**Architektúra počítačových sieti**: Počítačové siete umožňujú komunikáciu medzi počítačmi a inými zariadeniami. Medzi hlavné komponenty patrí hardvér (servery, klientské počítače, sieťové zariadenia), softvér (operačné systémy, sieťové aplikácie) a komunikačné protokoly (TCP/IP, HTTP, FTP).

**Referenčný model ISO/OSI**: Model ISO/OSI je sedemvrstvový model, ktorý štandardizuje rôzne sieťové funkcie:

1. Fyzická vrstva = Prenos bitov medzi zariadeniami zahŕňa fyzické médiá, ako sú káble (UTP,STP, koaxiálne) a optické káble.
2. Linková vrstva = Prenos rámcov medzi susednými uzlami, zahŕňa protokoly ako Ethernet a adresy MAC.
3. Sieťová vrstva = Smerovanie paketov medzi sieťami, zahŕňa protokol IP, ICMP a ARP.
4. Transportná vrstva = Spoľahlivý prenos údajov medzi koncovými bodmi, zahŕňa protokol TPC (Transmission Control Protocol) a UDP (User Datagram Protocol).
5. Relačná vrstva = Udržiavanie spojení a synchronizácia údajov, napríklad vzdialené volanie procedúr (RPC).
6. Prezentačná vrstva = Konverzia údajov do formátu zrozumiteľného pre aplikácie, vrátane SSL/TLS na šifrovanie.
7. Aplikačná vrstva = Sieťové aplikácie a ich protokoly, napr. HTTP, FTP, SMTP.

**Sieťový model TCP/IP**: Model TCP/IP má 4 vrstvy:

1. Sieťový prístup = Spája funkcie fyzickej a linkovej vrstvy ISO/OSI, zahŕňa technológie ako Ethernet, PPP.
2. Internetová vrstva = Mapuje sieťovú vrstvu ISO/OSI, zahŕňa internetový protokol (IP), protokol ICMP (Internet Control Message Protocol), protokol ARP (Address Resolution Protocol).
3. Transportná vrstva = Zabezpečuje spoľahlivý prenos údajov medzi aplikáciami, zahŕňa TCP a UDP.
4. Aplikačná vrstva = Zahŕňa aplikačnú, prezentačnú a reláčnú vrstvu ISO/OSI, zahŕňa protokoly ako HTTP, FTP, DNS.

**Fyzická vrstva**:

* metalické spoje = káble UTP (Unshielded Twisted Pair) pre väčšinu ethernetových sietí, káble STP (Shielded Twisted Pair) pre prostredia s vyšším elektromagnetickým rušením, koaxiálne káble pre staršie siete a káblovú televíziu.
* optické spoje = optické vlákna (jednovidové na dlhé vzdialenosti, viacmodové na kratšie vzdialenosti).
* hub = jednoduché sieťové zariadenie, ktoré opakuje signál do všetkých portov bez ohľadu na cieľovú adresu.

**Adresovanie na linkovej vrstve**:

* switch = smeruje údaje na základe adresy MAC, umožňuje oddelenie kolíznych domén a zlepšuje výkon siete.
* MAC adresy = jedinečné 48-bitové identifikátory sieťových zariadení, ktoré sa používajú na smerovanie údajov na linkovej vrstve.

**Ethernet**: Ethernetový rámec obsahuje cieľovú a zdrojovú adresu MAC, typ protokolu, údaje a kontrolný súčet (FCS). Technológie ako 10Base-T (10 Mbps), 100Base-TX (100 Mbps), 1000Base-T (1 Gbps).

**Protokol IP – siete a podsiete**:

* IPv4 = 32-bitové adresy rozdelené do tried A, B, C, D (multicast), E (rezervované). Na rozdelenie na siete a podsiete používa sieťové masky.
* IPv6 = 128-bitové adresy, rieši nedostatok adries IPv4, ponúka väčší adresný priestor a zabudované bezpečnostné funkcie.
* Multicast a Unicast = multicast posiela údaje viacerým príjemcom (skupinám), unicast posiela údaje jednému príjemcovi.
* Protokol ICMP = používa sa na diagnostiku a hlásenie chýb (ping, traceroute).
* Protokol ARP = prevádza adresy IP na adresy MAC, umožňuje zariadeniam v sieti nájsť fyzickú adresu pre danú adresu IP.

Sieťová maska: Maska siete určuje, ktorá časť IP adresy identifikuje sieť a ktorá časť identifikuje zariadenia v sieti. Napríklad maska 255.255.255.0 znamená, že prvé tri oktety sú sieťovou časťou a posledný oktet identifikuje zariadenie v sieti.

Brána: Sieťové zariadenie, ktoré spája miestnu sieť s inými sieťami, zvyčajne s internetom. Brána smeruje sieťovú prevádzku medzi miestnou sieťou a vzdialenými sieťami.

Router: sieťové zariadenie, ktoré smeruje dátové pakety medzi rôznymi sieťami na základe ich IP adries. Smerovače určujú najlepšiu cestu pre prenos dát a na rozhodovanie o smerovaní používajú smerovacie tabuľky.

**Smerovanie v sieťach**:

Statické smerovanie = manuálna konfigurácia ciest v smerovačoch, vhodná pre malé a stabilné siete.

Dynamické smerovanie = automatické učenie a aktualizácia ciest, používa smerovacie protokoly, ako sú RIP (Routing Information Protocol) a OSPF (Open Shortest Path First).

* RIP: používa počet skokov ako metriku, obmedzený na 15 skokov.
* OSPF: používa stav spojenia a je vhodný pre väčšie a zložité siete, poskytuje rýchlu konvergenciu.

**Prideľovanie adries – DHCP**: automatické prideľovanie IP adries, sieťovej masky, brány a DNS serverov. Zjednodušuje správu IP adries v sieti.

**Protokoly – UDP a TCP**:

UDP (User Datagram Protocol) = nespojitý, nespoľahlivý prenos dát, vhodný pre aplikácie, kde je dôležitá rýchlosť (streamovanie videa, online hry).

TCP (Transmission Control Protocol) = pripojený, spoľahlivý prenos dát, poskytuje kontrolu chýb, poradie a opakovanie stratených paketov. Vhodný pre aplikácie, kde je dôležitá spoľahlivosť (webové stránky, e-mail).

**NAT**: Preklad súkromných IP adries na verejné IP adresy na komunikáciu s internetom. Umožňuje zdieľanie jednej verejnej IP adresy medzi viacerými zariadeniami v miestnej sieti.

**Transportná vrstva a porty**:

* Porty: identifikujú konkrétne procesy na serveri (HTTP - port 80, HTTPS - port 443, FTP - port 21). Porty sú čísla od 0 do 65535, rozdelené na dobre známe porty (0-1023), registrované porty (1024-49151) a dynamické/súkromné porty (49152-65535).
* Prúdový prenos (TCP): Spojený, spoľahlivý, používa mechanizmy riadenia toku a detekcie chýb.
* Datagramový prenos (UDP): Nespojitý, nespoľahlivý, neposkytuje riadenie toku ani detekciu chýb.

**DNS a DNSSEC**:

DNS (Domain Name System): prevod doménových mien na IP adresy, hierarchický systém zahŕňajúci koreňové servery, servery TLD (Top Level Domain) a autoritatívne servery.

DNSSEC (DNS Security Extensions): zabezpečenie DNS, pridáva digitálne podpisy na overenie pravosti a integrity odpovedí.

**VPN (Virtual Private Network)**: Zabezpečené pripojenie cez internet, ktoré umožňuje bezpečnú komunikáciu medzi vzdialenými sieťami alebo zariadeniami. Typy VPN sú Site-to-Site (prepojenie dvoch sietí), Client-to-Site (prepojenie jednotlivého zariadenia so sieťou). Protokoly sú PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec (Internet Protocol Security).

**Bezdrôtová technológia**:

* WiFi router: prístupový bod pre bezdrôtovú sieť, používa štandardy ako 802.11a/b/g/n/ac/ax.
* Architektúra bezdrôtovej siete: infraštruktúra (prístupové body pripájajú zariadenia ku káblovej sieti) vs. ad-hoc (priame pripojenie medzi zariadeniami bez centrálneho prístupového bodu).
* Bluetooth: Krátka vzdialenosť, osobné zariadenia, používané na pripojenie periférnych zariadení, ako sú klávesnice, myši, slúchadlá.

**Aplikačné protokoly v sieťach**:

* FTP (File Transfer Protocol): prenos súborov medzi klientom a serverom, používa port 21 pre príkazy a port 20 pre dáta.
* HTTP (Hypertext Transfer Protocol): protokol na prenos webových stránok, používa port 80.
* HTTPS (HTTP Secure): šifrovaná verzia protokolu HTTP, používa protokol SSL/TLS na zabezpečenie prenosu údajov, používa port 443.

**Zabezpečenie sietí**:

* Firewall: Sieťové zariadenie alebo softvér, ktorý kontroluje a filtruje sieťovú prevádzku podľa definovaných pravidiel a chráni siete pred neoprávneným prístupom.
* Proxy: Sprostredkovateľ medzi klientom a serverom, zvyšuje bezpečnosť a anonymitu, môže tiež ukladať a filtrovať obsah.
* Útoky typu DoS (Denial of Service): Útoky, ktorých cieľom je preťažiť sieťové zdroje a spôsobiť nedostupnosť služieb.
* Zabezpečenie DNS: implementácia DNSSEC na ochranu pred falšovaním DNS a inými útokmi.

**Možnosti anonymizácie na internete**:

* Anonymizačné služby: Tor (The Onion Router) poskytuje anonymitu smerovaním komunikácie cez niekoľko šifrovaných uzlov.
* VPN: Bezpečné a šifrované pripojenie skrýva IP adresu používateľa.
* Proxy servery: Skrývajú IP adresu používateľa a poskytujú prístup k webovým stránkam.