APLIKAČNÍ VRSTVA

RNDr. Ing. Vladimir Smotlacha, Ph.D.

Katedra počítačových systémů
Fakulta informačních technologií
České vysoké učení technické v Praze

Počítačové sítě BI-PSI

LS 2018/19, Přednáška 7

https://courses.fit.cvut.cz/BI-PSI

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

OPPA PRAHA PRAGUE PRAGA PRAG EVROPSKÁ UNIE

OBSAH

Protokoly a aplikace

- FTP
- telnet / SSH
- Mail (SMTP / POP / IMAP)
- Web (HTTP / HTTPS)
- NTP
- DHCP / BOOTP / RARP
- streaming
- VoIP
- peer to peer

APLIKAČNÍ VRSTVA

Implementace protokolů a služeb

- využívají transportní vrstvu (TCP/IP model)
- nad prezentační vrstvou (OSI model)
  - OSI důsledně rozlišuje aplikaci a funkce relační a prezentační vrstvy

Modely

- klient / server
  - server nabízí službu
  - klient se připojí a službu využije
- peer-to-peer
  - nerozlišují se komunikující strany

File Transfer Protocol

- poprvé v RFC114, později RFC959, RFC2228, RFC2640

- přenos souborů mezi klientem a serverem
  - interaktivní procházení adresářů a zobrazení jmen souborů
  - příkazový kanál 21/TCP
  - datový kanál TCP, dynamicky přidělený port
    - aktivní – klient určí číslo portu a očekává na něm spojení
      - standardní způsob, server zahajuje přenos z portu 20
      - problémy pro firewall – datový kanál otevírá server
    - pasivní – server určí číslo portu pro datový kanál
      - snadná implementace ve firewallu – kanál otevírá klient

FTP

- klienti
  - **ftp** (řádkový, interaktivní)
  - implementován v browserech (URL ftp:// ....)
  - součást **mc** (Midnight Commander)
  - **WinSCP** (MS Windows)
- autentizace **user / password**
  - anonymní uživatel: *guest* nebo *anonymous*
    - heslo: někdy vyžadována e-mail adresa
- nevýhody
  - přenos hesla není kryptovaný
  - server je zranitelný, častý cíl útoků

TELNET

Interaktivní řádkový terminál

- vzdálený přístup k počítači
- prvotní specifikace RFC15 z roku 1969
- síťová alternativa k terminálu připojenému sériovou linkou

- port 23 / TCP
- autentizace **user / password**
- nevýhody
  - malá bezpečnost – žádné šifrování dat ani hesla
  - nepodporuje myš
- stále využíván (podpora v browserech)
  - např. konfigurace síťových zařízení

SSH

Secure Shell

- port 22 / TCP
- nahrazuje *telnet*
- implementuje kryptování (veřejný klíč)
  - varianty SSH-1 (zastaralé) a SSH-2
- kryptované autentizace **user / password**
  - alternativa: bez autentizace pro vybrané veřejné klíče
- přenos souborů (scp)
  - plně šifrovaný
  - není interaktivní

ELEKTRONICKÁ POŠTA

Elektronická pošta

- poprvé specifikováno v RFC561
  - SMTP poprvé v RFC821 (předtím nadstavba FTP)
- první masově využívané služba v Internetu

- software poštovního systému
  - MTA (Mail Transfer Agent)
  - MUA (Mail User Agent)
  - MDA (Mail Delivery Agent)

EMAIL - AGENTI

MTA (Mail Transfer Agent) – poštovní server

- předávání e-mailů
  - lokální adresát: doručení vyřeší MDA
  - vzdálený adresát: pošle se jinému MTA
- přepisovací pravidla pro adresy
- filtrování
- MTA navzájem komunikují protokolem SMTP
- příklad:
  - sendmail, postfix, qmail, Microsoft Exchange

EMAIL - AGENTI (2)

- MUA (Mail User Agent) – poštovní klient
  - uživatelský interface
  - příjem: přebírá maily od MTA
  - odesílání: posílá maily MTA
  - příklad: Thundebird, Opera, pine, Microsoft Outlook
- MDA (Mail Delivery Agent) – lokální zpracování
  - přeposílání (forward) mailů, filtrování
  - konfiguraci provádí uživatel
  - příklad: procmail
    - funkce často implementována v MUA

EMAIL - ADRESY

- v Internetu adresa obsahuje '@'
- interpretace adresy během přenosu
  - přepisovací pravidla
- část před '@' – lokální adresát
  - interpretuje se na cílovém počítači
    - většinou se přiřadí k uživatelskému jménu
- část za '@' – doména
  - MX záznam v DNS – přiřazení serveru k doméně
    - primární a záložní poštovní servery pro doménu
  - nebo konkrétní jméno serveru

EMAIL - PROTOKOLY

- SMTP
  - port 25 / TCP
  - komunikace mezi MTA
  - posílání zprávy od MUA k MTA
- POP3
  - port 110 / TCP
  - přenos zpráv od serveru ke klientovi (od MTA k MUA)
- IMAP4
  - port 143 / TCP
  - nahrazuje POP3
  - správa schránek na serveru
    - může přenášet jen samotné hlavičky zpráv

Základní příkazy

- HELO <*sendinghostname*>
  - navázání komunikace
- MAIL FROM: <*e-mail address*>
  - adresa odesílatele
- RCPT TO: <*e-mail address*>
  - adresa příjemce
- DATA
  - text zprávy, ukončeno tečkou (<CRLF>.<CRLF>)
  - včetně hlaviček (Subject:, ...)
- QUIT
  - ukončení spojení

EMAIL - SPAM

Spam – nevyžádané zprávy

- spam tvoří většinu provozu el. pošty
- filtrace (MDA, MUA) není uspokojivě vyřešena
  - pravidla
  - učící se algoritmy - „vypadá to jako spam, tak to asi bude spam“
- „black lists“
- omezení na úrovni MTA
  - doručování jen do vlastní a vybraných domén
  - identifikace odesílatele
    - původně MTA přijal o odeslal každý mail z každého serveru

World Wide Web

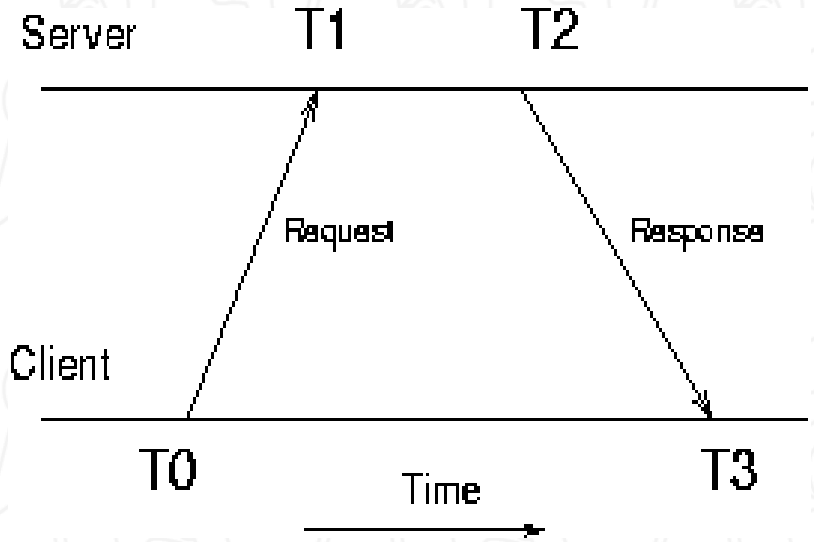
- počátky HTTP v 1990 (CERN)
- prohlížeč Mozaic – 1993
- nejrozšířenější služba v Internetu

- jazyk HTML (HyperText Markup Language)
  - vložení linků (odkazů) do textu
- protokol HTTP, port 80 / TCP (HTTPS, port 443)
  - server neukládá stavové informace
  - cookies – stav uložený u klienta
- scripty

Network Time Protocol

- protokol NTP, port 123 / UDP
- přenos času v síti
  - nastavení systémového času v počítači
  - podpora i na routerech
  - prakticky dosažitelná přesnost jednotky µs, typicky 1-10 ms
- hierarchický systém NTP serverů
  - klient využívá podmnožinu serverů ze všech v konfiguraci
  - číslo „Stratum“ vyjadřuje vzdálenost od primárního zdroje
    - konkrétní číslo nezaručuje přesnost
  - Stratum-1 – server s externím zdrojem času
    - atomové hodiny, GPS, DCF, ...

NTP - PRINCIP



delay $\delta = (T3 - T0) - (T2 - T1)$

offset $\theta_0 = [(T1 - T0) + (T2 - T3)] / 2$

$$\theta_0 - \delta/2 \leq \theta \leq \theta_0 + \delta/2$$

- předpoklad symetrického zpoždění v obou směrech
- nejistota výpočtu ≤ ½ celkového zpoždění

DHCP, BOOTP, RARP

Společná funkce: přidělení IP adresy počítači

- příklad využití:
  - bezdiskový stroj
  - dynamické IP
  - omezení na registrované adaptéry

- RARP (Reverse Address Resolution Protocol)
  - protokol síťové vrstvy,
  - stejný formát zprávy jako ARP
  - předává pouze IP adresu
    - je třeba znát i masku, gateway a případně DNS servery
  - nyní se již nepoužívá

BOOTP

Bootstrap Protocol

- umožní stanici získat IP adresu, masku, gateway, adresu DNS serveru a image operačního systému
  - funkce:
    - klient (port 68 / UDP) odešle dotaz „Kdo jsem?“ na adresu 255.255.255.255
    - server (port 67 / UDP) vyhledá údaje podle MAC adresy v databázi a odešle zpět
  - klient si stáhne image OS pomoci FTP nebo TFTP
- IP adresa je pevně přidělena pro MAC
  - nelze ji dynamicky sdílet

Dynamic Host Configuration Protocol

- náhrada protokolu BOOTP
  - stejné porty jako BOOTP
  - funkce:
    - *discovery*
    - *offer*
    - *request*
    - *confirmation*
  - přidělování IP adres
    - statické – pevně nastavené k konfiguraci
    - dynamické – volná adresa z vyhrazeného rozsahu
    - přidělení je časově omezené
  - další volitelné údaje
    - NTP, WINS, ...

STREAMING

Přenos audiovizuálního obsahu

- v reálném čase – TV, rozhlas
- „on demand“ – na základě požadavku příjemce (např. YouTube)
- protokoly
  - RTSP (Real-time Streaming Protocol)
  - RTP (Real-time Transport Protocol)
  - RTCP (Real-time Transport Control Protocol)
- unicast x multicast

STREAMING - FORMÁTY

- multimediální kontejner
  - obsahuje jeden nebo více streamů
  - OGG, MPEG, RealMedia, QuickTime, Windows Media,..
- kodeky (coder/decoder)
  - implementuje určitý formát
  - komprese a dekomprese streamu
- formáty
  - audio: WMA, MP3, Vorbis, AAC+ (16-256 kb/s)
  - video: MPEG-4, H.264, ...

Voice over IP

- Internetová telefonie
- kodeky
  - patentované standardy ITU, např. G.711, G.722, G.723, G.726, G.729, …
  - SPEEX (BSD licence)
- protokoly
  - H.323
    - standard ITU-T pro paketové sítě
    - signalizace, řízení
- SIP (Session Initiation Protocol)

VOIP - ZAŘÍZENÍ

Řídicí zařízení

- MCU (Multipoint Control Unit)
  - podpora videokonferencí
- VoIP gateway
  - přechod mezi telefonní sítí a VoIP
- VoIP gatekeeper
  - registrace klientů

Koncová zařízení

- IP telefonní přístroje
- videokonferenční zařízení
- software na počítači

PEER-TO-PEER

- klienti spolu komunikují přímo
- strukturované sítě
  - indexuje obsah ve formě distribuované tabulky (hash)
  - efektivní nasměrování požadavku
  - např. BitTorrent
- nestrukturované
  - „pure“ - dotaz posílán všem
  - centralizované indexování obsahu
    - např. Napster
  - hybridní model
    - např. GNUtella, Freenet

SKYPE

- P2P aplikace, od r. 2011 vlastní Microsoft
- pakety jsou šifrovány, protokol nebyl zveřejněn
  - mnoho různých kodeků (např. video 30 kb/s – 1 Mb/s)
  - klient x superklient
  - po přihlášení uživatele se klient spojí se supeklientem
  - schopnost procházet přes NAT i různé firewally
  - superklient je schopen zprostředkovat spojení (relay) i klientovi za NAT
- možnost realizovat audiokonferenci N účastníků
  - superklient zkombinuje N datových toků do jediného

Děkuji za pozornost