

Počítačové siete

2.4.2014

Network Address Translation (NAT)

- umožňuje komunikáciu zo siete so súkromnými adresami
- source NAT (SNAT)
 - zdroj spojenia má súkromnú adresu
- destination NAT (DNAT)
 - cieľ spojenia má súkromnú adresu
 - používa sa na sprístupnenie služby poskytovanej serverom so súkromnou adresou

Network Address Translation (NAT)

- router
 - si udržiava tabuľku „spojení“
 - adresa a port zdroja a cieľa,
 - protokol
 - preložená (vlastná) adresa a port
 - pri odosielaní prvého paketu spojenia von
 - prepíše adresu zdroja na preloženú
 - prepíše port zdroja na vlastný (voľný)
 - zapíše spojenie do tabuľky

Network Address Translation (NAT)

- router
 - pri odosielaní ďalšieho paketu spojenia von
 - nájde spojenie v tabuľke
 - prepíše adresu a port zdroja podľa tabuľky
 - pri prijatí paketu zvonku
 - nájde spojenie v tabuľke
 - prepíše adresu a port cieľa podľa tabuľky

Network Address Translation (NAT)

- DNAT
 - pri prijatí paketu zvonka na určenú verejnú adresu a port
 - ak je spojenie v tabuľke, prepíše cieľ podľa tabuľky
 - inak prepíše cieľ podľa konfigurácie a spojenie zapíše do tabuľky
 - pri odosielaní paketu von
 - nájde spojenie v tabuľke
 - prepíše zdroj podľa tabuľky

Network Address Translation (NAT)

- Ako dlho držať spojenie v tabuľke?
 - TCP – dá sa využiť sledovanie stavu spojenia
 - UDP – timeout
 - väčší timeout pre prúd UDP prúd (stream)
- Problémy s aplikačnými protokolmi
 - ak aplikačný protokol používa IP adresy a čísla portov
 - potreba podporných modulov pre udržiavanie tabuľky spojení a príp. prepisovanie dát aplikačnej vrstvy
 - napr. FTP

Aplikačná vrstva TCP/IP

- Rôzne aplikačné protokoly využívajúce TCP alebo UDP
 - WWW: HTTP – TCP/80, HTTPS – TCP/443
 - FTP – TCP/21, TCP/20
 - telnet – TCP/23
 - ssh – TCP/22
 - odosielanie e-mailov: SMTP – TCP/25
 - čítanie e-mailov: POP3 – TCP/110, IMAP - TCP/143
 - DNS – UDP/53, TCP/53

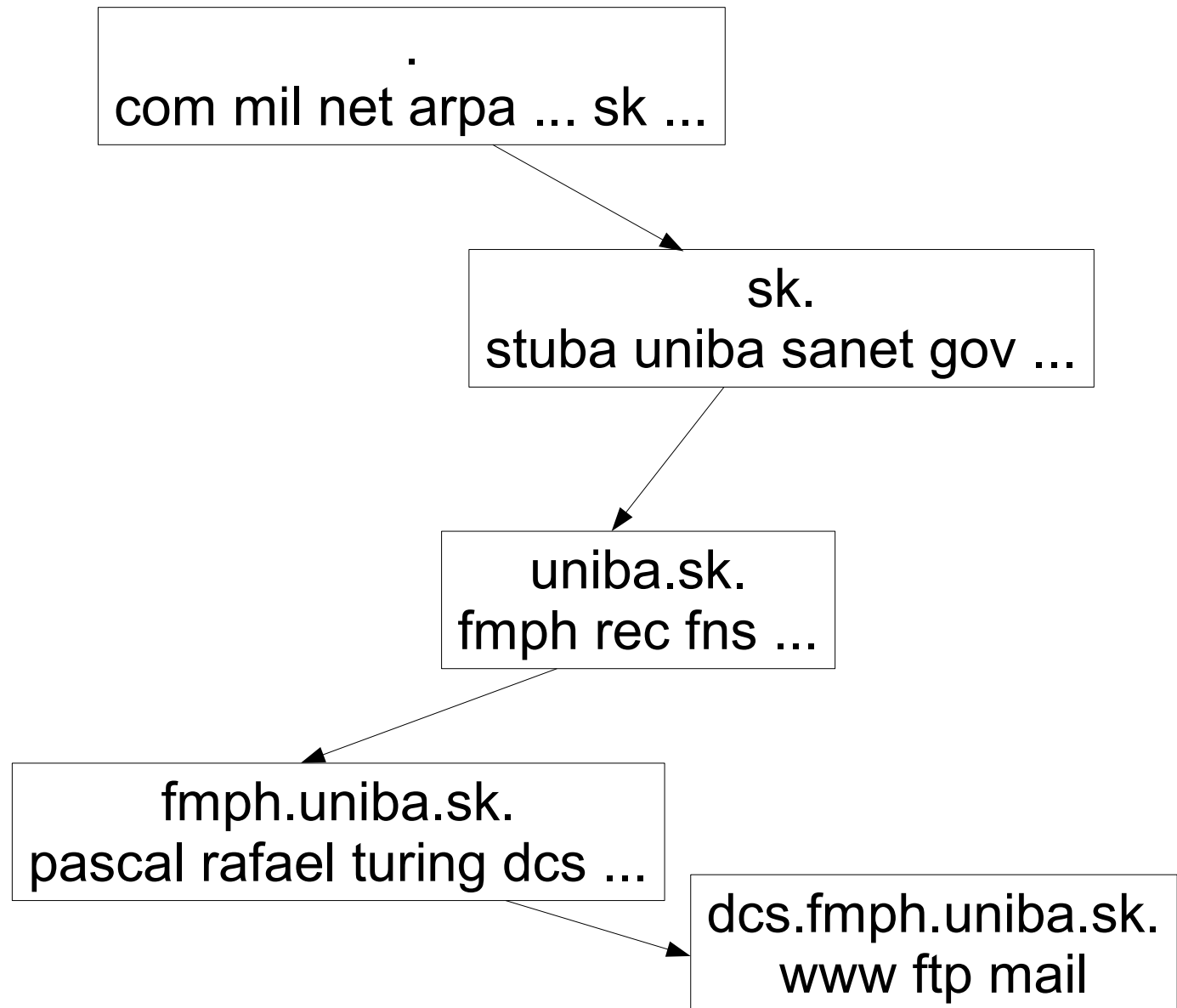
Domain Name System (DNS)

- IP adresy sa ľuďom zle pamätajú
- DNS – najväčšia distribuovaná databáza na prevod medzi doménovými menami a IP adresami
- doménové meno:
 - meno.doména_n.doména_n-1.doména_1
 - nič nehovorí o fyzickom umiestnení počítača
 - domény 1. (najvyššej úrovne)
 - generické: com, org, net, edu, gov, mil, int, biz, info, pro
 - podľa krajín: sk, cz, at, pl, hu, de, uk, ...
- informácie poskytujú DNS servery

Domain Name System (DNS)

- doménové mená tvoria strom
 - koreňom je .
 - xxx.yyy.tld je synom yyy.tld
- zóna = súvislá časť doménového stromu
 - celý podstrom
 - časť podstromu
 - t.j. bez (niektorých) jeho podstromov

Domain Name System



Domain Name System

- Rôzne typy záznamov
 - A – IP adresa
 - CNAME – alias
 - MX – mail exchanger – kam sa majú doručovať e-maily
 - NS – meno DNS servera pre poddoménu
 - SOA – základné informácie o doméne
 - PTR – používa sa pri opačnom vyhľadávaní
- A, MX a NS môže byť pre jedno meno aj viac

Domain Name System

- Ako pre danú IP adresu nájsť doménové meno?
- DNS je organizovaný podľa domén
 - prehľadanie celého stromu by trvalo veľmi dlho
- Adresu a.b.c.d vyhľadáme ako záznam typu PTR pre d.c.b.a.in-addr.arpa.
- Informácie na prevod mena na IP a naopak sú nezávislé, preto nemusia vždy súhlasiť.

DNS cache

- caching DNS server, rekurzívny DNS server
 - slúži iným počítačom v sieti
 - tie mu posielajú otázky (queries) pre DNS
 - získava údaje z DNS
 - ukladá ich do cache
 - odpovede prednostne hľadá v cache
- nerekurzívny, autoritatívny DNS server
 - odpovedá len na priame otázky týkajúce sa „jeho“ zón

Používanie DNS v praxi

- bežný počítač v sieti
 - má nastavený jeden alebo viac rekurzívnych DNS serverov
 - všetky otázky posiela len im
- rekurzívny DNS server
 - nájde finálnu odpoveď (otázkami do cache / DNS)
 - pozná minimálne DNS servery pre koreňovú zónu (.)
- nerekurzívny DNS server
 - má autoritatívne informácie o jednej / viac zónach

DNS – príklad

```
dig +norec www.google.sk @ns.sk-nic.sk
```

```
; <<>> DiG 9.7.3 <<>> +norec www.google.sk @ns.sk-nic.sk  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11415  
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
;www.google.sk.          IN  A
```

```
;; AUTHORITY SECTION:  
google.sk.      86400  IN  NS  ns4.google.com.  
google.sk.      86400  IN  NS  ns1.google.com.  
google.sk.      86400  IN  NS  ns3.google.com.  
google.sk.      86400  IN  NS  ns2.google.com.
```

```
;; Query time: 9 msec  
;; SERVER: 195.12.159.2#53(195.12.159.2)  
;; WHEN: Tue Mar 19 20:37:35 2013  
;; MSG SIZE rcvd: 113
```

DNS – príklad

:: flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 4

:: QUESTION SECTION:

;www.google.sk. IN A

:: ANSWER SECTION:

www.google.sk.	300	IN	A	173.194.44.255
www.google.sk.	300	IN	A	173.194.44.247
www.google.sk.	300	IN	A	173.194.44.248

:: AUTHORITY SECTION:

google.sk.	83358	IN	NS	ns3.google.com.
google.sk.	83358	IN	NS	ns4.google.com.
google.sk.	83358	IN	NS	ns1.google.com.
google.sk.	83358	IN	NS	ns2.google.com.

:: ADDITIONAL SECTION:

ns1.google.com.	134395	IN	A	216.239.32.10
ns2.google.com.	134395	IN	A	216.239.34.10
ns3.google.com.	134395	IN	A	216.239.36.10
ns4.google.com.	134395	IN	A	216.239.38.10

DHCP

- konfigurácia sieťových parametrov počítača
- DHCP klient
 - počítač, ktorý chce získať IP adresu
- DHCP server
 - prideľuje adresy DHCP klientom
 - staticky (napr. na základe linkovej adresy)
 - dynamicky (z množiny voľných adries, ktoré obhospodaruje)
 - snaha o „zachovanie“ adries

DHCP

- používá UDP
 - port na klientovi 68
 - port na serveri 67
 - zdrojová IP adresa na klientovi 0.0.0.0

DHCP

- DHCP DISCOVER
 - klient (0.0.0.0) -> server (255.255.255.255)
 - klient žiada o ponuku adresy
- DHCP OFFER
 - server -> klient
 - server ponúka adresu
 - v prípade ponúk od viacerých serverov si klient vyberie jednu

DHCP

- DHCP REQUEST
 - klient -> server (255.255.255.255)
 - klient žiada server o pridelenie ponúknutej adresy
- DHCP ACK
 - server -> klient
 - server potvrdzuje pridelenie adresy klientovi na určitý čas

DHCP

- DHCP NAK
 - server -> klient
 - server odmieta požiadavku klienta
- DHCP RELEASE
 - klient -> server
 - klient sa vzdáva adresy

DHCP

- DHCP DECLINE
 - klient -> server
 - klient odmieta adresu
- DHCP INFORM
 - klient -> server
 - klient s externe nakonfigurovanou IP adresou si pýta ďalšie konfiguračné informácie

DHCP

- obnovenie adresy
 - po reštarte alebo pre vypršaním
 - DHCP REQUEST
 - DHCP ACK alebo DHCP NAK

DHCP

- klient -> server
 - DHCP DISCOVER broadcast
 - DHCP REQUEST broadcast / unicast
 - DHCP RELEASE unicast
 - DHCP DECLINE broadcast
 - DHCP INFORM broadcast

DHCP

- server -> klient
 - DHCP OFFER, ACK
 - preferovane unicast na adresu ponúknutú klientovi a linkovú adresu klienta z požiadavky
 - DHCP NAK
 - broadcast

DHCP

- okrem IP adresy, ďalšie parametre
 - čas platnosti
 - maska, broadcast-ová adresa
 - default gateway
 - DNS server
 - meno (hostname), doména (domain name)
 - NTP server
 - ...

DHCP Relay

- jeden DHCP server môže spravovať adresy vo viacerých sieťach
- DHCP relay agent
 - preposiela DHCP požiadavky od klientov v sieti na určený DHCP server a späť

BOOTP

- predchodca DHCP
- nepodporoval pridelovanie adres na „určitý čas“
- technicky je DHCP rozšírením BOOTP
 - DHCP server môže podporovať aj BOOTP klientov

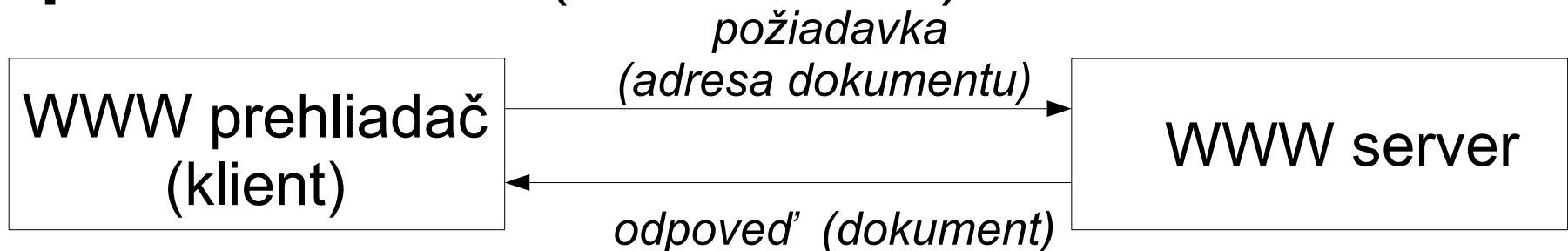
World Wide Web (WWW)

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

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

Základné princípy práce WWW

System 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

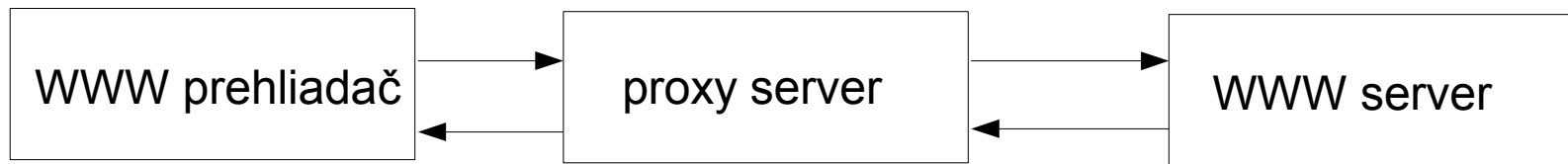
<HTML>

<HEAD>

<TITLE>Univerzita Komenského 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 majú cache – udržiavajú v nej často navštevované stránky – zvýšenie rýchlosti prístupu

HTML

<HTML>

<HEAD>

<TITLE> Moj dokument </TITLE>

</HEAD>

<BODY>

Toto je prvý odstavec

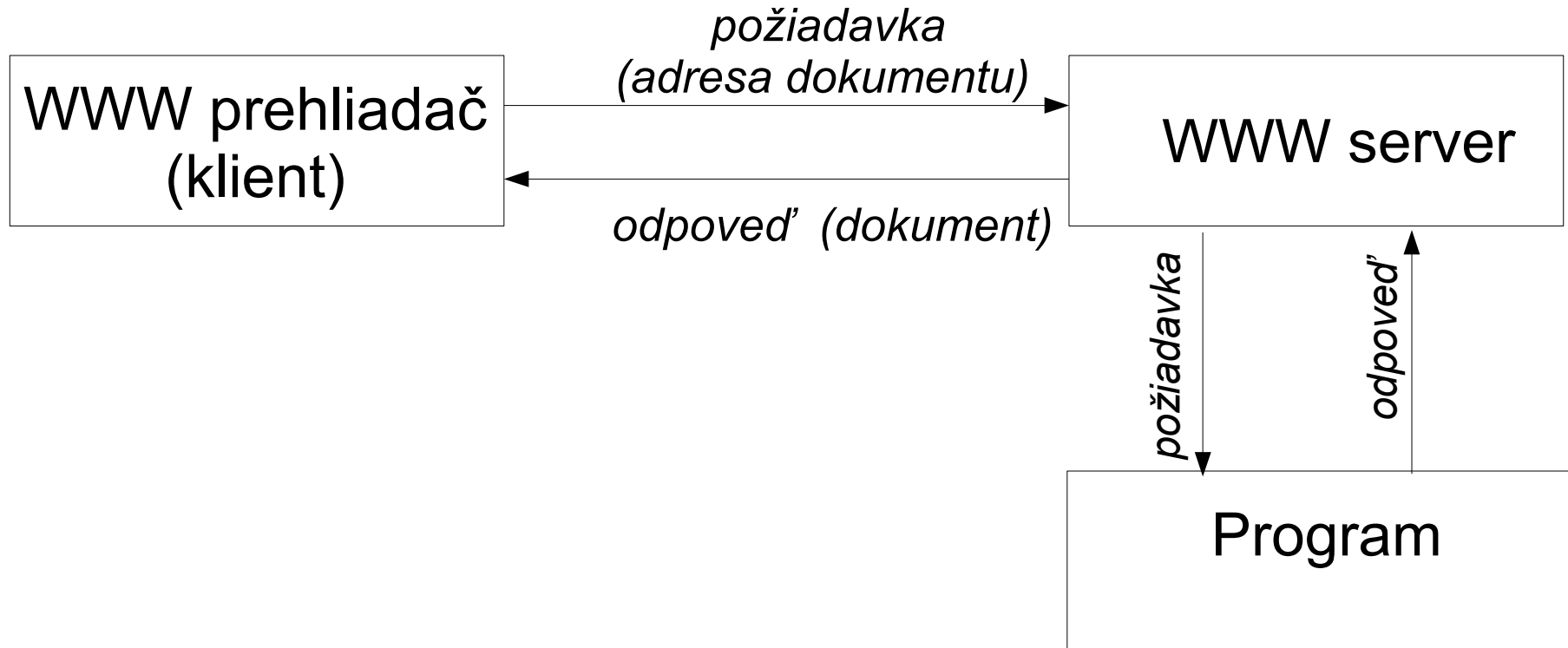
<P>

Toto druhy. A tu sa da prejsť na ďalší dokument

</BODY>

</HTML>

CGI skripty



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 – skriptovací jazyk interpretovaný prehliadačom

Elektronická pošta

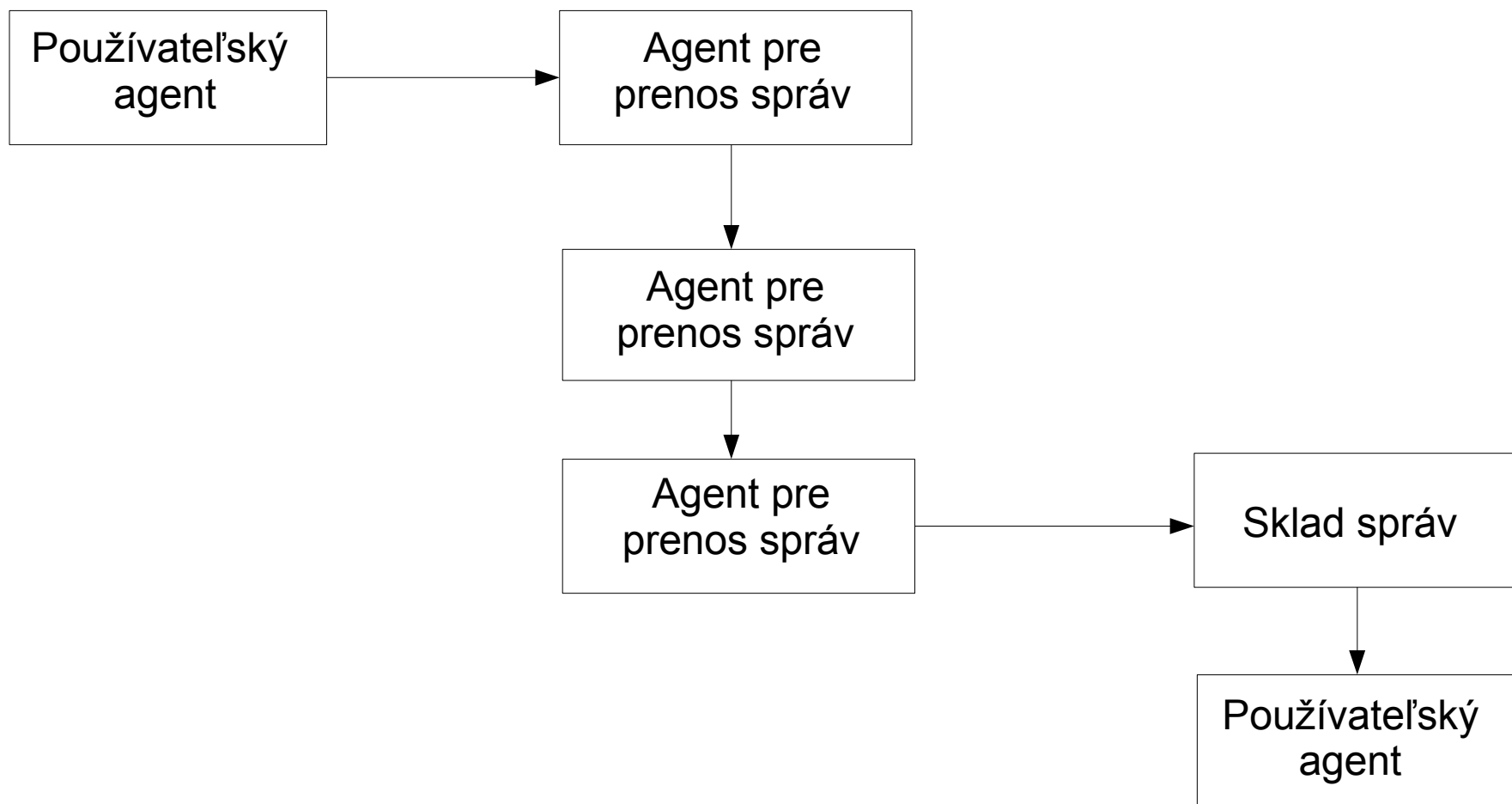
Elektronická pošta je analógiou klasickej pošty: umožňuje používateľom výmenu správ.

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 posielat' 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. Thunderbird, Outlook, mutt 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

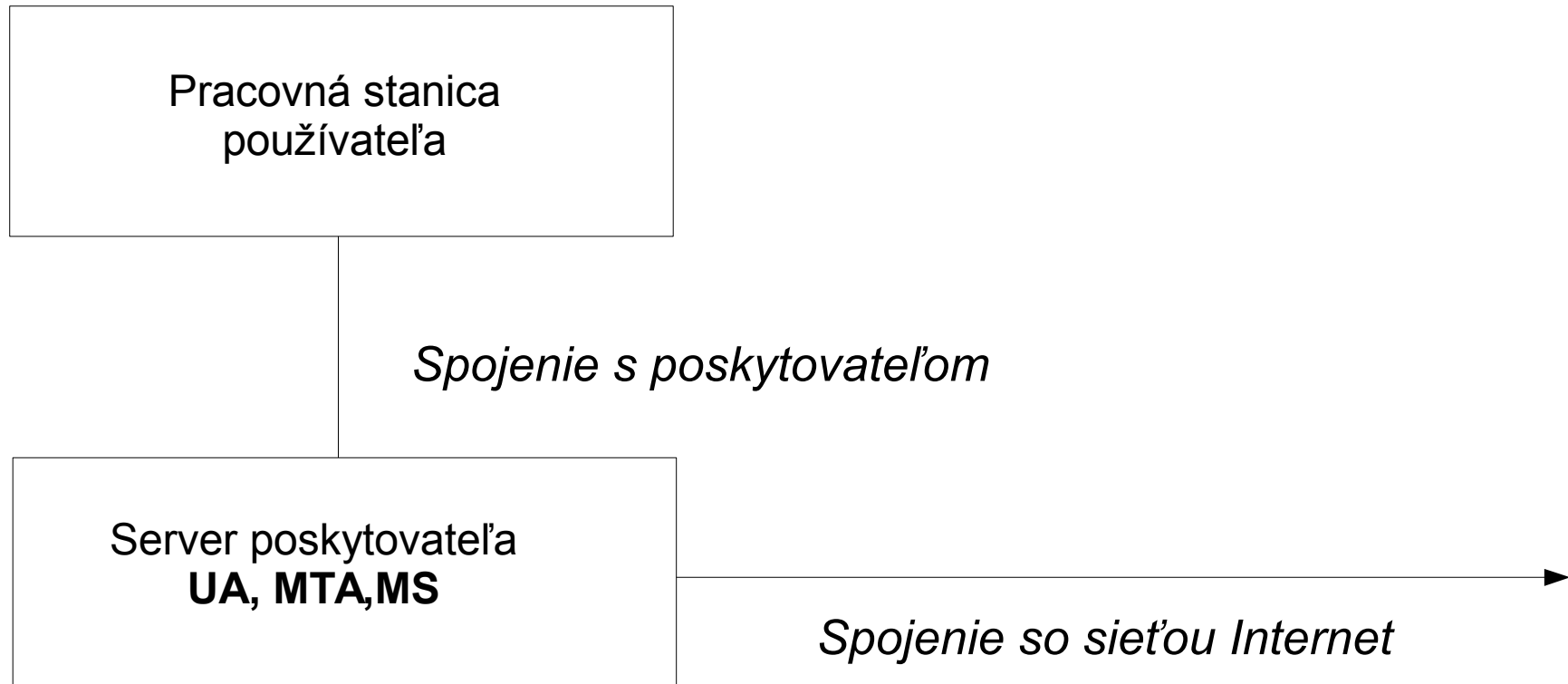
Vzájomný vzťah jednotlivých súčastí systému elektronickej pošty



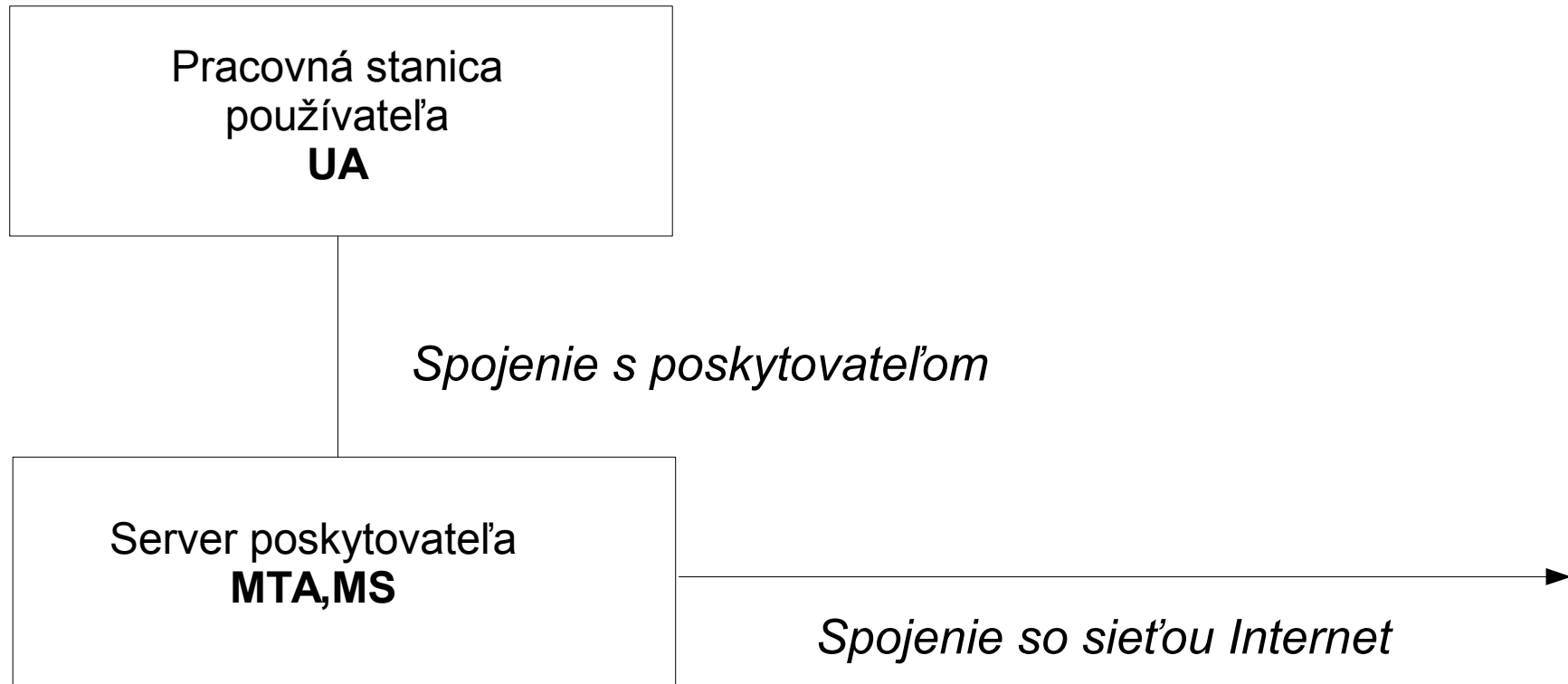
Najčastejšie možnosti usporiadania systému el. pošty

- použitie všeobecného tenkého klienta
 - napr. WWW prehliadač, emulátor terminálu
 - všetky špecifické programy na serveri poskytovateľa
- použitie špecifického programu pre poštu
 - UA beží na zariadení používateľa
- spracovanie pošty vo vlastnej LAN
 - vlastný poštový server

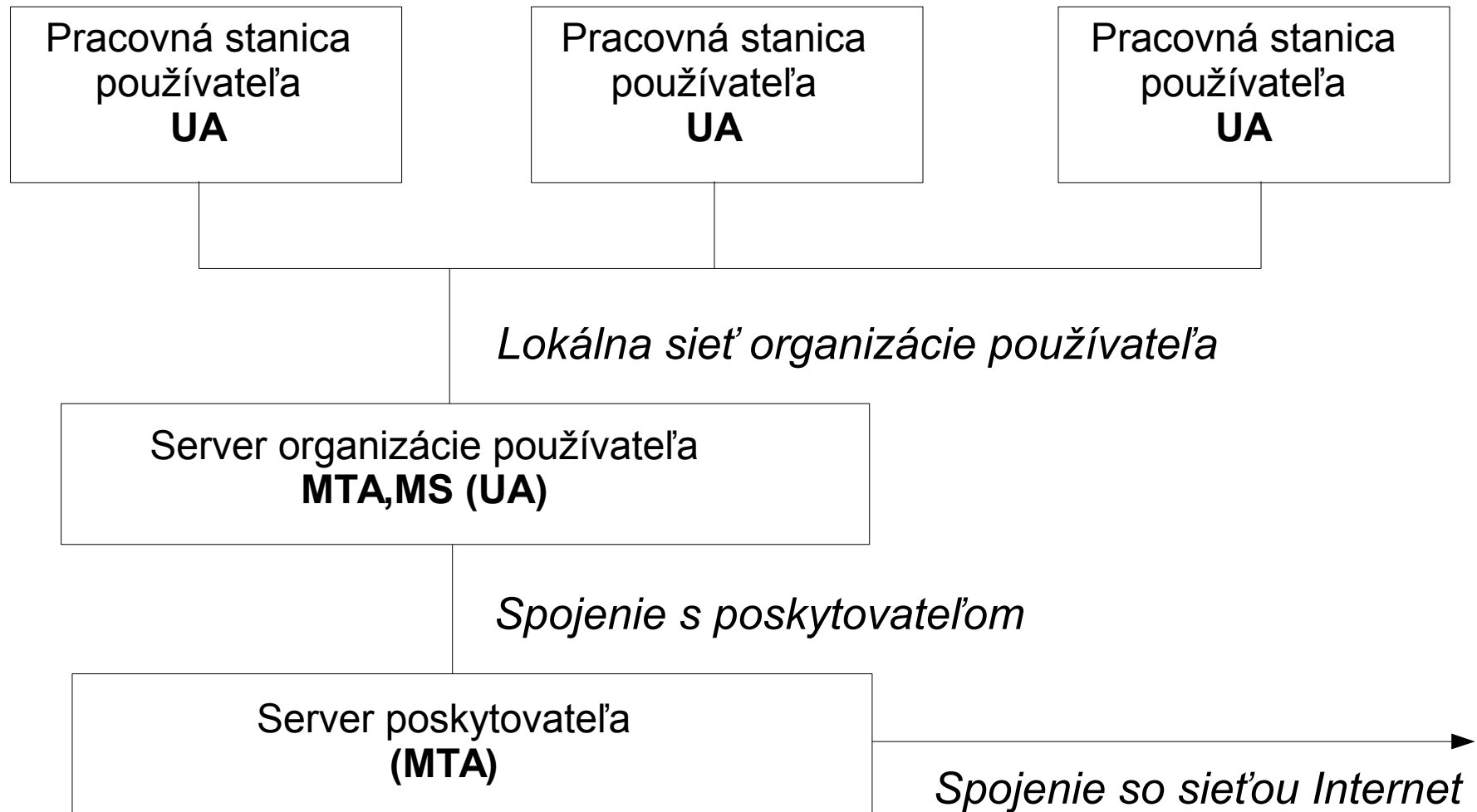
Použitie všeobecného tenkého klienta



Použitie špecifického klienta



Spracovanie pošty v LAN



Prenos správ v sieti Internet

- Simple Mail Transfer protocol (SMTP)
 - prenos medzi MTA
 - často aj prenos správ z UA k MTA
 - len textové 7-bit správy
 - TCP, port 25
 - využitie MX záznamov v DNS pre nájdenie servera

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 <cr>.<cr>

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

Čítanie správ el. pošty – komunikácia medzi UA a MS

- priamo cez súborový systém
 - ak je UA na tom istom systéme ako MS
- cez všeobecné služby prístupu k vzdialeným súborom
- použitím špecifických protokolov
 - POP3
 - IMAP

POP3

- starší, jednoduchý protokol
- TCP, port 110
- neumožňuje správu viacerých priečinkov pre poštu (len jeden INBOX)
- klient poštu prečíta a môže vymazať zo servera
- väčšina klientov nedokáže načítať najprv len hlavičky správ a telá až na vyžiadanie

IMAP

- Internet Message Access Protocol
- TCP, port 143
- umožňuje komplexnú správu priečinkov na serveri
 - presun správ medzi priečinkami, vytváranie/mazanie priečinkov, ...
- typicky sa najprv čítajú len hlavičky správ, telá až na vyžiadanie
- väčšina klientov umožňuje ukladať aj lokálnu kópiu správ

Prenos binárnych súborov poštou

- SMTP – len 7-bit text
- požiadavka na prenos ľubovoľných binárnych príloh
 - kódovanie do 7-bit textu
 - prenos 7-bit textu protokolom SMTP
 - dekódovanie

uuencode/uudecode

- uuencode
 - vstup sa rozdelí po 6 bitoch -> séria čísel 0-63
 - ku každému číslu sa pripočíta 32
 - tým získame tlačiteľné ASCII znaky
 - zalámeme do riadkov
- uudecode
 - opačne
- nedostatok informácie o type obsahu

MIME

- Multipurpose Internet Mail Extension
- pridáva nové hlavičky
 - MIME-Version
 - Content-Type
 - identifikuje typ dokumentu
 - Content-Transfer-Encoding
 - identifikuje typ kódovania

MIME – kódovanie

- BASE64
 - podobné kódovanie ako uuencode
- Quoted Printable
 - tlačiteľné ASCII znaky bez zmeny
 - znaky pod 32 a nad 127 sa nahradia =**XX**, kde XX je kód znaku v 16-kovej sústave
- bez kódovania
 - 7bit, 8bit, binary

MIME – typ obsahu

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/octet-stream	nešpecifikovaný formát
multipart/mixed	správa z viacerých častí (môžu byť rôznych typov)
multipart/alternative	rôzne formy rovnakého obsahu (napr. textová a HTML verzia)