**Architektura počítačových sítí:** Počítačové sítě umožňují komunikaci mezi počítači a jinými zařízeními. Mezi hlavní komponenty patří hardware (servery, klientské počítače, síťová zařízení), software (operační systémy, síťové aplikace) a komunikační protokoly (TCP/IP, HTTP, FTP).

**Referenční model ISO/OSI**: Model ISO/OSI je sedmivrstvý model, který standardizuje různé síťové funkce:

1. Fyzická vrstva = Přenos bitů mezi zařízeními, zahrnuje fyzická média jako jsou kabely (UTP, STP, koaxiální) a optické kabely.
2. Linková vrstva = Přenos rámců mezi sousedními uzly, zahrnuje protokoly jako Ethernet a adresy MAC.
3. Síťová vrstva = Směrování paketů mezi sítěmi, zahrnuje protokoly IP, ICMP a ARP.
4. Transportní vrstva = Spolehlivý přenos dat mezi koncovými body, zahrnuje protokoly TCP (Transmission Control Protocol) a UDP (User Datagram Protocol).
5. Relační vrstva = Udržování spojení a synchronizace dat, například vzdálené volání procedur (RPC).
6. Prezentační vrstva = Konverze dat do formátu srozumitelného pro aplikace, včetně SSL/TLS pro šifrování.
7. Aplikační vrstva = Síťové aplikace a jejich protokoly, např. HTTP, FTP, SMTP.

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

1. Síťový přístup = Spojuje funkce fyzické a linkové vrstvy ISO/OSI, zahrnuje technologie jako Ethernet a PPP.
2. Internetová vrstva = Mapuje síťovou vrstvu ISO/OSI, zahrnuje internetový protokol (IP), protokol ICMP (Internet Control Message Protocol), protokol ARP (Address Resolution Protocol).
3. Transportní vrstva = Zajišťuje spolehlivý přenos dat mezi aplikacemi, zahrnuje TCP a UDP.
4. Aplikační vrstva = Zahrnuje aplikační, prezentační a relační vrstvu ISO/OSI, zahrnuje protokoly jako HTTP, FTP, DNS.

**Fyzická vrstva:**

* + Metalické spoje = kabely UTP (Unshielded Twisted Pair) pro většinu ethernetových sítí, kabely STP (Shielded Twisted Pair) pro prostředí s vyšším elektromagnetickým rušením, koaxiální kabely pro starší sítě a kabelovou televizi.
  + Optické spoje = optická vlákna (jednovidová na dlouhé vzdálenosti, vícevidová na kratší vzdálenosti).
  + Hub = jednoduché síťové zařízení, které opakuje signál do všech portů bez ohledu na cílovou adresu.

**Adresování na linkové vrstvě:**

* + Switch = směruje data na základě adresy MAC, umožňuje oddělení kolizních domén a zlepšuje výkon sítě.
  + MAC adresy = jedinečné 48-bitové identifikátory síťových zařízení, které se používají na směrování dat na linkové vrstvě.

**Ethernet**: Ethernetový rámec obsahuje cílovou a zdrojovou adresu MAC, typ protokolu, data a kontrolní součet (FCS). Technologie jako 10Base-T (10 Mbps), 100Base-TX (100 Mbps), 1000Base-T (1 Gbps).

**Protokol IP – sítě a podsítě:**

* + IPv4 = 32-bitové adresy rozdělené do tříd A, B, C, D (multicast) a E (rezervované). Na rozdělení na sítě a podsítě používá síťové masky.
  + IPv6 = 128-bitové adresy, řeší nedostatek adres IPv4, nabízí větší adresní prostor a zabudované bezpečnostní funkce.
  + Multicast a Unicast = multicast posílá data více příjemcům (skupinám), unicast posílá data jednomu příjemci.
  + Protokol ICMP = používá se na diagnostiku a hlášení chyb (ping, traceroute).
  + Protokol ARP = převádí adresy IP na adresy MAC, umožňuje zařízením v síti najít fyzickou adresu pro danou adresu IP.

**Síťová maska**: Maska sítě určuje, která část IP adresy identifikuje síť a která část identifikuje zařízení v síti. Například maska 255.255.255.0 znamená, že první tři oktety jsou síťovou částí a poslední oktet identifikuje zařízení v síti.

**Brána**: Síťové zařízení, které spojuje místní síť s jinými sítěmi, obvykle s internetem. Brána směruje síťový provoz mezi místní sítí a vzdálenými sítěmi.

**Router**: Síťové zařízení, které směruje datové pakety mezi různými sítěmi na základě jejich IP adres. Směrovače určují nejlepší cestu pro přenos dat a na rozhodování o směrování používají směrovací tabulky.

**Směrování v sítích:**

* + Statické směrování = manuální konfigurace cest v směrovačích, vhodná pro malé a stabilní sítě.
  + Dynamické směrování = automatické učení a aktualizace cest, používá směrovací protokoly jako jsou RIP (Routing Information Protocol) a OSPF (Open Shortest Path First).
  + RIP: používá počet skoků jako metriku, omezený na 15 skoků.
  + OSPF: používá stav spojení a je vhodný pro větší a složité sítě, poskytuje rychlou konvergenci.

**Přidělování adres – DHCP**: automatické přidělování IP adres, síťové masky, brány a DNS serverů. Zjednodušuje správu IP adres v síti.

**Protokoly – UDP a TCP:**

* + UDP (User Datagram Protocol) = nespojitý, nespolehlivý přenos dat, vhodný pro aplikace, kde je důležitá rychlost (streamování videa, online hry).
  + TCP (Transmission Control Protocol) = připojený, spolehlivý přenos dat, poskytuje kontrolu chyb, pořadí a opakování ztracených paketů. Vhodný pro aplikace, kde je důležitá spolehlivost (webové stránky, e-mail).

**NAT**: Překlad soukromých IP adres na veřejné IP adresy pro komunikaci s internetem. Umožňuje sdílení jedné veřejné IP adresy mezi více zařízeními v místní síti.

**Transportní vrstva a porty**:

* + Porty: identifikují konkrétní procesy na serveru (HTTP - port 80, HTTPS - port 443, FTP - port 21). Porty jsou čísla od 0 do 65535, rozdělené na dobře známé porty (0-1023), registrované porty (1024-49151) a dynamické/soukromé porty (49152-65535).
  + Prúdový prenos (TCP): Spojený, spolehlivý, používá mechanizmy řízení toku a detekce chyb.
  + Datagramový prenos (UDP): Nespojitý, nespolehlivý, neposkytuje řízení toku ani detekci chyb.

**DNS a DNSSEC**:

* + DNS (Domain Name System): převod doménových jmen na IP adresy, hierarchický systém zahrnující kořenové servery, servery TLD (Top Level Domain) a autoritativní servery.
  + DNSSEC (DNS Security Extensions): zabezpečení DNS, přidává digitální podpisy na ověření pravosti a integrity odpovědí.

**VPN (Virtual Private Network):** Zabezpečené připojení přes internet, které umožňuje bezpečnou komunikaci mezi vzdálenými sítěmi nebo zařízeními. Typy VPN jsou Site-to-Site (propojení dvou sítí) a Client-to-Site (propojení jednotlivého zařízení se sítí). Protokoly jsou PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec (Internet Protocol Security).

**Bezdrátová technologie**:

* + WiFi router: přístupový bod pro bezdrátovou síť, používá standardy jako 802.11a/b/g/n/ac/ax.
  + Architektura bezdrátové sítě: infrastruktura (přístupové body připojují zařízení ke kabelové síti) vs. ad-hoc (přímé připojení mezi zařízeními bez centrálního přístupového bodu).
  + Bluetooth: Krátká vzdálenost, osobní zařízení, používané k připojení periferních zařízení jako jsou klávesnice, myši, sluchátka.

**Aplikační protokoly v sítích:**

* + FTP (File Transfer Protocol): přenos souborů mezi klientem a serverem, používá port 21 pro příkazy a port 20 pro data.
  + HTTP (Hypertext Transfer Protocol): protokol pro přenos webových stránek, používá port 80.
  + HTTPS (HTTP Secure): šifrovaná verze protokolu HTTP, používá protokol SSL/TLS na zabezpečení přenosu údajů, používá port 443.

**Zabezpečení sítí:**

* + Firewall: Síťové zařízení nebo software, které kontroluje a filtruje síťový provoz podle definovaných pravidel a chrání sítě před neoprávněným přístupem.
  + Proxy: Zprostředkovatel mezi klientem a serverem, zvyšuje bezpečnost a anonymitu, může také ukládat a filtrovat obsah.
  + Útoky typu DoS (Denial of Service): Útoky, jejichž cílem je přetížit síťové zdroje a způsobit nedostupnost služeb.
  + Zabezpečení DNS: implementace DNSSEC na ochranu před falšováním DNS a jinými útoky.

**Možnosti anonymizace na internetu:**

* + Anonymizační služby: Tor (The Onion Router) poskytuje anonymitu směrováním komunikace přes několik šifrovaných uzlů.
  + VPN: Bezpečné a šifrované připojení, skrývá IP adresu uživatele.
  + Proxy servery: Skrývají IP adresu uživatele a poskytují přístup k webovým stránkám.