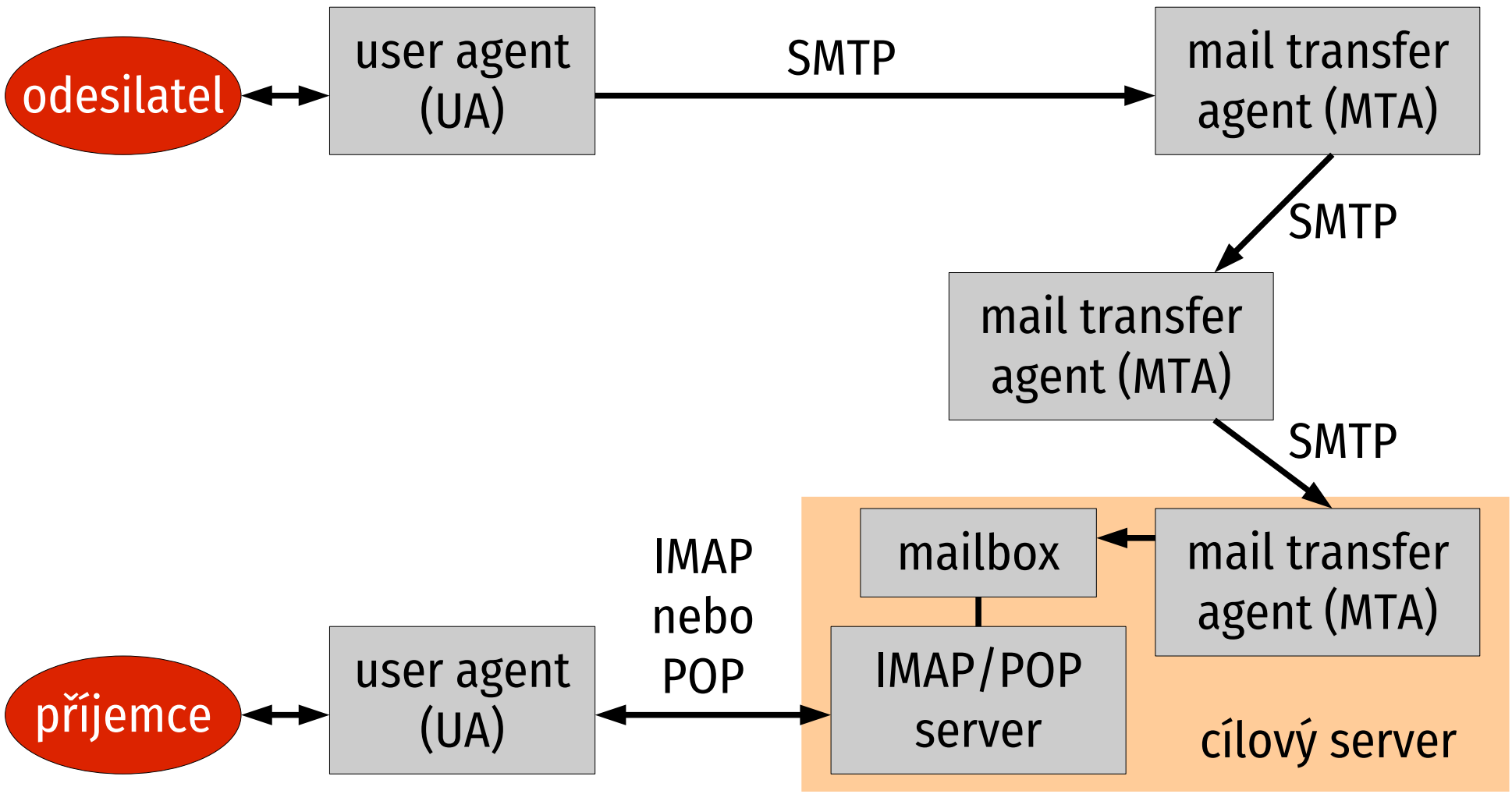
Aplikační protokoly

Elektronická pošta

Schéma elektronické pošty



Programy

- **User Agent (UA)**
  - uživatelské rozhraní poštovního systému
  - rozhodující pro uživatelský komfort
  - MS Outlook, Mozilla Thunderbird,...
- **Mail Transfer Agent (MTA)**
  - zajišťuje přepravu dopisů
  - neviditelný z hlediska uživatele
  - sendmail, Postfix, MS Exchange,...

SMTP

- **Simple Mail Transfer Protocol,** RFC 5321
- formát dopisu definuje RFC 5322:
  - **obálka:** přepravní informace, interní pro MTA, uživatel se o ní nedozví
  - **hlavičky:** kdo poslal, kudy prošlo,...; využívá UA, vychází z nich řada jeho funkcí (řazení dopisů, vyplňování adres při odpovědi,...
  - **tělo:** vlastní nesená zpráva, pro uživatele

Příklad dopisu

Received: from bubo.tul.cz (147.230.16.1) by tyto.tul.cz (Mercury 1.44)
with ESMTP; 19 May 06 08:53:09 +0200
Received: from relay.xyz.cz (relay.xyz.cz [123.24.128.45]) by
bubo.tul.cz (Postfix) with ESMTP; Mon, 19 May 2006 08:53:09 +0200
Received: from xyz.cz (office.xyz.cz [123.24.132.67]) by relay.xyz.cz
(Postfix) with ESMTP; Mon, 19 May 2006 08:53:11 +0200
Date: Mon, 19 May 2006 08:53:09 +0200
From: "Vitezslav T. Se'm" <travis@xyz.cz>
To: Petr Adamec <Petr.Adamec@tul.cz>
Cc: Pavel.Satrapa@tul.cz
Subject: Spam pres buba?

Zde je text tela dopisu.

Příklad SMTP komunikace

relay.xyz.cz (A) předává dopis na bubo.tul.cz (B)

A naváže TCP spojení s B na port 25, po něm proběhne tento dialog:

B: 220 bubo.tul.cz SMTP service ready
A: HELO relay.xyz.cz
B: 250 bubo.tul.cz says helo to relay.xyz.cz
A: MAIL FROM: <travis@xyz.cz>
B: 250 sender ok
A: RCPT TO: <petr.adamec@tul.cz>
B: 250 recipient OK
A: DATA
B: 354 Enter mail, end with "." on a line by itself
A: celý dopis – hlavičky a tělo
A: .
B: 250 message sent
A: QUIT
B: 221 relay.xyz.cz closing connection

E-mail a DNS

- používá DNS ke zjištění, kam posílat poštu
- MX záznamy (Mail eXchange)

  MX *priorita* *jméno*
- příklad: dopis pro pavel.satrapa@tul.cz
  - vyhledá v DNS MX záznamy pro tul.cz:

    0 bubo.tul.cz

    50 tul.cesnet.cz
  - pokusí se předat (po SMTP) na bubo.tul.cz
  - neuspěje-li, zkusí server s horší prioritou

Vzdálený přístup ke schránce

- schránka musí být stále dostupná, je umístěna na počítači s cílovým MTA
- UA často na jiném počítači (přístup z domova)
- **Post Office Protocol (POP)**
  - umí stáhnout dopisy na počítač a vymazat ze schránky
  - jednoduchý, široce implementovaný
- **Interactive Mail Access Protocol (IMAP)**
  - vzdálená práce se schránkami, větší možnosti, složitější
  - ideální kombinovat se SSL

MIME

- **Multipurpose Internet Mail Extensions,** RFC 2045 a další
- dle RFC 822 smí tělo dopisu tvořit jen US ASCII
  - problém s národními znaky, přílohami,...
- MIME zakóduje složitý dopis do podoby podle RFC 822 – lze přepravovat stávajícími MTA
- implementuje klient (UA) – kóduje/dekóduje

MIME hlavičky

- **MIME-Version**
  - je použito MIME
  - identifikuje verzi, zatím stále 1.0
- **Content-Type**
  - jakého typu je obsah dopisu
- **Content-Transfer-Encoding**
  - jak je kódován
  - **Quoted-Printable** pro text s akcenty,
    Base64 pro binární data

MIME typy (1)

- **typ/podtyp**
  - typ určuje základní charakter dat
  - podtyp identifikuje formát
- **text** – textová informace; text/plain, text/html
- **image** – obrázek; image/jpeg, image/gif
- **audio** – zvuk; audio/basic, audio/mpeg
- **video** – videosekvence; video/mpeg

MIME typy (2)

- **application** – data ke zpracování speciální aplikací; application/octet-stream, application/postcript
- **message** – obsahem je jiný dopis
- **multipart** – obsah má několik částí
  - multipart/mixed – prezentovat postupně (nejčastější)
  - multipart/parallel – prezentovat současně
  - multipart/alternative – různé varianty téhož obsahu
  - multipart/digest – každou částí je elektronický dopis
  - multipart/form-data – data z formuláře

Škodlivé dopisy (1)

- **spam** – nevyžádaná reklama
  - produkty i služby
  - oslovují koncové zákazníky i firmy
- **scam** – podvod
  - snaha vylákat peníze
  - typicky fiktivní velká cílová odměna (dědictví, výhra, dar) a vylákat z oběti „transakční poplatky“ po cestě k ní (právník, cestovné, administrativní poplatky, úplatky, …)

Škodlivé dopisy (2)

- **ransom** – vydírání
  - někdy skutečné – zašifrování obsahu disku
  - často fiktivní – máme vaše intimní nahrávky, jste obviněn(a) z trestného činu ...
- **phishing** – vylákání důvěrných údajů
  - přihlašovací údaje, číslo platební karty, ...
  - předstírání provozní události (přeplnění poštovní schránky, aktualizace zabezpečení, ...)
  - falešná stránka, která napodobuje původní

Možnosti ochrany

- **systémové**
  - greylisting
  - detekce virů, spamů apod.
- **uživatelské**
  - uživatel bývá nejslabším článkem
  - nedůvěřujte automaticky příchozí poště
  - pokud považujete za reálné, ověřte si jinou cestou (web, telefon), nepoužívejte odkazy z dopisu

Příznaky falešného dopisu

- skoro všechny výzvy typu „přihlaste se, abyste zabránili něčemu nepříjemnému“ jsou falešné
- nesmyslná adresa odesilatele (případně si zobrazte neformátovaný dopis a kontrolujte Received)
- falešné odkazy – vedou jinam, než se tváří
- špatná čeština, nevěrohodné formulace
- snaha vyvolat tlak, požadavek rychlé reakce

World-Wide Web

Základní prvky

- uspořádání klient–server
- **HyperText Transfer Protocol (HTTP)**
  - protokol pro komunikaci mezi klientem a serverem
- **HyperText Markup Language (HTML)**
  - jazyk pro definici obsahu stránky
  - XHTML – HTML přeformulováno do XML
  - vývoj koordinuje WWW konsorcium

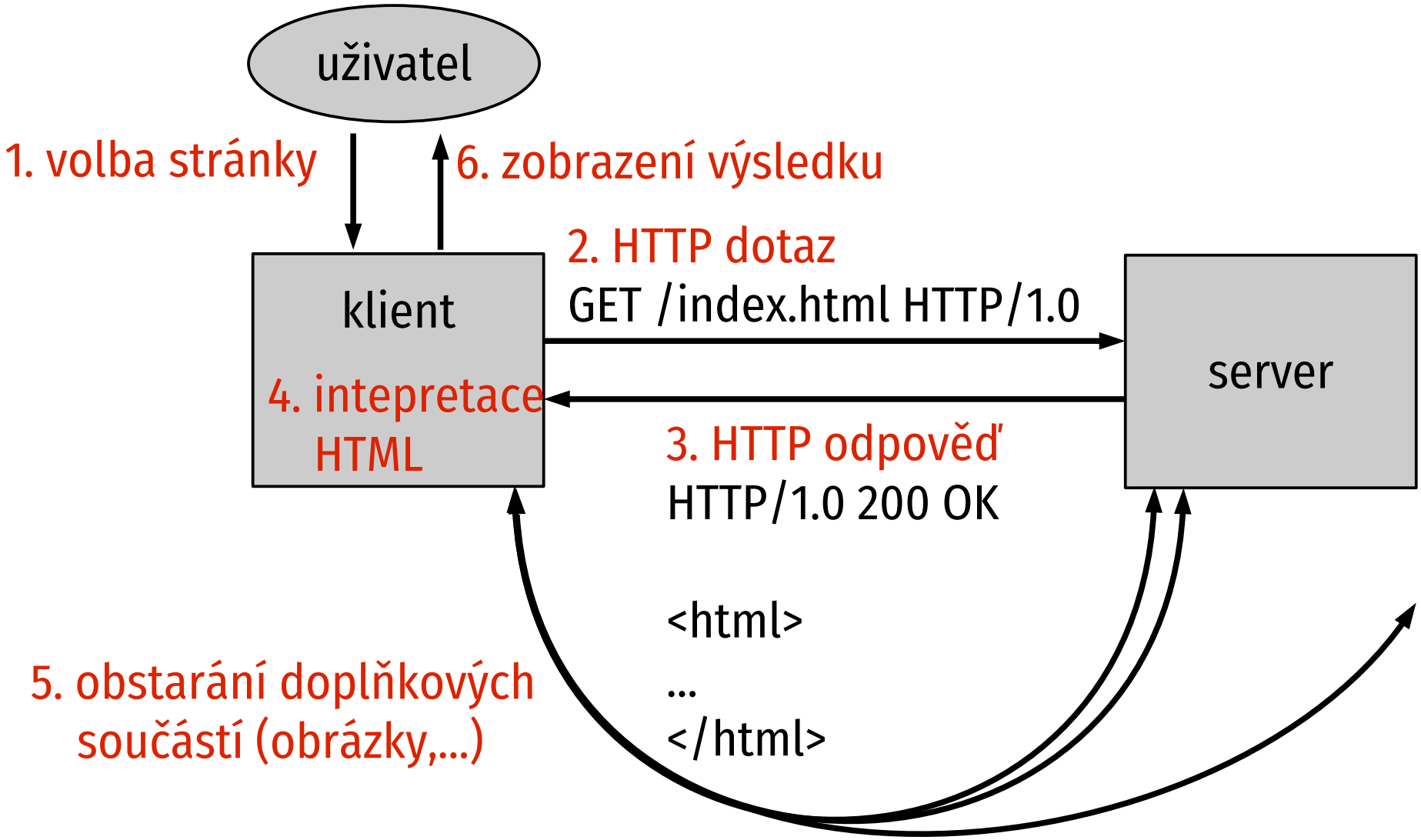
HTTP

- standardizace zpočátku chaotická (WWW konsorcium vs IETF, HTTP/1.0 nemá RFC)
- 2022 standardy zcela přepracovány
  - terminologie a sémantika – RFC 9110
  - HTTP/1.1 – RFC 9112
  - HTTP/2 – RFC 9113
  - HTTP/3 – RFC 9114

Účastníci HTTP provozu

- **prohlížeč** (uživatelský agent) – uživatelské rozhraní
- **server** – poskytuje obsah
  - často spojen s aplikací (e-shop, webmail,...)
- **prostředníci** – ne vždy, umožňují překonávat různá omezení
  - **cache** – ukládá obsah ze serverů
  - **proxy** – předává zprávy mezi prohlížečem a serverem

Komunikace klient–server



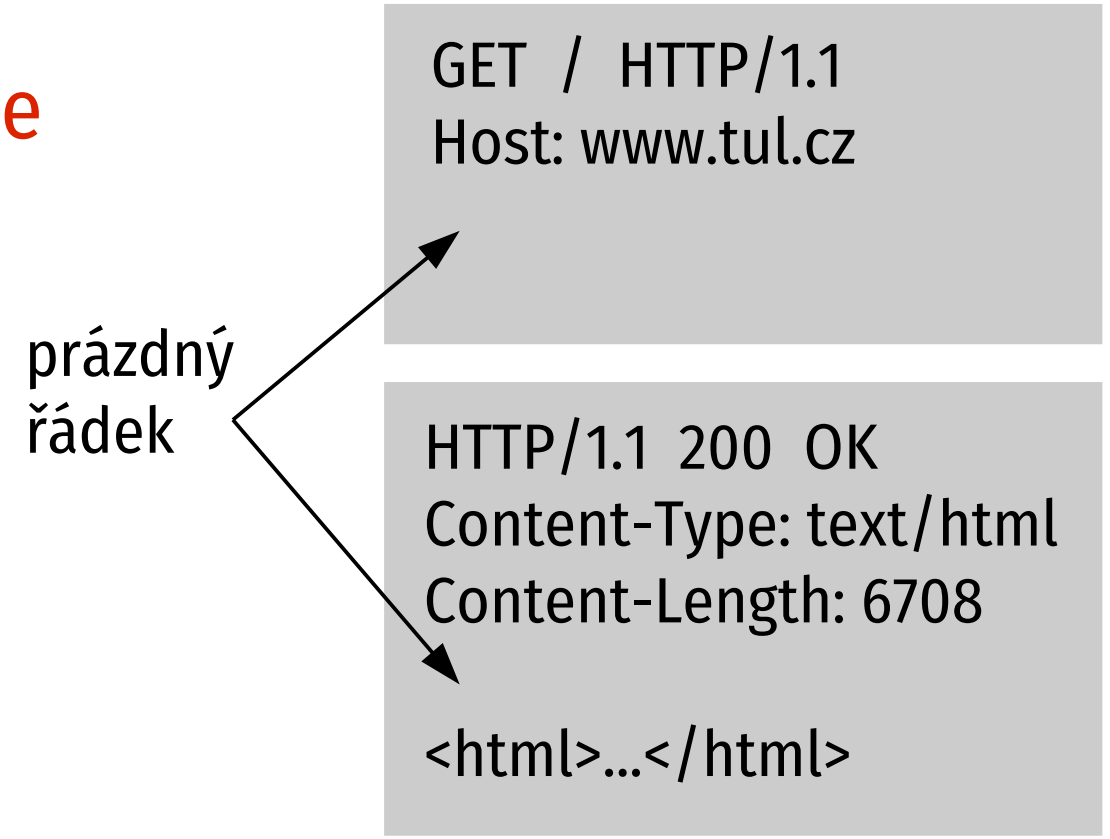
HTTP/1.1

- RFC 9112, TCP port 80
- **bezstavový protokol**
  - zodpovězením dotazu transakce pro server končí, neudržuje stavové informace o klientech
  - další dotaz nedává do souvislosti s předchozími
  - stav si uchovává klient
  - výhody: robustní, snadnější implementace
  - nevýhody: větší režie, některé služby vyžadují stavové informace (nákupní košík) – klient musí předat serveru

HTTP zprávy

- formátem připomínají elektronický dopis
- **dotaz:**
  metoda lokátor verze
  hlavičky (doplňují)
- **odpověď:**
  verze kód popis
  hlavičky

  tělo



Uniform Resource Locator

- univerzální adresa
- struktura: ***schéma:specifická část***
- typicky:
  http://www.kdesi.cz/doc/help.html
  schéma (protokol) | server | cesta
- elektronická pošta:
  mailto:Pavel.Satrapa@tul.cz

HTTPS

- HTTP + TLS (dříve SSL)
- TCP port 443
- **Transport Layer Security (TLS)**
  - RFC 8446
  - použitelné pro libovolný aplikační protokol
  - šifruje kompletní komunikaci (dotazy i odpovědi)
  - ověřuje autentičnost serveru (certifikát)
- doporučováno pro veškerý webový obsah

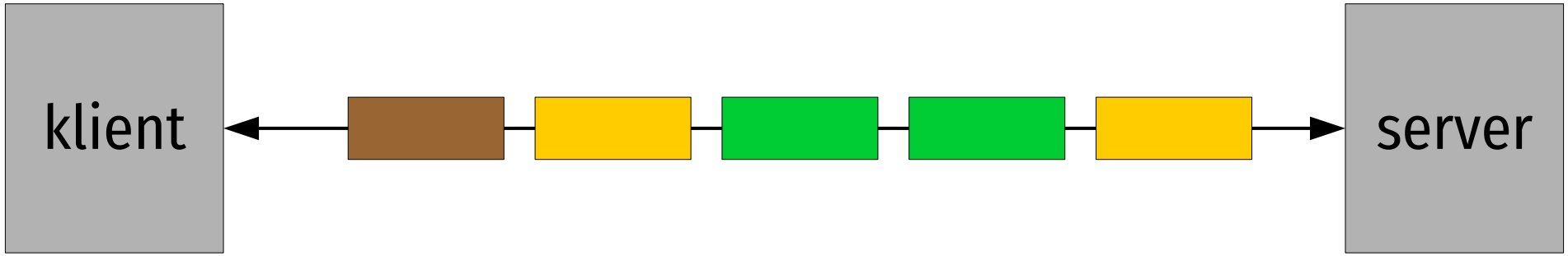
HTTP/2

- RFC 9113, navazuje na SPDY
- **binární přenos dat**
  - přenášeno v tzv. rámcích
  - 10 typů – hlavičky, data, nastavení,...
- **proudy (stream)**
  - klient navazuje jedno TCP spojení
  - každý dotaz/odpověď v něm přenášeny samostatným proudem (jen číslo proudu v hlavičkách)
  - navzájem se nezdržují

Porovnání protokolů

HTTP/1.x – několik TCP spojení

HTTP/2 – jedno TCP spojení, několik proudů v něm



Další vlastnosti HTTP/2

- **hlavičky** nadále u každého požadavku a odpovědi, ale silně **komprimovány** (RFC 7541)
- **server push**
  - server může poslat data, o která nebyl žádán, např. odeslal HTML a rovnou začne posílat obrázky pro stránku
  - klient může odmítnout
- předpokládá se použití s TLS
  - není povinné, klienti často podporují jen HTTP/2 + TLS
- aktivace: hlavička Upgrade

QUIC (1)

- původně: Quick UDP Internet Connection
- protokol transportní vrstvy
- vyvinul Google, standard: RFC 9000
- **UDP**, port 443
- QUIC spojení určeno identifikátorem – přežije i změnu portu klienta (občas způsobí NAT)
- vše šifrováno

QUIC (2)

- vhodný pro web – přenos více malých souborů
- uvnitř spojení **nezávislé proudy** (à la HTTP/2)
- každý proud má své potvrzování a opakování – zajišťuje spolehlivý přenos
- rychlejší navázání spojení (odpadá TCP handshake)
- pokud v HTTP/2 čeká TCP na opakování (ztráta paketu), brzdí všechny proudy; v QUIC zpoždění jednoho proudu neovlivňuje ostatní

HTTP/3

- RFC 9114
- podobné HTTP/2, ale využívá QUIC → jednodušší
- jedno QUIC spojení, v něm nezávislé proudy pro jednotlivé dotazy a odpovědi na ně
- komprimuje hlavičky (QPACK, RFC 9204)
- umožňuje server push

vytvořeno s podporou
projektu ESF