

## Úvod do počítačových sítí (NSWI141)

**Libor Forst, SISAL MFF UK**

- Základní pojmy z oblasti komunikací
- Vrstevnatý model sítě (OSI vs. TCP/IP, adresace, multiplexing, ...)
- Aplikační vrstva (DNS, FTP, email, web, VoIP, ...)
- Transportní vrstva
- Síťová vrstva (IPv4, IPv6, směrování, firewall, ...)
- Linková a fyzická vrstva (switch vs. repeater, Ethernet, Wi-Fi, kabeláž, ...)

## Literatura

- D. E. Comer, D. L. Stevens: Internetworking With TCP/IP; Prentice Hall 1991
- A. S. Tanenbaum: Computer Networks; Prentice Hall 2003
- C. Hunt: TCP/IP Network Administration; O'Reilly & Associates 1992
- P. Satrapa, J. A. Randus: LINUX - Internet server; Neokortex 1996; ISBN 80-902230-0-1
- L. Dostálek, A. Kabelová: Velký průvodce protokoly TCP/IP a systémem DNS; Computer Press 2002
- zdroje na internetu
- Request For Comment (RFC)
- <http://www.warriorsofthe.net>

„Klasické“ knihy jsou zde uvedeny převážně z historických důvodů. V současné době najdete v knihkupectvích a knihovnách řadu jiných, pokud dáváte přednost papíru před obrazovkou.

Další informace o našich tématech najdete na internetu samotném. Obecně platí, že informace z internetu nemusí být ve všech případech zcela správné. V tomto kurzu však nepůjdeme do tak velké hloubky, že by riziko chyby v nalezených informacích bylo příliš velké.

Naopak velmi přesné informace o většině protokolů, které budeme studovat, najdeme v oficiálních standardech publikovaných (na internetu) pod názvem RFC. Jsou však o dost podrobnější, než je pro náš kurz potřeba, takže k získání dostatečného přehledu o tématu obvykle stačí pouze úvodní kapitola.

Pro úplné nováčky lze doporučit video „Warriors of the Net“ jako „upoutávku“ na tento kurz, přestože je už poněkud postarší a v některých aspektech věci příliš zjednodušuje příp. formuluje mírně nepřesně.

### Obecné atributy komunikace

- Identifikace
  - komunikující strany se musí „najít“ (telefonní čísla), představit
- Metoda
  - př.: hluchoněmý u přepážky, zkusí znakovou řeč, recepční napíše na papír, že nerozumí a navrhne psanou formu komunikace
- Jazyk
  - obě strany se musí dohodnout na jazyku, který použijí
- Rychlost
  - obě strany se musí dohodnout na rychlosti komunikace
- Proces
  - požadavky, odpovědi, potvrzení

Úvod do počítačových sítí (2022)

SISAL

3

Začneme analýzou běžných způsobů komunikace mezi lidmi v reálném životě a pokusíme se najít atributy podobné těm, které se používají v síťové komunikaci, i když je v reálném životě necítíme jako přísná pravidla.

**Identifikace.** Při komunikaci tváří v tvář nepotřebujete žádné speciální prostředky pro identifikaci, vaše oči a mozek dělají svou práci přirozeně. Jedinou výjimkou je rozhovor s neznámou osobou, kdy je nutné se navzájem představit. U jiných způsobů komunikace používáte nějakou identifikaci, na kterou jste již zvyklí - poštovní adresu, telefonní číslo atd.

**Metoda.** Pokud jsou obě strany schopny používat všechny smysly, není obvykle nutné se dohodnout na nějaké metodě komunikace. Ale samozřejmě mohou existovat i výjimky. Pokud například používáte nějaké signály, musíte se domluvit, co který signál znamená. Pokud máte s některými smysly problém, bude dohoda o způsobu komunikace nezbytná.

**Jazyk.** V mezinárodním prostředí se musíte dohodnout na jazyce. Ve skutečnosti v tomto případě není vždy potřeba jediný společný jazyk, s přirozenými jazyky můžete dosáhnout rozumné úrovně porozumění také pomocí dvou různých jazyků, a to zejména v případě jazyků ze stejné rodiny, např. mezi různými slovanskými jazyky.

**Rychlost.** Někdy může rychlost mluvy působit problémy s porozuměním, zejména mezi rodilými a nerodilými mluvčími. Rozhodně pocítíte rozdíl v porozumění mezi rozhlasovým sportovním komentátorem a učitelem. V takovém případě je opět nutná nějaká neformální dohoda o rychlosti („pomaleji, prosím“).

**Proces.** V normální situaci obvykle nebudete potřebovat žádná přísná pravidla. Každý ví, že v rozhovoru musí svého partnera oslovit a pozdravit a na konci se rozloučit. A pokud na něco zapomenete, pravděpodobně to nezpůsobí mnoho potíží. Když vás však pozvou na návštěvu k prezidentovi (a vy neodmítnete), budete se muset naučit a dodržet složitý protokol.

Pokud přejdeme k síťové komunikaci, všechny tyto atributy se stanou mnohem formálnějšími a důležitějšími; většina rozdílů v nich může způsobit fatální nedorozumění a jen některé budou obě strany schopné akceptovat. Je ale dobré vědět, že všechny podobné atributy nejsou ničím novým; všechny pocházejí ze skutečného života, a zde byly pouze přizpůsobeny a formalizovány.

### Porovnání komunikací

- Běžná komunikace
  - hlas, signály, písmo
  - volná intuitivní pravidla
- Telekomunikace
  - složitá technologie se zabudovanými pravidly
  - řízení má na starosti síť, řídí i koncová zařízení
- Počítačová síť
  - pravidla jsou volně dostupná
  - značná část logiky je v koncových zařízeních
  - síť se stará jen o přenos
- Konvergovaná síť
  - spojuje svět spojů a počítačů (cena, efektivita...)
  - úspěšnější je konvergence na bázi počítačové sítě

Úvod do počítačových sítí (2022)

SISAL

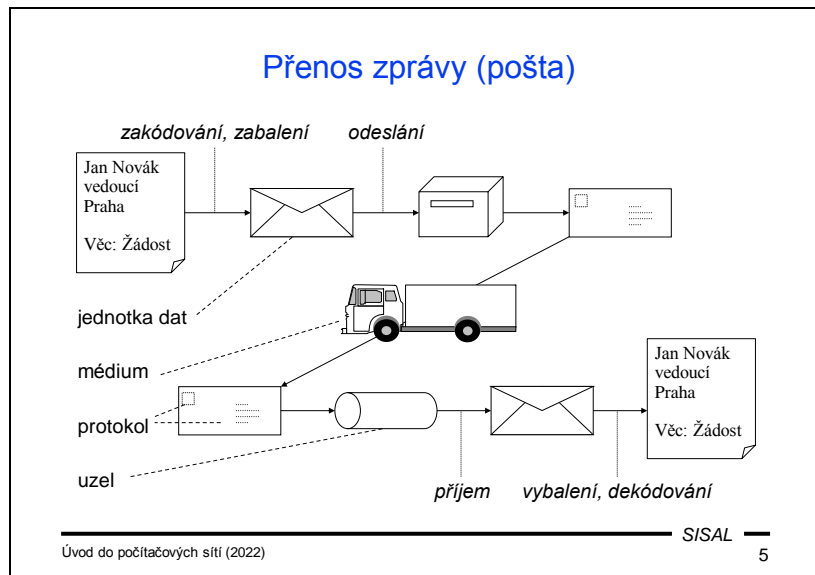
4

Až dosud jsme hovořili o běžných formách mezilidské komunikace a dospěli jsme k závěru, že se zde používají velmi volná a intuitivní pravidla.

Prvním globálním komunikačním prostředkem založeným na technologiích byly telefony. Od začátku byla telefonní síť budována jako prostředek pro byznys, takže všechny uzly byly pod centralizovanou kontrolou a pracovaly na základě neveřejných komplexních proprietárních pravidel zabudovaných přímo do komunikačních zařízení. Koncové zařízení (telefon) bylo pouze jednoduchým rozhraním pro přístup k infrastruktuře, která zabezpečovala veškerou aplikační a transportní logiku.

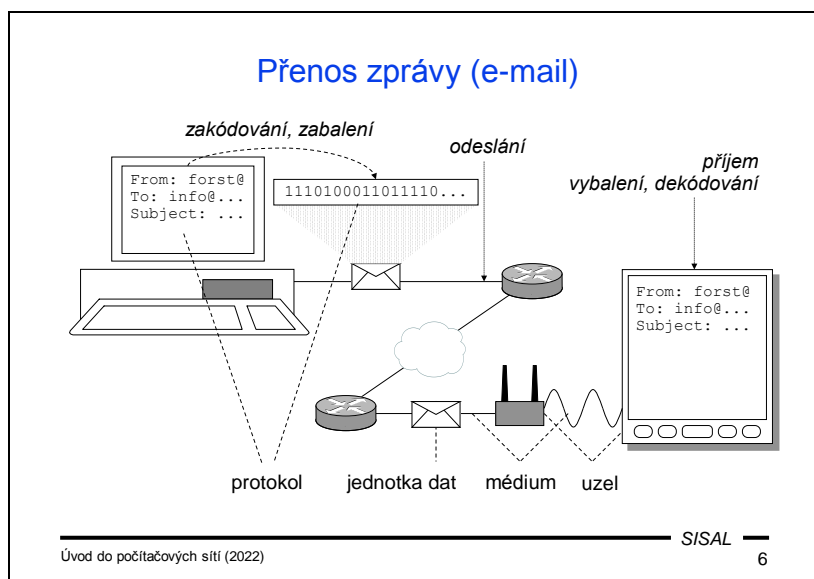
Počítačové sítě byly navrženy na úplně jiném principu: aplikační logika je soustředěna v koncových zařízeních a síťová infrastruktura ovládá pouze logiku přenosu. Proto bylo nutné navrhnout systém jako otevřený a pravidla zveřejnit, aby se podle nich mohl řídit každý implementátor aplikace.

Při studiu komunikací si musíme nutně položit otázku, jak tyto dva typy sítí propojit. V průběhu historie existovalo několik způsobů takového propojení. Původně počítačové sítě využívaly telekomunikační infrastrukturu (pronajaté linky). Postupem času se začala rozšiřovat vlastní kabeláž a situace se obrátila: v dnešní době se telefonie velmi často přenáší přes počítačovou síť (Voice over IP). Rozmach smartphonů s mobilními daty však v mnoha případech situaci opět vrátil k tomu, že síťová komunikace se přenáší po telefonních kanálech.



Podívejme se na proces přenosu zprávy (klasickou) poštou. Vezmete papír s napsanou zprávou, vložíte ho do obálky, napíšete adresu, nalepíte známku a hodíte do schránky. Tím předáte dopis organizaci, která zabezpečuje přenos (pošta), a ta ji pak dál zpracovává pomocí své infrastruktury a doručí ji do schránky příjemce. Po doručení příjemce otevře obálku a vytáhne papír se zprávou.

Pojďme nyní popsat celý proces pomocí termínů používaných při síťové komunikaci. Ty nejsou běžně používané, ale jsou plně srozumitelné. Vezmete list papíru se zprávou [datová jednotka], vložíte jej do obálky [zapouzdření], napíšete adresu [adresa cílového uzlu] a nalepíte známku [dodržujete poštovní protokol] a hodíte ho do schránky [odesílání]. Poté pošta zpracovává zprávu pomocí své infrastruktury [mezilehlé uzly propojené různými médii] a doručí ji do schránky příjemce [cílový uzel]. Po doručení příjemce otevře obálku [decapsulation] a vytáhne zprávu [zpráva doručena].

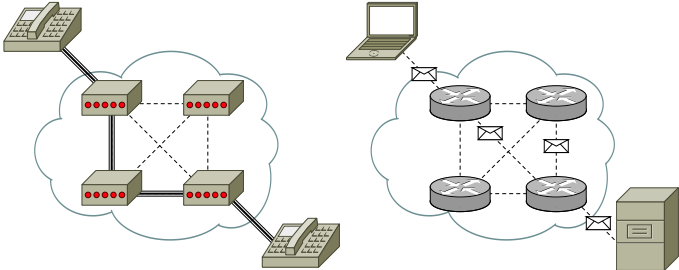


Velmi podobnými slovy můžeme popsat proces přenosu zprávy v případě elektronické pošty. Musíme také začít zakódováním a zapouzdřením podle správného protokolu, tím vytvoříme datovou jednotku, která musí být odeslána do místní sítě. Poté síťová infrastruktura posílá zprávu přes různé mezilehlé uzly a různé kanály, aby byla posléze doručena do cílové místní sítě a v rámci ní až na koncový uzel (váš osobní počítač, smartphone atd.), kde je rozbalena, dekódována a zobrazena na displeji.

Vidíme zde stejné herce, stejné role a stejné úkoly jako v klasické poště, pouze převedené na technickou platformu. Základní princip fungování je v obou případech stejný.

**Požadavky - odolnost**

- přepojování okruhů: rychlejší, plynulejší, ale při výpadku uzlu se spojení rozbije
- přepojování paketů: každý může jít jinou cestou, liší se doba přenosu, ale výpadek uzlu není fatální



Úvod do počítačových sítí (2022) SISAL 7

Za zrodem myšlenky využití elektronických prostředků pro přenos zpráv stálo několik základních požadavků. Některé z nich zůstaly dodnes prakticky nezměněné, některé se postupem času poněkud modifikovaly.

Zásadním požadavkem byla odolnost proti chybám. Ve skutečnosti za celou myšlenkou stála armáda (americké ministerstvo obrany). Řešili zásadní problém výpadků telefonních sítí v případě nepřátelského útoku. Běžná telekomunikační síť využívá takzvané *přepínání okruhů*. Když někomu zavoláte, síť najde posloupnost uzlů (okruh) potřebných k propojení vašeho zařízení a koncového zařízení, kterému voláte. Jakmile je tento okruh vytvořen, všechna zvuková data se přenášejí touto cestou. Pokud nepřítel napadne některý uzel okruhu, spojení je ztraceno.

Řešení tohoto problému je docela snadné. Data rozdělíme na menší bloky, tzv. *pakety*, a každý paket si najde vlastní cestu k cílovému uzlu. Pokud je napaden některý uzel, paket najde alternativní cestu. Přenos se tím trochu zpomalí, ale zpráva bude doručena. V dnešní době může být důvodem selhání uzlu nejen útok nepřítel (hackera), ale také výpadek napájení, chybná konfigurace atd. Riziko výpadku uzlu tedy stále existuje, a proto současné sítě pro doručování dat používají právě tento model, tzv. *přepínání paketů*.

Při porovnávání těchto metod lze říci, že přepínání obvodů je sice rychlejší ale méně spolehlivé, zatímco přepínání paketů je pomalejší, ale odolné vůči chybám.



### Požadavky – bezpečnost I

- Původní motivace požadavku na bezpečnost:
  - fyzické zabezpečení přenosu
- V době vzniku sítí bylo malé riziko, že útočník napadne síť jinak než fyzickou destrukcí
- Staré technologie byly naivní:
  - otevřená komunikace (umožňuje odposlech)
  - důvěra v identitu protistrany
  - důvěra ve správnost obsahu
  - důvěra v dostatečnost vlastních kapacit

Požadavek na odolnost úzce souvisí s obecnějším pojmem bezpečnosti, konkrétně fyzickou bezpečností, neboli bezpečností fyzické infrastruktury (uzlů a kabeláže). Při přípravě myšlenky počítačové sítě nebyla překvapivě zohledněna druhá strana mince – bezpečnost logická (ochrana dat). Důvodem je pravděpodobně to, že tehdejší rozměry a cena počítačů spolu s náročností programování spolehlivě bránily tomu, aby se útočník mohl dostatečně přiblížit se svým zařízením a zaútočit na data. Stejně tak nebylo reálné, aby útočník způsobil datovým útokem nefunkčnost našich výpočetních prostředků.

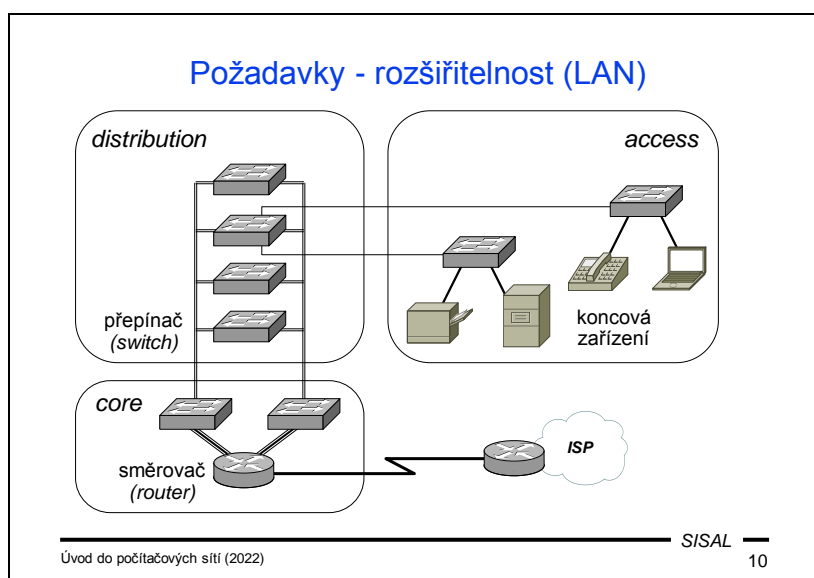
V současnosti je situace opačná - je velmi snadné získat počítač připojený do sítě a je docela snadné infikovat cílový počítač softwarem útočníka tak, aby mohl vidět nebo dokonce měnit přenášená data.

Všechny protokoly z dob počátků internetu mají stejný problém - nepoužívají žádné šifrování a důvěřují „odesílateli“ i obsahu dat. Stejně chování nyní bohužel můžete vidět u mnoha lidí, kteří důvěřují všemu, co dostanou elektronickou poštou nebo uvidí na webu.

## Požadavky – bezpečnost II

- Bezpečnostní rizika:
  - fyzické napadení infrastruktury
  - útok na data
  - DoS (Denial of Service)
- Bezpečnost infrastruktury:
  - omezení přístupu
  - záložní zdroje napájení, klimatizace...
  - záložní servery, konektivita...
- Bezpečnost dat:
  - ověřování uživatelů a kontrola přístupových práv
  - ověřování počítačů (serverů, příp. i klientů)
  - inspekce dat (aplikační proxy, antiviry, antispamy, IDS...)
  - kryptografie (šifrování a podpisy)

Požadavek na fyzickou bezpečnost samozřejmě nevymizel ani v současnosti. Kromě rizik vyplývajících z neoprávněného fyzického přístupu se ovšem připojila v přinejmenším stejné závažnosti i rizika technická jako jsou výpadky napájení, spojení atd. Daleko větší váhu postupem času získaly požadavky na bezpečnost dat, tj. zabránění neoprávněnému přístupu k datům příp. neoprávněné manipulaci s daty. S progresivním rozvojem konektivity a dostupnosti IT techniky se výrazně zvýšilo i riziko útoků DoS (Denial of Service), kdy útočník napadne masivní komunikací nějaký zdroj dat, takže ten pak nemůže komunikovat s řádnými uživateli. Takovýto útok navíc bývá obvykle zesílen tím, že útočník využije nějaké chyby/slabiny v implementaci určité služby a donutí cizí servery, aby zvýšený provoz generovaly nevědomky místo něj (tzv. DDoS – Distributed DoS).



Dalším důležitým požadavkem je škálovatelnost. To znamená, že celý systém musí být navržen tak, aby přidávání nového počítače nebo sítě bylo snadné a nebylo kvůli němu nutné provádět zásadní změny ve vzdálených částech sítě. Řešení požadavku škálovatelnosti pro přidávání počítače do (místní) sítě a přidávání nové sítě do internetu se sice technicky liší, ale hlavní myšlenka je velmi podobná.

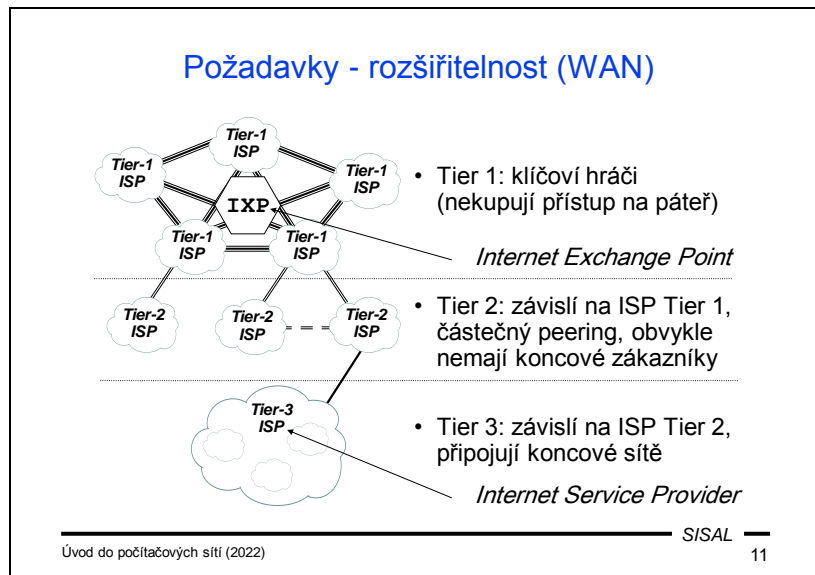
Doporučený přístup k návrhu místní sítě (LAN) je rozdělení infrastruktury na tři vrstvy:

Vrstva **core** je hlavní částí sítě, kde je ukotvena páteř celé sítě a síť je připojena k infrastruktuře poskytovatele připojení (ISP, Internet Service Provider). Zařízení, která jsou součástí této vrstvy, jsou obvykle umístěna ve speciální místnosti s klimatizací a záložním zdrojem napětí (UPS a/nebo generátorem). Klíčovým zařízením je *router*, uzel propojující různé sítě. Router na perimetru naší sítě je vstupním bodem celé sítě a je připojený k jinému routeru na straně ISP. Dalším důležitým zařízením je *switch* (přepínač), uzel propojující další uzly sítě navzájem. Vrstva core obvykle obsahuje několik hlavních switchů propojujících hlavní router se zbytkem místní sítě.

**Distribuční** vrstva je páteřní částí sítě, která zodpovídá za distribuci konektivity do všech částí budovy nebo kampusu. Někdy se jí také říká *vertikální* vrstva, protože se velmi často nachází ve svislé šachtě procházející všemi patry budovy.

Vrstva **přístupu** (access) je poslední částí sítě, která umožňuje přístup k síťovým službám všem koncovým zařízením, serverům, tiskárnám, osobním počítačům, telefonům atd. Někdy se také nazývá *horizontální* vrstva. Tato vrstva má svoje zakončení co nejbližší místům, kde se koncoví uživatelé potřebují připojit.

Tento přístup k návrhu místní sítě zaručuje snadné připojení nových počítačů resp. rozšíření služeb v určité části sítě. Samozřejmě je možné, že některá část sítě dosáhne maxima své kapacity, ale i v tomto případě další rozšíření sítě opět ovlivňuje pouze konkrétní části distribuční vrstvy.



Podobný koncept třívrstvého modelu se používá také pro svět za hranicí lokální sítě.

Na vrcholu hierarchie je vrstva s názvem **Tier 1**. V této vrstvě jsou klíčoví hráči internetu, tj. společnosti s přímým přístupem k páteři internetu, která propojuje všechny kontinenty. Příklady: AT&T, Deutsche Telekom, British Telecom.

Nejnižší vrstva stromu se nazývá **Tier 3**. Zde se nacházejí ISP, kteří připojují koncové zákazníky - obvykle společnosti, organizace, domácnosti atd. připojující své lokální sítě k internetu.

Někde mezi těmito dvěma extrémy leží vrstva **Tier 2** se společnostmi bez přímého přístupu k páteři, jejímiž zákazníky jsou jiní ISP. Typickým příkladem jsou regionální nebo národní operátoři.

## Požadavky - kvalita služeb (I)

- Přenosové parametry sítě:
  - zpoždění (*latence*, *delay*)
  - pravidelnost doručování (*jitter*, mat. rozptyl zpoždění)
  - ztrátovost dat
  - šířka pásma (*bandwidth*, „rychlost“)
- Různé aplikace mají různé požadavky pro zabezpečení dostatečné kvality služeb:
  - multimediální aplikace: pravidelné doručování
  - přenosy dat (WWW, pošta): nízká ztrátovost dat
  - ...

Posledním požadavkem je dostatečná kvalita služeb poskytovaných sítí jednotlivým aplikacím. Tento požadavek ovšem nevede k jednotnému přístupu, protože pro různé aplikace jsou důležité různé parametry síťového přenosu.

Hlavními přenosovými parametry, které můžeme zkoumat, jsou:

- **Latence**, neboli zpoždění komunikace, tj. doba od chvíle, kdy jsou určitá data odeslána do sítě, až do doby, kdy jsou doručena na místo určení.
- **Jitter** je rozptyl zpoždění; tato hodnota vyjadřuje, jak pravidelně jsou data doručována, tj. jak objem přijatých dat kolísá.
- **Ztrátovost** dat znamená, jak často dochází k tomu, že nějaký paket není doručen; vysoká ztrátovost dat vede buďto ke skutečné ztrátě informací během přenosu, anebo nutnosti opakovaného odesílání ztracených paketů.
- **Šířka pásma** (*bandwidth*), parametr často nazývaný „rychlost“, což je trochu zavádějící, protože rychlost přenosu signálů přes dané médium je vždy stejná (žádný ISP nemůže použít rychlejší světlo pro přenos přes optické vlákno); ve skutečnosti to znamená, kolik dat lze zakódovat a přenášet pomocí konkrétních fyzických signálů, nikoli skutečnou rychlost signálů.

Když se podíváme na tyto parametry, je snadné pochopit, že nevyhovující hodnoty některých z nich přinášejí vážné problémy pro různé aplikace. Například multimediální aplikace používají speciální kódování, která jsou odolnější proti ztrátě dat, takže poněkud větší ztrátovost dat u nich nepůsobí problémy. Vysoká latence může být kritická při používání takových aplikací v reálném čase (např. u telefonních hovorů), ale např. na sledování filmu nemá velký vliv. Ovšem vysoký rozptyl zpoždění už multimediálním aplikacím vadit bude. Naproti tomu pro aplikace založené na přenosu celých bloků dat (web, e-mail apod.) je vysoká ztrátovost dat. U nich

způsobuje přetížení přenosových kanálů a velké zpoždění v důsledku masivního přeposílání ztracených dat.

## Požadavky - kvalita služeb (II)

- Cíl:
  - garance vymezeného toku pro konkrétní typ provozu
  - garance rychlejšího doručení prioritních zpráv
- Implementace:
  - data obsahují klasifikaci QoS (Quality of Service)
  - strategie *garance kvality*: vyhrazená šířka pásma
    - zaručená kvalita, plýtvání kapacitou
  - strategie *best effort*: prioritní fronty
    - efektivní využití média, není záruka kvality

Obecně lze říci, že bychom rádi dosáhli dvou základních cílů:

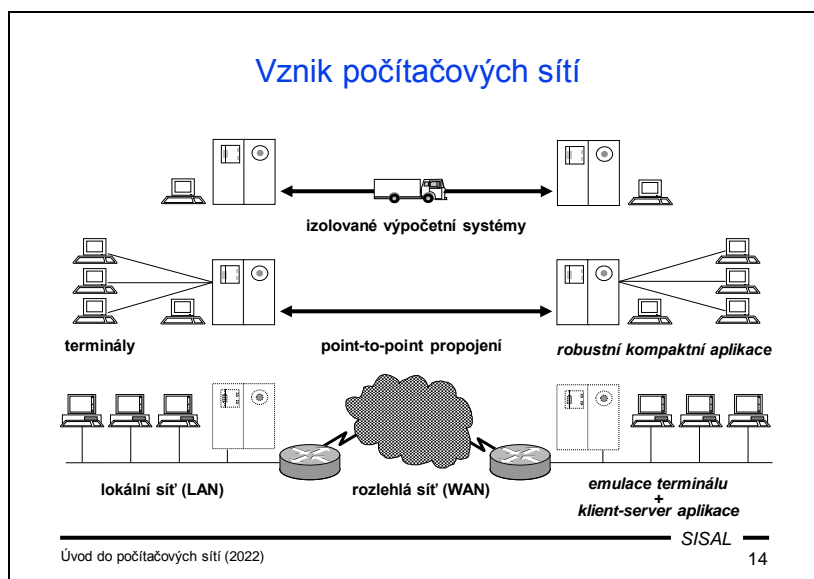
- U některých typů provozu chceme vyhradit určitou šířku pásma, která bude dostatečná pro to, aby konkrétní aplikace dobře fungovala.
- U některých typů provozu (nebo alespoň u některých typů zpráv) musíme zaručit dostatečně rychlé doručení - např. při masivním přenosu dat jednou aplikací stále potřebujeme rychle doručovat naléhavé zprávy.

Jaké jsou současné metody používané k dosažení těchto cílů:

- Základní podmínkou je, jak rozpoznat různé typy přenosu dat. Za tímto účelem odesílatel označuje pakety speciální značkou, tzv. QoS. Celý tento přístup samozřejmě funguje pouze za té podmínky, že se všechny aplikace chovají fér. Pokud aplikace začne podvádět a označí všechna data vysokou prioritou, systém se může zhroutit.
- Pro aplikace, u nichž potřebujeme zaručit dostatečnou propustnost, můžeme vymežit část šířky pásma přenosového kanálu. Tento přístup funguje dobře jen tehdy, pokud máme dostatečnou šířku pásma pro veškerý potřebný provoz. Problém tohoto přístupu spočívá v tom, že pokud konkrétní aplikace v nějakém okamžiku nevyužívá svou vyhrazenou část šířky pásma, zůstává tato část nevyužitá a ztrácíme přenosovou kapacitu kanálu.
- Zaručení dostatečné rychlosti doručení zpráv podle jejich deklarované priority lze vyřešit tzv. strategií *best effort* pomocí prioritních front. Síťový uzel má různé fronty pro zprávy s různými prioritami a podle priorit vybírá pro odesílání zprávy z různých front. Výhodou je, že nedochází k plýtvání kapacitou kanálu, ale při velkém zatížení nelze zabezpečit požadovanou rychlost doručení. Problém je hlavně na vstupní straně uzlu - když paket dorazí na vstup uzlu, uzel nedokáže rozpoznat typ paketu nebo klasifikaci priority, dokud nenačte dostatečnou část paketu. Pokud nechce paket zahodit, musí ho zpracovat celý, přestože může mít



nízkou prioritu, zatímco jiné pakety s vyšší prioritou mohou čekat na přijetí a zpracování.



V době vzniku myšlenky počítačové sítě existovalo jen několik izolovaných počítačů s velmi omezenými prostředky interakce mezi počítačem a uživateli i mezi počítači navzájem. Sálkový počítač měl obvykle jedinou alfanumerickou konzoli, ze které operátor ovládal všechny běžící úlohy. Omezené byly i možnosti vstupu a výstupu – k zadávání většího množství dat sloužily např. čtečky děrných štítků. Pokud bylo nutné přenášet data mezi počítači, obvykle nezbylo jiné řešení, než je naděrovat do sady děrných štítků, přenést je ke druhému počítači a načíst je tam.

Postupem času se počítače zlepšovaly a mohly obsloužit mnohem více uživatelů, takže bylo nutné přidat nějaký způsob, který uživatelům umožní přístup ke sdílenému počítači. Řešením byly terminálové sítě. *Terminál* je jednoduché zařízení s klávesnicí a monitorem, které dokáže přenášet stisky kláves do počítače a zobrazovat uživateli odpověď na obrazovce. Pro komunikaci mezi dvěma počítači bylo možné vybudovat privátní point-to-point komunikační kanál (obvykle prostřednictvím pronajatých telefonních linek) bez jakékoli složitější struktury. Aplikace používané v té době byly stále stejné jednolitě aplikace jako v předchozím období.

V poslední fázi vývoje došlo ke dvěma důležitým změnám. Množina náhodných dvoubodových propojení přerostla do formy globální strukturované sítě, tzv. *Wide Area Network*. Na lokální straně byly terminály nahrazeny osobními pracovními stanicemi a byly navzájem propojeny (a příp. připojeny k místnímu centrálnímu výpočetnímu systému) novým typem sítě *Local Area Network*, která nahradila starou terminálovou síť.

Jedním z důsledků této změny bylo také zavedení nového modelu aplikací, takzvaného modelu klient-server. Je založen na principu, že část výpočetního výkonu je přenesena do počítače na straně uživatele, takže aplikace má dvě části, *klienta*

běžícího na vašem počítači a *server* běžící někde na síti. Tyto dvě části spolu komunikují, přenášejí požadavky uživatelů z klienta na server a zprostředkovávají odpovědi uživateli. Pojmy klient a server tedy v původním významu tedy odkazují na software, i když se dnes přeneseně používají i pro označení počítače.

### Základní dělení sítí

- Lokální síť (Local Area Network)
  - sdílení prostředků (souborové a databázové servery, tiskárny)
  - menší vzdálenosti (budova, kampus), malé zpoždění
  - jednotné vlastnictví a řízení
- Rozlehlé síť (Wide Area Network)
  - vzdálený přístup, komunikace
  - velké vzdálenosti, větší zpoždění
  - mnoho vlastníků, distribuované řízení
- Dnes:
  - rozdíly se stírají (nejmarkantnější jsou ve vlastnictví)
  - vznikají mezistupně (MAN)
- Není to dělení technické (neexistuje definice), ale logické

Úvod do počítačových sítí (2022)
S/SAL 15

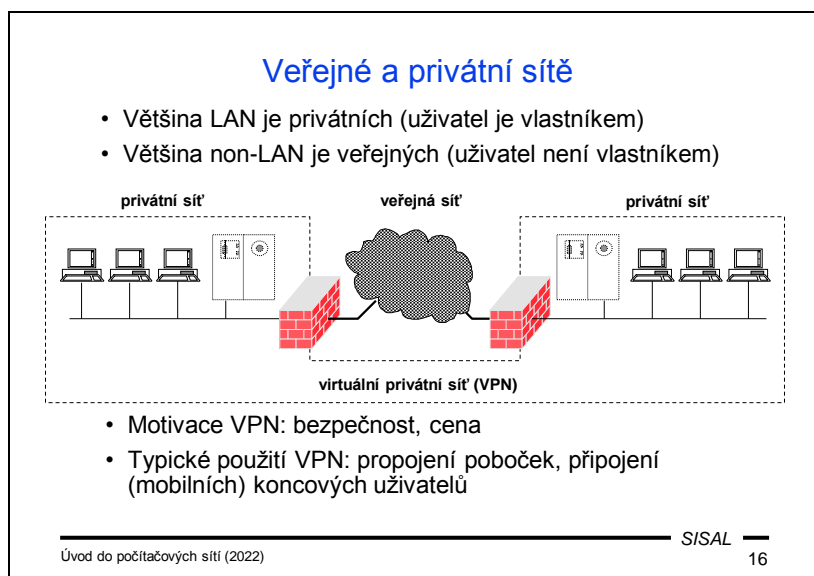
Po této exkurzi do historie se můžeme podívat na současnou terminologii používanou pro typy sítí podle jejich rozsahu.

Termín **Local Area Network** (lokální síť) označuje nástupce terminálových sítí, z čehož plyne, že jejich hlavním účelem je sdílení zdrojů mezi obvykle ne příliš vzdálenými počítači (za jeden ze sdílených zdrojů lze považovat i připojení k internetu). Obvykle jsou geograficky omezeny hranicemi budovy nebo kampusu, jehož vlastník buduje a spravuje síť především pro své zaměstnance, studenty, zákazníky atd.

Termín **Wide Area Network** (rozlehlá síť) označuje globální síť, které nahradily shluky náhodných dvoubodových propojení mezi počítači nebo počítačovými centry. Jejich hlavním účelem je komunikace a přenos dat na větší vzdálenosti. Jsou budovány a spravovány více organizacemi a používány uživateli stojícími mimo tyto organizace.

Mezi těmito dvěma extrémami široké škály sítí existuje několik dalších kategorií s ne zcela přesným významem, např. metropolitní síť.

V minulosti existovaly také poměrně přesně definované technické rozdíly mezi sítěmi LAN a WAN, například použitá technologie, šířka pásma atd. Postupem času však tyto rozdíly zmizely a v současné době je hlavním rozdílem vztah toho, kdo síť spravuje a kdo ji využívá. Na rozdíl od WAN jsou LAN obvykle soukromé. **Žádná definice jako „Síť je LAN, když ...“ neexistuje.**



Jak již bylo zmíněno, sítě LAN jsou ve většině případů soukromé, zatímco sítě WAN jsou většinou veřejné. To představuje pro projektování sítě problém, pokud potřebujeme rozšířit soukromou LAN na geograficky velkou oblast, například mezi pobočkami ve dvou vzdálených městech. Propojení takových míst soukromou kabeláží není reálné a používáním veřejné sítě ztrácíme soukromí.

Řešením je **virtuální privátní síť** (VPN). Základní myšlenkou je, že na hranici každé části LAN je zařízení, které je ke svému protějšku připojeno tzv. VPN tunelem, který vede přes veřejnou síť. Veškerý provoz směřovaný tunelem na druhou pobočku je šifrován při vstupu do tunelu, odeslán přes veřejnou síť, poté dešifrován na druhém konci tunelu a doručen v rámci druhé části LAN. Pro počítače v obou částech LAN je celý mechanismus transparentní a síť se tváří jako jedna LAN.

Jinou modifikací tohoto principu je, když je celá jedna strana tunelu nahrazena softwarem běžícím na osobním počítači (notebooku). Pak se tento počítač tváří jako normální uzel v soukromé síti, do které patří a do které se tunelem připojí.

*Poznámka:* Na konci semestru poznáme jiný termín, který zní velmi podobně, Virtual Local Area Network (VLAN), ale jeho význam je zcela odlišný, proto si je nepleťte.

### Historie Internetu

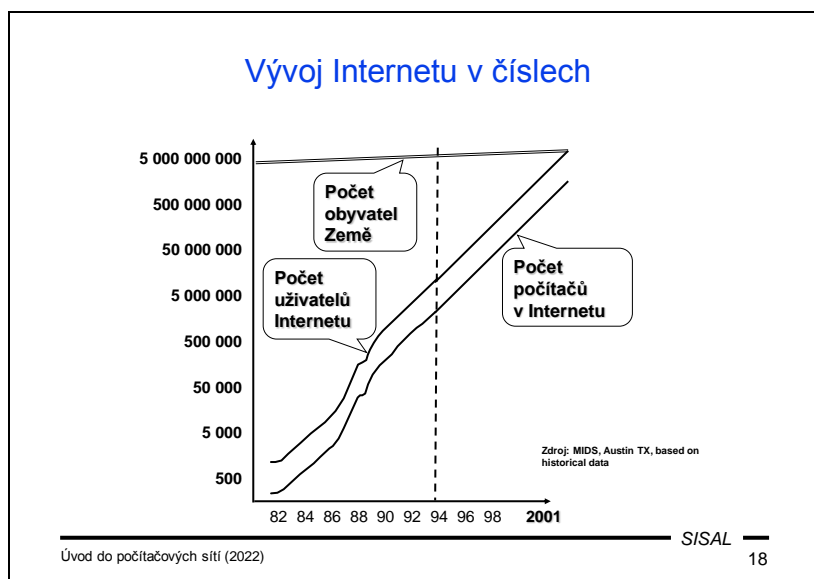
- zač. 60. let - koncepce „packet switching“
- 60.léta - US DoD podporuje koncept „packet switching“ pro odolnost proti fyzickému útoku
- 1969 - ARPANET - financuje Defense Advanced Research Project Agency, provozují akademická pracoviště, point-to-point, pevné linky
- 1974 - termín „Internet“ (zkratka „internetworking“) použit v RFC 675 definujícím TCP
- 1977 - na ARPANET páteř se připojuje první síť
- 1983 - TCP/IP nahrazuje NCP v ARPANETu
- pol. 80. - TCP/IP součástí BSD UNIXu

Myšlenka přepínání paketů se objevila na počátku 60. let na americkém ministerstvu obrany. To vytvořilo specializovanou agenturu Advanced Research Project Agency (ARPA), kde se několik akademických institucí pokusilo tuto myšlenku implementovat a vytvořit síť založenou na struktuře point-to-point spojení přes pronajaté telefonní linky. Tato síť byla vytvořena v roce 1969 a nazývala se ARPANET.

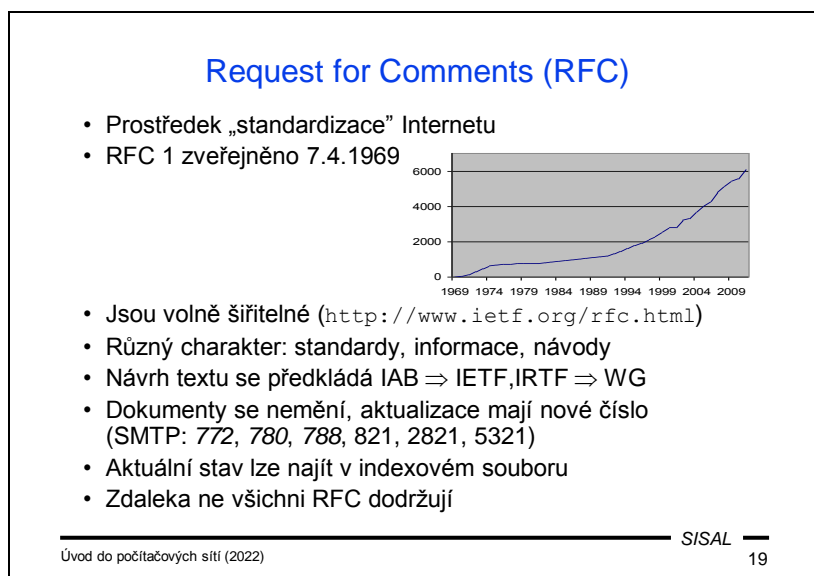
Původně propojovala pouze samostatné počítače a v roce 1977 byla na páteř ARPANETu připojena první síť. Tento okamžik přidal vlastně další význam pojmu „internet“, který se ovšem objevil už v roce 1974.

V současné době je dominantní síťovou technologií TCP/IP, která v roce 1983 nahradila v ARPANETu svého předchůdce Network Control Program (NCP).

Poslední klíčový milník vývoje nastal v polovině 80. let, kdy vývojáři klonu Berkeley System Distribution (BSD) operačního systému UNIX pochopili důležitost TCP/IP a přidali podporu TCP/IP přímo do jádra své verze UNIXu. Tím okamžikem vlastně dostali všichni uživatelé systému dostatečné prostředky pro připojení k internetu.



Jen jako perličku, která dokazuje, jak dramaticky se toto odvětví vyvíjí, se můžeme podívat na graf publikovaný v roce 1993 společností Internet Society. Použili extrapolaci vývoje sítě v předchozích čtyřech letech a výsledkem byl odhad, že v roce 2001 překročí počet uživatelů Internetu (uživatelů, nikoliv účtů) populaci Země ...



Dokumenty označované jako Requests for Comments představují v současnosti prostředek standardizace na internetu, ačkoli jejich název tomu nenasvědčuje.

V minulosti totiž sloužily k prezentaci myšlenek a diskusi o nich a rovněž ke zveřejňování různých dat. To je původní význam jejich názvu. Jako příklad toho, co v prehistorii internetu RFC obsahovaly, můžeme uvést, že např. změny počítačových adres byly publikovány právě prostřednictvím RFC. Tato praxe vcelku liberálního obsahu RFC skončila v 70. letech, a jak můžete vidět na grafu, nárůst počtu RFC rapidně poklesl.

V současné době je jejich publikování řízeno orgánem Internet Advisory Board, a to prostřednictvím dvou komisí, Internet Research Task Force and Internet Engineering Task Force a několika pracovních skupin. Když autor předloží návrh nového protokolu, příslušná pracovní skupina jej posoudí, a pokud to považuje za užitečné, dokument obdrží číslo a je **zveřejněn** „k připomínkování“ (jak říká původní význam „RFC“). Důležitým faktem je, že text dokumentu se **nikdy nemění** (kromě překlepů a chyb). Při studiu nějakého RFC tedy nemusíte hledat na Internetu nejnovější verzi. Všechny servery mají verzi obsahově stejnou. Pokud dojde k podstatnějším změnám, je dokument znovu vydán **s novým číslem**. Změny čísel RFC lze sledovat v souboru rfc-index.txt. Starší RFC jsou v něm označeny buďto jako „Obsoleted“ (zastaralý), anebo pouze „Updated“ (v takovém případě jsou platné oba dokumenty).

Dodržování pravidel chování protokolů definovaných v RFC je velmi důležité pro všechny implementátory. Některá pravidla jsou však trochu omezující a mnoho klientů a serverů je porušuje. Vzájemné porozumění pak závisí na rozsahu toho, jak moc obě strany pravidla porušují. Obecné doporučení pro implementátory zní: buďte na přijímací straně co nejtolerantnější a na vysílající straně co nejvíce konzervativní!



## Souhrn 1

- Jaké jsou výhody a nevýhody přepojování paketů?
- Jak se na síťových protokolech projevilo to, že vznik síť iniciovala armáda z důvodů zvýšení bezpečnosti komunikace?
- Co je smyslem požadavku na škálovatelnost sítě?
- Jak se liší nároky elektronické pošty a telefonování po IP síti na přenosové parametry sítě?
- Jaká je definice LAN?
- Co je podstatou VPN?