Elektronická pošta

- schéma funkce distribuce zprávy elektronického emailu (včetně role DNS)
- serverový a klientský software
- formát zprávy podle standardu RFC822
- protokoly pro práci s poštou
- MIME
- zabezpečení zprávy elektronického mailu

Elektronická pošta je forma datové komunikace po internetu, označována také jako e-mail nebo SMTP pošta (podle používaného protokolu zajišťující přenos), která není vlastněna žádnou osobou nebo firmou ☐ vychází z plně otevřených standardů (není proprietární).

Elektronická pošta je:

- rychlá (čas doručení v minutách a sekundách, i když může být ovlivněno stavem serveru...)
- levná (záleží na způsobu připojení, používaném softwaru...)
- pohodlná (možnost automatizace některých úkolů - třídění apod. (záleží na softwaru...))
- efektivní (snadná propojitelnost s ostatními aplikacemi, hromadné odesílání zpráv...)
- funguje "off-line" (nevyžaduje současné připojení odesílatele a příjemce)

Historický základ - Standardy

Původní zadání pro koncepci elektronické komunikace znělo asi takto: **Budou se přenášet co nejefektivněji krátké, čistě textové zprávy.** Od toho se odvíjí veškeré protokoly a techniky pro přenos, protože dnes se do tohoto zadání nevejdeme ☐ velké zprávy, nestandardní znakové sady, přílohy...

Koncepce elektronické pošty je dodnes založena na dvou dokumentech:

- RFC821 - definuje přenosový protokol SMTP
- RFC822 - definuje formát zpráv

RFC821 - Přenosový protokol SMTP

Tento dokument definuje přenosový protokol SMTP:

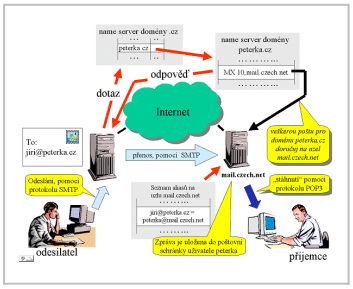
- Přenosový protokol **SMTP** (**S**imple **M**ail **T**ransfer **P**rotocol)
  - Podle tohoto protokolu spolu komunikují jednotlivé poštovní servery (jednotky MTA - Message Transfer Agents), když si mezi sebou předávají jednotlivé zprávy.
  - Spojení probíhá na smluveném **portu 25**
  - Předpokládá, že **přenášená data jsou sedmibitová**
    - Zpráva může obsahovat 128 ASCII znaků (základní sada ASCII)
    - Každý znak je zobrazitelný v sedmi bitech ($2^7 = 128$)
    - Při přenosu osmibitových zpráv není zaručen správný přenos

RFC822 - Definice zpráv

Tento dokument definuje formát zpráv přenášených přes SMTP. Říká že:

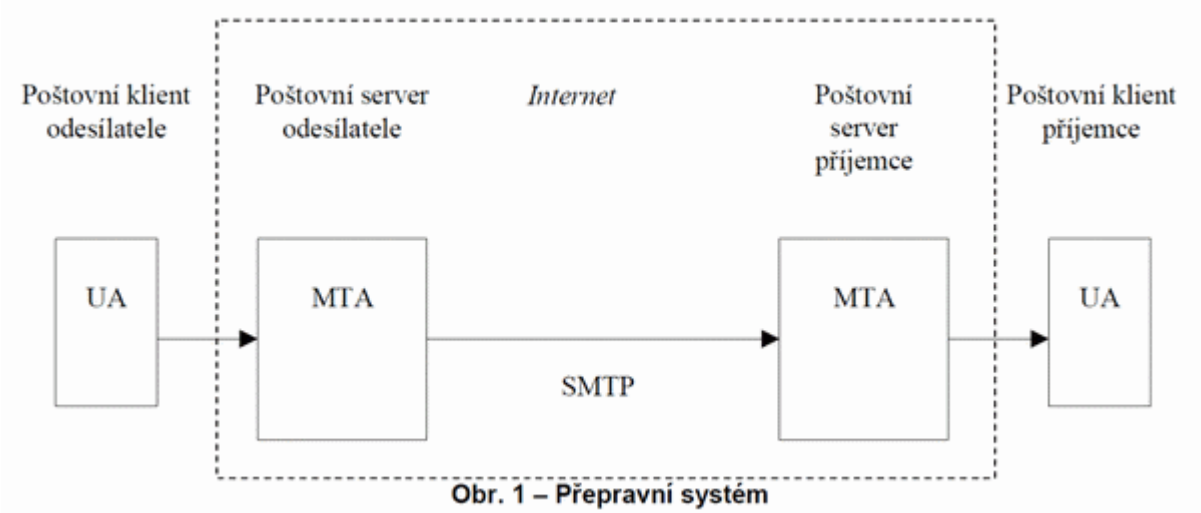
- Zpráva **se skládá** z hlavičky a těla
- Definuje typ a přesný tvar (syntaxi i sémantiku) jednotlivých položek v **hlavičce**:
  - **From:** adresy odesilatelů
  - **To:** adresáti
  - Cc: adresy na které se dopis odešle i když nejsou hlavními adresáty
  - Bcc: tajné kopie. Jako cc, ale adresy se vymažou z ostatních mailů
  - **Subject:** předmět
  - Return Path: zpáteční cesta k odesílateli
  - Received: záznamy přidané během zpracování
  - Reply to: adresa pro zaslání odpovědi
  - Sender: adresa skutečného odesílatele pokud je jiná než From: nebo je ve From: více adres.
  - Message ID: identifikace zprávy
  - Resent-klic: při přeposílání se klíče původních hlaviček uvodí Resent-
  - X-neco: doplňující hlavička (např. X-priority: 3)
  - Mime-version: použitá verze MIME. viz dále
- Říká, co smí a nesmí být v **těle zprávy**
- Definuje přesný **formát adres**, které lze používat pro potřeby elektronické pošty
  - `frantisek@vysmrkmaslo.cz`

Postup při komunikaci



- Uživatel spustí klientský program (**Microsoft Outlook**, **Mozilla Thunderbird**,...) a napíše zprávu
- Zpráva je upravena tak, aby vyhovovala standardu RFC822 a pokud zpráva obsahuje nepovolené znaky (diakritika) nebo přílohy, je na ni aplikován standard **MIME**.
- Poté je zpráva předána serveru pro odchozí poštu pomocí protokolu SMTP. Klientský program zde vystupuje jako SMTP klient.
  - Jako poštovní servery se používají např.: **Sendmail, Postfix**
- Zpráva je na serveru zařazena do fronty zpráv. Server se je postupně pokouší odeslat: (pokud se nezdaří, zpráva jde zpátky do fronty, v případě vypršení limitu je zpráva označena jako nedoručitelná...)
  - Nejprve se podívá na část adresy vpravo od zavináče (seznam.cz)
  - Snaží se ptát systému DNS kam má být doručena pošta pro "seznam.cz"
  - Odpověď mu může dát pouze cílový name server (seznam.cz), (cesta k němu může vést postupně nejdřív přes name server pro CZ doménu)
  - V name serveru Seznam.cz bude tzv. **MX** záznam (Mail Exchange), který nám řekne, kam tuto zprávu doručit
    - může existovat druhý MX záznam, který určuje adresu záložního serveru příjemce - tento server je použit v případě, kdy je primární server nedostupný

    - Odesílací server tedy naváže spojení se serverem příjemce a zprávu mu pošle pomocí SMTP protokolu (server odesílatele je zde jako SMTP klient)
- Podle části adresy vlevo od zavináče uloží server příjemce zprávu k příslušnému uživateli
- Příjemce si poté zprávu vyzvedne pomocí svého e-mailového klienta (klientského programu).
- E-mailový klient stahuje zprávy ze serveru pomocí protokolu **POP3**, nebo **IMAP**.



Obr. 1 – Přepravní systém

Problémy e-mailu

Mezi hlavní problém e-mailové komunikace patří především nevyžádaná pošta - **SPAM**. Jako obrana před SPAMem se nasazuje na cestě od serveru příjemce do e-mailového klienta příjemce tzv. antispamová ochrana. Jedním ze zástupců takové antispamové ochrany je např. SPAM Assassin.

Protokoly pro stahování zpráv

Pro stahování příchozích zpráv z poštovního serveru se používají dva protokoly:

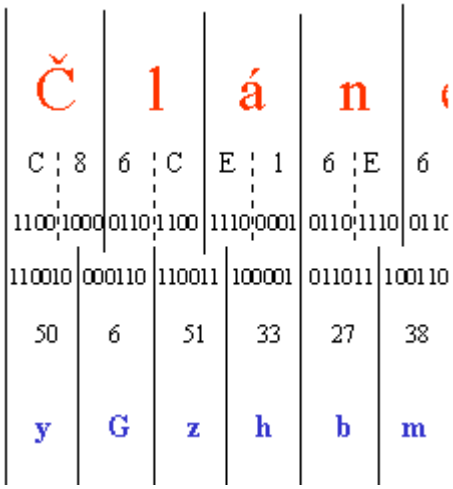
- **POP3**
    - Dávkově se stahuje pošta do PC, nezůstává na serveru
- **IMAP4**
    - Emaily zůstávají na serveru, pouze se stáhnou, když si je chceme prohlédnout

MIME

- Multipurpose Internet Mail Extension
- Umožňuje posílat nestandardní ASCII znaky (8-bitové - s ASCII kódem 128-255) a umožňuje posílat přílohy
- Pomocí MIME se 8-bitové znaky překódují do 7-bitového vyjádření, aby šli odeslat přes SMTP
- MIME je především záležitostí e-mailových klientů - ti mají za úkol zprávu používající MIME při odeslání zakódovat, při přijetí dekódovat
- Ukázka zprávy, na kterou bylo použito MIME ☐ viz. obrázek ☐
- Metody pro překódování nestandardních znaků do 7-bit. vyjádření:
    - **Quated Printable**

- použití tam, kde se text příliš neliší od čistého ASCII textu
- převod nestandardních znaků na základní ASCII znaky v 7-bitovém vyjádření
- např.: Č ☐ "=C8" (kód znaku v šestnáctkové soustavě)
- zakódovaný text je stále pro člověka čitelný (při malém výskytu cizích znaků)

- **Base64**
  - použití při větší odlišnosti textu od klasických ASCII znaků
  - určeno především pro obecná binární data
  - kódovaná data jsou o třetinu delší než originální text
  - pro člověka zcela nesrozumitelný text
  - text se rozdělí na bity a ty se pak po šesti useknou a vytvoří standardní ASCII znak ☐ viz. obrázek



Princip fungování Base64

Zabezpečení zprávy

Pro zabezpečení elektronických zpráv se využívá šifrování pomocí klíčů, které zajistí, že zprávu přečtou jen povolané osoby, a digitální podpisy pro ověření identity odesílatele.

Šifrování

- nebo-li moderní kryptografie
- dělí se na:
  - **Symetrické šifrování**
    - použití jednoho (privátního) klíče
    - privátním klíčem se šifruje i dešifruje
    - rychlejší, ale nemožnost bezpečného předání klíče
    - Přehled šifrovacích algoritmů:
      - DES
        - klíč o 56 bitech
        - používá se i víckrát za sebou (Double DES, Triple DES...)
      - RC
      - IDEA
  - **Asymetrické šifrování**
    - používá dva klíče - veřejný a privátní

    - předává se jen veřejný klíč, kterým druhá strana zprávu zašifruje a příjemce ho pak svým privátním klíčem dešifruje
    - šifruje se veřejným klíčem příjemce, přečíst zprávu jde jen pomocí příjemcova privátního klíče
    - algoritmus RSA - klíč s libovolnou délkou, používá se i jako základ pro digitální podpisy

- díky svým vlastnostem se v případě el. pošty spíše používá **asymetrické** šifrování, protože je výhodnější

Podepisování - HASH

- HASH = otisk
- díky HASHi máme jistotu, že zpráva nebyla změněna
- HASH je obsažen v digitálním podpisu, který je zašifrován privátním (podpisovým klíčem)
- V podpisu je Veřejný klíč odesílatele, zašifrovaný HASH a adresa odesílatele
    - Obsahuje také podpis certifikační autority
    - Celý certifikát obsahuje jak privátní tak veřejný klíč, ale posílá se pouze veřejná část !
    - Certifikáty mají příponu .P12

- **Hashovací algoritmy:**
    - MD5 (128 bitový výtah)
    - SHA (160 bitový výtah)

- Uložení certifikátu
    - v počítači (nedoporučuje se)
    - zakryptován pomocí operačního systému
    - Šifrovací token (iKey)
    - Čipová karta