UPV_0004 a UPVK_0004 Informační a komunikační technologie 1

Referenční model ISO/OSI

Protokoly

IEEE 802.11

Paměťové karty

Referenční model ISO/OSI

- vypracovala organizace ISO
- standardizace počítačových sítí nazvané OSI
- v roce 1984 ho přijala jako mezinárodní normu ISO 7498
- ISO/OSI model se používá jako názorný příklad řešení komunikace v počítačových sítí pomocí vrstevnatého modelu
  - jednotlivé vrstvy jsou nezávislé a snadno nahraditelné

Referenční model ISO/OSI

- síťová komunikace je vcelku složitý problém
  - rozdělena do tzv. vrstev, které znázorňují hierarchii činností
- má poskytnout základnu pro vypracování norem pro účely propojování systémů
- neříká, jak realizovat síťové systémy
  - uvádí všeobecné principy sedmivrstvé síťové architektury

Referenční model ISO/OSI

- přenos informací mezi vrstvami je přesně definován
  - vrstva vždy využívá služeb vrstvy nižší a poskytuje služby vrstvě vyšší

Referenční model ISO/OSI

- V praxi je model použit k programování součástí síťového subsystému v modulech, které reprezentují jednotlivé vrstvy a komunikují mezi sebou
  - to umožňuje jednotlivé části snadněji naprogramovat a nezávisle nahrazovat
    - vyměnit síťovou kartu, ovladač, aplikaci a zároveň ponechat ostatní součásti beze změny

Referenční model ISO/OSI

- architektura členěna do sedmi vrstev
  - aplikační (a*pplication laye*r)
  - prezentační (*presentation layer)*
  - relační (*session layer*)
  - transportní (*transport layer*)
  - síťová (*network layer)*
  - spojová/linková (*link layer)*
  - fyzická (*physical layer*)

Referenční model ISO/OSI

– aplikační (a*pplication laye*r)
  - účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci
  - služby a protokoly: ***FTP***, ***DNS***, ***DHCP***, ***POP3***, ***SMTP***, ***SSH***, ***Telnet***, TFTP

Referenční model ISO/OSI

- prezentační (*presentation layer)*
  - transformovat data do tvaru, který používají aplikace
  - dochází k transformaci pro účel přenosu dat nižšími vrstvami
    - převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů …
  - vrstva se zabývá strukturou dat, ne jejich významem, který je znám jen vrstvě aplikační

Referenční model ISO/OSI

- relační (*session layer)*
  - vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamovaní výjimečných stavů
  - k paketům přiřazuje synchronizační značky, které využije v případě vrácení paket k poskládání původního pořadí
    - z důvodu, že se během přenosu dat poškodí síť
  - patří sem: ***NetBIOS***, AppleTalk, RPC, ***SSL***

Referenční model ISO/OSI

– transportní (*transport layer*)
  - zajišťuje přenos dat mezi koncovými uzly
  - má poskytnout takovou kvalitu přenosu, jakou požadují vyšší vrstvy

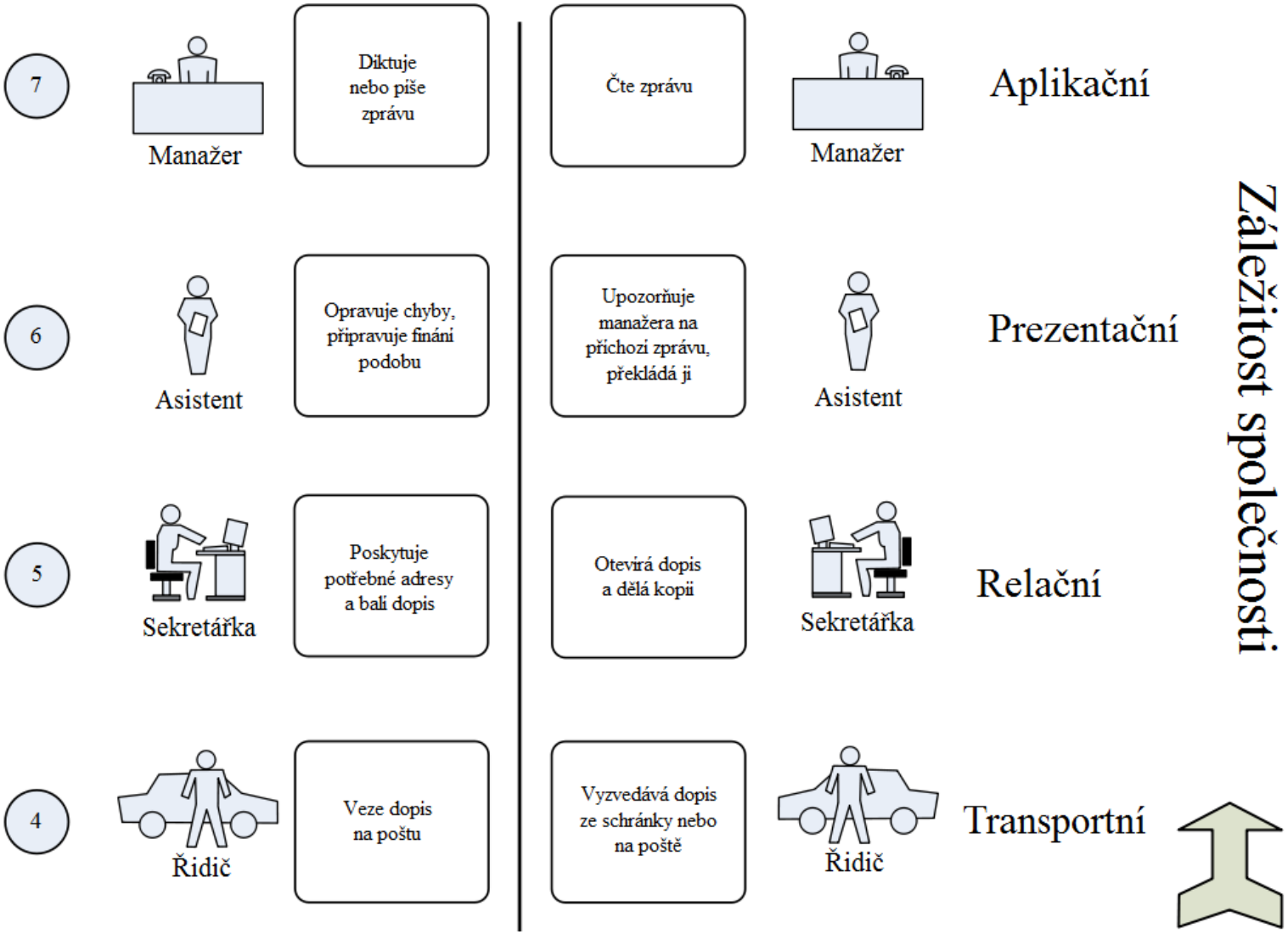
Referenční model ISO/OSI

– síťová (*network layer)*
  - poskytuje funkce k zajištění přenosu dat různé délky od zdroje k příjemci skrze jednu případně několik vzájemně propojených sítí při zachování kvality služby, kterou požaduje přenosová vrstva
  - na této vrstvě pracuje protokol ***IP*** (Internet Protocol)

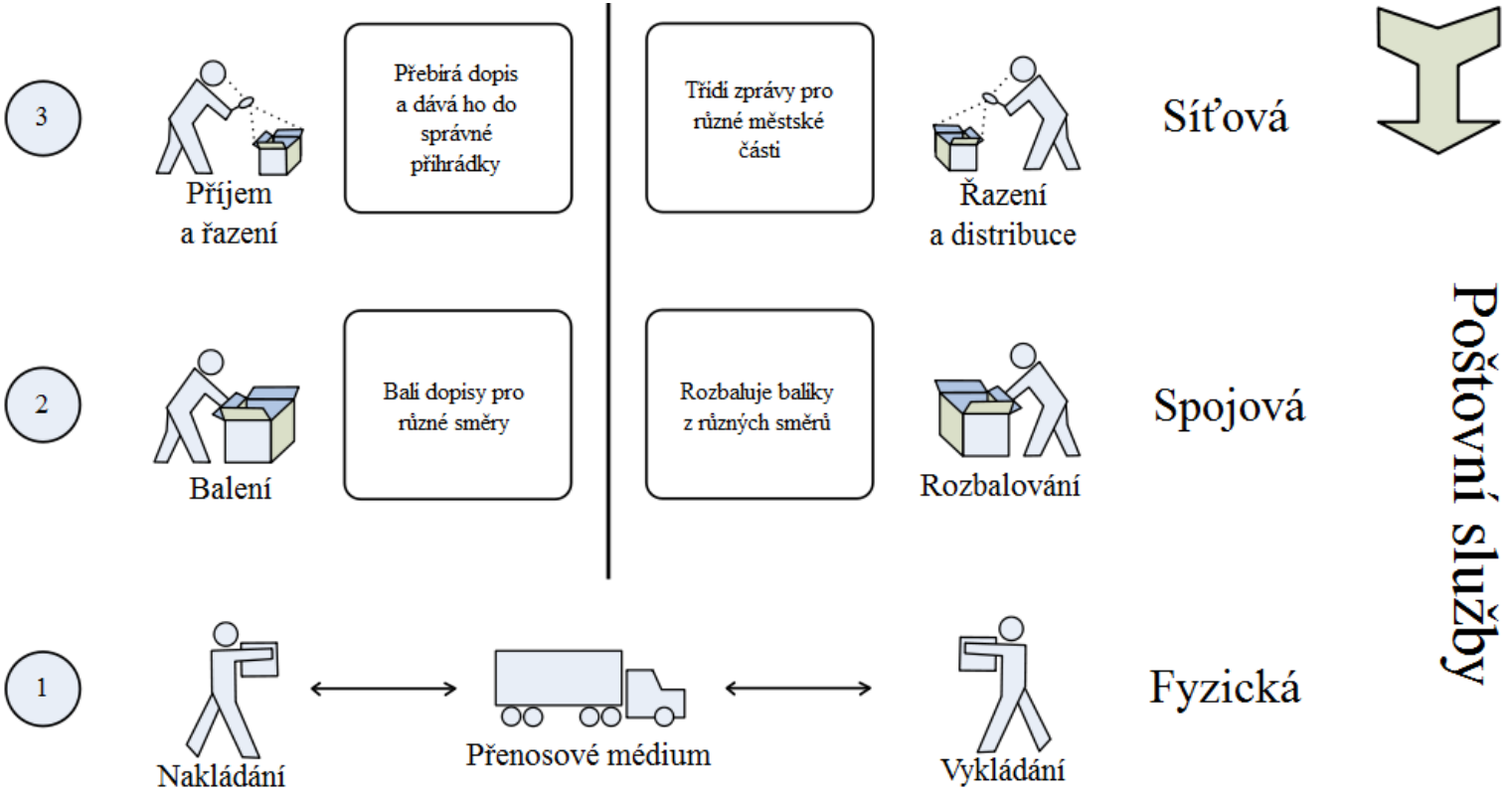
Referenční model ISO/OSI

– spojová/linková (*link layer)*
  - poskytuje spojení mezi dvěma sousedními systémy (switch ⇔ PC)
  - seřazuje přenášené rámce (data), stará se o nastavení parametrů přenosu linky
  - Formátuje fyzické rámce (data), opatřuje je fyzickou adresou (***MAC*** adresou)
– fyzická (*physical layer*)
  - zajišťuje fyzickou komunikaci
  - HW - Repeater, Hub, Modem, Síťová karta

Referenční model ISO/OSI



Referenční model ISO/OSI



Paralela mezi RM – OSI a dopisy

Protokoly

- ***TCP/IP*** (***T***ransmission ***C***ontrol ***P***rotocol/***I***nternet ***P***rotocol)
  - sada protokolů pro komunikaci v PC síti
  - hlavní protokol sítě Internet
  - architektura členěna do čtyř vrstev
    - ***aplikační*** (application layer)
    - ***transportní*** (transport layer)
    - ***síťová*** (network layer)
    - ***vrstva síťového rozhraní*** (network interface)

Protokoly

- ***Základní protokoly TCP/IP***
  - ***SSL*** (***S***ecure ***S***ockets ***L***ayer)
    - protokol (vrstva) vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP)
    - poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
    - následníkem protokol ***TLS*** (***T***ransport ***L***ayer ***S***ecurity)

Protokoly

- ***SSH*** (***S***ecure ***Sh***ell)
  - program a zároveň pro zabezpečený komunikační protokol v počítačových sítích
  - náhrada za telnet a další, které posílají heslo v nezabezpečené formě a umožňují tak jeho odposlechnutí při přenosu pomocí počítačové sítě
  - programy: ***PuTTY***, SSH klient

Protokoly

- ***IP*** (***I***nternet ***P***rotocol)
  - základní protokol síťové vrstvy a celého Internetu
  - ***IPv4*** (***I***nternet ***P***rotocol ***v***ersion ***4***)
    - 32 bitové adresy (4 x 8bitů)
      - » cca $4 \cdot 10^9$ (= 2^{32}) různých IP adres
      - » dnes nedostačující
  - ***IPv6*** (***I***nternet ***P***rotocol ***v***ersion ***6***)
    - 128 bitové adresy
      - » cca $3{,}4 \cdot 10^{38}$ (= 2^{128}) různých IP adres
    - podpora bezpečnosti
    - podpora pro mobilní zařízení
    - jednoduchý přechod z IPv4

Protokoly

- ***Aplikační protokoly (služby) TCP/IP***
  - ***HTTP*** (***H***yper***t***ext ***T***ransfer ***P***rotocol)
    - protokol pro přenos hypertextových dokumentů (HTML)
    - používá obvykle port 80
    - funguje způsobem dotaz-odpověď

Protokoly

- ***HTTPS*** (***H***yper***t***ext ***T***ransfer ***P***rotocol ***S***ecure)
  - nadstavba protokolu HTTP
  - přenášená data jsou šifrována pomocí SSL nebo TLS
  - na straně serveru používá obvykle port 443
  - umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem
    - před odposloucháváním, podvržením dat
    - umožňuje ověřit identitu protistrany

Protokoly

- ***WebDAV*** (***Web***-based ***D***istributed ***A***uthoring and ***V***ersioning)
  - rozšíření HTTP protokolu
  - poskytuje možnost kooperace a vzdálené správy souborů uložených na webovém serveru
  - postačuje internetový prohlížeč
- ***FTP*** (***F***ile ***T***ransfer ***P***rotocol)
  - protokol pro přenos souborů mezi PC pomocí sítě
  - používá obvykle porty 20 a 21
  - doporučuje se speciální program (Total Commander)

Protokoly

- ***POP3*** (***P***ost ***O***ffice ***P***rotocol version ***3***)
  - protokol pro stahování emailových zpráv ze vzdáleného serveru na klienta
  - ze serveru se stáhnou všechny zprávy
    - ty co uživatel nechce číst nebo spam
- ***IMAP*** (***I***nternet ***M***essage ***A***ccess ***P***rotocol)
  - protokol pro vzdálený přístup k e-mailové schránce
  - umí pracovat v tzv. on-line i off-line režimu
  - nabízí pokročilé možnosti vzdálené správy
    - práce se ***složkami***, přesouvání zpráv, prohledávání na straně serveru a podobně
  - v současnosti se používá protokol IMAP4

Protokoly

- ***DNS*** (***D***omain ***N***ame ***S***ystem)
  - úkolem jsou vzájemné převody doménových jmen a IP adres
  - http://www.centrum.cz = http://213.29.7.27
  - jednotlivé části (subdomény – viz následující slide)
    - mohou mít až 63 znaků
    - skládat se mohou až do celkové délky doménového jména 255 znaků
    - doména může mít až 127 úrovní

Protokoly

- Adresu webu tvoří několik domén oddělených tečkami
  - http://3_úroveň.2_úroveň.generická_doména
    - » Před třetí úrovní může být ještě čtvrtá, pátá atd.
  - Například: http://www.centrum.cz

1. cz - generická doména (doména 1. řádu)
2. centrum - doména 2. řádu (o tom to celé je)
3. www - doména 3 řádu (nejčastěji www nebo jméno počítače)
4. součástí adresy bývá i cesta k souboru psaná za lomítkem (v tomto případě tam není)

Protokoly

- ***DHCP*** (***D***ynamic ***H***ost ***C***onfiguration ***P***rotocol)
  - DHCP server přiděluje PC pomocí DHCP protokolu
    - IP adresu, masku sítě, implicitní bránu, adresu DNS serveru
    - platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje

IEEE 802.11

- ***SSID*** (***S***ervice ***S***et ***Id***entifier)
  - jedinečný identifikátor každé bezdrátové (WiFi) sítě
  - až 32 ASCII znaků
  - přístupový bod (***AP*** (***A***ccess ***P***oint)) vysílá pravidelně svůj identifikátor v tzv. majákovém rámci (beacon frame), lze ale zakázat vysílání SSID
  - klienti si mohou vybrat, ke které bezdrátové síti se připojí

IEEE 802.11

- ***Wi-Fi***
  - Název původně neměl znamenat nic
  - časem se z něj stala slovní hříčka ***wireless fidelity*** (bezdrátová věrnost)
    - analogicky k Hi-Fi (***high fidelity*** – vysoká věrnost)
  - používá bezplatného frekvenčního pásma ***2,4 GHz***

IEEE 802.11

- Zabezpečení Wi-Fi sítě
  - Zablokování vysílání SSID
  - Kontrola MAC adres
  - WEP (***W***ired ***E***quivalent ***P***rivacy)
    - šifrování pomocí statických WEP klíčů symetrické šifry (používá k šifrování i dešifrování jediný klíč)
    - ručně nastaveny na obou stranách bezdrátového spojení
    - lze jej „relativně snadno“ analyzovat ze zachycených paketů

IEEE 802.11

- WPA (***W***i-Fi ***P***rotected ***A***ccess)
  - využívá WEP klíče kvůli zpětné kompatibilitě
  - klíče jsou ale dynamicky bezpečným způsobem měněny
- WPA2(***W***i-Fi ***P***rotected ***A***ccess ***2***)
  - kvalitnější šifrování (šifra AES)
  - vyžaduje ale větší výpočetní výkon, proto nelze WPA2 používat na starších zařízeních
  - od 13. března 2006 je certifikace WPA2 povinná pro všechna nová zařízení, která chtějí být certifikována jako Wi-Fi

IEEE 802.11

Standard	Pásmo [GHz]	Maximální rychlost [Mbit/s]
IEEE 802.11 (původní)	2,4	2
IEEE 802.11a	5	54
IEEE 802.11b	2,4	11
IEEE 802.11g	2,4	54
IEEE 802.11n	2,4 nebo 5	150/300/600

IEEE 802.11

- Struktura bezdrátové sítě
  - Ad-hoc sítě
    - dva klienti se připojí navzájem, jsou v rovnocenné pozici (peer-to-peer)
  - Infrastrukturní sítě
    - obsahuje jeden nebo více přístupových bodů (AP (Access Point))
    - několik přístupových bodů může mít stejný SSID identifikátor

Paměťové karty

- Typy karet
  - CompactFlash (CF)
  - Secure Digital (SD)
    - Mini Secure Digital (Mini SD)
    - Micro Secure Digital (Micro SD, dříve TransFlash)
  - XD Picture card (XD)
  - Multimedia card (MMC)
    - Multimedia card mobile (MMCmobile)
    - Reduce size multimedia card (RSMMC)
    - Multimedia card plus (MMCplus)
    - Micro Multimedia card (MMCmicro)
  - Memory Stick (MS)

Paměťové karty

- Přenosová rychlost
  - buď jako přímé hodnoty v MB/s
    - například "30 MB/s„ většinou uvedeno jako ***maximální***
  - jako u optických mechanik násobkem základní čtecí rychlosti 150 kB/s
    - například "200x„ většinou uvedeno jako ***maximální***
      - 150 kB/s x 200 = 30 000 kB/s = 30 MB/s
  - třída rychlosti – ***minimální*** přenosová rychlost

2	4	6	10
2 MB/s	4 MB/s	6 MB/s	10 MB/s

Paměťové karty

- ***SD*** nebo ***SDHC***?
  - SD jsou určeny pro kapacity do 2 GB
    - díky formátu FAT16
  - SDHC jsou určeny pro kapacity nad 2 GB
    - díky formátu FAT32
  - rozměry a mechanické provedení obou karet je stejné
  - kartu typu SDHC nelze použít ve standardních SD slotech, musíte mít SDHC slot
    - opačně to ale lze, jsou zpětně kompatibilní

Paměťové karty

- Důležité parametry
  - Kapacita
  - Rychlost zápisu / čtení na kartu a Flash
    - Corsair Voyager GT (Flash Disk)
      - rychlost čtení až 34 MB/s
      - rychlost zápisu až 28 MB/s
    - SanDisk Secure Digital Extreme III
      - rychlost čtení a zápisu až 20 MB/s
  - U karet, do jakého zařízení ji potřebuji z tedy jaký typ potřebuji