



A2B32DAT

Datové sítě

Ing. Jakub Doležal

Katedra telekomunikační techniky
FEL ČVUT v Praze

dolezj12@fel.cvut.cz

Distribuovaný systém doménových jmén - DNS

„Domain Name System“

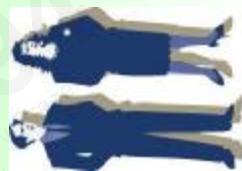
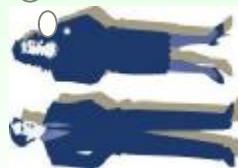
© CTU Faculty of Electrical Engineering
© České vysoké učení technické v Praze
© ČVUT v Praze, Fakulta elektrotechnická
12.-12. 2010



IP adresy a jména domén

Proč si máme
pamatovat ty
strašná čísla

a co takhle místo
čísel nějaké jméno
např. MujServer



Czech Technical University
Faculty of Electrical Engineering
© Czech vysoké učení technické
Fakulta elektrotechnická
29. 12. 2010

IP adresy a jména domén

- člověk preferuje jako odkaz spíše jméno, než číslo ve formě IP adresy

- doménová jména jsou alfanumerické názvy serverů nebo služeb nahrazujících přímou adresaci (IP nebo i jinou), např. www.seznam.cz, www.atlas.cz, www.cvut.cz

- **systém doménových imen – DNS (Domain Name System)** je celosvětově distribuovaná databáze, jež přiřazuje konkrétnímu doménovému jménu IP adresu koncové stanice nebo odpovídající služby (to je ale jen jedna z dnes nejrozšířenějších služeb DNS !!)



Co bylo před DNS

.... existoval v centru Internetu soubor HOSTS.TXT

- do roku 1985 se přiřazení nestrukturovaného jména k IP adresě realizovalo pomocí mapovacího souboru hosts.txt, který bylo nutné pravidelně stahovat z centrálního FTP serveru a takéž pravidelně aktualizovat
 - systém mapování pomocí hosts.txt souboru je stále ještě u většiny OS funkční a lze jej v případě potřeby, kdy není k dispozici DNS server, použít jako lokální databázi
 - jména v souboru neměla žádnou specifickou strukturu
- tento systém je nepoužitelný pro velký počet mapovacích záznamů !!



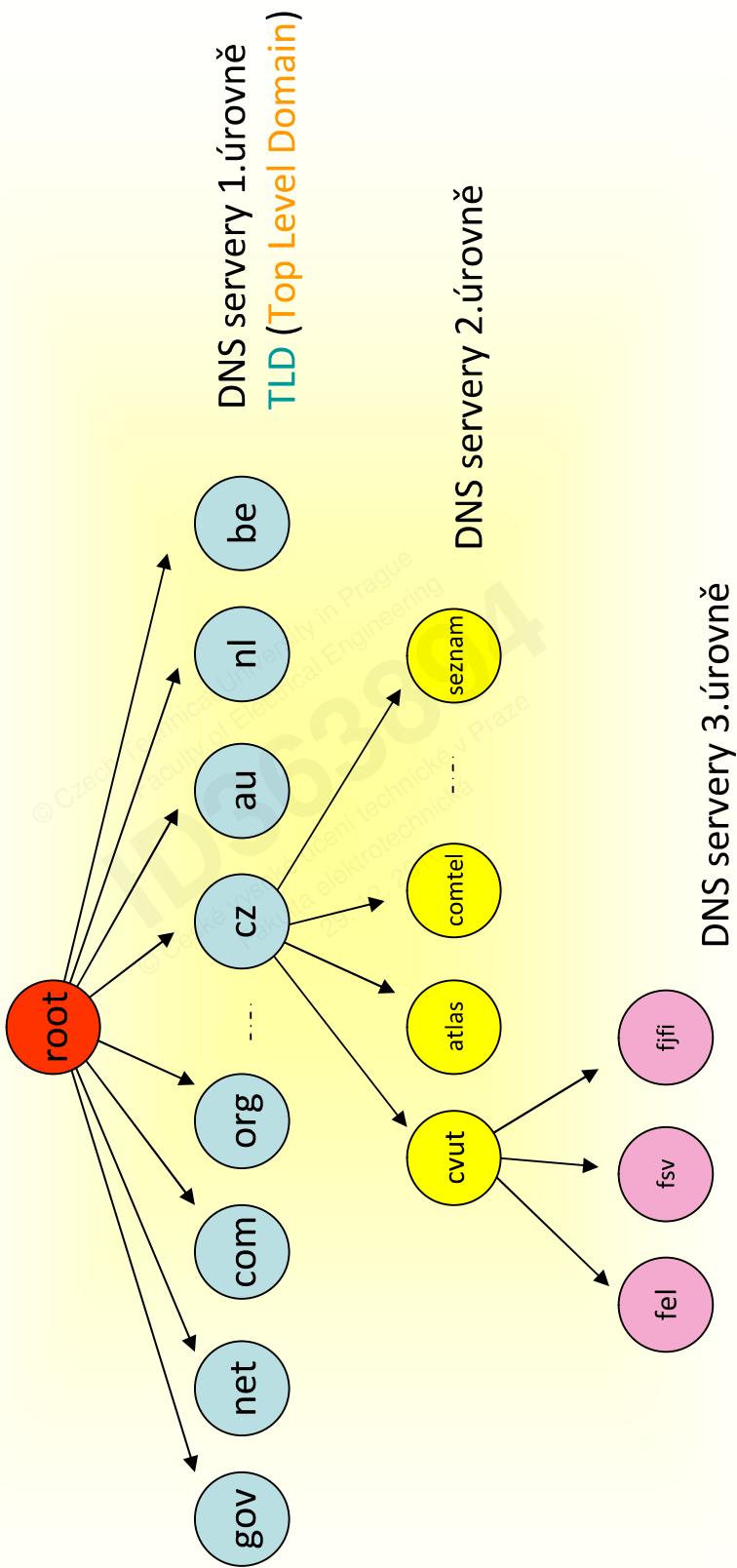
Technické principy DNS

- systém jmen na němž je DNS založen tvoří **hierarchickou stromovou strukturu**, které se říká **doménový jmenný prostor (domain name space)**
- organizace (obecně subjekt) obdrží oprávnění k určité části jmenného prostoru, kam může přidávat další úrovně nebo koncové uzly
- jména je možné vytvářet **bez přímé vazby na topologii IP sítě (výhoda); topologie sítě a DNS struktura jsou obecně na sobě nezávislé !!!**
- v praxi však **DNS struktura kopíruje strukturu přidělení IP adres**, protože IP adresace má podobnou hierarchii jako DNS jmenný prostor (není to technicky nutné, ale je to vhodné administrativně)
 - např., všechny koncové stanice v IP síti 147.32.0.0/16 mají doménovou příponu cvut.cz



Hierarchie jmen v DNS

ROOT servery (=tečka na konci DNS jména, www.seznam.cz.)



Hierarchie jmen v DNS

- hierarchii DNS lze reprezentovat **stromem**
- **kmenová (root)** a některé **nejvyšší domény (top-level)** jsou administrovány centrální registracní autoritou Internetu – **ICANN** (*Internet Corporation for Assigned Names and Numbers*)
- jmenný prostor pod nejvyššími doménami (**TLD**) je delegován jednotlivým organizacím do jejich správy
- každá organizace poté může dle potřeby rozdělit svou doménu na **poddomény (subdomains)** a **delegovat** zodpovědnost za ně na odpovídající nižše položené jmenné servery DNS systému nižší úrovně

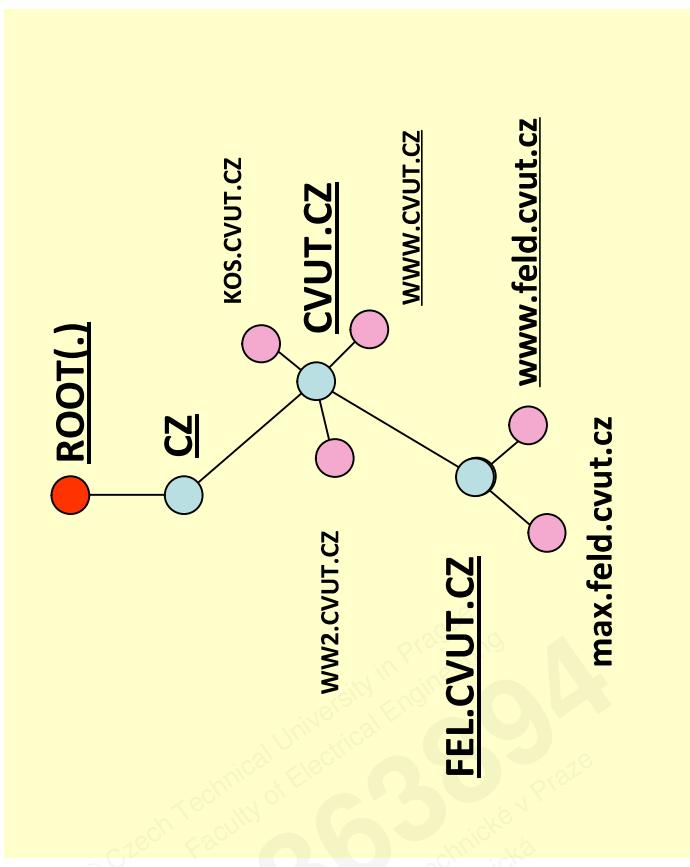


Hierarchie jmen v DNS

- každý list DNS stromu reprezentuje jedno DNS jméno služby nebo zařízení
- každá větev DNS stromu reprezentuje jednu DNS doménu

- DNS doména může obsahovat jak jména zařízení nebo služeb, tak i jména podřízených poddomén s odkazem na jejich jmenné DNS servery, na nichž jsou dostupné další informace o poddoménách

- příklad:
doména CVUT.CZ obsahuje jak jméno služby s DNS jménem www.cvut.cz, tak i subdoménu např. fel.cvut.cz, jejíž správa je delegována fakultě elektrotechnické ČVUT



Zápis DNS jména

- koncová zařízení, služby a domény jsou pojmenovány podle své pozice v DNS stromu
- každý uzel ve stromu DNS systému lze jednoznačně identifikovat pomocí jednoznačného plně kvalifikujícího doménového jména (Fully Qualified Domain Name - FQDN), FQDN určuje pozici jména v DNS stromu
- FQDN se skládá z několika návěstí ("cz", "cvut", "fel") oddělených tečkami (".")
- na konci FQDN DNS jména by správně měla být vždy tečka (ta označuje vlastní kmen stromu DNS, tzv. kmenovou (ROOT) doménu), často se pro jednoduchost vynechává
- každé návěští může být dlouhé maximálně 63 znaků
- celková délka DNS jména nesmí překročit včetně všech teček 255 znaků
- FQDN název by měl obsahovat jen alfanumerické ASCII znaky, číslice a pomlčku (-) (ta nesmí být na začátku, ani na konci žádného návěsti) (nebereme zde v úvahu mezinárodní rozšíření DNS systému !!!, které se zatím nerozšířilo)
- u FQDN nezáleží na velkých či malých písmenech (www.cvut.cz je stejně jako www.cvut.cz)

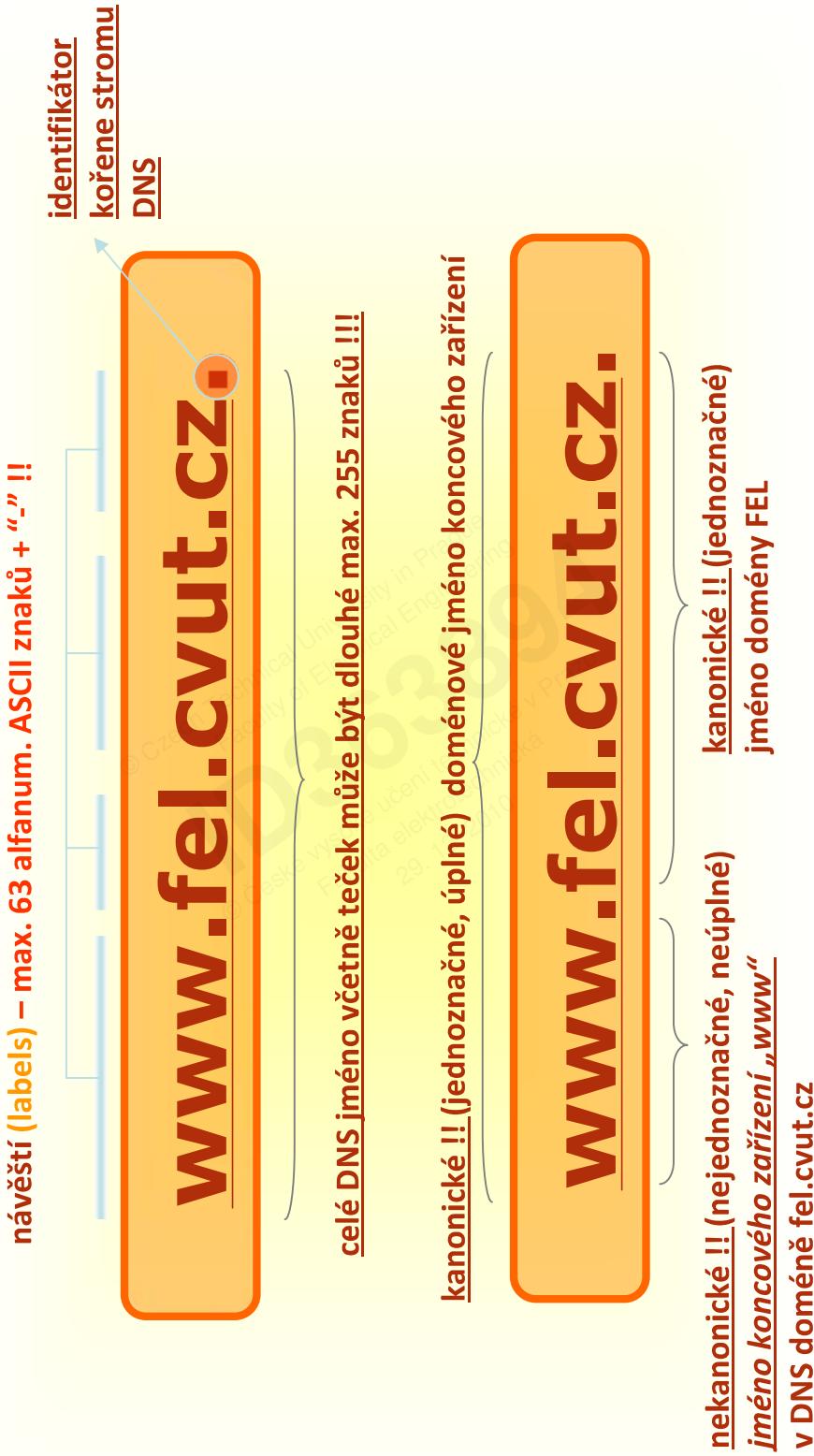
www.cvut.cz

=

www.cvut.cz



Zápis DNS jména



Domény nejvyšší úrovně

- tři typy domén nejvyšší úrovně:

–organizační a funkční: tři znaky určují charakter domény

- původní domény, hlavně v USA
 - příklad: **gov.**, **mil.**, **edu.**, **org.**, **com.**, **net.**
- geografické: dva znaky určují zemi
 - příklad: **us.**, **de.**, **cz.**, **be.**, **sk.**, atd.
- reverzní domény: speciální doména (**in-addr.arpa.**) určená pro zpětné mapování mezi IP adresou a jejím DNS jménem !!
(odpovidá DNS záznamu typu PTR)
- ENUM: doména překladu telefonních čísel na URI služby

- dnes existuje na **200 domén nejvyšší úrovně (TLD's)**



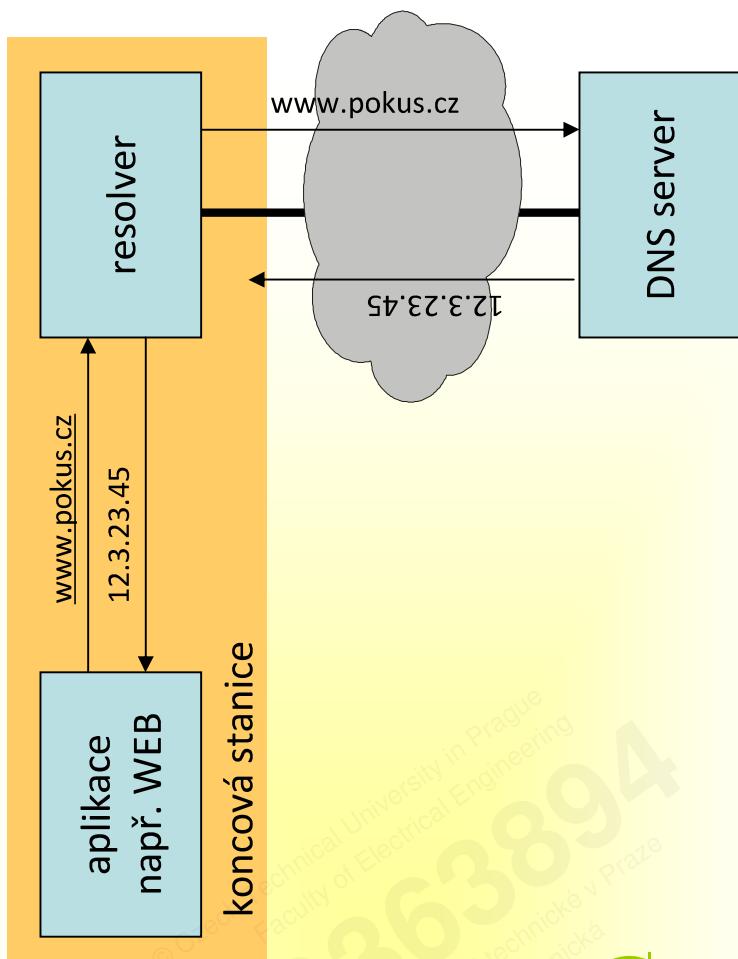
Organizační domény nejvyšší úrovně

com.	- komerční organizace
edu.	- vzdělávací organizace
gov.	- vládní instituce – USA
int.	- mezinárodní organizace
mil.	- U.S. vojenské instituce
net.	- síťové firmy, ISP, apod.
org.	- neziskové organizace



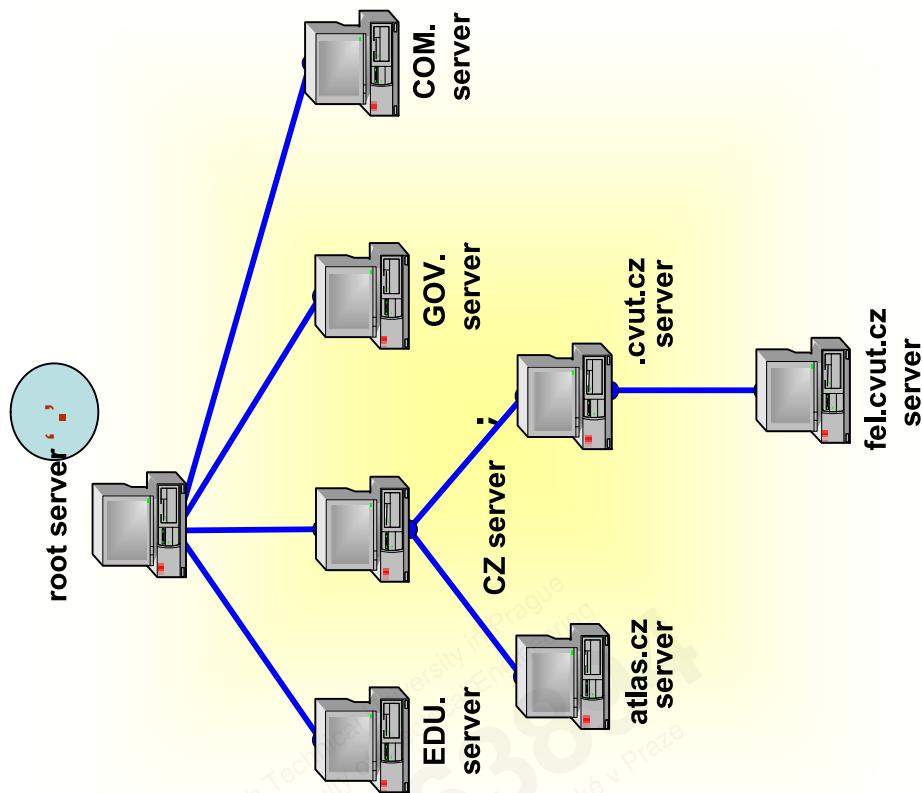
DNS klient a server

1. aplikáční program na straně koncové stanice přistupuje k DNS systému prostřednictvím DNS klienta, kterému se říká „**resolver**“ „resolver“ se spojí s DNS serverem a předá mu svůj dotaz
 2. DNS server vrátí zpět „**resolveru**“ odpověď
 3. DNS server vrátí zpět „**resolveru**“ odpověď
- **reverzní vyhledání (reverse lookup)**
je též možné ke známé IP adrese nalézt odpovídající jmenový DNS název, např. 12.3.23.45 => www.pokus.cz



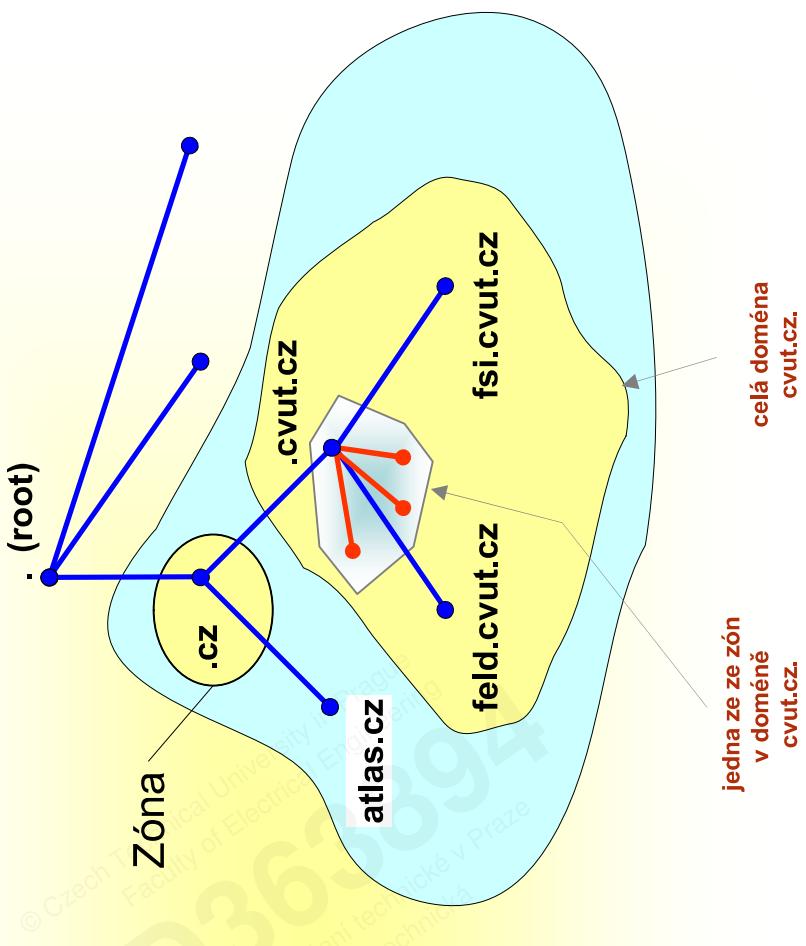
Hierarchie DNS serverů

- překlad hierarchické DNS adresy se realizuje systémem **hierarchicky svázaných zónám a DNS serverů**
 - každý DNS server je zodpovědný (**autoritativní**) za určitou část DNS prostoru které se říká **DNS zóna**
 - **zóna je část podstromu DNS**
 - DNS servery zodpovídají dotazy na koncové stanice nacházející se v jejich **zóně - autoritativní odpovědi**
 - pokud je dany server úschovného typu (**cache DNS server**), může odpovídat i na dotazy, pro něž nemá ve své databázi dané záznamy (není za ně odpovědný), které ale obdržel na základě vlastních dotazů od jiných DNS serverů kdysi v minulosti – **neautoritativní odpovědi**



DNS domény a zóny

- každá **zóna** je zakotvená ke **konkrétní doméně**, **nicméně zóna není to samé jako doména**
- **DNS doména je celou větví jmenného prostoru**
 - DNS zóna je jen částí DNS jmenného prostoru, jejíž data jsou uchovávány v **zónovém souboru na DNS serveru** (může obsahovat jen několik uzlů, záznamů dané domény)
 - administrátor DNS serveru zodpovědný za danou doménu (např. cvut.cz.) ji může rozdělit do částí - poddomén (např. field.cvut.cz., fsi.cvut.cz.) a **delegovat na jiné DNS servery jejich správu**; v tomto případě má každá nově delegovaná poddoména svoje vlastní DNS servery, které obsahují záznamy (všechny nebo jen některé) těchto poddomén, tyto servery mohou provádět delegování na další podpodomény, atd.



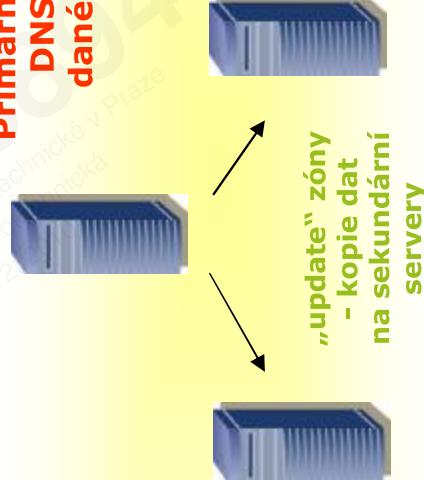
Primární a sekundární DNS servery

- pro každou DNS zónu musí existovat jeden **primární (MASTER)** a minimálně jeden **sekundární (SLAVE) DNS server**

– primární server udržuje soubor zóny, který obsahuje data o dané zóně. **Veškeré změny dat zóny se standardně provádějí na primárním serveru !!!**

- sekundární server si pravidelně kopíruje data zóny ze serveru primárního, pokud zde dojde k jejich změně
- sekundární servry se v **pravidelných intervalech** (dáno v SOA záznamu pro danou zónu na primárním serveru) připojují k primárnímu serveru a **zjišťují stav sériového čísla (serial number) dané zóny**, pokud je toto číslo větší než dřívější, znamená to, že se data na primárním serveru změnila a **je nutné provést přenos zóny** – přenos zóny se uskuteční **jen pokud je sériové číslo větší, než předchozí**
- další parametry potřebné pro sekundární server(y) jsou součástí **SOA DNS záznamu pro danou zónu na primárním serveru**
- **primární server může být nakonfigurován tak, že při změně dat zóny informuje sekundární servry automaticky o této skutečnosti – kopírování dat, ale i tak aktivují sekundární servry**

**Primární (MASTER)
DNS server
dané domény**



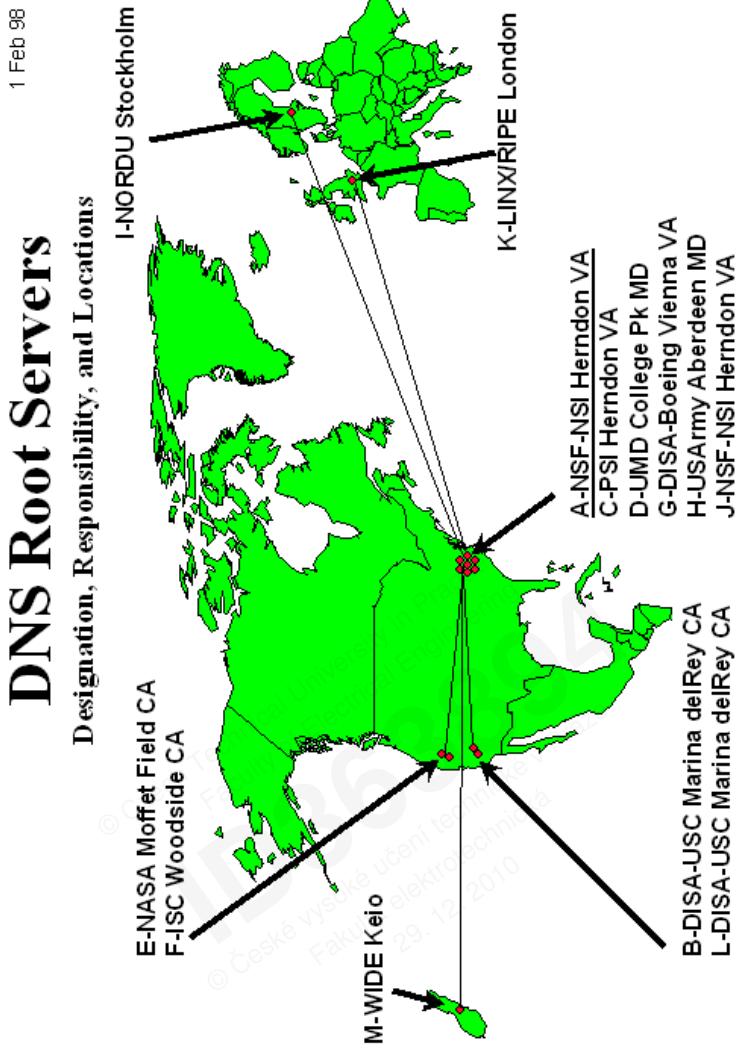
**Sekundární (SLAVE)
DNS server č.2**

„update“ zóny
- kopie dat
na sekundární
servery



Kmenové (Root) servery

- Kmenové DNS servery vědí jak nalézt autoritativní jmenné servery pro všechny nejvyšší TLD (top-level) zóny DNS systému
- existuje celosvětově 13 kmenových serverů (ve skutečnosti je jich ale mnohem více díky DNS anycastu)
- Kmenové servery jsou velice důležité pro funkci celého DNS systému v Internetu
- !!! Kmenové DNS servery jsou všechny delegačního typu, tj. sami o sobě nemají žádné primé odkazy na služby a zařízení !!! – obsahují jen NS a A (glue) záznamy (viz dále)



IP adresy kmenových serverů

A.ROOT-SERVERS.NET.	(formerly NS1.ISI.EDU)	198.41.0.4
B.ROOT-SERVERS.NET.	(formerly C.PSI.NET)	128.9.0.107
C.ROOT-SERVERS.NET.	(TERP.UMD.EDU)	192.33.4.12
D.ROOT-SERVERS.NET.	(NS.NASA.GOV)	128.8.10.90
E.ROOT-SERVERS.NET.	(NS.ISC.ORG)	192.203.23
F.ROOT-SERVERS.NET.	(NS.NIC.DDN.MIL)	192.5.5.241
G.ROOT-SERVERS.NET.	(AOS.ARL.ARMY.MIL)	192.112.36.4
H.ROOT-SERVERS.NET.	(NIC.NORDU.NET)	128.63.2.53
I.ROOT-SERVERS.NET.	(at NSI (InterNIC))	192.36.148.17
J.ROOT-SERVERS.NET.	(operated by RIPE NCC)	198.41.0.10
K.ROOT-SERVERS.NET.	(at ISI (IANA))	193.0.14.129
L.ROOT-SERVERS.NET.	(ICANN)	198.32.64
M.ROOT-SERVERS.NET.	(operated by WIDE, Japan)	202.12.27.33



Rekurzivní a iterativní DNS dotaz

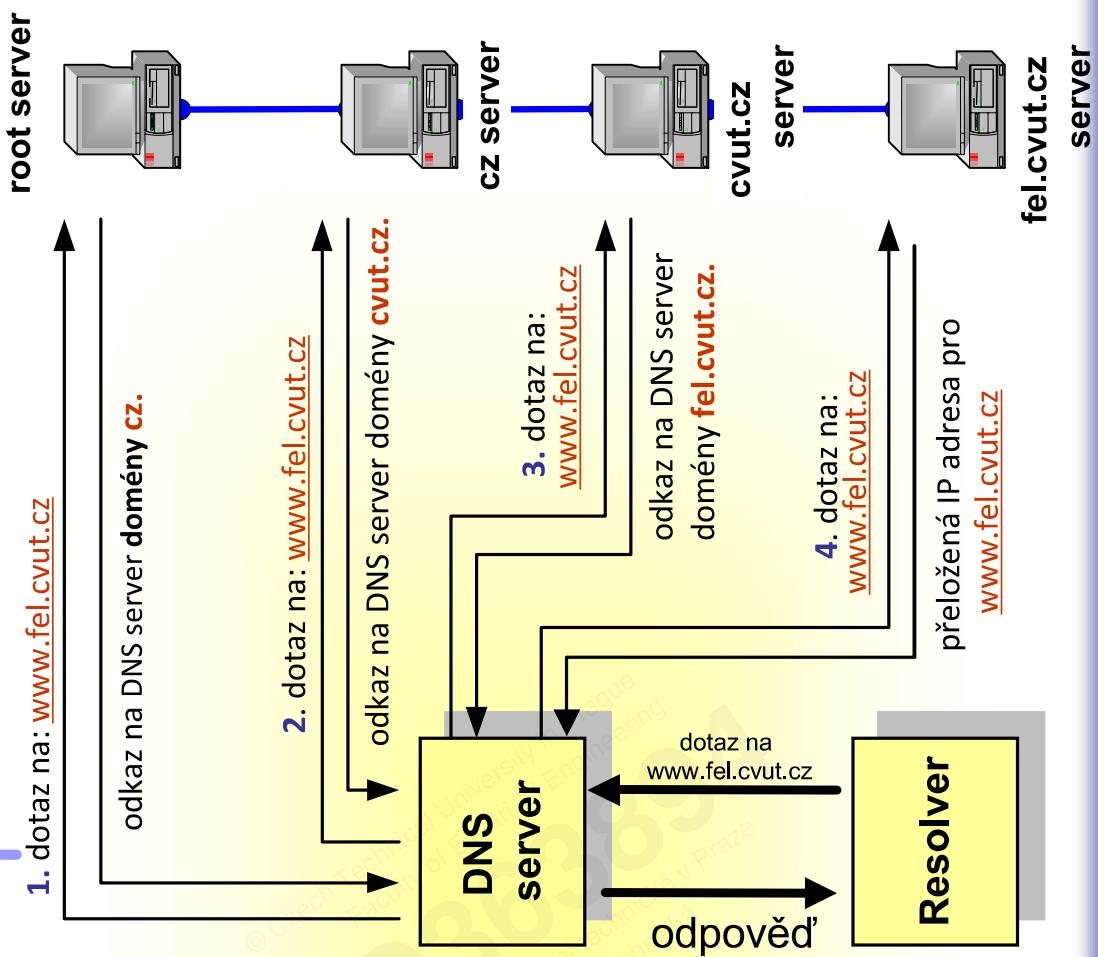
- existují dva typy dotazů v DNS:
 - rekurzivní dotazy !
 - iterativní (bez rekurze) dotazy !
- typ daného dotazu je určen !! jedním bitem ve zprávě DNS dotazu zasílaného DNS klientem !! – klientem může být i DNS server !!
- rekurzivní dotaz: když nemůže DNS server odpovědět přímo na daný dotaz (není pro daný dotaz autoritativní), provede sám další posloupnost dotazů na jiné DNS servery (pokud není již požadovaný překlad v místní výrovnávací paměti) - klientovi (resolveru) vrací výsledný „hotový“ překlad (pokud ale vůbec existuje)
- iterativní dotaz: když nemůže DNS server odpovědět přímo na daný dotaz, vrátí klientovi (resolveru) informace o DNS serveru(ech) o kterém se domnívá, že je schopen mu poskytnout další detaily k zodpovězení daného dotazu



Rekurzivní dotaz - příklad

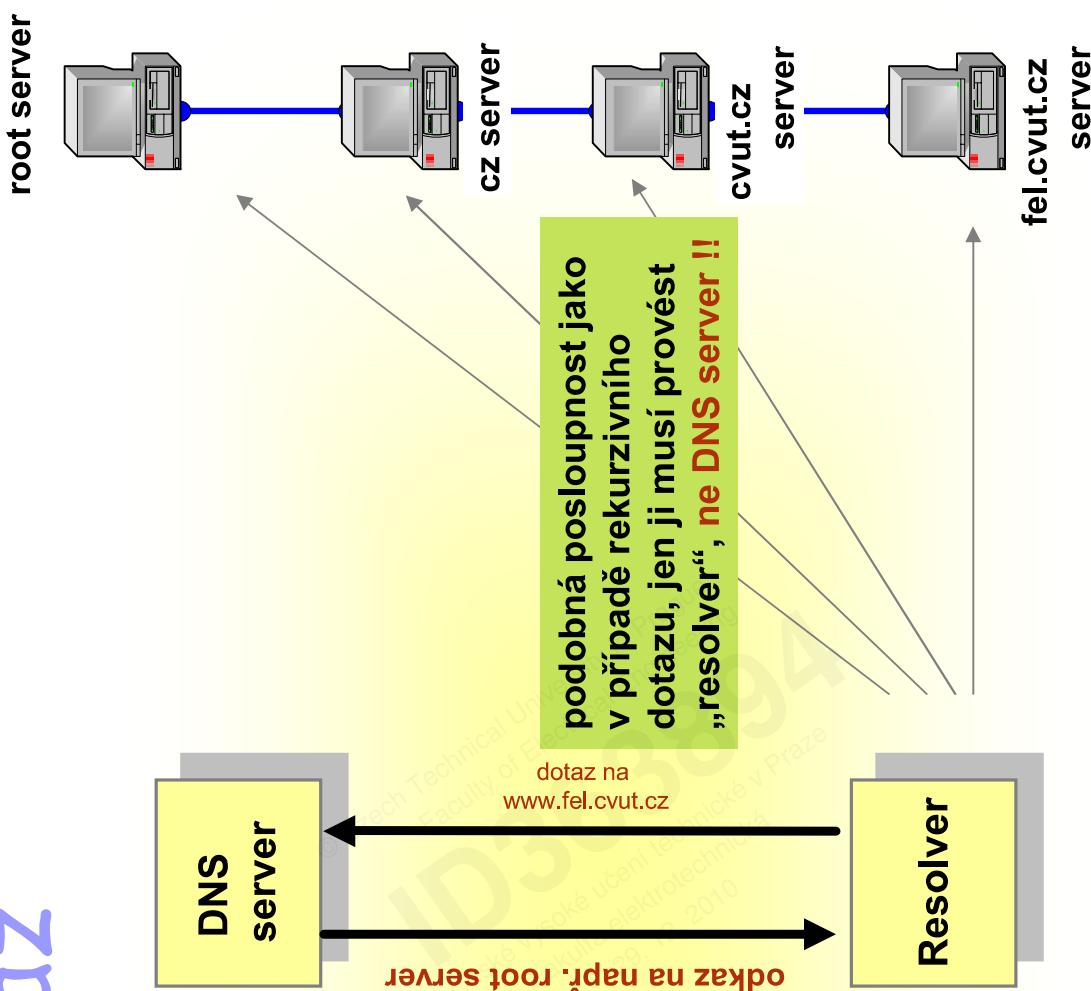
- u rekurzivního dotazu očekává „resolver“ úplné zodpovězení DNS dotazu

- pokud server není schopen provést sám překlad, pošle dotaz „blíže“ známému autoritativnímu DNS serveru (v nejhorším případě je nejbližší jeden kmenový server)
- kmenový server pošle zpět odkaz na DNS server TLD cz., ten potom na DNS server cvut.cz, atd.
- ve skutečnosti je dotaz mnohem kratší, protože jednotlivé informace jsou již ve využívací paměti (tzv. slangově jsou již *nakešované*)



Iterativní dotaz

- v tomto případě vrací DNS server, pokud není sám schopen dotaz zodpovědět přímo, referenci (referral) na nejbližší autoritativní server (např. na jeden kmenový server)
- výsledkem je více práce pro „resolver“, který zbytek překladu musí udělat sám



Dočasné ukládání – „caching“

- za účelem snížení DNS provozu si mohou ukládat DNS servery již zodpovězené dotazy do výrovnávací paměti slangově zvané „cache“ (keš)
- pokud požadovaný překlad související s daným dotazem je již v paměti, nekontakují se žádné jiné servery a dotaž se zodpoví tzv. z „keše“
- pozn.: pokud se použije odpověď uložená v „keši“, je označena jako „neautoritativní“ v DNS zprávě posílané zpět „resolveru“
- každý záznam může být v „keši“ jen předem definovanou dobu – TTL (Time-To-Live), tato doba je přenášena s každým záznamem a je definována na autoritativním serveru (primárním) pro daný záznam (nebo množinu záznamů společně)
- po uplynutí doby TTL pro daný záznam, musí být z „keš“ záZNAM vymazán
- **velké TTL, menší počet dotazů, ale problém s odezvou s častějšími aktualizacemi DNS**
- **malé TTL, možné rychlé aktualizace DNS na úkor většího provozu**



Soubor DNS zóny

příklad zónového souboru pro zónu „pokus.cz“

- data v DNS se nazývají **zdrojové záznamy (RR -resource records)**
- zdrojové záznamy jsou uloženy **v souborech zón na daném DNS serveru**

@ IN SOA pokus.cz. hostmaster.pokus.cz. (15 ; serial number	900 ; refresh	600 ; retry	86400 ; expire	3600) default TTL
NS	ns.pokus.cz.				
NS	ns2.trala.cz.				
NS	ppp.pokus.cz.				
A	2.2.2.2				
@					
@					
ppp					
ppp					
ethernet_r1					
ethernet_r2					
ns					
A	192.168.1.1				
A	192.168.2.1				
A	192.168.1.150				
A					
pc1	192.168.1.2				
pc2	192.168.2.2				
A					
serial_r1	192.168.3.1				
serial_r2	192.168.3.2				

- pokud není kterékoliv doménové jméno v DNS souboru zóny ukončeno znakem tečka („.“), je považováno za relativní a bude k němu implicitně z pravé strany dodáno jméno doménové přípona zóny, tak aby vzniklo absolutní doménové jméno (FQDN) končící vpravo tečkou např. jméno „ppp“ se transformuje pro zónu „pokus.cz“ na „ppp.pokus.cz.“ Všechny FQDN musí tedy končit vždy znakem tečky „.“



Soubor DNS zóny

příklad zónového souboru pro zónu „pokus.cz“

- v DNS se mohou vyskytnout různé typy zdrojových záznamů (někdy také záznamy prostředků - RR)
 - mezi nejčastější patří tyto záznamy – RR:
 - A – přiřazení IPv4 adresy k známému doménovému jménu zařízení (PC) nebo služby (WEB)
 - NS – definuje doménové jméno DNS serveru(ů), který je zodpovědný (autoritativní) za překlad jmen v dané poddoméně (delegace)
 - CNAME – definuje „alias“ k existujícímu FQDN jménu. K jednomu FQDN jménu může být přiřazeno i více „přezdivek“
 - MX – definuje cílový SMTP server pro danou doménu (nesmí být alias), musí být DNS jméno ne IP adresa
 - PTR – k IP adrese přiřazuje DNS jméno
 - SOA – detailní informace o dané zóně registrováno na 60 RR typů záznamů (<http://www.iana.org/assignments/dns-parameters>)

@ IN SOA ns.pokus.cz. hostmaster.pokus.cz. (15 ; serial number 900 ; refresh 600 ; retry 86400 ; expire 3600) ; default TTL	NS	ns.pokus.cz.
	NS	ns2.trala.cz.
	NS	ppp.pokus.cz.
	A	2.2.2.2
@ IN A ethernet_r1	A	192.168.1.1
	ethernet_r2	A
	ns	192.168.2.1
	pc1	192.168.1.150
	pc2	192.168.1.2
	serial_r1	192.168.2.2
	serial_r2	192.168.3.1
		192.168.3.2



Souboru zóny DNS

@	IN	SOA	ns.pokus.cz.	hostmaster.pokus.cz.	(15 ; serial number 900 ; refresh 600 ; retry 86400 ; expire 3600) ; default TTL	
@			NS	ns.pokus.cz.		
			NS	ns2.trida.cz.		
			NS	ppp.pokus.cz.		
			A	2.2.2.2		
					192.168.1.1	
					192.168.2.1	
					192.168.1.150	
					192.168.1.2	
					192.168.2.2	
					192.168.3.1	
					192.168.3.2	

zastupný symbol nahrazující řetězec „pokus.cz“
jméno zónové souboru nebo
argument \$ORIGIN=pokus.cz.

třída protokolů „IN“ = pro Internet , IP
adresace, všechny záznamy jsou stejné třídy,
není tedy třídu nutné opakovat u každého
záznamu zvlášť

Typ záznamu „Start Of Authority“, vyskytuje se
v zónovém souboru jen jednou
jméno serveru, na kterém je Master soubor
dané zóny (primární DNS)

email kontakt na administrátora dané zóny
hostmaster@pokus.cz



Souboru zóny DNS -sekundár

```
@ IN SOA ns.pokus.cz. hostmaster.pokus.cz. (  
    15 ; serial number  
    900 ; refresh  
    600 ; retry  
    86400 ; expire  
    3600 ); default TTL  
  
@ @ ppp ppp  
NS NS NS A  
    ns.pokus.cz.  
    ns2.trala.cz.  
    ppp.pokus.cz.  
    2.2.2.2  
  
    ethernet_r1 A  
    ethernet_r2 A  
    ns A  
    pc1 A  
    pc2 A  
    serial_r1 A  
    serial_r2 A
```

sériové číslo souboru; při každé změně údajů v souboru zóny se toto číslo musí zvětšit; vyjadřuje aktuálnost informací v dané zóně

po uplynutí dané „refresh“ doby se pokusí sekundární server spojit s primárním a zjistit, zda není zapotřebí aktualizovat data v dané zóně (údaj je v sekundách) změna seriového čísla udává, za jak dlouho se má ještě snažit sekundární server spojit s primárním, pokud první pokus o spojení selže

je časový interval, který udává jak dlouho maximálně může sekundární server držet kopie dat o dané zóně pokud se mu nepodaří spojit s primárním serverem (**MASTEREM**)

je to minimální hodnota TTL (Time To Live) RR (doba platnosti záznamu) pokud není u daného záznamu udaná přímo (tedy výchozí hodnota TTL pro RR záznamy v souboru zóny)



Lokální DNS cache – Windows

C:\>ipconfig /displaydns
Konfigurace IP systému Windows 2000
localhost.

Název záznamu	Typ záznamu	Hodnota	Délka dat	Sezka	(Hostiteľský) záznam
	localhost	1.0.0.1214	4	Answer	127.0.0.1

ns.seznam.cz.

Název záznamu	Typ záznamu	Hodnota	Délka dat	Sezka	(Hostiteľský) záznam
	localhost	15259	4	Answer	212.80.76.20

1.0.0.127.in-addr.arpa.

Název záznamu	Typ záznamu	Hodnota	Délka dat	Sezka	Záznam PTR
	localhost	12	4	Answer	

• lokálně uchované DNS převody místního „resolveru“ v OS systémech Windows lze zjistit zadáním příkazu **ipconfig /displaydns**

• smazání DNS cache lze provést příkazem **ipconfig /flushdns**



PDU DNS dotazu

Frame 5 (73 bytes on wire, 73 bytes captured)
Ethernet II, src: 00:02:3f:b6:37:fa, Dst: 00:0c:29:94:94:39
Internet Protocol, src Addr: 192.168.1.18 (192.168.1.18), Dst Addr: 192.168.1.150 (192.168.1.150)
User Datagram Protocol, src Port: 4440 (4440), dst Port: domain (53)
Source Port: 4440 (4440)
Destination port: domain (53)
Length: 39
Checksum: 0xd28a (correct)
Domain Name System (query)
Transaction ID: 0x6ed4
Flags: 0x0100 (standard query)
0... - Response: Message is a query
.000 0... - Opcode: Standard query (0)
... .0. - Truncated: Message is not truncated
....1 - Recursion desired: Do query recursively
.... .0... - Z: Reserved (0)
....0 - Non-authenticated data OK: Non-authenticated data is unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.seznam.cz: type A, class inet
Name: www.seznam.cz
Type: Host address
Class: inet

IP adresa DNS Serveru je

192.168.1.150

IP adresa DNS klienta je

192.168.1.18

dotaz je na A záznam

WWW.SEZNAME.CZ

DNS systém používá pro přenos svých PDU

UDP (klient a server)

nebo TCP (spojení mezi sekundárním a primárním serverem za účelem přenosu data dané zóny) na portu 53



PDU DNS odpovědi

```
Frame 6 (105 bytes on wire, 105 bytes captured)
Ethernet II, src: 00:0c:94:39, dst: 00:02:3f:b6:37:fa
Internet Protocol Version 4, Src Addr: 192.168.1.150 (192.168.1.150), Dst Addr: 192.168.1.18 (192.168.1.18)
User Datagram Protocol, Src Port: domain (53), Dst Port: 4440 (4440)
Source port: domain (53)
Destination port: 4440 (4440)
Length: 71
Checksum: 0xd0d9 (correct)

Domain Name System (Response)
Transaction ID: 0x0ed4
Flags: 0x8180 (Standard query response, No error)
    1... .... = Response: Message is a response
    .000 0... .... = Opcode: Standard query (0)
    .... 0... .... = Authoritative: Server is not an authority for domain
    .... 0. .... = Truncated: Message is not truncated
    .... 1.... = Recursion desired: Do query recursively
    .... 1... .... = Recursion available: Server can do recursive queries
    .... 0. .... = Z1: reserved (0)
    .... 0... .... = Z2: reserved (0)
    .... 0... .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... 0... .... = Reply code: No error (0)

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0

Queries
www.seznam.cz: Type A, class Inet
Name: www.seznam.cz
Type: Host address
Class: Inet

Answers
www.seznam.cz: type A, class Inet, addr 212.80.76.18
Name: www.seznam.cz
Type: Host address
Class: Inet
Time to live: 20 minutes, 34 seconds
Data length: 4
Addr: 212.80.76.18
www.seznam.cz: Type A, class Inet, addr 212.80.76.3
Name: www.seznam.cz
Type: Host address
Class: Inet
Time to live: 20 minutes, 34 seconds
Data length: 4
Addr: 212.80.76.3

IP adresa DNS Serveru je
192.168.1.150
IP adresa DNS klienta je
192.168.1.18
dotaz je na A záznam
WWW.SEZNAME.CZ
```



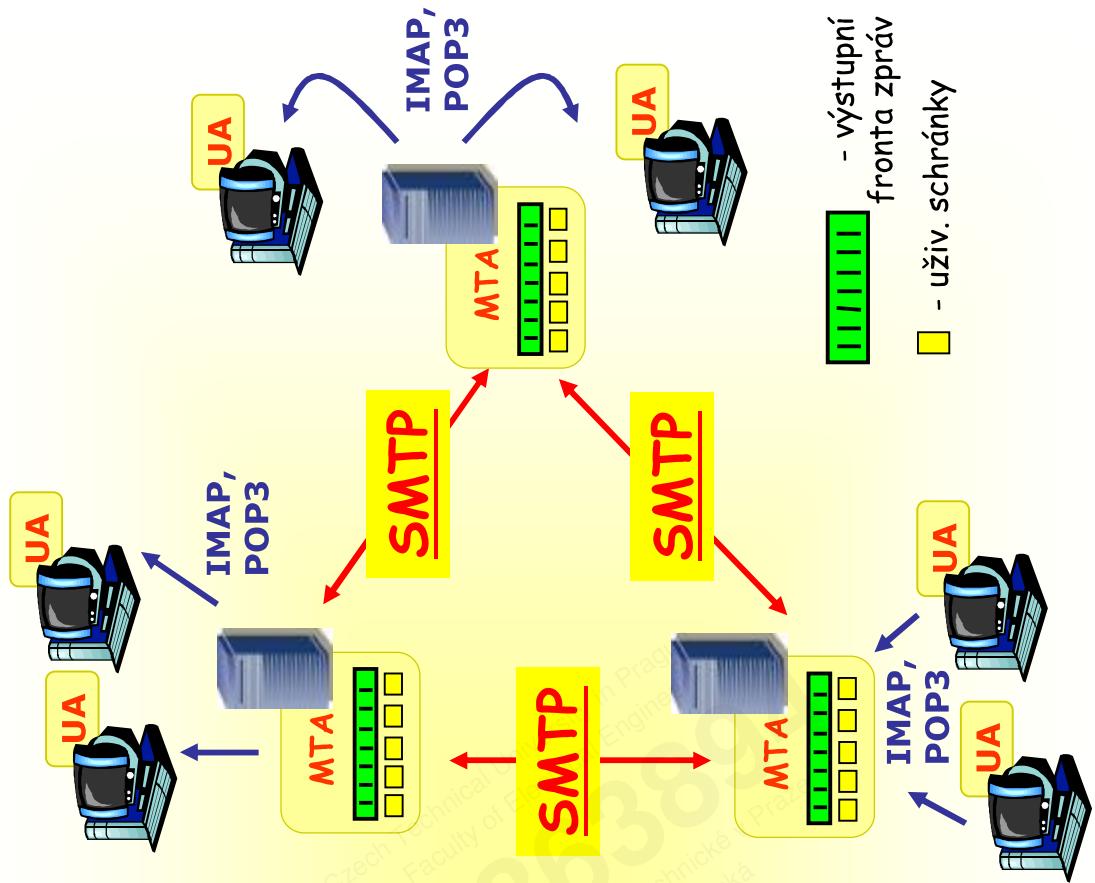
Elektronická pošta

Čtyři hlavní komponenty:

- uživatelský agent (UA) (nebo MUA)
- poštovní servery (MTA)
- protokol pro přenos zpráv SMTP
- protokoly pro stahování zpráv ze serveru na lokální počítač (např. POP3, IMAPv4)

Uživatelský klient

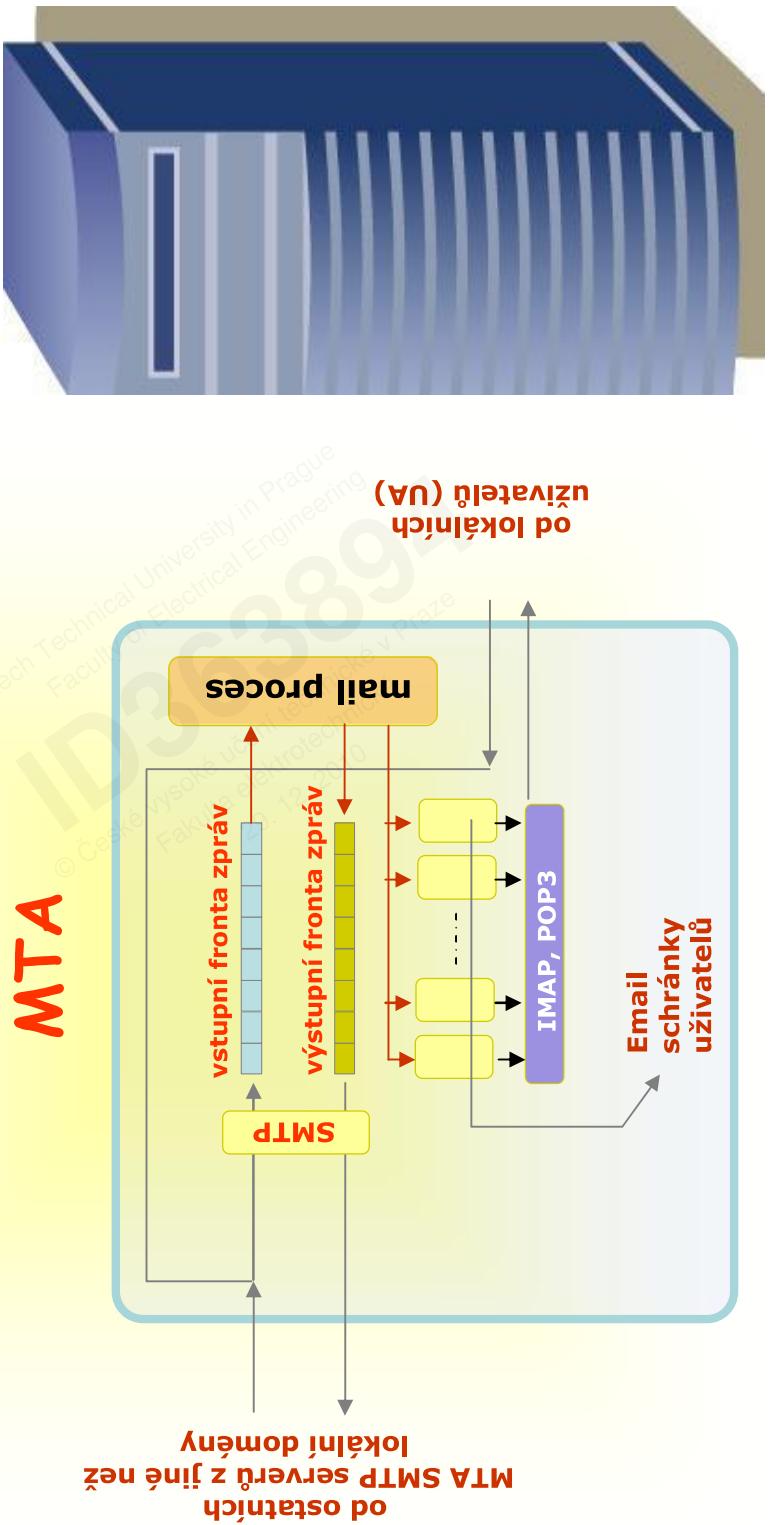
- aplikace určená ke čtení E-pošty
- slouží k vytváření, editaci, čtení a odesílání E-pošty (*Eudora, Outlook, elm, Netscape messenger, atd.*)



Poštovní servery

- schránka (mail box): obsahuje příchozí zprávy (ještě nepřečtené uživatelem)
- fronta zpráv (message queue): čekají zprávy na odeslání
- SMTP protokol mezi pošt. servery pro vzájemné
 - klient: posílá poštu
 - server: přijímá poštu

MTA



Elektronická pošta: SMTP [RFC 821]

- používá pro přenos **TCP transportní spojení** mezi klientem a serverem (server naslouchá typicky na **TCP portu 25**)
- **přímý přenos:** od zdrojové (**source**) serveru k cílovém (**destination**)
- tři fáze přenosu:
 - vzájemné představení (kdo je kdo)
 - zadání vnější obálky zprávy (kdo je odesílatel a komu je mail určený)
 - přenos vlastní zprávy (záhlaví, tělo, přílohy) – zde se opakuje odesíatel a příjemce – vnitřní obálka)
 - indikace konce zprávy
 - uzavření přenosu TCP spojení
- **způsob komunikace dotaz / odpověď**
 - příkaz(y): ASCII text
 - odpověď(i): stavový kód + fráze
- zprávy musí být kódovány v **7-bit ASCII** (původní specifikace SMTP bez podpory multimediálních zpráv - **MIME**)
- SMTP požaduje, aby všechny znaky zprávy (jak záhlaví, tak tělo zprávy) byly vyjádřeny v **7-bitovém ASCII formátu**
- **určité řetězce nejsou povolené ve zprávě** (e.g., <CRLF> . "<CRLF>" – kombinace ukončení zprávy) – zpráva se proto často kóduje, např. „**base-64**“



Příklad SMTP protokolu

..... klient sestaví spojení TCP na IP adresu SMTP serveru

Server: 220 pokus.cz
Klient: HELO (popř.EHLO) MY_PC_UA
Server: 250 Hello MY_PC_UA, pleased to meet you
Klient: MAIL FROM: <bohac@fel.cvut.cz>
Server: 250 bohac@fel.cvut.cz... Sender ok
Klient: RCPT TO: <bob@seznam.cz>
Server: 250 bob@seznam.cz... Recipient ok
Klient: DATA
Server: 354 Enter mail, end with ". " on a line by itself
Klient: From: bohac@fel.cvut.cz
Klient: To: bob@seznam.cz
Klient: Subject: Pokusny mail
Klient: Jak se mate?
Klient: .
Server: 250 Message accepted for delivery
Klient: QUIT
Server: 221 pokus.cz closing connection
..... server aktivně ukončí TCP spojení



Formát EMAIL zprávy

- formát Email je definován v dokumentu [RFC2822](#)
- Email zpráva je historicky textové (**ASCII**) orientovaná
- až později byla doplněna možností přenáset i „ne-ASCII“ orientovaný obsah (pomocí **MIME**)
- Email zpráva má řádkově orientovaný charakter, každá řádka je zakončena dvojznamenkou CRLF

Záhlaví

sledovací záhlaví (trace)
záhlaví odesílatele
záhlaví adresáta
záhlaví identifikace zprávy
volitelné záhlaví

<CRLF>

seznam MTA, kterými zpráva prošla

Return-path: ----
Received: ----

jaký(cí) je (jsou) odesílatel(é) email zprávy
From: <seznam email adres autorů zprávy>
Sender: <email toho, kdo fyzicky zprávu posílá>
(pokud je autor totožný s odesílatelem není nutné uvádět)
Reply-to: <email, kam má být poslána odpověď> – pokud není uveden, posílá se odpověď na všechny adresy uvedené v poli From:>

komu má být zpráva doručena

To: <seznam email adres adresátů>
Cc: <seznam emailů těch, jimž má být doručena kopie tohoto mailu>
Bcc: <seznam emailů těch, jimž má být doručena kopie tohoto mailu, bez toho, aniž by byly přímo uvedeny v mailu>

jednoznačný číselný identifikátor zprávy, definuje odesílatele

Message-ID: <číslo@mailer.domena.cz>

volitelná záhlaví upřesňují obsah dané zprávu

Subject: <ASCII subjekt>
Comments: <málo používaný>
Keywords: <málo používaný>

Tělo zprávy
(**ASCII** nebo
MIME formát)



Formát zprávy: multimedální rozšíření

- MIME: rozšíření zpráv, RFC 2045, 2005
- dodateční řádky v záhlaví zprávy deklarují MIME typ obsahu daného bloku

From: bohac@fel.cvut.cz
To: bob@seznam.cz
Subject: příklad
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

MIME verze
použitá metoda kódování dat
kódování dat
typ mediálních dat,
subtyp
deklarace parametrů
zakódovaná data

base64 zakódovaná data obrázku . . .
.
.base64 zakódovaná data obrázku



MIME typy

Content-Type: type/subtype; parameters

text

- příklady podtypů: plain,
html

obrázek (image)

- příklad podtypu: jpeg, gif

audio

- příklad podtypu: basic (8-bit µ-Law kódování),
32kpcm (32 kbit/s ADPCM kódování)

video

- příklad podtypu: mpeg,
quicktime
- aplikace
 - jiné typy dat, které musí být zpracovány nejprve danou aplikací, aby byly "viditelné"
- příklady podtypů: msword,
octet-stream



Zpráva s několika částmi - MIME

From: Jiri Vodrazka <vodrazka@fel.cvut.cz>
To: bohac@fel.cvut.cz
Subject:=?iso-8859-2?b?UPHleDo?= Re: skoleni
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="MOQ111597437388da9d7349fb8116a67108de0ce80259"
This message is in MIME format.

—MOQ111597437388da9d7349fb8116a67108de0ce80259
Content-Type: text/plain; charset=ISO-8859-2
Content-Transfer-Encoding: 8bit

Přeposlaná zpráva od TIA Praha <tiapraha@tiapraha.cz>

Datum: Fri, 13 May 2005 10:08:39 +0200
Od: TIA Praha <viplerova@tiapraha.cz>
Odpověď-komu: TIA Praha <viplerova@tiapraha.cz>
Předmět: Re: prosba
Komu: Jiri Vodrazka <vodrazka@fel.cvut.cz>

Děkuji Vám za odpověď,
v pondělí to bude stačit. Ráno se domluvíme kdy bych mohla za Vámi přijít.

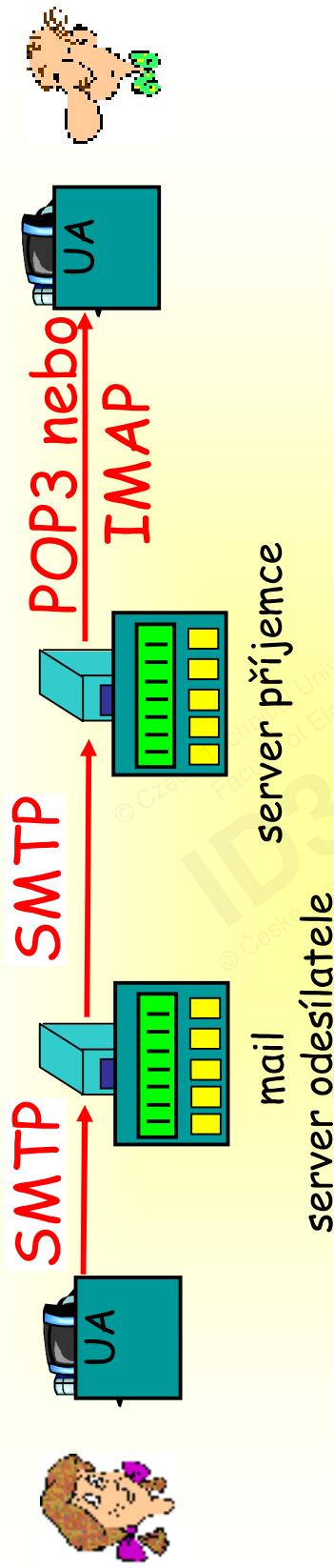
Mějte se moc hezký a příjemný víkend.
Viplerová

—MOQ111597437388da9d7349fb8116a67108de0ce80259
Content-Type: application/vnd.ms-excel; name="=?iso-8859-2?Q?Prezenen=ED_listina_19-20.5.xls?="
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="=?iso-8859-2?Q?Prezench=ED_listina_19-20.5.xls?="

ASDasdASDasdaSD



Protokoly pro přístup ke schránce



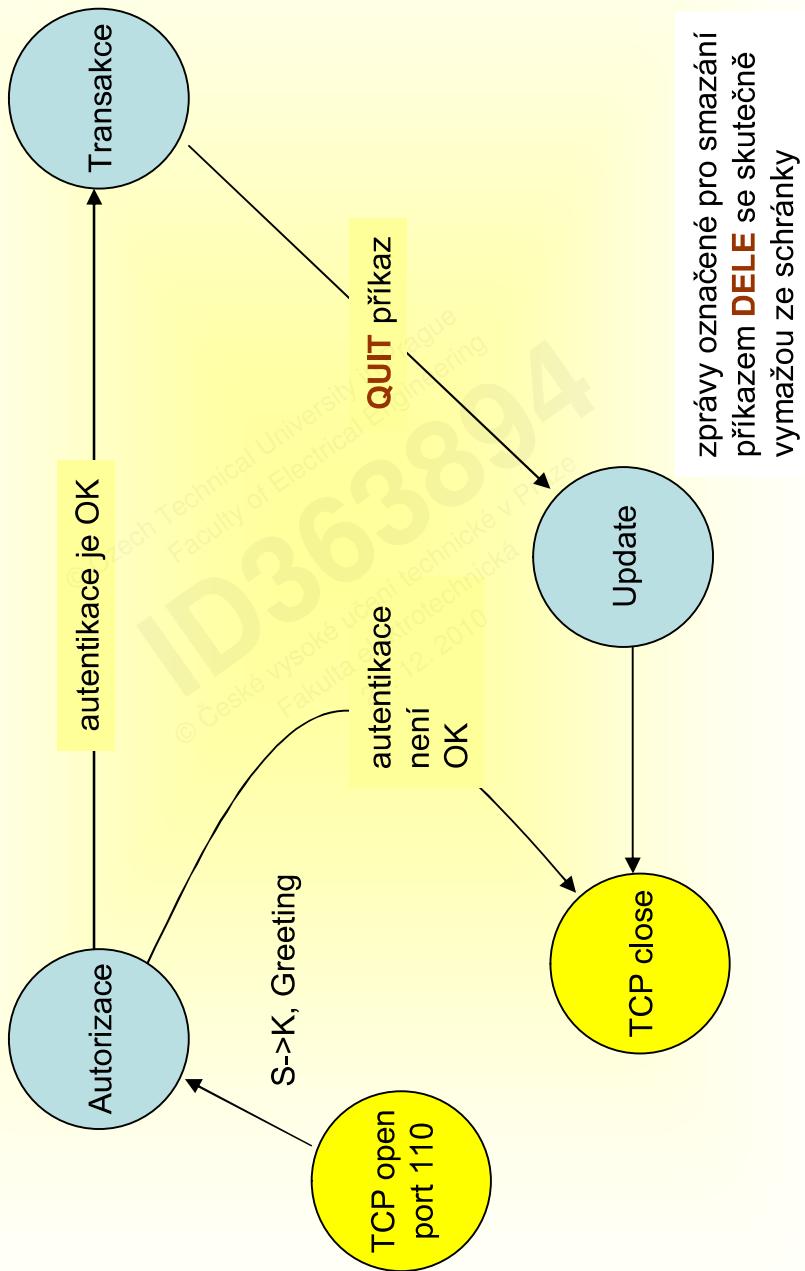
- SMTP: zajišťuje doručení email zpráv k cílovému Email serveru příjemce
- protokoly přístupu k mailu: stažení email zpráv ze serveru, případně **manipulace s nimi, vyhledávání a třídící funkce, apod.**

- **POP**: „Post Office Protocol“ - [RFC 1939]
 - autorizace (agent<-->server) s stažením k UA
- **IMAP**: „Internet Mail Access Protocol“ - [RFC 1730]
 - více funkcí (více komplexnější)
 - manipulace s uloženými zprávami na serveru
- **HTTP**: Hotmail , Yahoo! – přístup k mailu přes WEB

POP3 protokolové stavy

K->S, user <uživ.jméno>
K->S, pass <heslo>

LIST, RETR, DELE, atd.



POP3 příkazy – klíčová slova

STAT – jako odpověď vrací počet zpráv ve schránce a jejich celkovou velikost v bajtech
(např. +OK 2 320)

QUIT - tímto příkazem se přechází z transakčního stavu do stavu UPDATE

LIST – tento příkaz vrací víceřádkovou odpověď, na každém řádku je ID zprávy ve schránce a její velikost

RETR (ID) – tímto příkazem pošle v obráceném směru POP3 server klientovi danou email zprávu, jejíž ID je součástí argumentu (např. RETR 1, stáhne zprávu s ID č. 1.)

DELETE (ID) – tento příkaz označí zprávu s ID jako smazanou, ale daná zpráva se ještě nevymaže – to se provede až ve stavu UPDATE; v příkazu STAT či LIST se však již daná zpráva nezobrazí

NOOP – prázdná operace, server jen odpoví +OK zprávou klientovi

RSET (ID) – umožňuje zpětně „označit“ zprávu s daným ID jako nesmazanou, opak DELET
TOP (ID) n – „optional“ – z dané zprávy přenesou jen záhlaví a n bajtů z vlastního těla zprávy

UIDL – „optional“ ke každé dané zprávě vypíše jednoznačný její identifikátor (každá zpráva jedna řádka)

USER – používá se pro autentikaci uživatele

PASS – používá se pro autentikaci uživatele

APOP username MD5Hash – „optional“ místo jména a hesla se předává username a za ním výsledek MD5 hash funkce nad řetězem timestamp+heslo uživatele (timestamp vrací POP3 server jako součást prvního výpisu při připojení – „greeting“)



POP3 protokol

autorizační fáze —————

• příkazy klienta:

- **user**: „bob“
- **pass**: „password“
- odpovědi

— +OK

— -ERR

fáze transakce, klient:

- **list**: vypíše číselný seznam zpráv
- **retr**: stažení dané zprávy podle jejího čísla
- **delete**: smazání dané zprávy na serveru
- **quit**: ukončení

S: +OK POP3 server ready
C: user pokus

S: +OK

C: pass pokus

S: +OK user successfully logged on

C: list

S: 1 498

S: 2 912

S: .

C: retr 1

S: <message 1 contents>

S: .

C: dele 1

C: retr 2

S: <message 1 contents>

S: .

C: dele 2

C: quit

S: +OK POP3 server signing off



POP3 protokol – příklad spojení

- C:\Documents and Settings\bohac>telnet
192.168.1.150 110
 - ----- **Otevření TCP spojení s POP3 serverem**
 - +OK <980.64579593@lab.cz> ready for action (Mailtraq 2.6.3.1750/POP3)
 - **user pokus**
 - +OK verification deferred, password please
 - **pass pokus**
 - +OK verified, you have 1 message(s)
 - **list**
 - +OK 1 messages (805 octets)
1 805 LBCZ18350089
 - **delete 1**
 - +OK message marked for deletion
 - **list**
 - +OK 0 messages (805 octets)
 - **quit**
 - +OK closing connection, have a nice day
 - ----- **Uzavření spojení s POP3 serverem** -----
 - ----- **Connection to host lost.**
- C:\Documents and Settings\bohac>
- Message-ID:
<000d01c55941\$e804eb70\$0201a8c0@acer1>From:
"LEOS" <leos@lab.cz>
To: <pokus@lab.cz>
Subject:
Date: Sun, 15 May 2005 13:33:23 +0200



IMAP

- protokol je dnes nově definován v **RFC 3501**
- dokonalejším nástupcem POP3 protokolu
- pracuje opět na principu příkaz(dotaz)/odpověď'
- systém postaven na principu komunikace klient/server
- pro přenos používá TCP protokol (port 143)
- ke schránce může být klient připojen současně několika UA (u POP3 to nelze)
- zavádí možnost více záložek (folder) pro jednoho uživatele
- umožňuje podstatně větší možnosti s manipulací zpráv ve schránkám a vzájemné mezi nimi
- **primárně jsou všechny zprávy na IMAP serveru a uživatel jen s nimi manipuluje (přemisťuje, maže, kopíruje mezi záložkami) – lze je samozřejmě stáhnout i lokálně**
- IMAP umožňuje data ve schránkách vyhledávat podle různých kritérii
 - data je možné stahovat jen po částech (třeba jen záhlaví) a ne celá (nevýhoda POP)
 - došlé zprávy lze automaticky zařazovat do konkrétních schránek podle různých kritérií



IMAP - příklad komunikace

```
C:\WINNT\system32\cmd.exe
* OK lab.cz IMAP4rev1 Mailtraq <2.6.3.1750> ready
1 Login pokus pokus
1 OK LOGIN completed for pokus
list *
list NO * unsupported/unrecognised command
2 list *
* LIST <\Noselect> "/" ""
2 OK LIST completed
3 list 1
* LIST <\Noselect> "/" ""
3 OK LIST completed
4 list ""
* LIST >>> "INBOX"
* LIST >>> "Sent Items"
* LIST >>> "Drafts"
* LIST >>> "Trash"
* LIST >>> "Junk Mail"
* LIST >>> "Koncepty"
* LIST >>> "Odeslan&amp;OE- po&amp;ME-ta"
4 OK LIST completed
6 list 8
```



Literatura

- [1] Boháč, L. *Přednáška č. 2 – Aplikační protokoly DNS, HTTP, SMTP.* [cit. 2010-11-22]
Dostupné z: <<https://www.comtel.cz/files/download.php?id=4549>>
- [2] Boháč, L. *Přednáška č. 3 – Elektronická pošta a její protokoly SMTP, POP3 a IMAP.* [cit. 2010-11-22] Dostupné z: <<https://www.comtel.cz/files/download.php?id=4560>>

© Czech Technical University in Prague
Faculty of Electrical Engineering
© České vysoké učení technické v Praze
Fakulta elektrotechnická
29. 12. 2010

ID3638

Dotazy



Právní doložka (licence) k tomuto Dílu (elektronický materiál)

České vysoké učení technické v Praze (dále jen ČVUT) je ve smyslu autorského zákona vykonavatelem majetkových práv k Dílu či držitelem licence k užití Díla. Užívat Dílo smí pouze student nebo zaměstnanec ČVUT (dále jen Uživatel), a to za podmínek dále uvedených.

ČVUT poskytuje podle autorského zákona, v platném znění, oprávnění k užití tohoto Díla pouze Uživateli a pouze ke studijním nebo pedagogickým účelům na ČVUT. Toto Dílo ani jeho část nesmí být dále šířena (elektronicky, tiskově, vizuálně, audiem a jiným způsobem), rozmnožována (elektronicky, tiskově, vizuálně, audiem a jiným způsobem), využívána na školení, a to ani jako doplňkový materiál. Dílo nebo jeho část nesmí být bez souhlasu ČVUT využívána ke komerčním účelům. Uživateli je povoleno ponechat si Dílo i po skončení studia či pedagogické činnosti na ČVUT, výhradně pro vlastní osobní potřebu. Tím není dotčeno právo zákazu výše zmíněného užití Díla bez souhlasu ČVUT. Současně není dovoleno jakýmkoliv způsobem manipulovat s obsahem materiálu, zejména měnit jeho obsah včetně elektronických popisných dat, odstraňovat nebo měnit zabezpečení včetně vodoznaku a odstraňovat nebo měnit tyto licenční podmínky.

V případě, že Uživatel nebo jiná osoba, která drží toto Dílo (Držitel díla), nesouhlasí s touto licencí, nebo je touto licencí vyloučena z užití Díla, je jeho povinností zdržet se užívání Díla a je povinen toto Dílo trvale odstranit včetně veškerých kopií (elektronické, tiskové, vizuální, audio a zhotovených jiným způsobem) z elektronického zařízení a všech záznamových zařízení, na které jej Držitel díla umístil.