Protokoly služeb Internetu

Petr Grygárek

Emulace terminálu

Telnet

- emulátor terminálu přes síť (TCP/23)
  - znakový a řádkový režim
- na serveru démon telnetd, s daty z TCP spojení od klienta zacházeno jako s daty z fyzického terminálu
- příkazy pro oboustranné dohadování voleb
  - návrh a potvrzení/zamítnutí volby
  - volby dohadovány zvlášť pro obě strany
  - příklady voleb: echo, typ terminálu, flow control, ...
- klávesa přerušeni (Ctrl-C) - implementováno s použitím TCP Urgent Pointer

Koncepce virtuálního síťového terminálu (Network Virtual Terminal - NVT)

- NVT = virtuální znakové zařízení s klávesnicí a tiskárnou
- nejmenší možná množina společných parametrů splňovaných všemi reálnými terminály
- znaky kódovány "oficiálně" na 7 bitů
  - Reálně se většinou přenáší všech 8b
- Ukončení řádku: CR, LF

Secure Shell (SSH)

- Obdoba Telnetu, ale provoz šifrován
  - Využití asymetrické kryptografie
  - Klíče generovány automaticky s využitím Diffie-Hellmanova algoritmu
  - Podpora autentizace serveru
- Postaveno na šifrovací spojově orientované službě vrstvy SSL (Secure Socket Layer)
  - TCP/22
- Šifrovaný kanál lze použít i k dalším účelům
  - přenos souborů (scp), šifrované X-Window

Přenos souborů

File Transfer Protocol (FTP)

- (obousměrný) přenos souborů mezi dvěma systémy
- Přenos z klienta na server nebo opačně
  - (nebo přímo mezi dvěma vzdálenými servery)
- podpora autentizace uživatele (a autorizace)
- samostatné řídící (TCP/21) a datové (TCP/20) spojení
  - řídící spojení - příkazy
  - datové spojení (dočasné)- přenos souborů, výpis adresáře
- podpora transparentního přenosu i konverzí kódování textových souborů
- přenášená data chápana jako soubor
  - volitelně i jako záznamy/stránky

FTP – příkazy řídícího spojení

- USER, PASS - zaslání autentizačních údajů
- LIST - výpis adresáře
- PORT - stanovení TCP portu klienta, kam má server navazovat datové spojení
- TYPE - určení typu dat (ascii/binary)
- RETR, STOR - stažení, resp. zaslání souboru
- ABORT - ukončení přenosu
  - (řídící kanál aktivní i po dobu přenosu)
- PASV - přechod do pasivního režimu
- QUIT - ukončení relace a spojení

FTP – odpovědi na příkazy

- 3-místný kód pro strojové zpracování
  - jednotlivé číslice určují skupinu a podskupinu typů odpovědí
- doprovodný volitelný text (pro uživatele)
- možnost víceřádkových odpovědí s označením posledního řádku

FTP – aktivní a pasivní režim

- standardně aktivní režim
  - datové spojení navazuje **server**
    - (z portu 20 na klientův port zadaný příkazem PORT)
- volitelně pasivní režim
  - po zadání příkazu PASV
  - datové spojení navazuje klient
    - (z portu zadaného v příkazu PASV)
  - možnost průchodu přes firewally s jednosměrně dovoleným navazováním spojením

Trivial FTP (TFTP)

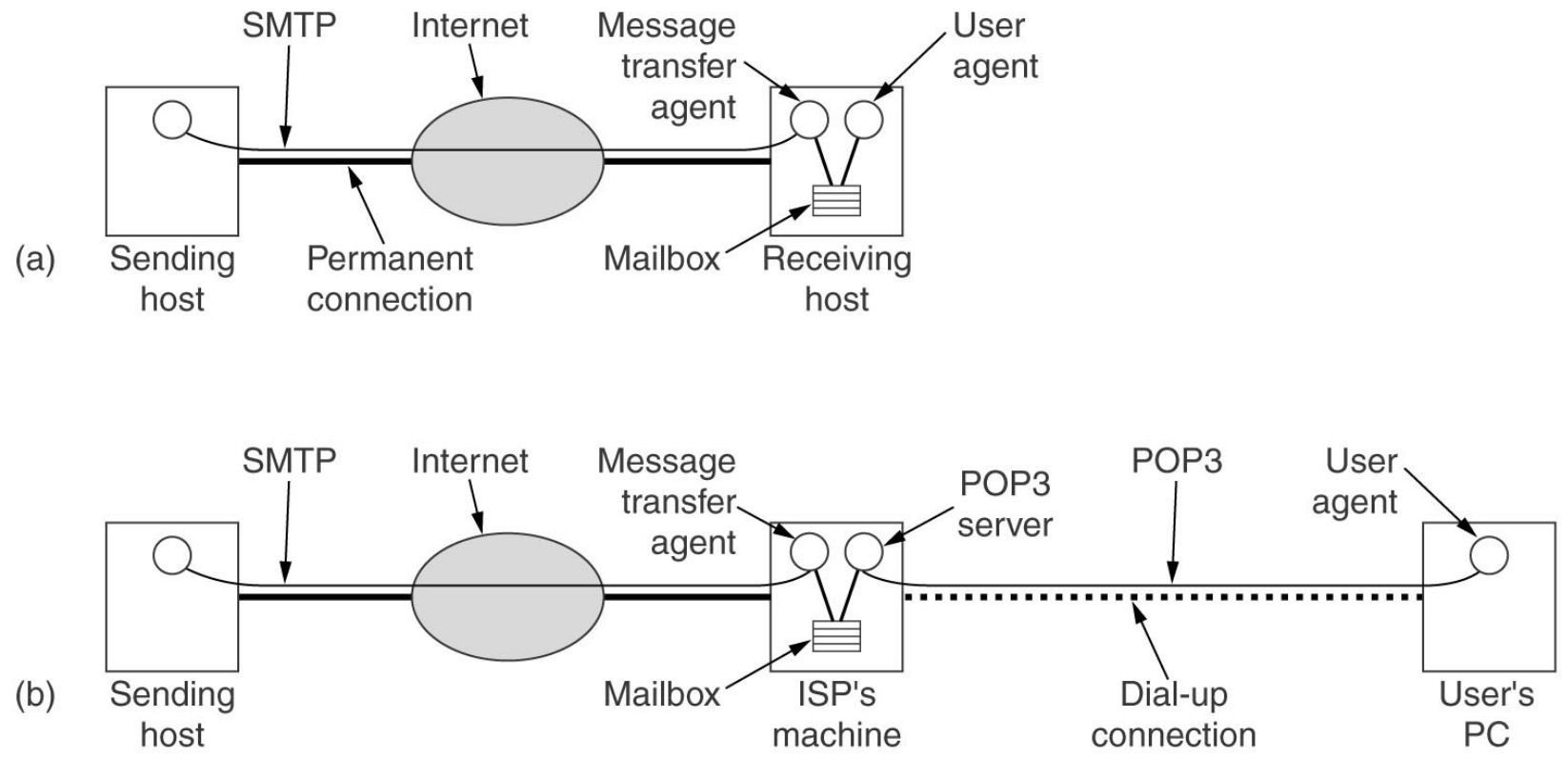
- jednoduchá implementace přenosu souborů
- nad UDP
  - stop and wait protokol
  - první paket s povelem pro zaslání/uložení souboru
  - číslování a potvrzování paketů, retransmise ztracených
  - bez autentizace
- často použití pro upload software a konfigurace síťových prvků nebo zavedení bootovací image stanice

Elektronická pošta

Základní pojmy

- User agent (UA)
- Message Transfer Agent (MTA
- Mailbox – poštovní přihrádka

Struktura a návaznost protokolů elektronické pošty



Upozornění !

- protokoly orientované textově
- neprovádí se šifrování
- SMTP bez autentizace
- POP a IMAP autentizace zpravidla cleartextovým heslem
  - lze i MD5
- možnost šifrování zabalením do SSL
  - (POP3S, IMAPS)

Struktura zprávy

- Obálka
  - identifikace odesílatele a příjemce
- Hlavička
  - seznam dvojic "jméno: hodnota" na zvláštních řádcích
  - od těla zprávy oddělena prázdným řádkem
  - mezilehlé poštovní servery (MTA) mohou hlavičku modifikovat (časy průchodů apod.)
- Tělo

Tělo zprávy

- Původně NVT ASCII (7-bit) bez struktury
  - délka řádku max 1kB, celková délka zprávy do 64kB
  - dnes obvykle mírnější omezení
- Dnes lze použít Multimedia Internet Mail Extension (MIME)
  - Zpráva nese binární reprezentaci různých typů médií
  - Podpora zpráv z více částí (multipart)
  - Informace o použité struktuře zprávy a typech přenášených multimediálních dat v hlavičce zprávy

Předávání zpráv

- Z klienta přímo na poštovní server příjemce
  - Problém, nemůže-li být zpráva doručena okamžitě
- Z klienta na některý poštovní server (výchozí SMTP brána)
  - Poštovní servery si zprávu spolehlivě předávají dále
  - Při neúspěchu opakování pokusu
    - po určitém počtu neúspěchů informace odesílateli
- Z poštovního klienta/serveru na bránu do jiných sítí

Simple Mail Transfer Protocol (SMTP)

- šíření zpráv od poštovního klienta k poštovnímu serveru nebo mezi poštovními servery
- TCP/25
  - nešifrováno
  - neautentizováno
- příkazy orientovány textově
- na jednom spojení může následovat mnoho zpráv
  - (i v obou směrech-příkaz TURN)

SMTP-základní příkazy

- HELO - identifikace "klienského" MTA (jen formální)
- MAIL FROM: - identifikace odesílatele
- RCPT TO: - identifikace příjemce
- DATA - uvozuje samotnou zprávu (hlavička + tělo)
- . - tečka jako první znak na samostatném řádku ukončí zprávu
- TURN - výměna rolí klient-server mezi MTA
  - (možnost předání zpráv ve druhém směru, jsou-li nějaké)
- QUIT - ukončení relace a spojení

SMTP-další příkazy

- VRFY - ověření existence mailing listu
- EXPN - rozvinutí mailing listu do seznamu účastníků
- …

Často zakázáno kvůli bezpečnosti

Multimedia Mail Extension (MIME)

- možnost strukturovat tělo zprávy
- možnost určení interpretace (multimediálních) dat (typ/podtyp, např. text/html)
- definuje způsob kódování binárních dat
- přidává další pole hlavičky informující příjemce o struktuře těla zpráv

Hlavičky MIME

- MIME-Version:
- Content-Type:
  - text, multipart, message, application, image, audio, video
- Content-Transfer-Encoding
  - 7bit (NVT ASCII, default), quoted-printable, base64, binary
- Content-Description:

Post Office Protocol v. 3 (POP3)

- protokol pro vybírání obsahu poštovních schránek
- architektura klient-server
- nad TCP, port 110
  - Nešifrováno
  - Autentizace cleartextovým heslem nebo MD5
- textově orientované příkazy

POP3 - příkazy

- USER PASS - zaslání autentizačních údajů
  - APOP - autentikace heslem kódovaným MD5
- LIST - výpis seznamu uložených zpráv a jejich ID
- RETR – výpis zprávy se zadaným ID
  - (do stejného TCP spojení)
- DELE - označení zprávy jako smazané
- RSET - zruší označení zpráv pro smazání
- QUIT - smazání označených zpráv, ukončí relaci a spojení
- UIDL - na základě pořadového čísla zprávy server vrátí jednoznačný identifikátor (přetrvává mezi relacemi)
- TOP - výpis prvních N řádků zadané zprávy

Internet Message Access Protocol (IMAP)

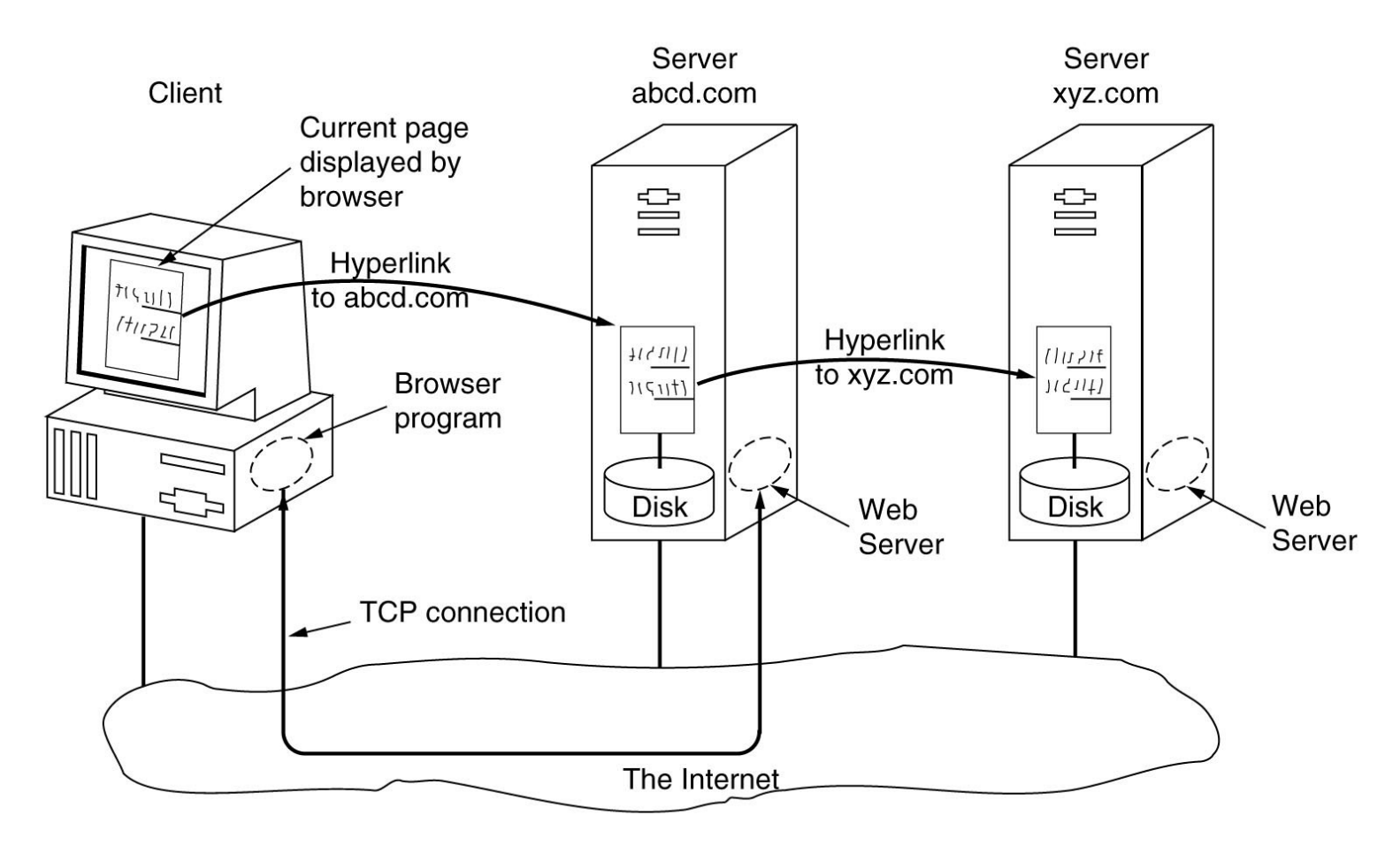
- dokonalejší obdoba POP3
- architektura klient-server, TCP/143
- předpokládá uchovávání zpráv na serveru (podpora "složek")
- vhodné zejména pro mobilní klienty
- vylepšené autentizační mechanismy
- cílem omezení dat přenášených na klienta
- možnost selektivního načítání zpráv a jejich částí
- možnost vyhledávání ve zprávách přímo na serveru

World Wide Web

Původ WWW

- CERN
- http://www.w3.org

Architektura WWW



Uniform Resource Locator (URL)

protokol://uživatel:heslo@stroj:port/cesta

Hypertext Transfer Protocol (HTTP)

- model klient-server, požadavek-odpověď
  - TCP/port 80
- návaznost na adresy URL
- využívá MIME (data se obalují hlavičkou MIME) => rozšiřitelný o formáty různých médií
  - na rozdíl od MIME předpokládá, že spojení je binární
- podpora pro autorizaci přístupu
- podpora pro relokaci stránek

HTTP - formát požadavku

- příkaz
- hlavička
- PRAZDNY_RADEK
- (data-obsah formuláře)

HTTP - formát odpovědi

- odpověď – stavový kód
- hlavička
- PRAZDNY_RADEK
- data-obsah WWW stránky

Základní příkazy (metody) HTTP

- GET
  - získání dokumentu specifikovaného zadanou cestou/URL
- HEAD
  - získání hlavičky dokumentu
- POST, PUT
  - zaslání obsahu formuláře na server

Další příkazy (metody) HTTP

- DELETE
  - smazání dokumentu (zpravidla nepodporováno nebo jen po autentizaci)
- LINK, UNLINK
  - vytvoření/smazání linku na dokument
    - (zpravidla nepodporováno nebo jen po autentizaci)
- OPTIONS
  - zjištění metod podporovaných serverem
- TRACE
  - sledování zpracování požadavku (pro debugging internetových aplikací)

Hlavičky požadavku (výběr) - I

- Accept
  - typ klientem akceptovatelného média, většinou *
- Accept-Charset
  - klientem akceptovatelné znakové sady
- Accept-Encoding
  - klientem akceptovatelná kódování Content-Encoding
- Accept-Language
  - klientem akcetovatelné jazyky
- Authorization
  - klientovy autentizační údaje

Hlavičky požadavku (výběr) - II

- If-Modified-Since
  - provést metodu, jen pokud byl dokument od zadaného data modifikován
- Referer
  - klient může zaslat URL, odkud získal odkaz na požadované URL
  - pro účely reklamy a dohledávání chybných odkazů
- User-Agent
  - jméno a verze WWW prohlížeče

Hlavičky odpovědi (výběr) - I

- Allow
  - výčet serverem podporovaných příkazů (metod)
- Content-Encoding
  - kódování dokumentu
- Content-Language
  - jazyk dokumentu
- Content-Length
  - délka dokumentu (důležité pro HTTP 1.1, kde po odpovědi serveru není spojení ukončováno)
- Content-Type
  - MIME typ těla zprávy (např.: text/html)
- MIME-Version
  - verze MIME

Hlavičky odpovědi (výběr) - II

- Date
  - datum zaslání dokumentu
- Expires
  - datum expirace platnosti obsahu dokumentu
- Last Modified
  - datum poslední modifikace dokumentu

Hlavičky odpovědi (výběr) - III

- Location
  - URL, kde se požadovaný dokument právě nachází
  - pro automatické přesměrovávání
- Retry After
  - čas doporučený pro další pokus při odpovědí Service Unavailable
- Server
  - jméno a software HTTP serveru
- WWW-Authenticate
  - serverem podporované autentikační mechanismy
- Refresh
  - přikazuje klientovi obnovit obsah dokumentu po určeném počtu sekund

HTTP 1.0 (RFC 1945)

- spojení iniciuje klient, ukončuje server po odeslání odpovědi
- sestává-li stránka z více dokumentů, každý se získává zvlášť po zvláštním TCP spojení

HTTP 1.1 (RFC 2068)

- klient může požádat o podržení TCP spojení po vyřízení požadavku serverem
  - (není třeba zřizovat TCP spojení zvlášť pro každý požadavek)
- podpora „virtual hosts“
  - více logických serverů se stejnou IP adresou
  - v příkazu GET musí být uvedeno celé URL, včetně jména (virtuálního) WWW serveru
- možnost přenosu části dokumentu (při výpadku spojení a novém načítání dokumentu)
  - prostor pro "download akcelerátory" při omezování propustnosti jednotlivých TCP spojení ISP :-)
- podpora komprese dat

HTTPS

- „secure" HTTP
- HTTP nad SSL

Cookies

- Podpora pro stavové transakce
- Využívá pole hlavičky
  - Set-Cookie (ze serveru na klienta)
  - Cookie (z klienta na server)
- Struktura (obsah) cokie
  - jméno, hodnota,
  - server, path (= při jakém URL cookie zasílat)
  - flag secure (=použít výhradně přes HTTPS)
  - comment
  - max-age

Protokoly pro podporu automatické konfigurace

Bootstrap Protocol (BOOTP)

- konfigurace parametrů protokolu TCP/IP stanice na základě MAC adresy
  - BOOTP server udržuje databázi mapování
  - BOOTP klienti požadují přidělení parametrů pro komunikaci
  - poskytuje IP adresu, masku podsítě, default gateway, boot TFTP server, boot image
- šíří se v UDP broadcastech
  - (lze zajistit průchod přes směrovače převodem na unicast)

Dynamic Host Configuration Protocol (DHCP)

- dočasné přiřazování adres klientům (na žádost) z poolu volných adres
  - pronájem adresy je třeba periodicky obnovovat
- lze přidělovat i vždy stejné parametry podle MAC adresy (a to i natrvalo)
  - kompatibilita s BOOTP
- žádost UDP broadcastem
  - mimo segment je třeba přeposílat routerem
- oproti BOOTP umí přidělit více parametrů
  - rozšiřitelné na obecně jakýkoli předávaný parametr

Zprávy protokolu DHCP

- DHCP Discover - vyhledání DHCP serveru (broadcast)
- DHCP Offer - DHCP server nabízí parametry k pronájmu
- DHCP Request - klient žádá o zarezervování jedné z nabídek
- DHCP Ack - žádaný server potvrzuje rezervaci

Relaying DHCP požadavků