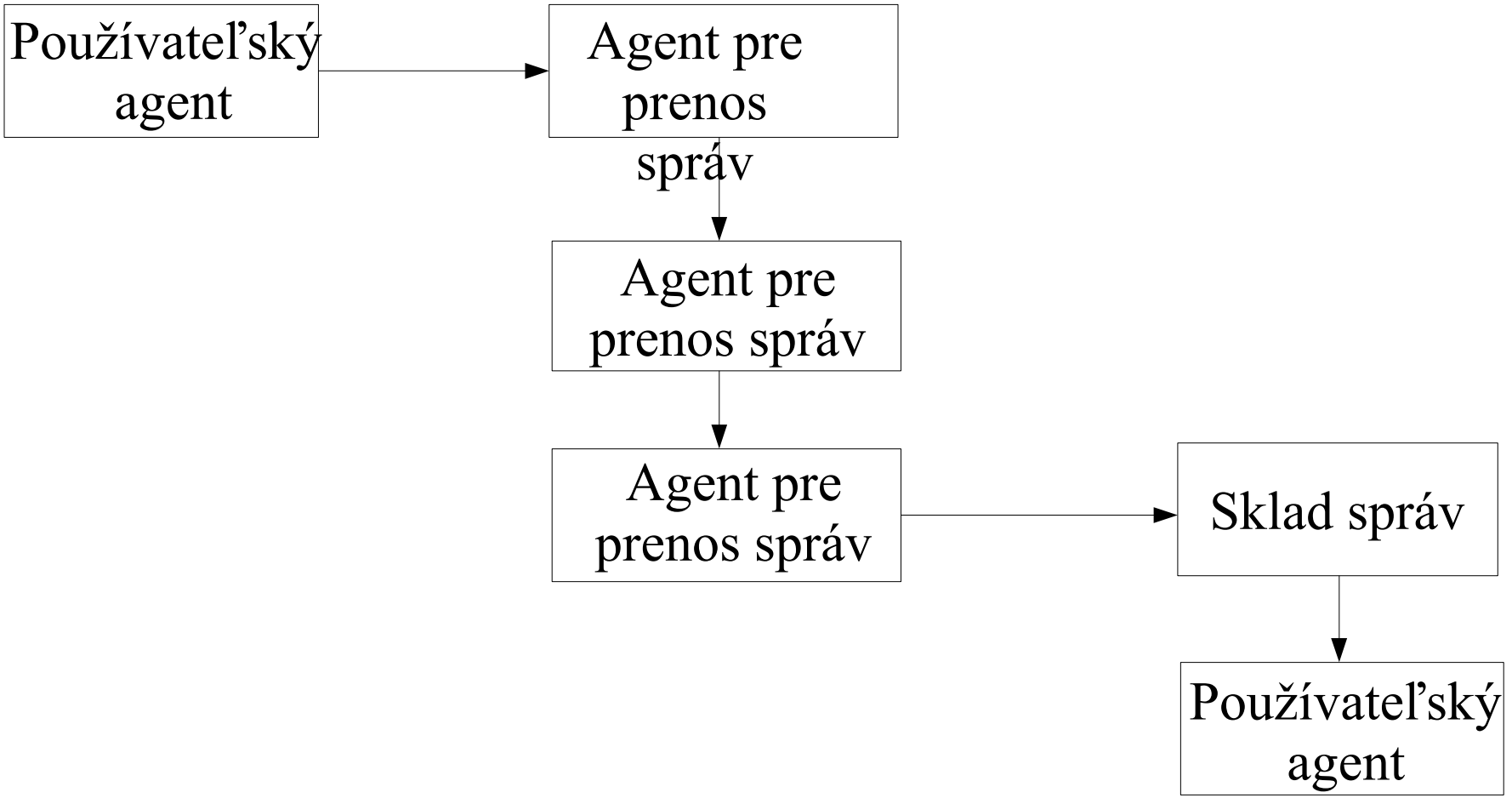
Elektronická pošta

Elektronická pošta je analógiou klasickej pošty: umožňuje používateľom výmenu správ.
Každý používateľ elektronickej pošty má vytvorenú **poštovú schránku** na niektorom z počítačov v sieti. Do tejto schránky sa ukladajú **správy**, ktoré dostáva. Správa sa skladá z **hlavičky** (informácie o odosielateľovi, adresátovi, dátume a čase odoslania a pod.) a **tela** (zvyšok správy). S poštovou schránkou je spojená používateľova **adresa**, na ktorú sa mu dajú posielať správy el. poštou. Má tvar:
označenie_používateľa@označenie_domény

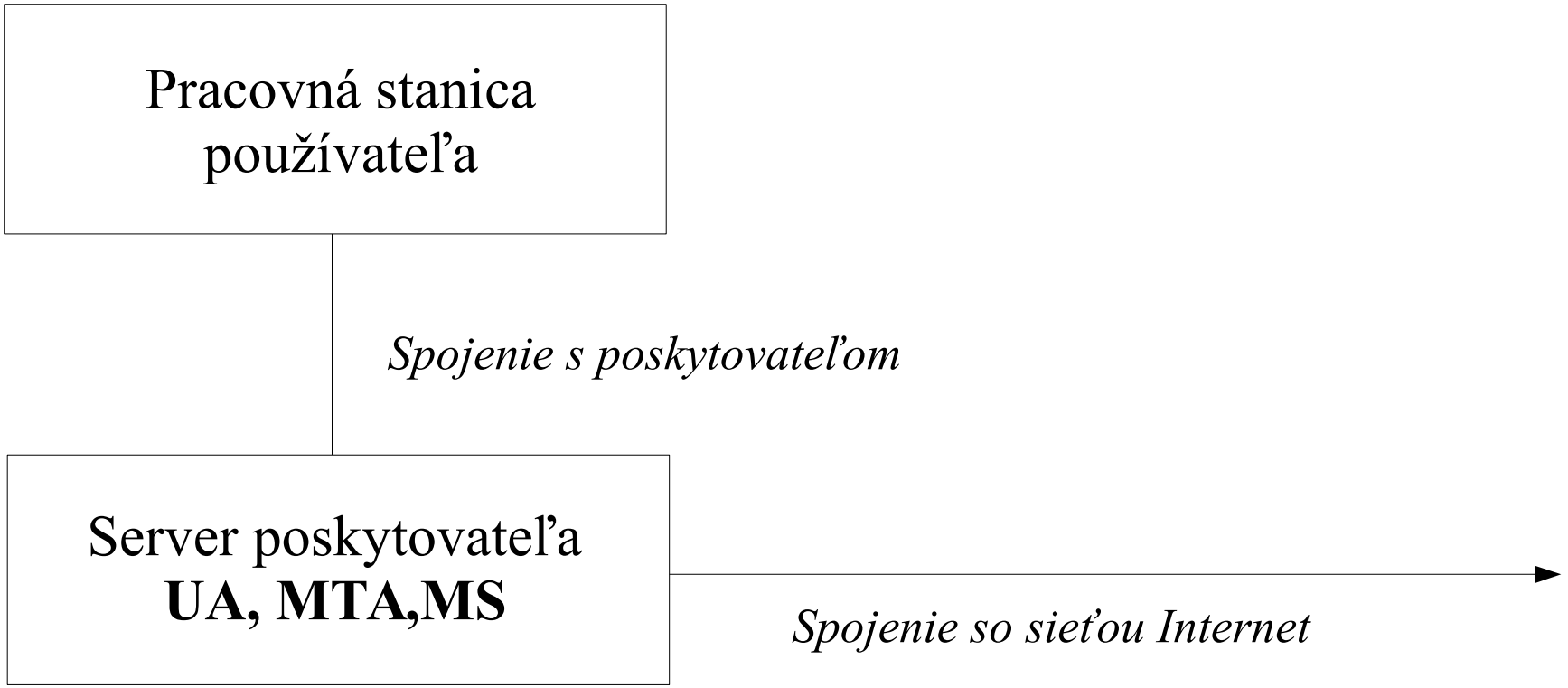
Všeobecná architektúra systému elektronickej pošty

- Používateľský agent (User Agent, UA)
  - program, pomocou ktorého používateľ spracúva správy, napr. Netscape Mail, elm a pod.
- Agent na prenos správ (Message Transfer Agent, MTA)
  - program, ktorý zabezpečuje prenos správ elektronickej pošty medzi jednotlivými počítačmi v sieti
- Sklad správ (Message store, MS)
  - miesto, kde sú uložené poštové schránky jednotlivých používateľov

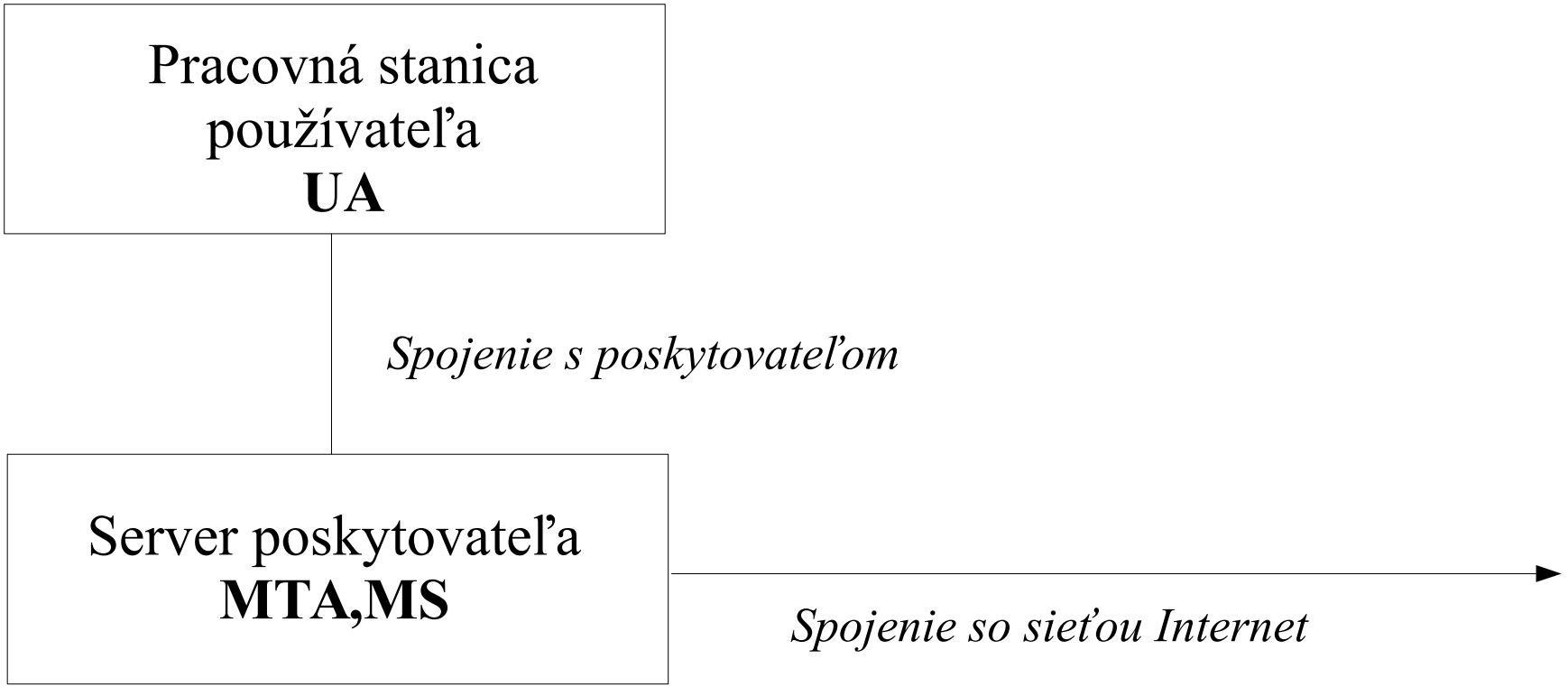
Vzájomný vzťah jednotlivých súčastí systému elektronickej pošty



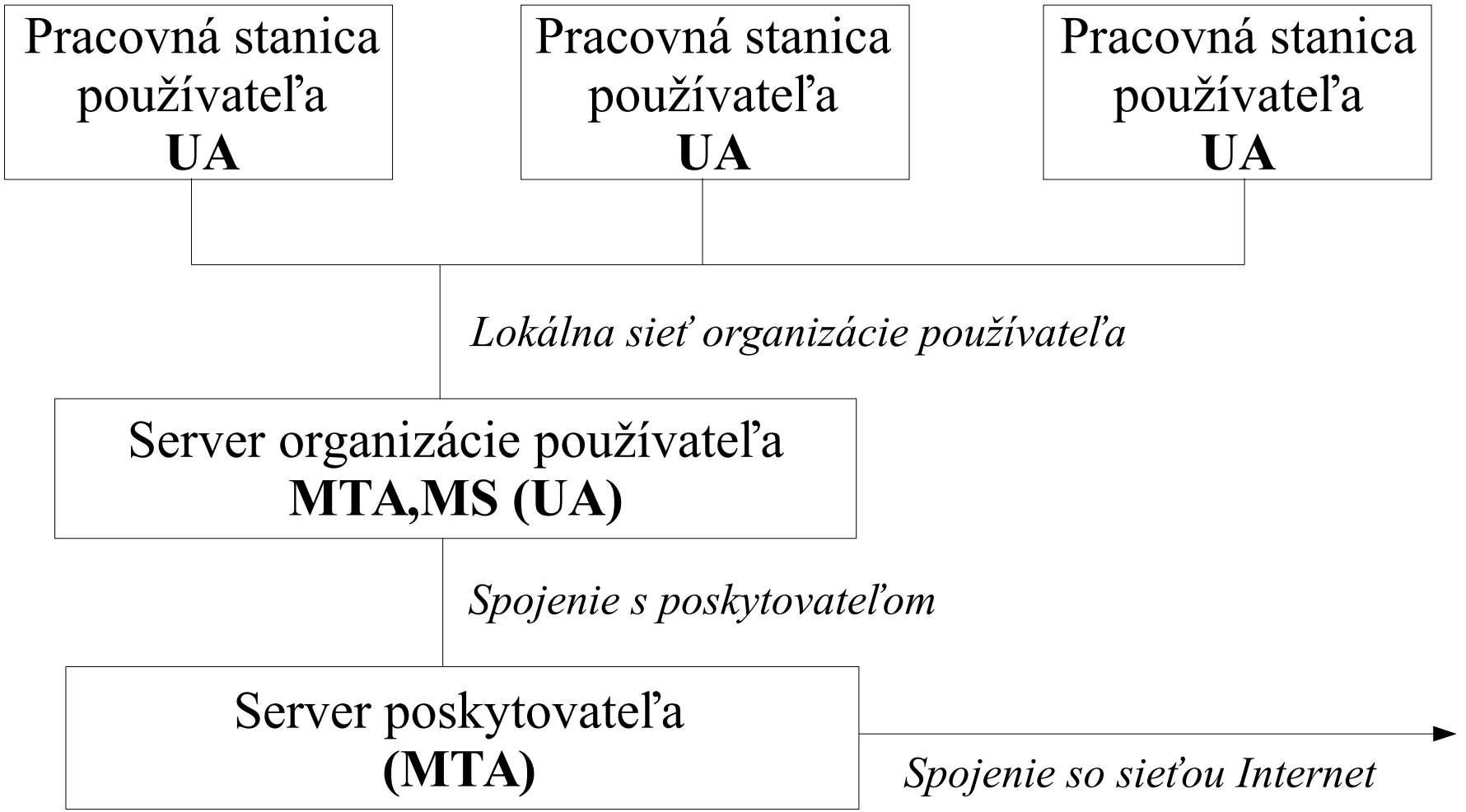
Použitie webmailu



Použitie mailového klienta u používateľa



Systém elektronickej pošty pri práci v lokálnej sieti



Prenos správ v sieti Internet

Ako prostriedok doručovania správ medzi MTA navzájom (a v istých prípadoch aj medzi UA a prvým MTA) sa používa protokol **SMTP** (Simple Mail Transfer Protocol). Ide o jednoduchý protokol, ktorý využíva protokol TCP. Možno ním posielať len správy obsahujúce 7- bitové údaje organizované ako text.

Príklad komunikácie protokolom SMTP na úrovni TCP spojenia

220 pascal MX V4.2 VAX SMTP server ready at Wed, 27 Aug 1997 19:43:36 MET
HELO center.fmph.uniba.sk
250 Hello, center.fmph.uniba.sk
MAIL FROM: <novak@fmph.uniba.sk>
250 MAIL command accepted
RCPT TO: <kovac@pascal.fmph.uniba.sk>
250 Recipient okay (at least in form)
DATA
354 Start mail input; end with <crlf>.<crlf>
Date: Wed, 27 Aug 1997 19:43:15 MET
From: Jan Novak <novak@fmph.uniba.sk>
To: kovac@pascal.fmph.uniba.sk
Subject: Skuska
Ahoj, ako sa mas? Jano
.
250 Message received and queued
QUIT
221 pascal Service closing transmission channel

Spojenie medzi používateľským agentom a poštovou schránkou.

Používateľský agent najčastejšie využíva služby zvláštneho programu, ktorého úlohou je sprístupňovať poštové schránky používateľským agentom.

- protokol **POP3** (Post Office Protocol 3) - starší a jednoduchší protokol
  - nepodporuje priečinky – len jeden priečinok prichádzajúcej pošty
- protokol **IMAP** (Internet Message Access Protocol) - novší a komplexnejší protokol
  - podporuje priečinky a presúvanie správ medzi nimi

Prenos binárnych súborov elektronickou poštou 1.

Protokolom SMTP možno posielať len správy obsahujúce 7- bitové údaje organizované ako text. Dnes sa však už posielajú aj obrázky, programy a pod., ktoré využívajú plných 8 bitov a ani nie sú organizované ako text (po riadkoch). Treba teda zabezpečiť aj posielanie takýchto údajov.
Spoločnou črtou riešení je, že pred odoslaním sú binárne údaje (využívajúce 8 bitov) transformované do textového tvaru s využitím 7 bitov, v tejto podobe prejdú systémom el. pošty a po doručení sú opäť transformované do pôvodného binárneho tvaru.

Prenos binárnych súborov elektronickou poštou 2.

Príklad riešení:

• programy **uuencode** a **uudecode** - uuencode vstupné údaje zakóduje do výstupného súboru nasledovne: vstup rozdelí na skupiny po 6 bitoch a každú takúto skupinu (reprezentujúcu číslo od 0 do 63) prevedie na jeden znak výstupu tak, že k nej pripočíta hodnotu 32, čím dostane tlačiteľný znak. Program uudecode postupuje obrátene. Nedostatok: príjemca má o druhu obsahu a formáte len veľmi málo údajov.

• **MIME** (Multipurpose Internet Mail Extensions) - novší spôsob kódovania informácií v textovom tvare, ktorý zavádza niektoré nové položky pre hlavičku správy (konkrétne MIME-version, Content-Type a Content-Transfer-Encoding)

MIME 1.

MIME pozná 3 základné spôsoby kódovania obsahu:

- **BASE64** - obsah súboru sa kóduje spôsobom podobným uuencode. Toto kódovanie sa používa pre binárne súbory.
- **Quoted Printable** - tlačiteľné znaky sa ponechajú tak, ako sú, kódujú sa len znaky s ASCII kódom nad 127 a pod 32. Kódovanie je realizované vložením znaku "=" nasledovaného hexadecimálnym zápisom ASCII kódu znaku, ktorý je potrebné zakódovať.
- **Bez kódovania** - obsah súboru sa ponechá tak, ako je. V položke Content-Transfer-Encoding sa uvedie jedna z hodnôt 7bit (ak ide o ASCII text nevyužívajúci ôsmy bit), 8bit (ak ide o ASCII text využívajúci aj ôsmy bit) alebo binary (ak ide o ľubovoľné binárne dáta).

MIME 2.

Na základe typu v položke Content-Type hlavičky správy dokážu programy na spracovanie pošty tento obsah spracovať. Príklady typov:

text/plain	obyčajný text
text/html	hypertextový dokument HTML
audio/basic	zvukový záznam (formát AU)
image/gif	obrázok vo formáte GIF
application/msword	dokument programu Microsoft Word
application/msexcel	dokument programu Microsoft Excel
application/octet-stream	nešpecifikovaný formát
multipart/mixed	správa z viacerých častí (môžu byť rôznych typov)

Bezpečnosť systému elektronickej pošty 1.

Správy elektronickej pošty sa z pohľadu bezpečnosti dajú prirovnať ku korešpondenčným lístkom písaným na písacom stroji (vrátane podpisu), lebo:

- vo všeobecnosti nie je možné overiť totožnosť odosielateľa správy
- každý, kto môže monitorovať prevádzku na komunikačných linkách, ktorými správa prechádza, môže čítať obsah správy

Predstava o úplnej bezpečnosti elektronickej pošty je teda mylná.

Bezpečnosť systému elektronickej pošty 2.

Ako zabezpečiť, že našu správu nebude čítať osoba, ktorej nie je určená a že príjemca si bude môcť overiť, že správu dostal naozaj od nás? Jediným riešením v súčasnosti je využiť možnosti kryptografie.

- "podpísať" správu pre overenie totožnosti a toho, že správa nebola počas prenosu zmenená
- zašifrovať správu tak, aby ju mohol čítať len príjemca

Toto umožňuje napr. program **PGP** (Pretty Good Privacy) alebo niektoré UA využitím **S/MIME**.

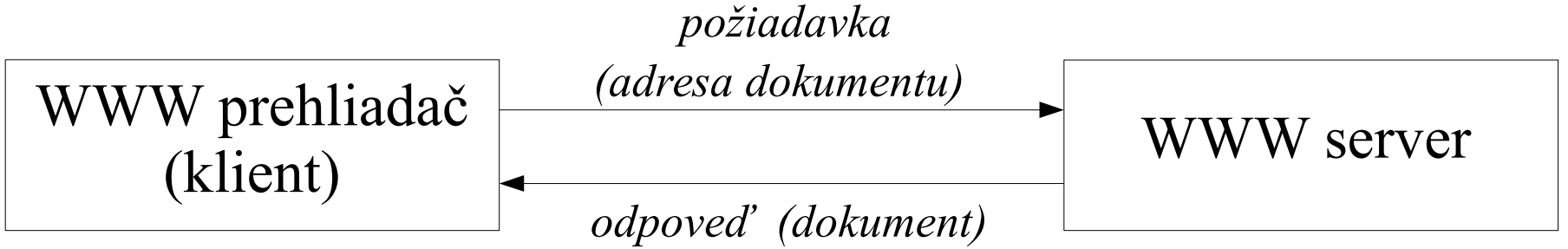
World Wide Web (WWW)

WWW je systém, ktorý umožňuje jednoduchým spôsobom pristupovať k hypertextovým a multimediálnym dokumentom.

- **hypertextový** - text dokumentu obsahuje spojenia na ďalšie dokumenty, resp. na iné miesta toho istého dokumentu
- **multimediálny** - súčasťou dokumentov môžu byť obrázky, zvukové záznamy a prípadne videosekvencie

Základné princípy práce WWW

Systém WWW pracuje na princípe klient-server. Dokumenty sú uložené na jednotlivých **WWW serveroch** (počítačoch, na ktorých beží špeciálny program nazývaný WWW server alebo HTTP server). Tieto servery ich sprístupňujú klientom, tzv. **WWW prehliadačom** (browserom).



Universal Resource Locator - adresa v systéme WWW

Adresy, ktoré sa používajú v systéme WWW (Universal Resource Locator - URL), majú tvar

prístupová metóda:špecifická časť

- prístupová metóda - spôsob, akým je daný dokument dosiahnuteľný, napr. http, ftp, news,...
- špecifická časť - závisí od prístupovej metódy. Napr. pre metódu "http" má URL nasledujúci tvar:

http://počítač:port/adresár/adresár/adresár/.../súbor

Dokumentom v systéme WWW sa hovorí aj **stránky** (pages). Spojenia medzi dokumentami sa nazývajú **odkazy** alebo **linky** (links).

Protokol HTTP (Hypertext Transfer Protocol)

Pre komunikáciu využíva HTTP protokol TCP, štandardné číslo portu je 80. Príklad:

GET /www/index.html HTTP/1.0

HTTP/1.0 200 Sending document
MIME-version: 1.0
Server: OSU/2.0
Content-type: text/html
Content-transfer-encoding: 8bit
Last-Modified: Wednesday, 27-Aug-97 07:24:20 GMT
Content-length: 2965

<HTML>
<HEAD>
<TITLE>Univerzita Komenskeho Bratislava</TITLE>
...

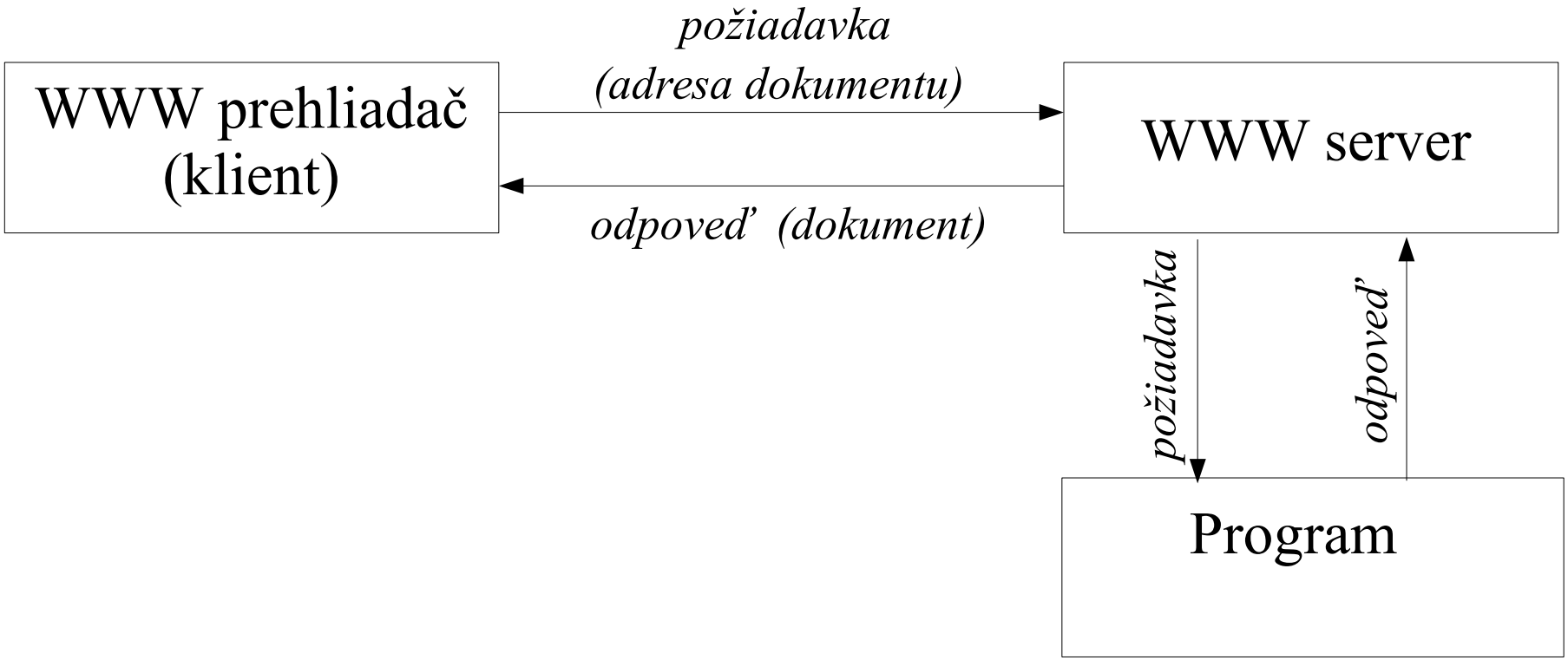
Proxy servery

- niekedy nie je možné vytvoriť priame spojenie medzi klientom a WWW serverom – napr. klient za firewallom alebo v sieti so súkromnými IP adresami
- proxy servery mávajú cache – udržiavajú v nej často navštevované stránky – zvýšenie rýchlosti prístupu

HTML

<HTML>
<HEAD>
<TITLE> Moj dokument </TITLE>
</HEAD>
<BODY>
<IMG SRC="obrazok.gif">
Toto je prvy odstavec
<P>
Toto druhy. A <A HREF="text2.html">tu sa da prejst na dalsi dokument</A>
</BODY>
</HTML>

CGI skripty


požiadavka
(adresa dokumentu)
WWW prehliadač
(klient)
WWW server
odpoveď (dokument)
požiadavka
odpoveď
Program

CGI skript

- CGI = Common Gateway Interface
- program, ktorý sa vykonáva na WWW serveri na základe požiadavky prijatej od WWW klienta
- napísaný v ľubovoľnom jazyku (C, C++, perl, PHP, sh)
- dostane údaje z formulárov
- výstupom je dokument, ktorý WWW server vráti klientovi

Programy na strane WWW klienta

- prečo nie priamo spúšťateľné programy
  - nezávislosť na platforme
  - bezpečnosť
- riešenia
  - JAVA – program v Jave (applet) sa stiahne z WWW servera a spustí v prehliadači
  - JavaScript – jednoduchší skriptovací jazyk interpretovaný prehliadačom

Zabezpečenie HTTP

- protokol HTTP prenáša údaje v “čistej” podobe
  - je možné odchytávať obsah komunikácie
  - nie je možné overiť identitu servera ani klienta
- HTTPS – HTTP over SSL
  - URL: https://www.mojabanka.sk/
  - využíva SSL protokol na šifrovanie komunikácie a na overenie identity servera a/alebo klienta
  - identita sa overuje použitím digitálnych podpisov, ktoré sa kontrolujú použitím certifikátov

Certifikáty

- certifikáty vydávajú **certifikačné autority**
- certifikačné autority môžu tvoriť hierarchickú štruktúru
  - certifikačné autority vyššej úrovne vydávajú certifikáty certifikačným autoritám nižšej úrovne
- certifikáty certifikačných autorít najvyššej úrovne musia byť prehliadaču známe
- ak prehliadač nevie overiť podpis, zobrazí upozornenie

Iné služby Internetu

- práca na vzdialených počítačoch
  - telnet, ssh
- prenos súborov – FTP (File Transfer Protocol)
- diskusné skupiny
  - mailing listy, news
- interaktívna komunikácia používateľov
  - talk, IRC, ICQ
- telefonovanie a videokonferencie