BPC-KOM

Komunikační technologie

Otázky ke státnicím

Bakalářský obor Informační bezpečnost, FEKT VUT

https://github.com/VUT-FEKT-IBE/BPC-IBE-SZZ

Text: dikubi, kámen u cesty, jedla
Korektura: kámen u cesty, czechbol

20. května 2023

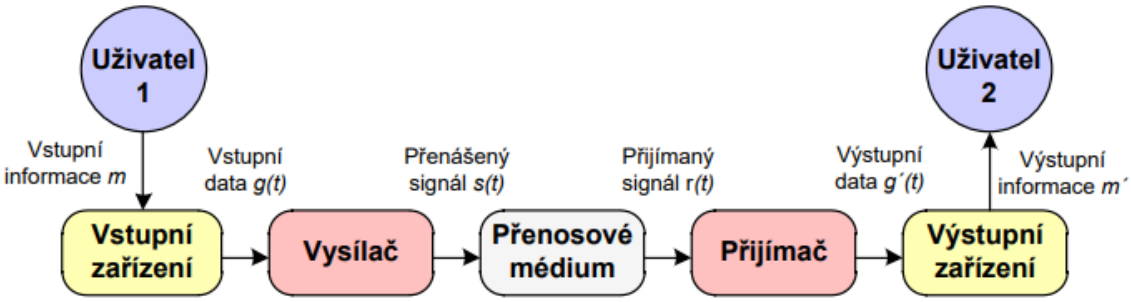
Obsah

1 Technika sítí a protokolů - komunikační modely, způsob přenosu informace, základní struktura sítí, typy sítí, architektura komunikace systémů.

1.1 Komunikační modely

Komunikaci mezi dvěma stranami lze rozlišit na dva typy: **komunikaci uvnitř sítí** a **komunikaci mezi koncovými uživateli** (nad sítěmi).

Data jsou reprezentace faktů, pojmů nebo instrukcí ve formální podobě vhodná pro komunikaci a interpretaci pro strojové zpracování. **Informace** je význam dat, důležitý typicky pro uživatele.



Obrázek 1: Zjednodušené blokové schéma datovké komunikace.
Informace m je pomocí vstupního zařízení reprentována jako data $g(t)$ ve formě proměnlivého časového signálu, který musí být přeložen do podoby vhodné pro přenosové médium, tj. do signálu $s(t)$, vysílačem. Na druhé straně se objeví jako signál $r(t)$, který se od odeslaného může odlišovat (šum, rušení). Je konvertován zpět do tvaru výstupních dat $g'(t)$ a výstupnímu zařízení jsou předána data m'.

Pomocí komunikačních sítí spolu komunikují koncoví uživatelé, v případě počítačů partnerské procesy na komunikujících počítačích. Základním předpokladem pro komunikaci uživatelů je definice rozhraní mezi uživatelem a sítí; musí konkretizovat strukturu a formát předávaných uživatelských a řídících dat.

Obrázek 2: Zjednodušené blokové schéma komunikace mezi procesy pracujícími na samostatných počítačích propojených obecnou sítí.

Základní úkoly pro přenos informace spočívají ve vlastním **přenosu** informace (kódování dat a jejich přizpůsobení pro telekomunikační kanál), vyhledání cesty spojení dvou uživatelů v síti (**směrování**) a použití vhodného způsobu komunikace a řízení (**protokoly**).

Komunikační řetězec zejména stará o **řízení výměny** informací (způsob organizace přenosu dat mezi zdrojem a cílem), **definice rozhraní** (včetně tvaru a velikosti signálu), **synchronizaci** (časové sjednocení), **formátování zpráv** (unifikace způsobu sestavení obsahu zprávy) a **adresování a směrování** (jednoznačný způsob určení cíle a nalezení cesty k němu).

Zpravidla umožňuje vícenásobné využití přenosových systémů (sdílení více uživateli/-procesy), **řízení systému** (konfigurace, dohled, reakce na chyby a přetížení), **detekci a korelaci chyb**, **zotavení** se ze ztrát v komunikačním systému, **řízení přenosu** (aby nedocházelo k zahlcení systému nadměrným množstvím dat) a ochranu zpráv (zaslaná data může přijímat pouze příjemce).

1.2 Přenos informace

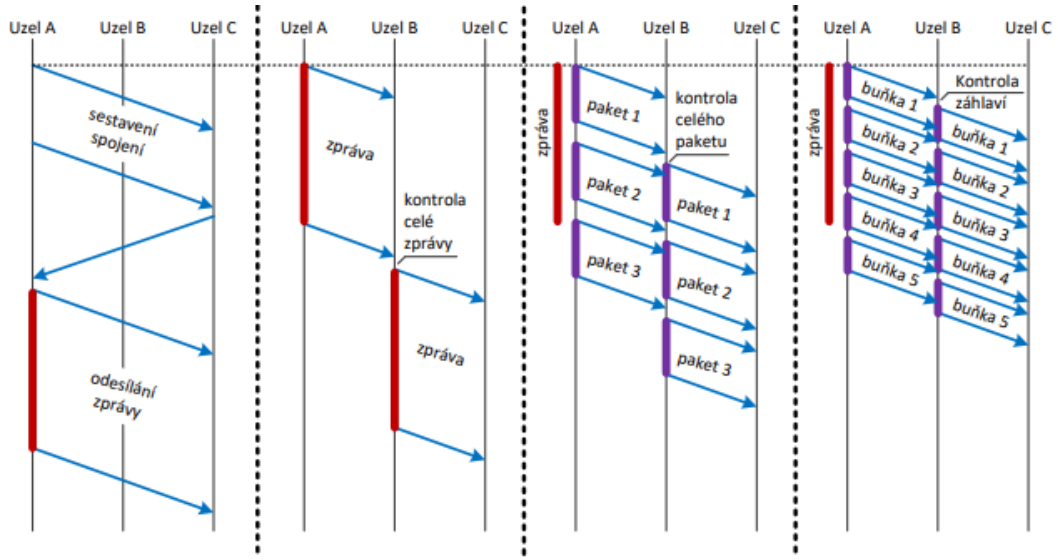
Při přenosu hovoru jsou mezi částmi přenášenené informace malé mezery, jde o přenos citlivý na zpoždění a má vysokou nadbytečnost. Přenos dat na počítači je naopak převážně dávkový, velmi spolehlivý a existence spojení není až tak kritická.

Komutace okruhů (Circuit Switching) Mezi koncovými účastníky je vytvořena dočasná přenosová cesta jako fyzické spojení (včetně spojovacích uzlů). Spojení je nutné sestavovat před vlastním přenosem informace, je potřeba rezervovat prostředky a kapacity pro následný přenos. Z hlediska nákladů jde o drahé spojení: cesta je vytížená i když k přenosu informace dochází pouze část alokované doby. Využívaná dříve pro přenos telefonních hovorů.

Komutace zpráv (Message Switching) Zdroj informace vyšle zprávu do prvního uzlu, kde se uloží, zkontroluje a pošle k dalšímu uzlu směrem k příjemci dat. Tento způsob klade velké nároky na mezilehlé uzly (musí být schopny zprávy uchovat v paměti; *store-and-forward*). Vždy je zatěžována pouze ta část sítě po které se zpráva přenáší.

Komutace paketů (Packet Switching) Zpráva je rozdělena na bloky dat (pakety) o definované maximální délce, sítí jsou přenášeny stejně jako zprávy. Pořadí doručení paketů nemusí být dodrženo, tato metoda vyžaduje dodatečné prostředky pro zajištění správnosti přenesení celé zprávy (pouhé protichybové zabezpečení již nestačí). Jde o nejčastější způsob přenosu.

Komutace buněk (Cell Switching) Zpráva je rozdělena na jednotky s přesně danou délkou. Při přenosu se provádí pouze kontrole záhlaví buňky/rámce a proto dochází jen k velmi malému zdržení v uzlu. Veškeré kontroly přenesených dat jsou prováděny u koncového uživatele. Využívá se u přenosu řeči i u klasických dat (ATM technologie[1]). Dochází k velké úspoře prostředků sítě, protože je blokována pouze nezbytná kapacita, a k urychlení odezvy, nevýhodou je však zmíněná fixní velikost přenášených jednotek.



a) komutace okruhů b) komutace zpráv c) komutace paketů d) komutace buněk

Obr. 3-3: Časové posloupnosti jednotlivých metod přenosu informace

1.3 Struktura sítí

Spoje jsou komponenty umožňující přenos zpráv mezi dvěma místy bez ohledu na druh prostředků či druh přenosu a propojují přepojovací prvky mezi sebou a s koncovými uzly. Jde o okruhy, kanály nebo linky.

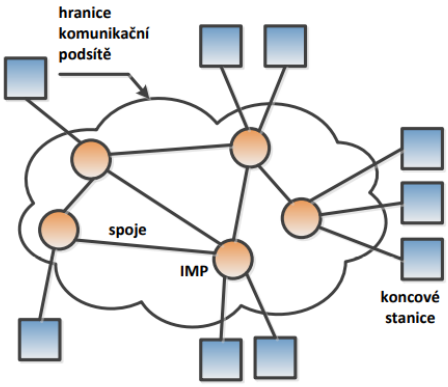
Přepojovací prvky jsou specializované systémy sloužící k propojení dvou a více spojů. Základní úlohou je vybrání správného výstupního spoje po kterém budou data poslána dále. Pro datové přenosy je to IMP (*Interface Message Processor*), předchůdce směrovačů v TCP/IP[2].

1.3.1 Architektura a topologie sítí

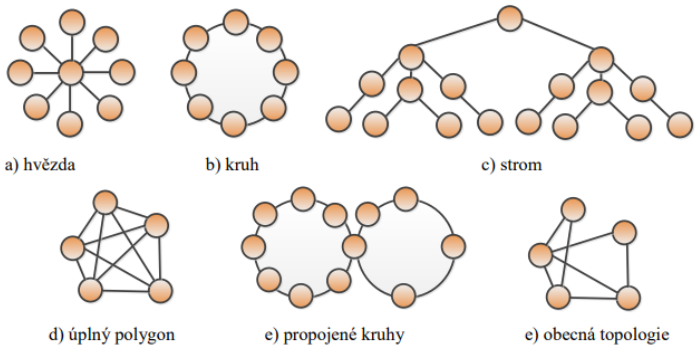
Dvoubodové spoje informace vyměňují nepřímo. Mezi možné struktury patří topolotie typu stromhvězda, kruh, strom, polygon, propojené kruhy nebo může jít o obecnou topologii (neúplný polygon).

[1] Asynchronous Transfer Mode: https://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode.

[2] Pro IMP se také používají názvy datová ústředna (*Data Switching Exchange*), mezilehý systém (*Intermediate System*) nebo uzel přepojování paketů (*Packet Switching Node*).

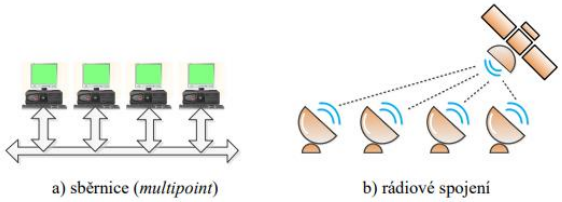


Obr. 3-4: Základní struktura sítě



Obr. 3-5: Topologie sítí založených na dvoubodovém spojení

Multipoint je topologické uspořádání ve kterém může být vytvořeno více kanálů mezi dvěma místy. **Broadcast** je hromadný přenos z jednoho zdroje do mnoha míst. Spadají sem převážně bezdrátové sítě: systémy mají jeden kanál který je využívaný všemi uživateli. Vyslaná data jsou přijmuta všemi, reaguje na ně obvykle pouze ten komu byla zaslána. Systémy se všesměrovým vysíláním také umožňují adresovat skupinu nebo všechny stroje pomocí speciálních adres (multicast).



Obr. 3-6: Topologie sítí založených na všesměrovém vysílání

1.4 Typy sítí

Nejčastěji se sítě dělí dle velikosti, dosahu nebo rozlohy. Některá řešení je obtížné zařadit do jedné konkrétní kategorie.

Personal Area Network (PAN) Využívá se pouze jednou osobu (příp. velmi nízkým počtem osob), zpravidla nízkými přenosovými rychlostmi (Mbps), často bezdrátově (Bluetooth, IrDA[3], ale i USB). Chytré telefony, PDA, tablety, scannery, tiskárny.

Local Area Network (LAN) Přenos informací v prostorově omezeném měřítku (budova až jednotky kilometrů). Obvykle v provedení hvězda nebo strom. Rychlosti 100 Mbps až 10 Gbps. Uzlů bývají desítky až stovky. Doba zpoždění přenosu se pohybuje od 10 µs do 1 ms. Domácnosti, firmy, budovy ve vlastnictví jedné osoby nebo organizace.

Metropolitan Area Network (MAN) Propojení LAN sítí s WAN sítěmi. Rozsah měst až národních sítí. Rychlosti v řádu Gbps a vyšších. Optické technologie, Ethernet v optických vláknech, dříve také ATM či FDDI[4]. MAN sítě jsou spravovány jednou organizací a její prostředky jsou využívány více subjekty. Zpoždění přenosu se pohybuje od 100 µs do 10 ms.

Wide Area Network (WAN) Globální sítě pokrývající stovky až tisíce kilometrů na úrovni států či kontinentů. Jejich hlavní úlohou je propojení geogreficky rozprostřených LAN a MAN sítí. Jedna WAN může být vystavena na více technologiích a její části mohou být vlastněny různými subjekty. Přepínání pektů, buněk i okruhů; technologie POS[5], MPLS[6], ATM či Frame Relay. Využívají se převážně optické technologie. Zpoždění bývá vhledem k velkým vzdálenostem vyšší (navzdory přenosu rychlostí světla), řádově jednotky až stovky ms. Nejpoužívanější WAN sítí je Internet.

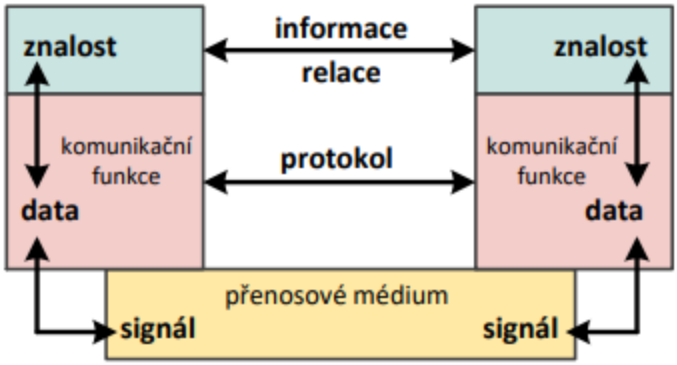
1.5 Architektura komunikace systémů

Přenos mezi stranami vždy probíhá dle dohodnutých pravidel (**protokolu**).

Vertikální komunikace probíhá od nejvyšší úrovně k nejnižší a naopak. Pro obě strany je transparentní, probíhá ale přes všechny úrovně systému.

Horizontální komunikace probíhá na odpovídajících úrovních domluveným protokolem, a s výjimkou fyzické vrstvy je pouze virtuální. Každá vrstva musí umět předat data nižší vrstvě a také od ní data převzít a „očistit“ je pro předání výše.

[3]IrDA: Infrared Data Association
[4]FDDI: Fiber Distributed Data Interface.
[5]POS: Packet over SONET/SDH (Synchronous Optical Network/Synchronous Digital Hierarchy).
[6]MPLS: Multiprotocol Label Switching



Obr. 3-7: Základní model komunikace – principiální schéma

2 Základní popis referenčního modelu ISO/OSI a srovnání s TCP/IP.

Na počátku mezipočítačové komunikace vznikaly různé vzájemně nekompatibilní systémy a uzavřené architektury. Postupem času rostl tlak na vznik otevřeného standardu, který byl standartizován jako ISO/OSI RM[7], který podchycuje všechny nezbytné aspekty komunikace. Stal se výchozím modelem pro počítačově řízenou výměnu dat a položil teoretický a vědecký základ pro realizaci datových sítí.

Zařízení vykonávající zpracování a přenos informace jsou označovány jako **reálné systémy**, prvky zpracovávající informace jsou **aplikační procesy**.

ISO/OSI RM nespecifikuje přesnou podobu sítě, ale uvádí všeobecné principy sedmivrstvé síťové architektury. Jsou to:

1. fyzická (*physical*) vrstva,
2. spojová (*data link*) vrstva,
3. síťová (*network*) vrstva,
4. transportní (*transport*) vrstva,
5. relační (*session*) vrstva,
6. prezentační (*presentation*) vrstva,
7. aplikační (*application*) vrstva.

Nejnižší dvě vrstvy bývají **hardwarové**, ostatní bývají implementovány **softwarově**.

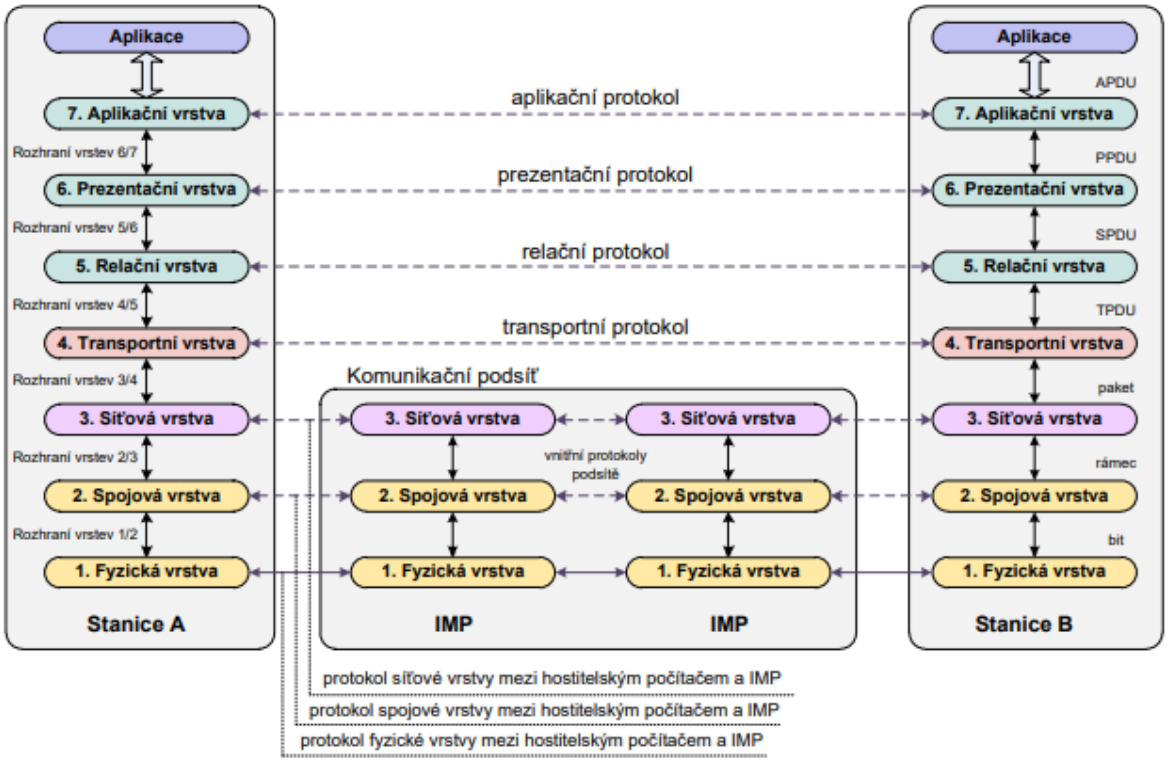
První čtyři vrstvy lze označit jako **poskytovatele** transportní služby, třetí až sedmou jako jejího **uživatele**.

První tři vrstvy jsou **lokální**, protože zajišťují komunikaci na lokální síťové infrastruktuře, čtyři vrchní jsou **koncové** a umožňují propojení komunikujících aplikací.

Datové jednotky se označují jako PDU (*Protocol Data Unit*) a každá vrstva má své označení: TPDU (*Transport PDU*), SPDU (*Session PDU*), PPDU (*Presentation PDU*), APDU (*Application PDU*)).

Partnerská komunikace vrstev je pouze iluze, data prochází všemi nižšími vrstvami. V mezilehém prvku dochází k průchodu do síťové vrstvy, kde je rozhodnuto o dalším směrování a následně data „sestoupí“ k fyzické vrstvě.

[7]International Organization for Standartization Open System Interconnection Reference Model.



Obr. 3-12: Architektura sítě založené na modelu ISO/OSI

Sestupem do nižší vrstvy se zvyšuje datová jednotka o záhlaví jednotlivých vrstev (tzv. **zapouzdřování**). V cílovém systému se v jednotlivých vrstvách zprávy rozbalují.

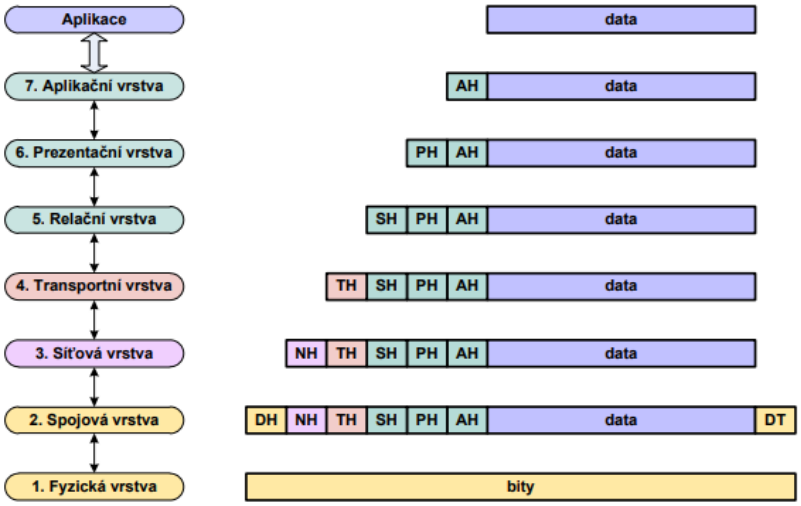
2.1 Vrstvy modelu ISO/OSI

Aplikační procesy rozptýlené po síti mezi sebou komunikují. Logické prostředí sítě je pro uživatele transparentní.

Fyzická vrstva Jde o prostý tok bitů přenosovým médiem (tj. přenos elektrického signálu s měnícími se napěťovými úrovněmi). Úkolem první vrstvy je příprava funkčních, procedurálních, mechanických a elektrických prostředků pro vytvoření, udržení a ukončení datových okruhů mezi prvky sítě. Kvalita je popisována **chybovostí**.

Reprezentace bitů, přenosová rychlost, synchronizace vysílače s přijímačem, přizpůsobení se kanálu a topologii, oboustranný přenos.

Spojová vrstva Přenášení rámců. Druhá vrstva připravuje prostředky pro vytvoření, udržení a rušení datových spojů mezi dvěma prvky sítě, mezi kterými může být jedno či více spojení, které vznikají a zanikají dynamicky. Krom práce s datovými spoji tato vrstva formátuje rámce, identifikuje koncové body, řadí přenášené rámce, detekuje a opravuje chyby a oznamuje chyby které nezvládá opravit.



Obr. 3-13: Znázornění tvorby PDU v jednotlivých vrstvách

Podvrstva řízení logického spoje (LLC, *Logical Link Control*) poskytuje rozhraní mezi přenosovým prvkem a síťovou vrstvou, podvrstva řízení přístupu k médiu (MAC, *Media Access Control*) poskytuje služby specifické pro daný přenosový prostředek.

Vytváření rámců, adresování v síti, řízení toku dat, řízení chybových stavů.

Síťová vrstva Směrování toku dat organizovaných do paketů. Třetí vrstva poskytuje prostředky pro transportní jednotky. Je zodpovědná za komunikaci na základě logických adres, směrování a přenos datových jednotek (datagram) k přijímači. Zajišťuje hlavně nezávislost transportní vrstvy na směrování a propojování, dále také síťovou adresaci, management síťových spojů, prioritizaci přenosu nebo řazení datagramů.

Může být **se spojením** nebo **bez spojení**. Směrování je vyhledání optimální cesty k cíli. Síťová vrstva také musí mít mechanismus mapování logických adres na fyzické.

Logické adresování, směrování mezi sítěmi.

Transportní vrstva Zvýšení kvality spojů na požadovanou úroveň: vyšší vrstvy nemusí určovat optimální cestu, kontrolovat tok dat nebo řešit problémy s přetížením či chybami. Protokoly čtvrté a vyšší vrstvy pracují v koncových systémech. Koncové body transportního přenosu jsou odlišeny pomocí **portů**. **Kvalita služeb** závisí na přenášených datech.

Adresace konkrétní služby, segmentace a skládání, řízení spojení, toku dat a chybových stavů.

Relační vrstva Informace pro řízení a synchronizaci dialogu. Pátá vrstva organizuje a synchronizuje dialog aplikačních procesů. V rámci jedné relace může vzniknout více transportních spojení, více transportních spojení může reprezentovat jednu relaci.

Řízení dialogu aplikačních protokolů, synchronizace.

Prezentační vrstva Koordinace kódování a syntaxe vyměňovaných dat. Šestá vrstva transformuje data aplikační vrstvy do společného formátu: převod kódů a abeced či uspořádání dat. V ISO/OSI modelu je jedinou vrstvou která může zasahovat do samotných přenášených dat. Data může také komprimovat či šifrovat.

Transformace kódování, šifrování, komprese.

Aplikační vrstva Informačním systémům zpřístupňuje prostředí OSI. Sedmá vrstva se dá nazvat jako síťové rozšíření operačního systému. Zajišťuje přenos zpráv, identifikaci partnerů, zjišťování připravenosti partnera, určení kvality služeb, zajištění synchronizace zpráv, dohodu syntaxe apod.

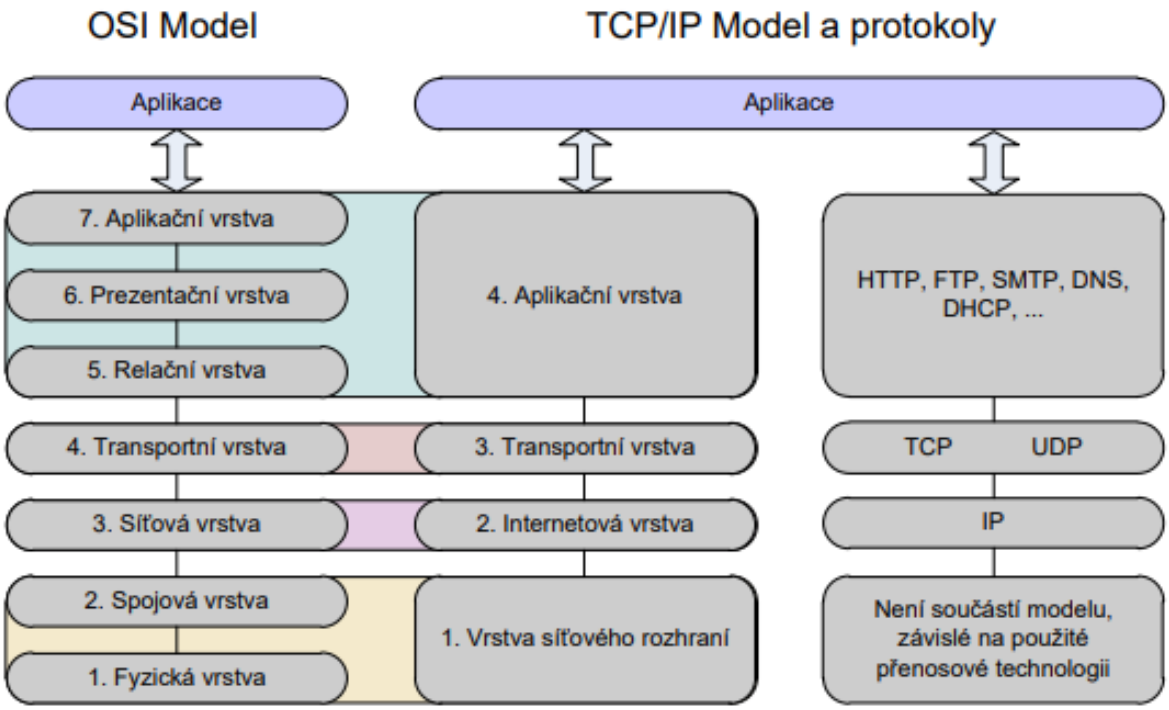
Příklady jsou například přenos souborů, elektronická pošta nebo vzdálený přístup, které jsou dnes využívány pouze nad TCP/IP.

3 Základní popis síťového modelu TCP/IP a srovnání s ISO/OSI.

Navzdory názvu TCP/IP označuje celou sadu protokolů a náhledů na stavění a fungování datových sítí. Na rozdíl od ISO/OSI je praktická pro reálnou implementaci.

Při vytváření RM OSI měly hlavní slovo organizace kladoucí důraz na vlastnosti sítě (na jejich spojovaný a spolehlivý charakter) s tím, že připojované hostitelské počítače nebudou muset provádět tolik práce. Vyšší vrstvy ale nemohly spoléhat na opravy vrstev nižších a spolehlivost si musely zajišťovat samy, a ve výsledku se tím zabývala každá vrstva.

Tvůrci TCP/IP naopak vycházeli z předpokladu, že zajištění spolehlivosti je problémem koncových zákazníků a mělo by být řešeno až na úrovni transportní vrstvy a výše. Komunikační síť nemusí ztrácet část přenosové kapacity kontrolou a opakovaným vysíláním paketů a je tak plně využita vlastními datovými přenosy. V síti může dojít ke ztrátě či zahození paketu bez varování a snahy o nápravu, pakety by však neměly být zahazovány bezdůvodně (naopak by se o doručení měly snažit: *best effort*). **TCP/IP předpokládá jednoduchou a rychlou podsíť ke které se připojují inteligentní počítače**.



Obr. 3-14: Srovnání modelu RM ISO/OSI a TCP/IP

3.1 Vrstvy modelu TCP/IP

Vrstva síťového rozhraní Ovládání konkrétní přenosové cesty mezi dvěma síťovými prvky. Není blíže specifikována protože je závislá na přenosové technologii.

Internetová vrstva Realizace protokolem IP (v4, v6). Funkčně odpovídá síťové vrstvě ISO/OSI modelu a bývá tak i označována. Předává pakety mezi odesílatelem a příjemcem přes mezilehá zařízení (směrovače). Jde o nespojovanou datagramovou službu, která se musí vyrovnávat s odlištnostmi částí cesty (odlišné adresy, různá maximální velikost paketů).

Transportní vrstva Zajištění přenosu mezi dvěma koncovými účastníky (aplikačními programy). Podle nároků reguluje tok dat oběma směry, zajišťuje spolehlivost přenosu a mění nespojovaný charakter internetové vrstvy na spojovaný. Bývá realizována spolehlivým protokolem TCP (*Transmission Control Protocol*), nespolehlivým UDP (*User Datagram Protocol*) nebo i jinými.

Aplikační vrstva Případné prezentační a relační služby (šifrování, komprese) si musí aplikace realizovat samy (a pokud je aplikace nevyžaduje, nevzniká zbytečná režie). Mezi hlavní protokoly patří DNS, DHCP, HTTP, SSH, FTP, ...

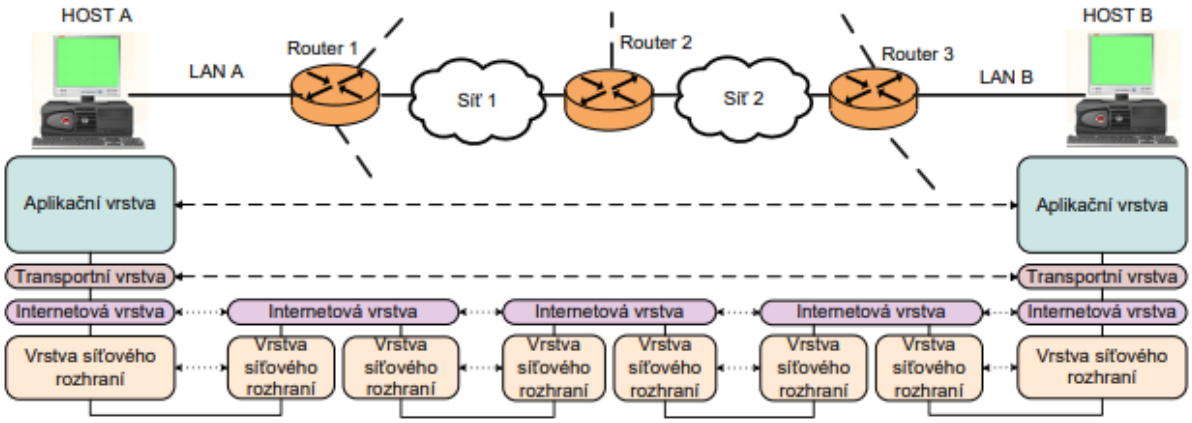
3.2 Propojování sítí

TCP/IP usiluje o co nejuniverzálnější propojení sítí všech typů: od lokálních typu Ethernet přes veřejné datové sítě až po internet. Cílem je umožnit každému uzlu komunikovat s kterýmkoliv jiným uzlem bez ohledu na to, jestli mezi nimi existuje přímé spojení, nebo jsou odděleny několika sítěmi.

Z pohledu uživatele by vnitřní struktura soustavy měla být transparentní a *internetworking* by se jim měl jevit jako jedna velká síť, ke které jsou připojeny jednotlivé počítače (*hosts*). Ve skutečnosti je to ale spousta dílčích sítí vzájemně propojených na úrovni síťové vrstvy pomocí směrovačů (*router*).

Výhodou IP je existence jednotého formátu adres, adresování a dat na úrovni síťové vrstvy.

Každé zařízení má fyzickou adresu spjatou s konkrétním hardware. Pomocí MAC nelze komunikovat mezi různými sítěmi, proto jsou definovány globálně platné IP adresy.



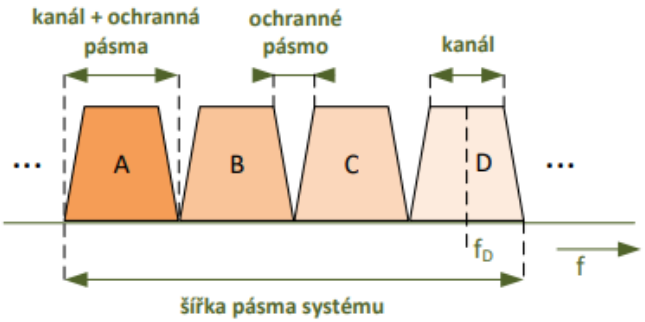
Obr. 3-15: Ukázka propojení sítí v rámci Internetu

4 Principy komunikačních technik – vícenásobné využití cest, zajištění obousměrné komunikace.

Nejlepšího ekonomického zhodnocení přenosových cest se dosáhne jejich vícenásobným využitím. Pro to se využívají techniky multiplexování, kdy je přes jedno médium přenášeno více signálů z více zdrojů do více cílů. Techniky multiplexování se často kombinují.

Prostorové dělení *Space-Division Mutliplex* je např. více paralelních vedení v rámci jednoho kabelu; toto však není pravé multiplexování.

Kmitočtové dělení *Frequency-Division Multiplex* pro různé přenosy využívá různé kmitočty, resp. pásma kmitočtů. Typickým příkladem je FM rádio nebo GSM. Z FDM vychází OFDM (*Orthogonal FDM*), které využívá například xDSL[8]. Kmitočtové dělení může být také použito k odlišení směrů komunikace (jedno pásmo tam, druhé zpět).



Obr. 4-5: Princip kmitočtového dělení do kanálů a ochranných pásem

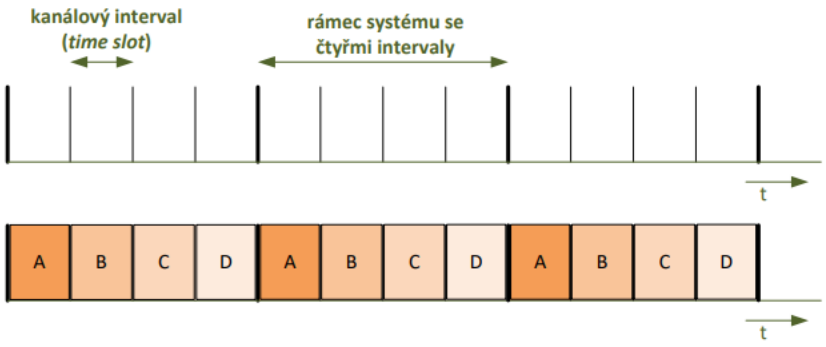
Vlnové dělení *Wavelength-Division Multiplex* se využívá v optice: v jednom optickém vlákně je více signálů odlišených vlnovou délkou (barvou).

Časové dělení *Time-Division Multiplex* se využívá především v digitálním přenosu, kdy se vysílací strany střídají.

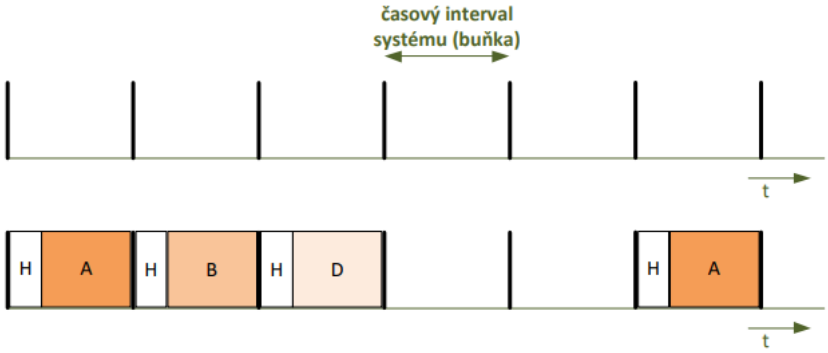
V **synchronním** módu je každému zařízení vyhrazeno $\frac{1}{n}$ celkové kapacity: když stanice nevysílá, blokuje svou alokovanou část a přenos se stává neefektivním, všechny stanice také musí odesílaná data fragmentovat na přesně dané a stejně velké jednotky. V **asynchronním** módu jsou stanoveny časové intervaly s přesně danou velikostí, ale nejsou nikým rezervované a použity jsou pouze v případě potřeby. V **paketovém** módu je možné vysílat různě velké zprávy v libovolném čase. Každá zpráva musí obsahovat záhlaví s identifikátorem vysílací stanice. Systém však nezaručuje žádnou vysílací kapacitu.

Kódové dělení *Code-Division Multiplex* jednotlivé přenosy odlišuje speciální kódovou sekvencí.

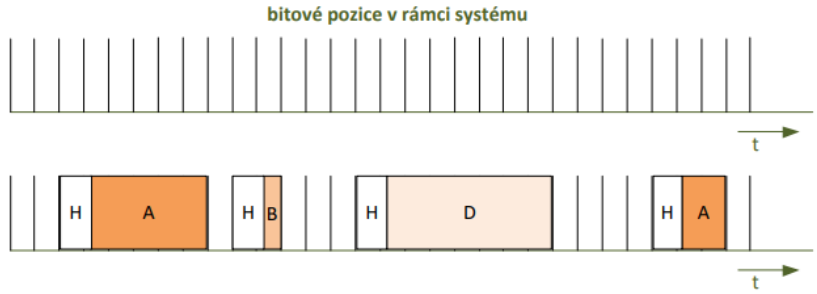
[8] xDSL: Digital Subscriber Line.



Obr. 4-2: Příklad synchronního přenosového módu – rovnoměrné rozdělení kapacity mezi čtyři stanice



Obr. 4-4: Příklad asynchronního přenosového módu – čtyři stanice (C nevysílá), jednotky umístěné v libovolném intervalu, se záhlavím, a vždy se stejnou velikostí rámce



Obr. 4-3: Příklad paketového přenosového módu – čtyři stanice (C nevysílá), různá velikost jednotek se záhlavím (značeno H), libovolná bitová pozice

4.1 Metody zajištění obousměrné komunikace

Simplex spojení umožňuje jednosměrnou komunikaci. Takže odesílatel nemůže přijímat data ale může je pouze odesílat. Nejčastěji to jsou rozhlasové a televizní vysílání, signalizační a senzorové systémy.

Half-duplex spojení umožňuje obousměrnou komunikaci, ale ne v jednom okamžiku zároveň; protistrany se o přenosovou kapacitu musí dělit. Jsou to například vysílačky, kde si komunikující musí slovně předávat signál že dohovořili.

Duplexní spojení umožňuje současnou komunikaci oběma směry. V nejjednodušším případě existuje mezi oběma stanicemi dvojice kanálů, u rádiových přenosů se *full-duplex* emuluje časovým nebo frekvenčním dělením.

5 Fyzická vrstva přenosových systémů – přenosová média a jejich základní vlastnosti, aktivní síťové prvky fyzické vrstvy.

5.1 Přenosová media

Přenosové medium představuje fyzické medium, kterým je přenášen signál od zdroje k cíli. Můžou to být elektrické vodiče (symetrický (UTP, STP) a koaxiální kabel), optická vlákna (jednovidová, vícevidová), volný prostor. Základními charakteristikami, které se sledují jsou:

- Šířka pásma určuje jaké množství dat se dá přenést na daném mediu. Vyjadřuje se v Hz nebo b/s.
- Útlum určuje postupnou ztrátu amplitudy (velikosti) signálu na mediu. Je závislý na vzdálenosti a udává se v dB (decibel). Existují 3 typy útlumu: napětí, proudu a výkonu.
- Odolnost proti vnějšímu elektromagnetickému rušení určuje odolnost proti energii ostatních signálů. Může způsobit zkreslení přenášeného signálu.
- Impedance představuje velikost odporu vůči střídavému elektrickému proudu. Udává se v Ω (Ohm) a dělíme ji na vstupní, výstupní a charakteristickou.
- Přeslech mezi vodiči představuje rušení signálem sousedních kanálů, okruhů nebo vodičů. Udává se v dB.
- Cena hlavně z ekonomického hlediska.

5.2 Analogová a digitální modulace

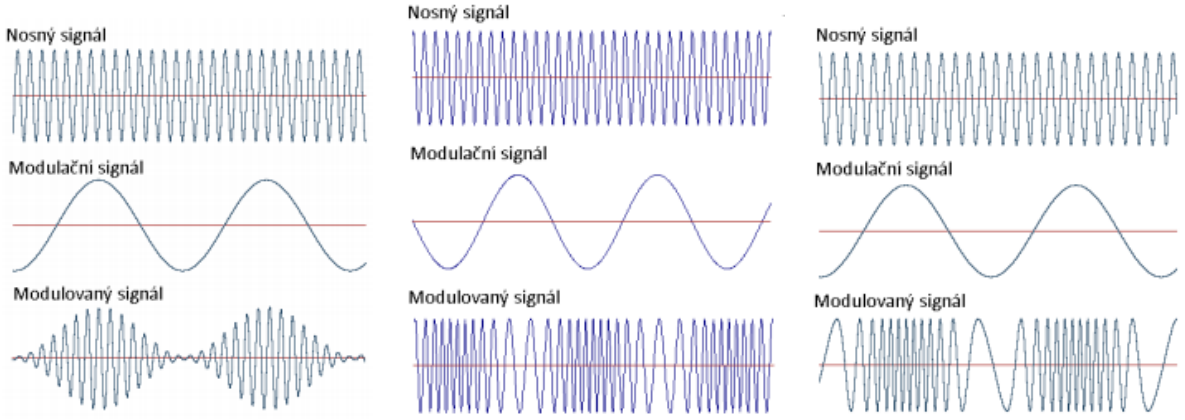
Analogový signál je spojitý a vyskytuje se běžně v přírodě; je určený amplitudou a frekvencí. **Digitální signál** je nespojitý v čase a amplitudě; vyjadřuje se v podobě 0 a 1 a je vytvořen člověkem.

5.2.1 Analogová modulace

U analogových modulací se skládá vstupní analogový signál se signálem nosné frekvence spojitě v čase. Výsledek je modulovaný analogový signál přenesený na jiném kmitočtu a s jinými vlastnostmi.

Typy modulace:

– Amplitudová modulace (AM) v závislosti na změně modulačního signálu se mění amplituda nosného signálu a ostatní parametry se nemění. Využívá se v rádiovém vysílání (dlouhé vlny).
– Kmitočtová modulace (FM) v závislosti na změně modulačního signálu se mění kmitočet nosné vlny a amplituda se nemění. Využívá se v rádiovém vysílání (krátké vlny).
– Fázová modulace (PM) u této modulace dochází na základě modulačního signálu ke změně okamžité fáze nosného signálu. Složitá demodulace.



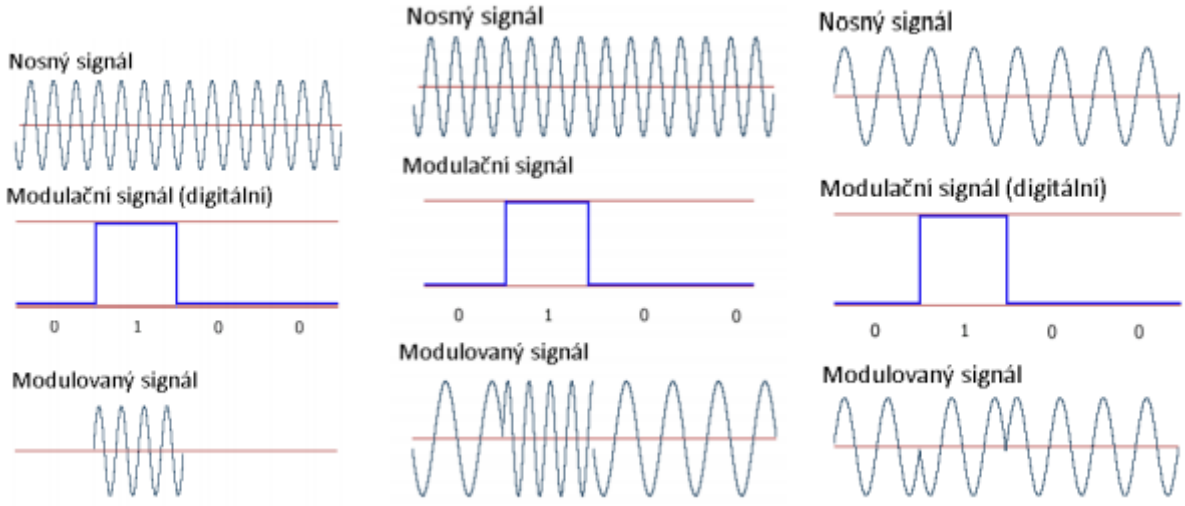
Amplitudová modulace Kmitočtová modulace Fázová modulace

5.2.2 Digitální modulace

Přenos digitálního signálu v přenesením pásmu probíhá pomocí klíčování (modulace). Rozdílem oproti analogovým modulacím je že modulační signál je diskrétní. Digitální klíčovací techniky se často využívají v bezdrátových přenosových signálech nebo i u ADSL.

Jelikož je modulační signál diskrétní dochází u nosného signálu (harmonický) ke skokovým změnám.

– **Amplitudové klíčovaní** (ASK) modulační signál střídavě spíná a vypíná podle toho jestli je právě modulována 1 nebo 0. Používá se spíše v kombinaci s dalšími typy.
– U **frekvenční klíčování** (FSK) se v závislosti na modulačním signálu skokově mění frekvence nosného signálu. Potřebuje minimálně dvě frekvence, které přepínají hodnoty $\{0, 1\}$.
– **Fázové klíčování** (PSK) spočívá v ovlivňování počáteční fáze v daném intervalu. Základně platí že 0 je jedna hodnota počáteční fáze a hodnota 1 je fází opačnou (posunutá/otočená o 180°).



Amplitudové klíčovaní Frekvenční klíčování Fázové klíčování

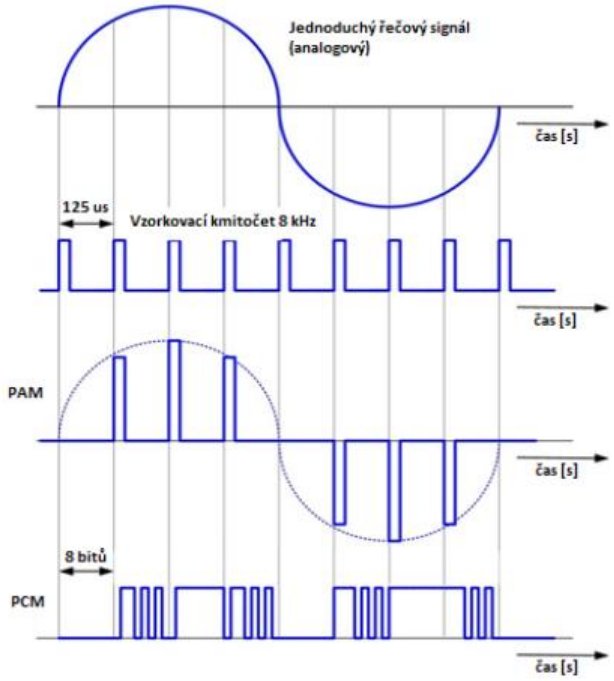
V moderních přenosech se využívá efektivnější **vícestavové klíčovaní**. Pro vyjádření n bitů je třeba 2^n stavů (čtyřstavovým se přenáší 2 bity). Čím víc stavů tím efektivnější přenos, ale zvyšuje se i složitost na straně vysílače i příjemce. Také se snižuje odolnost přenosu vůči chybám, rušení atd. Nejčastěji se využívá fázových modulací.

Kombinované fázové a amplitudové klíčování. Pro dosáhnutí co největšího počtu stavů je vhodné kombinovat více druhů klíčování (nejčastěji fázové a amplitudové klíčování). Při kombinování je modulačním signálem ovlivňována fáze tak amplituda nosného signálu často nazývaná jako QAM (kvadraturní amplitudová modulace). Často se využívá 8QAM, 16QAM, ..., kde číslo značí počet stavů nosného signálu.

5.3 Digitalizace řečového signálu

Digitalizace řečového signálu je převod mluveného slova na digitální signál. Provádí se ve třech po sobě navazujících krocích:

- **Vzorkování** má za úkol ze spojitého signálu snímat aktuální hodnoty vhodnou rychlostí (určitou frekvencí, nazývá se vzorkovací kmitočet). Ze signálu se spojitým časem získáme signál, kde se vyskytují vzorky pouze v diskrétní hodnoty času.
- Při **kvantování** se signál stává diskrétním, kdy se z neomezeného množství hladin vytvoří pouze určitý počet (16 256) hodnot. Zde se zaokrouhlují navzorkované hodnoty na nejbližší kvantovací úroveň. Dochází zde ke zkreslení signálu, který při dostatečném počtu kvantovacích úrovní nemusí být znatelný.
- Při **kódování** je stanovení hladině přiřazena určitá posloupnost, která danou hodnotu reprezentuje v použitém kódu (kódovací techniky k digitalizaci řeči lišící se v požadavcích na šířku pásma a dosahované kvalitě původního signálu).



Obr. 5-13: Ukázka principu digitalizace řečového signálu v systému PCM

5.4 Aktivní síťové prvky fyzické vrstvy

- **Opakovač** – repeater (regeneruje signál, jen 1 vstup a 1 výstup)
- **Rozbočovač** – hub (regeneruje, posílá na všechna připojená média kromě toho, odkud signál přišel)

Tyto prvky nemají adresu, nelze je rozpoznat na trase, nerozumí přenášeným datům. Pracují jen se signálem. Použití opakovače je např. u podmořských optických kabelů, rozbočovače se používaly na metalické síti, dnes už spíše ne.

6 Spojová vrstva přenosových systémů – podvrstvy, rámce spojové vrstvy, adresace, metody zajištění spolehlivého přenosu.

6.1 Podvrstvy

LLC (logical link control) poskytuje rozhraní mezi konkrétním přenosovým prostředkem a síťovou vrstvou. Stará se o multiplexování požadavků síťové vrstvy, které přicházejí od IP, IPX nebo Appletalk protokolu a umožňuje jim koexistovat v jedné infrastruktuře. Může se také starat o kontrolu toku dat a řízení chybových stavů mezi uzly (u TCP/IP se stará transportní vrstva).

MAC (media access control) poskytuje specifické služby pro daný přenosový prostředek (kódování, přenosové schéma, adresování nebo práce s rámci). V případě sítí s mnohonásobným přístupem pak řeší problematiku přístupu k mediu s ohledem na ostatní uzly sítě (sdlení kapacity, řešení kolizí).

6.2 Rámec spojové vrstvy

Rámec je základní jednotka, se kterou pracuje spojová vrstva. Protokoly potřebují řídící informace: které uzly spolu komunikují, kdy komunikace začíná a končí, zda došlo při přenosu k chybám, kdo bude komunikovat jako další.

Rámec se obvykle skládá ze tří částí:

- Záhlaví (header) obsahuje řídící informace:
  - začátek rámce (preambule) slouží k identifikaci začátku danou sekvencí bitů,
  - zdrojovou a cílovou adresu k identifikaci komunikujících uzlů.
- Datová část obsahuje nejčastěji paket.
- Zápatí (trailer) obsahuje řídící informace k zjištění chyb:
  - kontrolní sekvence rámce (FCS) detekce chyb přenosu,
  - zápatí identifikuje konec celého rámce předem danou sekvencí bitů.

6.2.1 Rámec standardu ethernet

Existuje víc typů rámců Ethernet. Nejpoužívanější jsou Ethernet II a IEEE 802.3. Rozdíl je v hodnotě délka/typ. Pokud je v poli dekadická hodnota menší jak 1500, jedná se o délku udávající datovou délku rámce. Pokud je větší jak 1500, určuje typ protokolu v datové části.

Obr. 6-4: Formát rámce u Ethernetu IEEE 802.3

Obr. 6-5: Formát rámce Ethernet II

Dalšími typy rámců můžou být rámce protokolů BiSync, PPP a HDLC nebo rámce technologií ATM a Frame Relay.

6.3 Adresace

Adresy jsou označovány jako fyzické adresy (MAC), které jsou při komunikaci uloženy v záhlaví rámce a specifikují cíl na lokální síti (pro odpověď se uvádí i MAC odesílatele). MAC adresy jsou používány jen pro lokální adresování, při změně sítě se vytváří nový rámec. Vznikají zapouzdřením rámce vyšší vrstvy.

Každý uzel sítě má unikátní MAC, která je uložena v paměti uzlu. Adresa je přednastavena výrobcem a je celosvětově unikátní. Délka je 48 bitů s tvarem `FE:DC:BA:98:76:54`. První polovina značí výrobce a druhá kód konkrétního rozhraní.

6.4 Techniky detekce chyb

6.4.1 Základní přístupy k detekci chyb

Nejjednodušším způsobem je přenesední rámce dvakrát (což je nevýhodné kvůli velké zátěži; nelze také detekovat dvakrát stejnou chybu). Lze požádat o opakované poslání rámce a špatný zahodit, nebo se chybu pokusit opravit automaticky. Kvůli tomu se k rámci přidávají redundantní informace.

6.4.2 Metody zabezpečení proti chybám

Paritní bit je nejjednodušší způsob zabezpečení. V každých sedmi bitech se přidá paritní osmý (doplní se {0, 1} dle sudé či liché parity výsledku), tento způsob však nedetekuje sudý počet chyb.

Kontrolní součty provádí součet celého rámce a výsledek ukládají jako kontrolní hodnotu za rámec, nejsou odolné proti záměně pořadí bitů.

Cyklické redundantní kontroly (CRC) jsou používané všemi spojovými protokoly. Fungují na principu dělení polynomu polynomem a do pole FCS je ukládán zbytek po dělení. Vyžadují malou redundanci a pravděpodobnost detekce chyby je vysoká. Odesílatel před odesláním spočítá kontrolní sekvenci a přidá ji do FCS. Příjemce také spočítá kontrolní sekvenci a pokud se FCS rovná, je rámec považován za neporušený.

6.5 Spolehlivý přenos

Při určení spolehlivosti se rozlišují chyby uvnitř rámce (poškození) nebo jeho kompletní ztrátu (nelze ho detekovat a rozpoznat).

Pokud byl ztracen, příjemce neví o jeho existenci a proto musí existovat nadřazené mechanismy pro opakované vysílání. Spojové protokoly neposkytují spolehlivý přenos a detekci nechávají na vyšších vrstvách.

Základní předpoklady pro řízení chybových stavů a toku dat:

– velikost vyrovnávací paměti příjemce není neomezená,
– delší rámec znamená větší pravděpodobnost výskytu chyb,
– kratší rámec znamená rychlejší detekci chyb,
– stanice nemůže blokovat medium na neomezeně dlouhou dobu,
– existuje snaha dosáhnout co nejmenší chybovosti (alespoň 10^{-9}).

Systémy detekce ztracených rámců **Kladné potvrzení** je oznámení bezchybného přijetí rámce. Nepotvrzené rámce jsou znovu odeslány, je tedy třeba vyšší kapacita. **Záporné potvrzení** je zaslání oznámení se žádostí o opakované vysílání, vysílač je kontaktován v případě problému. Nereagování přijímače ale nemusí značit bezchybný stav. **ARQ** (*Automatic Repeat Request*).

Stop-and-wait ARQ je nejjednodušší metoda: vysílač i přijímač pracují sekvenčně. Vysílač odešle rámec a čeká na potvrzení; přijímač zkontroluje CRC a při doručení odpovědi vysílači je zaslán rámec další; při chybě či určité době ho vysílač zašle znovu. Tento přenos je časově velmi neefektivní a nevyužívá se.

Technika klouzavého okna kvůli efektivitě nečeká na potvrzení rámce před posláním nového ale odesílá je po sobě a průběžně pak čeká i na potvrzení (při full-duplexu). Vysílač vysílá určitý počet rámců před potvrzením (velikost okna). Pro výpočet minimální velikosti okna se použije vzorec *(přenosová rychlost · zpoždění)/(velikost rámce)*. Rámce musí být číslovány.

Go-back-N ARQ využívá mechanismus klouzavého okna, kdy se při chybě vrací do určitého stavu. Při nalezení chyby přijímač všechny další přijaté rámce zahazuje a informuje vysílač o nové zaslání od špatného rámce. Přijímač používá pouze dva druhy zpráv: kladné (`RR`: Recieve Ready, `ACK`: Acknowledged) a negativní (`REJ`: Go back to N, `NACK`) potvrzení.

Selective Repeat ARQ je podobný Go-back-N, ale správné rámce nejsou zahozeny a místo toho jsou uloženy do cache. Přijímač pouze požádá o chybný rámec (`SREJ`) a při jeho korektním přijetí ho zařadí mezi ostatní. Tento způsob je náročnější na paměť přijímače, ale šetří přenosový kanál.

Technika klouzavého okna a řízení toku slouží k zajištění spolehlivého přenosu rámců přes kanály s chybami. Má také další dvě funkce: zajištění správného pořadí rámců a řízení toku. Zajištění správného pořadí rámců řeší číslováním rámců. Řízení toku umožňuje přijímači poskytnout zpětnou vazbu, že stíhá nebo nestíhá přijímat (může nastat zahlcení).

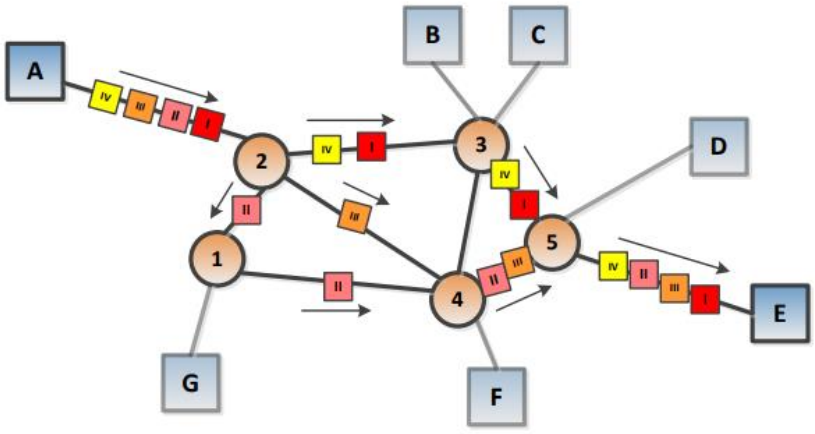
7 Síťová vrstva přenosových systémů – spínání paketů, služby síťové vrstvy, IPv4 adresy, techniky směrování, IPv4 datagram.

7.1 Přepojování paketů

Síťová vrstva hledá optimální cestu mezilehých uzlů mezi dvěma účastíky komunikace. I když je více způsobů komutace (viz otázku 1), využívá se komutace paketů s typickou maximální délkou 1000–1500 B.

Služba se spojením *Connection-Oriented Network Services* před přenosem navazuje spojení: během přenosu je zřejmé odkud kam pakety putují a proto nemusí obsahovat informaci o příjemci, mají však **identifikátor toku**. Jde o tzv. virtuální okruhy, kdy síťová vrstva poskytuje dokonalý bezchybný kanál dodržující pořadí datových jednotek při přenosu. Dočasný virtuální okruh (SVC, *Switched Virtual Connection*) spojení připravuje před každým přenosem, pevný virtuální okruh (PVC, *Permanent Virtual Connection*) je definovaný v komunikačních uzlech, sestavuje se při zapnutí a není využitelný dalšími uživateli.

Služby bez spojení Také datagramové služby. *Connectionless Network Services* vyžaduje cílovou adresu v každém paketu. Při přenosu paketu může dojít ke změně pořadí nebo ztrátě paketu.



Obr. 7-3: Ukázka nespojovaného přepojování paketů v síti (služba bez spojení)

7.2 Služby síťové vrstvy

7.2.1 Služby síťové vrstvy na zdrojové stanici

Základní službou je **vytváření paketů**: zapouzdření jednotky vyšší vrstvy, přidání záhlaví (adresy, informace). **Vyhledání logické adresy** dalšího uzlu: vyhledání cíle pro první skok s využitím směrovací tabulky. **Vyhledání linkové adresy** dalšího uzlu: překlad logické adresy pro přenos po fyzickém médiu. **Rozdělení datagramu** na menší jednotky v případě potřeby (pokud je vytvořený paket větší než maximální povolená velikost).

7.2.2 Služby sítové vrstvy na směrovači

Kontrola bezchybnosti přenosu paketu, vyhledání logické a linkové adresy dalšího prvku, rozdělení datagramu, je-li to v mezilehých uzlech povoleno.

7.2.3 Služby síťové vrstvy z pohledu cílové stanice

Kontrola bezchybnosti přenosu paketu, **defragmentace** rozdělených částí a **předání vyšší vrstvě**.

7.3 Další služby síťové vrstvy

I když **řízení chybových stavů** řeší až transportní vrstva, síťová vrstva obsahuje protokol ICMP/ICMPv6, který řízení chybových stavů částečně poskytuje, např. může zasílat *choke packet* signalizující požadavek o zpomalení.

Kvalita služeb (*Quality of Services*) spočívá ve vyhrazení dostatečné kapacity pro aplikace, které ji vyžadují (videohovory a další aplikace běžící v reálném čase). **Směrování** umožňuje dynamicky zjišťovat informace o vzdálených sítích pro účely směrování. **Bezpečnost** nebyla původně vůbec řešena, využívá se IPSec.

7.4 Služby síťové vrstvy poskytované transportní vrstvě

Přenos datových jednotek je prováděn z pohledu transportní vrstvy transparentně. **Výběr kvality služby** určuje chybovost, dostupnost, spolehlivost, propustnost, zpoždění při přenosu či řízení. **Výběr typu**: se spojením či bez něj. **Oznamování chyb** neopravených síťovou vrstvou. **Dodržení pořadí** datových jednotek, **řízení toku dat**.

7.5 IPv4

IPv4 adresa má délku 32 bitů. Počet všech adres je označován jako **adresní prostor** s velikostí 2^{32}, tj. zhruba čtyři miliardy adres. IPv4 adresy se zapisují jako čtyři čísla v rozsahu $[0, 255]$ oddělena tečkou, např. `147.229.71.29`.

Maska sítě rozděluje IP adresu na adresu sítě a stanice. Jde o nepřerušenou řadu bitů zleva, která je reprezentována číslem $[1, 32]$ reprezentujícím počet bitů masky. Adresa `147.229.71.29/24` znamená síť `147.229.71.0`, stanici `0.0.0.29` a masku `255.255.255.0`: `11111111 11111111 11111111 00000000`. Číslo za lomítkem se označuje jako délka prefixu: prefix `/18` odpovídá masce `255.255.192.0`.

V síti je první adresa rezervovaná pro síť samotnou a poslední adresa pro všesměrové vysílání (pakety jsou doručovány všem v síti); ostatní adresy mohou být přiřazeny stanicím.

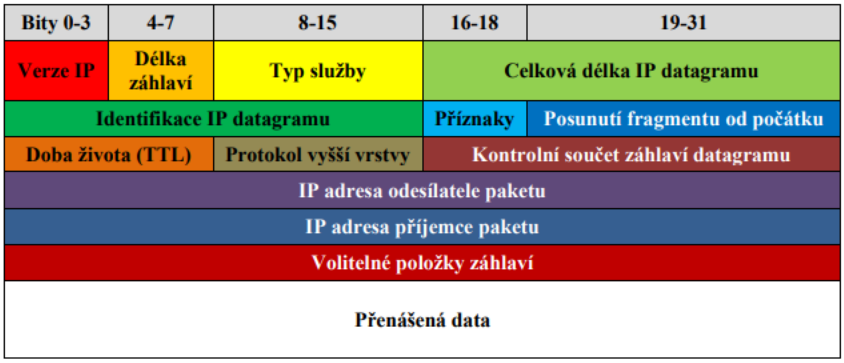
Historicky se adresní prostor IPv4 rozděloval pomocí tříd. V devadesátých letech se přešlo k beztřídnímu adresování, což umožnilo prostor rozdělit efektivněji.

7.5.1 IPv4 datagram

Při přenosu je zabalen do paketu vyšší vrstvy (Ethernet, ATM, ...). Zabalený datagram zůstává neměnný, s výjimkou proměnných polí jako hodnota čítače životnosti paketu.

Tab. 3: Historické dělení adresního prostoru IP protokolu na třídy

Třída	Rozsah prvního oktetu adresy (dekadicky)	Dělení adresy na adresu Sítě a Hosta	Standardní maska sítě (dekadicky)	Délka prefixu sítě	Počet možných sítí / hostů na jednu síť
A	0 – 127	S.H.H.H	255.0.0.0	/8	128 / 16 777 214
B	128 – 191	S.S.H.H	255.255.0.0	/16	16 383 / 65 534
C	192 – 223	S.S.S.H	255.255.255.0	/24	2 097 150 / 254
D	224 – 239	-	Multicastové adresy		
E	240 – 255	-	Experimentální adresy		



Obr. 7-20: Detail struktury IPv4 datagramu z hlediska položek záhlaví a umístění datové části

Verze: `4`. Délka záhlaví: `20` až `60` v bajtech. Typ služby: hodnota QoS.

7.6 Směrování

Existují dva typy směrovaní: statické a dynamické. Statické se téměř nepoužívá, protože je ho nutné ručně udržovat aktuální; lze ho však využít v koncových (a převážně statických) sítích.

Dynamické směrovaní průběžně reaguje na změny a upravuje tak směrovací tabulky. Nejčastějšími typy dynamického směrování jsou:

- Centralizované směrovače posílají informace o okolních sítích do jednoho řídícího centra a to pak rozesílá směrovací tabulky zpět směrovačům.
- Distribuované informace o změnách se předávají mezi sousedními směrovači.
- Hierarchické sítě se rozdělují do několika oblastí, kde koncové prvky těchto oblastí předávají informace mezi sebou. Každá oblast si provádí vlastní směrovaní.
- Izolované směrovače si nevyměňují informace ale rozhodují se samy.

Nejznámější distribuované protokoly jsou **RIP** (nejmenší počet skoků, obnova informací každých 30 sekund); **OSPF** (hledání nejkratší cesty, obnova informací až při změně v síti) nabízí také možnost hierarchického směrování. Většina dynamických směrovacích proto-

kolů využívá nějakého algoritmu na nalezení nejkratší cesty. Základní požadavky na protokoly jsou minimalizace velikosti směrovacích tabulek (rychlost vyhledávání), minimalizace počtu přenášených zpráv (menší zátěž), robustnost (aby nedošlo k zacyklení paketu) a využití optimálních tras (nemusí být vždy nejrychlejší nebo nejkratší).

Dynamické protokoly se dělí na *Distance Vector* (starší, periodicky posílají celou routing table všem sousedům, zástupce je RIP) a *Link State* (tabulku přeposílají jen při nějaké události, zejména změna stavu média, zástupci jsou OSPF, IS-IS). Link State konverguje rychle i ve velkých sítích, zatímco u Distance Vector protokolů trvá dlouho, než se změna přepíše do všech směrovačů v síti.

8 Síťová vrstva přenosových systémů – tunelování paketů, ARP, NAT, ICMPv4, IPv6.

8.1 Tunelování paketů

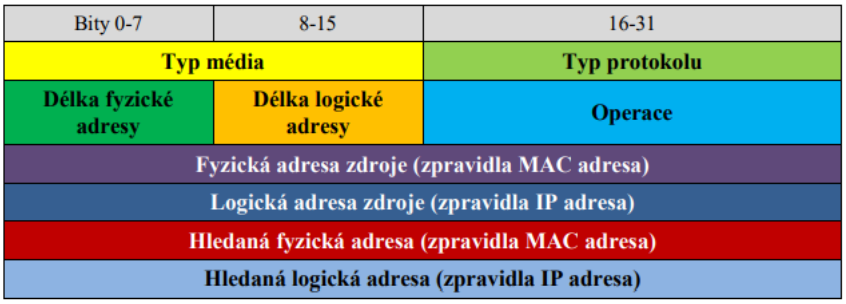
Princip tunelování je zapouzdření původního paketu a přidání nového záhlaví. Záhlaví se liší tím, že má jinou cílovou a zdrojovou IP adresu.

Typy tunelování:

- Tunelovaní spolu s IPsec protokolem (celý packet je šifrován pomocí IPsec a k tomuto zašifrovanému paketu se přidá nové IP záhlaví).
- IP tunelování je vhodné pokud se přechází mezi verzemi IP protokolu (IPv4 a IPv6). Při přechodu mezi verzemi se přidá nové záhlaví před to původní.

8.2 ARP (Address Resolution Protocol)

ARP slouží k nalezení neznámé fyzické adresy (MAC) k IPv4 adrese. Jedná se o dynamicky distribuovaný protokol schopný reagovat na změny v síti. Informace se ukládají do ARP tabulky v podobě `<IP:MAC:type>`. Pracuje mezi spojovou a sítovou vrstvou, používá rámce spojové. Stanice pro zjištění vysílá broadcast požadavek a jen stanice, která má požadovanou adresu, odpoví.



Obr. 7-25: Členění ARP paketu na jednotlivá pole

8.3 NAT (Network Address Translation)

NAT (překlad síťových adres) umožňuje směrovači změnu IP adresy v záhlaví paketu a oddělit tak interní sít od internetu. Na cestě může být změna provedena několikrát (a to i mezi různými typy IP protokolů: NAT-PT). Po aplikaci NAT překladu má více zařízení v lokální síti jednu veřejnou IP adresu.

Základní druhy NAT:

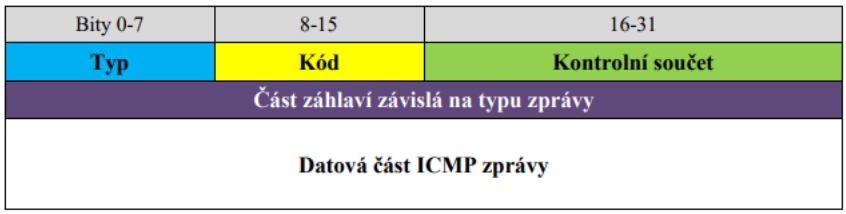
– SNAT (source NAT) překládá zdrojové IP adresy a potom až adresy transportní. Komunikace je možná pouze z vnitřní sítě.
– DNAT překládá cílové IP adresy a až potom případné transportní adresy. Používá se ke zveřejnění služby z interní sítě na veřejně přístupnou IP adresu.

8.4 ICMPv4

Protokol ICMP je servisní protokol (nepřenáší žádná uživatelská data). Slouží k testování konektivity, umožňuje signalizaci mimořádných událostí.

Tabulka 1: Vybrané typy ICMP zpráv

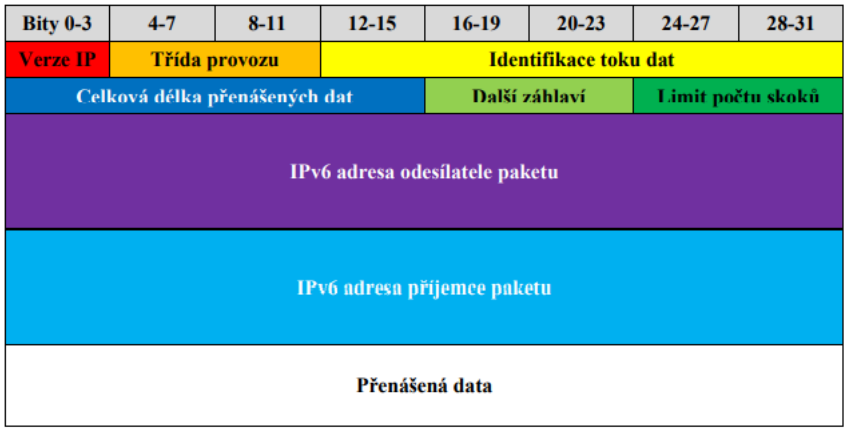
kategorie	typ	zpráva
hlášení chyb	3	*Destination unreachable*
	4	*Source quench* (snížení rychlosti odesílání)
	5	*Redirection*
	11	*Time exceeded*
	12	*Parameter problem*
dotazování	8	*Echo request*
	0	*Echo reply*
	13	*Timestamp request*
	14	*Timestamp reply*



Obr. 7-32: Obecný formát ICMPv4 zprávy

8.5 IPv6

IPv6 je nekompatibilní s IPv4; hlavním rozdílem je změna zápisu adres (`fe80:1a3d::0/64`) a rozšíření velikosti adresního prostoru z 32 bitů na 128 bitů. Pro přechodné zajištění kompatibility se využívá technik jako souběh protokolů (SW a HW podporuje oba dva druhy), tunelování (většinou zapouzdření IPv6 do IPv4 paketu) a překlad adres (podobné nat jen s rozdílem že se zaměňují přímo adresy obou verzí, nazývá se to NAT-PT [protocol translator]).



Obr. 7-35: Základní záhlaví IP datagramu verze 6

Třída provozu nastavuje prioritu paketu, identifikace toku dat umožňuje zjednodušení směrování, celková délka přenášených dat je velikost bez záhlaví, další záhlaví určuje informace o vnořeném záhlaví.

Existují 3 druhy adresování:

- Unicast (individuální) jsou adresy identifikující jednotlivá síťová rozhraní.
  - Globální unikátní (`2000::/3`)
  - Linkové unikátní (`FE80::/10`)
  - Lokální smyčka (`::1/128`)
  - Nespecifikovaná adresa (`::/128`)
  - lokální unikátní (`FC00::/7`)
  - IPv4 kompatibilní (`::/80`)
- Multicast (skupinové) pro skupiny a pakety jsou doručeny všem ve skupině. Patří sem i broadcast adresy.
  - Přiřazená adresa (`FF00::/8`)
  - Vyzývaný uzel (`FF02::1:ff00:0/104`)
- Anycast (výběrové) také skupina ale paket je do doručen pouze jedinému členovy (nejčastěji nejbližší).

9 Transportní vrstva přenosových systémů – služby transportní vrstvy, UDP protokol, TCP protokol.

9.1 Služby transportní vrstvy

Shrnutí:

- **Komunikace procesů** (odlišuje komunikaci různých procesů mezi stejnými stanicemi)
- **Adresování** (port)
- **Zapouzdření dat** (datagram L4 = „segment“)
- **Multiplexování a demultiplexování v transportní vrstvě** (řazení požadavků vyšších vrstev do fronty, předání síťové vrstvě)
- **Řízení přenosu v transportní vrstvě** (flow control, error control, congestion control, součástí UDP je jen error control v hlavičce, ostatní jsou jen v TCP)
- **Charakter poskytovaných služeb** – bez spojení / se spojením
- **Network and Port Address Translation** (NAT, PAT společně se síťovou vrstvou)

Delší verze:
Transportní vrstva poskytuje komunikační prostředky pro komunikaci procesů v TCP/IP. Slouží pro rozlišení a doručení konkrétnímu procesu na zařízení.

Pro adresaci na transportní vrstvě je třeba rozlišit 4 adresy, kterými jsou lokální host (stanice), lokální proces (aplikace), vzdálený host (stanice), vzdálený proces (aplikace). Komunikuje jako klient-server. Adresaci stanic má na starosti síťová vrstva a o adresy procesu se stará transportní vrstva. Protokoly UDP a TCP adresují na základě portů.

Port má velikost 16 bitů (čísla 0 - 65535). Porty 0 – 1023 slouží pro známé aplikace (FTP, HTTP atd), 1024 – 49151 slouží pro méně používané aplikace, které jsou registrovány u IANA nebo volné přístupné uživatelské porty, 49152 – 65535 jsou soukromé a dynamické porty přiřazované na straně klientské aplikace.

Socket je označení pro kombinaci IP adresy a portu sloužící k identifikaci koncového bodu komunikace. Kombinace zdrojového a cílového socketu je vždy jedinečná (neexistují dvě probíhající komunikace se všemi 4 stejnými hodnotami).

Segmentace je je dělení velkého množství dat na části, kdy ke každé části je přidána záhlaví. Operace přidání záhlaví se nazývá zapouzdření a je prováděna u odesílatele. Opačný proces se nazývá odpouzdření a je prováděna až konečným příjemcem. Segment se záhlavím je předán síťové vrstvě a zapouzdřen IP záhlavím a odeslán jako paket. Příjemce

segment předá transportní vrstvě zbavený záhlaví a na základě portu předá konkrétní aplikaci. TCP do záhlaví přidává pořadové číslo odesílaného bajtu, UDP toto neumožňuje.

K multiplexování dochází jestliže se v jednom bodě střetávají požadavky z různých zdrojů a mají být nějakým způsobem obslouženy. Jsou postupně zařazeny do fronty a vyřizovány. Demultiplexování je opačný postup multiplexovaní.

Řízení toku na transportní vrstvě zajišťují mechanismy:

- Řízení toku dat (flow control) spočívá ve způsobu organizace komunikace mezi koncovými body, realizace front a vyrovnávacích pamětí.
- Řízení chybových stavů (error control) spočívá v číslovaní přenášených dat a potvrzování úspěšného přenosu. Řízení chybových stavů a toku dat je kombinováno v rámci techniky posuvného okna.
- Předcházení zahlcení (congestion control) je řešeno pomocí techniky posuvného okna a následného nastavení dalších parametrů (pravidla pro opakovaný přenos, potvrzovaní přenosu...).

Řízení toku na transportní vrstvě řeší celý přenosový řetězec dohromady, což je klíčové pro komunikaci.

9.2 UDP user datagram protocol

UDP je jednoduchý transportní protokol, který umožnuje nespojovaný a nespolehlivý přenos dat (best effort). Přenášeným jednotkám se říká datagramy. Nepotvrzuje doručení musí být řešeno na aplikační vrstvě. Oproti síťové umí UDP provádět přenos mezi konkrétními procesy. Má minimální režii přenosu a zpoždění. Je vhodný na přenos krátkých zpráv u kterých není potřeba bezztrátovost.

Bity 0-15	16-31
Zdrojový port	**Cílový port**
Celková délka	**Kontrolní součet**
Data aplikace	

Obr. 8-6: Záhlaví UDP protokolu

Zdrojový port určuje port na straně odesílatele, cílový port na straně příjemce, celková délka určuje velikost datagramu v bytech a kontrolní součet slouží k základní detekci chyb.

Služby UDP:

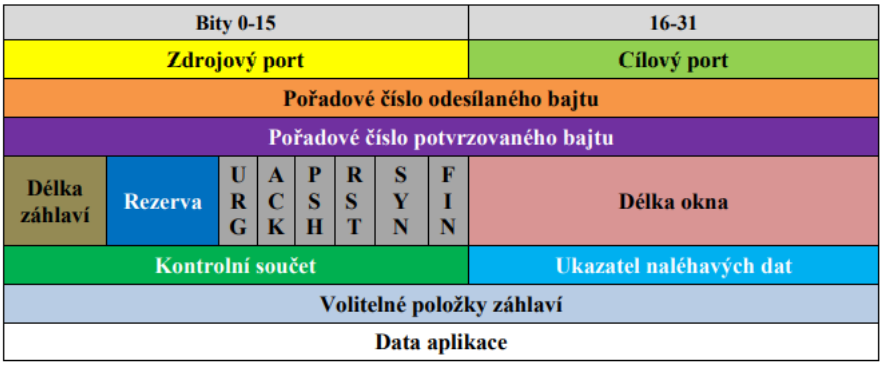
- Komunikace proces–proces (komunikace socketových adres).

– Přenos dat bez spojení, každý datagram je přenášen samostatně (před komunikací není navozováno spojení).
– Žádné řízení toku dat, řízení proti zahlcení či řízení chybových stavů.
– Zapouzdřování a odpouzdřování dat (pokud není detekována chyba).
– Frontování, multiplxování a demultiplexování (fronty jsou vytvářeny dle portů) a na těchto frontách lze provádět multiplexování a demultiplexování.

Využití ve službách dotaz-odpověď (DNS) nebo ve VoIP službách.

9.3 TCP Transmission Control Protocol

TCP umožňuje spojovaný a spolehlivý přenos dat. Přenášeným jednotkám se říká segmenty. Tyto segmenty jsou číslované. Číslovaní odesílaných a potvrzovaných bytů (odeslané byty jedné strany, odeslané byty druhé strany, byty potvrzované jednou stanou a byty potvrzované druhou stranou). Umožňuje řízení toku dat, chybových stavů a stavů zahlcení. Má velkou režii přenosu.



Obr. 8-7: Struktura TCP záhlaví

Pořadové číslo odesílaného bytu (SEQ, pořadové číslo prvního z odeslaných bytů segmentu), pořadové číslo potvrzovacího bytu (ACK) hodnota dalšího očekávaného bytu, délka záhlaví (musí být uvedeno kvůli volitelným položkám záhlaví, které mají 0-40 bytů), příznakové bity (když jsou nastaveny na 1 jsou aktivní), délka okna (maximální počet odeslaných bytů aniž by bylo potřeba potvrzení přijímače), kontrolní součet (podobný UDP), ukazatel naléhavých dat (jen pokud URG je 1) a volitelné položky záhlaví (nejsou povinná).

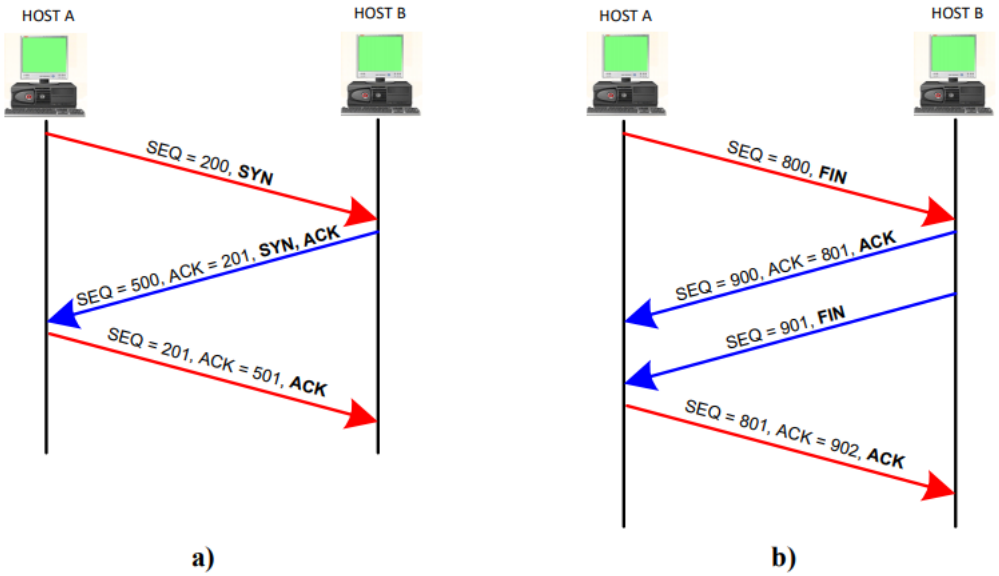
Příznakové bity:

– URG urgentní data
– ACK indikuje platnost pole potvrzovacího bytu
– PSH data mají být předána po přijetí hned aplikaci (push)

– RST odmítnutí spojení
– SYN navazování spojení
– FIN ukončení spojení

Služby TCP:

– Komunikace proces–proces (komunikace socketových adres).
– Přenos toku dat (vytváří dojem propojení komunikujících procesů okruhem).
– Plně duplexní přenos dat (komunikace oběma směry zároveň).
– Multiplexování a demultiplexování (stejné jako UDP).
– Spojovaně orientovaná služba (musí být prvně navázáno spojení a na konci ukončeno).
– Spolehlivý přenos dat (využití potvrzovacích mechanizmů).



Obr. 8-8: Průběh spojení TCP a) navázání, b) ukončení

Navázání probíhá pomocí 3-cestného handshaku a ukončení pomocí 4-cestného handshaku (existuje 3-cestná varianta na obrázku kde ACK a FIN jsou sloučeny do jedné zprávy).

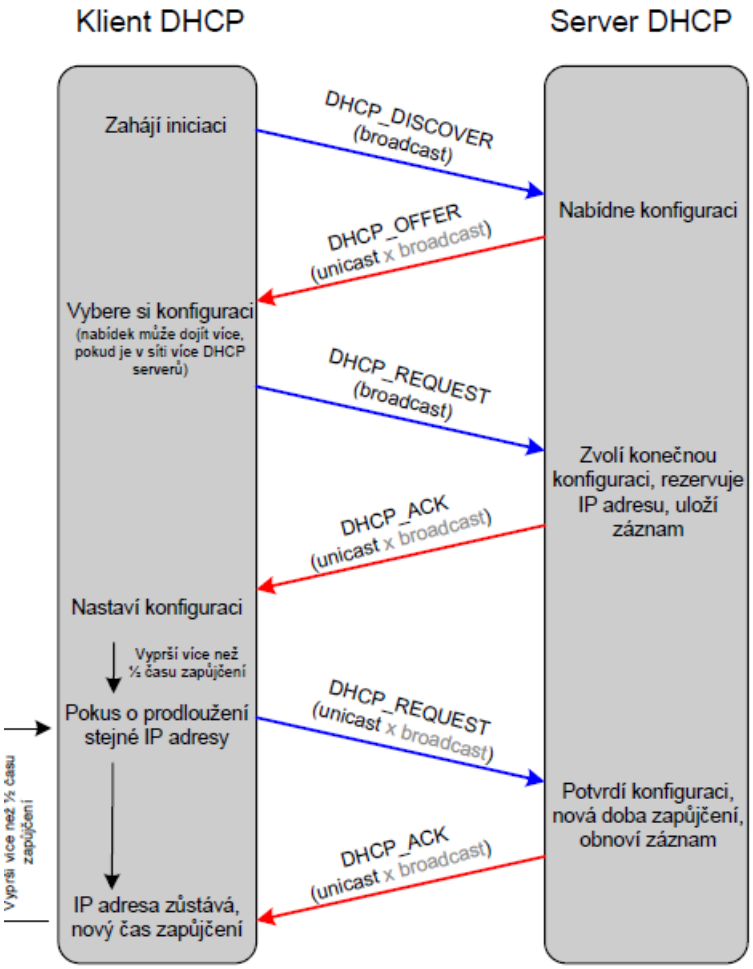
Záhlaví TCP obsahuje délku okna sloužící k nastavení přenosu maxima bytů bez potvrzení. Jelikož je spojení plně duplexní tak jsou okna vždy dvě a nemusí mít stejnou velikost. Tento mechanismus se nazývá technika posuvného okna.

Využití na službách HTTP, FTP, SMTP a v dalších službách kde je potřeba spolehlivého přenosu.

10 Aplikační vrstva přenosových systémů – DHCP protokol, DNS systém, přenos souborů, webové protokoly, elektronická pošta.

10.1 DHCP Dynamic host configuration protocol

DHCP je protokol aplikační vrstvy, který má na starost dynamické nastavování parametrů sítě. Nastavuje IP adresu, masku sítě, výchozí bránu, DNS a případně další. Funguje na principu klient-server. DHCP server vždy zapůjčí IP adresu na určitou dobu po které bude klient zbaven přístupu k této IP, pokud si zapůjčení neprodlouží. Využívá UDP porty 68 pro komunikaci a server 67 pro naslouchání. Existuje DHCP relay agent, který přeposílá broadcast zprávy do jiných sítí pokud se tam nachází DHCP server.



10.2 DNS domain name system

Překládá těžko zapamatovatelné IP adresy na jednodušeji zapamatovatelná jména v podobě řetězce znaků. Pokud by DNS neexistovalo a tak při změně IP adresy by si lidé museli znovu zapamatovávat IP adresu. Při existenci DNS se přepíše záznam jen na DNS serveru a tento problém se nemusí řešit. Ke komunikaci využívá porty UDP 53 a TCP 53. Funguje na principu klient-server, kdy jedinou IP adresou, kterou musíme znát je adresa DNS serveru. Vazba mezi je IP adresou a doménovým jménem je uložena v celosvětově distribuované DNS databázi. Základní jednotkou systému je DNS server (name server, jmenný server, rekurzivní resolver). DNS servery jsou primární (poskytuje autoritativní odpovědi) a sekundární (záloha primárního) a pomocný (pracuje jako vyrovnávací paměť). Server nejdřív hledá v pomocném serveru jestli záznam není uložen v paměti (cache) a musí mít vlastní DNS server, kterého se může zeptat.

Je vytvářena hierarchie domén, která začíná od kořene a jde postupně níže. Prvně se jde od domény nejvyššího řádu k nižším řádům domény. Domény nejvyššího řádu se dělí na generické (.edu, .com) a národní domény (.cz). Doménové jméno může mít maximální délku 255 znaků, kdy jeden řád (úroveň) může mít maximálně 63 znaků. Maximální počet řádů může být 127.

Postup dotazu na fekt.vutbr.cz. Klient se zeptá lokálního DNS serveru na IP pro tuto doménu. Jelikož ten to často neví tak se zeptá kořenových DNS serverů. Jelikož často kořenový neví, ale ví adresu další DNs serveru pro doménu nejvyššího řádu, tak mu odešle IP na ten server. Tak se postupuje stejným způsobem dokud se nenajde server, který danou IP adresu zná. Tuto IP adresu poté lokální DNS server zašle klientovy[9].

10.3 FTP file transfer protokol

FTP je protokol na aplikační vrstvě sloužící pro přenos souborů mezi dvěma stanicemi. Využívá TCP porty 20 a 21, kdy 20 slouží k přenosu dat a na 21 naslouchá na příchozí spojení. Funguje na principu klient-server, kdy spojení navazuje pouze klient. Datová spojení jsou jednorázová a přenos není zabezpečený (i heslo se přenáší v prostém textu).

Přihlásit se lze buď anonymně, že server nepožaduje žádnou autentizaci uživatele nebo zadáním konkrétního přihlašovacího jména a hesla (při přenosu nejsou šifrovány).

Po navázání spojení klient posílá řídící příkazy (interpretace pomocí NVT protokolu) a server na tyto příkazy odpovídá (rozlišují se pomocí tří číselného kódu).

[9] https://cs.wikipedia.org/wiki/Domain_Name_System#/media/Soubor:Dns-wikipedia.png

Pracovní režim rozdělujeme na aktivní a pasivní. V aktivní režimu klient otevře náhodný port > 1023 a pošle serveru vybrané číslo portu. Následně klient na portu naslouchá a čeká na navázání datového spojení. Můžou nastat problémy pokud síť využívá filtrování nevyžádaného provozu, je za NATem nebo další. V pasivním režimu probíhá spojení naopak. Server otevírá port > 1023 a vyzve klienta k navázání spojení. Pasivní režim je výhodný pokud je klient uvnitř privátní sítě s vlastní adresou a server se nemůže na jeho port připojit.

10.3.1 Zabezpečené alternativy

SCP (Secure Copy Protocol), využívá SSH (Secure Shell) šifrovaný kanál. Port serveru je 22 (stejně jako SSH).
SFTP (SSH File Transfer Protocol), taky využívá SSH, funkcionalita postavená na FTP. Port je taky 22.

10.4 Webové protokoly

Technologie WWW v základu využívá HTML, protokolu HTTP a URL.

URL (Uniform Resource Locator) představuje jednoznačné síťové umístění nějakého zdroje nebo dokumentu. Tvar protokol://uživatel:heslo@počítač:port/cesta/#část_stránky. Protokol je povinný, uživatel nepovinný, heslo nepovinné, počítač ve tvaru IP nebo DNS jména, port je nepovinný, cesta v rámci serveru nebo počítače (nepovinná), část stránky je část dokumentu (nepovinná).

HTTP (Hyper Text Trasfer Protocol) slouží pro přenos HTML dokumentů mezi klientem (prohlížeč) a www serverem. Využívá TCP port 80 a jeho zabezpečená verze HTTPS využívá TCP 443. Funguje na způsobu dotaz–odpověď. Protokol HTTP do verze 1.1 je bezstavový, takže jeden dotaz na server je jeden klient. Pro každé spojení vytváří samostatné TCP spojení. Od verze 1.1 už lze podat více dotazů v jedné relaci, takže se nemusí vytvářet pokaždé nové TCP spojení a po určité době je spojení ukončeno. Nejčastějšími dotazy (request methods) jsou GET (požadavek na uvedený objekt se zasláním případných dat), HEAD (podobný GET jen nepředává data), POST (odesílání dat na server), PUT (nahrává data na server) a DELETE (smaže uvedená data ze serveru).

10.5 Elektronická pošta

Je založena na modelu klient-server. Klient posílá zprávu (email) pomocí MUA (mail user agent, poštovní klient) přes protokol SMTP na svůj poštovní server MSA (mail/message submission agent). MSA předává email na svůj MTA (mail transfer agent, přenos zpráv mezi servery). Často je MSA spojen do jednoho s MTA. MTA (server) vyhodnotí adresáta

a určí na jaký další server to předat. Jak je zpráva na posledním MTA (serveru) předá se MDA (mail delivery agent, lokální doručování v rámci jednoho serveru). Jakmile je zpráva uložena na lokálním serveru MUA příjemce si vyzvedne zprávu pomocí POP3/IMAP. Komunikace až na vyzvednutí zprávy probíhá přes SMTP.

Elektronická pošta obsahuje záhlaví (header, obsahují informace pro přenos, standardizovaný formát) a tělo zprávy (body, vlastní text). Protokol jako takový přenáší pouze sedmibitová data, překlad binárních dat nebo diakritiky zajišťuje rozšíření MIME.

SMTP (Simple Mail Transfer Protocol) je primární standard pro přenos emailů od klienta na server a mezi servery. Využívá TCP port 25. Je založený na komunikaci klient-server (poštovní server musí být klient i server). Klient zadává čtyřznakové příkazy a server odpovídá stavovými kódy. Nejčastěji se používá ESMTP (extended SMTP), které umožňuje přenos potvrzení o doručení zprávy.