John Oscar
PUBLISHING

ZÁKLADY POČÍTAČOVÝCH SÍTÍ

Předmět: *KIV/ZPS*
Školní rok: *2000/2001 ZS*
Přednášející: *Ing. Jiří Ledvina CSc.*

Jan Přibáň, 2000
john.oscar@post.cz

Vytvořeno programem MS Word 2000

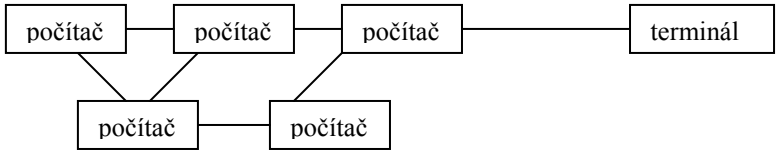
POČÍTAČOVÁ SÍŤ

- soubor počítačů a komunikačních prvků propojených komunikačními spoji

Historický vývoj

1. **Systémy vzdáleného přístupu**
- veškeré výpočty jsou uskutečňovány na vzdáleném počítači

2. **Počítačové sítě**
- počítačová siť umožňuje realizovat výpočet kdekoliv, nejen na jednom konkrétním počítači
- úloha jako celek běží většinou na jednom počítači ⇒ nutnost programového vybavení i dat nutných k řešení úlohy na tomto počítači



3. **Distribuované systémy**
- množina počítačů a terminálů
- výpočet neprobíhá pouze na jednom počítači, ale na několika najednou
- nutnost rozdělení úloh v síti

- většina dnešních sítí se pohybuje mezi jednotlivými vývojovými druhy počítačových sítí

Požadavky na počítačové sítě

- zvýšení spolehlivosti ⇒ v síti by porucha jedné komponenty neměla ovlivnit zbytek sítě
- zvýšení průchodnosti ⇒ více úloh v časovém intervalu
- zvýšení dostupnosti (nějaké služby)

Rozsah počítačových sítí

- v dnešní době počítačové sítě překonávají velké vzdálenosti a rozprostírají se na velké ploše naší planety

WAN – Wide Area Networks
- národní, nadnárodní a světové počítačové sítě ⇒ tisíce a stovky kilometrů
- využití současných infrastruktur ⇒ přenos dat a telefonních hovorů po jedné síti
- původní rychlost 100 kb/s dnes až 100 Mb/s

MAN – Metropolitan Area Networks
- sítě v městských oblastech a regionech ⇒ několik desítek kilometrů, např. v Plzni již 2 : sít Plzeňského magistrátu, WEB-NET ve vlastnictví ZČU
- propojení pomocí optických spojů a radiových směrových spojů
- rychlost přenosu až 100 Mb/s

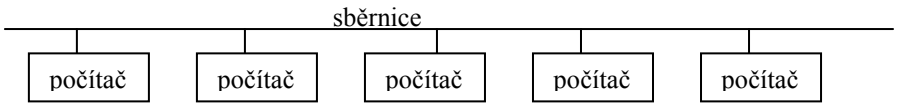
LAN – Local Area Networks
- počítačové sítě uvnitř budov a areálů ⇒ několik metrů až několik kilometrů
- většinou v majetku instituce, která je vytvořila
- využití speciálních spojení (kroucená dvoulinka, koaxiální kabel, optické vlákno) např. ETHERNET – 10 Mb/s, 100 Mb/s, 1 Gb/s

Topologie počítačových sítí

Spoje dvoubodové
- dva počítače vzájemně propojené mezi sebou, zejména v rozlehlých sítích, např. připojení z domova do počítačové sítě

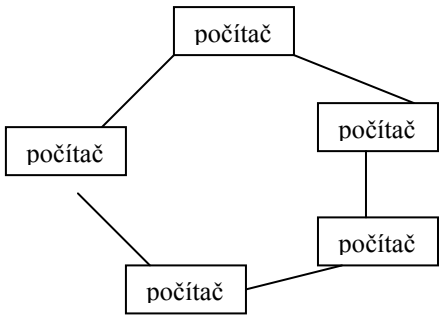
Spoje mnohabodové
- sběrnicové spoje
- zejména lokální počítačové sítě (LAN)

- *sběrnicové*

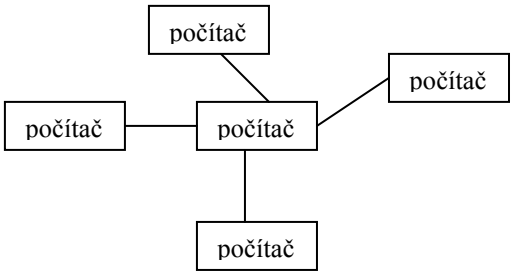


- *kruhové*

– zejména v LAN – sítě typu FDDI (100 Mb/s) nebo TOKEN RING (kvalitnější a dražší)

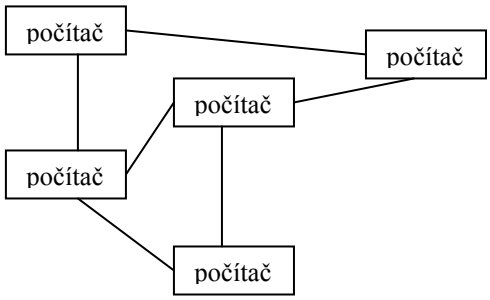


- *hvězdicové*



- *obecné*

- ve tvaru jakéhokoliv obecného grafu
- použití zejména v rozsáhlých sítích



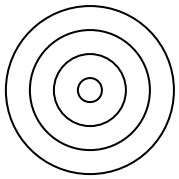
Komunikační média

Měděné vodiče (kroucená dvoulinka)

- 8 žil, několik druhů CAT3 – připojení telefonu(10 Mb/s), CAT5, CAT6 (100 Mb/s)
- proud ve vodiči teče oběma směry – tam i zpět ⇒ eliminace rušivých vlivů

Koaxiální kabel

- signál je veden vnitřním vodičem, opředení funguje jako uzemnění ⇒ stínění vnitřního vodiče



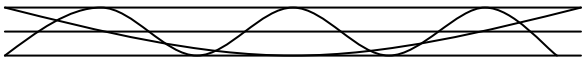
1. jádro – měděný drát
2. izolace
3. opředení měděným vodičem
4. vnější izolace

Optická vlákna

- výroba tažením ze speciálního skla, průměr 50 μm, délka až 1 km

konstantní index lomu

- skleněné vlákno je obaleno teflonem, který má jiný index lomu



- paprsky jsou vysílány pod různým úhlem
- každý paprsek tak letí jinak dlouhou cestu, potřebují k tomu jiné množství času⇒ omezení šířky pásma kvůli slévání ⇒ omezeno na 10 Mb/s

vlákno s proměnným indexem lomu
- při okrajích je vlákno „řidší“ ⇒ paprsek při okrajích letí rychleji, u středu pomaleji ⇒ celková dráha jednotlivých paprsků je různá ale čas je stejný
- omezení až na 1 Gb/s

Jednovidová vlákna
- průměr 2 μm, signál se šíří pouze středem
- rychlost až několik Gb/s
- výhodou je menší útlum signálu ⇒ možnost vedení na větší vzdálenosti (20-30 km)

Radiové spoje
všesměrové
- rozhlasové a televizní spoje
- nevýhodou je zabrání celého frekvenčního pásma

směrové
- signál se šíří v daném směru na vzdálenost až 30 km
- u počítačových sítí zejména toto použití ⇒ minimální výkon a maximální kapacita, minimální investiční náklady
- 2,5 GHz ⇒ 1 až 10 Mb/s

družicové
- vyšší přenosové frekvence asi 11 000 GHz
- využití geostacionárních družic (telefon, televize a počítačové sítě) – nevýhodou je veliká vzdálenost 40 000 km ⇒ zpoždění tedy 270 milisekund
- využití družic nízké oběžné dráhy – nevýhodou je nenulová rychlost oběhu družic nad zemí a natáčení parabol na povrchu zemském a výhodou malá vzdálenost, např. program IRIDIUM = systém 78 družic – použití u telefonních hovorů

Optické((laserové) spoje

Cíle počítačové sítě

- ✓ dovoluje sdílený přístup k výpočetním zdrojům
- ✓ dovoluje sdílený přístup k programům a datovým souborům
- ✓ medium pomocí kterého mohou geograficky rozptýlení uživatelé komunikovat (e-mail, teleconferencing apod.)
- ✓ elektronická obec – skupina uživatelů
- ✓ informační dálnice, národní informační struktura
- ✓ cyberprostor

Prvky počítačové sítě

- komunikační linky – dvoubodové nebo mnohabodové spoje
- vyrovnávací paměti
- sít – soubor uzlů (hostitelských systémů, směrovačů, bran) v jedné administrativní doméně
- intersít (internetwork) – soubor propojených sítí
- aktivní sítové prvky (počítače na kterých běží komunikační protokoly)

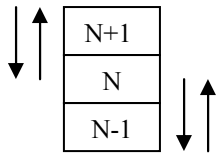
host - počítač, na kterém běží aplikace používající sít
opakovač - elektronické zařízení pro zesílení signálu
most - počítač propojující dvě a více fyzických sítí (propojení LAN + filtrování ⇒ signál může tak zůstat pouze v subsíti ⇒ snižuje to zatížení celé sítě)
směrovač - počítač, který směruje pakety mezi sítěmi
brána - směrovač, přímo připojený k více sítím, slouží k propojení nehomogenních sítí
switch - prvek nahrazující opakovač ⇒ propojí ty komponenty, které v danou chvíli spolu komunikují, né ostatní

Protokoly

- pravidla, podle kterých sítové komponenty vzájemně komunikují
- definují formáty vyměňovaných zpráv a akce spojené s přenosem zpráv mezi entitami
- protokoly známé z běžného života: řízení dopravy, komunikace lidí, problémy souběžného přístupu apod.
- telekomunikační společnost CCITT vytvořila nejprve protokoly v telekomunikačních sítích a poté se věnovala tvorbě protokolů v sítě počítačové

Úrovňová architektura

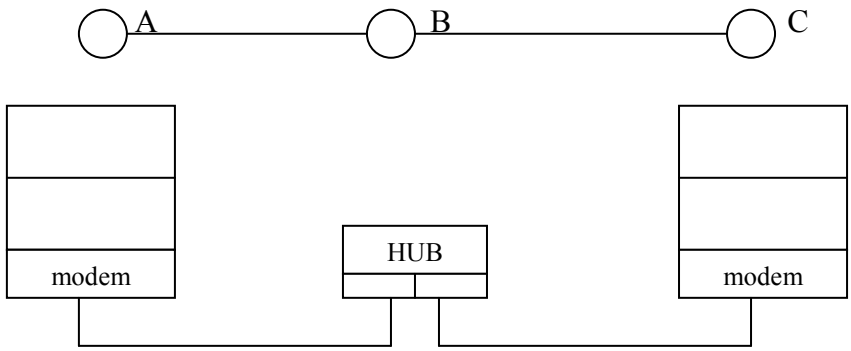
- architektura složitých systémů může být zjednodušena rozdělením do více úrovní
- úroveň N využívá služeb úrovně N-1 zajišťuje služby pro úroveň N+1



- služby poskytované nižší úrovni jsou nezávislé na tom, jak jsou tyto služby realizovány ⇒ skrytí složitosti nižších úrovní, změna úrovně N neovlivní ostatní úrovně
- rozhraní definuje jak lze službu využívat

Distribuovaná sítová architektura

- sít je složena z geograficky distribuovaných technických i programových komponent
- stejnorodé entity (např. procesy) na úrovni N poskytují služby komunikací (posíláním zpráv nebo paketů) sobě navzájem; používají při tom komunikační služby úrovně N-1
- logická kontrola fyzické komunikace



Relační model ISO/OSI

- ISO…….zkratka Mezinárodní organizace pro standardizaci
- OSI…….Open Systems Interconection (architektura pro propojování otevřených systémů)

- sedmiúrovňový model:

aplikační úroveň (7.)
- komunikace mezi procesy
- všechny existující úrovně podporují aplikační úroveň
- např. elektronická pošta, teleconferencing, www, ftp, telnet, distribuovaná databáze apod.

prezentační úroveň
- konverze dat do společného formátu
- komprese dat (ztrátová, bezztrátová)
- ochrana dat (šifrování)

relační úroveň
- spojení dvou aplikací pomocí relace
- vytvoření relace (ověřování)
- obnova po chybě
- sdílení relačního spojení

transportní úroveň
- univerzální transportní služby: přenos mezi koncovými procesy
- komunikace mezi koncovými uzly
- multiplexování toku dat z vyšších úrovní (možnost spuštění více aplikací)
- součást TCP/IP
- *spojované služby* – spojení dvou uzlů, srovnání rychlosti vysílače a přijímač; řízení toku dat; realizované služby jsou spolehlivé ⇒ přijímací strana se nemusí starat jak je služba uskutečňována

- *nespojované služby* – datagramové služby ⇒ posílání krátkých zpráv (datagramů) samostatně ⇒ tento systém nezaručuje přenos, neduplicitu apod. v případě posílání více datagramů; použití nejčastěji v systémech pracujících v reálném čase

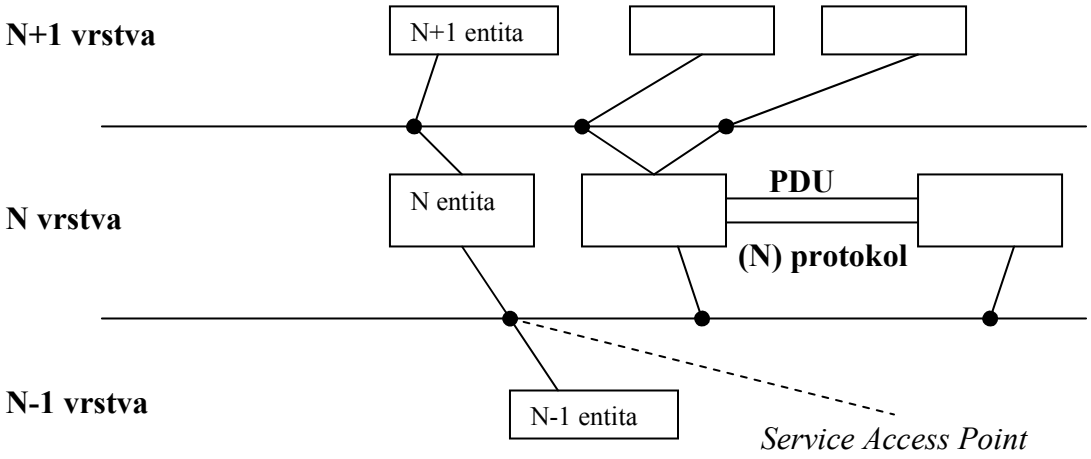
síťová úroveň
- přijímání paketů z vyšších úrovní a určení jejich cesty do koncových uzlů
- řízení směrování
- předcházení zahlcení a kolizím
- adresování v síti
  - ✓ *metoda škrticích paketů* – posílání protipaketů pro zpomalení sítě
  - ✓ *zahazování (odmítání) zpráv*

linková úroveň
- komunikace mezi dvěma sousedními uzly
- zajištění bezchybného přenosu ⇒ nejdůležitější úkol
- řízení rychlosti přenosu mezi sousedními uzly
- např. připojení z domova na Internet

ARQ (opakování vysílání chybně přijaté zprávy)
- s kladným potvrzováním – potvrzování každé dobře přijaté zprávy, mlčení znamená nepřijetí zprávy
- záporného potvrzování – ohlášení neporozumění (použití v pomalých systémech)
- kombinace obou – potvrzování úplně všech zpráv

FEC (metoda s dopředenou korekcí chyb)
- vysílání zpráv s dostatečnou redundantností (systém si dokáže odvodit správnou zprávu)
- použití zejména v mezipozemských přenosech

fyzická úroveň
- transporty jednotlivých bitů komunikačním vedením
- kódování přenášených informací



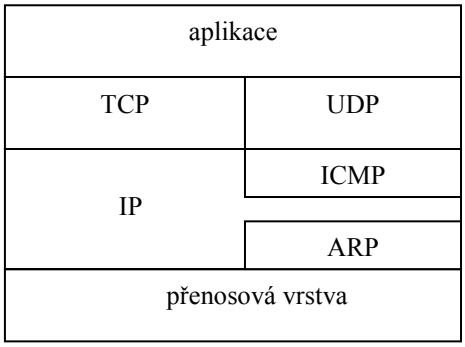
INTERNET

- byla velká snaha uvést sedmiúrovňový model v život, jenže bylo mnoho proti: nutnost celé řady protokolů, vysoké náklady, malá používanost
- americké ministerstvo obrany zadalo projekty univerzitám (zač 70. let), aby vymysleli systém pro posílení armády, jedním z úkolů byla také počítačová síť
- došlo k vytvoření modelu přenosu dat přepínáním paketů (rozdělení, posílání samostatně, opětovné spojování)
- koncem 70. let představení tohoto modelu veřejnosti ⇒ velký zájem univerzit podílet se na tomto projektu
- začátkem 80. let je už dost přípojných bodů, dochází k oddělení vojenské části
- počátkem 90. let komercionalizace ⇒ vznik Internetu

- Internet je postaven na přenosových protokolech z 70. let: **TCP/IP**
- TCP……Transport Control Protocol ……. 4. úroveň
- IP……Internet Protocol……3. úroveň

- Internet – celosvětová síť
- internet – propojení sítí s TCP/IP

-architektura TCP/IP:



fyzická + linková úroveň
přenosová vrstva – spolupráce se současnými schopnostmi, přenos informací z jednoho uzlu do druhého
síťová úroveň
ICMP……Internet Control Message Protocol – přenos řídících zpráv
ARP……..Adress Resolution Protocol – převod síťové adresy na fyzickou
transportní úroveň
UDP……..User Datagram Protocol – datagramové služby

Adresování v internetu

- každý objekt (PC) je označen jménem a jednoznačným identifikátorem (IP adresou)
- adresa je 32 bitové číslo v tečkové notaci (desítková čísla jsou oddělena tečkami) např. 147.228.67.23 toto je IP verze 4
- dnes už v důsledku počtu PC na celém světe IP verze 6 (modifikace), délka adresy již 128 bitové číslo ⇒ 4x delší, množství adres se zvětšilo 2^{96}

- IP adresy rozděleny do několika tříd:

Třída A
- první číslo síť, další tří čísla host
- maximálně může být 2^7 (mínus asi 7) sítí ⇒ asi tedy 115 sítí
- ve dvojkové soustavě tato třída má na začátku vyhrazenou 0 (např. 001101.011.0001.00011)

Třída B
- první dvě čísla síť, další dvě čísla host
- maximálně může být 2^{14} sítí a 2^{16} host
- ve dvojkové soustavě tato třída má na začátku vyhrazeno 01 (např. 011001.1001.01.01111101)
- tuto třídu má např. ZČU: 147.228.67.23

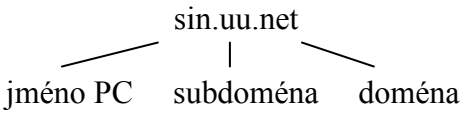
Třída C
- první tři čísla síť, poslední host
- maximálně může být 2^{21} sítí a 254 host
- ve dvojkové soustavě má tato třída vyhrazeno na začátku 110

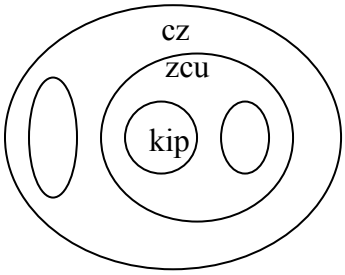
Třída D
- bez vnitřní struktury
- jedná se o skupinovou adresu ⇒ skupinové adresování ⇒ čím dál větší význam při přenosu v reálném čase např. u netrádia (nenavazuje se spojení s každým PC zvlášť, ale signál je šířen všem najednou)
- ve dvojkové soustavě má tato třída vyhrazeno na začátku 1110

Třída E
- tato třída používána při experimentech
- ve dvojkové soustavě má tato třída na začátku vyhrazeno 1111

Jména

- zavádí se kvůli srozumitelnosti a zapamatovatelnosti
- nemusí být jednoznačná
- na Internetu je zaveden hierarchický ***jmenný prostor***
- rozlišovací domény např.: edu, com, gov, mil, net,…..cz, sk, pl, hu

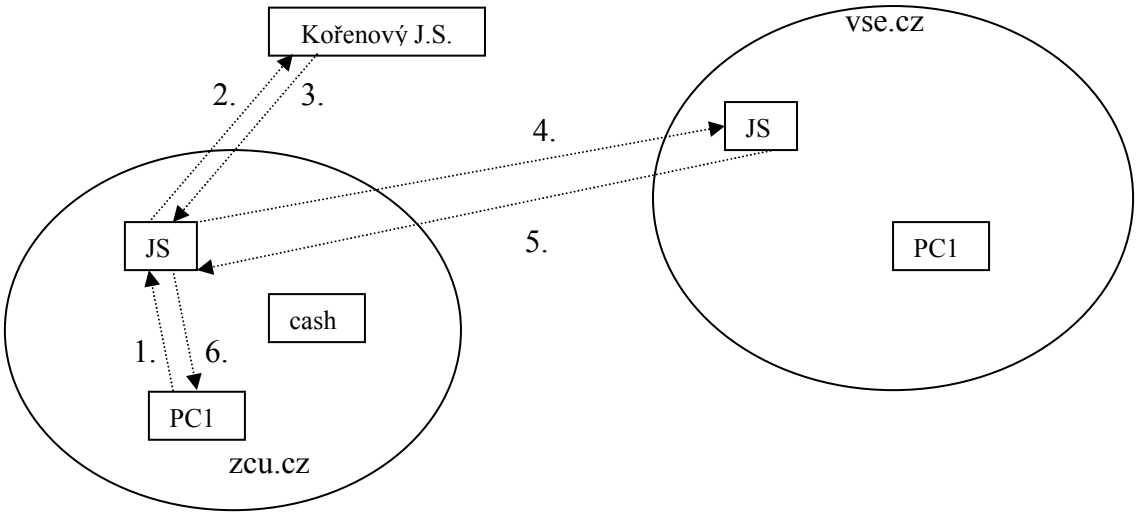




- převod mezi jménem a adresou:
  - jméno ⇒ adresa
  - adresa ⇒ jméno

- převod je prováděn decentralizovaně ⇒ decentralizovaný systém
- základ tvoří tzv. ***jmenné servery (JS)*** - uložené části databáze jmen
  - vytváří hierarchii
  - spolupráce při převodu
  - vyřízené dotazy si po dobu 1 dne ukládá do „cash“

- ***kořenové jmenné servery***
- ve světě jich je asi 7 – jejich zatížení je rovnoměrné
- jejich databáze jsou identické
-



Aliasy (přezdívky)

- funkční jména – většinou podle poskytovaných služeb
- jeden počítač tedy můžeme identifikovat podle: adresy, jména, několika alias

www.zcu.cz
ftp.zcu.cz aliasy jednoho PC
time.zcu.cz
gopher.zcu.cz

- převod nejen jména a adresy, ale i zjištění operačního systému, poštovního servru daného počítače atd.

APLIKAČNÍ ÚROVEŇ

Procesy

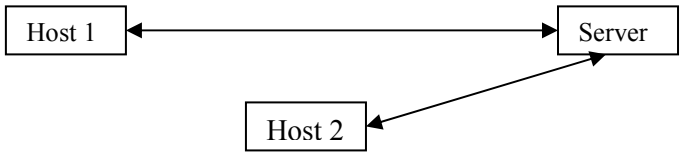
- **Proces**
- programový modul
- paměť
- data
- procesor
- **Modely**
- model server/klient
- model peer-to-peer ⇒ rovnoprávný (stejná funkce na všech komponentách)
- **Realizace servrů**
- podle služeb:
  - ✓ *datagramové* – pro aplikace jednotného charakteru, např. jmenné služby, čas apod.
  - ✓ *virtuální okruhy* – při přenášení velkého množství dat, kde záleží na bezchybném přenesení
- podle způsobu práce:
  - ✓ *interaktivní* – v jednu chvíli obhospodařují 1 požadavek
  - ✓ *procesně orientované* – vytvoření spec. procesu na uspokojení našeho požadavku a poté zrušení tohoto procesu; počet procesů je omezen (u ftp, gopher atd.)
- podle zapamatování stavu:
  - ✓ *stavový*
  - ✓ *bezstavový* – pamatují si stav rozpracovaní ⇒ pokračování práce tam, kde došlo k přerušení; server si nemusí nic pamatovat, informace o úplnosti posílá na hostitelský počítač

Typy servrů a služeb aplikační úrovně

Souborový server

- slouží k ukládání souborů na vybraném PC
- souborový systém se dělí na : svazky, adresáře, soubory
- možnost sdílení dat, ale nutnost vytvoření ověřovacích mechanismů uživatele a mechanismus přístupových práv k souborům

  R……čtení W…...zápis
  X……spuštění programu ….
- využití mapování disků k ztotožňování svazku s nějakou částí adresářového stromu disku na souborovém serveru



- typy: NOVEL v 5.x (Dos)
  NFS – Network File System (Unix)
  NTFS – NT File System (NT Server)
  AFS – Andrew File System (Orion)

Diskový server

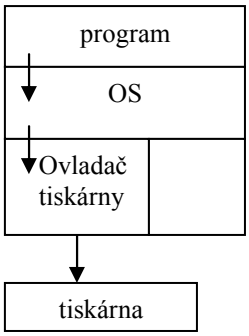
- dnes už se příliš nepoužívá
- přístup je pouze k celému disku, né pouze např. k jednomu souboru
- uživatelé tedy přistupují k disku jako celku
- výhodou větší jednoduchost přístupu
- nevýhodou je vytažení přístupových práv pouze na celý disk
- sdílené disky jsou pouze pro čtení, každý uživatel má pak pro čtení a zápis svůj vlastní disk

Tiskový server

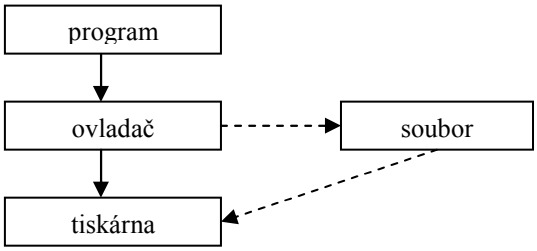
- realizování disků na společné tiskárně ⇒ síťové tiskárny

- ***lokální tisk***

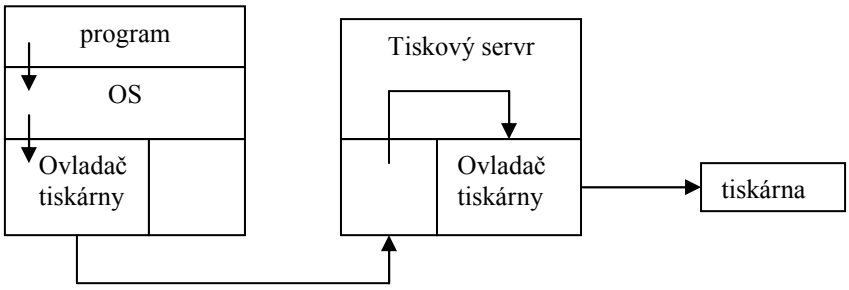
- text, který chceme vytisknout se nejprve převede do jazyka tiskárny a poté až je vytištěn



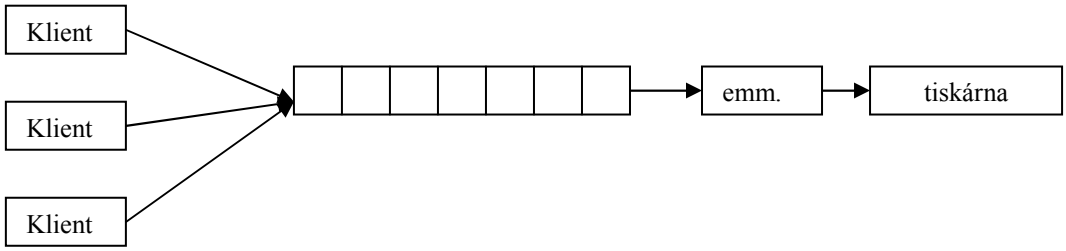
- jazyky: PostScript – univerzální jazyk, možnost uložení do souboru a až poté vytištění



- ***síťový tisk***



- síťový server obsluhuje více klientů současně ⇒ vznik *fronty*

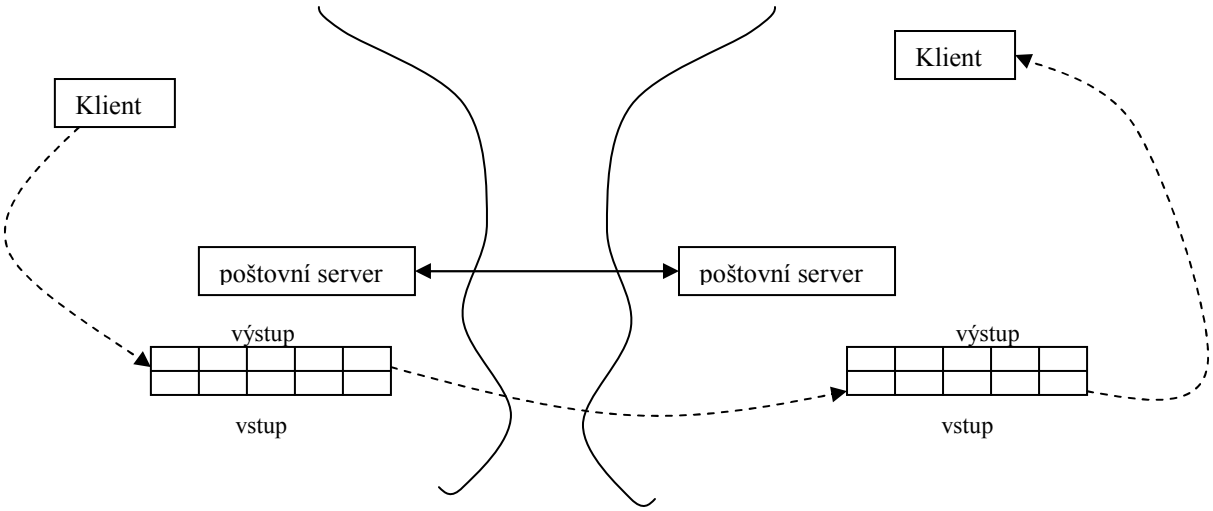


- požadavky na tisk se řadí tedy do fronty, kde existují následující stavy: vytváří se, připraven k tisku, tiskne se
- existují také příkazy např. na upřednostňování ve frontě, mazání z fronty apod.
- <u>přístup k tiskovému serveru:</u>
  - ✓ *přesměrováním* – převedení tisku na síťovou tiskárnu; v Novelu příkazy „capture, endcap“
  - ✓ *tisk souboru* – a) uložení tiskové sestavy do souboru
    b) kopírování souboru na tiskárnu (copy/b soubor.prn lpt2)

Poštovní server a elektronická pošta

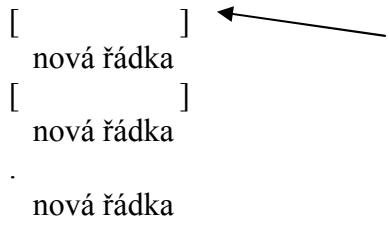
- slouží k přenosu zpráv v datovém režimu
- přenáší se :
  - text (původně) – ASCII znaky
  - formátované dokumenty (text) – např. .pdf (portable data formular)
  - zvuk ⇒ voicemail
  - obraz
  - video
  - data (programy) – binární data

- <u>funkce elektronické pošty:</u>



- k chybě může dojít např. přeplněním poštovního serveru

- formát přenášených zpráv:
- dvě základní části: záhlaví, data

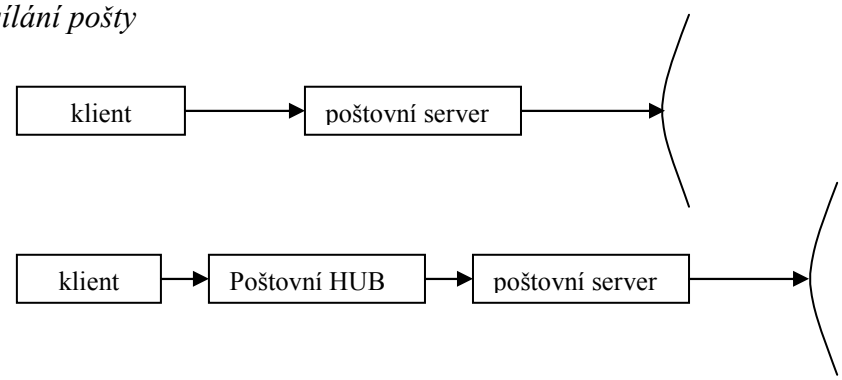


- adresy vypadají následovně: adresa@počítač.subdoména.doména
- poštovní servery umí pracovat s aliasy (přezdívkami)

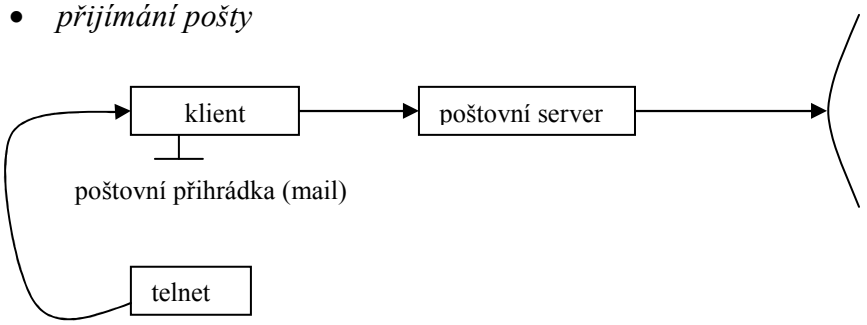
context transfer encoding – base 64 – kódování
context type – typ přenášené informace
- typ/podtyp např. text/plain, image/jpg, aplication/msword ……

- MIME – Multipurpose Information Mail Exchange

- prostředky pro přístup k elektronické poště:
  - *odesílání pošty*

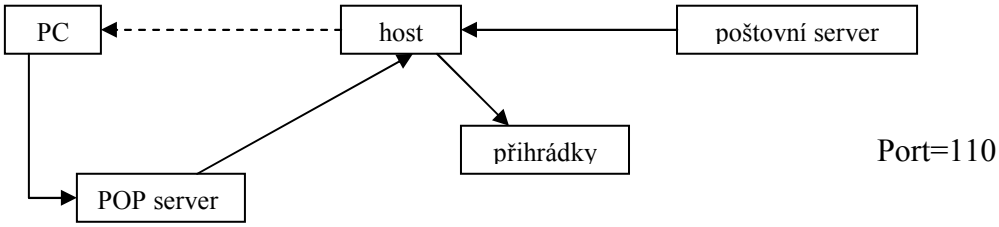


  - *přijímání pošty*



…..programy: pine, elm ….umí manipulovat se soubory v pošt. adresáři

- vzdálený přístup k elektronické poště:
  - ✓ ***POP – Post Office Protocol***

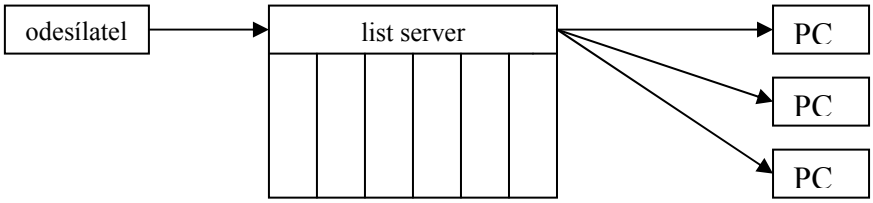


    - na PC běží tzv. POP klient
    - název POP servru ZČU je pop.zcu.cz
    - příkazy pro telnet: user, pass, list, retr, quit, dele

  - ✓ ***IMAP – Internet Mail Access Protocol***
    - funguje obdobně, ale umožňuje pracovat s poštou i částečně: přenesení autorů zpráv, věcí apod.

List server - Elektronická konference

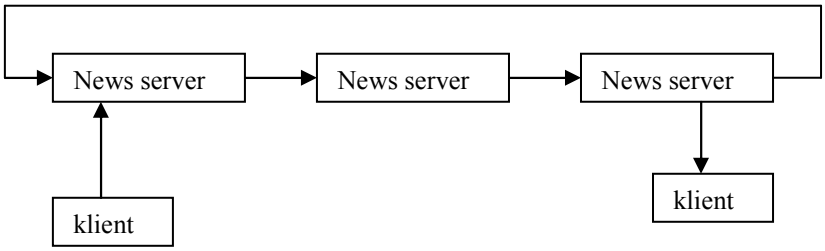
- vytvoření zájmových skupin a těmto pak rozesílání zpráv (příspěvků) od různých členů ⇒ např. server list.zcu.cz
  - *uzavřené*
  - *otevřené*
    - druhé členění na:
  - *moderované*
  - *nemoderované*



- komunikace:
  - ✓ ***administrativní (řídící) kanál***
    - umožňuje přihlášení, odhlášení, pozastavení a obnovení členství, výpis seznamu konferencí, seznamu členů, help
    - např. listserver@list.zcu.cz, majordomo@….., název konference-request@….
  - ✓ ***datový kanál***
    - samotný přenos zpráv
    - např. webnet@list.zcu.cz

News server - Elektronické news

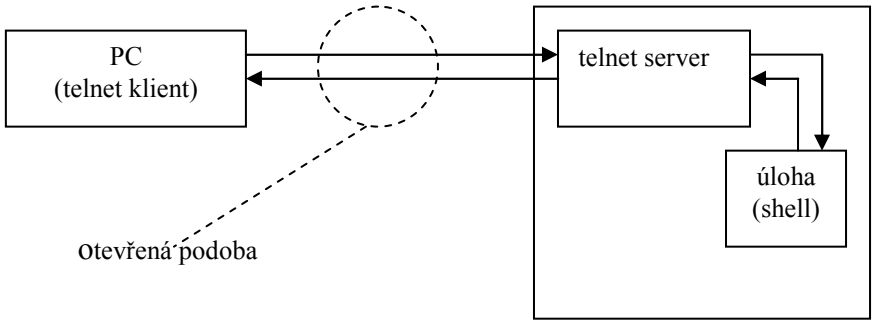
- zaslané příspěvky se pouze ukládají na servery, na kterých je možné si je přečíst ⇒ nedochází k odesílání klientům



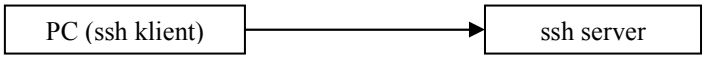
Služby aplikační úrovně

- telnet, ftp, gopher, www, finger, netfind, whois, X500, videokonference, time servery

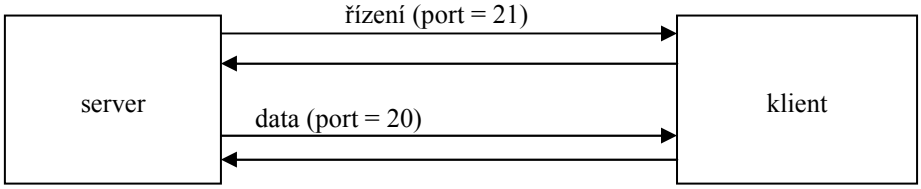
- **TELNET – vzdálený terminál**
- jedná se v podstatě o emulaci terminálu
  - ✓ navázání spojení
  - ✓ dohodovací fáze (určení typu terminálu)
  - ✓ přenos dat
  - ✓ ukončení spojení
- historicky různé typy terminálů: VT100, VT320… (čím větší číslo tím dokonalejší)
- služba telnetu je implicitně přístupná přes port = 23
- znaky na telnet klientovi se zobrazují na obrazovce až po vrácení z telnet servru



- proti odzírání ve formě otevřené podoby se používá ***ssh –secured shell*** ⇒ prostředek umožňující normální funkce, ale v šifrované podobě; použití port = 22



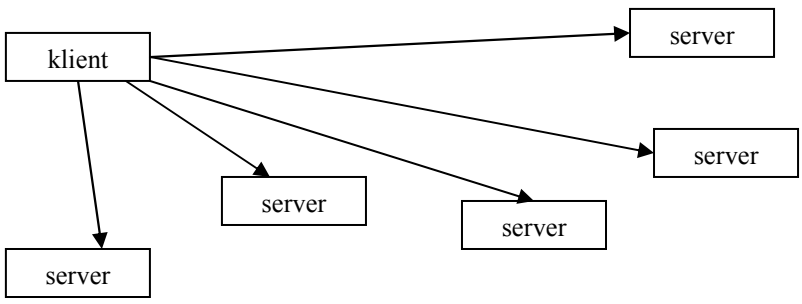
- **FTP – File Transfer protocol**
  - ✓ navázání spojení
  - ✓ přenos příkazů
  - ✓ přenos dat (příkazy: dir, get, ls, put, cd, mget, mput, bye)
  - ✓ ukončení spojení



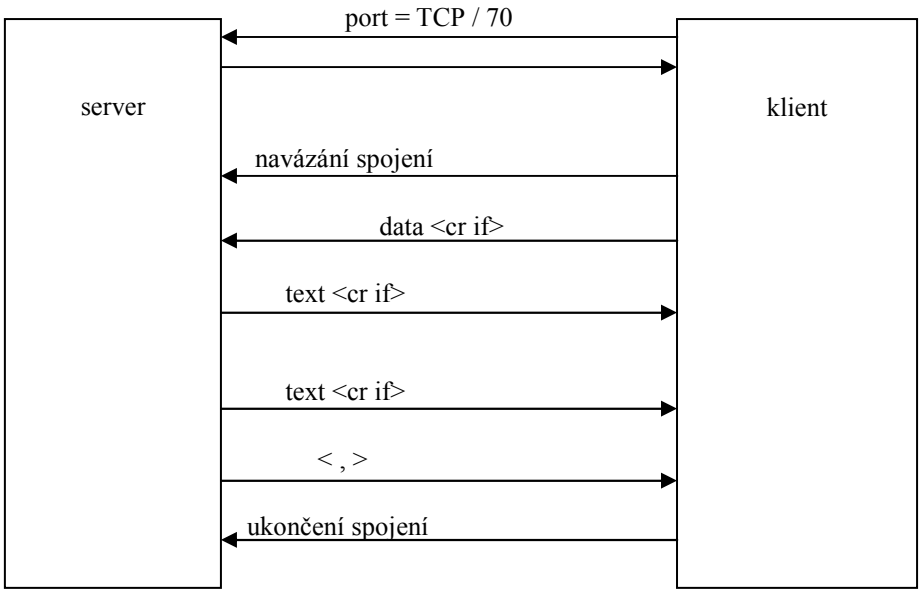
bin…….čtení souborů binárně
ascii……...čtení textových souborů
promt…….přepínač, zapíná/vypínání dotazů
hash……zobrazování křížku za každý přenesený kb
!……..ovládání v našem vlastním adresáři
lcd……..změna domácího adresáře

- ftp souborů je ve světě hodně
- zvláštní formou jsou pak indexové servry ⇒ *archie servry* (jméno programu a místo uložení)

- **GOPHER**
  - typy informací:
    - ***adresáře***
      - chápáno jako seznam dokumentů
      - prohlížení informace
      - uspořádání do skupin podle typu informace
    - ***link***
      - adresování adresářů na cizích strojích
    - ***textové soubory***
    - ***prohledávání pošty***
      - spec. typ adresáře
      - specifikace klíčových slov pro vyhledávání
    - ***telefonní seznam (speciální aplikace)***
    - ***telnet relace (přihlášení na jiný stroj)***
    - ***multimédia (obrázky, zvuk, video)***
    - ***formátovaný text (postscrip)***



- protokol:



- přenášená data:

<typ> <text> <sektor> <adresa hosta> <port>

0....soubor	7....prohledávání	g.....gif soubor
1....adresář	9…binární soubor	….
2…telefonní seznam	8…telnet	

- nevýhoda: samy musíme prohledávat jednotlivé servry a jednotlivé adresáře

- **WWW server**
  - TCP port 80
  - hypertextové spojení s dokumenty
  - přenos textu, souborů, obrazů, zvuků, videa apod.
  - systém dotazovacích servrů

  - základní pojmy:
    HTTP – Hypertext Transfer Protocol
    - kromě zobrazitelných znaků obsahuje i další odkazy na související text

    HTML – Hypertext Markup Language
    - obsahuje řídící znaky a texty
    - obsahuje formáty a odkazy

    URL – Uniform Resource Locator
    - *schéma: //jméno:heslo@počítač:port-cesta k souboru?parametr*
    - schéma: http, shttp, ftp, telnet, gopher, news, mailto, file
    - parametr: parametry předávané úloze běžící na servru

- URL může být lokální (do téhož dokumentu…#), nebo globální; může také být absolutní nebo relativní (obsah se doplňuje automaticky, není vázáno k určitému paměťovému médiu)

- ***SERVER*** – http server ⇒ relativně jednoduchý
- ***KLIENT*** – relativně složitý, univerzální

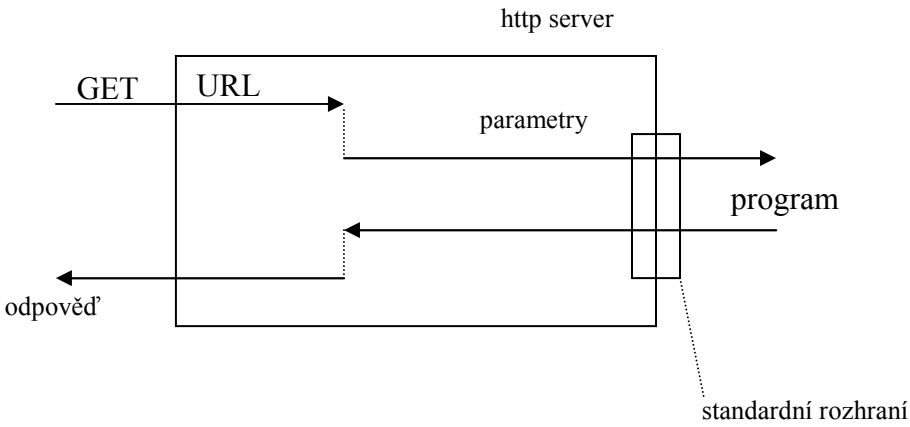
- <u>formát přenášených dat:</u>

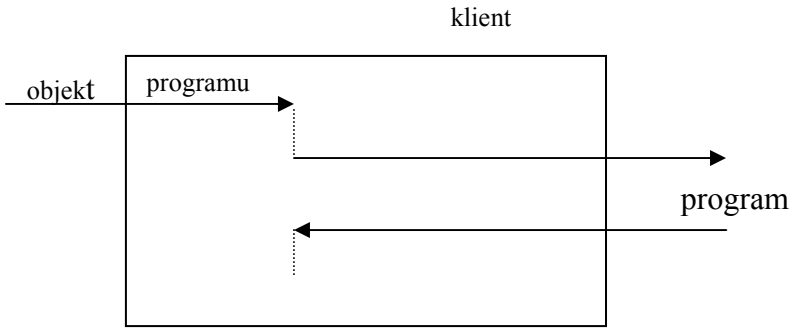
```
<HTML>
  <HEAD>          záhlaví…autorská práva, vypršení platnosti, kódování
  </HEAD>
  <BODY>
  </BODY>         vlastní tělo….vlastní stránka
</HTML>
```

…… značky v dokumentu buď párové nebo nepárové (např. <p>)

- <u>protokol:</u>
- různé metody
- HEAD – klient požaduje zaslání hlavičky dokumentu ⇒ optimalizace přenosu
- GET – dovoluje vyžádat si nějaký dokument, za ? parametry (omezení)
- POST – neomezený počet parametrů – server zpracovává jiným způsobem
- PUT – umožňuje zapsat stánku na server
- DELETE – mazání

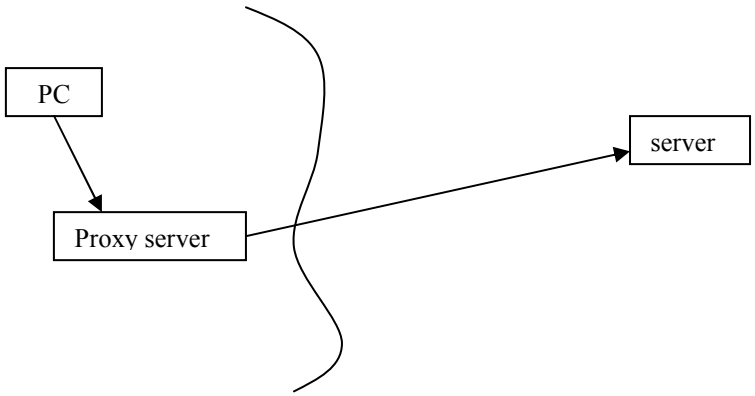
- <u>dokumenty (html stránky):</u>
  - **statické** – soubory předem vytvořené přenášené do počítače
  - **dynamicky vytvářené** – podle aktuálního požadavku uživatele
    - vyžadují existenci programu pro vytvoření té podoby stránky jak na straně servru, tak i na straně klienta
    - používání CGI skriptu „Common Gateway Interface“ – jazyk vyšší úrovně (většinou interpretační) – PHP, Perl



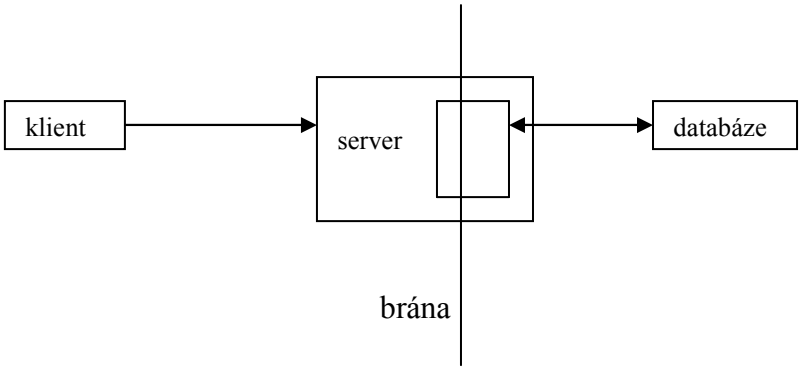


Java skript

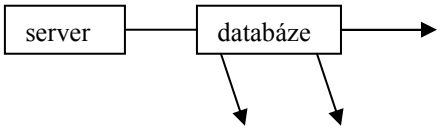
- problémy:
- vyžaduje přenos velkého objemu dat ⇒ zavedení vyrovnávacích pamětí (cash)
- tyto vyrovnávací paměti jsou uložené v mezilehlých uzlech ⇒ proxy servry (zástupné)
- možnost filtrace, a kontroly práce na síti (problémem např. v bankovnictví)



- brány:
- umožnění komunikace, překlad do html a přesun klientům
- např. netfind, whois, protokoly

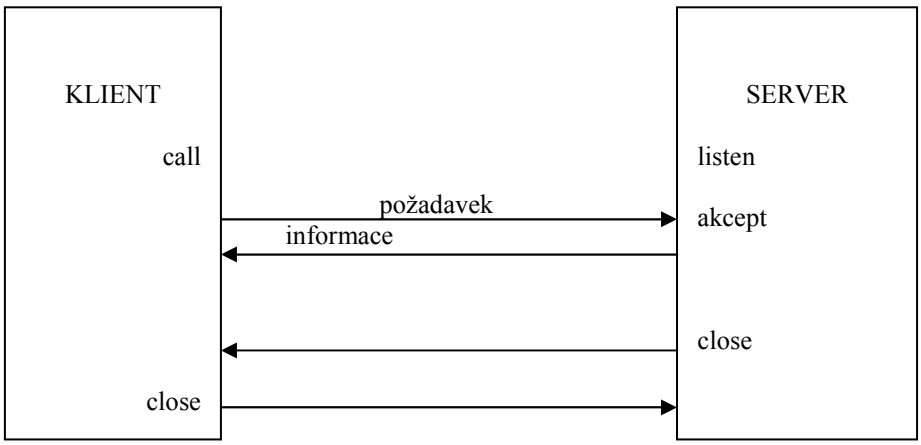


- prohledávání:
- roboti, spider
- server – shromažďuje informace formou registrace



- jazyk dokumentů – zadávání klíčových slov, vytváření logických výrazů: AND, NOT, OR, NEAR apod.
- portál – odkazy roztříděny podle skupin

- **FINGER**
  - získávání informací o uživatelích vzdáleného systému
  - textově orientovaný protokol
  - protokol TCP port = 79
  - architektura server/klient



- požadavek:
  - ✓ jméno uživatele
  - ✓ přihlašovací jméno uživatele

  + @jméno hosta

- informace:
  - ✓ výpis informací o uživateli
  - ✓ výpis informací o přihlášených uživatelích

  např. <cr><lf> <jmeno>@stroj<cr><cf>
  /w <cr><lf> @stroj <cr><lf>

- **NETFIND**
  - získávání informací o uživatelích nějaké domény
  - ve světě několik servrů, které podporují tudle službu (většinou podle pro jednotlivé státy, např. u nás: netfind.vslib.cz
  - přístup k této službě pomocí telnetu nebo bránou přes http protokol

    telnet netfind.vslib.cz
    login: netfind
    pass: netfind

    zadání dotazu - jméno subdoména doména
    Novak zcu cz

- **WHOIS**
  - prostřednictvím centralizované databáze poskytuje tato služba informace o zaregistrovaných uživatelích
  - interaktivní prostředí, ve kterém pak pomocí dotazů získáváme informaci o nějakém člověku

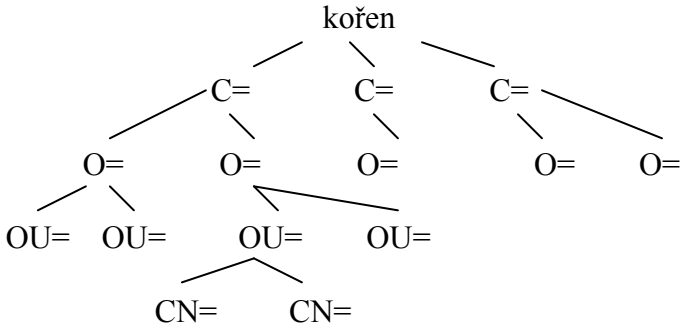
- **X500**
  - následníkem služby „whois“
  - tzv. directory services – adresářová služba
  - dovoluje získávat informace o nějakých objektech umístěných v decentralizovaných databázích
  - 2 složky:
    vlastní protokol
    - relativně velmi jednoduchý
    - operace charakteru: prohlédni, přečti, zapiš, porovnej, zruš, modifikuj..

    vlastní databáze
    - adresný prostor objektů ⇒ objektům jsou přiřazeny atributy ⇒ hierarchický systém objektů

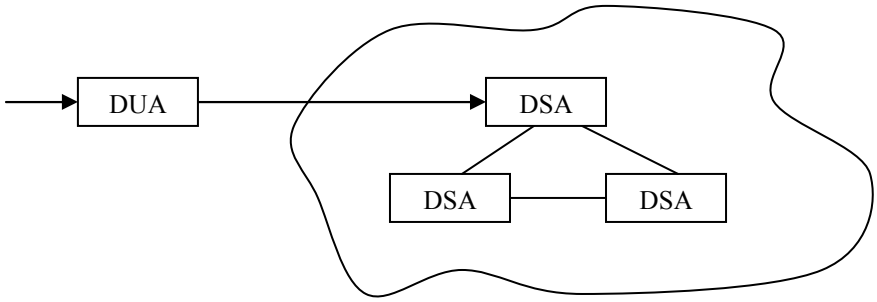
atributy: jméno=hodnota

0…….jméno organizace	SA……..street adress
OU….organizační jednotka	L……lokalita
C……země	CN……..označení objektu

[C=CZ, O=ZCU, OU=KIV, CN=…]

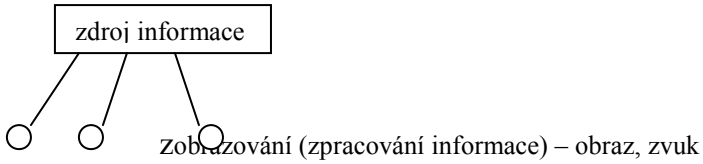


- vyhledávání (2 komponenty):
  - ✓ ***DUA –Directory User Agent***
  - ✓ ***DSA – Directory System Agent***



- realizace:
- vytvořen protokol pro zjednodušování ***LDAP Lightweight Directory Access Protocol*** ⇒ přístup k adresářovým službám

- **VIDEOKONFERENCE**
  - přenos obrazu a zvuku
  - internetové radio, internetová televize, videokonference

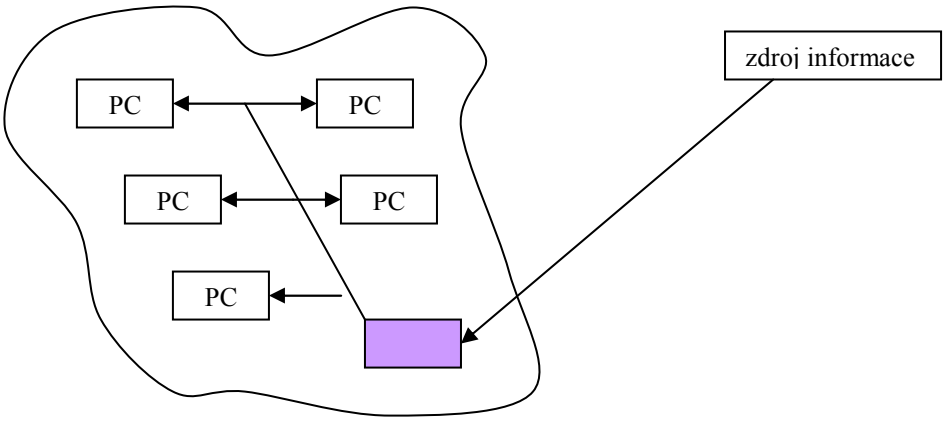


- např. *Net Meeting* – výměna informací mezi 2 účastníky ⇒ obraz, zvuk, obrázky (white board), textová informace

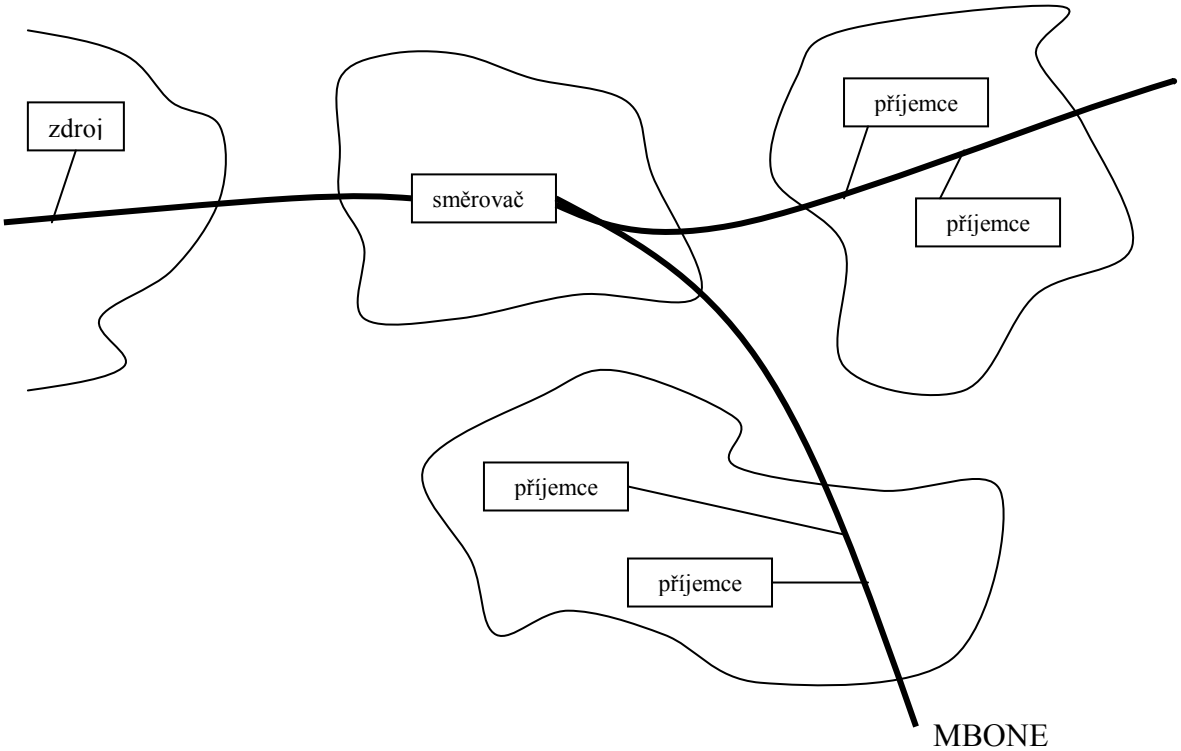
- požadavky na přenosové kapacity:
- zvuk v kvalitě audio CD, stereo 44,1 KHz ⇒ 1,411 Mb/s
- obraz 768x576 b, 25 frames, 24 b/na 1 bod ⇒ 33 MB/s

- komprese dat:
- ***Motion Picture Expert Group***
- MPEG1 – 352x288 b, 25 frames ⇒ 1,5 Mb/s
- MPEG 2 – 768x576 b,25 frames ⇒ 2-10 Mb/s (komprese 1:30 - 1:200)
- MPEG 4 – 176x144 b,10 frames ⇒ 64 kb/s

- pro přenos multimediálních dat je nutná kvalitní infrastruktura
- přenos obrazové a zvukové informace se realizuje pomocí tzv. **skupinového adresování** ⇒ skupina počítačů má stejnou skupinovou adresu
- dochází tak k přenosu 1:N

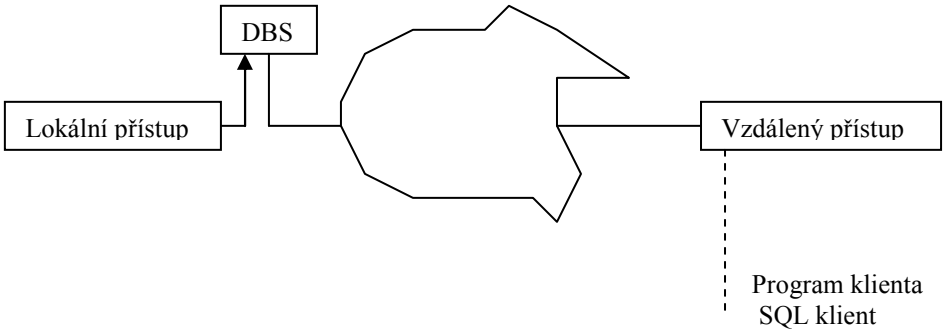


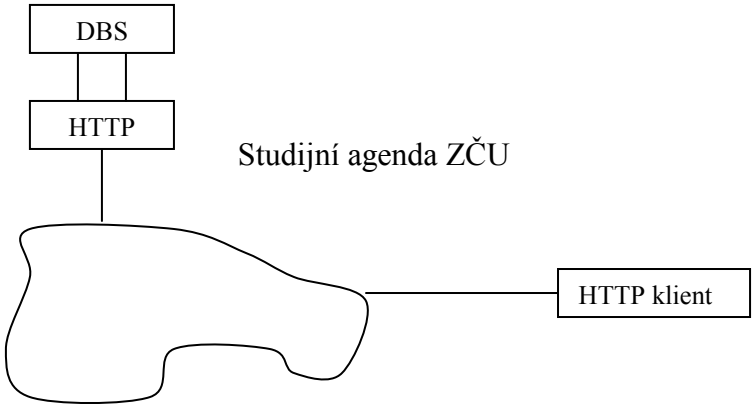
- využívání tzv. ***MBONE*** **–** páteřních sítí pro přenos skupinových dat (dat na skupinové adresy)
- realizováno nad sítí Internet
- nutná celá řada směrovačů ⇒ nutnost tedy dovybavit sítě prostředky pro skupinové směrování
- výhodou je možnost využití již stávající infrastruktury
- nutností je také zajistit synchronní přenos dat ⇒ vysílací rychlost musí být stejná jako rychlost přijímací (např. řešeno pomocí načítání do „bufferů“)
- přijatelné je pouze zpoždění



- **ČAS, ČASOVÉ SERVERY**
  - pro připojení do počítačové sítě dochází k synchronizaci času mezi naším počítačem a servrem, ke kterému se připojujeme
  - u rozsáhlých sítí je to složitější ⇒ existují časové servry, které poskytují přesný čas (buď získaný z jiného časového servru, nebo přímo z časového etalonu – atomové hodiny, signál šířený dlouhými radiovými vlnami)

- **DATABÁZOVÉ SERVERY**
  - jazykem pro přístup k databázím je ***SQL- Structure Query Language***
  - unifikovaný přístup

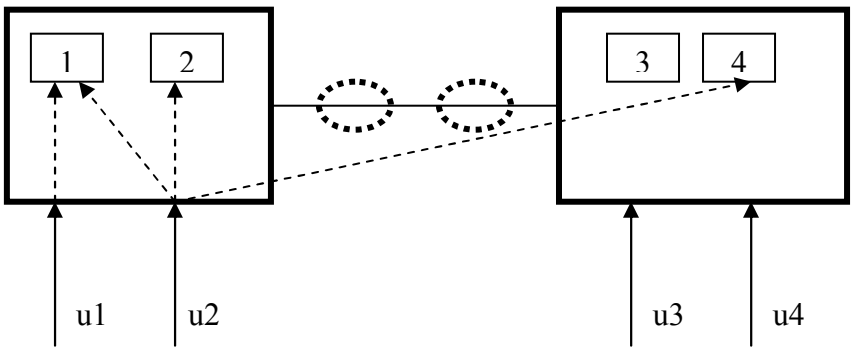




  - ***síťový management*** – prostředky pro diagnostiku a sledování dění na síti

BEZPEČNOST POČÍTAČOVÉ SÍTĚ

- počítačová síť je otevřená
  - nebezpečí napadení počítačové sítě i jednotlivých počítačů
  - nebezpečí odposlechu přenášených informací



….ochrana uvnitř systému, vstupu do systému
….ochrana komunikačních cest

- napadení:
- ***aktivní*** – modifikace, zadržování dat (komunikace)
- ***pasivní*** – odezírání
- hlavními příčinami většinou odhadnutí hesel nebo napadení cest

- šifrování:
- ***symetrické šifry*** – jeden klíč pro šifrování a dešifrování ⇒ rychlé
- ***nesymetrické šifry*** – dvojice klíčů, pro šifrování je veřejný, druhý neveřejný
- musí být nemožné odvodit šifrovací klíč

$$\text{text} \longrightarrow K=f_E(T) \longrightarrow T=g_E(U)$$

  - DES – USA, šifrování vládních dokumentů – klíč 56 bitů
  - 3DES – trojnásobné použití klíče DES – klíč 112 bitů
  - SAFER

- útoky na počítačovou síť:
  - ***pasivní***
    - kradení/únik informace – získávání obsahu zprávy
    - analýza přenosu – odkud, kam, délka bloků, množství dat
  - ***aktivní***
    - modifikace toku dat – změna obsahu, opakování, změna pořadí, rušení, vkládání, syntéza zpráv, změna adresy, změna dat, modifikace požadované informace
    - blokování přenosu mezi dvěma entitami
    - zadržování – zpožděné odesílání zpráv
    - vytváření falešného spojení (maskování se) – autorizace entit, časová integrita

- cíle zabezpečení:
- prevence pasivního útoku
- detekce aktivního útoku

Ohodnocení bezpečnosti

- existuje více způsobů ohodnocení bezpečnosti
- jedním z nich je ***TCB- Trusted Computing Base***
- uvedeno v ***Orange Book – The Trusted Computer Evolution Criteria***

  - úplný ochranný mechanismus ve výpočetních systémech
  - zahrnuje software, hardware, firmware
  - podpora výrobců spolehlivých operačních systémů

- vlastní klasifikace – rozdělení do 4 skupin:

  skupina D
  - bez zajištění bezpečnosti – minimální ochrana (MS-DOS)

  skupina C
  - volná ochrana – ponecháno na uvážení
  - např. systémy založené na ověřování uživatele

  skupina B
  - nařízená, vymezená ochrana

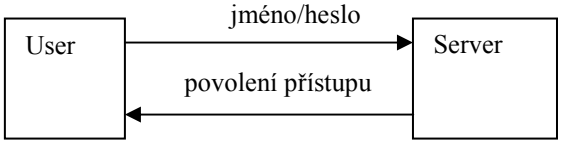
  skupina A
  - verifikovaná ochrana
  - vyžaduje úplný formální návrh systému
  - orientováno na klasifikaci informace

Zajištění bezpečnosti

- ověřování uživatele……přístup do výpočetních systémů
- zabezpečení přenosu……..šifrování, „kontrolní součet“ ⇒ proti změnám
- zabezpečení nepopiratelnosti…….elektronický podpis

1. *Ověřování uživatele heslem*

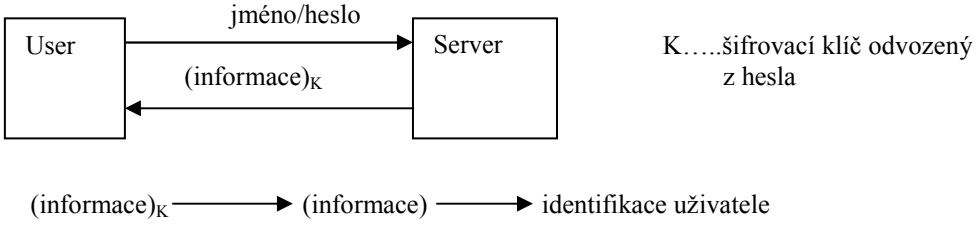
- jednoduché ověření
- nevýhodou je přenos jména a hesla v otevřené podobě



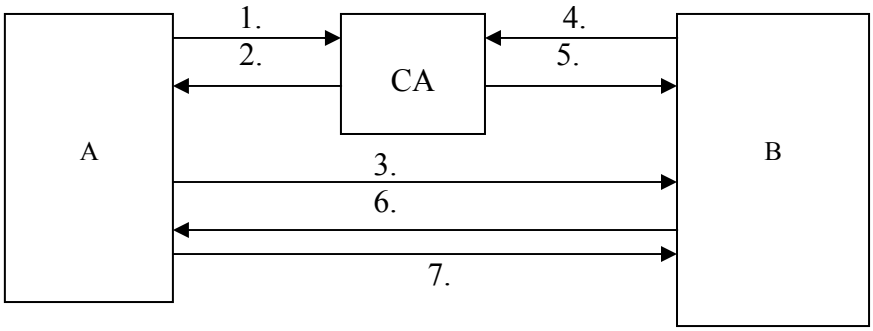
Login	Pass
Honza	Blb
lumir	vlk

- možnost přenosu hesla a jména v zašifrované podobě ⇒ SSH

2. ***Ověřování uživatele pomocí ověřovacího serveru***
   - ověřovací server = bezpečný počítač
   - udržuje databázi uživatelů a jejich hesel
   - přenos relačního klíče – šifrovací klíč pro komunikaci
   - KERBEROS – systém používaný v systému OrionNT



3. ***Ověřování uživatele pomocí certifikační autority (CA)***
   - nejmodernější způsob identifikace subjektů



   - CA vystaví každému subjektu tzv. certifikát: (x.509)

CA – ID
Doba platnosti
Subjekt ID
Subjekt – Kv (veřejný klíč)
Podpis CA

L O K Á L N Í P O Č Í T A Č O V É S Í T Ě

- rozloha 1 – 10 km
- většinou jeden vlastník
- vyhrazené komunikační médium (kroucená dvoulinka, koaxial, optické vlákno, radiové spoje)
- přenosová rychlost: 10 Mb/s – 1 Gb/s
- topologie: sběrnicová, kruhová topologie, hvězdicová topologie

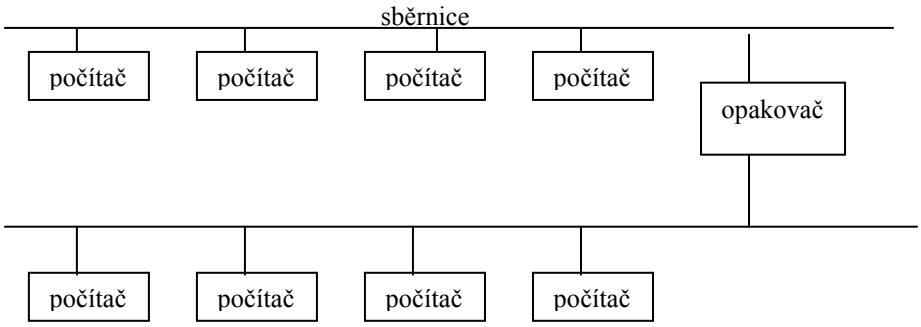
- řízení přístupu ke komunikačnímu médiu:
  - ***centralizované –*** nepoužívá se – metoda výběru, metoda výzvy
  - ***decentralizované*** – větší spolehlivost, snížení režie

    a. **metody náhodné**
       - předpokládají kolize při přenosu, není ochrana proti zahlcení
       - opakování zprávy po opakování náhodné doby
       - metody naléhající – ihned po přestání začne rychlá, velké nebezpečí kolize, může vést k zahlcení sítě (neustálé skákání si do řeči)
       - metody nenaléhající – automatické přeplánování na pozdější dobu, méně agresivní, pomalá, malé nebezpečí kolize, nedojde k zahlcení sítě
    b. **metody rovnoměrného přístupu**
    c. **metody prioritní**

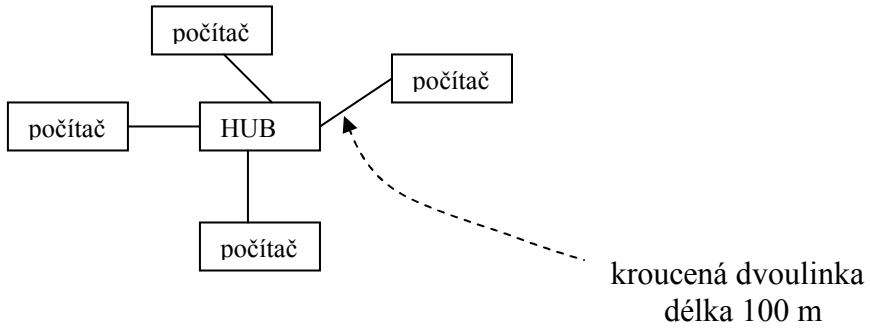
Příklady LAN

- **ETHERNET**

- vznik začátkem 80. let
- na vývoji se podíleli firmy: INTEL, XEROX, DEC
- vychází z metod náhodného přístupu – metoda CSMA-CD – naslouchání nosné vlny + detekce kolize
- snaha o zvýšení propustnosti sítě ⇒ přenosové rychlosti
- topologie: sběrnicová, hvězdicová, stromová



- nesmí dojít ke vzniku smyček !!!!!



- HUB – rozbočovač – 8, 16, 24…..vstupů

- přenosová rychlost – 10 Mb/s, 100 Mb/s, 1 Gb/s (páteřní sítě), 10 Gb/s (ve vývoji)
- komunikační médium – koaxiální kabel, kroucená dvoulinka, optické vlákno

- typy:
  - ***10 BASE 5*** - 10 Mb/s, základní pásmo, 500 m dlouhý segment
  - ***10 BASE 2*** - cheaper net, 200 m, koaxial, začátkem 90. let
  - ***10 BASE T*** - twist – kroucená dvoulinka, ELIE 45 – 200 m až 1 km
  - ***10 BASE F*** - optické vlákno

  - ***100 BASE Tx*** - 100 Mb/s, kroucená dvoulinka CAT 5
  - ***100 BASE Fx*** - 100 Mb/s, optické vlákno
  - ***100 BASE T4*** - 4 páry vodičů ⇒ speciální modulační metoda

  - ***1000 BASE T*** - 1 Gb/s, kroucená dvoulinka
  - ***1000 BASE F*** - 1 Gb/s, optické vlákno

- adresování v Ethernetu:
  - **individuální –** délka 48 bitů (6 slabik) – 24 bitů výrobce, 24 bitů další rozlišení; jedinečná
  - **všeobecná –** 48 bitů – samé 1….1, slyšení zprávy všemi stanicemi najednou; použití např. pro šíření výzev apod.
  - **skupinová** – (1x…….x), adresování skupin stanic

  - délka přenášených dat – 46-1500 slabik
  - v 1 segmentu max 100 stanic

- **TOKEN RING**

- fyzický kruh – kruhová síť s předáváním pověření
- odposlouchává pouze příslušný počítač
- metoda přenosu – předávání pověření – metoda rovnoměrného přístupu ⇒ bez kolizí
- rychlost přenosu – 4 Mb/s (stejná propustnost jako 10 Mb/s Ethernet), 16 Mb/s
- maximální počet stanic 250
- médium – kroucená dvoulinka
- adresa – 48 bit – individuální, všeobecné a skupinové adresování
- délka paketu – 4 099 slabik
- 1985 – velký úspěch – 20 % na trhu
- do ČR se moc nedostal, pro svojí cenu
- použití tam, kde je třeba nezahlcujících se sítí – např. banky, Škoda MB

- **FDDI (Fibre Data Distributed Interface)**

- optická síť
- realizováno dvojitým kruhem (kruhová topologie) ⇒ primární a záložní
- rozlehlost 100 km
- rychlost přenosu 100 Mb/s
- zařízení buď ***plné připojení*** (DUAL ATTACHMENT) nebo ***připojení pouze k primárnímu okruhu*** (SINGLE ATTACHMENT)
- použití jako páteřní sítě, metropolitní sítě ⇒ připojení významných serverů
- rychlé připojení pracovních stanic
- délka paketu 5 kB
- vysoká odolnost proti výpadkům ⇒ v případě poruchy se síť automaticky překonfiguruje a začne používat sekundární okruh

- **DALŠÍ**

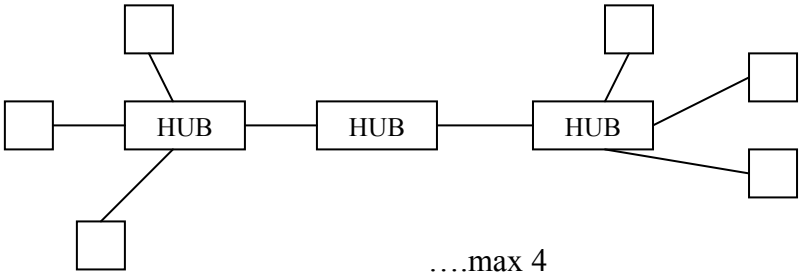
Standardizace protokolů lokální počítačové sítě

ISO…….ISO 8802
IEEE…….. IEEE 802

802.3…….Ethernet
802.5…….Token Ring
802.12……...100 GU AnyLAN…….HP síť 100 Mb/s, telefonní vedení

Propojení lokálních počítačových sítí

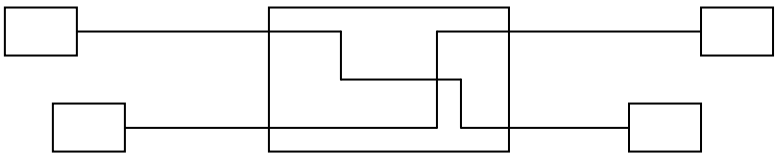
Rozbočovače (opakovače) HUB



….max 4

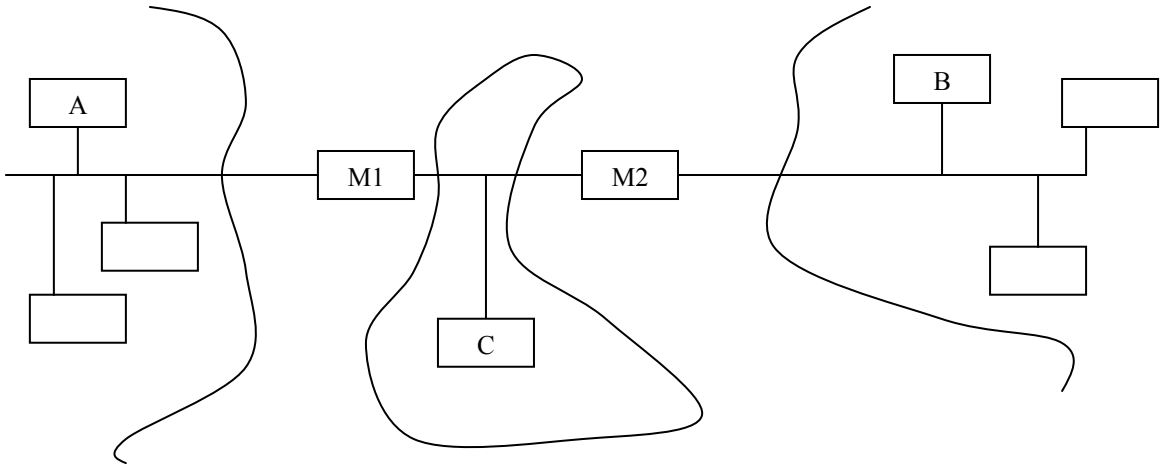
Přepínače (switch)

- propojuje pouze stanice, které spolu mají komunikovat
- zvýšení výkonu, méně kolizí

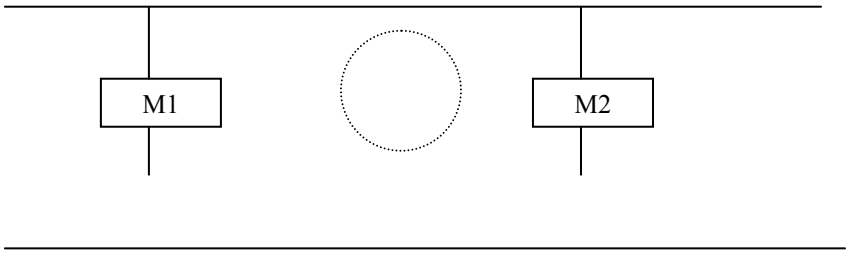


Mosty(bridge)

- oddělují jednotlivé LAN
- filtrují přenos paketů podle adresy
- mají 3 funkce: propouštění, filtrování, učení/zapomínání



- nesmí vznikat smyčky ⇒ nesmí dojít k zacyklení
- příklad umístění dvou mostů (z důvodu zálohování)
- použití ***spaning tree algoritmu*** – odpojení mostů vytvářejících smyčku + kontrola připojení všech



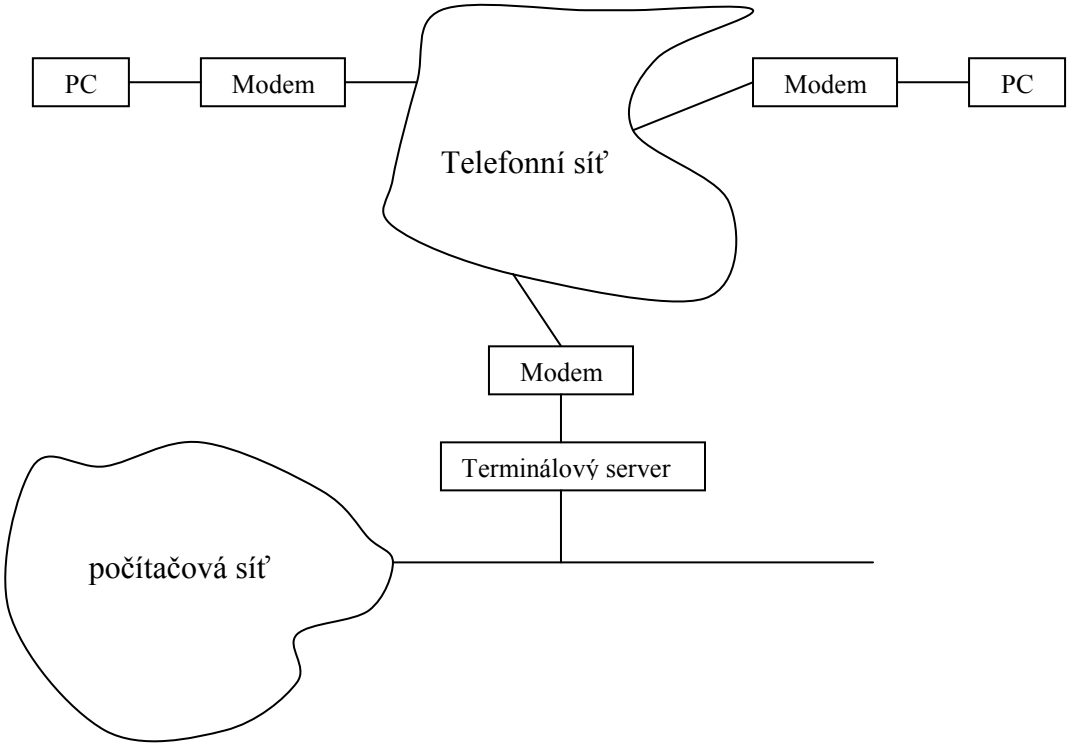
R O Z L E H L É P O Č Í T A Č O V É S Í T Ě

Přenos dat v rozlehlých počítačových sítích

- dvoubodové spoje, 10 Kb/s (individuální účastník), 100 Mb/s (realizace páteřních sítí)
- média: telefonní vedení, radiové spoje směrové a družicové, optická vlákna

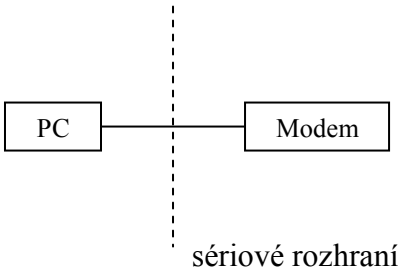
Modemy

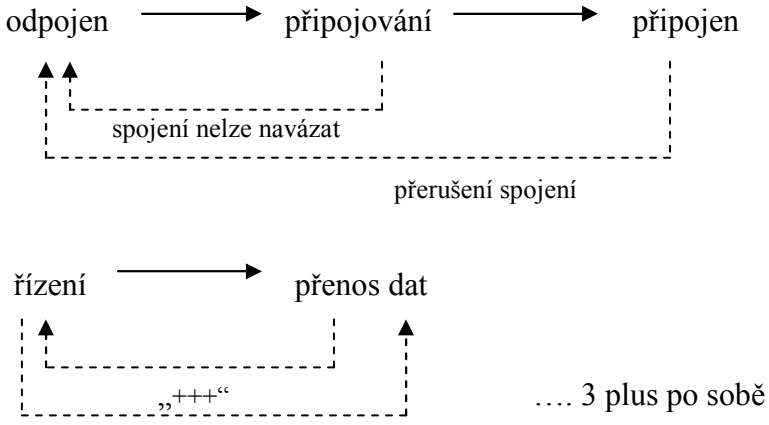
- název odvozen od pojmů modulátor a demodulátor
- propojení digitální techniky (počítače) s počítačovou sítí za pomoci analogového vedení



- funkce modemu:
  - převádí číslicový signál na signál analogový a opačně
  - vytáčení telefonní čísla, vytvoření spojení
  - dohodnutí parametrů spojení
  - komprimace dat

- stavy modemu:
- duplexní spojení
  - ***řízení*** – řídící příkazy
  - ***data*** – přenos dat

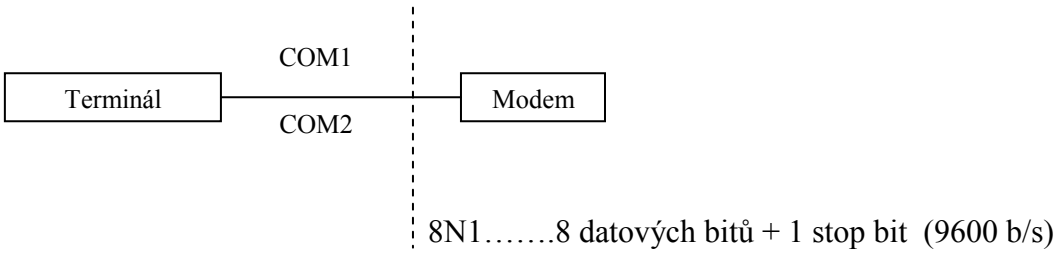


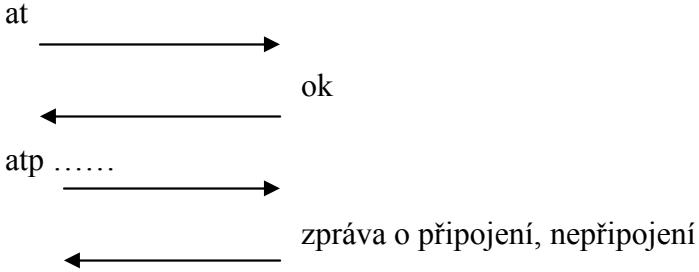


- data modem interpretuje ve stavu řízení jako řídící příkazy
- ve stavu přenosu dat je přenáší dál
- ze stavu řízení do stavu přenosu dat může přejít:
  - *navázáním spojení*
  - *přepnutím ze stavu navazování spojení*

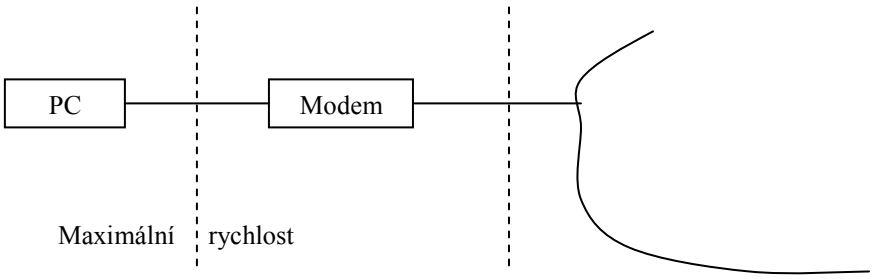
- příkazy modemu:
- vymyslela je firma ***AT&T*** ⇒ mluvíme o tzv. AT příkazech
  - ***atz***……..nastavení přednastavených atributů
  - ***atd***…….vytočení telefonního čísla
    - atdp……pulsní volba
    - atdt…….tónová volba (např. atdt 01974912222)
  - ***ath***…….zavěšení
  - ***atm***……zeslabení/zesílení poslechu

  - nastavní parametrů modemu je uloženo v S-registrech 50 –540
  - ats0…….práce s registrem 0





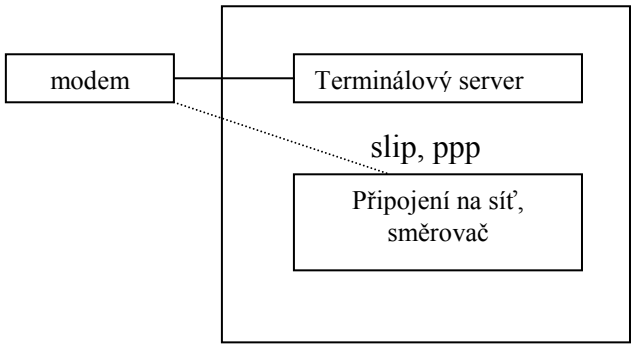
- přenosové rychlosti modemu:
- normalizovány: 150, 300, 600, 1200 b/s
  14 400 b/s, 16 800 b/s, 33 600 b/s, 56 Kb/s



- přenosové protokoly (mezi modemy):
- firemní protokoly ***MNP – Microcom Network Protocol***
  MNP2 – MNP10
  MNP5….standard
  délka přenášeného rámce
  přenosová rychlost
  opakování přenosu při chybě
  MNP10...určeno pro velmi špatné komunikační linky ⇒ radiové sítě - navázání spojení s nízkou přenosovou rychlostí ⇒ postupně se tato rychlost zvyšuje, zvětšují se a zkracují délky rámců
  V.x…….doporučení ***ITU*** týkající se protokolů, kódování, komprimace

Terminálový server a vzdálená přihlášení

- přihlášení ke vzdálenému systému
  - ***přihlášení v terminálovém režimu*** ⇒ (jméno + heslo)
  - ***v režimu připojení jako uzel počítačové sítě*** ⇒ možnost využití všech dostupných služeb



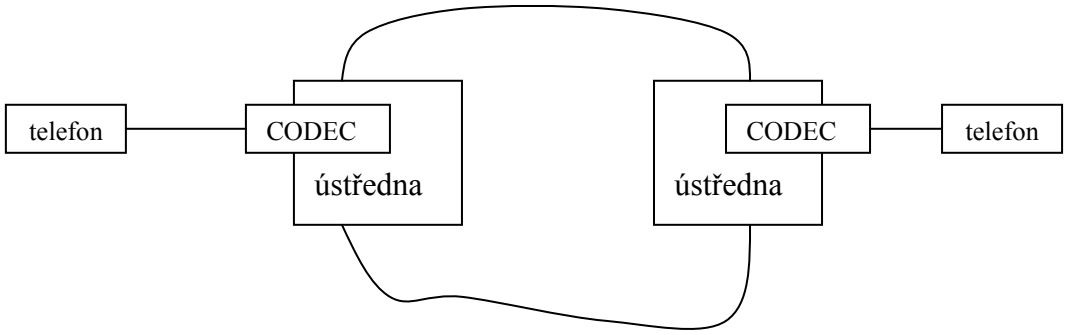
slip……Serial Line Internet Protocol

ppp…….Point To Point Protocol

- ***BOOTHP, DHCP*** – protokoly umožňující přenést informace o IP adrese, masce…

Digitální telefonní sítě

- přenáší číslicovou informaci ⇒ informaci v číselné podobě
- zařízení jménem ***CODEC*** – coder, decoder ⇒ převod analogového signálu na číslicový
- výhody: méně poruch, lepší možnost propojování sítí ⇒ kvalitnější přenos



- převod signálu – využití ***PCM – pulsní kódové modulace***

⇒ posloupnost 8 bitových slabik vždy po 125 2 μs
c = 8 bitů + 8 000 = 64 Kb/s

ISDN Integrated Services Data Network

- datové sítě integrovaných služeb
- *domácí přípojky ISDN*
  - dovolují připojení našich přístrojů přímo na síť
  - k dispozici 2 x 64 Kb/s a jeden kanál řídící 16 Kb/s = 144 Kb/s
- *domácí digitální miniústředna (NT2)*
  - digitální telefon
  - počítač vybavený ISDN rozhraním
  - možnost zapojení až 8 zařízení

- základní kanály s poté sdružují ⇒ vznikají přenosové systémy **T** (T1…T4) - Amerika, Japonsko a **E** (E1….E5) - Evropa

T1…….24 kanálů 64 Kb/s = 1,536 Mb/s
T2…….4 x T1
T3…….7 x T2
T4…….6 x T3 = 274 Mb/s

E1…….30 x 64 Kb/s = 2,048 Mb/s

- synchronní přenos ⇒ 8 000 vzorků za sekundu

B-ISDN

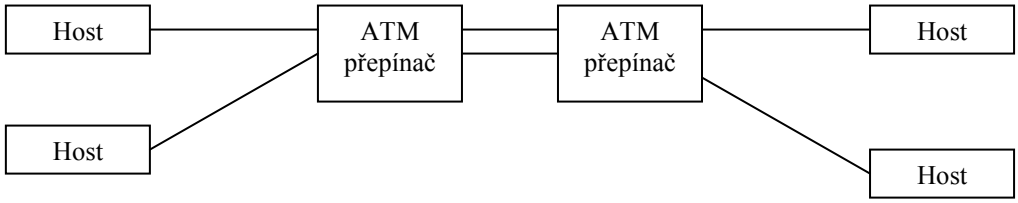
- širokopásmové ISDN, využití ATM technologie
- hodí se pro přenos zvuku, pohyblivého obrazu a dat
- nároky na kvalitu přenosu – musí být zajištěn synchronní přenos
  - *rychlost snímání = rychlosti reprodukce*
  - *snímání konstantní rychlosti*

- informace se přenáší komprimovaně ⇒ komprimace
  - ztrátová – zpětným obnovením nedostaneme to samé
  - bezeztrátová

  - rychlost přenosu: 155 Mb/s, 625 Mb/s……2 Gb/s
  - médium: optické vlákno, metalické vodiče (na krátké vzdálenosti)
  - data jdou normálně s telefonními hovory

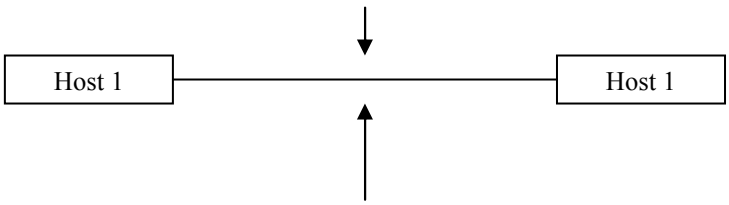
ATM (Asynchronous Transfer Mode) technologie

- data se rozdělí na buňky 53 slabik (5 řízení, 48 data)
- výhoda – konstantní rozdělení do buněk usnadňuje přenos
- přenos – na základě virtuálních kanálů
- přenos je identifikován **virtuálním obvodem (VCI)** a **virtuální cestou (VPI)**



- existují virtuální sítě vytvoření nad ATM
- ***IP over ATM*** – akademická síť v České republice

LINKOVÁ ÚROVEŇ – Ochrana proti chybám



- existují 2 způsoby:
  - ***ARQ detekce chyb + opakování přenosu***
    - použití při normálních přenosech – detekce chyb zabere v paketu málo místa
  - ***FEC detekce chyb + odstranění***
    - při přenosu, který nelze opakovat ⇒ věrný přenos zvuku a obrazu, meziplanetární přenosy ⇒ samoopravitelné systémy ⇒ redundatnost přenosu dat – musíme přenášet mnoho informací navíc

Hamingova vzdálenost

- minimální vzdálenost dvou znaků abecedy
- uvádí se v počtu bitů ve stejnolehlých pozicích

- při **h = n** dokážeme detekovat **n-1** chyb
- při **h = n** dokážeme opravit **n/2** chyb

Kódy pro detekci chyb

- paritní kódy:
  - ***liché*** - lichý počet jedniček
  - ***sudé*** - sudý počet jedniček

  - ***příčná parita***
  - ***podélná parita***

- v moderních systémech se používá zabezpečení pomocí **cyklických kódů (CRC)**
- sítě typu ETHERNET jsou zabezpečovány 32-bitovým polynomem
- s rostoucím počtem chyb a se zvolením špatného způsobu zabezpečení, narůstá možnost špatné detekce a opravy chyb

Model komunikačního kanálu

- přenos je binární, symetrický, bez paměti (přenos dalšího bitů neovlivňuje přenos dalšího)
- pravděpodobnost chyb: $\mathbf{P_n = p^n}$ n……počet bitů

NEPROŠLO JAZYKOVOU ÚPRAVOU ÚSTAVU PRO JAZYK ČESKÝ - ČSAV

John Oscar
PUBLISHING
Honza Přibáň

http://home.zcu.cz/~chairman