Počítačové sítě

Jan Outrata

KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI

přednášky

Tyto slajdy byly jako výukové a studijní materiály vytvořeny za podpory grantu FRVŠ 1358/2010/F1a.

Síťové architektury

Síťová architektura

- snaha o vytvoření univerzálního konceptu sítě – topologie, formy a pravidla komunikace, poskytované služby atd.
- vytvářely (a vytvářejí) souběžně, ale nezávisle firmy (IBM), (telekomunikační) organizace, **normalizační instituce** (ITU-T, ISO, IEEE, IEC, ANSI, IETF a další (ČSNI)) a **průmyslová konsorcia** (GEA, WLANA aj.) → nekompatibilní řešení
- **požadavky**: decentralizace služeb, rozumná adresace uzlů, navazování spojení mezi uzly, data zasílána v nezávislých blocích, směrování bloků, zabezpečení, kontrola a řízení přenosu, aj.
- dříve proprietární uzavřená řešení, následně standardizace s koncepcí komunikace nezávisle na implementaci (výrobci zařízení)

→ komunikace ve **vrstvách**:

- definovaných službami poskytovanými (sousedním) vyšším vrstvám a využívajících služeb (sousedních) nižších vrstev, implementace skryté před okolními vrstvami
- samostatné, s funkcemi podobnými v rámci vrstvy a odlišnými v různých vrstvách, nezávislé na implementaci

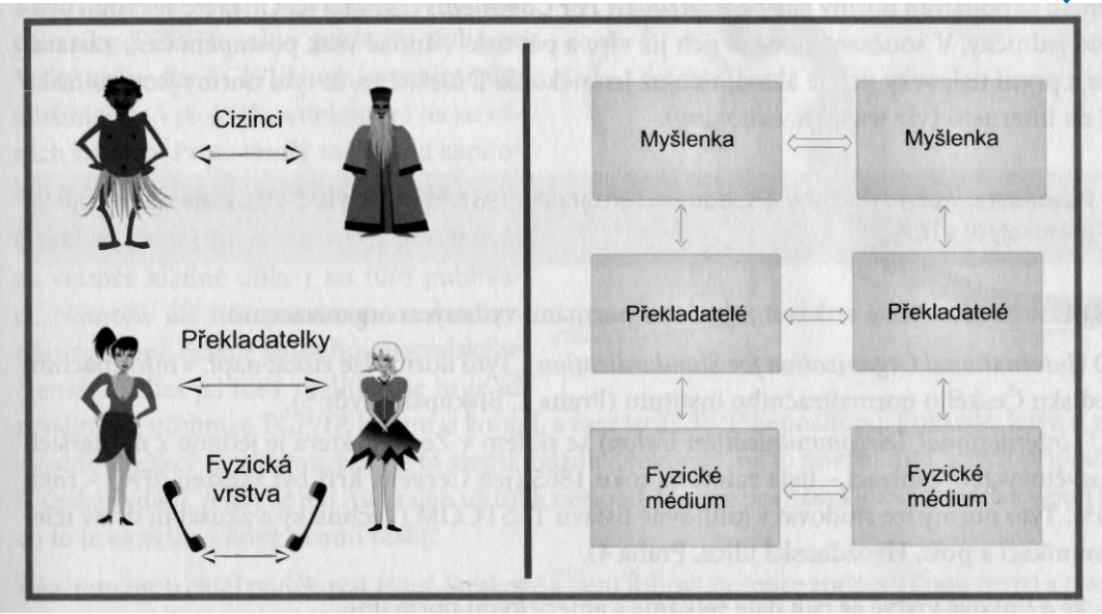
Síťová architektura

- komunikace mezi vrstvami (svislý směr) pomocí **mezivrstvových protokolů** – na každé komunikující straně zvlášť, skrze **programová rozhraní**, prostřednictvím přístupových bodů, využívajících tzv. služební primitiva, fyzická, př. komunikace člověka s překladatelem

Obrázek: Obrázek průvodce 16

- obecná **služební primitiva** (druhé a poslední nepovinná):
  - žádost o službu (**request**)
  - oznámení poskytovatele o přijetí žádosti (**indication**)
  - odezva poskytovatele (**response**), příp. vytvoření spojení
  - potvrzení odezvy žadatelem (**confirmation**)
- komunikace mezi entitami (zařízeními) ve stejnolehlých vrstvách (vodorovný směr) pomocí **vrstvových protokolů** – entity z různých komunikujících stran, implementace služebních primitiv, fyzická na nejnižší vrstvě, jinak virtuální (zprostředkovaná nižšími vrstvami), př. komunikace cizinců

Síťová architektura



Síťová architektura

Protokol = souhrn pravidel (**norem** a **doporučení**) a procedur pro komunikaci (výměnu dat), synt. a sem. pravidla výměny protokolových datových jednotek

- **protokolové datové jednotky** = **režijní informace** a data, např. rámce, pakety, segmenty
- komunikace zprostředkovaná sousední nižší vrstvou
- na straně odesílatele od nejvyšší po nejnižší vrstvu **„zapouzdřování“** dat do protokolových jednotek, na straně příjemce v opačném směru **„rozbalování“** dat, př.
- pro komunikaci na jedné vrstvě je možné použít více různých protokolů na sousední nižší vrstvě
- protokol může garantovat příjem dat v pořadí odeslaní (typicky u spojovaných, spolehlivých služeb), ale také nemusí (typicky u nespojovaných, nespolehlivých služeb, přeskládání do správného pořadí řeší vyšší vrstva)
- vydávají normalizační instituce a průmyslová konsorcia, některé jsou zdarma (RFC, RIPE)

Síťová architektura

Síťová (protokolová) architektura = definice vrstev, služeb, funkcí, protokolů a forem komunikace

- **normalizované** de jure (normy OSI) i de facto (TCP/IP, doporučení a normy RFC)
- firemní proprietární (Novell NetWare, Apple Appletalk, Microsoft NetBEUI a SMB aj.)

Abstraktní referenční síťový model architektur od ISO

= **abstrakce** konkrétních síťových architektur, reference pro nové

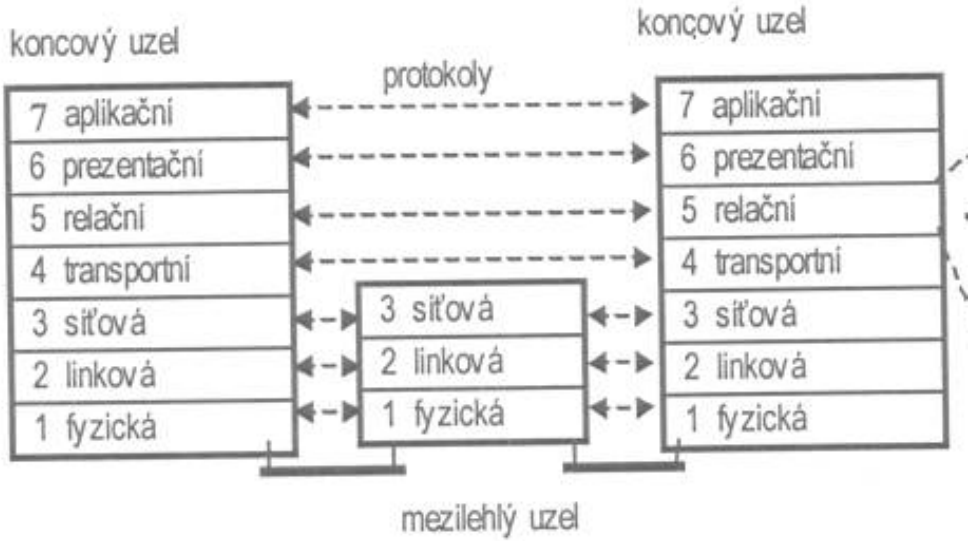
- architektury nemusí podporovat všechny funkce modelu (např. průmyslové sítě nepodporují směrování, sítě jsou propojeny pomocí mostů a bran)

Referenční model ISO OSI (Open Systems Interconnection)

- **propojení otevřených systémů** = zařízení podporujících příslušné normy
- obecně platné principy implementace systémů (abstrakce síťové architektury), pozn. existuje i konkrétní architektura OSI s konktrétními protokoly!
- norma ISO IS 7498, 1979, referenční model ITU X.200, 1984
- definuje **koncové uzly** (**koncová datové zařízení, DTE**) a **mezilehlé uzly** zprostředkovávající komunikaci (**propojovací prvky, DCE**)
- vrstvy: fyzická, linková, síťová, transportní, relační, prezentační a aplikační

Obrázek: Obrázek sítě 32

Referenční model ISO OSI (Open Systems Interconnection)



RM OSI – Fyzická vrstva

- způsoby fyzické komunikace, **přenos sledu signálů** (bitů nebo skupin bitů) mezi přímo propojenými zařízeními, **bez ohledu na význam** bitů
- přenosové cesty elektrické, optické, drátové, bezdrátové
- komunikující zařízení na **fyzickém** nebo **virtuálním okruhu** (pevný nebo komutovaný)
- funkce a služby:
  - správa fyzických spojení a okruhů mezi DTE a DCE, identifikace okruhů
  - seřazování bitů (stejné na vstupu i výstupu)
  - udržování **parametrů** (přenosová rychlost, doba, ztráta) a oznamování poruch
- protokoly specifikující bity jako signály (kódování 0 a 1), tvary konektorů, typy médií (kroucená dvojlinka, optické vlákno, mikrovlny), přenosovou rychlost a jiné parametry apod.
- protokoly př. V.24/RS 232, **EIA/TIA 568A/B**, WiFi/Bluetooth, ISDN, DSL, vydávají organizace ITU-T, EIA/TIA aj.
- HW zařízení (nejsou součástí modelu) př. fyzické rozhraní síťové karty/adaptéru, propojovací kabely a panely, modem, sériová linka a porty, opakovač aj.

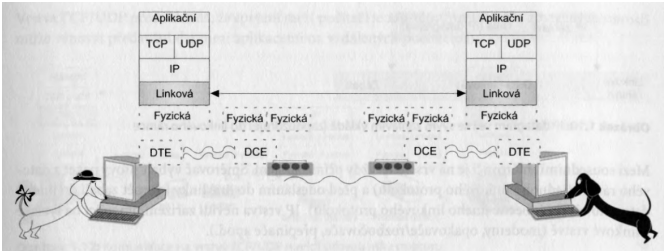
RM OSI – Linková vrstva

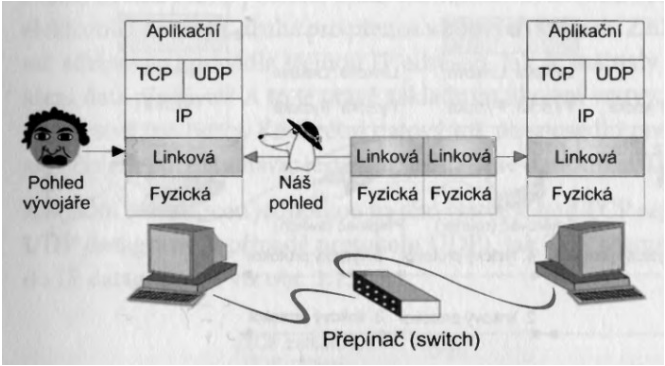
- (dynamické) zajištění **výměny dat mezi sousedními zařízeními** (DTE) = **v dosahu protokolu** (v MAN/WAN nebo v rámci LAN), bity mají význam (data)
- zařízení má jednu **linkovou adresu**

Obrázek: Obrázek průvodce 21

- jednotka přenosu = **datový rámec**: **záhlaví** s linkovou adresou příjemnce a odesílatele (př. MAC u Ethernetu) + data + **zápatí** s kontrolním součtem (CRC) **celého rámce**, přenášen fyzickou cestou
- funkce a služby:
  - správa linkových spojení, řízení fyzických okruhů, identifikace zařízení
  - formátování rámců
  - oznamování (neopravitelných) chyb, detekce a oprava chyb
- protokoly př. **Ethernet**, **WiFi**, Bluetooth, PPP/DSL, SLIP, ISDN, Frame Relay, FDDI aj.
- HW zařízení př. síťová karta/adaptér, přepínač, most, přístupový bod aj.

RM OSI – Linková vrstva





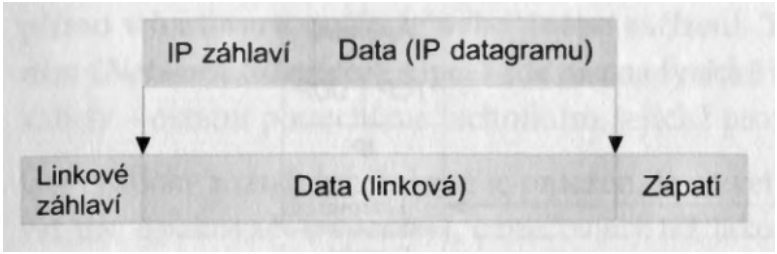
RM OSI – Síťová vrstva

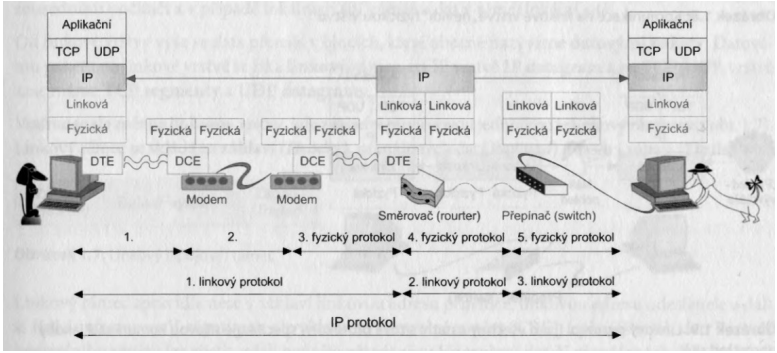
- zajišťuje **přenos dat mezi vzdálenými, nesousedními zařízeními** v různých sítích spojených do jedné rozsáhlé sítě (př. WAN, Internet)
- zařízení může mít více jednoznačných **síťových adres**

Obrázek: Obrázek průvodce 22

- jednotka přenosu = **síťový paket**: **záhlaví** se síťovou adresou příjemce a odesílatele (např. IP u Internetu) + data + zápatí jen vyjímečně, přenášen v datovém rámci (datové části)
- funkce:
  - **abstrakce** různých linkových technologií
  - správa linkových spojení, **multiplexování** síťových spojení do linkových
  - formátování dat do paketů
  - **směrování** paketů
  - zjišťování a oprava chyb
  - vytváření **podsítí**

RM OSI – Síťová vrstva





RM OSI – Síťová vrstva

- služby:
  - síťové adresování
  - správa síťových spojení
  - převod transportních paketů (datagramů) na síťové pakety
  - oznamování chyb, řízení toku dat
- přenos dat **se spojením (proudový = stream)** nebo **bez spojení (datagramový)**
- protokoly př. **IP** (bez spojení), CONP a CLNP, X.25 (WAN)
- HW zařízení př. síťová karta (vyšší funkce), směrovač, brána

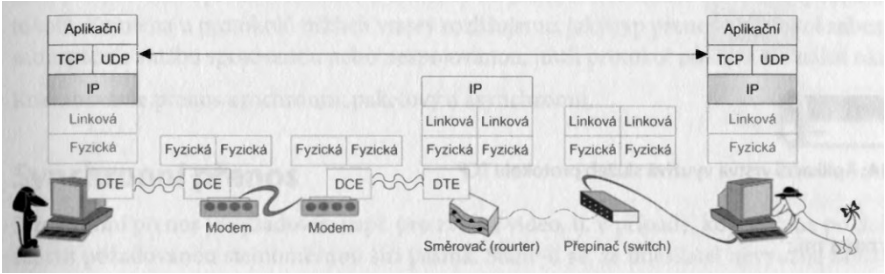
RM OSI – Transportní vrstva

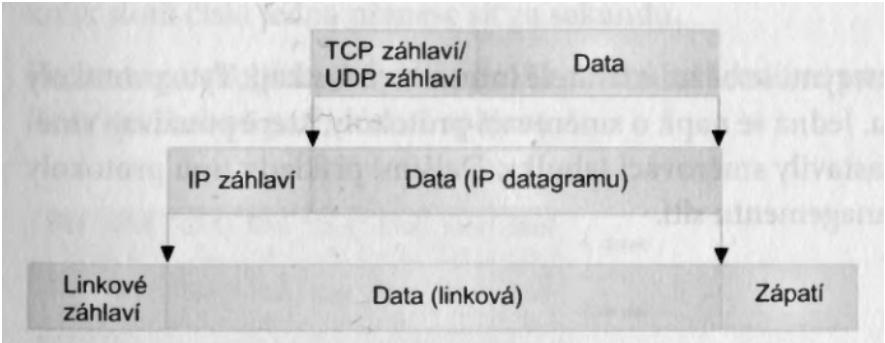
- zprostředkovává **transparentní spojení** s přenosem dat s požadovanou kvalitou **mezi klienty (aplikacemi)** v rámci jednoho síťového zařízení (počítače)
- aplikace může mít více **transportních adres**
- **propojení koncových zařízení**, nejnižší vrstva s entitami pouze v koncových systémech
- stojí mezi uživatelem a sítí

Obrázek: Obrázek průvodce 23

- jednotka přenosu = **transportní paket (datagram)**: **záhlaví** s transportní adresou příjemnce a odesílatele (např. TCP/UDP port u Internetu) + data, přenášen v síťovém paketu

RM OSI – Transportní vrstva





RM OSI – Transportní vrstva

- funkce:
  - adresování (transportní na síťové)
  - správa síťových spojení nebo přenosu datagramů
  - **multiplexování a větvení** transportních spojení do síťových
  - rozdělení dat na datagramy, formátování, **segmentace**
  - **řízení "proudu" dat** (správné pořadí datagramů), optimalizace služeb
  - koncová detekce a oprava chyb
- služby (parametrizované - propustnost/rychlost přenosu, doba):
  - transparentní přenos dat s **potvrzováním** (**"spolehlivý"**) nebo bez potvrzování (**"nespolehlivý"**)
  - správa transportních spojení
  - identifikace relační entity (transportní adresou)
  - **duplexní** přenos, **zacházení s daty jako s proudem**
- protokoly **TCP, UDP**, TP0-4, všechny koncové

RM OSI – Relační vrstva

- zabezpečuje **organizovanou výměnu dat mezi aplikacemi**, zprostředkovává **relaci/sezení** (např. sdílení síťového disku)
- jednotka přenosu = **relační paket**: pouze data, přenášen v datagramu
- funkce:
  - organizace a synchronizace dialogu výměny dat (pomocí **kontrolních bodů**)
  - zobrazení (několika) relačních spojení do (několika) transportních
  - správa transportních spojení
- služby:
  - správa a řízení relace (spojení)
  - různý přenos zpráv, řízení interakce
- protokol př. RPC, X.225, X.215 (OSI)

RM OSI – Prezentační vrstva

- poskytuje **jednotnou reprezentaci a zabezpečení informace** (dat, struktur), v jaké jsou dostupné aplikacím a v jaké se přenáší sítí
- funkce a služby:
  - transformace a výběr reprezentace dat (převod kódů, př. který je nejvyšší bit - **big**/little **endian**)
  - formátování, komprese, zapezpečení (šifrování), integrita dat
  - žádosti o správu relace, transparentní přenos zpráv (nezná jejich význam)
- "protokoly" př. **ASCII**, ASN.1 (kódování BER, DER), multimediální formáty, X.226, X.216 (OSI)

RM OSI – Aplikační vrstva

- poskytuje aplikacím **přístup ke komunikačnímu systému** a **aplikační funkce a služby**
- předepisuje **aplikační formát dat**, **záhlaví dat** + data
- funkce:
  - zprostředkování funkcionality sítě
  - řešení aplikační funkcionality – přenos zpráv, určení kvality, synchronizace
  - identifikace, stanovení pověření
  - dohoda o ochraně, dohody o opravách chyb a syntaxi (kódy, abecedy)
- protokoly př. SMTP, MHS (pošta), FTP, FTAM (přenos souborů), Telnet, VT (vzdálený přístup), SNMP, CMIP (management) a mnoho dalších

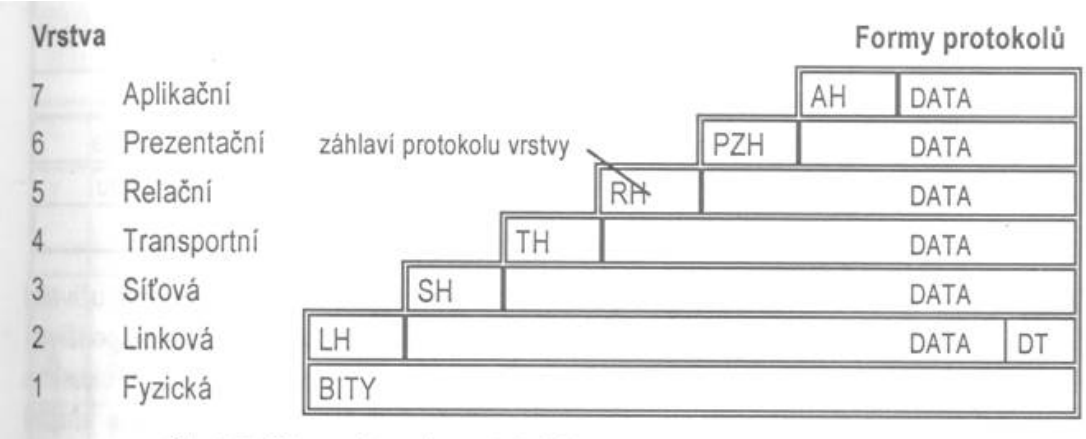
RM OSI – funkce společné více vrstvám

- výměna dat až po vytvoření spojení všemi nižšími vrstvami
- řízení toku, formátování a zabezpečení dat

Obrázek: Obrázek sítě 33

- **rozkládání a skládání datových jednotek** – fragmentace a segmentace: datagramy, pakety, rámce, sled bitů nebo oktety

RM OSI – funkce společné více vrstvám



RM OSI – funkce společné více vrstvám

- komunikace **se spojením** má 3 fáze: 1. navázání spojení, 2. přenos dat, 3. ukončení spojení
  - dohoda na parametrech, identifikace spojení
  - použití **potvrzování** přijetí či nepřijetí datových jednotek protokolu ("**spolehlivost**")
  - **stejné pořadí dat** na vstupu i výstupu
- komunikace **bez spojení**
  - při každém přenosu vždy všechny parametry
  - **nezávislý přenos** datových jednotek
  - může být různé pořadí datových jednotek na vstupu a výstupu
  - **datagramová služba**, může být "spolehlivá" i "nespolehlivá"
- konverze mezi těmito typy služby (původně ale jen se spojením, transportní služby musí být se spojením)

TCP/IP (Transmission Control Protocol/Internet Protocol)

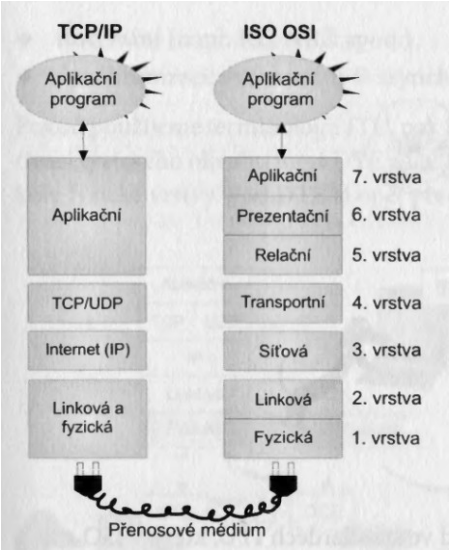
- použití v síti **Internet** (největší celosvětová síť propojených heterogenních sítí), **nejpoužívanější síťová architektura**
- všechny informace (konvence, protokoly, doporučení) v **RFC (Request For Comments)** od IAB (rada pro architekturu Internetu), de facto normy **IETF** (komise s pracovními skupinami Internetu)
- historie:
  - vyvinuta v 60.-70. letech na objednávku (D)ARPA USA: propojení počítačů vojenských, výzkumných a akademických pracovišť
  - **ARPANET** 1971 (23 uzlů, 1973 VB a Norsko, 1989 s více jak 1000 uzly zrušen, místo něj NSFNET)
  - původní protokol NCP (Network Control Protocol)
  - 70. léta univerzitní vývoj (Network Measurement Centre, UCLA, **Vinton G. Cerf**), vznikají RFC
  - 1982 **TCP/IP** = Internet, implementace v OS UNIX
  - od počátku 90. let i soukromé využití (výrobní společnosti, poskytovatelé služeb, soukromé osoby a další)
  - dnešní rozsah těžké odhadnout

TCP/IP (Transmission Control Protocol/Internet Protocol)

Obrázek: Obrázek průvodce 17

- vrstvy: síťového rozhraní (odpovídá fyzické a linkové z RM OSI), mezisíťová (internet, síťová z RM OSI), transportní, aplikační (3 nejvyšší z RM OSI)
- **vlastní protokoly**, obecně nesrovnatelné s protokoly OSI (TCP/IP vznikla dřív), ale protokoly TCP/IP využívají protokolů OSI a naopak
- dominantní: rozšiřování Internetu, propojení (privátních) sítí, internetové aplikace
- síť tvořena: směrovači (modemy), specializovanými bránami (bezpečnostní, aplikační, telekomunikační), lokálními sítěmi a koncovými zařízeními

TCP/IP (Transmission Control Protocol/Internet Protocol)



TCP/IP (Transmission Control Protocol/Internet Protocol)

Vrstva síťového rozhraní

- **přístup** k přenosovému médiu, **specifická** pro každé přenosové prostředí
- využívá všech typů přenosových prostředí a protokolů fyzické a linkové vrstvy z RM OSI, **využití** definováno v RFC

Vrstva internet

- řeší přenos a **směrování** datagramů na základě síťových (IP) adres
- protokoly **IP** (v4 a v6, síťový), (R)ARP (mapování adres), ICMP (řídící hlášení), OSPF, IGRP (směrování)

Transportní

- transportní služba se spojením ("spolehlivý" protokol **TCP**) nebo bez spojení ("nespolehlivý" protokol **UDP**)
- také směrovací protokoly RIP, BGP
- identifikace aplikačního protokolu **číslem portu** (seznam v RFC 1700)

TCP/IP (Transmission Control Protocol/Internet Protocol)

Aplikační

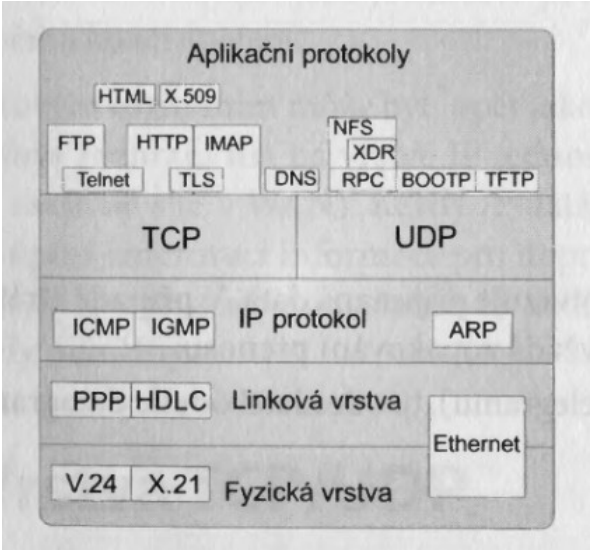
- **mnoho protokolů**, některé používají TCP, jiné UDP, některé oba, nelze o nich říct nic obecného, služby i protokoly se principiálně liší
- uživatelské protokoly:
  - TCP: **HTTP**, **SMTP**, Telnet, **SSH**, FTP, **IMAP**, POP3, Talk
  - UDP: NFS, BOOTP, TFTP, RPC
  - UDP, TCP: NTP
- služební protokoly (pro funkci sítě):
  - UDP, TCP: **DNS**
  - UDP: DHCP
  - TCP: směrovací, SNMP
- „prezentační-aplikační“ protokoly: **SSL**, S/MIME (zabezpečení dat), virtuální terminál (prezentace, **Telnet**, FTP, SMTP), ASN.1

TCP/IP (Transmission Control Protocol/Internet Protocol)

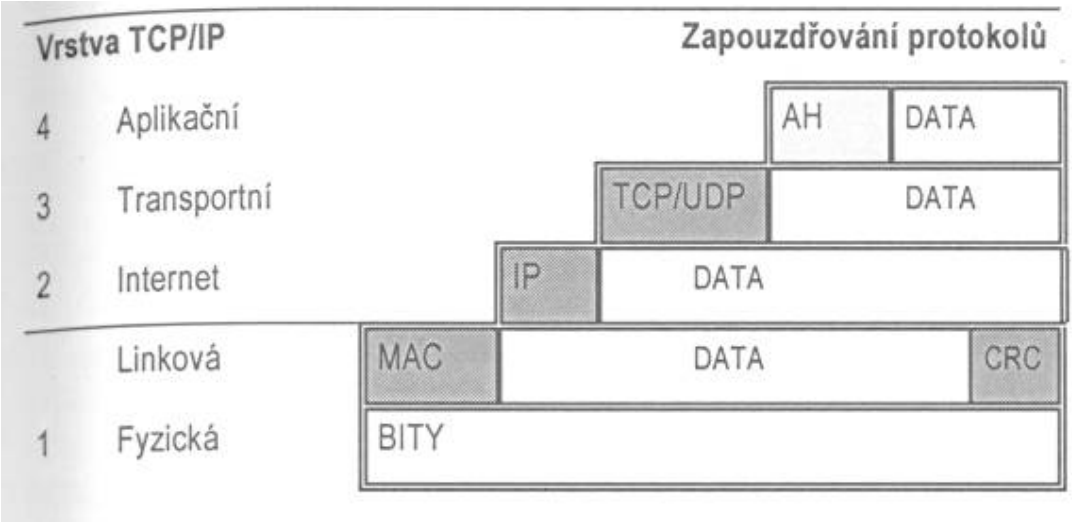
Obrázek: Obrázek průvodce 24

Obrázek: Obrázek sítě 37

TCP/IP (Transmission Control Protocol/Internet Protocol)



TCP/IP (Transmission Control Protocol/Internet Protocol)



Ostatní síťové architektury

Firemní (proprietární) protokolové architektury ze 70.–90. let.

Novell NetWare

- vylepšení Xerox XNS, jednodušší než TCP/IP (spíše pro LAN), (v minulosti) nepoužívanější po TCP/IP
- distribuovaný systém klient-server skrze **volání vzdálených procedur (RPC)**
- nejnižší vrstva podporuje všechny typy přenosových prostředků
- síťová vrstva
  - protokol **IPX (Internet Packet eXchange)** - datagramový, nespojový, podobný IP
  - směrovací protokoly
- transportní vrstva: protokol **SPX (Sequenced Packet eXchange)** - spolehlivý, spojový
- vyšší vrstvy:
  - protokoly SAP (Service Advertising Protocol) a **NCP (NetWare Core Protocol)**
  - zprostředkování zpráv, doplňkové moduly (NLM)
  - emulátor NetBIOS (viz dále)

Apple AppleTalk

- distribuovaný systém klient-server
- spodní vrstvy podporují několik přenosových prostředků (př. EtherTalk) a **LocalTalk** (firemní protokol přístupu k médiu)
- síťová vrstva: dynamická adresace, vytváření sítí a zón, protokoly DDP a AARP
- transportní vrstva: několik transportních, směrovacích a specifických protokolů (ATP, RTMP)
- vyšší vrstvy: aplikační protokoly ADSP, PAP, **AFP** (přenos souborů)

IBM/Microsoft Network

- vlastní architektura založená na **IBM LAN Manager**
- původním základem protokol 3COM **NetBEUI** (NetBIOS Extended User Interface) implementující IBM **NetBIOS** (Network BIOS):
  - nejstarší **API pro LAN**
  - elementární I/O operace přenosu dat, 19 služeb (jmenné, relační, datagramové, všeobecné)
  - bez směrování, funkce linkové, transportní a částečně relační vrstvy, ne síťové $\Rightarrow$ použitelný jen v LAN
- nyní TCP/IP pro NetBIOS a aplikační protokol IBM/Microsoft **SMB** (Server Message Block) / **CIFS** (Common Internet File System):
  - nejpoužívanější pro souborové a tiskové servery v LAN
  - model klient-server se zabezpečným přístupem ke **sdíleným prostředkům** na různých úrovních (disky, adresáře, tiskové fronty)

Další (minulost): Xerox Networks Systems (XNS), Banyan Vines, Digital DECnet aj.

OSI

- řeší přenos dat mezi systémy nezávislými na fyzických prostředích, skrze spolupráci systémů na úkolech – **obecná řešení**
- definuje koncové a mezilehlé systémy, oblasti, správní domény aj.
- fyzická a linková vrstva: normalizovaná rozhraní a linkové protokoly (HDLC, LAPB)
- síťová vrstva: služby se spojením (CONS, protokol **CONP**) a bez spojení (CLNS, **CLNP**)
- transportní vrstva: spojové protokoly **TP0-4**
- vyšší vrstvy: relace pomocí tokenů, prezentační formát **ASN.1**, aplikační služby, systém zprostředkování zpráv, adresářový systém a další protokoly (FTAM, VTP)

Management sítě

= sledování zahajování, ukončování a monitorování činností síťových zařízení a optimalizace datových přenosů v síti, (automatická) rekonfigurace sítě

- součást aplikační vrstvy
- u OSI protokol **CMIP (Common Management Information Protocol)**:
  - centralizovaný
  - různé modely managementu, řešení poruch, konfigurace, účtování, výkonnosti, bezpečnosti zařízení a datových přenosů
- u TCP/IP protokol **SNMP (Simple Network Management Protocol)**:
  - distribuovaný, transakční, jednodušší, nejpoužívanější
  - agent (program řízeného systému, ukládá data) a manažer (aplikace řídící agenty, sbírá data)
- vzdálené monitorování (RMON) – vzdálené monitorovací sondy
- např. management založený na WWW (WBEM), Java JMAPI a další

Bezpečnost a ochrana sítě

- na odpovídajících vrstvách zajištění integrity rámce, paketu, datagramu atd.
- ochrana proti čemu?
  1. **obsah**: ideologie, ohrožující mravní výchovu, aj.
  2. **útoky** na činnost systému a neoprávněný přístup k datům
  3. organizační a fyzická - **sociální inženýrství** („ukecat“ pracovníka s právy, „servis“ si odnese disk s daty apod.)
- útoky zvenčí a zevnitř – řeší **podniková bezpečnostní politika**
- kritéria hodnocení bezpečnosti (ITSEC): důvěrnosti informací (dostupné jen oprávněným osobám), integrita (nenarušení neoprávněnou osobou), dostupnost (zaručení přístupu)
- obecné metody ochrany
  - omezování přenosu dat a přístupu k síti: blokování, filtrace
  - autorizace přístupu: obvykle jméno a (jednorázové) heslo, vícefaktorové, specializované protokoly
  - zabezpečení kanálu: šifrování, výměna klíčů
  - autenticita zpráv: digitální podpis (hashování), certifikáty a certifikační autority

Bezpečnost a ochrana sítě

OSI

- řešení rozpoznání neautorizovaného chování (autentizace, řízení přístupu, zajištění důvěrnosti a integrity dat)
- zabezpečovací protokoly
- snaha o minimalizaci zranitelných míst

TCP/IP

- **původně žádné zabezpečení** (**“Internet je nebezpečný!”**), ponecháno na aplikace
- typicky jednoduchá autorizace jménem a heslem (plain text)
- útoky:
  - falešná adresace (spoofing)
  - na hesla (analýza protokolů, „trojské koně“, apod.)
  - odposlech
  - odmítnutí služby (DoS = Denial of Service, zahlcení, vyčerpání zdrojů)
  - zneužití chyb aplikací (exploit, šíření přes služby WWW a email)
  - ...

Bezpečnost a ochrana sítě

TCP/IP

- ochrana
  - **firewall** (oddělení vnitřní sítě od vnější) s **demilitarizovanou zónou (DMZ)** – filtrace provozu a kontrola adres (prevence před DoS)
  - **překlad adres (NAT)** – vlastní „skrytá“ adresace
  - **aplikační brány (proxy)**, zástupné servery
  - autentizace komunikujících stran, autorizace přístupu k prostředkům (datům)
  - zabezpečení komunikace (šifrování)
  - opatření proti zahlcení aplikace
  - ...
- protokoly **bezpečnostní architektury pro IP**: **IPSec** (bezpečná komunikace na síťové vrstvě), **SSL/TLS** (na transportní vrstvě), **RADIUS** (autentizace a autorizace)