Základní pojmy technických sítí

Historicky můžeme hovořit o dvou typech koexistujících sítí – telekomunikačních a počítačových. Každý z těchto sítí pracuje na jiném principu, avšak s jejich vývojem dochází k jejich prolínání a postupnému spojení. Přesto však stále existují zásadní rozdíly v jejich technické specifikaci.

přepojování okruhů

Ve spojových sítích (telekomunikačních) se předpokládá úplné využití přiděleného zdroje (linky). Pracuje se s principem tzv. **přepojování okruhů**. Jako **okruh** se zde rozumí **přenosová cesta mezi dvěma účastníky sítě**, která je **obousměrná a má určenou kapacitu**. Okruh obvykle vzniká a zaniká na žádost některého z účastníků sítě. Okruh tak může existovat bez ohledu na množství právě přenášených dat, což má za následek plýtvání s celkovou přenosovou kapacitou. Právě díky tomu je budování a provoz tohoto typu sítí nákladné.

Hlavní **výhodou** přepojování okruhů **je** zejména **garance přenosové kapacity a jasně odhadnutelná rychlost přenosu** (ta je dána technickou specifikací okruhu). **Nevýhoda** již byla zmíněna – jedná se o **nemožnost poskytnutí volné kapacity** okruhu jinému účastníku sítě.

přepojování paketů

paket

V počítačových sítích se využívá technologie **přepojování paketů**. V síti je k dispozici určitá přenosová kapacita a každý účastník sítě má možnost se sítí komunikovat (přijímat a odesílat pakety). **Paketem zde rozumíme „balíček" dat opatřený adresou příjemce a odesílatele**. Tento paket je odeslán do sítě a síť zajistí jeho doručení.

Store&Forward

vstupní a výstupní fronta

Je zřejmé, že síť musí obsahovat nějaké „chytré" prvky, které zajistí pomocí vhodné technologie správu paketů v síti. Tato technologie (či spíše mechanismus) je často označována jako **Store&Forward**. Nějaký aktivní prvek sítě paket přijme a uloží jej do vyrovnávací paměti (vstupní fronty). Z ní (a ze spousty dalších vyrovnávacích paměti ostatních prvků) si jej odebere jiný „aktivní a chytrý" prvek a zajistí předání paketů do jiné části sítě, přesněji do výstupní fronty. Z této fronty je odeslán k místu určení dle možností přenosové kapacity sítě.

zpoždění přenosu

rozptýlení paketů

Neexistence jednoznačně definované cesty mezi odesílatelem a příjemcem má za následek určité **zpoždění přenosu**. Během přenosu může také dojít k tzv. **rozptýlení paketů** v rámci sítě (tzn. že pakety jedné zprávy půjdou jinými cestami). Rychlost přenosu mezi dvěma uživateli v různých časech bude tak spíše náhodná veličina.

sdílení

agregace

Při připojení více uživatelů k jedné společné lince dochází ke **sdílení** společné linky. To je velice výhodné z hlediska efektivity využití celkové kapacity přenosového spoje. Je však zřejmé, že **míra sdílení** bude mít přímý vliv na kvalitu poskytovaných služeb. Míra sdílení je často označována jako **agregace**, tedy počet uživatelů sdílejících jednu přenosovou kapacitu. Např. u linek ADSL pro domácnosti je obvyklá agregace 1:50.

best effort

Služby provozované na sdílených sítích fungují obvykle bez garantované kvality. Kvalita záleží na celkové zátěži, přičemž není zajištěno, že dojde k uspokojení všech požadavků na přenos paketů. Může dokonce dojít k zahození některých paketů jen proto, aby nedošlo k úplnému zahlcení sítě. Protože ale funguje princip rovného přístupu, jsou pakety k zahození vybírány náhodně. Tento typ přístupu k lince se označuje jako **princip maximální snahy** (best effort).

QoS

FUP

V mnoha případech však může být výhodné určit prioritu jednotlivých přenosů v síti, aby mohlo dojít k zahazování paketů méně důležitých procesů. Takový typ přenosu je

označován jako **QoS (Quality of Service)**. Tento princip je používán např. u linek ADSL a nastaveným **FUP** (Fair Use Policy), kdy je konkrétním uživatelům s překročeným limitem přenesených dat snížena priorita jeho paketů.

spolehlivost přenosu

V souvislosti se zahazováním paketů nás však jistě napadne otázka **spolehlivosti přenosu**. Pokud síť některý paket zahodí, může toto buď oznámit či neoznámit. Podle toho pak označujeme celý přenos jako **spolehlivý či nespolehlivý**. Spolehlivost je možné zajistit na mnoha úrovních přenosu. O kontrolu přenesených dat se mohou postarat samotné aplikace, spolehlivost však může zajišťovat sama síť. Je ale zřejmé, že v případě síťového zajištění se bude muset část přenosové kapacity vyhradit na zasílání kontrolních součtů, popř. nových žádostí o zahozené či jinak porušené pakety.

V případě sítí fungujících na principu přepojovaní okruhů se obvykle realizuje přenos spolehlivý. Sítě s přepojováním paketů pak fungují povětšinou nespolehlivě s možností volby spolehlivého přenosu pro konkrétní aplikace.

Rozdělení počítačových sítí

Jednoznačná taxonomie počítačových sítí neexistuje. Můžeme si vytvořit spoustu „umělých“ kritérií a podle těch pak různé sítě rozdělovat, k čemu by to ale bylo? Omezme tedy tuto kapitolu spíše na výklad pojmů, které se mohou v souvislosti se „škatulkováním“ vyskytnout.

Rodina sítí -AN

LAN, MAN, WAN, PAN

Nejznámější dělení sítí bere v úvahu jejich velikost, odtud pak zkratky WAN, MAN, LAN a PAN. Všechny zkratky vznikají z anglických pojmů: Wide- Metropolitan- Local- Personal- Area Network. Z dnešního pohledu je však poměrně složité určit hranice velikosti sítě. Lokální síť je obvykle umístěna v rámci jedné budovy či firmy, metropolitní síť pak pokrývá oblast města, WAN může být síť velké nadnárodní korporace a naopak PAN (relativně nový pojem) síť osobních pomůcek jednoho uživatele s dosahem několika metrů (mobilní telefon, PDA, atp.).

Internet

internet

Vzájemným propojením lokálních sítí vzniká propojená soustava označovaná anglickým pojmem internetwork. Pro uživatele se tak skrývá vnitřní struktura jednotlivých sítí a přistupují ke všem jako k jednomu celku. Zářným příkladem takto propojených sítí je právě Internet.

Intranet a extranet

intranet, extranet

Počítačová síť vzniká většinou proto, aby přinášela uživateli nějakou službu. Na základě toho, komu je služba poskytována rozlišujeme sítě pro vnitřní a vnější použití. Intranet je obvykle provozován pro vnitřní potřebu majitele (provozovatele) sítě. Často se jedná o jakýsi vnitřní komunikační kanál v rámci firmy. Naproti tomu extranet poskytuje služby zvnějšku, což nejčastěji budou internetové prezentace včetně různých obchodů, online náhledů do skladu, možnost publikování atp.

Sítě serverové a peer-to-peer

server

peer-to-peer

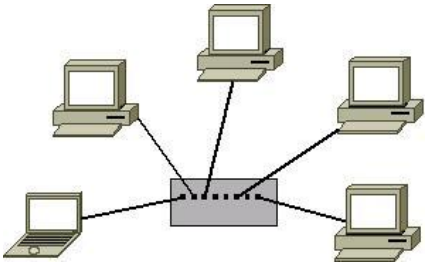
A další dělení – nyní podle technického „pozadí“ sítě. Přijmeme-li, že síť je tvořena z počítačů a další nutné síťové infrastruktury, pak postavení jednotlivých počítačů v síti může být různé. Budujeme-li malou síť v rámci domácnosti, budou si asi všechny počítače „rovny“. Na jednom budou uloženy filmy, na druhém fotky, jeden bude sloužit jako zprostředkovatel tiskárny atp. Zároveň však platí, že na každém z těchto počítačů se bude i normálně pracovat. Zde se bude jednat o síť typu peer-to-peer. Objeví-li se však v síti vyhrazený počítač, který bude vykonávat výhradně služby pro ostatní účastníky sítě, budeme mluvit o síti serverového typu. Typickými servery jsou servery souborové, tiskové, atd.

Topologie sítí

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 (nebude-li uvedeno jinak).

Fyzická topologie popisuje technické uspořádání sítě, konkrétně fyzické propojení jednotlivých uzlů. V současné době se nejčastěji využívá tzv. hvězdicové propojení, pro úplnost však popisujeme ještě sběrnicovou topologii a kruhovou topologii sítě.

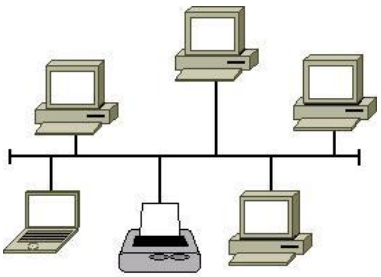
Hvězdicová topologie



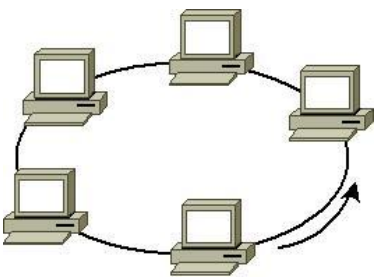
V současnosti nejpoužívanější topologie, která umožňuje relativně jednoduché rozšiřování lokální sítě. Základním prvkem je přípojné místo pro uzly sítě. K tomuto místu musí být připojen každý uzel sítě. Nejčastějším přípojným místem je switch (přepínač), ve starších sítích hub (rozbočovač). Hlavní výhodou 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. Připojování každého uzlu ke switchi může být za určitých podmínek komplikované.

Sběrnicová topologie

Sběrnicová topologie využívá jedné sběrnice, na kterou jsou připojoeny uzly sítě. V počítačových sítích se většinou jednalo o koaxiální kabel zakončený na obou stranách speciálním prvkem. V současnosti se sběrnicová topologie využívá například při kontrukci inteligentních budov. Výhodou je jednoduché připojování uzlů, nevýhodou pak vysoká závislost na sběrnici, kde při přerušení znamená výpadek celé sítě.



Kruhová topologie

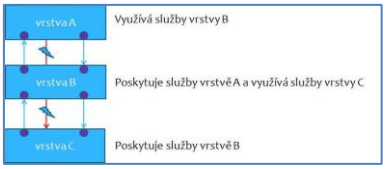


Kruhová toplogie předpokládá propojení uzlů sítě v „kruhu“. Komunikace na takové síti funguje zcela řízeně – po síti je přádáváno právo přistupu k médiu. Vysílat do sítě tak může jen jeden z uzlů. Tím je zaručeno, že nedojde k zahlcení sítě a nebude docházet ke ztrátě dat. Zcela zřejmě je ale síť náchylná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

Síť jako celek, síťový model

Zajistit bezchybnou funkčnost síťě 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.

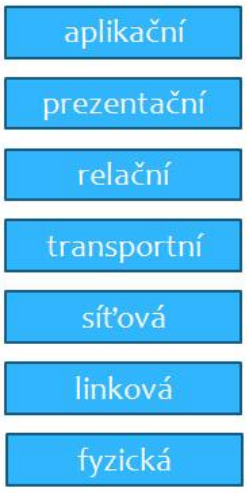
Pravidla vrstevnatých modelů



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.

Referenční model ISO/OSI

Referenční model ISO/OSI vznikl jako reakce na požadavek univerzální síťové platformy. Lze jej chápat jako ucelenou představu o tom, jak mají sítě fungovat, jak mají být řešeny atp. Základní myšlenka modelu je právě existence uspořádaných vrstev. Při jeho tvorbě se postupovalo od obecného ke konkrétnímu, tzn. že se vůbec neřešily konkrétní problémy z praxe, ale navrhoval se obecný princip komunikace v sítích. Z původní myšlenky se však muselo mírně slevit – řešení trvalo dlouho a zahrnovalo obrovské množství obecných požadavků na sítě. Model ISO/OSI se tak stal spíše „ideálním“ standardem pro sítě, v praxi se prosadil jednodušší model TCP/IP.



Referenční model ISO/OSI však v žádném případě není nic mrtvého. Obsahuje mnoho dílčích řešení, které mají stále reálnou šanci na existenci ve světě sítí. Právě tak i vrstavnatý princip se přenesl (byť ve zredukované podobě) do modelu TCP/IP.

Model ISO/OSI poskytuje spojované a spolehlivé služby. Každá vrstva modelu obsahuje mechanismy pro případnou nápravu chyby, což spotřebovává velkmé množství prostředků. Později byla do modelu přidána možnost nespolehlivé komunikace. Na další tlak odborné veřejnosti byla dodatečně dopracována i podpora nespojované služby.

Základní funkce vrstev

Fyzická vrstva definuje technické podrobnosti přenosu signálu. Ve skutečnosti se bude jednat o konkrétní technickou specifikaci (napětí, časování, paralelní či sériová přenos atp.). Vrstva tak skutečně zajišťuje pouze přenos elektrického signálu (ne informace) ve formě bitů.

Vrstva linková (spojová)

Na této vrstvě dochází ke shlukování bitů do formy rámců. Na tomto místě se stávají z dat informace. Každý rámec je označen příznakem začátku a konce a následně

předán vyšší vrstvě. Linková vrstva také zajišťuje řízený přístup uzlu k přenosovému médiu (aby nedocházelo k zahlcení). Spojení lze realizovat výhradně v dosahu přímého spojení (na cestě nemůže být žádný přepojovací prvek – např. switch).

Vrstva síťová

Nejdůležitější funkcí síťové vrstvy je nasměrování dat od zdroje k cíli – tedy nalezení cesty v síti. Na této vrstvě již přenášíme skutečné pakety označené odesílatelem a adresátem a vrstva zajišťuje jejich správné směrování. Musí tedy znát topologii sítě a v případě zahlcení musí být schopna toto řešit.

Transportní vrstva

Na úrovni transportní vrstvy dochází k řízení datových toků, resp. Správnému přiřazování paketů k tokům. Vrstva také může volitelně zajišťovat spolehlivost přenosu. Vrstva může změnit nespojový přenos na spojový.

Relační vrstva

Relační vrstva je první z vrstev, které se věnuje rozpoznávání jednotlivých uživatelů v síti. Dokáže sledovat platnost hesla, dobu přihlášení, regulovat tok dat jednotlivých uživatelů atp. Zajišťuje také správu relací, včetně případné šifrované komunikace mezi dvěma účastníky sítě.

Prezentační vrstva

Vzhledem k tomu, že v síťovém prostředí se může vyskytovat spousta různých počítačů s rozdílnou architekturou, je nutné zajistit konverzi přenášených dat. Jestliže jeden počítač odešle znakovou zprávu „IP23“, je nutné aby ji příjemce opět dostal jako čtyři znaky „IP23“ a ne např. jako dva znaky a jedno číslo. O tuto stránku věci se stará právě prezentační vrstva. Vrstvu již ale nezajímá skutečný význam předané zprávy, pouze data předá dále.

Aplikační vrstva

Aplikační vrstva zajišťuje aplikacím přístup do síťového prostředí. V této vrstvě jsou definovány mnohé uživatelsky orientované protokoly (POP3, SMTP, DNS, DHCP, SSH, FTP, …). Vrstva zprostředkovává aplikacím veškeré služby, které síť nabízí.

Referenční model TCP/IP

Spíše než referenčním modelem je TCP/IP souborem protokolů. Jedná se o „konkurenční“ model fungování sítí k modelu ISO/OSI. Často pro TCP/IP nalezneme i označení síťová architektura. Počátky TCP/IP se datují do konce 60. let, kdy bylo nutné zajistit fungování sítě ARPANET. Dnešní podoba byla dotvořena v letech 1977 až 1979.

Při tvorbě modelu TCP/IP se na rozdíl od ISO/OSI nesnažili tvůrci zajistit spolehlivost přenosu. Její zajištění bylo ponecháno na vlastní aplikaci, či spíše na transportní vrstvě modelu. Vše co je pod transportní vrstvou tak nemusí být ztíženou zbytečnou režií, kterou s sebou vynucená spolehlivost přináší (kontrolní součty, opětovné přenosy, potvrzování atp.). Architektura TCP/IP tak pracuje jako nespojovaná a nespolehlivá služba na principu best effort – maximální snahy o doručení.

Vrstva síťového rozhraní

Linková vrstva (jak se také označuje) zajišťuje vše, co je spojeno s příjmem a odesíláním paketů. TCP/IP model neobsahuje žádné další bližší specifikace způsobu přenosu, neboť způsob přenosu může být různý.

Síťová vrstva

Tato vrstva využívá služeb předchozí vrstvy, není tedy závislá na použité technologii. Často je označována jako IP vrstva, neboť její realizace je zajištěna protokolem IP. Vrstva má jeden zásadní úkol – dopravit pakety od odesílatele k příjemci a to i přes případné směrovače (brány). Protokoly této vrstvy jsou zejména ARP a ICMP.

Transportní vrstva

Transportní vrstva poskytuje služby poslední vrstvě TCP/IP modelu, tedy vrstvě aplikační. Pracuje s protokoly TCP nebo UDP v závislosti na požadavku aplikační vrstvy. Komunikace mezi aplikační a transportní vrstvou probíhá pomocí tzv. portů.

Aplikační vrstva

Na této vrstvě jsou definovány protokly jako http, ftp, telnet, pop3, smtp, imap atp. Tyto protokoly využívají aplikace k vzájemné komunikaci na úrovní aplikační vrstvy modelů různých síťových uzlů.