8. Počítačové sítě

Architektura počítačových sítí

Architektura počítačových sítí zahrnuje hardware, software a síťové protokoly, které společně umožňují propojení a komunikaci mezi zařízeními. Typická síť se skládá z klientských počítačů, serverů, síťových zařízení (routery, switche, přístupové body) a komunikačních protokolů, které určují pravidla předávání dat. Síťová architektura definuje také topologii propojení (např. hvězdicová, sběrnicová, kruhová) a rozdělení funkcí mezi jednotlivé vrstvy.

Referenční model ISO/OSI

Referenční model **ISO/OSI** (Open Systems Interconnection) je teoretický rámec, který rozděluje komunikaci v síti do sedmi vrstev, z nichž každá má přesně vymezené úkoly:

1. **Fyzická vrstva:** Přenos jednotlivých bitů po fyzickém médiu (kabely, optika).
2. **Linková vrstva:** Přenos rámců mezi sousedními zařízeními, zajištění detekce chyb a řízení přístupu k médiu (MAC adresy, Ethernet).
3. **Síťová vrstva:** Směrování paketů mezi různými sítěmi (IP, ICMP, ARP).
4. **Transportní vrstva:** Zajišťuje spolehlivý přenos dat mezi koncovými body (TCP, UDP).
5. **Relační vrstva:** Správa relací a spojení mezi aplikacemi.
6. **Prezentační vrstva:** Převod a šifrování dat do formátu srozumitelného pro aplikace.
7. **Aplikační vrstva:** Síťové aplikace a jejich protokoly (HTTP, FTP, SMTP).

Síťový model TCP/IP

TCP/IP model je praktičtější a dnes používaný standard, který rozděluje komunikaci do čtyř vrstev:

1. **Síťový přístup (Network Access):** Fyzická a linková vrstva OSI (Ethernet, WiFi, MAC).
2. **Internetová vrstva:** Zajišťuje směrování (IP, ICMP, ARP).
3. **Transportní vrstva:** Spolehlivý i nespolehlivý přenos mezi aplikacemi (TCP, UDP).
4. **Aplikační vrstva:** Protokoly pro konkrétní aplikace (HTTP, FTP, DNS, SMTP).

TCP/IP model je základem internetu a většiny moderních sítí.

Fyzická vrstva (metalické, optické spoje, hub)

Fyzická vrstva řeší fyzické propojení zařízení. Nejčastější přenosová média:

- **Metalické kabely:** UTP (běžné ethernetové sítě), STP (stíněné pro vyšší rušení), koaxiální kabely (dříve pro starší ethernet, dnes spíše TV).
- **Optické kabely:** Pro vysokorychlostní a dlouhé spoje; dělí se na jednovidové (single-mode, dlouhé vzdálenosti) a vícevidové (multi-mode, kratší).
- **Hub:** Základní síťové zařízení, které rozesílá signál na všechny porty bez ohledu na cílovou adresu (nevytváří oddělené kolizní domény, dnes již nahrazeno switchem).

Adresování na linkové vrstvě (switch, MAC)

Adresování na linkové vrstvě je založeno na **MAC adresách**, což jsou unikátní 48bitové identifikátory síťových zařízení.

- **Switch** je inteligentní zařízení, které směruje rámce jen na konkrétní port podle MAC adresy, čímž snižuje provoz a zlepšuje výkon sítě.
- MAC adresa je vypálena výrobcem do síťového zařízení (NIC) a slouží k jednoznačné identifikaci v rámci místní sítě.

Ethernet

Ethernet je nejrozšířenější technologie pro lokální sítě (LAN). Ethernetový rámec obsahuje cílovou a zdrojovou MAC adresu, typ protokolu, data a kontrolní součet (FCS).

Technologie Ethernet zahrnuje různé rychlosti (např. 10Base-T – 10 Mbps, 100Base-TX – 100 Mbps, 1000Base-T – 1 Gbps). Dnes se často používá i gigabitový Ethernet a vyšší.

Protokol IP – sítě a podsítě (maska, brána, router)

IP protokol je základní protokol síťové vrstvy, slouží k adresování a směrování datových paketů mezi sítěmi.

Síťová maska určuje, která část IP adresy identifikuje síť a která hosta (např. 255.255.255.0).

Brána (gateway) je zařízení (typicky router), které propojuje místní síť s jinými sítěmi nebo internetem.

Router směruje pakety mezi sítěmi na základě IP adres a směrovacích tabulek.

IPv4

IPv4 využívá 32bitové adresy (např. 192.168.0.1) a poskytuje cca 4 miliardy unikátních adres.

Adresy jsou rozděleny do tříd (A, B, C, D – multicast, E – rezervované).

Kvůli nedostatku adres se využívá NAT a vznikl nový standard IPv6.

IPv6

IPv6 používá 128bitové adresy (např. 2001:0db8:85a3:0000:0000:8a2e:0370:7334), což umožňuje obrovský počet unikátních adres a řeší omezení IPv4.

Navíc podporuje nové mechanismy (automatickou konfiguraci, zabudované zabezpečení, multicast), zjednodušuje směrování a odstranil potřebu NAT.

Multicast a unicast

Unicast je přenos od jednoho odesílatele k jednomu příjemci (běžné přenosy v síti).

Multicast umožňuje odeslat data skupině vybraných příjemců současně (například IPTV, videokonference).

ICMP protokol

ICMP (Internet Control Message Protocol) slouží pro diagnostiku a hlášení chyb v síti. Pomáhá například při zjišťování dostupnosti hostu (ping), trasování cesty (traceroute), hlášení nedoručitelných paketů apod.

ARP protokol

ARP (Address Resolution Protocol) překládá IP adresy na MAC adresy v místní síti. Když zařízení potřebuje znát MAC adresu odpovídající IP adrese, vyšle ARP požadavek; zařízení s danou IP adresou odpoví svou MAC adresou.

Směrování v sítích (statické, dynamické, RIP a OSPF protokol)

Směrování je proces výběru cesty, kudy budou data přenášena přes síť:

- **Statické směrování:** Ruční nastavení cest; vhodné pro malé sítě.
- **Dynamické směrování:** Automatické učení a aktualizace tras pomocí směrovacích protokolů.
    - **RIP (Routing Information Protocol):** Jednoduchý, používá počet skoků jako metriku, max. 15 skoků.
    - **OSPF (Open Shortest Path First):** Vhodný pro větší sítě, rychlá konvergence, pracuje na bázi stavu spojení.

Přidělování adres – DHCP

DHCP (Dynamic Host Configuration Protocol) umožňuje automatické přidělování IP adres, síťových masek, bran a DNS serverů zařízení v síti. Zjednodušuje správu a minimalizuje ruční konfiguraci.

Protokoly UDP a TCP

UDP (User Datagram Protocol): Rychlý, nespolehlivý, nespojovaný protokol. Vhodný pro aplikace, kde je důležitá rychlost a nevadí ztráta paketů (streamování, VoIP, online hry).

TCP (Transmission Control Protocol): Spolehlivý, spojovaný protokol. Poskytuje řízení toku, opětovné odesílání ztracených paketů a zajišťuje pořadí doručení. Používá se tam, kde je vyžadována spolehlivost (web, e-mail, přenos souborů).

NAT

NAT (Network Address Translation) umožňuje překlad soukromých IP adres (vnitřní síť) na veřejnou IP adresu (internet). Umožňuje sdílení jedné veřejné adresy více zařízeními a zvyšuje bezpečnost sítě před vnějším přístupem.

Transportní vrstva a porty

Transportní vrstva zajišťuje přenos dat mezi aplikacemi na různých zařízeních.

Porty: 16bitové identifikátory procesu (např. HTTP – 80, HTTPS – 443, FTP – 21).

- Porty jsou rozděleny na: známé (0–1023), registrované (1024–49151) a dynamické (49152–65535).
- TCP používá porty pro vytvoření spojení, UDP pro rychlý přenos.

Streamovaný a datagramový přenos dat

Streamovaný přenos (TCP): Data proudí spojitě mezi dvěma body, zajišťuje spolehlivost a správné pořadí.

Datagramový přenos (UDP): Každý datagram je samostatná jednotka, přenos je rychlý, ale bez záruky doručení nebo pořadí.

DNS

DNS (Domain Name System) překládá doménová jména (např. www.google.com) na IP adresy. Je to hierarchický systém, který zajišťuje snadné vyhledávání a komunikaci v síti.

DNSSEC

DNSSEC (DNS Security Extensions) rozšiřuje DNS o ověřování pravosti a integrity odpovědí pomocí digitálních podpisů, čímž zabraňuje podvržení a útokům typu DNS spoofing.

VPN

VPN (Virtual Private Network) umožňuje bezpečnou, šifrovanou komunikaci mezi zařízeními nebo sítěmi přes veřejný internet. Typy VPN:

- **Site-to-Site:** Propojuje dvě celé sítě.
- **Client-to-Site:** Umožňuje vzdálenému zařízení připojit se do sítě.

Nejčastější protokoly: **IPSec**, **L2TP**, **OpenVPN**.

Bezdrátové technologie (WiFi router, architektura bezdrátové sítě, Bluetooth)

WiFi router: Přístupový bod pro bezdrátovou síť, často v domácnosti či kanceláři, používá standardy IEEE 802.11.

Architektura bezdrátové sítě: Infrastrukturní (přes AP/router) nebo ad-hoc (přímé propojení zařízení).

Bluetooth: Technologie pro krátké vzdálenosti, používána např. pro sluchátka, klávesnice, myši, IoT zařízení.

Protokoly aplikací v sítích (ftp, http, https)

- **FTP (File Transfer Protocol):** Přenos souborů mezi klientem a serverem, port 21.
- **HTTP (Hypertext Transfer Protocol):** Protokol pro přenos webových stránek, port 80.
- **HTTPS:** Šifrovaný HTTP s použitím SSL/TLS, port 443; zajišťuje bezpečný přenos dat na webu.

Bezpečnost na sítích

Zabezpečení počítačových sítí je zásadní pro ochranu dat a systémů před útoky a zneužitím:

- **Firewall:** Filtruje síťový provoz na základě pravidel, zabraňuje neoprávněnému přístupu.
- **Proxy server:** Zprostředkovatel mezi klientem a serverem, zvyšuje bezpečnost a anonymitu.
- **DoS útoky (Denial of Service):** Cílené přetížení služby nebo sítě, která se stává nedostupnou pro legitimní uživatele.
- **Zabezpečení DNS:** Implementace DNSSEC, ochrana před podvržením.
- **Možnosti anonymizace:** VPN, proxy, Tor (směrování přes více uzlů, vysoká anonymita); tyto technologie skrývají skutečnou IP adresu uživatele a chrání soukromí.