vzdialenostiach. Príklady WAN zahŕňajú internet, globálne telekomunikačné siete a siete spravované poskytovateľmi telekomunikačných služieb.

#### - **načrtnite niektoré topológie sietí**

Tu sú niektoré základné topológie sietí:

- Hviezdicová topológia:
  - o V hviezdicovej topológii sú všetky zariadenia pripojené priamo k centrálnemu uzlu, ktorý sa nazýva hub alebo switch. Všetky komunikácie medzi zariadeniami prechádzajú cez tento centrálny uzol. Táto topológia je jednoduchá na správu a rozšírenie, ale v prípade zlyhania centrálného uzla môže dôjsť k výpadkom celej siete.
- Kruhová (Ring) topológia:
  - o V kruhovej topológii sú zariadenia pripojené do kruhu, pričom každé zariadenie je pripojené priamo k dvom susedným zariadeniam. Dáta sa prenášajú v jednom smere po kruhu. Táto topológia je jednoduchá a spoľahlivá, ale môže byť náchylná na výpadky v prípade, že sa poruší jeden z káblov alebo zariadení.
- Rozvetvená (Bus) topológia:
  - o V rozvetvenej topológii sú všetky zariadenia pripojené k jednému hlavnému káblu, ktorý sa nazýva trunk alebo backbone. Každé zariadenie zdieľa rovnaké médium pre prenos dát. Ak je kábel alebo zariadenie poškodené, môže to viesť k výpadku celej siete.
- Stromová (Tree) topológia:
  - o Stromová topológia kombinuje vlastnosti hviezdicovej a rozvetvenej topológie. Zariadenia sú usporiadané do hierarchickej štruktúry podobnej stromu, kde

každé zariadenie je pripojené k centrálnemu uzlu alebo vetve. Táto topológia umožňuje jednoduchú správu a škálovateľnosť.

- Mesh (Mriežková) topológia:

- V mriežkovej topológii sú všetky zariadenia pripojené priamo ku každému inému zariadeniu v sieti. Táto topológia poskytuje vysokú spoľahlivosť a redundantnosť, pretože v prípade výpadku jedného spojenia sa dáta môžu prenášať alternatívnou cestou. Mriežková topológia je však nákladná na implementáciu a správu.

- **porovnajte siete typu client - server a sietí peer – to - peer**

Siete typu klient-server a siete typu peer-to-peer (P2P) sú dva hlavné modely distribúcie zdrojov a komunikácie v počítačových sieťach. Tu je porovnanie medzi nimi:

Client-Server:

- Charakteristika: V sieti typu klient-server sú zdroje a služby zväčša centralizované a umiestnené na centrálnej serverovej stanici, ktorá poskytuje zdroje klientom na vyžiadanie.
- Rozloženie úloh: Centrálny server poskytuje zdroje a služby, zatiaľ čo klienti žiadajú o tieto zdroje a služby a používajú ich.
- Bezpečnosť: Centrálny server môže poskytovať lepšiu kontrolu prístupu a zabezpečenie, pretože je možné implementovať centralizované politiky zabezpečenia.
- Výhody: Centralizovaný prístup umožňuje efektívne spravovať a kontrolovať zdroje a poskytovať centralizovanú podporu a údržbu. Je vhodný pre podnikové prostredia alebo veľké webové aplikácie.
- Nevýhody: Môže vzniknúť jediný bod zlyhania, keďže všetka komunikácia a zdroje sú závislé od centrálného servera.

Peer-to-Peer (P2P):

- Charakteristika: V sieti typu peer-to-peer sú zdroje distribuované medzi všetkými počítačmi alebo zariadeniami v sieti, čím každé zariadenie môže byť súčasne klientom aj serverom.
- Rozloženie úloh: V P2P sieti každé zariadenie zdieľa zdroje, ako sú súbory alebo výpočtová sila, a súčasne môže pristupovať k zdrojom, ktoré sú zdieľané inými zariadeniami v sieti.
- Bezpečnosť: Bezpečnosť v P2P sieťach je ťažšie riadiť, pretože zdieľané zdroje môžu byť dostupné pre všetkých účastníkov siete, a nie je možné implementovať centrálnu kontrolu prístupu.
- Výhody: V P2P sieťach je zvýšená odolnosť voči výpadkom, pretože neexistuje jediný bod zlyhania. Tento model je vhodný pre aplikácie s distribuovanou architektúrou, ako sú súbory zdieľané medzi používateľmi alebo distribuované výpočty.
- Nevýhody: Ťažšia správa a kontrola, zložitejšie vyhľadávanie zdrojov a môže dôjsť k problémom s autorskými právami alebo nelegálnym obsahom.

V závislosti od konkrétnych potrieb a požiadaviek na aplikáciu môže byť vhodnejší jeden model siete alebo druhý. Klient-server model je vhodný pre centralizované správy a kontroly, zatiaľ čo

P2P model je lepší pre distribuované prostredia s väčšou odolnosťou voči výpadkom a decentralizovanou povahou zdieľaných zdrojov.

- **popíšte jednotlivé komponenty sietí**

Siete pozostávajú z niekoľkých kľúčových komponentov, ktoré spoločne umožňujú komunikáciu, zdieľanie zdrojov a poskytovanie služieb. Tu je popis niektorých hlavných komponentov sietí:

Zariadenia:

- Zariadenia tvoria koncové body siete a môžu zahŕňať počítače, servery, tlačiarne, telefóny, routery, switche, access pointy a ďalšie. Tieto zariadenia slúžia na spracovanie, ukladanie, zdieľanie a prenos dát v sieti.

Mediá:

- Mediá sú fyzické médiá alebo bezdrôtové prostriedky, cez ktoré sa prenášajú dáta medzi zariadeniami v sieti. Mediá môžu zahŕňať káblové médiá, ako sú koaxiálne káble, vláknové optické káble alebo twisted-pair káble, ako aj bezdrôtové médiá, ako je elektromagnetické spektrum pre Wi-Fi alebo mikrovlnné prenosy.

Protokoly:

- Protokoly sú súbor pravidiel a postupov, ktoré určujú, ako sa dáta prenášajú, spracovávajú a komunikujú v sieti. Protokoly definujú formát dátových paketov, adresáciu, spôsoby detekcie chýb, routovanie a iné aspekty komunikácie v sieti.

Služby:

- Služby sú funkcie a možnosti, ktoré sú poskytované používateľom alebo aplikáciám v sieti. Môžu zahŕňať zdieľanie súborov, tlač, prístup k internetu, e-mail, videohovory, streamovanie médií a mnoho ďalších.

Routery a switche:

- Routery a switche sú sieťové zariadenia, ktoré smerujú a prepájajú dátové pakety v sieti. Routery sú zodpovedné za prenos dát medzi rôznymi sieťami a rozhodujú o najlepšej ceste pre prenos dát. Switche fungujú na úrovni lokálnej siete a prepájajú zariadenia v rovnakej sieti.

Protokolové koncové body:

- Protokolové koncové body sú softvérové alebo hardvérové komponenty, ktoré implementujú určité sieťové protokoly a zabezpečujú komunikáciu medzi rôznymi zariadeniami v sieti. Tieto koncové body môžu zahŕňať napríklad sieťové adaptéry, softvérové aplikácie alebo sieťové rozhrania zariadení.

Tieto komponenty spoločne tvoria sieťové prostredie, ktoré umožňuje spoľahlivú komunikáciu a zdieľanie zdrojov medzi rôznymi zariadeniami a používateľmi v sieti. Každý komponent má svoju špecifickú úlohu a prispieva k celkovej funkčnosti a výkonnosti siete.

- **načrtnite zariadenia ktoré používame v LAN a WAN**

Tu je prehľad niektorých zariadení, ktoré sa bežne používajú v LAN (Local Area Network) a WAN (Wide Area Network):

**\*\*Zariadenia v LAN:\*\***

1. **\*\*Switch:\*\***

- Switche sú zariadenia, ktoré umožňujú lokálne prepájanie zariadení v LAN. Slúžia na posielanie dátových rámcov medzi zariadeniami vo vnútri LAN podľa MAC adres.

2. **\*\*Router:\*\***

- Routery sa často používajú v LAN na rozdeľovanie siete na podrobnosti a na posielanie dát medzi rôznymi LAN alebo medzi LAN a inými sieťami.

3. **\*\*Access Point (AP):\*\***

- Access Pointy umožňujú bezdrôtovým zariadeniam pripojiť sa k LAN. Sú zodpovedné za vytvorenie bezdrôtovej siete a poskytujú pripojenie pre mobilné zariadenia a iné bezdrôtové klienty.

4. **\*\*Hub:\*\***

- Huby sú zariadenia, ktoré umožňujú pripojenie viacerých zariadení do LAN. Huby však nie sú schopné inteligentne rozhodovať o prenose dát a jednoducho posielajú dáta na všetky pripojené zariadenia.

**\*\*Zariadenia v WAN:\*\***

1. **\*\*Router:\*\***

- Routery sú kľúčové zariadenia v WAN, ktoré umožňujú pripojenie k rôznym sieťovým zariadeniam a prenos dát medzi nimi cez veľké vzdialenosti.

2. **\*\*Modem:\*\***

- Modemy sú zariadenia, ktoré umožňujú pripojenie k internetu alebo iným sieťam WAN. Existujú rôzne typy modemov, ako sú DSL modemy, kábelové modemy alebo bezdrôtové modemy, ktoré sa používajú na rôzne typy pripojení.

3. **\*\*CSU/DSU (Channel Service Unit / Data Service Unit):\*\***

- CSU/DSU je zariadenie, ktoré sa často používa na pripojenie k telefonickej linke alebo T1/E1 linky poskytovateľa služieb WAN. CSU/DSU prevádza dátové rámce na formáty, ktoré sú vhodné pre prenos po linke WAN.

4. **\*\*Multiplexer/Demultiplexer:\*\***

- Multiplexéry a demultiplexéry sú zariadenia, ktoré umožňujú zoskupovať viacero dátových kanálov do jedného prenosového média a naopak. Používajú sa na optimalizáciu prenosu dát v WAN.

- **porovnajte konvergované siete a tradičné oddelené siete**

Konvergované siete a tradičné oddelené siete predstavujú dva rozdielne prístupy k architektúre sietí. Tu je porovnanie medzi nimi:

## 1. **\*\*Konvergované siete:\*\***

- **\*\*Charakteristika:\*\*** Konvergované siete kombinujú dátovú, hlasovú a video komunikáciu do jednej siete. Tento prístup eliminuje potrebu oddelených sietí pre jednotlivé typy komunikácie a umožňuje zdieľanie infraštruktúry a zdrojov.

- **\*\*Výhody:\*\***

- Jednoduchšia správa a údržba: Jednotná infraštruktúra umožňuje jednoduchšiu správu a údržbu siete.

- Nízke náklady: Zdieľanie infraštruktúry a zdrojov vedie k nižším nákladom na prevádzku a správu siete.

- Flexibilita: Konvergované siete umožňujú rýchlu adaptáciu a prispôsobenie sa meniacim sa potrebám podniku alebo organizácie.

- **\*\*Nevýhody:\*\***

- Bezpečnosť: Konvergované siete môžu mať vyššie bezpečnostné riziká, pretože útok na jednu časť siete môže ovplyvniť všetky typy komunikácie.

- Špecifické požiadavky na prevádzku: Niektoré aplikácie, ako napríklad hlasová komunikácia, môžu vyžadovať špecifické požiadavky na sieťovú prevádzku, ktoré môžu ovplyvniť výkon a kvalitu služby pre ostatné typy komunikácie.

## 2. **\*\*Tradičné oddelené siete:\*\***

- **\*\*Charakteristika:\*\*** Tradičné oddelené siete používajú samostatné siete pre rôzne typy komunikácie, ako sú dátové siete, hlasové siete a videokonferencie. Každá sieť je navrhnutá a spravovaná samostatne.

- **\*\*Výhody:\*\***

- Bezpečnosť: Oddelené siete môžu poskytovať vyššiu úroveň bezpečnosti tým, že izolujú rôzne typy komunikácie.

- Špecializované riešenia: Každá sieť môže byť navrhnutá a optimalizovaná pre konkrétne požiadavky a špecifikácie aplikácie.

- Kvalita služby: Oddelené siete môžu poskytovať lepšiu kvalitu služby pre špecifické typy komunikácie, ako je napríklad hlasová komunikácia.

- **\*\*Nevýhody:\*\***

- Vyššie náklady: Prevádzka a správa oddelených sietí môže byť nákladnejšia v porovnaní s konvergovanými sieťami, pretože vyžaduje viac zdrojov a infraštruktúry.

- Komplexita: Správa viacerých samostatných sietí môže byť zložitejšia a vyžadovať väčšiu expertízu.

Celkovo vzaté, výber medzi konvergovanými a tradičnými oddelenými sieťami závisí od špecifických požiadaviek a potrieb organizácie, ako aj od faktorov ako bezpečnosť, náklady a kvalita služby. Každý prístup má svoje výhody a nevýhody, a preto je dôležité zvážiť ich v kontexte konkrétnej situácie.

### - **vysvetlite intranet, extranet a internet**

Intranet, extranet a internet sú rôzne typy počítačových sietí, ktoré sa používajú na komunikáciu a zdieľanie informácií. Tu je vysvetlenie každého z týchto termínov:

## 1. **\*\*Intranet:\*\***

- Intranet je interná počítačová sieť, ktorá je obmedzená len na interné použitie v rámci organizácie alebo firmy. Slúži na zdieľanie informácií, dokumentov, aplikácií a iných zdrojov medzi zamestnancami alebo oddeleniami v rámci organizácie.

- Typické vlastnosti intranetu zahŕňajú:
  - Prístup len pre autorizovaných používateľov.
  - Interné webové stránky, diskusné fóra, spoločné úložisko dokumentov a aplikácie.
  - Často je chránený firewallom, aby sa zabránilo neoprávnenému prístupu zvonka.

## 2. \*\*Extranet:\*\*

- Extranet je rozšírenie intranetu, ktoré umožňuje vybraným externým používateľom prístup k niektorým častiam intranetu. Extranet umožňuje spoluprácu a výmenu informácií medzi organizáciou a externými partnermi, dodávateľmi, klientmi alebo ďalšími zainteresovanými stranami.

- Typické vlastnosti extranetu zahŕňajú:
  - Autorizovaný prístup pre externých používateľov, ktorí majú oprávnenie na prístup k určitým zdrojom.
  - Zdieľanie dokumentov, komunikácia a spolupráca s externými partnermi.
  - Často je zabezpečený pomocou VPN (Virtual Private Network) alebo iných metód šifrovania pre zabezpečenie dôvernosti a integrity údajov.

## 3. \*\*Internet:\*\*

- Internet je globálna počítačová sieť, ktorá umožňuje komunikáciu medzi množstvom zariadení a používateľov po celom svete. Je to verejná sieť, ktorá umožňuje prístup k informáciám, webovým stránkam, aplikáciám, službám a ďalším zdrojom, ktoré sú dostupné na internete.

- Typické vlastnosti internetu zahŕňajú:
  - Voľný prístup pre všetkých používateľov bez ohľadu na miesto alebo organizáciu.
  - Možnosť prístupu k rôznym zdrojom a informáciám na celom svete.
    - Dostupnosť rôznych služieb a aplikácií, ako sú elektronická pošta, sociálne siete, vyhľadávače, e-commerce a ďalšie.

Tieto typy sietí majú rôzne účely a využitie, pričom intranet a extranet sú zamerané na internú a obmedzenú komunikáciu, zatiaľ čo internet je verejná sieť, ktorá umožňuje komunikáciu po celom svete.

- **ilustrujte na príkladoch, ako efektívne viete využiť ľubovoľné Vami navrhnuté riešenia sietí PAN pri zbere a spracovaní dát v teréne**

Rozmýšľajme o situácii, kde je potrebné zbierať dáta v teréne pomocou rôznych senzorov a zariadení a následne ich spracovať a analyzovať. Pre túto úlohu môžeme využiť siete typu PAN (Personal Area Network), ktoré sú vhodné pre pripojenie zariadení v blízkej fyzickej blízkosti. Tu je niekoľko príkladov, ako by sme mohli efektívne využiť sieť typu PAN v teréne:

Monitorovanie prostredia:

- Predstavme si, že máme sieť senzorov na monitorovanie kvality ovzdušia, pôdy alebo vody v určitom teréne. Každý senzor môže byť pripojený k malému zberaču dát (napr. mikrokontrolér alebo minipočítač) cez bezdrôtové technológie, ako je Bluetooth alebo Zigbee, vytvárajúc tak sieť

typu PAN. Tieto zberače dát môžu byť ďalej pripojené k mobilnému zariadeniu (napr. smartfónu alebo tabletu) prostredníctvom bezdrôtového rozhrania, ako je napríklad Bluetooth. Použitie siete PAN umožňuje pohodlné a efektívne monitorovanie a zber dát v teréne bez potreby vedenia káblov alebo inštalácie infraštruktúry.

Zber geografických údajov:

- V prípade potreby zberu geografických údajov v teréne, ako sú napríklad GPS súradnice, výškové údaje alebo fotografia okolia, môžeme využiť sieť typu PAN. GPS prístroje, fotoaparáty a ďalšie zariadenia môžu byť pripojené k mobilnému zariadeniu cez Bluetooth alebo iné bezdrôtové rozhrania, vytvárajúc tak malú sieť PAN. Toto umožňuje efektívne zber geografických údajov v teréne s možnosťou okamžitého spracovania a analýzy na mobilnom zariadení.

Monitorovanie zdravia a wellness:

- V prípade sledovania zdravotného stavu alebo wellness dát v teréne (napr. pri športových aktivitách alebo na turistických túrach) môžeme využiť nositeľné senzory, ako sú napríklad fitness náramky alebo inteligentné hodinky. Tieto senzory môžu byť pripojené k mobilnému telefónu alebo smartfónu prostredníctvom technológií typu PAN, ako je Bluetooth, umožňujúc tak monitorovanie aktivity, srdcového tepu, spánku a ďalších zdravotných údajov v reálnom čase.

Tieto príklady ukazujú, ako môžeme efektívne využiť siete typu PAN pre zber a spracovanie dát v teréne pomocou bezdrôtových technológií a zariadení. Siete PAN umožňujú rýchlu a flexibilnú komunikáciu medzi zariadeniami v blízkej fyzickej blízkosti, čo je ideálne pre aplikácie v teréne, kde je potrebné mobilné a bezdrôtové riešenia.

#### **- navrhnete najvhodnejšie riešenie na vybudovanie WLAN v domácnosti alebo v kancelárii**

Na vybudovanie WLAN (Wireless Local Area Network) v domácnosti alebo v kancelárii existuje niekoľko faktorov, ktoré treba zvážiť, vrátane veľkosti priestoru, požiadaviek na pripojenie, dostupnosti zariadení a bezpečnostných požiadaviek. Tu je návrh najvhodnejšieho riešenia:

##### **1. \*\*Router s integrovaným bezdrôtovým prístupovým bodom (AP):\*\***

- Začnite s nákupom kvalitného routera, ktorý má integrovaný bezdrôtový prístupový bod (AP). Takýto router poskytne spoľahlivé pripojenie k internetu a súčasne umožní bezdrôtové pripojenie pre vaše zariadenia v domácnosti alebo kancelárii.

- Zabezpečte, aby router bol kompatibilný s najnovšími bezdrôtovými štandardmi (napr. Wi-Fi 6) a mal dostatočný dosah a rýchlosť, aby pokryl celý priestor.

##### **2. \*\*Rozmiestnenie AP a optimalizácia signálu:\*\***

- Umiestnite router s AP na miesto, ktoré je vo vašom dome alebo kancelárii centrálnym a vysoko dostupným. Ideálne umiestnenie je vo vyvýšenom mieste voľne v priestore, aby sa minimalizovali prekážky pre signál.

- Ak je vaša domácnosť alebo kancelária väčšia, môžete použiť viacero AP umiestnených strategicky po celej oblasti, aby ste zabezpečili rovnomerné pokrytie signálu.



### 3. **\*\*Zabezpečenie siete:\*\***

- Aktivujte bezpečnostné funkcie vo vašom routeri, ako sú WPA2/WPA3 šifrovanie, heslovaný prístup a filtrovanie MAC adries. Tieto kroky pomôžu chrániť vašu sieť pred neoprávneným prístupom.

- Zmena predvolených hesiel a názvov siete (SSID) tiež prispieva k zvýšeniu bezpečnosti siete.

### 4. **\*\*Správa siete:\*\***

- Použite aplikáciu alebo webové rozhranie vášho routera na správu siete, monitorovanie pripojených zariadení a konfiguráciu nastavení siete podľa vašich potrieb.

- Pravidelná aktualizácia firmvéru vášho routera môže zabezpečiť, že vaša sieť bude chránená pred známymi bezpečnostnými chybami a bude fungovať s najnovšími štandardmi a technológiami.

Týmto spôsobom navrhnuté riešenie poskytuje spoľahlivé a bezpečné bezdrôtové pripojenie pre vašu domácnosť alebo kanceláriu s minimálnymi nákladmi a úsilím. Dôležité je venovať pozornosť správneho rozmiestneniu zariadení, zabezpečeniu siete a pravidelnej údržbe a aktualizáciám, aby sa zabezpečila optimálna výkonnosť a bezpečnosť siete.

#### **- vytvorte cenovú ponuku vami navrhnuť siete WLAN**

Na základe predchádzajúceho návrhu siete WLAN v domácnosti alebo v kancelárii, tu je cenová ponuka s odhadom nákladov na základe typických cien dostupných zariadení na trhu:

#### 1. **\*\*Router s integrovaným bezdrôtovým prístupovým bodom (AP):\*\***

- Cenový rozsah: \$50 - \$150 USD

- Odporúčaný model: TP-Link Archer A7 (v cenovom rozpätí \$50 - \$60 USD) alebo Asus RT-AC66U B1 (v cenovom rozpätí \$100 - \$120 USD)

#### 2. **\*\*Prípadné ďalšie prístupové body (AP):\*\***

- Ak je potrebné viacero AP pre pokrytie väčšej oblasti, cena ďalších prístupových bodov sa môže pohybovať medzi \$50 - \$150 USD za kus, v závislosti od modelu a funkcií.

#### 3. **\*\*Zabezpečenie siete:\*\***

- Ceny štandardných sieťových zabezpečovacích funkcií (WPA2/WPA3 šifrovanie, filtrovanie MAC adries) sú zahrnuté v cene routera.

- Prípadné dodatočné náklady na softvér alebo služby sú minimálne.

Celková cena vybudovania siete WLAN v domácnosti alebo v kancelárii sa môže pohybovať v rozmedzí medzi \$50 až \$300 alebo viac, v závislosti od počtu prístupových bodov potrebných na pokrytie oblasti, zvoleného modelu routera a ďalších prípadných doplnkových služieb alebo zariadení. Celková cena môže byť ovplyvnená aj faktormi ako zľavy, ponuky alebo individuálne preferencie zákazníka pri výbere konkrétnych zariadení.

# ADAPTÉRY POČÍTAČOVÝCH SIETÍ

## - popíšte typy sieťových kariet

Existuje niekoľko typov sieťových kariet, ktoré sa líšia v závislosti od použitia, technológie a rozhrania. Tu sú niektoré z najbežnejších typov:

Ethernetové karty (NICs):

- Ethernetové karty sú najčastejšie používané sieťové karty v počítačových sieťach. Používajú štandardný Ethernetový protokol na prenos dát a sú k dispozícii v rôznych formátoch, vrátane PCI, PCIe, USB a integrovaných na základných doskách.

Wi-Fi adaptéry:

- Wi-Fi adaptéry, tiež nazývané bezdrôtové karty, umožňujú pripojenie počítača k bezdrôtovej sieti (Wi-Fi). Existujú vo forme PCI, PCIe, USB a integrovaných riešení. Wi-Fi adaptéry používajú rôzne štandardy Wi-Fi, ako sú 802.11n, 802.11ac alebo 802.11ax.

Bluetooth adaptéry:

- Bluetooth adaptéry umožňujú pripojenie počítača k zariadeniam s podporou Bluetooth, ako sú klávesnice, myši, slúchadlá a ďalšie periférne zariadenia.

Modemové karty:

- Modemové karty boli v minulosti bežné pre pripojenie k internetu cez telefónnu linku. Dnes sú menej časté kvôli rozšíreniu širšieho pásma a vysoko rýchlostného pripojenia.

Fiber Optic adaptéry:

- Fiber Optic adaptéry sú určené pre použitie v optickej počítačovej sieti. Používajú optickej vlákno na prenos dát, čo umožňuje veľmi vysoké rýchlosti prenosu a väčšiu odolnosť voči rušeniu.

Token Ring adaptéry:

- Token Ring adaptéry boli kedysi používané v počítačových sieťach s topológiou Token Ring. Dnes sú zastarané a zriedkavo sa používajú.

InfiniBand adaptéry:

- InfiniBand adaptéry sú určené pre vysokovýkonné výpočtové a dátové centrá. Používajú štandard InfiniBand na prenos dát s vysokou priepustnosťou a nízkou latenciou.

Powerline adaptéry:

- Powerline adaptéry umožňujú využívať elektrické vedenie v budove na prenos dát. Tieto adaptéry sú vhodné pre pripojenie zariadení k sieti, ak nie je možné alebo žiaduce použiť Wi-Fi alebo káblové pripojenie.

Každý typ sieťovej karty má svoje vlastné výhody a nevýhody a je určený pre špecifické použitie a prostredie. Je dôležité vybrať si správny typ sieťovej karty podľa potrieb a požiadaviek vašej siete.

- **definujte priradenie sieťového adaptéra ku konkrétnej vrstve RM OSI**

V prípade modelu ISO/OSI, sieťový adaptér (Network Interface Card - NIC) je typicky priradený k dvom vrstvám:

1. **\*\*Fyzická vrstva (Physical Layer):\*\***

- Na úrovni fyzickej vrstvy sa sieťový adaptér zaoberá fyzickými aspektmi prenosu dát, ako je napríklad prenos signálov cez kábel alebo bezdrôtové médium. Sieťový adaptér zabezpečuje prevod digitálnych dát na fyzické signály a naopak. Ďalej sa stará o správne fyzické pripojenie do siete, či už pomocou Ethernetového kábla, Wi-Fi signálu alebo iných médií.

2. **\*\*Linková vrstva (Data Link Layer):\*\***

- Linková vrstva zabezpečuje správne doručenie rámca v rámci miestnej siete. Na tejto úrovni sa sieťový adaptér stará o adresáciu rámca (pripojenie MAC adresy), detekciu a opravu chýb v prenose dát (ak je potrebné), riadenie toku dát a prípadne o obsluhu prístupu k médiu (MAC protokol). Sieťový adaptér teda umožňuje komunikáciu medzi rôznymi zariadeniami v rámci lokálnej siete.

Celkovo vzaté, sieťový adaptér funguje na fyzickej vrstve ako prevodník dát medzi digitálnymi dátami a fyzickými signálmi pre prenos po médiu a na linkovej vrstve ako prostriedok na správne doručenie a riadenie prenášaných rámcov v miestnej sieti.

- **kategorizujte rozhranie sieťových adaptérov pre metalické médiá**

Rozhrania sieťových adaptérov pre metalické médiá sa môžu kategorizovať podľa rôznych faktorov, vrátane typu konektora, rýchlosti prenosu dát a použitej technológie. Tu je kategorizácia niektorých bežných typov rozhraní pre metalické médiá:

1. **\*\*RJ-45 konektor:\*\***

- RJ-45 konektor je najbežnejší typ konektora pre Ethernetové káble (CAT5e, CAT6, CAT6a atď.). Tento konektor je široko používaný vo fyzickej vrstve Ethernetových sietí a zabezpečuje spoľahlivé pripojenie pre prenos dát.

2. **\*\*RJ-11 konektor:\*\***

- RJ-11 konektor sa bežne používa pre telefónne linky, ale niekedy sa môže vyskytnúť aj v počítačových sieťach. Je obvykle menší ako RJ-45 a má menej kontaktov.

3. **\*\*BNC konektor:\*\***

- BNC konektor (Bayonet Neill-Concelman) sa bežne používa v koaxiálnych kábloch pre prenos dát, ako napríklad v sieťových topológiách typu koaxiálny kábel alebo v niektorých videonahrávacích systémoch.

4. **\*\*ST konektor:\*\***

- ST (Straight Tip) konektor je typickým konektorom pre multimódové optické vlákno. Je to zásuvka s pevným krytom, ktorý sa otočí na zabezpečenie spojenia.

5. **\*\*SC konektor:\*\***

- SC (Subscriber Connector alebo Square Connector) konektor je ďalším typom optického konektora, ktorý sa používa pre multimódové aj jedno módové optické vlákno.

## 6. **\*\*LC konektor:\*\***

- LC (Lucent Connector) konektor je malý, zúžený konektor, ktorý sa často používa v dátových a telekomunikačných sieťach. Je vhodný pre vysoké rýchlosti prenosu dát a používa sa najmä pre jednovidové optické vlákno.

Tieto kategórie rozhraní sieťových adaptérov pre metalické médiá zohľadňujú rôzne typy konektorov a technológií, ktoré sa používajú v súčasných počítačových a komunikačných sieťach.

### - **uved'te druhy a spôsoby ukončovania metalických káblov**

K ukončovaniu metalických káblov sa používajú rôzne druhy konektorov a spôsoby, aby sa zabezpečilo spoľahlivé a stabilné pripojenie. Tu sú niektoré bežné druhy konektorov a spôsoby ich ukončenia:

#### 1. **\*\*RJ-45 konektor:\*\***

- RJ-45 konektor je najčastejším typom konektora pre metalické káble v Ethernetových sieťach. K ukončeniu tohto konektora sa často používa metóda "crimping", pri ktorej sa vodiče z kábla usporiadajú do správneho poradia a potom sa zatláčajú do konektora, ktorý sa následne zatlačí pomocou špeciálneho nástroja.

#### 2. **\*\*BNC konektor:\*\***

- BNC konektor sa používa v koaxiálnych kábloch pre prenos dát. Na ukončenie BNC konektora sa používa metóda "compression", ktorá zahŕňa stlačenie káblov do konektora pomocou špeciálneho nástroja.

#### 3. **\*\*ST a SC konektory (optické vlákno):\*\***

- Pri ukončovaní optických vlákien pomocou konektorov ST alebo SC sa zvyčajne používa metóda "fusion splicing" alebo "mechanické ukončenie". "Fusion splicing" zahŕňa zlúčenie koncoviek optických vlákien pomocou vysokého tepla, zatiaľ čo "mechanické ukončenie" využíva mechanické spoje a konektory.

#### 4. **\*\*LC konektor:\*\***

- LC konektor, podobne ako SC, sa používa pre optické vlákna. Na ukončenie LC konektora sa používa metóda "prepolievanie" alebo "mechanické ukončenie", podobne ako pri ST a SC konektoroch.

#### 5. **\*\*RJ-11 konektor:\*\***

- RJ-11 konektor sa používa pre telefónne káble. Na ukončenie RJ-11 konektora sa zvyčajne používa metóda "crimping" alebo "pripojenie skrutkami", kde sa vodiče kábla umiestnia do príslušných kontaktov konektora a zatlačia alebo pripoja skrutkami.

Tieto spôsoby ukončovania metalických káblov zabezpečujú spoľahlivé a trvanlivé pripojenie, čo je kľúčové pre správnu prevádzku a výkon počítačových a komunikačných sietí.

### - **popíšte rozhranie sieťových adaptérov pre optické médiá**

Rozhrania sieťových adaptérov pre optické médiá sú navrhnuté na použitie s optickými vláknami a poskytujú spoľahlivý a vysokorýchlostný prenos dát cez optické káble. Tu sú niektoré z najbežnejších typov rozhraní sieťových adaptérov pre optické médiá:

1. **\*\*ST konektor (Straight Tip):\*\***

- ST konektor je jeden z najstarších a najpoužívanejších typov konektorov pre optické vlákna. Je to guľovitý konektor so zámkovým mechanizmom, ktorý sa otáča na zabezpečenie spojenia. ST konektor sa často používa v starších optických sieťach.

2. **\*\*SC konektor (Subscriber Connector alebo Square Connector):\*\***

- SC konektor je veľmi populárny a široko používaný v súčasných optických sieťach. Je to malej veľkosti konektor, ktorý sa ľahko zasunie a vytvorí spoľahlivé pripojenie. SC konektor je dvojbodový konektor sádka/vtýčka a je ideálny pre použitie vo viacerých aplikáciách.

3. **\*\*LC konektor (Lucent Connector):\*\***

- LC konektor je malý, zúžený konektor, ktorý sa stáva čoraz populárnejším pre optické médiá. Jeho kompaktný dizajn umožňuje hustejšiu inštaláciu a poskytuje spoľahlivé a trvanlivé pripojenie. LC konektor sa často používa vo vysokorýchlostných optických sieťach.

4. **\*\*MT-RJ konektor (Mechanical Transfer Registered Jack):\*\***

- MT-RJ konektor je hybridný konektor, ktorý kombinuje dva optické vlákna a dva elektrické vodiče do jedného malého konektora. Tento typ konektora je špeciálne navrhnutý pre multimódové optické vlákna a je vhodný pre použitie v miestach, kde je priestor obmedzený.

5. **\*\*MPO/MTP konektor (Multi-Fiber Push-On/Pull-Off):\*\***

- MPO/MTP konektor je viacvláknový konektor, ktorý umožňuje pripojenie viacerých optických vlákien súčasne. Tento typ konektora je často používaný v optických sieťach s veľkou hustotou vlákien, ako sú datové centrá a telekomunikačné systémy.

Tieto typy rozhraní sieťových adaptérov pre optické médiá umožňujú spoľahlivé a vysokorýchlostné prenosy dát cez optické vlákna a poskytujú široké možnosti pre inštaláciu a rozvoj optických komunikačných sietí.

- **uved'te štandardy bezdrôtovej dátovej komunikácie**

Existuje niekoľko štandardov bezdrôtovej dátovej komunikácie, ktoré definujú spôsoby prenosu dát cez bezdrôtové médiá. Tu sú niektoré z najznámejších štandardov:

1. **\*\*Wi-Fi (IEEE 802.11):\*\***

- Wi-Fi je najpoužívanejší štandard bezdrôtovej dátovej komunikácie. Definuje sériu štandardov IEEE 802.11, ako sú 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac a 802.11ax. Tieto štandardy sa líšia vo frekvencii, rýchlosti prenosu dát a iných technických špecifikáciách.

2. **\*\*Bluetooth (IEEE 802.15.1):\*\***

- Bluetooth je bezdrôtový štandard určený pre krátkodobú dátovú komunikáciu medzi zariadeniami v blízkom dosahu. Používa sa pre bezdrôtové pripojenie slúchadiel, klávesníc, myší, telefónov a ďalších periférnych zariadení.

3. **\*\*Zigbee (IEEE 802.15.4):\*\***

- Zigbee je štandard určený pre nízkonákladové, nízkoenergetické bezdrôtové siete pre vzdialené monitorovanie a ovládanie zariadení. Často sa používa v aplikáciách inteligentných domov, automatizácii budov, priemysle a v iných oblastiach.

#### 4. **\*\*Z-Wave:\*\***

- Z-Wave je iný štandard pre nízkoenergetické bezdrôtové siete, ktorý sa často používa v inteligentných domácnostiach na ovládanie osvetlenia, termostátov, dverových zámkov a ďalších zariadení.

#### 5. **\*\*LTE (Long-Term Evolution):\*\***

- LTE je mobilný bezdrôtový štandard, ktorý poskytuje vysokorýchlostné pripojenie k internetu pre mobilné zariadenia. LTE je štandardom pre siete 4. generácie (4G) a ponúka vysoké rýchlosti prenosu dát pre mobilné dáta a internetový prístup.

#### 6. **\*\*5G (Fifth Generation):\*\***

- 5G je najnovší štandard mobilnej bezdrôtovej komunikácie, ktorý poskytuje ešte vyššie rýchlosti prenosu dát, nižšiu oneskorenú a lepšiu spoľahlivosť v porovnaní s predchádzajúcimi generáciami sietí. 5G sa očakáva, že umožní pokročilé aplikácie, ako sú autonómne vozidlá, rozšírená realita (AR) a internet vecí (IoT).

Tieto štandardy poskytujú rôzne možnosti bezdrôtovej dátovej komunikácie pre rôzne použitia a prostredia a sú dôležitou súčasťou moderných bezdrôtových komunikačných technológií.

#### - **posúďte spôsoby zabezpečenia technológie Wi-Fi**

Zabezpečenie technológie Wi-Fi je kľúčové pre ochranu siete pred neoprávneným prístupom a útokmi. Tu je posúdenie niektorých spôsobov zabezpečenia technológie Wi-Fi:

##### 1. **\*\*Šifrovanie:\*\***

- Používanie šifrovania dát je základným krokom pri zabezpečovaní Wi-Fi siete. Šifrovanie dát, ako napríklad WPA2 (Wi-Fi Protected Access 2) alebo novšie WPA3, zabezpečuje, že dáta prenášané cez Wi-Fi sieť sú chránené pred odpočúvaním a úpravou.

##### 2. **\*\*Silné heslá:\*\***

- Používanie silných a unikátnych hesiel na prístup k Wi-Fi sieti je nevyhnutné. Heslá by mali byť dostatočne dlhé, obsahovať kombináciu veľkých a malých písmen, číslíc a špeciálnych znakov. Vyhnite sa používaniu ľahko uhádnuteľných hesiel, ako sú dátumy narodenia alebo jednoduché slová.

##### 3. **\*\*Zmena predvolených nastavení:\*\***

- Zabezpečenie Wi-Fi siete zahŕňa aj zmenu predvolených nastavení smerovača, ako sú predvolené heslá a názov siete (SSID). Predvolené hodnoty sú bežnými cieľmi pre útočníkov, preto je dôležité ich zmeniť na jedinečné hodnoty.

##### 4. **\*\*Vypnutie nepotrebných funkcií:\*\***

- Vypnutie nepotrebných funkcií smerovača, ako sú WPS (Wi-Fi Protected Setup), UPnP (Universal Plug and Play) a remote management, môže znížiť zraniteľnosti siete a znížiť riziko útoku.

##### 5. **\*\*Segmentácia siete:\*\***

- Rozdelenie siete na viacero segmentov alebo VLAN (Virtual Local Area Networks) môže zlepšiť zabezpečenie tým, že obmedzí prístup k určitým častiam siete pre rôzne skupiny používateľov alebo zariadení.

#### 6. **\*\*Aktualizácie a patche:\*\***

- Pravidelné aktualizácie firmvéru smerovača a zariadení pripojených k Wi-Fi sieti sú dôležité na zabezpečenie proti novým zraniteľnostiam a hrozbám.

#### 7. **\*\*Používanie VPN:\*\***

- Použitie virtuálnych privátnych sietí (VPN) môže poskytnúť dodatočnú vrstvu zabezpečenia pre komunikáciu medzi zariadeniami a internetom tým, že šifruje všetky dáta prenášané cez sieť.

Celkovo vzaté, kombinácia týchto opatrení môže zabezpečiť robustné a spoľahlivé zabezpečenie Wi-Fi siete pred rôznymi hrozbami a útokmi. Je dôležité vybrať si správne opatrenia v závislosti od konkrétnych potrieb a prostredia siete.

### **- aplikujte princíp potlačenia elektromagnetického rušenia v symetrickom vedení pomocou operačného zosilňovača**

Potlačenie elektromagnetického rušenia (EMI) v symetrickom vedení pomocou operačného zosilňovača môže byť dosiahnuté pomocou diferenciálnej konfigurácie operačného zosilňovača. Tu je spôsob, ako môže byť toto dosiahnuté:

#### 1. **\*\*Diferenciálna konfigurácia operačného zosilňovača:\*\***

- V diferenciálnej konfigurácii operačný zosilňovač má dva vstupy: inverzný (-) a neinverzný (+). Signál na neinverznom vstupe sa vydáva na výstup zosilňovača s rovnakou polaritou, zatiaľ čo signál na inverznom vstupe sa vydáva na výstup s opačnou polaritou.

#### 2. **\*\*Použitie diferenciálneho vstupu:\*\***

- Pri použití diferenciálneho vstupu operačného zosilňovača je možné dosiahnuť potlačenie EMI. Symetrické vedenie je pripojené k oboom vstupom operačného zosilňovača, pričom vstupy sú umiestnené na rovnakej vzdialenosti od zdroja rušenia. Ak je rušenie rovnako silné na oboch vstupoch, operačný zosilňovač bude potláčať toto rušenie, pretože rozdielový signál, ktorý je zosilnený, bude minimálny.

#### 3. **\*\*Výstupný filter:\*\***

- Na výstupné napäťové signály operačného zosilňovača možno aplikovať filter, ktorý odstráni vyššie frekvencie, ktoré môžu byť spojené s EMI. Tento filter môže byť navrhnutý tak, aby zosilňoval len požadované signály a potláčal nežiaduce vysokofrekvenčné rušenie.

Týmto spôsobom môže byť elektromagnetické rušenie v symetrickom vedení účinne potlačené pomocou operačného zosilňovača v diferenciálnej konfigurácii. Je dôležité, aby bol operačný zosilňovač správne navrhnutý a správne nastavený, aby bol dosiahnutý požadovaný výsledok.

### **- analyzujte podmienky inštalácie Wi-Fi zariadení**

Inštalácia Wi-Fi zariadení môže byť úspešná len vtedy, ak sú splnené určité podmienky a faktory. Tu je analýza niektorých z týchto podmienok:

### 1. **\*\*Pokrytie signálom:\*\***

- Jedným z najdôležitejších faktorov je dostatočné pokrytie signálom vo všetkých oblastiach, kde je očakávané používanie Wi-Fi zariadení. To znamená, že signál by mal byť silný a spoľahlivý vo všetkých častiach priestoru, čo môže vyžadovať správne umiestnenie prístupových bodov alebo opakovačov signálu.

### 2. **\*\*Frekvenčný pás a kanál:\*\***

- Pri inštalácii Wi-Fi zariadení je dôležité zvoliť správny frekvenčný pás (2,4 GHz alebo 5 GHz) a kanál, aby sa minimalizovalo rušenie a interferencia od iných zariadení v blízkosti. Ideálny kanál je ten, ktorý má najmenšiu hladinu rušenia od ostatných sietí v okolí.

### 3. **\*\*Bezpečnostné opatrenia:\*\***

- Pri inštalácii Wi-Fi zariadení je nevyhnutné zabezpečiť sieť správnym spôsobom. To zahŕňa použitie silných hesiel, šifrovanie dát pomocou WPA2 alebo WPA3 a vypnutie nepotrebných funkcií, ako je WPS (Wi-Fi Protected Setup), ktoré môžu predstavovať bezpečnostné riziko.

### 4. **\*\*Optimalizácia výkonu:\*\***

- Optimalizácia výkonu Wi-Fi siete môže zahŕňať nastavenie vhodných parametrov smerovača, ako sú výkonné antény, rýchlosti prenosu dát a riadiace funkcie, aby sa dosiahol najlepší možný výkon a spoľahlivosť siete.

### 5. **\*\*Správne umiestnenie prístupových bodov:\*\***

- Umiestnenie prístupových bodov je dôležité pre dosiahnutie rovnomerného pokrytia signálom vo všetkých oblastiach. Prístupové body by mali byť umiestnené v centrálnej polohe, aby sa minimalizovali prekážky a interferencie.

### 6. **\*\*Berú sa do úvahy materiály a prostredie:\*\***

- Pri inštalácii je dôležité zohľadniť typy materiálov, ktoré môžu ovplyvniť prenos signálu, ako sú steny, stropy a ďalšie prekážky. Niekedy môže byť potrebné použiť väčší počet prístupových bodov alebo opakovačov signálu na prekonanie prekážok.

Celkovo vzaté, inštalácia Wi-Fi zariadení si vyžaduje dôkladnú analýzu a plánovanie, aby sa dosiahlo optimálne pokrytie signálom a spoľahlivý výkon siete. Všetky tieto faktory a podmienky musia byť zohľadnené pri návrhu a realizácii inštalácie Wi-Fi.

### - **vysvetlite konkurenciu medzi výrobcami adaptérov na trhu**

Konkurencia medzi výrobcami adaptérov na trhu je výrazná a zahrňuje niekoľko kľúčových faktorov, ktoré ovplyvňujú ich pozíciu a úspech. Tu sú niektoré z hlavných aspektov konkurencie medzi výrobcami adaptérov:

#### 1. **\*\*Cena:\*\***

- Cena je jedným z najdôležitejších faktorov konkurencie. Výrobcovia sa často snažia ponúkať svoje adaptéry za konkurencieschopné ceny, často sa angažujú v cenovej vojne, aby získali viac zákazníkov.

#### 2. **\*\*Kvalita:\*\***



- Kvalita produktu je dôležitá pre získanie a udržanie zákazníkov. Výrobcovia sú nútení súťažiť na základe kvality svojich adaptérov, čo zahŕňa spoľahlivosť, výkon, kompatibilitu a životnosť produktu.

### 3. **\*\*Funkcie a vlastnosti:\*\***

- Výrobcovia sú nútení inovovať a poskytovať nové funkcie a vlastnosti, ktoré sú atraktívne pre zákazníkov. To môže zahŕňať vysokorýchlostné pripojenie, rozšírené bezpečnostné funkcie, jednoduchú inštaláciu a ďalšie.

### 4. **\*\*Marketing a značka:\*\***

- Úspešní výrobcovia investujú do marketingu a budovania značky, aby zvýšili povedomie o svojich produktoch a vytvorili lojalitu zákazníkov. Silná značka a efektívny marketing môžu vytvoriť konkurenčnú výhodu na trhu.

### 5. **\*\*Podpora a zákaznícka služba:\*\***

- Kvalitná zákaznícka podpora a služby sú dôležité pre zákazníkov pri výbere adaptérov. Výrobcovia s dobrým povestou v oblasti podpory a zákazníckej služby môžu získať konkurenčnú výhodu.

### 6. **\*\*Partnerstvá a distribúcia:\*\***

- Výrobcovia často uzatvárajú partnerstvá s maloobchodnými predajcami a distribútormi, aby zabezpečili široké pokrytie trhu a dostupnosť svojich adaptérov.

### 7. **\*\*Technologický vývoj:\*\***

- Vzhľadom na rýchly technologický vývoj v oblasti bezdrôtových technológií sa výrobcovia snažia udržať krok s najnovšími trendmi a ponúkať najmodernejšie a najvýkonnejšie adaptéry.

Vzhľadom na tieto faktory je trh s adaptérmí prepojený s intenzívnou konkurenciou a výrobcovia sú nútení neustále inovovať a zlepšovať svoje produkty, aby uspeli na trhu.

## **BEZDRÔTOVÁ DÁTOVÁ KOMUNIKÁCIA WI-FI**

### **- popíšte vývoj bezdrôtovej dátovej komunikácie,**

Vývoj bezdrôtovej dátovej komunikácie je dlhý a dynamický proces, ktorý sa v priebehu času výrazne zmenil a rozvinul. Tu je stručný prehľad vývoja bezdrôtovej dátovej komunikácie:

#### 1. **\*\*Počiatky:\*\***

- Bezdrôtová komunikácia má korene už v 19. storočí s vynálezom rádiových vlniek Marconiho a ďalších. Prvé bezdrôtové komunikačné systémy boli jednoduché a obmedzené na krátke vzdialenosti.

#### 2. **\*\*Rozvoj rádiových technológií:\*\***

- V 20. storočí sa rýchlo rozvíjala rádiová technológia s nástupom rádiových vysieláčov, ktoré umožnili komunikáciu na väčšie vzdialenosti. Rádiové frekvencie sa stali štandardom pre bezdrôtovú komunikáciu.

### 3. **\*\*Vznik mobilných komunikačných sietí:\*\***

- V 80. a 90. rokoch 20. storočia sa začali vyvíjať mobilné komunikačné siete, ako sú prvé generácie (1G) a neskôr 2G, ktoré umožňovali hlasovú komunikáciu. Neskôr prichádzajúce generácie (3G, 4G, 5G) poskytovali stále rýchlejšie dáta a nové funkcie.

### 4. **\*\*Vznik WiFi:\*\***

- V 90. rokoch 20. storočia sa začala používať technológia WiFi, ktorá umožňuje bezdrôtovú komunikáciu v lokálnych sieťach. WiFi sa stalo populárnym štandardom pre bezdrôtový prístup k internetu a dátovú komunikáciu v domácnostiach, podnikoch a verejných priestoroch.

### 5. **\*\*Rozvoj Bluetooth a ZigBee:\*\***

- Bluetooth a ZigBee sú ďalšie technológie bezdrôtovej komunikácie, ktoré boli vyvinuté pre špecifické použitia, ako sú krátkodobé pripojenia medzi zariadeniami (Bluetooth) alebo nízkoenergetické senzorové siete (ZigBee).

### 6. **\*\*Internet vecí (IoT):\*\***

- S nástupom internetu vecí (IoT) sa bezdrôtová dátová komunikácia stala ešte dôležitejšou. IoT zariadenia často komunikujú bezdrôtovo cez rôzne technológie, ako sú WiFi, Bluetooth, ZigBee, LTE-M, NB-IoT a ďalšie.

### 7. **\*\*Stále rýchlejšie a spoľahlivejšie pripojenie:\*\***

- S rastom dopytu po dátach a nároky na vyššiu rýchlosť a spoľahlivosť bezdrôtovej komunikácie sa neustále vyvíjajú nové technológie a štandardy, ako sú WiFi 6 (802.11ax), 5G NR (New Radio) a ďalšie.

Celkový vývoj bezdrôtovej dátovej komunikácie od prvých rádiových vlniek až po súčasné rýchle a spoľahlivé technológie je impozantný a pokračuje neustále s rastúcim dopytom a novými technologickými pokrokmi.

#### - **vysvetlite spôsoby prenosu bezdrôtovej dátovej komunikácie;**

Existuje niekoľko spôsobov prenosu bezdrôtovej dátovej komunikácie, ktoré sa používajú v rôznych aplikáciách a prostrediach. Tu je stručný prehľad niektorých hlavných spôsobov:

#### 1. **\*\*Rádiové prenosy:\*\***

- Rádiové prenosy sú najbežnejším spôsobom prenosu bezdrôtovej komunikácie. Používajú rádiové vlny na prenos dát medzi zariadeniami. Rôzne technológie rádiových prenosov, ako sú WiFi, Bluetooth, ZigBee a iné, poskytujú rôzne rýchlosti, dosahy a kapacity prenosu.

#### 2. **\*\*Infraprenosy:\*\***

- Infraprenosy využívajú infračervené svetlo na prenos dát medzi zariadeniami. Tento spôsob komunikácie je obvykle obmedzený na krátke vzdialenosti a vyžaduje priamu viditeľnosť medzi zariadeniami. Infraprenosy sa často používajú na pripojenie rôznych zariadení, ako sú diaľkové ovládače, mobilné telefóny a iné.

#### 3. **\*\*Mikrovlnné prenosy:\*\***

- Mikrovlnné prenosy používajú mikrovlnné frekvencie na prenos dát medzi zariadeniami. Tento spôsob prenosu je často využívaný v rádiových spojoch a bezdrôtových sieťach s vysokým dosahom a rýchlosťou.

#### 4. **\*\*Satelitná komunikácia:\*\***

- Satelitná komunikácia umožňuje prenos dát medzi zariadeniami prostredníctvom komunikačných družíc umiestnených vo vesmíre. Tento spôsob komunikácie poskytuje pokrytie aj na odľahlých miestach, kde nie je možné inak použiť rádiové alebo iné spojenia.

#### 5. **\*\*Optické vlákna:\*\***

- Optické vlákna sú často používané na prenos dát vo vysokorýchlostných bezdrôtových sieťach. Optické vlákna využívajú svetelné signály na prenos dát cez tenké sklenené vlákna. Tento spôsob prenosu poskytuje veľmi vysoké rýchlosti a kapacity prenosu.

Tieto spôsoby prenosu bezdrôtovej dátovej komunikácie sa líšia vo svojich vlastnostiach, dosahu, rýchlosti, spôsobe použitia a iných faktoroch. Vo väčšine prípadov sa používa kombinácia týchto technológií na zabezpečenie spoľahlivej a efektívnej komunikácie.

### **- charakterizujte klientské a chrbticové Wi-Fi zariadenia, pričom porovnajte spôsob komunikácie v režime client a accesspoint,hotspot,**

Klientské a chrbticové Wi-Fi zariadenia sú zariadenia, ktoré sa používajú na bezdrôtové pripojenie k bezdrôtovej sieti (Wi-Fi). Tu je charakteristika a porovnanie spôsobov komunikácie v režime client, access point (prístupový bod) a hotspot:

#### 1. **\*\*Klientské Wi-Fi zariadenia:\*\***

- Klientské Wi-Fi zariadenia sú zariadenia, ktoré sa pripájajú k existujúcej bezdrôtovej sieti ako klienti. Príklady klientských zariadení zahŕňajú počítače, mobilné telefóny, tablety, tlačiarne a ďalšie.

- V režime client tieto zariadenia komunikujú so smerovačom alebo prístupovým bodom a využívajú bezdrôtové spojenie na prenos dát medzi sieťou a koncovým zariadením.

- Klientské zariadenia požadujú autentifikáciu a autorizáciu zo strany prístupového bodu alebo smerovača, aby sa mohli pripojiť k sieti.

#### 2. **\*\*Chrbticové Wi-Fi zariadenia:\*\***

- Chrbticové Wi-Fi zariadenia sú zariadenia, ktoré slúžia ako prístupové body (AP) alebo rozširujúce body siete (repeater). Tieto zariadenia umožňujú pripojenie klientov k bezdrôtovej sieti.

- V režime access point tieto zariadenia vytvárajú bezdrôtovú sieť a umožňujú klientom pripojiť sa k nej. Poskytujú prístup k lokálnej sieti alebo internetu.

- Chrbticové zariadenia majú schopnosť spravovať viacerých klientov súčasne a riadiť prenos dát medzi klientmi a sieťou.

#### 3. **\*\*Hotspot:\*\***

- Hotspot je verejný prístupový bod k internetu, ktorý je spravidla dostupný v verejných priestoroch, ako sú kaviarne, letiská, hotely, reštaurácie a ďalšie.

- V režime hotspot môžu byť chrbticové Wi-Fi zariadenia nakonfigurované na poskytovanie verejného prístupu k internetu. Používatelia môžu pripojiť svoje klientské zariadenia k tomuto hotspotu a získať prístup k internetu.

Porovnanie:

- Klientské zariadenia sú určené na pripojenie k existujúcej sieti a využívajú ju na prístup k internetu alebo zdieľanie dát.
- Chrbticové zariadenia sú navrhnuté tak, aby vytvárali bezdrôtovú sieť a umožňovali pripojenie klientov k tejto sieti.
- Hotspot je špecifický prípad chrbticového zariadenia, ktoré poskytuje verejný prístup k internetu v určitých verejných priestoroch.

Všetky tieto typy zariadení sú dôležité pre bezdrôtovú komunikáciu a poskytujú rôzne funkcie a možnosti pripojenia.

- **definujte špecifikácie komunikačného štandardu 802.11 bezdrôtových sietí,**  
Špecifikácie komunikačného štandardu 802.11 sú sada noriem definujúcich technické parametre a protokoly pre bezdrôtové lokálne siete (WLAN). Tu je stručný prehľad hlavných špecifikácií tohto štandardu:

1. **\*\*Frekvencie:\*\***

- Štandard 802.11 podporuje použitie viacerých frekvenčných pásiem vrátane 2,4 GHz a 5 GHz. Frekvencie sú špecifikované v rámci štandardu, pričom každé pásmo má svoje vlastné charakteristiky a použitie.

2. **\*\*Rýchlosť prenosu dát:\*\***

- Štandard 802.11 definuje rôzne rýchlosti prenosu dát v závislosti od použitej technológie a frekvencie. V starších verziách štandardu (802.11b, 802.11g) bola maximálna rýchlosť obvykle do 54 Mbps, zatiaľ čo novšie verzie (802.11n, 802.11ac, 802.11ax) poskytujú vyššie rýchlosti až do niekoľkých gigabitov za sekundu.

3. **\*\*Modulácia:\*\***

- Štandard 802.11 definuje rôzne modulačné schémy pre prenos dát, ktoré ovplyvňujú efektívnosť a rýchlosť prenosu dát. Medzi bežné modulačné schémy patrí DSSS (Direct Sequence Spread Spectrum), OFDM (Orthogonal Frequency Division Multiplexing) a iné.

4. **\*\*Bezpečnosť:\*\***

- Štandard 802.11 obsahuje aj špecifikácie pre bezpečnostné protokoly a mechanizmy, ktoré zabezpečujú komunikáciu v bezdrôtových sieťach. Medzi bežné bezpečnostné mechanizmy patria WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) a WPA2 (Wi-Fi Protected Access 2).

5. **\*\*Moduly a rozhrania:\*\***

- Štandard 802.11 definuje rôzne typy modulov a rozhraní pre bezdrôtové zariadenia, ktoré sú používané na pripojenie k bezdrôtovej sieti. Tieto moduly môžu byť implementované v rôznych zariadeniach, ako sú smerovače, prístupové body, karty PCI a USB adaptéry.

6. **\*\*Podpora viacerých používateľov (MU-MIMO):\*\***

- Novšie verzie štandardu 802.11 (napr. 802.11ac a 802.11ax) zahŕňajú funkcie podpory viacerých používateľov (MU-MIMO), ktoré umožňujú zariadeniam komunikovať s viacerými klientmi súčasne a zlepšiť tak výkon a efektívnosť siete.

Tieto špecifikácie a parametre štandardu 802.11 sú neustále vyvíjané a aktualizované, aby sa zlepšovala bezdrôtová komunikácia a poskytovali sa nové funkcie a vlastnosti pre bezdrôtové siete. Novšie verzie štandardu sa zameriavajú na zvyšovanie rýchlostí prenosu dát, zlepšenie bezpečnosti a podporu nových technológií ako je IoT a 5G.

- **analyzujte spôsoby distribúcie Wi-Fi signálu,**

Distribúcia Wi-Fi signálu sa môže líšiť v závislosti od architektúry a prostredia siete. Tu je analýza niekoľkých spôsobov distribúcie Wi-Fi signálu:

1. **\*\*Prístupové body (Access Points - APs):\*\***

- Prístupové body sú zariadenia, ktoré vytvárajú bezdrôtovú sieť a umožňujú pripojenie klientov k sieti. Distribúcia signálu z prístupových bodov závisí od ich umiestnenia a konfigurácie. Viacero prístupových bodov môže byť použitých na pokrytie väčšej oblasti alebo elimináciu oblastí so slabým signálom (tzv. dead zones).

2. **\*\*Rozširujúce body siete (Wireless Extenders):\*\***

- Rozširujúce body siete sú zariadenia, ktoré sa používajú na zvýšenie dosahu existujúcej bezdrôtovej siete. Tieto zariadenia sa umiestňujú medzi prístupovými bodmi a oblasťami so slabým signálom, aby sa zlepšil dosah a pokrytie siete.

3. **\*\*Mesh siete:\*\***

- Mesh siete sú sieťové topológie, kde sú prístupové body vzájomne prepojené a vytvárajú vzájomnú sieťovú infraštruktúru. Tento spôsob distribúcie umožňuje dynamické prekládanie signálu medzi viacerými zariadeniami a zvyšuje spoľahlivosť a dostupnosť siete.

4. **\*\*Powerline adaptéry:\*\***

- Powerline adaptéry umožňujú distribúciu Wi-Fi signálu cez elektrické vedenie v budove. Tieto zariadenia sa pripájajú k bežným zásuvkám a umožňujú prenos dát medzi rôznymi miestnosťami pomocou existujúcej elektrickej infraštruktúry.

5. **\*\*Roaming a Fast Roaming:\*\***

- Roaming je proces, ktorý umožňuje bezdrôtovému klientovi pripojiť sa k najlepšiemu dostupnému prístupovému bodu v priebehu pohybu v rámci siete. Fast Roaming je pokročilejšia technika, ktorá znižuje čas potrebný na prepájanie medzi prístupovými bodmi a minimalizuje prerušenia spojenia.

6. **\*\*Optimalizácia signálu:\*\***

- Optimalizácia signálu zahŕňa použitie techník ako je umiestnenie prístupových bodov na optimálnych miestach, použitie antén s väčším ziskom, optimalizácia kanálov a vyváženie záťaže medzi rôznymi prístupovými bodmi.

Tieto spôsoby distribúcie Wi-Fi signálu sa často kombinujú a prispôbujú sa konkrétnym potrebám a prostrediam siete. Cieľom je poskytnúť spoľahlivé a vysokorýchlostné pripojenie k Wi-Fi sieti v rôznych častiach budovy alebo oblasti.

- **zhodnot'te najvhodnejšie kanály na komunikáciu prostredníctvom Wi-Fi,**

Výber najvhodnejších kanálov na komunikáciu prostredníctvom Wi-Fi závisí od viacerých faktorov, ako sú frekvenčné pásma, miestne prostredie a záťaž siete. Tu je zhodnotenie niektorých faktorov, ktoré ovplyvňujú výber kanálov:

1. **\*\*Frekvenčné pásma:\*\***

- Štandard 802.11 definuje používanie dvoch hlavných frekvenčných pásiem pre Wi-Fi: 2,4 GHz a 5 GHz. Každé pásmo má svoje výhody a nevýhody, ktoré ovplyvňujú výber kanálov.
- V pásmach 2,4 GHz je k dispozícii menej kanálov a sú náchylné na rušenie od iných zariadení, ako sú mikrovlnné rúry, Bluetooth zariadenia a bezdrôtové telefóny.
- V pásmach 5 GHz je viac kanálov a menej rušenia od iných zariadení, čo zvyčajne umožňuje vyššie rýchlosti prenosu dát.

2. **\*\*Záťaž siete:\*\***

- V miestach s vysokou záťažou siete môže byť kritické optimalizovať výber kanálov pre minimalizáciu interferencie a maximalizáciu priepustnosti.
- Distribúcia záťaže medzi rôznymi kanálmi môže pomôcť vyhnúť sa preplneniu a zlepšiť celkový výkon siete.

3. **\*\*Interferencia:\*\***

- Interferencia od iných bezdrôtových zariadení a elektronických zariadení v okolí môže mať významný vplyv na výkon Wi-Fi siete.
- Voľba kanálov s minimálnou interferenciou od iných zariadení môže zlepšiť spoľahlivosť a rýchlosť pripojenia k sieti.

4. **\*\*Využitie šírky pásma:\*\***

- Niekedy je možné použiť širšie kanály (napr. 40 MHz alebo 80 MHz) na zvýšenie rýchlosti prenosu dát. Avšak širšie kanály môžu spôsobiť väčšiu interferenciu a sú menej odolné voči rušeniu.

5. **\*\*Automatické nastavenie kanálov (Auto Channel Selection):\*\***

- Niektoré prístupové body majú funkciu automatického výberu kanálov, ktorá umožňuje zariadeniu vybrať najmenej rušený kanál v danom okolí.

Na základe týchto faktorov je ťažké stanoviť univerzálny "najvhodnejší" kanál pre Wi-Fi komunikáciu. Je dôležité vykonať dôkladnú analýzu prostredia a zvážiť rôzne faktory, aby sa dosiahol optimálny výber kanálov pre danú sieť. Niektoré nástroje pre správu sietí môžu poskytnúť informácie o využití kanálov a rušení, čo umožní lepšie rozhodnutia pri výbere kanálov.

- **porovnajte topológie a spôsoby komunikácie v režime AD - HOC, BSS a ESS;**

Topológie a spôsoby komunikácie v režime Ad-hoc, BSS a ESS sa líšia v závislosti od toho, ako sú bezdrôtové siete organizované a koordinované. Tu je porovnanie týchto režimov:

1. **\*\*Ad-hoc (IBSS - Independent Basic Service Set):\*\***

- V ad-hoc režime sa bezdrôtové zariadenia pripájajú priamo k sebe navzájom bez potreby prístupového bodu (AP).
- Každé zariadenie v ad-hoc sieti je rovnocenným uzlom a môže komunikovať s ostatnými zariadeniami priamo.

- Topológia siete je typicky mriežkovitá (mesh) alebo hviezdicová, kde sú všetky zariadenia medzi sebou priamo prepojené.

## 2. \*\*BSS (Basic Service Set):\*\*

- V BSS režime je bezdrôtová sieť organizovaná okolo jedného prístupového bodu (AP).
- Prístupový bod koordinuje komunikáciu medzi klientmi v sieti a zabezpečuje správu prenosu dát.
- Klienti v BSS sú spojení s AP a komunikujú cez neho. Topológia siete je typicky hviezdicová, kde všetky komunikácie prechádzajú cez AP.

## 3. \*\*ESS (Extended Service Set):\*\*

- V ESS režime sa viaceré BSS môžu rozšíriť a prepojiť pomocou viacerých prístupových bodov (AP), čím sa vytvorí rozsiahlejšia bezdrôtová sieť.
- Klienti môžu pohybovať medzi jednotlivými BSS v rámci ESS, pričom sa pripájajú k rôznym prístupovým bodom v závislosti od dostupnosti a kvality signálu.
- Tento režim umožňuje väčšiu pokrytosť siete a lepšiu mobilitu pre klientov, pretože môžu voľne prechádzať medzi rôznymi BSS v rámci ESS.

### Porovnanie:

- V režime Ad-hoc a BSS je sieť organizovaná okolo jedného prístupového bodu alebo priamo medzi klientmi, zatiaľ čo v režime ESS môže byť sieť rozšírená cez viacero prístupových bodov.
- Ad-hoc režim nevyžaduje prístupový bod a umožňuje klientom priamy pripojenie medzi sebou, zatiaľ čo BSS a ESS vyžadujú prístupové body pre koordináciu komunikácie.
- ESS umožňuje väčšiu mobilitu klientov a rozšírenie siete na väčšiu plochu, zatiaľ čo Ad-hoc a BSS sú vhodné pre menšie siete alebo dočasné pripojenia bez prístupového bodu.

- **analyzujte podmienky inštalácie Wi-Fi zariadení v saturovanom prostredí,**  
Inštalácia Wi-Fi zariadení v saturovanom prostredí, kde je veľa bezdrôtových sietí a zariadení, vyžaduje dôkladnú analýzu a plánovanie, aby sa minimalizovali interferencie a zabezpečilo sa optimálne fungovanie siete. Tu sú niektoré podmienky, ktoré treba zvážiť pri inštalácii Wi-Fi zariadení v saturovanom prostredí:

### Analýza kanálov a frekvencií:

- Je nevyhnutné vykonať dôkladnú analýzu kanálov a frekvencií v okolí, aby sa vybrali najmenej rušené kanály pre Wi-Fi komunikáciu.
- Kanály by mali byť vybrané tak, aby minimalizovali interferencie od iných sietí a zariadení v okolí.

### Rozmiestnenie prístupových bodov:

- Prístupové body by mali byť umiestnené tak, aby pokryli celú oblasť s minimálnym prekrytím a maximalizovaním dosahu signálu.
- Pri umiestňovaní prístupových bodov je potrebné zohľadniť fyzické prekážky, ako sú steny a podlahy, ktoré môžu ovplyvniť prenos signálu.

### Optimalizácia výkonu:

- Nastavenia výkonu prístupových bodov by mali byť optimalizované tak, aby sa minimalizovala interferencia a zároveň zabezpečilo dostatočné pokrytie siete.

- Prebytočný výkon môže spôsobiť interferencie a preťaženie siete, zatiaľ čo nedostatočný výkon môže viesť k slabému signálu a zhoršenému výkonu.

Bezpečnosť a autentifikácia:

- V saturovanom prostredí je dôležité zabezpečiť sieť pomocou silných bezpečnostných mechanizmov, ako je šifrovanie (napr. WPA2) a autentifikácia (napr. RADIUS).
- Bezpečnostné mechanizmy pomáhajú chrániť sieť pred neoprávneným prístupom a zneužitím, čo môže byť ešte dôležitejšie v prostredí s vysokou hustotou sietí.

Monitorovanie a správa:

- Kontinuálne monitorovanie a správa siete je kľúčové pre identifikáciu problémov a optimalizáciu výkonu.
- Nástroje pre monitorovanie siete môžu poskytnúť informácie o využití kanálov, kvalite signálu a iných parametroch, ktoré sú dôležité pre riadne fungovanie siete.

Inštalácia Wi-Fi zariadení v saturovanom prostredí je výzvou, ale s vhodným plánovaním, analýzou a správou je možné dosiahnuť spoľahlivú a vysoko výkonnú bezdrôtovú sieť. Dôkladná analýza prostredia a použitie správnych techník a nástrojov sú kľúčové pre úspech v takýchto prostrediach.

### - **posúďte spôsoby zabezpečenia technológie Wi-Fi,**

Zabezpečenie technológie Wi-Fi je kľúčové pre ochranu siete pred neoprávneným prístupom a útokmi. Existuje niekoľko spôsobov, ako zabezpečiť Wi-Fi sieť:

#### 1. **\*\*Šifrovanie:\*\***

- Použitie šifrovania na zašifrovanie prenášaných dát je jedným z najzákladnejších spôsobov zabezpečenia Wi-Fi siete. Dva najbežnejšie typy šifrovania sú WEP (Wired Equivalent Privacy) a WPA/WPA2 (Wi-Fi Protected Access).

- WEP je staršia a menej bezpečná metóda šifrovania, ktorá môže byť ľahko prelomená. WPA/WPA2 je moderný a bezpečnejší štandard, ktorý ponúka silnejšie šifrovanie a lepšiu ochranu siete.

#### 2. **\*\*Autentifikácia:\*\***

- Autentifikácia sa používa na overenie toho, či klienti majú oprávnenie pripojiť sa k sieti. Existujú rôzne metódy autentifikácie, vrátane:

- PSK (Pre-Shared Key): Používateľom sa pridelený predom zdieľaný kľúč, ktorý musia zadať pri pripájaní k sieti.

- EAP (Extensible Authentication Protocol): Klienti sú autentifikovaní pomocou servera, ako je RADIUS (Remote Authentication Dial-In User Service).

- Autentifikácia zabezpečuje, že len oprávnení používatelia majú prístup k sieti.

#### 3. **\*\*Skrytie SSID (Service Set Identifier):\*\***

- Skrytie SSID je metóda, pri ktorej sa názov siete (SSID) nezobrazuje v zozname sietí, ktoré sú viditeľné pre používateľov.



- Táto metóda môže zvýšiť úroveň bezpečnosti tým, že skryje existenciu siete pred neoprávnenými používateľmi, ale nie je to úplne spoľahlivá metóda ochrany.

#### 4. **\*\*Filtrovanie MAC adries:\*\***

- Filtrovanie MAC adries umožňuje určiť, ktoré zariadenia majú povolený prístup k sieti na základe ich MAC adries.

- Aj keď je táto metóda pomerne jednoduchá na implementáciu, MAC adresy môžu byť ľahko falošne a je ťažké spravovať väčšie množstvo zariadení.

#### 5. **\*\*Aktualizácie a správa:\*\***

- Pravidelné aktualizácie firmvéru a správa zariadení sú nevyhnutné pre udržanie bezpečnosti siete. Aktualizácie často opravujú známe bezpečnostné chyby a zraniteľnosti.

#### 6. **\*\*VPN (Virtual Private Network):\*\***

- VPN môže byť použité na zabezpečenie komunikácie medzi zariadeniami v Wi-Fi sieti tým, že vytvára šifrovaný tunel pre prenos dát.

Každá z týchto metód má svoje výhody a nevýhody, a ideálne je kombinovať niekoľko z nich pre maximálnu úroveň zabezpečenia. Bezpečnosť Wi-Fi siete je neustály proces, a je dôležité monitorovať a aktualizovať zabezpečenie siete v reakcii na nové hrozby a zraniteľnosti.

- **navrhnete najvhodnejšie riešenie na vybudovanie predmetného dátového spoja aj s konfiguračnými parametrami ak je medzi nimi prekážka a vypočítajte materiállové náklady na vybudovanie Vami navrhnutého dátového spoja,**

Na vybudovanie dátového spoja s prekážkou medzi zariadeniami je možné použiť technológiu Wi-Fi s využitím bodu-miesta a bodu-bodu (point-to-point) pre prekonanie prekážky. Tu je navrhované riešenie:

#### 1. **\*\*Technológia:\*\***

- Použitie bodu-miesta (Access Point) na strane bez prekážky a bodu-bodu (Bridge) na strane s prekážkou.

- Pre dátový spoj medzi bodmi použite bezdrôtové zariadenia, ktoré podporujú technológiu Wi-Fi s vyšším dosahom a prenosovými rýchlosťami.

- Zabezpečenie spoja pomocou šifrovania WPA2 pre ochranu prenášaných dát.

#### 2. **\*\*Konfiguračné parametre:\*\***

- Na strane bodu-miesta (AP) je potrebné nastaviť sieťové parametre, vrátane SSID, šifrovania (WPA2) a priradenia kanálu.

- Na strane bodu-bodu (Bridge) je potrebné nastaviť rovnaké sieťové parametre ako na strane bodu-miesta (AP), a taktiež zabezpečenie spoja (WPA2).

#### 3. **\*\*Umístnenie zariadení:\*\***

- Bod-miesto (AP) by mal byť umiestnený tak, aby mal priamy výhľad na bod-bodu (Bridge) a minimalizoval prekážky medzi nimi.

- Bod-bodu (Bridge) by mal byť umiestnený na mieste s prekážkou, kde sa bude prekonávať prekážka (napr. budova, strom).

#### 4. **\*\*Materiálové náklady:\*\***

- Materiálové náklady budú závisieť od použitých zariadení a ich kvality. Priemerné náklady na jedno zariadenie (bod-miesto alebo bod-bodu) môžu byť v rozsahu od \$50 do \$200 alebo viac v závislosti od modelu a funkcií.
- Ďalšie náklady môžu zahŕňať príslušenstvo ako antény a montážne potreby.

Celkové materiálové náklady na vybudovanie dátového spoja pomocou technológie Wi-Fi môžu byť odhadované na \$100 až \$400 alebo viac v závislosti od konkrétnych potrieb, kvality zariadení a umiestnenia. Je dôležité zvážiť nielen cenu, ale aj spoľahlivosť a výkonnosť zariadení pri výbere riešenia.

#### - **vysvetlite postup kalkulácie nákladov pri výrobe Wi-Fi zariadení.**

Kalkulácia nákladov pri výrobe Wi-Fi zariadení je komplexný proces, ktorý zahŕňa rôzne faktory a fázy. Tu je postup, ako by sa mohli kalkulovať náklady pri výrobe Wi-Fi zariadení:

#### 1. **\*\*Identifikácia požiadaviek:\*\***

- Prvým krokom je identifikácia požiadaviek na Wi-Fi zariadenie. To zahŕňa určenie funkcií a špecifikácií, ako sú rýchlosť prenosu dát, dosah signálu, typy antén, podpora štandardov (napr. 802.11ac, 802.11ax), bezpečnostné funkcie a ďalšie.

#### 2. **\*\*Návrh a vývoj:\*\***

- Návrh a vývoj zahŕňajú vytvorenie hardvéru a softvéru zariadenia. To môže zahŕňať dizajn obvodu, výber komponentov, vývoj softvéru pre ovládanie a správu zariadenia, integráciu bezpečnostných funkcií a podobne.
- Tento krok tiež zahŕňa testovanie prototypov a vývojových vzoriek na overenie funkčnosti a zhody so špecifikáciami.

#### 3. **\*\*Výroba a montáž:\*\***

- Po schválení návrhu sa začína výroba a montáž zariadenia. To zahŕňa získanie komponentov a materiálov, výrobu dosiek plošných spojov (PCB), montáž komponentov na dosku, integrovanie antén, výrobu a montáž vonkajšej alebo vnútornej obálky a iné.

#### 4. **\*\*Testovanie a overovanie:\*\***

- Po montáži sa zariadenie testuje a overuje, aby sa zabezpečilo, že spĺňa špecifikácie a požiadavky. To zahŕňa testovanie prenosu dát, dosahu signálu, bezpečnostných funkcií, interoperability s inými zariadeniami a podobne.

#### 5. **\*\*Certifikácia a regulácie:\*\***

- Niektoré krajiny vyžadujú, aby boli Wi-Fi zariadenia certifikované a spĺňovali určité regulácie. To zahŕňa získanie certifikátov a povolení, ako aj splnenie pravidiel pre frekvencie, výkony a bezpečnosť.

#### 6. **\*\*Výrobné náklady:\*\***

- Výrobné náklady zahŕňajú náklady na materiály, pracovnú silu, náklady na výrobu a montáž, náklady na testovanie a certifikáciu, náklady na prevádzku továrne a iné prevádzkové náklady.

Celkové náklady pri výrobe Wi-Fi zariadenia sa stanovujú zahrnutím všetkých týchto faktorov. Je dôležité mať na pamäti, že ceny komponentov a náklady na výrobu sa môžu meniť v závislosti od trhu, technologických zmien a iných faktorov.

# IP ADRESNÝ PLÁN PRE IPv4

## - vysvetlite význam a opodstatnenie IP adries

IP adresy (Internet Protocol addresses) sú identifikátory priradené každému zariadeniu pripojenému do počítačovej siete, čo umožňuje identifikáciu a komunikáciu medzi týmito zariadeniami v rámci siete. Ich význam a opodstatnenie spočíva v niekoľkých kľúčových aspektoch:

### 1. \*\*Unikátna identifikácia:\*\*

- IP adresy poskytujú jedinečnú identifikáciu každého zariadenia v sieti, čo umožňuje spoľahlivú komunikáciu medzi nimi.

- Každá IP adresa je unikátna v rámci svojej siete a umožňuje zariadeniam efektívne identifikovať a lokalizovať cieľové zariadenie.

### 2. \*\*Adresácia a smerovanie:\*\*

- IP adresy sú nevyhnutné pre proces adresácie a smerovania dát v sieti. Pomáhajú smerovačom určiť cieľovú destináciu dát a zabezpečiť ich presun z jedného zariadenia do druhého cez rôzne smerovače a siete.

### 3. \*\*Identifikácia siete a hosta:\*\*

- IP adresy sa skladajú z dvoch hlavných častí: sít'ovej adresy a hostiteľskej adresy. Sít'ová adresa identifikuje sieť, do ktorej je zariadenie pripojené, zatiaľ čo hostiteľská adresa identifikuje konkrétne zariadenie v tejto sieti.

### 4. \*\*Komunikácia a služby:\*\*

- IP adresy umožňujú zariadeniam komunikovať medzi sebou v rámci lokálnej siete alebo cez internet. Poskytujú základnú infraštruktúru pre poskytovanie rôznych služieb, ako sú e-mail, webové prehliadače, súbory a iné.

### 5. \*\*Virtuálne a vzdialené pripojenie:\*\*

- IP adresy umožňujú vzdialeným zariadeniam pripojiť sa k sieti cez internet pomocou virtuálnych súkromných sietí (VPN) alebo iných technológií, čím umožňujú vzdialený prístup a správu zariadení a zdrojov.

Celkovo možno povedať, že IP adresy sú kľúčové pre fungovanie internetu a počítačových sietí, pretože umožňujú identifikáciu, adresáciu, smerovanie a komunikáciu medzi rôznymi zariadeniami a sieťami. Bez IP adries by bolo ťažké alebo dokonca nemožné efektívne využívať a spravovať súčasné počítačové siete a služby.

## - definujte triedy IP adries v IPv4

V IPv4 (Internet Protocol version 4) sú IP adresy rozdelené do niekoľkých tried, ktoré určujú rozsah adries a ich použitie v sieti. Triedy IP adries v IPv4 sú:

### 1. \*\*Trieda A:\*\*

- Trieda A adresy majú prvý oktet adres vyhradený pre sieťovú identifikáciu, zatiaľ čo zvyšné tri oktety sú priradené hostiteľom.
- Rozsah adres pre triedu A je od 1.0.0.0 do 126.255.255.255.
- Trieda A umožňuje veľké množstvo adres, ale má len niekoľko sietí s veľkým počtom hostiteľov.

## 2. \*\*Trieda B:\*\*

- Trieda B adresy majú prvých dva oktety vyhradené pre sieťovú identifikáciu, zatiaľ čo zvyšné dva oktety sú priradené hostiteľom.
- Rozsah adres pre triedu B je od 128.0.0.0 do 191.255.255.255.
- Trieda B umožňuje stredné množstvo adres a sietí s mierne menším počtom hostiteľov ako trieda A.

## 3. \*\*Trieda C:\*\*

- Trieda C adresy majú prvých tri oktety vyhradené pre sieťovú identifikáciu, zatiaľ čo posledný oktet je priradený hostiteľom.
- Rozsah adres pre triedu C je od 192.0.0.0 do 223.255.255.255.
- Trieda C poskytuje veľké množstvo sietí s malým počtom hostiteľov, čo je ideálne pre malé a stredné siete.

## 4. \*\*Trieda D (multicast):\*\*

- Trieda D adresy sú vyhradené pre multicastovú komunikáciu, čo umožňuje zasielať dáta viacerým príjemcom naraz.
- Rozsah adres pre triedu D je od 224.0.0.0 do 239.255.255.255.
- Adresy triedy D nie sú priradené konkrétnym hostiteľom alebo sieťam, ale používajú sa na multicastovú komunikáciu.

## 5. \*\*Trieda E (rezervované):\*\*

- Trieda E adresy sú rezervované pre budúce alebo experimentálne použitie a nie sú v súčasnosti používané v bežných sieťových aplikáciách.
- Rozsah adres pre triedu E je od 240.0.0.0 do 255.255.255.255.

Tieto triedy boli pôvodne navrhnuté pre organizáciu a alokáciu IP adres, ale v dnešnej dobe sa používa adresovanie pomocou prefixov (CIDR), ktoré umožňuje flexibilnejšie priradzovanie adres.

### - **analyzujte význam jednotlivých bajtov IP adresy v IPv4**

V IPv4 adrese je každá adresa rozdelená na štyri bajty, z ktorých každý je základnou jednotkou adresácie. Každý bajt obsahuje 8 bitov, čo umožňuje reprezentovať čísla od 0 do 255. Analyzujeme význam jednotlivých bajtov v IPv4 adrese:

## 1. \*\*Prvý bajt:\*\*

- Prvý bajt určuje sieťovú triedu adresy. Sieťová trieda určuje, ako sú adresy rozdelené a používané v sieti. Prvý bajt tiež indikuje rozsah adres a typ siete. Napríklad, ak je prvý bajt v rozsahu od 1 do 126, ide o adresu triedy A. Ak je v rozsahu od 128 do 191, ide o adresu triedy B. Od 192 do 223 je trieda C. Adresy s prvým bajtom 224 a vyššie sú vyhradené pre špeciálne účely.

## 2. **\*\*Druhý bajt:\*\***

- Druhý bajt je tiež súčasťou sieťovej adresy a spolu s prvým bajtom určuje rozsah adresy siete. V adresách triedy A určuje prvý a druhý bajt celkový rozsah adres siete.

## 3. **\*\*Tretí bajt:\*\***

- Tretí bajt spolu s prvým a druhým bajtom určuje konkrétnu sieťovú adresu. V adresách triedy A a B spolu s prvým a druhým bajtom tvorí identifikátor siete. V adresách triedy C je tretí bajt identifikátorom siete.

## 4. **\*\*Štvrtý bajt:\*\***

- Štvrtý bajt určuje hostiteľskú adresu v sieti. Tento bajt identifikuje konkrétny hostiteľ alebo zariadenie v danej sieti. Každý hostiteľ v sieti má svoju jedinečnú hostiteľskú adresu.

Spolu tieto štyri bajty tvoria jednu IPv4 adresu, ktorá je použitá na identifikáciu konkrétneho zariadenia v počítačovej sieti. Adresa siete (prvé tri bajty) a hostiteľská adresa (posledný bajt) spolu tvoria jedinečnú identifikáciu zariadenia v sieti. Týmto spôsobom je možné rozhodnúť, do ktorej siete patrí daná adresa a ktorý konkrétny hostiteľ je identifikovaný touto adresou.

### - **určte možnosti podsieťovania aj s adresnými kapacitami v IP adresách triedy C,**

V triede C IPv4 adres (s rozsahom od 192.0.0.0 do 223.255.255.255) je sieťová adresa reprezentovaná prvými trojicou oktetov, teda prvými 24 bitmi, zatiaľ čo posledný oktet, teda posledných 8 bitov, slúži na identifikáciu jednotlivých hostiteľov v sieti. Možnosti podsieťovania v triede C IPv4 adres umožňujú flexibilné priradovanie adres jednotlivým podsietiam v rámci určitej siete.

Pri podsieťovaní je potrebné vyčleniť určitý počet bitov pre identifikáciu podsietí a zvyšné bity pre identifikáciu hostiteľov v rámci každej podsiete. Počet bitov vyčlenených pre identifikáciu podsiete je známy ako "prefix" alebo "prefixová dĺžka" a umožňuje definovať veľkosť podsiete.

V prípade triedy C je možné vyčleniť rôzny počet bitov pre identifikáciu podsietí, čo má za následok rôzne veľkosti podsietí a počet použiteľných adres v každej podsieti. Tu sú niektoré možné varianty podsieťovania triedy C IPv4 adres s príkladmi prefixových dĺžok a ich adresných kapacít:

### 1. **\*\*/24 (255.255.255.0):\*\***

- Tento formát používa predvolenú subnet masku triedy C. Poskytuje 256 adres v každej podsieti (254 použiteľných adres pre hostiteľov, jedna pre sieťovú adresu a jedna pre broadcast adresu).

### 2. **\*\*/25 (255.255.255.128):\*\***

- Poskytuje 128 adres v každej podsieti (126 použiteľných adres pre hostiteľov, jedna pre sieťovú adresu a jedna pre broadcast adresu).

### 3. **\*\*/26 (255.255.255.192):\*\***

- Poskytuje 64 adres v každej podsieti (62 použiteľných adres pre hostiteľov, jedna pre sieťovú adresu a jedna pre broadcast adresu).

#### 4. **\*\*/27 (255.255.255.224):\*\***

- Poskytuje 32 adries v každej podsieti (30 použiteľných adries pre hostiteľov, jedna pre sieťovú adresu a jedna pre broadcast adresu).

A tak ďalej. Prefixová dĺžka /24 je najbežnejšie používaná pre malé a stredne veľké siete, zatiaľ čo menšie prefixové dĺžky sa často používajú v rozsiahlejších sieťach, kde je potrebné efektívnejšie využitie adries. Je dôležité si všimnúť, že čím menší je prefix, tým viac podsietí môže byť vytvorených, ale menej adries bude k dispozícii pre každú podsieť.

#### - **porovnajte vplyv vytvoreného podsiet'ovania na parametre siete**

Vytváranie podsietí má významný vplyv na parametre siete a môže ovplyvniť rôzne aspekty siete, vrátane adresácie, výkonu, efektívnosti využitia adries a správy siete. Tu je porovnanie vplyvu vytvoreného podsiet'ovania na niektoré kľúčové parametre siete:

##### 1. **\*\*Adresácia:\*\***

- Podsiet'ovanie umožňuje efektívne využívanie dostupných IP adries v sieti tým, že rozdelí celú adresnú rozsahu na menšie bloky adries pre každú podsieť. Tým sa minimalizuje množstvo nevyužitých adries a umožňuje flexibilné prirad'ovanie adries pre každú podsieť podľa potreby.

##### 2. **\*\*Výkon a prenosová rýchlosť:\*\***

- Podsiet'ovanie môže mať pozitívny vplyv na výkon a prenosovú rýchlosť siete tým, že umožňuje lepšiu správu sieťového toku a zamedzenie nadmernej záťaže na jednotlivých segmentoch siete. Rovnomerne rozdelené podsiete môžu minimalizovať množstvo prenosových kolízií a zlepšiť celkový výkon siete.

##### 3. **\*\*Správa siete:\*\***

- Podsiet'ovanie zjednodušuje správu siete tým, že umožňuje lepšiu segmentáciu a organizáciu siete. Administrátor môže jednoduchšie sledovať a spravovať každú podsieť samostatne, čo uľahčuje diagnostiku problémov, prirad'ovanie adries a implementáciu bezpečnostných politík.

##### 4. **\*\*Bezpečnosť:\*\***

- Vytváranie podsietí môže zlepšiť bezpečnosť siete tým, že umožní implementáciu lepších bezpečnostných politík a kontrol prístupu. Každá podsieť môže mať svoje vlastné bezpečnostné nastavenia a firewall pravidlá, čím sa zvýši ochrana siete pred neoprávneným prístupom a útokmi.

##### 5. **\*\*Škálovateľnosť:\*\***

- Podsiet'ovanie umožňuje zvýšiť škálovateľnosť siete tým, že umožňuje ľahké pridávanie nových zariadení a rozširovanie siete bez výrazného vplyvu na celkovú infraštruktúru siete. Nové podsiete môžu byť jednoducho vytvorené podľa potreby a integrované do existujúcej siete.

Celkovo možno povedať, že vytváranie podsietí má pozitívny vplyv na parametre siete tým, že zlepšuje adresáciu, výkon, správu, bezpečnosť a škálovateľnosť siete. To robí z podsiet'ovania kľúčový nástroj pre efektívne riadenie a optimalizáciu sietí rôznych veľkostí a komplexity.

#### - **vytvorte IP adresný plán podľa priložených podkladov (projektová dokumentácia) alebo podľa vlastného návrhu**

Bohužiaľ, ako AI model, nemám prístup k externým súborom alebo príloham, takže nemôžem vytvoriť IP adresný plán na základe priložených podkladov. Avšak, môžem Vám poskytnúť príklad IP adresného plánu na základe typických potrieb siete.

Predpokladajme, že máme sieť s viacerými oddeleniami v kancelárii a potrebujeme vytvoriť IP adresný plán pre každé oddelenie a sieťové zariadenia.

### Príklad IP adresného plánu:

1. **\*\*Oddelenie IT:\*\***

- Sieťová adresa: 192.168.1.0/24
- Rozsah pre počítače: 192.168.1.1 - 192.168.1.100
- Rozsah pre tlačiarne: 192.168.1.101 - 192.168.1.110
- Rozsah pre servere: 192.168.1.111 - 192.168.1.120
- Gateway: 192.168.1.254

2. **\*\*Oddelenie Marketing:\*\***

- Sieťová adresa: 192.168.2.0/24
- Rozsah pre počítače: 192.168.2.1 - 192.168.2.100
- Rozsah pre tlačiarne: 192.168.2.101 - 192.168.2.110
- Rozsah pre konferenčné miestnosti: 192.168.2.111 - 192.168.2.120
- Gateway: 192.168.2.254

3. **\*\*Oddelenie Vývoja:\*\***

- Sieťová adresa: 192.168.3.0/24
- Rozsah pre počítače: 192.168.3.1 - 192.168.3.100
- Rozsah pre tlačiarne: 192.168.3.101 - 192.168.3.110
- Rozsah pre vývojové servery: 192.168.3.111 - 192.168.3.120
- Gateway: 192.168.3.254

4. **\*\*Bezpečnostná kamera:\*\***

- Sieťová adresa: 192.168.4.0/24
- Rozsah pre kamery: 192.168.4.1 - 192.168.4.50
- Gateway: 192.168.4.254

5. **\*\*Hostovanie verejnej webovej stránky:\*\***

- Sieťová adresa: 192.168.5.0/24
- Rozsah pre webové servery: 192.168.5.1 - 192.168.5.10
- Gateway: 192.168.5.254

Toto je len príklad IP adresného plánu. Skutočný IP adresný plán by mal byť navrhnutý v súlade s konkrétnymi potrebami a požiadavkami siete. Je dôležité dbať na dostatočný počet adries pre každú podsieť a zvoliť vhodné prefixové dĺžky pre každú podsieť v závislosti od očakávanej veľkosti a počtu zariadení.

- **napište IP adresy zariadení uvedených v priloženom zadani (alebo podľa vlastného návrhu)**

- **zistíte na PC IP adresu, ktorá je na ňom nakonfigurovaná**
- **analyzujete, prečo IP adresný plán podľa IPv4 nemá potrebnú adresnú kapacitu**
- **popíšete modernú formu platobného styku- elektronické bankovníctvo**

Elektronické bankovníctvo, známe aj ako internetové bankovníctvo alebo online bankovníctvo, je moderná forma platobného styku, ktorá umožňuje klientom banky vykonávať rôzne bankové transakcie prostredníctvom internetu alebo mobilných zariadení. Tento spôsob platobného styku prináša množstvo výhod a pohodlia pre používateľov a banky.

### Funkcie elektronického bankovníctva:

1. **\*\*Overenie účtu:\*\*** Používatelia môžu sledovať stav svojich účtov a transakcií online, čo im umožňuje mať neustály prehľad o svojich financiách.
2. **\*\*Prevody peňazí:\*\*** Elektronické bankovníctvo umožňuje klientom vykonávať prevody peňazí medzi ich vlastnými účtami, ale aj na účty iných osôb alebo iné banky, a to buď doma alebo v zahraničí.
3. **\*\*Platby faktúr:\*\*** Používatelia môžu vykonávať platby za faktúry a účty priamo cez internet, čo uľahčuje správu a reguláciu ich financií.
4. **\*\*Správa investícií:\*\*** Niektoré elektronické bankové platformy umožňujú klientom sledovať a spravovať svoje investície a portfóliá, ako aj vykonávať obchody na finančných trhoch.
5. **\*\*Karty a úvery:\*\*** Klienti môžu sledovať svoje kreditné a debetné karty, platiť úvery, žiadať o nové karty alebo zmeny limitov, všetko online.
6. **\*\*Služby zasielania správ:\*\*** Banky často poskytujú elektronické bankovníctvo aj na zasielanie dôležitých správ a upozornení klientom, ako sú transakčné upozornenia, pripomienky o platbách a podobne.

### Výhody elektronického bankovníctva:

- **\*\*Pohodlie a prístupnosť:\*\*** Klienti môžu vykonávať bankové operácie kedykoľvek a kdekoľvek, kde majú prístup k internetu.
- **\*\*Spolahlivosť a bezpečnosť:\*\*** Moderné elektronické bankové platformy ponúkajú vysokú úroveň bezpečnosti a šifrovanie, aby chránili citlivé údaje klientov.
- **\*\*Efektívnosť a úspora času:\*\*** Elektronické bankovníctvo eliminuje potrebu fyzickej návštevy banky alebo použitia bankomatov na vykonávanie transakcií.



- **\*\*Jednoduchosť správy financií:\*\*** Klienti majú neustály prehľad o svojich financiách, čo umožňuje lepšiu kontrolu a plánovanie.

Elektronické bankovníctvo je pre moderných ľudí neoddeliteľnou súčasťou ich finančného života a poskytuje rýchly, pohodlný a bezpečný spôsob riadenia ich finančných prostriedkov.

## **SMEROVANIE A SMEROVACIE PROTOKOLY**

### **- porovnajte statické a dynamické smerovanie (routing)**

Statické a dynamické smerovanie sú dva základné prístupy k riadeniu smerovania dátových paketov v počítačových sieťach. Tu je porovnanie oboch prístupov:

#### **1. \*\*Statické smerovanie:\*\***

- **\*\*Definícia:\*\*** Pri statickom smerovaní sú smerovacie informácie ručne nakonfigurované a nastavené administrátorom siete na každom smerovači. Každý smerovač má staticky definovanú smerovaciu tabuľku, ktorá určuje, kam majú byť dáta posielané na základe ciest k jednotlivým sieťovým segmentom.

##### **- \*\*Výhody:\*\***

- **Jednoduchosť:** Statické smerovanie je jednoduché na implementáciu a správu, pretože administrátor ručne definuje smerovacie informácie.

- **Predvídateľnosť:** Smerovacia cesta zostáva konštantná, čo znamená, že sa dá ľahko predpovedať a spravovať.

##### **- \*\*Nevýhody:\*\***

- **Nevhodné pre veľké siete:** Statické smerovanie môže byť neefektívne a nepraktické pre veľké a komplexné siete, kde sa topológia často mení.

- **Časovo náročné:** Ručné nastavenie statických smerovacích informácií môže byť časovo náročné a náchylné na chyby.

#### **2. \*\*Dynamické smerovanie:\*\***

- **\*\*Definícia:\*\*** Dynamické smerovanie využíva smerovacie protokoly, ktoré umožňujú smerovačom komunikovať a automaticky sa dohodnúť na optimálnych cestách pre prenos dátových paketov. Smerovacie protokoly ako RIP (Routing Information Protocol), OSPF (Open Shortest Path First) a BGP (Border Gateway Protocol) sú bežne používané v dynamickom smerovaní.

##### **- \*\*Výhody:\*\***

- **Flexibilita:** Dynamické smerovacie protokoly umožňujú sieti prispôbiť sa zmenám topológie siete a zabezpečiť optimálne cesty pre dátový prenos.

- **Efektívnosť:** Vďaka schopnosti automaticky aktualizovať smerovacie informácie je dynamické smerovanie efektívnejšie v dynamických prostrediach.

##### **- \*\*Nevýhody:\*\***

- **Komplexnosť:** Dynamické smerovacie protokoly sú komplexnejšie na implementáciu a správu v porovnaní so statickým smerovaním.

- **Možnosť chýb:** Dynamické smerovanie môže byť náchylné na chyby a problémy, najmä ak nie je správne konfigurované alebo monitorované.

Celkovo vzaté, statické a dynamické smerovanie majú svoje vlastné výhody a nevýhody a vhodnosť každého prístupu závisí od veľkosti a komplexnosti siete, ako aj od potrieb a preferencií konkrétnej organizácie.

- **zhodnot'te úlohu routra v počítačovej sieti**

Úloha routra v počítačovej sieti je kritická a zahrňuje niekoľko dôležitých funkcií a úloh, ktoré umožňujú efektívne a spoľahlivé fungovanie siete. Tu je zhodnotenie niektorých z hlavných úloh a funkcií, ktoré routery vykonávajú v počítačových sieťach:

1. **\*\*Smerovanie dátových paketov:\*\***

- Hlavná úloha routra je smerovanie dátových paketov medzi rôznymi sieťovými segmentmi alebo medzi rôznymi sieťami. Router rozhoduje, kadiaľ majú byť pakety posielané na základe smerovacej tabuľky a informácií, ktoré získa od susedných smerovačov.

2. **\*\*Vydávanie IP adries:\*\***

- Mnohé routery môžu slúžiť aj ako DHCP (Dynamic Host Configuration Protocol) server, ktorý automaticky pridáva IP adresy zariadeniam pripojeným k sieti. Týmto spôsobom routery uľahčujú konfiguráciu siete a znižujú administratívnu záťaž.

3. **\*\*Zabezpečenie siete:\*\***

- Routery poskytujú rôzne bezpečnostné funkcie, vrátane firewallu a NAT (Network Address Translation), ktoré chránia sieť pred neoprávneným prístupom a útokmi z vonku. Firewall môže filtrovať dátové pakety a NAT umožňuje skryť vnútorné adresy siete za jednu verejnú IP adresu.

4. **\*\*Zmena topológie siete:\*\***

- Routery umožňujú flexibilitu a skalovateľnosť siete tým, že umožňujú pridávanie nových sietí a pripojenie nových zariadení bez potreby zásadných zmenových úprav. Týmto spôsobom sú schopné prispôbiť sa rôznym požiadavkám a potrebám siete.

5. **\*\*Optimalizácia smerovania:\*\***

- Niektoré routery môžu používať rôzne algoritmy smerovania, ako je napríklad OSPF (Open Shortest Path First) alebo EIGRP (Enhanced Interior Gateway Routing Protocol), ktoré optimalizujú cesty a zabezpečujú rýchle a efektívne smerovanie dátových paketov v sieti.

6. **\*\*Monitorovanie a diagnostika:\*\***

- Routery môžu poskytovať nástroje na monitorovanie a diagnostiku siete, čo umožňuje administrátorom sledovať stav siete, identifikovať problémy a riešiť ich v reálnom čase.

Celkovo vzaté, úloha routra v počítačovej sieti je kľúčová pre efektívne a spoľahlivé fungovanie siete. Routery zabezpečujú presmerovanie dátových paketov, poskytujú zabezpečenie siete, umožňujú zmenu topológie siete a optimalizujú smerovanie, čo robí ich nevyhnutnými zložkami modernej počítačovej siete.

- **popíšte vlastnosti sieťových protokolov**

Sieťové protokoly majú rôzne vlastnosti, ktoré určujú ich schopnosti, spôsob komunikácie a spôsob, ako riadia prenos dát v počítačových sieťach. Tu sú niektoré z hlavných vlastností sieťových protokolov:

1. **\*\*Adresovanie:\*\***

- Sieťové protokoly umožňujú adresovanie zariadení a služieb v sieti pomocou unikátnych identifikátorov, ako sú IP adresy, MAC adresy alebo portové čísla.

2. **\*\*Smerovanie:\*\***

- Niektoré sieťové protokoly zabezpečujú smerovanie dátových paketov medzi rôznymi zariadeniami a sieťami. Tieto protokoly určujú cestu, ktorou majú byť dáta poslané na základe topológie siete a smerovacej tabuľky.

3. **\*\*Spôsob komunikácie:\*\***

- Sieťové protokoly môžu podporovať rôzne spôsoby komunikácie medzi zariadeniami, vrátane unicastu (jednoznačného prenosu dát do konkrétneho zariadenia), multicastu (preposielania dát do skupiny zariadení) a broadcastu (preposielania dát do všetkých zariadení v sieti).

4. **\*\*Šifrovanie a bezpečnosť:\*\***

- Niektoré sieťové protokoly poskytujú šifrovanie dát pre zabezpečenie komunikácie a ochranu pred neoprávneným prístupom. Tieto protokoly môžu zahŕňať SSL/TLS (Secure Sockets Layer/Transport Layer Security) pre webovú komunikáciu alebo IPSec (Internet Protocol Security) pre virtuálne privátne siete (VPN).

5. **\*\*Výkon a spôsobilosť:\*\***

- Niektoré sieťové protokoly majú lepšiu výkonnosť a spôsobilosť pre rôzne aplikácie a požiadavky siete. Napríklad protokoly ako UDP (User Datagram Protocol) majú nižšiu latenciu a menšiu záťaž siete ako TCP (Transmission Control Protocol), ale nemajú zabudovanú spätnú väzbu na overovanie doručenia paketov.

6. **\*\*Modularita a rozšíriteľnosť:\*\***

- Niektoré sieťové protokoly sú navrhnuté s modulárnym a rozšíriteľným dizajnom, ktorý umožňuje pridávať nové funkcie a vlastnosti bez zásadných zmien v existujúcej infraštruktúre siete. Tieto protokoly sú flexibilné a prispôsobiteľné meniacim sa potrebám siete.

7. **\*\*Kompatibilita a interoperabilita:\*\***

- Dôležitou vlastnosťou sieťových protokolov je ich schopnosť spolupracovať s inými zariadeniami a protokolmi v sieti. Kompatibilné a interoperabilné protokoly umožňujú rôznym zariadeniam a systémom komunikovať a pracovať spolu bez problémov.

Tieto vlastnosti určujú schopnosti a použitie jednotlivých sieťových protokolov v počítačových sieťach a ovplyvňujú ich účinnosť a výkon. Je dôležité zvážiť tieto vlastnosti pri výbere a implementácii sieťových protokolov v sieti.

- **načrtnite spôsoby nastavenia komunikácie v sieti LAN**

Nastavenie komunikácie v sieti LAN (Local Area Network) môže byť dosiahnuté pomocou niekoľkých spôsobov. Tu sú niektoré z hlavných spôsobov nastavenia komunikácie v sieti LAN:

1. **\*\*Statické priradenie IP adries:\*\***

- Administrátor siete môže ručne priradiť statické IP adresy každému zariadeniu v sieti. Tento spôsob umožňuje presnú kontrolu nad priradením adries a umožňuje jednoduchú identifikáciu zariadení v sieti.

2. **\*\*Použitie DHCP:\*\***

- Dynamický protokol priradzovania adries (DHCP) je automatický spôsob priradenia IP adries zariadeniam v sieti. DHCP server automaticky priradí IP adresy zariadeniam, keď sa pripoja k sieti, čo zjednodušuje proces správy siete.

3. **\*\*Konfigurácia smerovača:\*\***

- Smerovač (router) môže byť konfigurovaný na preposielanie paketov medzi rôznymi sieťovými segmentmi v rámci LAN. Týmto spôsobom môžu zariadenia v rôznych častiach siete komunikovať medzi sebou.

4. **\*\*Použitie sieťových pravidiel a firewallu:\*\***

- Sieťové pravidlá a firewally môžu byť použité na riadenie prístupu a komunikácie v sieti LAN. Administrátor môže definovať pravidlá, ktoré určujú, ktoré typy komunikácie sú povolené alebo blokové medzi rôznymi zariadeniami v sieti.

5. **\*\*Vytváranie VLAN:\*\***

- Virtual LAN (VLAN) umožňuje segmentovať fyzickú sieť na logické skupiny na základe funkčných alebo organizačných kritérií. Týmto spôsobom môžu byť zariadenia v rôznych VLAN komunikovať medzi sebou, ale nie s zariadeniami v iných VLAN.

6. **\*\*Použitie sieťových protokolov:\*\***

- Sieťové protokoly ako TCP/IP, UDP a ICMP sú používané na riadenie komunikácie medzi zariadeniami v sieti LAN. Tieto protokoly definujú formát a pravidlá pre prenos dát medzi zariadeniami.

7. **\*\*Aktivácia a konfigurácia sieťových služieb:\*\***

- Sieťové služby ako sú samba, NFS, FTP a HTTP umožňujú zdieľanie súborov, tlačiarenských zariadení a ďalších zdrojov medzi zariadeniami v sieti LAN. Aktivácia a konfigurácia týchto služieb umožňuje zlepšiť komunikáciu a zdieľanie zdrojov v sieti.

Tieto spôsoby umožňujú nastaviť a riadiť komunikáciu v sieti LAN v závislosti od potrieb a požiadaviek organizácie alebo používateľa. Každý spôsob má svoje vlastné výhody a nevýhody a môže byť vhodný pre rôzne typy sietí a prostredí.

- **porovnajte hlavičky IPv4 a IPv6 protokolov**

Hlavičky IPv4 a IPv6 protokolov sú základnými časťami dátových paketov, ktoré sa používajú na prenos dát v počítačových sieťach. Tu je porovnanie hlavných rozdielov medzi hlavičkami IPv4 a IPv6:

1. **\*\*Veľkosť hlavičky:\*\***

- Hlavička IPv4 má fixnú veľkosť 20 bajtov, ale môže byť väčšia kvôli rôznym voľiteľným položkám a možnostiam.
- Hlavička IPv6 má fixnú veľkosť 40 bajtov bez ohľadu na prítomnosť voľiteľných položiek.

2. **\*\*Adresovanie:\*\***

- IPv4 používa 32-bitové IP adresy, ktoré majú formát x.x.x.x, kde x je číslo od 0 do 255.
- IPv6 používa 128-bitové IP adresy, ktoré majú formát xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, kde x je hexadecimálne číslo.

3. **\*\*Podpora možností:\*\***

- IPv4 hlavička obsahuje niekoľko voľiteľných položiek, ako sú možnosti voľby, identifikácia fragmentácie a kontrola chyby.
- IPv6 hlavička obsahuje veľmi málo voľiteľných položiek, pretože mnoho funkcií, ktoré boli voľiteľné v IPv4, sú v IPv6 integrované priamo do hlavičky alebo sú riešené inými spôsobmi.

4. **\*\*Fragmentácia:\*\***

- IPv4 podporuje fragmentáciu paketov na menšie časti v prípade, že sú príliš veľké na prenos cez sieťové segmenty s menšou maximálnou veľkosťou paketu (MTU).
- IPv6 zvyčajne neumožňuje fragmentáciu na smerovačiach. Fragmentácia je povolená len na koncových zariadeniach, ak je to nevyhnutné.

5. **\*\*Zabezpečenie:\*\***

- IPv4 nemá zabudované žiadne bezpečnostné mechanizmy. Pre zabezpečenie sa musia použiť dodatočné protokoly, ako je napríklad IPsec.
- IPv6 obsahuje integrovanú podporu pre bezpečnostné funkcie, ako sú autentifikácia a šifrovanie, prostredníctvom protokolu IPsec.

6. **\*\*Číslo verzie:\*\***

- IPv4 má hodnotu 4 v poli verzie.
- IPv6 má hodnotu 6 v poli verzie.

Tieto rozdiely v hlavičkách IPv4 a IPv6 protokolov sú dôležité pre rôzne aspekty sieťovej komunikácie, vrátane adresovania, fragmentácie, bezpečnosti a podpory rôznych možností. IPv6 bol navrhnutý s cieľom adresovať niektoré nedostatky IPv4 a poskytnúť riešenia pre rastúce požiadavky na internetovú konektivitu.

- **zdôvodnite potrebu default gateway**

Default gateway je sieťový prvok, ktorý slúži ako „východ“ z lokálnej siete, ktorá umožňuje pripojeným zariadeniam komunikovať so zariadeniami mimo svojej lokálnej siete. Existujú nasledujúce dôvody, prečo je default gateway nevyhnutný v počítačových sieťach:

1. **\*\*Pristupový bod k externým sieťam:\*\*** Default gateway je povinný v prípade, že zariadenia v lokálnej sieti potrebujú komunikovať so zariadeniami mimo svojej lokality, ako sú zariadenia v iných lokálnych sieťach alebo internet.

2. **\*\*Presmerovanie paketov:\*\*** Keď zariadenie v lokálnej sieti potrebuje poslať paket do cieľovej siete, ktorá nie je priamo dostupná v jeho lokálnej sieti, použije sa default gateway na presmerovanie paketu na správnu destináciu.

3. **\*\*Prístup na internet:\*\*** V domácej alebo podnikovej sieti default gateway umožňuje pripojeným zariadeniam prístup na internet. Zariadenia v lokálnej sieti môžu odosielať požiadavky na internetové zdroje cez default gateway, ktorý ich potom smeruje cez internetovú bránu (gateway) do vonkajšej siete.

4. **\*\*Riadenie toku dát:\*\*** Default gateway môže slúžiť aj na riadenie toku dát v sieti. Môže napríklad filtrovať alebo presmerovať niektoré typy dátových tokov na základe nastavených pravidiel.

5. **\*\*Zabezpečenie siete:\*\*** Default gateway môže byť miestom, kde sú implementované bezpečnostné mechanizmy, ako sú firewally a filtrovanie obsahu. Pomáha to chrániť lokálnu sieť pred neoprávneným prístupom alebo útokmi z vonkajšieho prostredia.

Vzhľadom na tieto dôvody je default gateway nevyhnutným prvkom v počítačových sieťach, ktorý umožňuje pripojeným zariadeniam komunikovať s externými sieťami a zabezpečuje prístup na internet a ďalšie externé zdroje. Bez default gateway by boli zariadenia v izolácii a obmedzené na komunikáciu iba v rámci svojej lokálnej siete.

#### - **vysvetlite spôsoby zobrazenia rutovacej tabuľky**

Rutovacia tabuľka, tiež známa ako smerovacia tabuľka, je záznam obsahujúci informácie o cestách k dostupným sieťovým cieľom. Existuje niekoľko spôsobov, ako môže byť rutovacia tabuľka zobrazená a prezentovaná, vrátane nasledujúcich:

1. **\*\*Textový výstup v príkazovom riadku:\*\***

- Väčšina sieťových zariadení umožňuje administrátorovi zobraziť rutovacu tabuľku pomocou príkazu v príkazovom riadku, napríklad príkazy `show ip route` pre IPv4 alebo `show ipv6 route` pre IPv6 na Cisco smerovačoch. Textový výstup poskytuje podrobnosti o dostupných cestách, ich cieľových sieťach, metrikách a rozhraniach.

2. **\*\*Grafické užívateľské rozhranie (GUI):\*\***

- Niektoré sieťové manažérske nástroje poskytujú grafické užívateľské rozhranie, ktoré umožňuje zobraziť rutovacu tabuľku v prehľadnejšom a vizuálnejšom formáte. Tieto nástroje môžu zobrazovať informácie o smerovaní pomocou grafov, diagramov alebo tabuliek.

3. **\*\*Tabuľkové zobrazenie v webovom rozhraní:\*\***

- Niekedy je rutovacia tabuľka k dispozícii prostredníctvom webového rozhrania sieťového zariadenia, ako sú smerovače alebo prepínače. Administrátor môže prehliadať a zobrazovať informácie o smerovaní pomocou tabuľkového zobrazenia v rámci webového rozhrania.

#### 4. **\*\*Export do súboru:\*\***

- Niektoré sieťové zariadenia umožňujú exportovať rutovaciú tabuľku do súboru v určenom formáte, napríklad do formátu CSV alebo textového súboru. Tento súbor potom môže byť otvorený v textovom editore alebo ďalšom nástroji na analýzu.

#### 5. **\*\*Monitorovacie nástroje a aplikácie:\*\***

- Existujú rôzne monitorovacie nástroje a aplikácie, ktoré sú schopné monitorovať a zobrazovať informácie o smerovaní v sieťach. Tieto nástroje môžu zobrazovať rutovaciú tabuľku v reálnom čase a poskytovať ďalšie štatistiky a grafy súvisiace so smerovaním.

Zobrazenie rutovacej tabuľky je kľúčové pre administrátorov sietí, pretože poskytuje dôležité informácie o tom, ako sú dáta smerované v sieti. Rôzne spôsoby zobrazenia umožňujú administrátorom efektívne monitorovať a spravovať smerovanie v ich sieťach podľa ich preferencií a požiadaviek.

- **vyhl'adajte a zobrazte na počítači rutovaciú tabuľku**
- **popíšte nájdenú rutovaciú tabuľku**

## **PREPÍNAČE A APLIKÁCIA VLAN**

#### - **popíšte funkciu prepínača (switch)**

Prepínač (switch) je základné sieťové zariadenie, ktoré sa používa na lokálne prepájanie zariadení v rámci lokálnej počítačovej siete (LAN). Jeho hlavnou funkciou je preposielanie dátových rámcov medzi rôznymi zariadeniami v sieti podľa ich MAC adries. Tu je bližší popis funkcie prepínača:

##### 1. **\*\*Prepínanie rámcov:\*\***

- Prepínač dokáže analyzovať dátové rámčeky, ktoré prichádzajú na jeho porty, a následne ich preposiela iba na tie porty, ktoré sú určené cieľovým zariadeniam. Tým sa minimalizuje záťaž siete a zvyšuje sa efektívnosť prenosu dát.

##### 2. **\*\*Ukladanie MAC adries:\*\***

- Prepínač si uchováva tabuľku MAC adries, v ktorej je mapovaná každá známa MAC adresa na príslušný port, na ktorom je dané zariadenie pripojené. Táto tabuľka sa vytvára automaticky na základe komunikácie medzi zariadeniami a prepínačom.

##### 3. **\*\*Vysoká rýchlosť prenosu:\*\***

- Prepínač dokáže pracovať na vyšších rýchlostiach prenosu dát v porovnaní s hubom, pretože prenáša dáta iba na konkrétne porty podľa cieľových adries, nie na všetky porty siete ako hub.

##### 4. **\*\*Segmentácia siete:\*\***

- Pomocou prepínača je možné rozdeliť sieť na viaceré segmenty, čím sa znižuje záťaž siete a zvyšuje sa bezpečnosť a výkon komunikácie.

#### 5. **\*\*Autonegotiation a detekcia dátových rýchlostí:\*\***

- Prepínač dokáže automaticky detekovať dátové rýchlosti a konfigurácie pripojených zariadení a prispôbovať sa im pomocou autonegociácie.

Celkovo vzaté, prepínač je kľúčovým zariadením v počítačových sieťach, ktoré umožňuje efektívnu a spoľahlivú komunikáciu medzi rôznymi zariadeniami v rámci LAN siete. Jeho schopnosť efektívne preposielať dáta na základe MAC adres a udržiavať tabuľku mapovania MAC adres ho robí neodmysliteľnou súčasťou moderných počítačových sietí.

#### - **vysvetlite pojemmetóda kontroly k prístupu na médium**

Metóda kontroly prístupu k médiu (MAC - Media Access Control) je spôsob, ako sa zariadenia v počítačovej sieti snažia získať prístup k prenosovému médiu (napríklad kábel, bezdrôtový signál) na komunikáciu s ostatnými zariadeniami v sieti. Táto metóda je dôležitá pre správne riadenie prístupu k médiu a zabráňovanie kolíziám dátových rámcov, ktoré by mohli spôsobiť rušenie a zníženie výkonu siete. Existujú rôzne typy metód kontroly prístupu k médiu, ktoré sa používajú v závislosti od typu siete a použitých technológií. Tu sú niektoré z najbežnejších metód kontroly prístupu k médiu:

##### 1. **\*\*CSMA/CD (Carrier Sense Multiple Access with Collision Detection):\*\***

- Táto metóda je typická pre Ethernet siete, kde zariadenie najprv „poslúcha“ sieť, aby zistilo, či je médium voľné. Ak je voľné, zariadenie začne posielať svoje dáta. V prípade kolízie (keď sa viacero zariadení pokúša prenášať dáta súčasne) sa zariadenia snažia zistiť kolíziu a následne ju riešia pomocou algoritmu CD (Collision Detection).

##### 2. **\*\*CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):\*\***

- Tento prístup sa používa v bezdrôtových sieťach, ako je napríklad Wi-Fi. Zariadenia sledujú stav kanála a snažia sa predísť kolíziám pomocou metódy CA (Collision Avoidance). Zariadenia komunikujú pomocou signálov, ktoré oznamujú ich úmysel prenosu, a prípadne čakajú na náhodné oneskorenie pred prenosom, aby sa minimalizovala pravdepodobnosť kolízií.

##### 3. **\*\*Token Passing:\*\***

- Táto metóda sa často používa v káblových sieťach, kde sa „token“ (virtuálny signál) prenáša medzi zariadeniami v sieti. Len zariadenie, ktoré drží token, má povolenie posielať dáta. Po odoslaní dát token prechádza na ďalšie zariadenie.

##### 4. **\*\*Polling:\*\***

- Tento prístup je založený na tom, že riadiace zariadenie periodicky požiadava jednotlivé zariadenia v sieti o odoslanie dát. Tento prístup sa však používa menej často, pretože môže spôsobiť väčšie oneskorenie a môže byť menej efektívny v rôznych typoch sietí.

Metódy kontroly prístupu k médiu sú kľúčové pre správne fungovanie počítačových sietí a zabezpečujú, aby zariadenia v sieti mohli efektívne a spoľahlivo komunikovať bez zbytočných kolízií alebo konfliktov o prístup k médiu. Každá metóda má svoje vlastné výhody a nevýhody a je vhodná pre rôzne typy sietí a použití.

#### - **porovnajete funkciu LLC a MAC podvrstvy**



LLC (Logical Link Control) a MAC (Media Access Control) sú dve podvrstvy z rámca IEEE 802, ktoré sú súčasťou vrstvy údajovej prenosu (Data Link Layer) v OSI modeli. Tu je porovnanie ich funkcií:

1. **LLC (Logical Link Control):**

- **Funkcia:** LLC je zodpovedná za riadenie logických spojení medzi zariadeniami v počítačovej sieti. Riadi komunikáciu medzi sieťovou vrstvou (vrstva 3) a MAC podvrstvou. Taktiež poskytuje služby spoľahlivosti, riadenia toku a detekcie chýb.
- **Protokoly:** Používa protokoly ako napríklad HDLC (High-Level Data Link Control) alebo PPP (Point-to-Point Protocol), ktoré definujú spôsob riadenia logických spojení.

2. **MAC (Media Access Control):**

- **Funkcia:** MAC je zodpovedná za riadenie prístupu k prenosovému médiu (napríklad Ethernet, Wi-Fi) v počítačovej sieti. Riadi prístup jednotlivých zariadení k médiu a zabezpečuje, aby dáta boli prenášané bez kolízií.
- **Protokoly:** Definuje rôzne metódy kontroly prístupu k médiu (MAC protokoly) ako napríklad CSMA/CD (Carrier Sense Multiple Access with Collision Detection) pre Ethernet alebo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pre Wi-Fi.

**Porovnanie:**

- **Úroveň v modeli OSI:** Obidve podvrstvy sú súčasťou vrstvy údajovej prenosu (Data Link Layer) v OSI modeli.
- **Riadenie spojení vs. prístup k médiu:** LLC sa zaoberá riadením logických spojení a službami spoľahlivosti, zatiaľ čo MAC sa zaoberá riadením prístupu k fyzickému médiu a minimalizáciou kolízií dátových rámcov.
- **Protokoly:** LLC používa protokoly na riadenie spojení, zatiaľ čo MAC používa metódy kontroly prístupu k médiu, ktoré sú špecifické pre daný typ prenosového média (napríklad Ethernet, Wi-Fi).

V zásade LLC a MAC spolupracujú na správnom fungovaní vrstvy údajovej prenosu, pričom každá podvrstva má svoje vlastné úlohy a zodpovednosti voči vyšším a nižším vrstvám v rámci modelu OSI.

- **vysvetlite význam virtuálnych lokálnych sietí (VLAN)**

Virtuálne lokálne siete (VLAN) sú spôsob segmentácie fyzickej počítačovej siete na logické skupiny, ktoré môžu komunikovať medzi sebou, aj keď sú fyzicky umiestnené na rôznych častiach siete. Tento koncept umožňuje lepšiu organizáciu a správu siete a poskytuje viac flexibilitu v rámci jej správy a konfigurácie. Tu je význam VLAN:

1. **Segmentácia siete:**

- VLAN umožňuje administrátorom rozdeliť fyzickú sieť na logické segmenty na základe funkčných, organizačných alebo bezpečnostných potrieb. Tým sa znižuje prenos dát medzi rôznymi skupinami zariadení a zlepšuje sa bezpečnosť siete.

2. **Logická izolácia:**

- Zariadenia v rámci jednej VLAN môžu komunikovať medzi sebou, ale sú izolované od zariadení v iných VLAN. To znamená, že zariadenia v jednej VLAN nemôžu získavať prístup k zariadeniam v iných VLAN bez adekvátnej autentifikácie a povolení.

### 3. **\*\*Optimalizácia sieťového toku:\*\***

- VLAN umožňuje lepšiu kontrolu a optimalizáciu sieťového toku, pretože komunikácia v rámci jednej VLAN je obmedzená na zariadenia v tej istej VLAN. Tým sa znižuje preťaženie siete a zvyšuje sa jej výkon.

### 4. **\*\*Zlepšená bezpečnosť:\*\***

- VLAN umožňuje implementáciu bezpečnostných politík na úrovni skupín zariadení, čo zvyšuje bezpečnosť siete. Administrátor môže priradovať prístupové kontroly na základe VLAN, čím sa minimalizuje riziko neoprávneného prístupu alebo šírenia hrozieb v sieti.

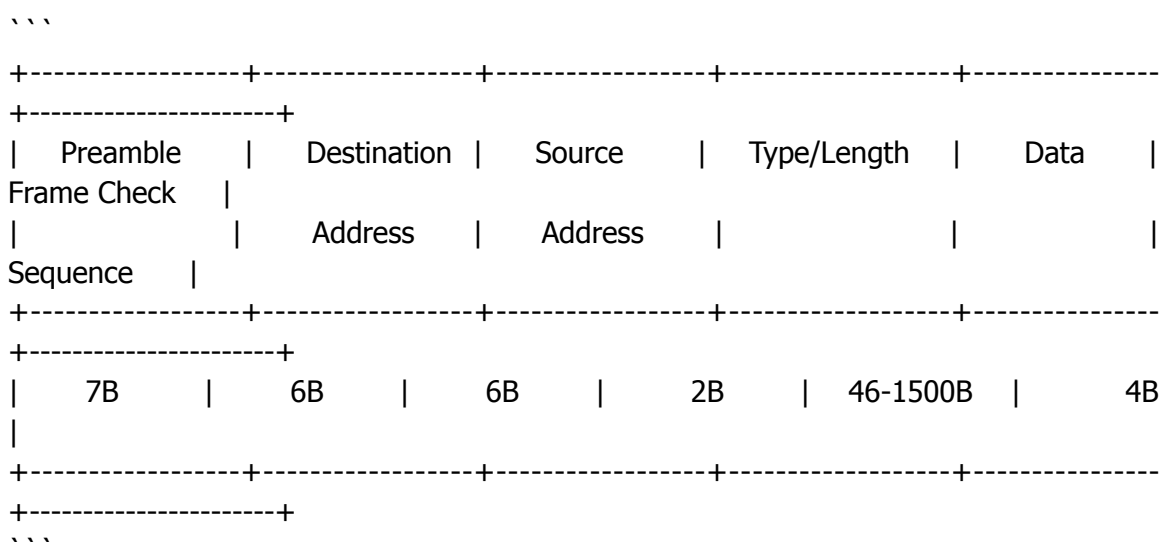
### 5. **\*\*Flexibilita a správa:\*\***

- VLAN poskytuje administrátorom flexibilitu a jednoduchosť pri správe siete. Zmeny v konfigurácii siete môžu byť ľahko vykonané na úrovni VLAN, čo umožňuje rýchlu a efektívnu reakciu na potreby siete a zmeny v organizácii.

Celkovo vzaté, VLAN je užitočný nástroj na segmentáciu a organizáciu fyzickej počítačovej siete, čo umožňuje lepšiu správu, bezpečnosť a výkon siete. Pomáha optimalizovať sieťový tok a poskytuje administrátorom viac možností kontroly nad sieťou vo vzťahu k jej používateľom a aplikáciám.

## - **načrtnite štruktúru rámca (frame)**

Štruktúra rámca (frame) je základným formátom pre prenos dát v rámci počítačových sietí, najmä na úrovni vrstvy údajovej prenosu (Data Link Layer) v OSI modeli. Tu je typická štruktúra rámca:



### 1. **\*\*Preamble (Preambula):\*\***

- Preambula je séria bitov, ktoré oznamujú príchod rámca a umožňujú synchronizáciu prijímateľa s vysielateľom. Zvyčajne pozostáva z 7 bajtov.

2. **\*\*Destination Address (Adresa cieľa):\*\***

- Adresa cieľa je MAC adresa (Media Access Control), ktorá identifikuje zariadenie, pre ktoré je rámec určený. Zvyčajne má veľkosť 6 bajtov.

3. **\*\*Source Address (Zdrojová adresa):\*\***

- Zdrojová adresa je MAC adresa zariadenia, ktoré rámec vysiela. Zvyčajne má veľkosť 6 bajtov.

4. **\*\*Type/Length (Typ/Dĺžka):\*\***

- Toto pole obsahuje informáciu buď o type dát v rámci (napr. IP, ARP, IPv6) alebo o dĺžke dát. Zvyčajne má veľkosť 2 bajty.

5. **\*\*Data (Dáta):\*\***

- Táto časť obsahuje samotné užitočné dáta, ktoré sú prenášané cez sieť. Ich veľkosť môže byť od 46 do 1500 bajtov.

6. **\*\*Frame Check Sequence (Kontrolný súčet rámca):\*\***

- Toto pole obsahuje kontrolný súčet pre dáta v rámci, ktorý sa používa na detekciu chýb v prenášaných dátach. Zvyčajne má veľkosť 4 bajty.

Celková dĺžka rámca môže byť rôzna v závislosti od typu siete a použitých technológií. V prípade Ethernetu je maximálna dĺžka rámca 1518 bajtov, vrátane preambuly a kontrolného súčtu, avšak minimálna dĺžka rámca je 64 bajtov. Štruktúra rámca sa môže líšiť v závislosti od špecifikácií konkrétnej siete a protokolu použitého na prenos dát.

- **popíšte spôsoby tvorby tabuľky MAC adries na switch**

Tabuľka MAC adries na prepínači (switch) sa vytvára automaticky v priebehu prevádzky siete na základe komunikácie medzi zariadeniami v sieti a prepínačom. Existujú rôzne spôsoby, ako sa táto tabuľka MAC adries vytvára a aktualizuje:

1. **\*\*Learnovanie adries (Learning):\*\***

- Základným spôsobom tvorby tabuľky MAC adries je proces learnovania. Keď prepínač prijme dátový rámec od zariadenia na určitom porte, zaznamená si MAC adresu odosielateľa a asociačné informácie o tom, na ktorom porte sa táto adresa nachádza. Tento proces sa opakuje pre každý rámec, ktorý prepínač prijme, čo umožňuje postupné zostavovanie tabuľky MAC adries.

2. **\*\*Vysielanie (Floodovanie):\*\***

- Ak prepínač dostane rámec s cieľovou MAC adresou, ktorá nie je zaznamenaná v jeho tabuľke MAC adries, môže sa rozhodnúť preposlať tento rámec na všetky svoje porty (s výnimkou portu, na ktorom ho prijal). Tento proces sa nazýva floodovanie a pomáha prepínaču zistiť, ktorý port je správny pre danú MAC adresu. Keď zariadenie s danou MAC adresou odpovie, prepínač si túto informáciu zaznamená do svojej tabuľky MAC adries.

3. **\*\*Aging (Starnutie):\*\***

- Tabuľka MAC adries má aj mechanizmus starnutia, čo znamená, že záznamy v nej môžu byť automaticky odstránené po určitom čase, ak sa z daného portu neaktualizujú.

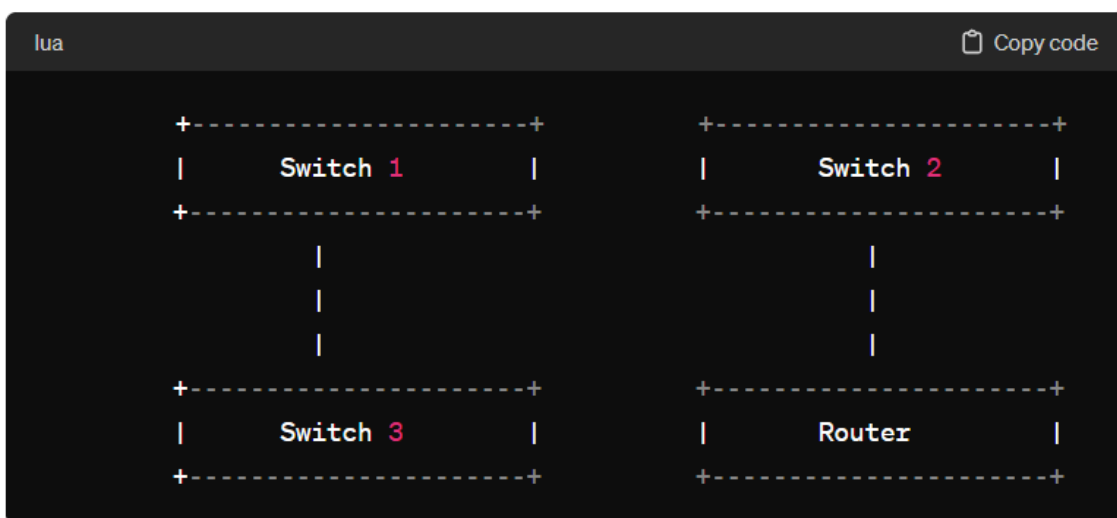
Tento proces pomáha udržiavať tabuľku aktuálnu a zabrániť neefektívnemu využitiu zdrojov.

#### 4. **\*\*Ručné nastavenie (Statická konfigurácia):\*\***

- Administrátor má tiež možnosť manuálne pridať záznamy do tabuľky MAC adries. Tento prístup sa používa v prípade, že je potrebné zabezpečiť konkrétne pripojenie určitého zariadenia k určitému portu na prepínači.

Všetky tieto spôsoby spolupracujú na tvorbe a udržiavaní tabuľky MAC adries na prepínači, čo je nevyhnutné pre správne fungovanie sieťového prepínača a efektívne routovanie dát medzi zariadeniami v sieti.

- **načrtnite schému zapojenia troch switchov pripojených k smerovaču (routru)**  
Tu je jednoduché schéma zapojenia troch prepínačov (Switch) pripojených k smerovaču (Router) pomocou Ethernetových káblov:



V tomto zapojení sú všetky tri prepínače (Switch 1, Switch 2, Switch 3) pripojené k smerovaču (Router) prostredníctvom Ethernetových káblov. Každý prepínač je reprezentovaný štvorcovým blokom a smerovač je reprezentovaný obdĺžnikovým blokom.

Ethernetové káble sú použité na prepojenie všetkých troch prepínačov so smerovačom. Toto zapojenie umožňuje všetkým zariadeniam pripojeným k jednotlivým prepínačom komunikovať medzi sebou a tiež smerovačom, čo umožňuje prístup k internetu alebo k ďalším sieťovým zdrojom, ktoré sú pripojené k smerovaču.

- **zhodnot'ite možnosti a spôsoby vzdialeného prístupu na switch**

Existuje niekoľko možností, ako môžete zabezpečiť vzdialený prístup k sieťovému prepínaču (switch). Tu sú niektoré z najbežnejších spôsobov:

Telnet:

- Telnet je protokol pre vzdialený prístup, ktorý umožňuje administrátorom pripojiť sa k sieťovému prepínaču cez TCP/IP sieť a pracovať s jeho konfiguráciou a riadením. Telnet však neposkytuje šifrovanie, čo môže viesť k riziku úniku citlivých údajov (napríklad hesiel) cez sieť.

SSH (Secure Shell):

- SSH je šifrovaný protokol pre vzdialený prístup, ktorý umožňuje bezpečnú komunikáciu medzi administrátorom a sieťovým prepínačom. SSH poskytuje silné šifrovanie dát a autentifikáciu, čo robí túto možnosť vhodnou pre vzdialený prístup v bezpečnostne citlivých prostrediach.

Web rozhranie:

- Mnoho moderných prepínačov poskytuje webové rozhranie, cez ktoré môžete pristupovať a spravovať prepínač pomocou webového prehliadača. Toto rozhranie môže byť prístupné prostredníctvom HTTPS protokolu, čo zabezpečuje šifrovanú komunikáciu medzi klientom a prepínačom.

Konzolový port:

- Ak máte fyzický prístup k prepínaču, môžete použiť konzolový port na pripojenie sa k nástenke prepínača pomocou sériového kábla. Tento spôsob prístupu sa používa hlavne pri odstraňovaní problémov alebo pri konfigurácii prepínača počas inštalácie.

Ostatné protokoly:

- Okrem uvedených existujú aj ďalšie protokoly a metódy na vzdialený prístup k prepínačom, ako napríklad SNMP (Simple Network Management Protocol) pre monitorovanie a riadenie prepínača, alebo RADIUS/TACACS+ pre autentifikáciu užívateľov.

Pri výbere metódy vzdialeného prístupu k prepínaču je dôležité zvážiť bezpečnostné požiadavky, dostupné možnosti a jednoduchosť implementácie. Vo všeobecnosti je odporúčané používať šifrované protokoly ako SSH a HTTPS pre zabezpečený vzdialený prístup k sieťovým zariadeniam.

### - **popíšte rozpočtový proces a faktory, ktoré ovplyvňujú štátny rozpočet**

Rozpočtový proces je postup, ktorým štát alebo vláda plánuje, vypracúva, schvaľuje a monitoruje svoje výdavky a príjmy na určité obdobie, obvykle na ročnej báze. Tu je stručný prehľad rozpočtového procesu a faktorov, ktoré ovplyvňujú štátny rozpočet:

## **Rozpočtový proces:**

Plánovanie:

- Štát alebo vláda vypracúva plán výdavkov a príjmov na určité obdobie, obvykle na základe prioritných politických cieľov a ekonomických predpokladov.

Vypracovanie návrhu rozpočtu:

- Na základe plánovaných výdavkov a príjmov sa vypracuje návrh rozpočtu, ktorý zahŕňa alokáciu finančných prostriedkov na rôzne sektory a programy.

Schvaľovanie:

- Návrh rozpočtu sa predkladá k schváleniu parlamentu, kde sa koná diskusia a hlasovanie o jeho prijatí alebo zmenách.

Implementácia:

- Po schválení sa rozpočet implementuje prostredníctvom vykonávajúcich orgánov a ministerstiev, ktoré riadia príslušné programy a projekty.

Monitorovanie a revízia:

- Rozpočet je monitorovaný počas finančného roka na zabezpečenie dodržiavania plánovaných výdavkov a príjmov. V prípade potreby môže byť vykonaná revízia rozpočtu a vykonané úpravy.

## Faktory ovplyvňujúce štátny rozpočet:

Hospodárska situácia:

- Hospodárska aktivita, rast HDP, inflácia a nezamestnanosť sú dôležité faktory, ktoré ovplyvňujú príjmy štátu a výdavky na sociálne dávky a verejné služby.

Politické priority:

- Politické priority a priority vlády ovplyvňujú alokáciu finančných prostriedkov na rôzne oblasti, ako sú zdravotníctvo, vzdelávanie, obrana, infraštruktúra a sociálne programy.

Demografické trendy:

- Zmeny v demografii, ako je starnutie populácie a migrácia, môžu ovplyvniť náklady na zdravotníctvo, dôchodky a ďalšie sociálne programy.

Zmeny v legislatíve:

- Zmeny v legislatíve a reguláciách môžu mať vplyv na príjmy a výdavky štátu, ako aj na daňové sadzby a daňové povinnosti.

Vojenské výdavky:

- Výdavky na obranu a bezpečnosť sú dôležitou súčasťou štátneho rozpočtu a sú ovplyvnené geopolitickými udalosťami a bezpečnostnými hrozbami.

Celkovo vzaté, štátny rozpočet je komplexný proces, ktorý zohľadňuje množstvo faktorov a záujmov a je základom pre fungovanie verejných financií a hospodárstva krajiny.

### - vysvetlite vzťah medzi štátnym rozpočtom a daňami

Vzťah medzi štátnym rozpočtom a daňami je úzko prepojený, pretože daňové príjmy sú hlavným zdrojom financovania štátneho rozpočtu. Tu je vysvetlenie tohto vzťahu:

Financovanie verejných výdavkov:

- Štátny rozpočet slúži na plánovanie a riadenie verejných výdavkov, ako sú sociálne programy, zdravotníctvo, vzdelávanie, doprava, obrana a ďalšie verejné služby. Tieto výdavky sú financované z príjmov, ktoré štát získa z daní.

Daňové príjmy:

- Daňové príjmy predstavujú peniaze, ktoré štát získa od občanov a podnikov v rámci daní a poplatkov. Medzi hlavné formy daňových príjmov

patria príjmy z daní z príjmov, dane z pridanej hodnoty (DPH), dane z príjmu právnických osôb, dane z nehnuteľností a ďalšie.

Plánovanie rozpočtu:

- Pri tvorbe štátneho rozpočtu sa berú do úvahy očakávané daňové príjmy a plánujú sa výdavky v súlade s týmito príjmami. Štát musí zabezpečiť, aby výdavky nepresiahli príjmy, aby sa predišlo deficitu a neudržateľnej zadlženosti.

Regulácia hospodárstva:

- V niektorých prípadoch môže štát použiť daňovú politiku ako nástroj na reguláciu hospodárskej činnosti. Zvýšením alebo znížením daní môže štát ovplyvniť spotrebu, investície, výrobu a ďalšie ekonomické faktory.

Sociálna spravodlivosť a solidarita:

- Daňová politika môže slúžiť aj na dosiahnutie sociálnej spravodlivosti a solidarity v spoločnosti. Progresívne dane, ktoré zvýhodňujú nižšie príjmy, a sociálne dávky financované z daní môžu pomôcť vyrovnať ekonomické nerovnosti a poskytnúť podporu tým, ktorí ju najviac potrebujú.

Celkovo vzaté, štátny rozpočet a dane sú neoddeliteľne prepojené, pretože daňové príjmy tvoria základ financovania verejných výdavkov a sú hlavným nástrojom, cez ktorý štát reguluje hospodárstvo a podporuje sociálne ciele.

## **DIAGNOSTICKÉ NÁSTROJE PRE SPRÁVU POČÍTAČOVEJ SIETE**

### **- vysvetlite zásady diagnostiky problémov v počítačových sieťach na RM OSI**

Diagnostika problémov v počítačových sieťach na základe modelu OSI (Open Systems Interconnection) je postup, ktorý umožňuje identifikovať a riešiť problémy v sieťach pomocou rozdelenia komplexných problémov na jednotlivé vrstvy modelu OSI. Tu sú základné zásady diagnostiky problémov v počítačových sieťach na základe modelu OSI:

Rozdelenie problému na jednotlivé vrstvy:

- Prvým krokom pri diagnostike problému je identifikovať, na ktorej vrstve modelu OSI sa problém vyskytuje. Rozdelenie problému na jednotlivé vrstvy umožňuje štruktúrovaný prístup k identifikácii a riešeniu problémov.

Vyhľadávanie príznakov a symptómov:

- Po rozdelení problému na jednotlivé vrstvy je potrebné vyhľadávať príznaky a symptómy, ktoré súvisia s každou konkrétnou vrstvou. Tieto príznaky môžu zahŕňať straty paketov, oneskorenie prenosu dát, nesprávne konfigurácie a podobne.

Testovanie konektivity:

- Testovanie konektivity je dôležitou súčasťou diagnostiky problémov v počítačových sieťach. Tento test sa zvyčajne vykonáva pomocou nástrojov ako ping, ktorý overuje, či sú zariadenia v sieti schopné komunikovať medzi sebou.

Overenie konfigurácií a nastavení:

- Overenie konfigurácií a nastavení na každej vrstve modelu OSI je dôležitým krokom pri diagnostikovaní problémov. Tento proces zahŕňa kontrolu sieťových parametrov, ako sú IP adresy, smerovanie, nastavenia firewallu a podobne.

Použitie sieťových nástrojov:

- Pri diagnostike problémov v počítačových sieťach môžu byť užitočné rôzne sieťové nástroje, ako sú sieťové analyzátory, sniffer-y, monitorovacie nástroje a podobne. Tieto nástroje umožňujú podrobnejšiu analýzu prevádzky v sieti a identifikáciu problémových oblastí.

Postupné testovanie a overovanie:

- Pri diagnostike problémov v počítačových sieťach je dôležité postupne testovať a overovať jednotlivé časti siete, aby sa presne lokalizovala a identifikovala problematická oblasť. Tento postupný prístup umožňuje systematicky riešiť problémy a minimalizovať riziko nežiaducich vedľajších účinkov.

Tieto zásady diagnostiky problémov v počítačových sieťach na základe modelu OSI pomáhajú systematicky identifikovať a riešiť problémy v sieťach a zabezpečiť ich efektívne fungovanie.

#### - **vymenujte základné softvérové nástroje pre diagnostiku počítačovej siete**

Existuje mnoho softvérových nástrojov určených na diagnostiku počítačových sietí, ktoré umožňujú monitorovanie, analýzu a riešenie problémov v sieťach. Tu je niekoľko základných softvérových nástrojov:

**Ping:** Ping je jednoduchý nástroj, ktorý umožňuje testovať konektivitu medzi dvoma zariadeniami v sieti. Posiela ICMP echo požiadavky na cieľové zariadenie a čaká na odpoveď, čo umožňuje overiť, či je zariadenie dostupné a odpovedá na sieťové požiadavky.

**Traceroute (tracert):** Traceroute je nástroj, ktorý umožňuje sledovať cestu, ktorou pakety prechádzajú z jedného zariadenia do druhého cez internetovú sieť. Poskytuje podrobné informácie o každom medzipočítačovom skoku, vrátane IP adres a časových oneskorení.

**Wireshark:** Wireshark je populárny sieťový analyzátor, ktorý umožňuje zachytávať, zobrazovať a analyzovať sieťovú prevádzku v reálnom čase. Poskytuje detailné informácie o paketoch v sieti, vrátane ich obsahu, zdrojových a cieľových adries a ďalších relevantných údajov.

**Netcat (nc):** Netcat je utilita určená na čítanie a zasielanie dát pomocou TCP alebo UDP na konkrétnom portu. Je často používaná na testovanie pripojenia na určité porty na zariadeniach v sieti.

**Nmap:** Nmap je nástroj na skenovanie sietí, ktorý umožňuje objavovať a mapovať zariadenia v sieti, analyzovať ich porty a služby a zisťovať ich bezpečnostné riziká. Poskytuje rozsiahle možnosti skenovania a detekcie zraniteľností.



**Sysinternals Suite:** Sysinternals Suite je sada nástrojov pre operačné systémy Windows, ktoré zahŕňajú rôzne utility na diagnostiku a správu sietí, ako je Process Monitor, TCPView, Autoruns a ďalšie.

**Zenmap:** Zenmap je grafické užívateľské rozhranie pre Nmap, ktoré umožňuje pohodlnejšie používanie Nmap na skenovanie sietí a analýzu ich bezpečnostných rizík.

Tieto softvérové nástroje poskytujú rôzne možnosti na diagnostiku, monitorovanie a analýzu počítačových sietí, čo umožňuje efektívne riešenie problémov a zabezpečenie optimálneho fungovania siete.

#### - **načrtnite spôsoby ako nastaviť na routri požadované parametre**

Nastavenie požadovaných parametrov na routri závisí od konkrétnych potrieb a požiadaviek siete, ako aj od typu a značky routera. Tu je všeobecný náčrt spôsobov, ako nastaviť niektoré základné parametre na routri:

Pripojenie k routeru:

- Použite webový prehliadač na pripojenie k rozhraniu routeru. Väčšina routerov má prednastavenú IP adresu (často 192.168.1.1 alebo 192.168.0.1), na ktorú sa dá pripojiť.

Prihlasovacie údaje:

- Prihláste sa do rozhrania routeru pomocou prednastavených prihlasovacích údajov (ktoré sa často nachádzajú na zadnej strane alebo na spodnej strane routeru) alebo pomocou vlastných prihlasovacích údajov, ak ste ich už zmenili.

Zabezpečenie siete:

- Zabezpečte sieť zmenou prednastavených hesiel a prihlasovacích údajov na unikátne a silné kombinácie. Aktivujte šifrovanie siete, ako je WPA2, a nastavte silné heslá pre prístup.

Nastavenie smerovania:

- Nastavte statické smerovanie, ak je potrebné, alebo povoľte protokoly dynamického smerovania, ako je RIP, OSPF alebo BGP, ak sa používajú v sieti.

Nastavenie firewallu:

- Konfigurujte firewall routeru na blokovanie nežiaducich sieťových spojení a služieb. Definujte pravidlá pre presmerovanie portov, ak je to potrebné.

NAT a port forwarding:

- Nastavte sieťový preklad adres (NAT) na umožnenie súkromným adresám pripojenie k internetu a nastavte port forwarding na presmerovanie špecifických portov na určité zariadenia v sieti.

DHCP:

- Ak je potrebné, aktivujte DHCP server na routeri na automatické pridelenie IP adres a ďalších sieťových parametrov zariadeniam v sieti.

Aktualizácie a zálohovanie konfigurácií:

- Pravidelne aktualizujte firmvérové a softvérové verzie routeru a pravidelne zálohujte konfigurácie routeru, aby ste mohli obnoviť nastavenia v prípade potreby.

Monitorovanie a logovanie:

- Aktivujte funkcie monitorovania a logovania routeru na sledovanie prevádzky, monitorovanie udalostí a identifikáciu problémov v sieti.

Tieto kroky slúžia ako všeobecný náčrt nastavenia požadovaných parametrov na routeri. Presné nastavenie bude závisieť od špecifik siete a požiadaviek na bezpečnosť a funkčnosť. Je dôležité dodržiavať bezpečnostné postupy a odporúčania pri nastavovaní routeru a siete.

## - **popíšte postup pre overenie dosiahnuteľnosti ľubovoľného hosta v počítačovej sieti**

Overenie dosiahnuteľnosti ľubovoľného hosta v počítačovej sieti môže byť vykonané pomocou niekoľkých rôznych metód. Tu je postup, ako môžete overiť dosiahnuteľnosť hosta v sieti:

Získanie IP adresy hosta:

- Pred začatím overenia dosiahnuteľnosti musíte získať IP adresu cieľového hosta. Túto informáciu môžete získať z konfigurácie siete, administrátora siete, zariadenia alebo pomocou nástrojov na skenovanie siete ako napríklad nmap.

Pingovanie hosta:

- Použite príkaz ping na overenie dosiahnuteľnosti hosta. Ping je jednoduchý nástroj, ktorý zasiela ICMP echo požiadavky na cieľovú IP adresu a čaká na odpoveď. Pre pingovanie hosta stačí otvoriť príkazový riadok a zadajte príkaz `ping <IP_adresa_hosta>`. Ak je host dosiahnuteľný, mali by ste vidieť odpovede na ping požiadavky.

Skúmanie výsledkov pingu:

- Ak pingovanie zlyhá, môže to naznačovať problémy s dostupnosťou hosta. Skontrolujte, či ste správne zadali IP adresu hosta a či je host zapnutý a pripojený k sieti. Ak je host sprostredkovaný cez firewall alebo NAT, môže byť potrebné prídanie pravidla pre povolenie ICMP echo odpovedí.

Využitie traceroute (tracert):

- Ak pingovanie neprinieslo úspech a chcete zistiť, kde presne sa nachádza problém v sieti, môžete použiť traceroute (tracert). Tento nástroj vám umožňuje sledovať cestu, ktorou prechádzajú pakety k cieľovému hostovi. Pre spustenie traceroute stačí otvoriť príkazový riadok a zadajte príkaz `tracert <IP_adresa_hosta>`.

Analyzovanie výsledkov traceroute:

- Výsledky traceroute vám ukážu všetky medzipočítačové skoky (routery), ktoré pakety prechádzajú na ceste k cieľovému hostovi. Ak vidíte, že pakety neprichádzajú k cieľovému hostovi, môžete zistiť, kde sa nachádza problém a skontrolovať konfiguráciu každého routeru na ceste.

Tento postup vám umožní overiť dosiahnuteľnosť ľubovoľného hosta v počítačovej sieti a identifikovať prípadné problémy, ktoré môžu brániť v komunikácii s daným hostom.

## - **vysvetlite dôvody a spôsoby kryptovania hesiel na sieťových zariadeniach**

Kryptovanie hesiel na sieťových zariadeniach je dôležitým opatrením na zvýšenie bezpečnosti siete. Tu sú hlavné dôvody a spôsoby kryptovania hesiel:

Ochrana pred odhalením hesiel:

- Heslá uložené v konfigurácii sieťových zariadení môžu byť cenným cieľom pre útočníkov. Kryptovanie hesiel zabezpečuje, že aj keby sa útočníkovi podarilo získať prístup k konfiguračným súborom, nebudú môcť jednoducho získať heslá voči sieťovým zariadeniam.

Ochrana pred neoprávneným prístupom:

- Kryptovanie hesiel zabraňuje neoprávneným osobám v prístupe k dôležitým sieťovým zariadeniam. Dokonca aj v prípade, že útočník získa prístup k konfiguračným súborom, nebude schopný dekódovať kryptované heslá a získať prístup k sieťovým zariadeniam.

Zabezpečenie citlivých informácií:

- Heslá často poskytujú prístup k citlivým informáciám a zdrojom v sieti. Kryptovanie hesiel zabezpečuje, že tieto informácie sú chránené a nedostupné pre neoprávnených užívateľov, aj keď majú prístup k konfiguračným súborom.

Dôvernosť hesiel:

- Kryptovanie hesiel zvyšuje dôvernosť informácií uložených v konfiguračných súboroch sieťových zariadení. Použitím silných kryptografických algoritmov sa zabezpečuje, že heslá zostanú dôverné a chránené.

Spôsoby kryptovania hesiel na sieťových zariadeniach zahŕňajú:

- Hashovanie hesiel: Heslá môžu byť uložené v hashovanej podobe, kde sa heslo pretransformuje do hashovanej hodnoty pomocou kryptografického hashovacieho algoritmu. Táto hashovaná hodnota je uložená v konfiguračnom súbore a pri overovaní hesla sa porovnáva s hashovanou hodnotou uloženou v konfigurácii.
- Šifrovanie hesiel: Heslá môžu byť šifrované pomocou kryptografických algoritmov na ochranu citlivých informácií. Pri tomto prístupe je heslo zašifrované pomocou kľúča, a pre jeho dešifrovanie je potrebný rovnaký kľúč.
- Použitie silných hesiel: Aj keď kryptovanie hesiel môže zvýšiť bezpečnosť, je dôležité tiež používať silné a bezpečné heslá. Silné heslá zvyšujú odolnosť voči rôznym útokom na heslá.

Kryptovanie hesiel na sieťových zariadeniach je kľúčovým prvkom zabezpečenia siete a ochrany citlivých informácií pred neoprávneným prístupom.

- **uved'te postup pre zobrazenie nastavených parametrov na sieťovom zariadení**

Postup pre zobrazenie nastavených parametrov na sieťovom zariadení závisí od typu a modelu zariadenia, ako aj od používaného operačného systému. Tu je všeobecný postup, ktorý môžete použiť na zobrazenie nastavených parametrov:

Pripojenie k sieťovému zariadeniu:

- Pripojte sa k sieťovému zariadeniu pomocou vhodného prostriedku prístupu, ako je konzolový port, telnet, SSH alebo webové rozhranie (ak je k dispozícii).

Prihlásenie do zariadenia:

- Použite príslušné prihlasovacie údaje (užívateľské meno a heslo), aby ste sa prihlásili do konfiguračného rozhrania zariadenia.

Prezeranie nastavených parametrov:

- Po úspešnom prihlásení sa zobrazí príkazový riadok alebo grafické rozhranie, v ktorom môžete prezeranie nastavených parametrov zariadenia.
- V príkazovom riadku môžete použiť rôzne príkazy na zobrazenie nastavení, ako sú napríklad:
  - `show running-config` alebo `show config`: Zobrazí aktuálnu konfiguráciu zariadenia, vrátane nastavených rozhraní, routovacích tabuliek, firewall pravidiel a ďalších parametrov.
  - `show ip interface brief` alebo `show interfaces`: Zobrazí základné informácie o všetkých rozhraniach zariadenia, ako sú IP adresy, stav rozhraní a podobne.
  - `show ip route` alebo `show route`: Zobrazí aktuálnu routovaciu tabuľku zariadenia, ktorá obsahuje informácie o dostupných sieťach a cestách k nim.
  - Ďalšie príkazy závisiace od konkrétneho typu a modelu zariadenia a operačného systému.
- V grafickom rozhraní môžete prechádzať rôznymi záložkami alebo sekciami, ktoré zobrazujú konfiguračné parametre a informácie o zariadení.

Analýza a interpretácia výstupu:

- Po zobrazení nastavených parametrov zariadenia analyzujte výstup a overte, či je konfigurácia nastavená podľa požiadaviek a bezpečnostných štandardov siete.

Tento postup vám umožní zobraziť a skontrolovať nastavené parametre na sieťovom zariadení a poskytne vám prehľad o konfigurácii a stave zariadenia.

#### - vysvetlite význam protokolu ARP

Protokol ARP (Address Resolution Protocol) má kľúčový význam v počítačových sieťach, pretože umožňuje mapovanie medzi IP adresami a fyzickými MAC adresami na lokálnej sieti.

Tu je podrobnejší význam protokolu ARP:

Mapovanie IP adres na MAC adresy:

- Protokol ARP umožňuje získanie fyzickej MAC adresy zariadenia (ako napríklad počítača alebo routeru) na základe jeho IP adresy v lokálnej sieti. Toto

mapovanie je nevyhnutné pre správne doručenie paketov na správne zariadenie v sieti.

Proces ARP dotazovania:

- Keď počítač potrebuje zistiť fyzickú MAC adresu zariadenia s určitou IP adresou, pošle ARP dotazovanie na lokálnu sieť. Tento dotaz obsahuje IP adresu cieľového zariadenia a MAC adresu vysielateľa. Ostatné zariadenia v sieti, ktoré majú zadanú IP adresu, odpovedia so svojou fyzickou MAC adresou.

Tabuľka ARP:

- Počítač udržiava tabuľku ARP, ktorá obsahuje mapovanie IP adries na fyzické MAC adresy pre nedávno komunikované zariadenia v sieti. Táto tabuľka sa využíva na ušetrenie času a zdrojov pri opakovaných komunikáciách s rovnakými zariadeniami.

Dynamickej aktualizácie tabuľky ARP:

- Tabuľka ARP je dynamicky aktualizovaná na základe komunikácie v sieti. Pri každej komunikácii sa IP adresa a fyzická MAC adresa zariadenia zapíšu do tabuľky ARP. Toto umožňuje, že sa tabuľka automaticky aktualizuje v prípade, že sa MAC adresa zariadenia zmení alebo zariadenie opustí sieť.

Využitie pri komunikácii v rámci lokálnej siete:

- Protokol ARP je dôležitý pri komunikácii v rámci lokálnej siete, kde je doručenie paketov založené na fyzických MAC adresách. Bez správnej mapovacej informácie by bolo nemožné správne doručiť pakety na cieľové zariadenie.

Celkovo je protokol ARP kľúčovým prvkom v správnej funkcii lokálnych počítačových sietí, pretože umožňuje správne doručiť pakety na cieľové zariadenie v sieti na základe jeho IP adresy.

#### - **popíšte diagnostiku a odstraňovanie porúch v navrhutej počítačovej sieti**

Diagnostika a odstraňovanie porúch v počítačovej sieti je kľúčovým procesom pre zabezpečenie správneho fungovania a výkonnosti siete. Tu je postup, ako by mohla vyzeráť diagnostika a odstraňovanie porúch v navrhutej počítačovej sieti:

Zozbieranie informácií:

- Začnite získavaním informácií o probléme. Rozhovorte sa s používateľmi siete, aby ste zistili, aké problémy alebo symptómy zažívajú. Skontrolujte, či je problém lokalizovaný len na jedno určité zariadenie alebo sa týka celej siete.

Fyzická kontrola zariadení:

- Skontrolujte fyzický stav všetkých sieťových zariadení, ako sú switche, routery, access pointy, káble a konektory. Overte, či sú všetky zariadenia správne pripojené a či nie sú poškodené.

Overenie konfigurácie:

- Skontrolujte konfiguráciu sieťových zariadení, ako sú IP adresy, smerovanie, VLAN nastavenia, firewall pravidlá a podobne. Overte, či konfigurácia zodpovedá navrhnutému návrhu siete a či neexistujú konflikty alebo chyby v nastaveniach.

Testovanie konektivity:

- Použite nástroje na testovanie konektivity, ako je ping, na overenie dostupnosti zariadení v sieti. Pingujte rôzne zariadenia v sieti a zistite, či sú dostupné a či je dostupnosť konzistentná.

Použitie sieťových nástrojov:

- Využite sieťové nástroje, ako sú Wireshark, traceroute, SNMP monitorovanie a podobne, na podrobnejšiu analýzu sieťového provozu a identifikáciu problémových oblastí.

Overenie fyzických médií:

- Ak máte podozrenie, že problém môže byť spojený s fyzickými médiami (napríklad poruchy káblov), použite tester káblov alebo iné nástroje na overenie integrity káblov a fyzických pripojení.

Riešenie problémov postupne:

- Riešte problémy postupne a systémovo. Začnite s jednoduchými a zrejmými problémami a postupne sa pohybujte k zložitejším problémom. Overujte každú časť siete a zisťujte, kde sa vyskytujú problémy.

Dokumentácia a záznamy:

- Zaznamenajte všetky kroky, ktoré vykonávate pri diagnostike a odstraňovaní porúch. Tieto záznamy vám môžu pomôcť pri budúcich problémoch a umožnia vám analyzovať a zlepšovať výkonnosť siete.

Monitorovanie a prevencia:

- Po odstránení poruchy nezabudnite monitorovať sieť a vykonávať preventívne opatrenia, aby sa zabránilo opakovaniu problémov v budúcnosti.

Tento postup vám umožní systematicky diagnostikovať a odstraňovať poruchy v navrhutej počítačovej sieti a zabezpečiť jej správne fungovanie a výkonnosť.

## - **popíšte možnosti diaľkového prístupu k sieťovým zariadeniam pri správe**

Pri správe sieťových zariadení existuje niekoľko možností diaľkového prístupu, ktoré umožňujú administrátorom získavať prístup k týmto zariadeniam z ľubovoľného miesta. Tu sú niektoré z najpoužívanejších možností diaľkového prístupu:

SSH (Secure Shell):

- SSH je kryptografický sieťový protokol, ktorý umožňuje bezpečný a šifrovaný prístup k sieťovým zariadeniam cez nezabezpečené siete. SSH sa používa na vzdialené pripojenie k konzolovému rozhraniu zariadenia, čím poskytuje administrátorovi možnosť konfigurovať a spravovať zariadenia aj z diaľky.

Telnet:

- Telnet je starší sieťový protokol, ktorý umožňuje vzdialený prístup k konzolovému rozhraniu sieťových zariadení. Avšak Telnet neposkytuje šifrovanie, čo znamená, že použitie Telnetu môže predstavovať bezpečnostné riziko, pretože prihlasovacie údaje sa prenášajú nezašifrované.

Web-based management:

- Mnoho moderných sieťových zariadení poskytuje webové rozhranie na správu a konfiguráciu zariadenia. Tieto webové rozhrania umožňujú administrátorom prístup k rôznym funkcionalitám zariadenia pomocou bežného webového prehliadača, čo zjednodušuje diaľkovú správu.

Konzolové servery:

- Konzolové servery sú zariadenia navrhnuté na centralizované pripájanie k sériovým konzolovým portom (napríklad RS-232) rôznych sieťových zariadení. Tieto zariadenia umožňujú administrátorom prístup k konzolovým rozhraniám rôznych zariadení z jedného miesta pomocou sieťovej siete.

VPN (Virtual Private Network):

- VPN umožňuje vytvoriť bezpečné a šifrované pripojenie medzi vzdialeným administrátorom a sieťovým zariadením prostredníctvom verejnej siete, ako je internet. VPN umožňuje administrátorom pripojiť sa k sieti, akoby boli priamo pripojení do vnútornej siete organizácie.

Out-of-band management:

- Out-of-band management umožňuje administrátorom prístup k sieťovým zariadeniam prostredníctvom alternatívnych komunikačných kanálov, ako sú sériové konzolové porty alebo iné alternatívne siete. Tento prístup umožňuje správu zariadení aj v prípade, že hlavná sieť je nedostupná.

Tieto možnosti diaľkového prístupu k sieťovým zariadeniam umožňujú administrátorom efektívne spravovať a konfigurovať sieťové zariadenia aj z diaľky, čo je kľúčové pre riadne fungovanie a údržbu siete. Pri výbere metódy je dôležité zvážiť bezpečnostné požiadavky a potreby organizácie.

## **- porovnajtenastavenia na sieťovom zariadení ak ho manažujete z rôznych druhov počítačových sietí**

Nastavenia sieťového zariadenia môžu byť ovplyvnené rôznymi faktormi v závislosti od toho, akým spôsobom a z akých počítačových sietí je zariadenie manažované. Tu je porovnanie nastavení na sieťovom zariadení, ak ho manažujete z rôznych druhov počítačových sietí:

Lokálna sieť:

- Ak manažujete sieťové zariadenie z lokálnej siete, môžete mať priamy prístup k zariadeniu prostredníctvom interných sieťových zdrojov. Môžete mať rýchly a jednoduchý prístup k zariadeniu bez potreby použitia špeciálnych bezpečnostných opatrení, ak je sieť dobre zabezpečená.

Vzdialená sieť s VPN:

- V prípade manažovania sieťového zariadenia z vzdialenej siete prostredníctvom VPN (Virtual Private Network) budete musieť najprv vytvoriť bezpečné pripojenie do siete. Potom budete mať prístup k zariadeniu tak, ako by ste boli pripojení z lokálnej siete. Tento spôsob zabezpečuje šifrovanie komunikácie a ochranu pred neoprávneným prístupom.

Internet:

- Manažovanie sieťového zariadenia cez internet vyžaduje príslušné bezpečnostné opatrenia, pretože je vystavené rôznym bezpečnostným hrozbám. Zvyčajne sa používajú metódy ako SSH alebo webové rozhrania s HTTPS, ktoré zabezpečujú šifrovanú komunikáciu. Môžu sa tiež používať firewally alebo VPN pre zvýšenie bezpečnosti.

Mobilné siete:

- Ak je sieťové zariadenie manažované cez mobilné siete, napríklad pomocou mobilného dátového pripojenia alebo Wi-Fi siete, môžu byť rýchlosť a spoľahlivosť pripojenia obmedzené v porovnaní s pevnými sieťami. Používa sa preto obvykle spoľahlivý protokol pre diaľkový prístup, ako je SSH, aby sa minimalizovalo množstvo dátového prenosu a zabezpečilo spoľahlivé pripojenie.

Každý typ počítačovej siete prináša svoje vlastné výzvy a požiadavky na manažovanie sieťových zariadení. Je dôležité zvážiť bezpečnostné požiadavky, dostupnosť a špecifické potreby organizácie pri manažovaní sieťových zariadení z rôznych druhov počítačových sietí.