

# KOMUNIKAČNÍ TECHNOLOGIE (BPC-KOM)

Ústav telekomunikací

Fakulta elektrotechniky a komunikačních technologií

VUT v Brně

doc. Ing. Jan Jeřábek, Ph.D.

[jerabekj@feec.vutbr.cz](mailto:jerabekj@feec.vutbr.cz)

RELAČNÍ VRSTVA PŘENOSOVÝCH  
SYSTÉMŮ

PREZENTAČNÍ VRSTVA  
PŘENOSOVÝCH SYSTÉMŮ



# Plán přednášky

3

- Relační vrstva
- Prezentační vrstva
  - ▣ Prezentace dat
  - ▣ Komprese dat
  - ▣ Šifrování dat

# Relační vrstva

4

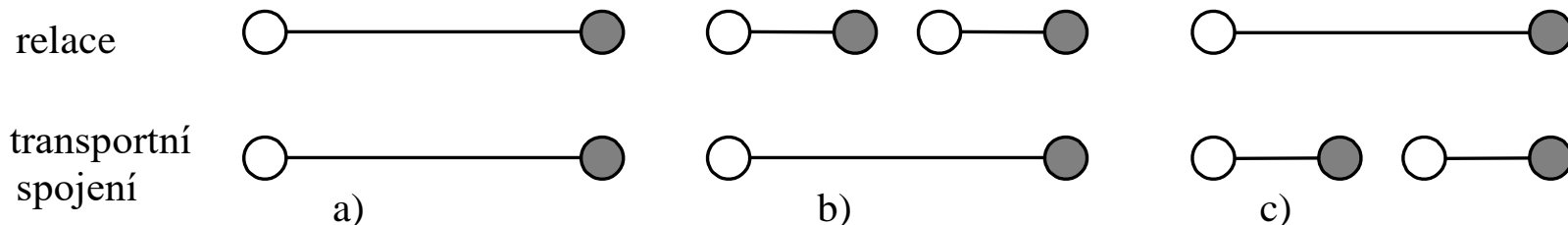
- pátou vrstvou modelu ISO/OSI
- relace = *session*
- v TCP/IP není přímo definována
  - ▣ pokud jsou její služby vyžadovány, řazeny do aplikační vrstvy, částečně pak i transportní vrstvy
- základní popis v rámci kap. 1
- účelem relační vrstvy
  - ▣ poskytnout prostředky pro spolupráci vyšších vrstev
  - ▣ synchronizaci jejich dialogu
  - ▣ řízení výměny dat na této úrovni
  - ▣ jinými slovy poskytování síťových služeb aplikaci
    - kde je jednodušší síťová struktura nebo kde je dostatečná transportní služba nemusí tato vrstva existovat vůbec (případ TCP/IP)

# Služby relační vrstvy

5

## □ Zřízení spojení

- vytvoření nastavby transportního spojení
- možné různé režimy vzájemného promítnutí transportního a relačního spojení, typicky 1:1
- doba života těchto dvou spojení může být rozdílná



## □ Přenos dat

- spočívající nejen v přenášení dat, ale i v zajištění mechanismů proti zahlcení daty
- spojení v rámci relační vrstvy, v rámci kterých probíhá přenos dat, mohou být simplexní, poloduplexní či plně duplexní
- relační vrstva umožňuje zpravidla rozlišovat i priority jednotlivých dat

# Služby relační vrstvy

6

## □ **Uvolnění spojení**

- bud' byl skončen přenos dat a může být tak ukončeno i spojení
- nebo došlo k zadání požadavku na ukončení spojení bez ohledu na to, zda byl přenos dokončen či nikoliv

## □ **Garantovaná služba**

- podržení a zkompletování přijatých dat na úrovni relační vrstvy a jejich následné předání prezentační vrstvě

## □ **Synchronizace relačního spojení**

- definice a identifikace určitých synchronizačních bodů
- nastavení dohodnutého výchozího stavu relačního spojení při ztrátě synchronizace na nižší úrovni
- udržení dialogu při ztrátě dat na transportní úrovni

## □ **Řízení relační vrstvy**

- spuštění, přerušení či rušení aktivit relační vrstvy
- řešení výjimečných stavů

# Prezentační vrstva

7

- samostatně definována pouze v rámci modelu ISO/OSI
- v TCP/IP spadá do aplikační vrstvy
  - ▣ prezentační funkce jsou i v TCP/IP často nezbytné
- stručně popsána již v rámci kap. 1
- hlavní funkce
  - ▣ **prezentace dat**
  - ▣ **komprese dat**
  - ▣ **šifrování dat**

# Prezentace dat

8

- reprezentace dat
  - ▣ každý počítač (OS) může mít svoji vlastní (vnitřní)
  - ▣ způsob jak jsou jednotlivé symboly, znaky apod. ukládány
  - ▣ k porozumění počítačů nutno zabezpečit při komunikaci provádění změn přenášených dat, aniž by se změnil význam přenášené informace
  - ▣ data se převádí do tzv. vnější reprezentace dat
- prezenční vrstva umožňuje překlenutí rozdílů v reprezentaci dat a činností jednotlivých entit aplikační úrovně
- problematikou prezentace se zabývá prakticky každý aplikační protokol
- data protějšího procesu jsou místnímu procesu prezentována v takové formě, kterou běžně používá
  - ▣ nezbytná definice vnější typové reprezentace a převody mezi abecedami či formáty
  - ▣ transformace příkazů s povely podle vlastností jejich příjemce



# Prezentace dat

9

- přenášená data mohou být ve třech syntaktických verzích
  - ▣ **syntaxe vysílače**
    - interně používána vysílací aplikační entitou
  - ▣ **syntaxe přijímače**
    - interně použita přijímací entitou
  - ▣ **přenosová syntaxe**
    - dojednaná syntaxe používaná na přenosové trase
    - referenční (prezentační)
    - důležitá proto, aby existovalo co nejméně různých typů převodu
    - možné, aby se verze příjemce či odesílatele shodovala s verzí přenosovou

# Abstract Syntax Notation One (ASN.1)

10

- jeden ze standardních způsobů reprezentace přenášených informací (data, řídicí pokyny)
- používá se v telekomunikacích a v různých protokolech počítačových sítí
- základní vlastností abstrakce, která umožňuje zápis
  - ▣ ve formě určené pro přenos sítí
  - ▣ nezávisle na specifickém přístupu konkrétní platformy
- standard více organizací (ISO, ITU a další) vedený nejnověji pod označením X.680
- každý datový objekt je vyjádřen pomocí tří polí, tzv. **TLV kódování**
  - ▣ **Typ** – indikace konkrétní typu
  - ▣ **Délka** – délka kódované hodnoty
  - ▣ **Hodnota** – vlastní hodnota dané délky
- neomezuje vlastní implementaci kódování a dekódování
- existuje celá řada kódovacích sad
- lze využít k popisu PDU aplikační úrovně
- Příklad: SNMP (*Simple Network Management Protocol*), protokol k řízení sítě

# Abstract Syntax Notation One (ASN.1)

11

- výstupem posloupnost bitů
  - ▣ určitý počet bitů reprezentuje zvolený typ
  - ▣ určitý počet bitů délku dále uvedené hodnoty
  - ▣ počet bitů daný předcházející veličinu reprezentuje konkrétní hodnotu
- Příklad na jiný přístup – **textový režim**
  - ▣ využíván u několika klasických aplikačních protokolů
    - HTTP
    - FTP
    - SMTP
  - ▣ přenášeny předem dohodnuté textové značky daného typu a vlastní hodnoty

# Kompresa dat

12

- komunikační okruh
  - výměna zpráv mezi procesy
  - cílem maximální propustnost
  - žádoucí předkládat zprávu pro přenos v minimální formě, při zachování informačního obsahu -> kódování zprávy
  - služba komprese dat
- základní kódy dat
  - typicky reprezentují znaky zprávy kódovány určitým počtem bitů
  - např. 8 bitů, tj. existuje až 256 různých znaků
  - znak na vstupu kodéru je na výstupu reprezentován právě jako 8 bitů
  - neefektivní, pravděpodobnost výskytu různých znaků není stejná
- základní metoda komprese dat
  - různá délka reprezentace daného symbolu dle pravděpodobnosti jeho výskytu
  - častější symbol je vyjádřen menším počtem bitů
  - využívají se i vazby mezi symboly, které umožňují kódovat určité kombinace jako by se jednalo o jeden znak

# Kompresa dat

13

## □ Základní kompresní kódy

### □ Huffmanovo kódování

- kóduje každý symbol nezávisle na ostatních znacích
- odpovídá principiálně Morseově abecedě, prvky abecedy mají různé délky (různý počet bitů)
- počet použitých bitů u nejméně pravděpodobného znaku závislý na počtu možných symbolů v systému

### □ Aritmetické kódování

- založeno na reprezentaci znaků a skupin znaků reálnými čísly z rozsahu 0 až 1

### □ LZW (Lempel–Ziv–Welch) kódování

- tabulková metoda
- obě strany komunikace znají určité převodní tabulky
- využívá se společná reprezentace pravděpodobných kombinací znaků

## □ Příklad možnosti komprese v TCP/IP – protokol SSH (Secure Shell)

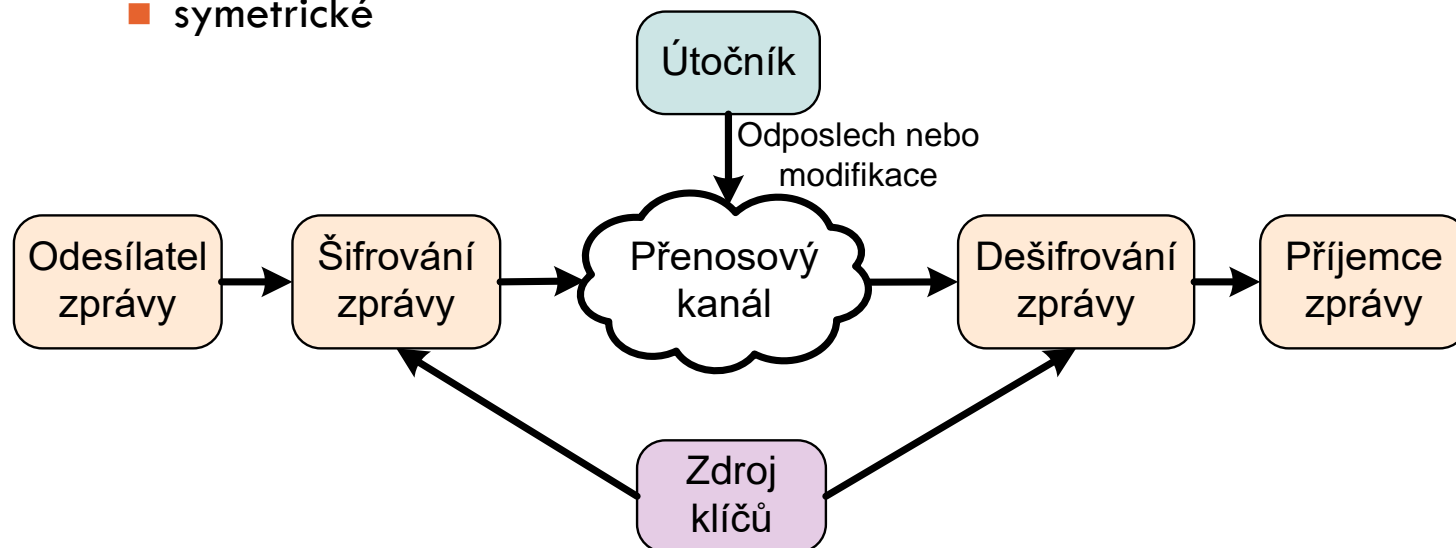
## □ Kompresa dat významná u pomalých přenosových tras, kde časová náročnost provedení komprese bude malá vzhledem k úspoře času vlastního přenosu

# Šifrování dat

14

## □ Kryptografie

- ▣ nauka o metodách utajení obsahu (přenášené) zprávy
- ▣ transformace do podoby, která je čitelná pouze vlastníkoví speciální znalosti
- ▣ může sloužit i k autentizaci nebo jiným účelům
- ▣ opakem dešifrování
- ▣ dva základní způsoby
  - asymetrické
  - symetrické



# Šifrování dat

15

- metoda kódování dat
- může být obecně prováděno i na jiných vrstvách
- v rámci TCP/IP často protokoly TLS/SSL (*Transport Layer Security / Secure Socket Layer*)
  - ▣ umožňující zabezpečenou komunikaci
  - ▣ zabezpečení nad transportní úrovní
  - ▣ řadí se do aplikační vrstvy, formálně prezentační vrstva
  - ▣ šifrovány pouze data aplikační vrstvy
  - ▣ šifrovaný kanál má koncový charakter, bez zásahu mezilehlých prvků či uzlů
  - ▣ detailní popis protokolů nad rámec kurzu
  - ▣ př.: protokol HTTPS (zabezpečená verze HTTP protokolu)

