**Architektura sítí**

**EDUCAnet Pardubice, Jiří Flek**

* Počítačová síť je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači
* Umožňuje uživatelům komunikaci podle určitých pravidel, za účelem sdílení využívání společných zdrojů nebo výměny zpráv

**Historie sítí**

* Sahá až do 60. Let 20. Století, kdy začaly první pokusy
* 1962 – projekt ARPA, americká armádní agentura zabývající se vývojem technologií, které mají uplatnění ve vojenství
* 1969 – síť Arpanet se čtyřmi uzly, univerzitní PC v různých částech USA
* 1972 – k síti ARPANET připojeno 50 výzkumných a vojenských center. Později byla síť rozdělena na dvě, na Arpanet a Milnet, což byla armádní síť
* Za první síť je považován systém ARQ, který byl vyvinut v průběhu II. světové války
* Systém dokázal poslat skupinu znaků a následně analyzovat, jestli nedošlo k chybě. Pokud chyba nastala, příjemce vyslal signál na opakování přenosu. Do jisté míry se tento systém zachoval dodnes.
* V průběhu byla vytvořena celá řada síťových technologií
* V poslední době jsou všechny sítě postupně spojovány do globální celosvětové sítě internet, která používá sadu protokolů TCP/IP

**Přínosy sítí**

* Komunikační prostředek
* Elektrický přenos dat
* Sdílení
* Centrální řízení a dohled
* Prostředek vzdělávání
* Zábava
* Elektronický obchod
* Cloud computing

**Negativa sítí**

* Prostředek porušování autorských práv
* Viry
* Nebezpečí útoku
* Možnost odposlechu
* Šíření poplašných zpráv

**Typy uzlů**

* Servery – poskytují ostatním stanicím určité služby (souborové, aplikační, tikové, databázové, poštovní, terminálové), může být v síti i více serverů (v malých nemusí být žádný)
* Pracovní stanice – počítač, u kterého je uživatel, využívá služeb poskytovaných severem

**Síťová architektura**

**= struktura řízení komunikace**

* Komunikace a její řízení je složitý problém, proto se dělí na několik vrstev
* Členění do vrstev odpovídá hierarchii činností, které se při řízení komunikace vykonávají
* Každá vrstva sítě je definována službou, která je poskytována vyšší sousední vrstvě, a funkcemi, které vykonává v rámci protokolu
* Řízení komunikace slouží ke spolupráci komunikujících prvků, tato spolupráce musí být koordinována pomocí řídících údajů
* Koordinaci zajišťují protokoly, které definují formální stránku komunikace. Protokoly jsou tedy tvořeny souhrnem pravidel, formátů a procedur, které určují výměnu údajů mezi dvěma či více komunikačními prvky
* Tato síťová architektura, tzv. architektura otevřených systémů (zvaná též OSA, původem v anglickém Open System Architecture). Byla normalizována organizací ISO, která vytvořila referenční model OSI
* Praktickou realizací vrstvové síťové architektury je sada protokolů TCP/IP, i když neodpovídá přesně referenčnímu modelu ISO
* Rozlišujeme dva zákl. typy architektury: peer to peer a klient-server

**PEER TO PEER (P2P)**

* Síťová architektura, kde jsou si všechny PC rovny
* Každá stanice v síti může vyčlenit některý svůj prostředek pro sdílení. Jiná stanice je může používat, pokud se prostředek připojí a uživatel zná heslo
* Sdílení a hesla mohou být kdykoliv změněna nebo zrušena uživatelem, který u stanice pracuje.
* Tuto síť nelze centrálně spravovat
* Př. sdílení souborů a systémových prostředků v různých OS a souborů v internetových sítích.

**Klient-server**

* Jeden nebo více PC je nadřazených jinému PC (klientovi)
* Server poskytuje služby běžným stanicím – klientům
* Serverů může být více typů podle poskytovaných služeb (souborový server, tiskový server, poštovní server, WWW server, FTP server atd.) nemusí platit, že server je počítač, u malých sítí plní úlohu několika typů serverů jeden „fyzický“ počítač, u velkých serverů může počítač plnit pouze funkci tiskového serveru. Server může dokonce sloužit i jako běžná pracovní stanice sítě (je to ovšem ojedinělé, snižuje se výkonnost a bezpečnost sítě)

**Klasifikace sítí**

* sítě dělíme podle přepojování, podle druhu přenášených signálů, podle uživatele, podle přenosu dat a nejužívanějším je dělení sítí z hlediska rozlehlosti a účelu.
* **Dělení sítí podle přepojování:**
	+ Komutační síť (ISDN)
	+ Paketová síť (Ethernet)
	+ Kombinovaná síť (ATM)
* **Dělení podle druhů přenášených signálů:**
	+ Analogová síť
	+ Digitální síť
* **Dělení sítí podle jejich rozlehlosti**
	+ PAN
	+ LAN - lokální
	+ MAN - metropolitní
	+ WAN - celosvětová
* **Dělení sítí podle uživatele**
	+ Veřejná síť
	+ Privátní síť
* **Dělení sítě podle způsobu přenosu dat**
	+ Kabelová síť
	+ Bezdrátová síť

**Komutační síť**

* Jedná se o starší technologii, která se využívá již od počátků telegrafie a telefonie a od pozdějších let i v architektuře ISDN (Integrated Services Digital Network).
* Jejím hlavním úkolem je zajistit spojení mezi zdrojovým a cílovým uzlem (vyhradí se kapacita) a tato nově vzniklá cesta je jim k dispozici po celou dobu, dokud spojení neukončí.
* Data jsou posílána po předem sestaveném okruhu.

**Paketová síť**

* Základem je, že cesta, kterou paket "putuje", není od zdrojového po cílový uzel známá. Každý paket se tak přenáší jinou trasou, která je ovlivněná topologií sítě, její propustnostní a výpadky uzlů.
* Každá část v sobě nese informaci o cíli své cesty a je počítačovou sítí doručována samostatně.
* Příklad je Ethernet.

**Kombinovaná síť**

* Některé sítě vykazují vlastnosti sítí komutačních i paketových. Příkladem takové sítě je třeba ATM, která spíše přepojuje okruhy, ale může přepojovat i pakety.

**Analogová síť**

* Analogový signál má stavů nekonečně (nazýván někdy spojitý) a digitální konečně mnoho (2,4,20,50... stavů).

**Digitální síť**

* Digitální signál je často pouze binárním signálem, přenášené hodnoty jsou jen dvě - nula a jednička.

**Podle rozlehlostí sítí a zároveň podle účelu sítí rozdělujeme sítě na 4 základní skupiny:**

* **PAN** - původem anglické Personal Area Network, též označována jako osobní síť, je to velice malá počítačová síť používaná pro propojení jeho osobních elektronických zařízení typu mobilní telefon, PDA, notebook atd., rozlehlost je ze sítí nejmenší, příkladem je Bluetooth, IrDA..
* **LAN** - původem v anglickém Local Area Network, též zván lokální síť nebo místní síť, je to síť spojující uzly v rámci jedné budovy nebo několika blízkých budov, vzdálenosti stovky metrů až kilometry (při použití optiky), rozlehlost je teda větší než rozlehlost PAN, ale menší než rozlehlost MAN, nejpoužívanějším typem je dnes Ethernet;
* **MAN** - původem anglické Metropolitan Area Network, též zván Metropolitní síť, je to síť propojující lokální sítě v městské zástavbě, slouží především pro přenos dat, zvuku a obrazu, spojuje vzdálenosti řádově jednotek až desítek kilometrů a rozlehlost je tedy větší, než rozlehlost LAN, ale menší, než WAN.
* **WAN** - původem v anglickém Wide Area Network, též zván rozlehlá síť, je to sítě spojující LAN a MAN sítě, mají největší působnost (třeba i po celém státě, kontinentu, nebo kamkoli po zeměkouli nebo i do nejbližšího vesmíru).

**Sítě podle uživatele**

* Oblíbeným způsobem klasifikace počítačových sítí je i jejich rozdělování na privátní a veřejné. Hranice mezi těmito dvěma kategoriemi přitom bývala dosti přesně vymezená, ale v poslední době se začíná rozlišování mezi privátními a veřejnými sítěmi poněkud komplikovat - což souvisí mj. i s tím, že se stále více prosazují i tzv. virtuální privátní sítě, vytvářené v rámci sítí veřejných.
* Veřejná síť
	+ Pod veřejnou sítí chápeme tu síť, do které má přistup každý uživatel.
* Privátní síť
	+ Pod privátní sítí chápeme tu síť, která slouží jednomu konkrétnímu subjektu (např. firmě, podniku, organizace apod.).

**Sítě podle přenosu dat**

* Kabelová síť
	+ Kabelová síť je typ počítačové sítě, ve které je spojení mezi jednotlivými účastníky sítě uskutečňováno pomocí kabelů.
	+ Metalické a nemetalické.
* Bezdrátová síť
	+ Bezdrátová síť je typ počítačové sítě, ve které je spojení mezi jednotlivými účastníky sítě uskutečňováno pomocí bezdrátové komunikace, nejčastěji elektromagnetických vln.

**TOPOLOGIE SÍTÍ**

* zabývá se zapojením různých prvků do sítí a zachycením jejich skutečné a logické podoby
* topologii lze brát jako strukturu sítě
* Například počítače v malé domácí síti mohou být uspořádány v pomyslném kruhu, ale nemusí to nutně znamenat, že jejich logické zapojení představuje příklad kruhové topologie



**Struktura sítí LAN**

* Propojené uzly mohou vytvářet různé konfigurace, které jsou určeny typem dané sítě, přičemž struktura závidí na úrovni pohledu:
* **Fyzická topologie** popisuje reálnou konstrukci sítě, zapojená zařízení a jejich umístění včetně nainstalovaných kabelů
* **Logická topologie** se vztahuje k tomu, jak jsou data v síti přenášena a kudy protékají z jednoho zařízení do druhého (nemusí nutně kopírovat fyzické schéma sítě)
* **Signálová topologie** mapuje skutečné propojení mezi uzly v síti sledováním, kudy signál prochází

**SBĚRNICE**

* Sdílí fyzicky či logicky jeden přenosový kanál v každém směru. Stanice jsou k fyzické sběrnici připojeny vysokoimpedačně, takže vypnutí či výpadek stanice neohrozí činnost sítě. Síť nepotřebuje centrální prvek
* V jeden okamžik na sběrnici může vysílat jen jeden PC, pokud začnou dva, dojde ke kolizi dat

Plusy: není potřeba centrální prvek, náklady, snadné připojení dalších stanic, porucha 1 stanice nemá vliv na ostatní

Mínusy: při vysokém počtu stanic nízká rychlost, špatná lokalizace závad, při poškození sběrnice nebo vadném t-konektoru spadne celá síť

Struktury sítí LAN – sběrnice (nahoře bus)

* CSMA – je pravděpodobnostní protokol přístupu k médiu, ve kterém uzel ověřuje nepřítomnost dalšího provozu před vysíláním na sdílené fyzické médium

Struktury sílí LAN – hvězdicová topologie (nahoře star)

* Propojení počítačů do útvaru hvězdy
* Nejpoužívanější způsob zapojení
* Při zkolabování hubu zkolabuje celá síť

**Přenosové a přístupové metody**

jiří Flek, EDUCAnet - Střední odborná škola Pardubice, s.r.o

**Přenosové metody**

- Přenosové metody dělíme pro sítě LAN, podle počtu cílových uzlů, ke kterým je cílový paket směrován.

- Rozlušujeme následující přenosové metody:

 - unicast

 - multicast

 - broadcast

**Unicast**

 - paket je posílán od zdroje informace na definované místo určené v síti. Vysílací zdrojová stanice musí určit cílovou stanici její adresou. Následně je paket odeslán do sítě, která se musí postarat o doručení předmětného paketu cílové stanici v síti.

**Multicast**

 - Spočívá v odeslání určeného paketu předem určené podmnožině uzlů v síti. Zdrojový uzel sítě adresuje paket s použitím zvláštní adresy, která je použita v síti k vytvoření kopií paketu a k odeslání těchto kopí každému příjímacímu uzlu, jehož adresa je součástí určené podmnožiny uzlů.

**Broadcast**

 - Používá se k odeslání paketu všem uzlům v síti. Paket je speciální adresou a jeho úlohou je, aby se vytvořila kopie paketu a byla odeslána všem uzlům v síti.

 - Je to vyysílání jednoho všem, tedy vysílyný paket je zachycen všemi zařízením v síti, lepe řečeno v dané broadcast doméně (subnetu). Toto vysílání se používá převážně v LAN sítích (ne WAN). Broadcasty jsou dnes používány pro řadu účelů (třeba DHCP, ARP) a využívá je velké množství aplikací.

 - Broadcast domain je logická část sítě, ve které mohou připojená zařízení přímo komunikovat. Mělo by se tedy jednat o jeden subnet a hranicí je router, který by broadcasty neměl přeposílat.

 - Subnet Directed Broadcast je speciálním případem broadcastu, který se použije ve chvíli, kdy chceme zaslat broadcast do jiného subnetu, než v kterém se nacházíme.

 - Funguje to tak, že rámec (frame) putuje sítí jako unicast přes routery až na router, který má cílový subnet (určený broadcastovou adresou subnetu) jako přímo připojený. Tento router upraví rámec na běžný broadcast a odešle jej na odpovídající rozhranní.

 - Protože však tato technika byla používána k útokům, tak bývá na routerech nebo i firewallech většinou zakázána. To se týká routeru, který by měl rámec převést na broadcast, přes ostatní by měl rámec projít normálně.

**Přístupové metody**

- Signál nesoucí informaci se přenáší určitým komunikačním kanálem, který musí být v okamžiku vysílání volný, aby nedocházelo k znehodnocení vyslané informace. Často se totiž stává, že daná přenosová kapacita spoje je využívána pro mnoho přenosů.

- Musí být tedy implementovány metody, které řeší problematiku sdílení přenosové kapacity. Metody lze v nejhrubším pohledu rozdělit na statické a dynamické.

**Statické**

Princip statických přístupových metod spočívá v tom, že danému přenosu je po celou dobu

komunikace (komutované spoje) či dokonce stále (pevné spoje) vyhrazena určitá přenosová

kapacita. Princip odpovídá spojování okruhů. Existuje řada způsobů:

**SD (Space Division)** - prostorové dělení, každý spoj je řešen zvláštním vedením. U bezdrátových

spojů je to řešeno dostatečnou vzdáleností v prostoru.

**FDMA (Frequency Division Multiple Access)** – kmitočtový multiplex, každé spojení je realizováno v

jiném kmitočtovém pásmu

**TDMA (Time Division Multiple Access)** – časový multiplex, signál je sdružen se signály ostatních

spojů do jednoho vysokorychlostního spoje. Vzniká tak rámec, kde každému spoji je přidělen určitý

časový slot.

**CDMA (Code Division Multiple Access)** - kódový multiplex, přenos s rozprostřeným spektrem, kdy

každému spoji je přidělena určitá posloupnost, která řídí způsob vysílání:

**FHSS (Frequency Hopping Spread Spectrum)** - s přeskakováním kmitočtů,

**THSS (Time Hopping Spread Spectrum)** - s přeskakování časových slotů,

**DSSS (Direct Sequence Spread Spectrum)** - s přímým rozprostřením spektra,

**OFDMA (Orthogonal Frequency Division Multiple Access)** - ortogonální kmitočtový multiplex

**VOFDMA (Vectored OFDMA)** - Řada aplikací využívá kombinace několika výše uvedených metod.

Například systém GSM pracuje na bázi kombinace FDMA, SD a TDMA.

**Dynamické přístupové metody**

- u dynamických metod je celá přenosová kapacity k dispozici všem přenosům a jednotlivé zdroje se musí o přidělení možnosti vysílat určitým způsobem ucházet - často soupeřit

- Dynamické přístupové metody lze rozdělit do několika skupin:

 - deterministické

 - distribuované

 - náhodné

- Deterministické metody s centrálním přidělováním umožňují implementaci priorit.

- V síti existuje centrální uzel, který uděluje koncovým stanicím oprávnění k vysílání a to:

 - na žádost - koncová stanice žádá centrální uzel o právo vysílat

 - na výzvu - centrální stanice se dotazuje koncových stanic, zda nechtějí vysílat

 **Fyzický kruh**

- stanice spojené do fyzického kruhu si mezi sebou po směru vysílání předávají pověřovací rámec, který probíhá mezi stanicemi. Stanice, která chce využívat přenosovou kapacitu si tento rámec na určitou dobu zablokuje pro sebe a zabere si tak přenosou kapacitu kruhu (např. Token Ring)

**Logický kruh**

 - stanice jsou fyzicky spojeny do jiné topologie (sběrnice, hvězda), avšak z hlediska řízení přístupu tvoří logický kruh, kdy si stanice opět předávají pověření opravňující přístup ke sdílenému přenosovému kanálu

- přístup ke sdílenému kanálu je náhodný proces, není zaručeno, kdy se stanice dostane k možnosti odeslat zprávu

**Aloha** - koncová stanice zahájí vysílání v kterýkoliv okamžik, aniž by si ověřila, zda již nevysílá jiná stanice. Pokud do určité doby nedostane potvrzení, pošle zprávu znovu. Tato metoda vykazuje velmi nízké procento reálné propustnosti z celkové kapacity kanálu asi (při více stanicích asi jen 20 %)

**Slotted Aloha (taktovaná)** - koncová stanice může zahájit vysílání pouze v pevně stanovených okamžicích (čas je rozdělen do slotů). Maximální dosažitelné využití kapacity se tak téměř zdvojnásobí (35 %)

**CSMA (carrier Sense multiple access)** - koncová stanice před vlastním vysíláním kontroluje obsazení kanálu. Pokud je kanál obsazený, stanice čeká a pravidelně kontroluje jeho stav. Je-li volný, pak záleží na podtypu metody.

1) **Naléhající CSMA (1-persistant CSMA)**

* před odesláním rámce se testuje stav kanálu
* je-li kanál obsazen, odloží se vysílání na okamžik jeho uvolnění
* riziko kolize stanic čekajících na uvolnění kanálu
* při kolizi čekání náhodnou dobu před dalším pokusem

2) **Nenaléhající CSMA (non-persistant CSMA)**

* při detekci obsazeného kanálu se počká náhodnou dobu, pak opět test obsazení.
* čekací doba se obvykle volí jako k-násobek doby průchodu signálu sdíleným médiem

**3) p-naléhající CSMA (p-persistant CSMA)**

* při potřebě vysílání se počká na okamžik uvolnění kanálu (nebo byl volný okamžitě)
* s pravděpodobností p začne vysílat, s pravděpodobností (1-p) se počká 1 timeslot a opakuje se do úspěšného odeslání rámce
* pokud mezitím začala vysílat jiná stanice, počká se náhodnou dobu (jako při kolizi)
* volbou p lze nastavit optimální využití kanálu pro danou zátěž
* pro p=1 jde o naléhající CSMA
* pro velmi malá p značně narůstá průměrná doba doručení paketu

**CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**

* patří v počítačových sítích do třídy protokolů označovaných jako metody s vícenásobným přístupem a nasloucháním nosné (CSMA). Jejich charakteristikou je, že před začátkem vysílání paketu stanice určitý čas poslouchá, zda je přenosové médium volné. Pokud ano, může zahájit vysílání. V opačném případě čeká na konec právě probíhajícího vysílání.
* Protokoly skupiny CSMA/CA na rozdíl od CSMA/CD nezjišťují výskyt kolizí (současného vysílání více stanic). Jednotlivé varianty se od sebe mírně odlišují. V CSMA/CA protokolu použitém v síti LocalTalk stanice při volném médiu nejprve ohlásí ostatním, že bude vysílat a médium si tak „zamluví“. Následně odvysílá datový rámec. Bezdrátové sítě standardu 802.11 používají jiný přístup - zde stanice při volném médiu počká náhodně zvolenou dobu a pokud do té doby neobsadí médium někdo jiný, odvysílá datový rámec a následně čeká na jeho potvrzení.

**CSMA/CD (Carrier Sense with Multiple Access and Collision Detection)**

* Stanice (síťová karta), která potřebuje vysílat, naslouchá co se děje na přenosovém médiu. Pokud je v klidu, začne stanice vysílat. Může se stát (v důsledku zpoždění signálu), že dvě stanice začnou vysílat přibližně ve stejný okamžik. Jejich signály se pochopitelně navzájem zkomolí. Tato situace se nazývá kolize a vysílající stanice ji poznají podle toho, že během svého vysílání zároveň zjistí příchod cizího signálu.
* Stanice, která detekuje kolizi, vyšle krátký signál (jam o 32 bitech). Poté se všechny vysílající stanice odmlčí a později se pokusí o nové vysílání.
* Mezi opakovanými pokusy o vysílání stanice počká vždy náhodnou dobu. Interval, ze kterého se čekací doba náhodně vybírá, se během prvních deseti pokusů vždy zdvojnásobuje. Stanice tak při opakovaných neúspěších „ředí“ své pokusy o vysílání a zvyšuje tak pravděpodobnost, že se o sdílené médium úspěšně podělí s ostatními. Pokud se během šestnácti pokusů nepodaří rámec odvysílat, stanice své snažení ukončí a ohlásí nadřízené vrstvě neúspěch.
* Ke kolizi může dojít jen v době, která uplyne od začátku vysílání do okamžiku, kdy signál vysílaný stanicí obsadí celé médium (pak již případní další zájemci o vysílání zjistí, že médium není volné a počkají na jeho uvolnění). Tento interval se nazývá kolizní okénko a musí být kratší, než je doba vysílání nejkratšího rámce. Jinak by mohlo docházet k nezjištěným kolizím (dvě vzdálené stanice odvysílají krátké rámce, které se na kabelu protnou a zkomolí, ale obě stanice ukončí vysílání dříve, než k nim dorazí kolidující signál).
* Tato metoda přístupu k médiu je velmi efektivní při nižším zatížení sítě (cca 30 % šířky pásma). Její efektivita klesá při větším počtu zájemců o vysílání, kdy může dojít k exponenciálnímu nárůstu kolizí. Efektivita CSMA/CD je vyšší pro delší rámce, protože při jejich přenosu je výhodnější poměr mezi trváním kolizního okénka a vysílání dat.

**Model ISO/OSI**

**Vrstevnatá filosofie:**

* Implementovat funkčí síť je hodně složité a náročné (stejně jako při řešení velkých SW celků)
* Jde o jeden velký problém, který se vyplatí dekomponovat (rozdělit na menší části, které je možné řešit samostatně)
* Dekompozice se provede po hierarchicky uspořádaných vrstvách
	+ Kolik vrstev?
	+ Co která vrstva dělá?
	+ Jak vrstvy spolupracují?
* **Horizontální komunikace:**
	+ Vzájemná komunikace stejnolehlých vrstev se musí řídit dohodnutými pravidly
	+ Pravidla této vzájemné komunikace definuje tzv. protokol
	+ Protokol definuje:
	+ co si komunikující strany posílají, význam, kódování, formát
	+ jak komunikace probíhá, jak mají strany reagovat na různé situace
	+ Představa, že si stejnolehlé vrstvy skutečně mezi sebou předávají data (pakety, rámce) přímo je pouze iluzí
	+ Ve skutečnosti je předávají nižší vrstvě s požadavkem na doručení druhé straně.
	+ Při předávání (bezprostředně) nižší vrstvě k doručení pokračuje až k nejnižší vrstvě (fyzické)
	+ Pouze tato nejnižší vrstva skutečně přenáší nějaká data (po jednotlivých bitech)
* **Vertikální komunikace:**
	+ Vertikální komunikace má charakter poskytování služeb (vrstva poskytuje své služby bezprostředně vyšší vrstvě)
	+ Vyšší vrstva využívá služeb poskytovaných nížší vrstvou.
	+ Př: Fyzická vrstva přenáší jednotlivé bity, vyšší vrstva (linková) využívá přenosu jednotlivých bitů k tomu, aby přenášela celé bloky dat

**Síťový model**

* Síťový model je ucelená představa o tom, jak mají být sítě řešeny (zahrnuje představu o počtu vrstev, o tom co má která vrstva na starosti; nezahrnuje jak má která vrstva úkoly plnit - nezahrnuje síťový protokol).
* Příklad síťového modelu je model ISO/OSI

**Síťová architektura**

* Obsahuje navíc konkrétní protokoly.
* Příkladem je rodina protokolů TCP/IP.

**ISO/OSI**

* Byl pokusem o vytvoření univerzální síťové architektury - skončil jako síťový model, tzn. bez protokolů
* Referenční model ISO/OSI vypracovala organizace ISO (Mezinárodní organizace pro normalizaci) jako hlavní část snahy o standardizaci počítačových sítí nazvané OSI
* V roce 1984 ho ISO přijala jako mezinárodní normu ISO 7498. Kompletní text normy přijala také CCITT jako doporučení X.200
* Referenční model ISO/OSI se používá jako názorný příklad řešení komunikace v počítačových sítích pomocí vrstevnatého modelu, kde jsou jednotlivé vrstvy nezávislé a snadno nahraditelné
* Autoři ISO/OSI se dlouho přeli o počtu vrstev, nakonec zvítězil návrh se 7 vrstvami.



Obrázek - ISO/OSI vrstvy - Zdola nahoru!

**Fyzická vrstva: přenos dat (jednotlivé bity), signály, fyzické parametry a spoje**

* Zabývá se výhradně přenosem bitů a v rámci tohoto přenosu otázkami:
	+ Kódování
	+ Modulace
	+ Časování
	+ Synchronizace
	+ El. Parametry signálů
	+ Konektory
	+ …
* Nabízí služby typu: přijmi bit, odešli bit
* Jednotlivým přenášeným bitům nepřisuzuje žádný význam (neprovádí interpretaci)
* Na úrovni fyzické vrstvy rozlišujeme: paralelní a sériový přenos; synchronní x asynchronní x arytmický přenos; přenos v základním, přeloženém pásmu
* Pro přenos mohou být použita drátová x bezdrátová média
* Na úrovni fyzické vrstvy pracujeme s pojmy jako je šířka pásma a přenosová rychlost
* Synchronní:
	+ Po odeslání zprávy systém čeká na odpověď a nic nedělá
	+ Okamžiky přenosu jednotlivých bitů stejně vzdáleny
* Asynchronní:
	+ Po odeslání dat dále něco vykonává (např. odesílá dále)
	+ Okamžiky přenosu nejsou stejně vzdálené
* Arytmicky:
	+ Přenos znaků asynchronní, ale bity ve znacích synchronní

|  |  |  |  |
| --- | --- | --- | --- |
| Fyzická | Bits (bity) | Fyzické parametry linky – média (kabely, rádio, světlo), signály a binární přenos. Řeší fyzické poslání dat (přenášeným bitům nepřiřazuje žádný význam).; | 100BaseT(ethernet), RS-232(sériový přenos),802.11g (wi-fi) |

**Linková vrstva: rámce(bloky dat), jejich sestavení, řeší přístup ke sdílenému médiu**

* Přenáší celé bloky dat tzv. rámce, využívá k tomu služeb fyzické vrstvy
* Může fungovat buď spolehlivě x nespolehlivě; spojovaně x nespojovaně
* Může využívat různé přenosové technologie
* Úkoly:
	+ Synchronizace na úrovni rámců (rozpoznání začátků, konců, jednotlivých částí)
	+ Zajištění spolehlivosti (detekce chyb a náprava)
	+ Řízení toku (aby vysílající nezahltil příjemce)
	+ Formátuje fyzické rámce, opatřuje je fyzickou adresou (MAC)
	+ Přístup ke sdílenému médiu (řeší konflikty) – tento úkol nebyl původně implementován – z toho důvodu se později rozpadla na dvě podvrstvy (LLC a MAC)
* Spolehlivý:
	+ V případě chyby o tom dostane odesílatel zprávu
* MAC vrstva:
	+ Fyzické adresování
	+ Zajišťuje přístup ke sdílenému médiu
* LLC vrstva:
	+ Zajišťuje multiplexaci protokolů vysílaných na MAC vrstvu (vysílání) a demultiplexaci (příjem)
	+ Realizuje řízení toku a zabezpečení proti chybám
	+ Přenos fyzických rámců na konkrétní médium

|  |  |  |  |
| --- | --- | --- | --- |
| Linková | Frames (rámce) | Fyzická adresace, MAC – media access control a LLC – logical link control, datový tok, synchronizace rámců, komunikace 1 hop, používá MAC adresy. Detekce chyb, řízení toku a přístupu na médium. Komunikace mezi dvěma zařízeními v jednom subnetu (nebo na bránu) pomocí MAC adresy. Vytváří rámce (hlavička + data + zápatí). | Ethernet, FDDI, Token Ring, PPP, SLIP |

**Síťová vrstva: hledá vhodnou cestu, provádí směrování**

* Hlavním úkolem síťové vrstvy je tzv. směrování, neboli nalezení vhodné cesty vedoucí od odesílatele dat až k jejich koncovému příjemci.
* V praxi nemusí být každá dvojice odesílatel/příjemce vždy sousední v tom smyslu, že by mezi nimi existovalo přímé spojení (tj. v „dosahu“ linkové vrstvy).
* Častěji je spíše případ, kdy mezi odesílatelem a koncovým příjemcem vede cesta pouze přes několik jiných uzlů (přestupních, mezilehlých uzlů).
* V takovém případě je ale nutné najít potřebnou cestu přes mezilehlé uzly (právě v tom spočívá směrování, anglicky „routing“) a potřebný přenos přes mezilehlé uzly fakticky realizovat.
* Také síťová vrstva přenáší data po blocích, kterým se říká pakety (anglicky „packets“), zatímco na úrovni linkové vrstvy se jim říká rámce.
* Představa fungování je taková, že síťová vrstva v určitém uzlu rozhodne o dalším směru, kterým by měl být konkrétní paket přenesen k některému ze sousedních uzlů.
* Poté jej předá své linkové vrstvě, která paket vloží do svého rámce a přenese k příslušnému sousednímu uzlu.
* Zde jej partnerská linková vrstva vybalí a předá datový paket své bezprostředně vyšší síťové vrstvě. Ta rozhodne, kterým směrem by měl být paket dále odeslán… a to vše se opakuje, dokud datový paket nedorazí ke svému konečnému cíli (viz. Obrázek)
* Tato vrstva tedy zajišťuje doručení paketů až ke konečnému adresátovi (hledá vhodnou cestu až k cíli – provádí směrování)
	+ Toto může obnášet „přeskoky“ přes různé mezilehlé úhly (linková vrstva se stará o doručování k přímým sousedům, nestará se o přeskoky)
	+ Přeskok vyžaduje
		- ROUTING (směrování) – rozhodnutí o dalším směu
		- FORWARDING – faktické vykonání přeskoku

|  |  |  |  |
| --- | --- | --- | --- |
| Síťová | Packets (pakety) | Logická adresace – routování – určení cesty paketu, přenos dat z bodu do bodu, používá IP adresy. Komunikace mezi zdrojovým a cílovým zařízením pomocí IP adresy. | IP, ICMP, ARP, RIP |

**Transportní vrstva:**

* Úkolem transportní vrstvy je přizpůsobení možností tří nejnižších vrstev (síťové, linkové a fyzické) představám vyšších vrstev.
* Konkrétní představy a možnosti se přitom mohou dotýkat různých věcí, ale nejčastěji jde o rozdíly ve spolehlivosti přenosových služeb a v jejich spojovaném či nespojovaném charakteru.
* Spolehlivost se týká toho, co se má stát při výskytu nějaké chyby při přenosu:
	+ O spolehlivou službu se jedná tehdy, že pokud někdo zjistí chybu, je povinen postarat se o nápravu této chyby.
	+ Naopak nespolehlivou službou je takový případ, kdy ten, kdo zjistí určitou chyby, nemá za povinnost ji napravovat (ale může poškozené data jednoduše zahodit a pokračovat dále).
* Logika nespolehlivých služeb je v tom, že mají menší režii a dokáží přenášet data rychleji a pravidelněji, přičemž o případnou nápravu se mohou efektivněji postarat vyšší vrstvy.
* Dalším významným úkolem transportní vrstvy (kromě již naznačeného přizpůsobení) je i rozlišování různých příjemců a odesilatelů v rámci jednotlivých uzlů.
* Až do síťové vrstvy včetně se totiž všechny přenosy týkají jednotlivých uzlů jako celků (a také příslušné adresy identifikují pouze uzly jako celky).
* Teprve transportní vrstva jde dále a rozlišuje jednotlivé příjemce v rámci těchto uzlů.
* Transportní vrstva již rozlišuje konkrétní entity (jednotlivé procesy, úlohy) v rámci každého uzlu – např. čísla portů v TCP/IP.

**Relační vrstva:**

* Původní představa:
	+ Zajišťování vedení relací (navazování, vedení, ukončování relací)
	+ Vedení více relací pomocí jednoho transportního spojení
	+ Přenos jednotlivých částí (dat) v rámci probíhající relace
	+ Synchronizace komunikace
* Realita:
	+ Relační vrstva je nejčastěji kritizovanou vrstvou referenčního modelu ISO/OSI, protože právě ona toho má co nejméně na práci v porovnání s ostatními vrstvami.
	+ Především má podporovat vedení relací.
* Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačnímu vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizace a obnovení spojení, oznamování výjimečných stavů.

**Prezentační vrstva:**

* Funkcí vrstvy je transformovat data do tvaru, které používají aplikace (šifrování, konvertování, komprimace).
* Formát dat (datové struktury) se může lišit na obou komunikujících systémech, navíc dochází k transformaci pro účel přenosu dat nižšímu vrstvami.
* Mezi funkce patří např. převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů apod.
* Vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační.

|  |  |  |  |
| --- | --- | --- | --- |
| Prezentační | Data | Prezentace dat a šifrování. Řeší rozdíly v reprezentaci dat mezi aplikací a síťovým formátem – kóduje data pro přenos. | MIDI, MPEG |

* Až do úrovně prezentační vrstvy se všechny nižší vrstvy úzkostlivě snaží, aby přenesly data přesně v takové podobě, v jaké byly odeslány, tedy bit po bitu.
* Někdy ale jeden a tentýž řetězec bitů může mít pro různé uzly různý význam (například když každý z nich používá jiný způsob kódování znaků, je nutné provést potřebnou konverzi).
* A právě to je úkolem prezentační vrstvy. Obecně jde o to, aby přenesená data měla pro příjemce stejný význam, jaký měla pro odesílatele.

**Aplikační vrstva:**

* Původní představa:
	+ Bude obsahovat aplikace
	+ Problémem bylo, že aplikací je moc a musely by být všechny standardizovány
* Později:
	+ Aplikační vrstva bude obsahovat pouze „jádro“ aplikací, které má smysl standardizovat (například přenosové mechanismy elektronické pošty)
* Účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci.

|  |  |  |  |
| --- | --- | --- | --- |
| Aplikační | Data | Síťové procesy pro aplikaci, ověření uživatelů, vše závislé na aplikační vrstvě. | Telnet, FTP |

* Dále sem spadají např. protokoly DNS, DHCP, POP3

**TCP/IP**

Architektura TCP/IP

* TCP/IP je síťovou architekturou protože zahrnuje představu o vrstvách a také o konkrétních protokolech(>100)
	+ Dále k TCP/IP patří také:
		- Standardizační proces (technická řešení se stávají standardy)
		- Správa jmenného prostoru (koncept DNS, správa domén nejvyšší úrovně)
		- Správa adresního prostoru (IPv4, IPv6, přidělování IP)
		- Koordinace číselných parametrů (portů)
* Nejprve vznikaly protokoly, až potom vrstvy
* Vznik v akademickém prostředí
* Prosadilo se i v komerčním prostředí
* Od vzniku se změnilo jen velmi málo
* Nejpoužívanější síťová technologie

Historie TCP/IP

* Souvisí s ARPANETem – po výstavbě první velké sítě (ARPAnetu bylo potřeba ověřit životaschopnost paketové technologie)
* Pro zárodečnou síť byl vytvořen protokol NCP (network control program); nebyl však vhodný pro rutinní používání
* DoD se po otestování paketové technologie rozhodl síť nezrušit, ale předat ji akademické sféře pro rutinní používání
* Na původní ARPAnet se nabalovaly další sítě – vznik Internetu; bylo však potřeba vyvinout nové prokoly
* Protokoly TCP/IP byly vyvíjeny jako definitivní řešení pro vznikající Internet
* Specifikace protokolů jsou volně dostupné (financováno DoD z daní)
* 1.1.1983 přechází celý Internet na protokoly TCP/IP
* 1983 – 1986 nástup protokolů do praxe (protokoly TCP/IP jsou postupně implementovány do různých operačních systémů)
* Původní požadavky na ARPAnet:
	+ Žádná centrální část (decentralizovaný charakter – provideři)
	+ Musí být robustní (funkční i při ztrátě části sítě – preferují se nespolehlivé a nespojované přenosy)
	+ Propojení jednotlivých menších sítí
* Nebylo požadováno:
	+ Zabezpečení
	+ Mobilita
	+ Různá kvalita služeb

Filosofie TCP/IP

* Preference nespojovaného způsobu přenosu (lépe se vyrovnává s výpadky a změnami topologie)
* Preference nespolehlivého přenosu (ne každá aplikace/služba potřebuje spolehlivost – multimédia; věc koncových uzlů)
* Preference principu best effort:
	+ Best Effort – Nelze zajistit individuální kvalitu přenosu, všem je měřeno stejně. Přenos není garantovaný, vyhovuje se všem požadavkům dokud stačí zdroje, pak se omezují všichni stejně.
	+ Quality of Service: Přenosům se nabízí různá kvalita přenosu. S garancí – rezervace zdrojů, bez garance – formou prioritizace
* Dodnes se jeví jako správné 1,2; -> 3 nevyhovuje multimédiím.

TCP/IP x ISO/OSI

* TCP/IP pouze 4 vrstvy.. vrstva síťového rozhraní, síťová vrstva, transportní vrstva, aplikační vrstva

**Filosofie TCP/IP**

Vrstva síťového rozhraní

* Nevymýšlet znovu to, co již bylo vymyšleno:
	+ Pokud již existuje nějaká přenosová technologie (na úrovni fyzické a linkové vrstvy), pak ji rovnou použijeme – např. Ethernet
	+ Soustředíme se na to, jak ji využít co nejlépe (jak nejlépe balit IP pakety do Ethernetových rámců)
* Důsledek:
	+ TCP/IP nepokrývá linkovou ani fyzickou vrstvu v tom smyslu, že by definoval vlastní protokoly pro tyto vrstvy
	+ TCP/IP nerozlišuje mezi linkovou a fyzickou vrstvou, místo toho je sdružuje do jediné – vrstvy síťového rozhraní-

**Filosofie TCP/IP**
-        Nevymýšlet znovu něco, co již bylo vymyšleno
-        Nedefinuje linkovou a fyzickou vrstvu, místo toho je sdružuje do jediné
-        Nevnucovat někomu něco, co nutně nepotřebuje
-        Důsledkem je absence aplikační a prezentační vrstvy u TCP/IP
-        Má pouze 4 vrstvy, z nichž jednu vůbec nedefinuje (vrstva síťového rozhraní)
-        Role vrstev je v podstatě stejná jako v ISO/OSI, liší se ale představa o tom, jak by daná vrstva měla svou roli plnit
-        Název TCP/IP vychází z toho, že původně měl mít ještě méně vrstev
Aplikační vrstva – aplikační protokoly: SMTP, http, FTP, SIP, Telnet, NFS, …
Transportní vrstva – alternativně: protokol TCP (spolehlivý, spojovaný) nebo protokol UDP (jako IP: nespolehlivý, nespojovaný)
Síťová vrstva – protokol IP
Vrstva síťového rozhraní – TCP/IP sám „nezabydluje“, ale využívá zde řešení, vzniklá jinde, výjimkou jsou protokoly SLIP a PPP
SLIP – protokol pro sér. Přenos dat mezi 2 uzly po samostatném vedení
PPP – vylepšení protokolu SLIP

**Vrstva síťového rozhraní**
-        Umožňuje přístup k fyzickému přenosovému médiu
-        Podrobněji není v rámci TCP/IP architektury specifikována
-        Může být implementována na jakémkoliv typu sítě z hlediska používané technologie
**Síťová vrstva**
-        Všechny přenosové technologie zastřešuje
-        Zastřešujícím elementem je protokol IP

**Síťová vrstva – protokol IP**

* IP protokol podporuje komunikace mezi síťovými uzly
* Protokol IP má všude stejné vlastnosti a všude poskytuje stejné služby
* Je nespojovaný (pakety, neznáme cestu) a nespolehlivý (rychlý, ale nemáme jistotu, zda data dojdou)
* Provádí také fragmentaci a defragmentaci datagramu
* Protokol IP funguje nad „čímkoliv“, nad jakýmkoliv přenosovým mechanismem
* Protokolům vyšších vrstev vytváří jednotné prostředí pro jejich fungování

**Transportní vrstva**

* Zajišťuje transportní službu pro předání dat mezi koncovými uživatelskými procesy
* Využívá nespojovaný (neznáme dopředu cestu) a nespolehlivý (nemáme jistotu, že data dojdou) přenos, ale alternativně využívá spojovaný a spolehlivý přenos
* Aplikace si sami vybírají dle svých potřeb:
* Protokol UDP – zajišťuje nespojovaný a nespolehlivý přenos
* Protokol TCP – zajišťuje spojovaný a spolehlivý přenos

Chybí prezentační a relační vrstva proto, že služby budou potřebovat jen některé aplikace a pak nemá smysl dělat tyto dvě samostatné vrstvy.

* Aplikace, které tyto služby potřebují, si je musí realizovat samostatně.

**Aplikační vrstva**

* Představují ji aplikace, které využívají přenosu dat po síti ke konkrétním službám pro uživatele
* Příklady: Telnet, FTP, http, DHCP, DNS
* Jednotlivé aplikace odlišeny číslem portu
* Pro aplikace využívající mult. Charakter není best effort vhodné
* Prakticky všechny tradiční aplikace v rámci TCP/IP založeny na architektuře klient-server (uzpůsobeny komunikaci 1:1 – 1 server a 1 klient) 🡪 není vhodné pro multimédia
* Tyto aplikace potřebují dopravovat stejná data od 1 zdroje více příjemcům 🡪 přenosové mechanismy TCP/IP však toto neumí
* Toto řeší protokol IPv6

**Aplikace v TCP/IP - QoS**

* Prioritizace
* Rezervace – multimediálním aplikacím vyhradíme větší přenosovou kapacitu

**Bezpečnost**

* Přenosové mechanismy neposkytují žádné zabezpečení
* Pokud nějaká aplikace potřebuje určité zabezpečení, musí si ho zajistit sama

**Standardizace**

* Standarty jsou otevřené (nejsou v rukou jediné firmy, jsou přijímány na základě všeobecného souhlasu, jsou zdarma)

**Protokoly TCP/IP**

* ICMP - používá se pro výměnu stavových a chybových informací
* ARP - slouží pro zjištění fyz. adresy (MAC adresy) zařízení na základě jeho IP adresy
* RARP - Slouží k získání vlastní IP adresy PC při znalosti MAC adresy
* TCP - Protokol garantuje spolehlivé doručování a ve správném pořadí
* Slouží tedy pro řízení komunikace
* UDP -
* TELNET - umožňuje připojení k jinému PC a spravovat ho
* SSL - slouží pro zabezpečenou komunikaci
* DNS - slouží při přiřazování IP adres doménovým jménům
* DHCP - pro automatic. Přidělování IP adres
* FFTP – přenos souborů
* FTP - přenos souborů po síti (např. stahování)
* HTTP - pro výměnu hypertextových dokumentů ve formátu HTML
* POP3 - pro stahování e-mailových zpráv ve vzdál. Serveru na klienta
* SMTP - odesílání a doručení pošty
* IMAP - vzdálený přístup k e-mailové schránce

**PASIVNÍ SÍŤOVÉ PRVKY**

* Všechno, co přenáší data, ale nijak je neovlivňuje

**Pasivní**

* + Kabely
	+ Konektory
	+ Rozvaděče
	+ Spojky
	+ Zásuvky

**Kabely**

Parametry, které nás budou zajímat:

* + Přenosová rychlost – jedná se o rychlost přenosu dat, uvádí se v Mb/s
	+ Útlum – říká, jaká je míra zeslabení signálu při jeho průchodu kabelem, uvádí se v dB (decibely)
	+ Odolnost vůči elektromagnetickému rušení
	+ Impedance – zdánlivý odpor, který kabel představuje pro připojené zařízení, impedance kabelu i zařízení mají být shodné, uvádí se v ohmech
	+ Přeslech – vzájemné ovlivnění více vodičů mezi sebou, mění se obvykle pro každou dvojici vodičů a udává se v dB
* Koaxiální kabel je nejstarším typem používaným v počítačových sítích, měl velký vliv na rozvoj počítačových sítí (LAN).
* Koaxiální kabel je asymetrický elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým vodičem vnitřním.
* Vnější vodič nazýváme často stíněním a vnitřní vodič jádrem.
* Vnější a vnitřní vodič jsou odděleny nevodivou vrstvou (dielektrikum).
* Vnitřní vodič (také střední vodič, jádro) – bývá zhotoven z mědi, má podobu plného drátu nebo lanka spleteného z více drátků
* Vnější vodič (také stínění) – bývá zhotoven z hliníkové nebo měděné fólie nebo je tvořen jako opletení dielektrika měděnými vlákny, případně kombinace obojího. Hlavní efekt vodivého opletení spočívá především v odstínění vnitřního vodiče od vlivu vnějšího rušení – koaxiální kabely jsou proto vůči rušení dosti odolné.
* Dielektrikum – je izolační vrstva vložená mezi vnitřní a vnější vodič. Velkou měrou ovlivňuje vysokofrekvenční vlastnosti koaxiálního kabelu. Bývá zhotoveno obvykle z polyethylenu , vzduchu, ale i jiných izolačních materiálů.
* Kvůli velké vlnové impedanci je rychlost šíření signálu koaxiálním kabelem cca dvoutřetinová proti kroucené dvojlince, což byl mj. také důvod, proč se pro rychlé lokální sítě už s koaxiálním nepočítalo.
* Další nevýhodou je špatná práce s konektory i samotnými kabely.
* Přeslechy jsou díky stínění velmi nízké. Dle provedení přenáší signály (analogové) až do 6000 MHz!
* Útlum koaxiálního kabelu je asi od 3 dB/km a je značně závislý na frekvenci.
* Koaxiální kabel se používá pro digitální přenos obvykle na krátké vzdálenosti do rychlostí 500 Mbit/s, pro analogový přenos (kabelové televize, antény) do několika Gbit/s.
* Zpočátku se používal tzv. tlustý koaxiální kabel (průměr 10 mm), který měl velmi dobré elektrické vlastnosti, ale byl málo ohebný a připojení stanic k tomuto kabelu bylo technicky náročné.
* Proto byl nahrazen tenkým koaxiálním kabelem, jehož elektrické vlastnosti jsou o něco horší, ale realizace sítě je jednodušší.
* U tenkého koaxiálního kabelu se pro připojení k počítači se používá BNC konektor, tenký koaxiální kabel je s počítači připojen T-konektorem, na konci sběrnice pak musí být zakončovací odpor (obvykle 50 ohmů) kvůli zabránění odrazům signálu na volném konci.
* Existují různé typy koaxiálních kabelů – nejrozšířenější jsou ethernetové s impedancí 50 ohmů.
* Nejčastěji se používá pro zapojení PC do sběrnicové topologie, rychlost dat je 10 Mb/s.
* V PC sítích jsou tyto kabely již na ústupu, ale používají se dále v jiných oblastech (v rozvodech kabelových TV jsou jen 75-80 ohmů).
*