

**Otázka:** Síťové modely a architektury

**Předmět:** Informatika

**Přidal(a):** Lukáš Hodbod'

K této otázce je k dispozici i prezentace:

<https://prezmania.cz/sitove-modely-a-architektury-prezentace/>

## **A) TOPOLOGIE**

Topologie sítě popisuje způsob propojení jednotlivých uzlů sítě (tedy počítačů, síťových tiskáren atp.). Rozlišujeme topologii fyzickou (technické propojení) a logickou (způsob komunikace uzlů). Popisované informace se budou vztahovat k topologii fyzické. Fyzická topologie popisuje technické uspořádání sítě, konkrétně fyzické propojení jednotlivých uzlů. V současné době se nejčastěji využívá tzv. hvězdicové a stromové propojení, pro úplnost však popisujeme ještě sběrníkovou topologii a kruhovou topologii sítě.

### **Hvězdicová topologie**

V současnosti **nejpoužívanější topologie**, která umožňuje relativně jednoduché rozšiřování lokální sítě. Základním prvkem je přípojný místo pro uzly sítě. K tomuto místu musí být připojen každý uzel sítě. Nejčastějším přípojným místem je **switch (přepínač)**, ve starších sítích hub (rozbočovač). Hlavní výhodou je snadná rozšiřitelnost sítě přidáním dalšího

switche, dále pak vysoká stabilita při odpojení jednotlivých uzlů a možnost připojování a odpojování uzlů za běhu sítě. Nevýhodou je pak to, že při výpadku switche dojde k vyřazení celého segmentu sítě.

## Výhody

Pokud selže jeden počítač nebo kabel nebude fungovat spojení pouze pro jednu stanicí a ostatní stanice mohou vysílat i přijímat nadále. Dobrá výkonnost v porovnání se sběrníkovou topologií. To souvisí s tím, že na jednom kabelu je připojen pouze jeden počítač a tudíž jednak nedochází ke kolizím mezi pakety a také může současně přenášet data více počítačů. Snadno se nastavuje a rozšiřuje. Závady se dají snadno nalézt

## Nevýhody

U větších sítí vyžadováno velké množství kabelů – ke každému počítači jeden. Potřeba extra hardware v porovnání se sběrníkovou topologií. Toto dnes ale není vzhledem k pořizovacím cenám příliš důležité (výjimkou je gigabitethernet, ale to se do budoucna jistě změní). V případě selhání centrálního síťového prvku přestane fungovat celá síť.

## Stromová topologie

V počítačových sítích pojem stromová topologie označuje propojení počítačů do útvaru tvarem připomínající strom. **Vycházejí z hvězdicové topologie** spojením aktivních síťových prvků, které jsou v centrech jednotlivých hvězd. Takovéto propojení se používá především v **rozsáhlých počítačových sítích** ve velkých firmách. Jednotlivé hvězdice často představují jednotlivá oddělení firmy, patra budovy nebo celé budovy. Tyto hvězdice jsou pak znovu spojeny hvězdíkovitým způsobem.

## **Výhody**

Pokud selže jeden aktivní síťový prvek, ostatní části sítě mohou dále pokračovat. Snižuje se potřebné množství kabelů. Zvýšení bezpečnosti - zvyšuje se obtížnost odposlouchávání síťové komunikace.

## **Nevýhody**

Pokud je špatně udělána a selže-li vysoce postavený síťový prvek (prvek, který je blízko kmenového prvku), ona větev, nemůže s kmenovým prvkem komunikovat.

## **Sběrníková topologie**

Sběrníková topologie využívá jedné **sběrnice**, na kterou jsou připojeny uzly sítě. V počítačových sítích se většinou jednalo o **koaxiální kabel** zakončený na obou stranách speciálním prvkem. V současnosti se sběrníková topologie využívá například při konstrukci inteligentních budov.

Výhodou je jednoduché připojování uzlů, nevýhodou pak vysoká závislost na sběrnici, kde při přerušení znamená výpadek celé sítě.

## **Výhody**

Snadná realizace a snadné rozšíření již stávající sítě. Nevyžaduje tolik kabeláže jako např. hvězdicová topologie. Vhodná pro malé nebo dočasné sítě, které nevyžadují velké rychlosti přenosu.

## Nevýhody

Nesnadné odstraňování závad. Omezená délka kabelu a také počtu stanic. Pokud nastane nějaký problém s kabelem, celá síť přestane fungovat. Výkon celé sítě rapidně klesá při větších počtech stanic nebo při velkém provozu.

## Kruhová topologie

Kruhová topologie předpokládá propojení uzlů sítě v „**kruhu**“. Komunikace na takové síti funguje zcela řízeně – po síti je požadováno právo přístupu k médiu. Vysílat do sítě tak může jen jeden z uzlů. Tím je zaručeno, že nedojde k zahlcení sítě a nebude docházet ke ztrátě dat. Zcela zřejmě je ale síť **náchylná na výpadek kterékoliv stanice**. Proto se často používá tzv., redundantní kruhová topologie (princip náhradního okruhu).

## Výhody

Přenos dat je relativně jednoduchý, protože pakety se posílají jedním směrem. Přidání dalšího uzlu má jen malý dopad na šířku pásma. Nevznikají kolize. Náklady jsou menší než u hvězdicové topologie.

## Nevýhody

Data musí projít přes každý počítač mezi odesílatelem a příjemcem, což zvyšuje dobu trvání přenosu. Pokud se zhroutí jeden uzel, zhroutí se s ním celá síť a data nemohou být správně přenášena. Je těžké najít a odstranit závadu. Protože jsou všechny stanice navzájem propojené, musí se kvůli přidání nového uzlu dočasně vypnout celá síť.

## **B) PRINCIP DEKOMPOZICE**

Zajistit bezchybnou funkčnost sítě jako celku je poměrně složitý problém. Proto je při řešení tohoto úkolu rozkladu celého problému na dílčí celky. Každý celek se věnuje jinému problému (např. přenosu na dat na různých technologiích, komunikaci různých aplikací, atp.) a sestavením pak vznikne funkční síť. Toto řešení se v sítích označuje jako dekompozice sítě na vrstvy.

Základním pravidlem modelu je, že vrstvy jsou hierarchicky uspořádány. Každá vrstva je pak řešena samostatně, musí tedy být jednoznačně vymezeno komunikační rozhraní s okolními vrstvami. Vrstva také nemůže v rámci uzlu komunikovat s jinou vrstvou, než se svou sousedící. V rámci modelů různých uzlů pak spolu komunikují pouze shodné vrstvy.

## **C) MODEL ISO/OSI**

Tento model byl vypracován mezinárodní organizací pro normalizaci ISO za účelem sjednocení a standardizace počítačových sítí a za účelem vypracování norem pro propojování různých systémů. V jednotlivých vrstvách sedmivrstvého OSI modelu se popisují funkce síťových zařízení a protokoly těchto vrstev.

### **7. Aplikační vrstva**

Umožňuje aplikacím na obou stranách přenosu spolupracovat.

FTP, TFTP, DNS, DHCP, SMTP, POP3, SSH a další...

## 6. Prezentační vrstva

Převádí data do tvaru čitelného pro aplikaci, tento tvar může být různý na obou stranách přenosu.

Zajišťuje kódování a konverzi dat do podoby čitelné v cílovém zařízení. Provádí kompresi dat tak, aby je cílové zařízení mohlo dekomprimovat.

Kryptuje data tak, aby nebyla čitelná v síťových mezičláncích, ale až v cílovém zařízení.

## 5. Relační vrstva

Zajišťuje synchronizaci přenosu mezi relačními vrstvami obou stran. Vytváří, obnovuje, a ukončuje relaci mezi protistranami.

NetBIOS, Apple Talk, SSL

## 4. Transportní vrstva

Obsahuje údaje o **zdrojovém a cílovém portu**, čímž je umožněno více současných přenosů. Porty slouží k identifikování procesu (aplikace), který má daná data zpracovat.

Informace o portech jsou nutné, protože běžně mezi počítači probíhá více datových přenosů.

Tato vrstva kontroluje kvalitu přenosu.

TCP, UDP

### 3. Síťová vrstva

Obsahuje informace o zdrojové a cílové **síťové adrese**. Tato informace je nutná především v případě, jestliže síťový přenos probíhá mezi **různými oddělenými lokálními sítěmi**. Na hranici každé lokální sítě je směrovač (nebo podobné zařízení), který zkoumá síťové adresy uvedené v **paketu**, data opět zapouzdří do rámce a odesílaná data přepne na rozhraní, jenž vede k cíli.

Na této vrstvě pracují **směrovače**.

ICMP, ARP, IP

### 2. Spojovací vrstva

Obsahuje informace o zdrojové a cílové **fyzické adrese**. Tyto adresy jsou zodpovědné za doručení rámce v oblasti **lokální sítě**. Pokud jsou data posílána mimo lokální síť, jsou na hraničním zařízení (typicky směrovači) informace o fyzických adresách vyměněny za nové. **Rámec** vždy obsahuje údaje o **MAC adresách** zdrojového a cílového zařízení v aktuální lokální síti, ve které se data pohybují.

Na této vrstvě pracují **přepínače**, mosty a síťové karty.

### 1. Fyzická vrstva

Zabývá se synchronizací a časováním bitů posílaných na síť tak, aby bylo možné data odeslat požadovanou přenosovou rychlostí zvolenou technologií.

## **D) ARCHITEKTURA TCP/IP**

Architektura TCP/IP je členěna do čtyř vrstev (na rozdíl od referenčního modelu OSI se sedmi vrstvami):

aplikační vrstva (application layer)

transportní vrstva (transport layer)

síťová vrstva (internet layer)

vrstva síťového rozhraní (network interface)

### **Vrstva síťového rozhraní**

Nejnižší vrstva umožňuje přístup k fyzickému přenosovému médium. Je specifická pro každou síť v závislosti na její implementaci. Příklady sítí: Ethernet, Token ring, FDDI, 100BaseVG, X.25, SMDS.

### **Síťová vrstva**

Vrstva zajišťuje především síťovou adresaci, směrování a předávání datagramů. Protokoly: IP, ARP, RARP, ICMP, IGMP, IGRP, IPSEC. Je implementována ve všech prvcích sítě – směrovačích i koncových zařízeních.

### **Transportní vrstva**

Transportní vrstva je implementována až v koncových zařízeních (počítačích) a umožňuje



proto přizpůsobit chování sítě potřebám aplikace. Poskytuje transportní služby kontrolovaným spojením spolehlivým protokolem TCP (transmission control protocol) nebo nekontrolovaným spojením nespolehlivým protokolem UDP (user datagram protocol).

## **Aplikační vrstva**

Vrstva aplikací. To jsou programy (procesy), které využívají přenosu dat po síti ke konkrétním službám pro uživatele. Příklady: Telnet, FTP, HTTP, DHCP, DNS.

Aplikační protokoly používají vždy jednu ze dvou základních služeb transportní vrstvy: TCP nebo UDP, případně obě dvě (např. DNS). Pro rozlišení aplikačních protokolů se používají tzv. porty, což jsou domluvená číselná označení aplikací. Každé síťové spojení aplikace je jednoznačně určeno číslem portu a transportním protokolem (a samozřejmě adresou počítače).

## **E) ETHERNET**

**Ethernet** je v informatice **technologie, která se používá pro budování lokálních sítí (LAN)**. V referenčním modelu ISO/OSI **realizuje fyzickou a spojovou vrstvu**, v modelu TCP/IP pak **vrstvu síťového rozhraní**. Jeho popularita spočívá v **jednoduchosti protokolu a tím i snadné implementaci i instalaci**.

Původní protokol s přenosovou rychlostí 10 Mbit/s byl vyvinut firmami DEC, Intel a Xerox pro potřeby kancelářských aplikací. Později byl v poněkud pozměněné podobě normalizován institutem IEEE jako norma IEEE 802.3. Tato norma byla převzata ISO jako ISO 8802-3. Autoři původního Ethernetu vytvořili upravenou verzi *Ethernet II* (tzv. průmyslový standard), která změnila některé časové konstanty s cílem dosáhnout vyšší compatibility se standardem 802.3. Mezi oběma specifikacemi však zůstal rozdíl ve formátu rámce.

V současné době je nejpoužívanější síťovou technologií Ethernet. Tato technologie je,

nezávisle na tom zda jde klasický 10 Megabitový Ethernet nebo jeho rychlejší mutace (Fast a Gigabit Ethernet), založena na velice jednoduchém principu, nazývaném CSMA/CD.

Klasický Ethernet používal sběrníkovou topologii – tedy sdílené médium, kde všichni slyší všechno, a v každém okamžiku **může vysílat jen jeden**. Jednotlivé stanice jsou na něm identifikovány svými hardwarovými adresami (MAC adresa). Když stanice obdrží paket s jinou než vlastní adresou, zahodí jej (karty lze ovšem přepnout do promiskuitního režimu, kdy přijímají všechny pakety, tato možnost se využívá např. při monitorování sítě).

## **F) PŘÍSTUPOVÉ METODY**

Přístupové metody definují pravidla, podle kterých stanice v síti přistupují ke komunikačnímu kanálu (např. kabelu), který společně sdílejí. Zabezpečují, aby v jednom okamžiku komunikovala prostřednictvím komunikačního kanálu pouze jedna stanice. Při současném vysílání více stanic jedním kanálem (např. vodičem) dojde ke vzájemnému rušení, což znemožní přenos dat. Přístupová metoda je jedním z podstatných znaků síťového standardu.

### **CSMA / CD (Carrier-sense Multiple Access with Collision Detection)**

**CSMA (Carrier Sense Multiple Access)** – stanice připravená vysílat data si „poslechne“ zda přenosové médium (kabel) nepoužívá jiná stanice. V případě, že ano, stanice zkouší přístup později až do té doby dokud není médium volné. V okamžiku kdy se médium uvolní, začne stanice vysílat svá data.

**CD (Collision Detection)** – stanice během vysílání sleduje, zda je na médiu signál odpovídající vysílaným úrovním (tedy aby se např. v okamžiku, kdy vysílá signál 0, nevyskytl signál 1). Případ, kdy dojde k interakci signálů více stanic, se nazývá kolize. V případě detekce kolize stanice generuje signál JAM a obě (všechny) stanice, které v daném okamžiku vysílaly, generují náhodnou hodnotu času, po níž se pokusí vysílání zopakovat.

## **CSMA / CA (Carrier-sense Multiple Access with Collision Avoidance)**

Metoda vícenásobného přístupu ke komunikačnímu kanálu se zabráněním vzniku kolize. Používá se u bezdrátových sítí standardu Wi-Fi pro zprostředkování komunikace mezi zařízeními. Pokud chce klientská stanice vysílat, poslouchá, je-li v příslušném komunikačním kanálu nějaká aktivita. Pokud ano, počká náhodně dlouhou dobu a poté se pokusí ke kanálu přistoupit znovu. Pokud je kanál volný, musí klientská stanice nejprve požádat přístupový bod (AP) o vysílání. Vyšle signál RTS (Request To Send – požadavek na přenos) a vyčkává, dokud od přístupového bodu nedostane povolení k vysílání ve formě signálu CTS (Clear To Send). Ostatní klientské stanice připojené k AP mají povel nevysílat.

## **Full-Duplex**

Využívá se u současných sítí hvězdicové topologie. TP kabel obsahuje 4 páry vodičů. 1 pár vodičů je vyčleněn pro přenos dat z počítače do switchu, 1 pár vodičů pro směr opačný. Zbylé páry propojovacího (patch kabelu) nejsou využity. Komunikace prostřednictvím TP kabelu probíhá obousměrně, každé zařízení (např. počítač-switch, počítač-počítač, atd.) má své pevně přidělené vodiče, pomocí nichž může vysílat kdykoliv. Odpadá sdílení média a s ním i důvody pro nasazení algoritmu CSMA/CD. Odpadají zde prostoje způsobené kolizemi a přenosová rychlost odpovídá maximální možné.

## **Token ring**

Používá se především u kruhové topologie sítě. Síť putuje speciální paket – tzv. token. Vysílat může jen ta stanice, která tento paket vlastní. Vysílat může tedy jen jedna stanice. Token si stanice postupně předávají. Paket putuje v kruhu od jedné stanice ke druhé.