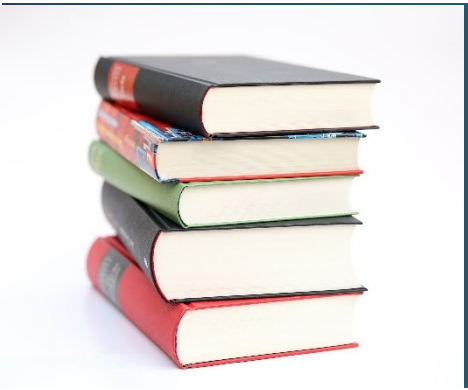
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

PIKS, prednáška 10
Aplikačná vrstva

Introduction to Networks v6.0

Katedra informačných sietí
Fakulta riadenia a informatiky, UNIZA

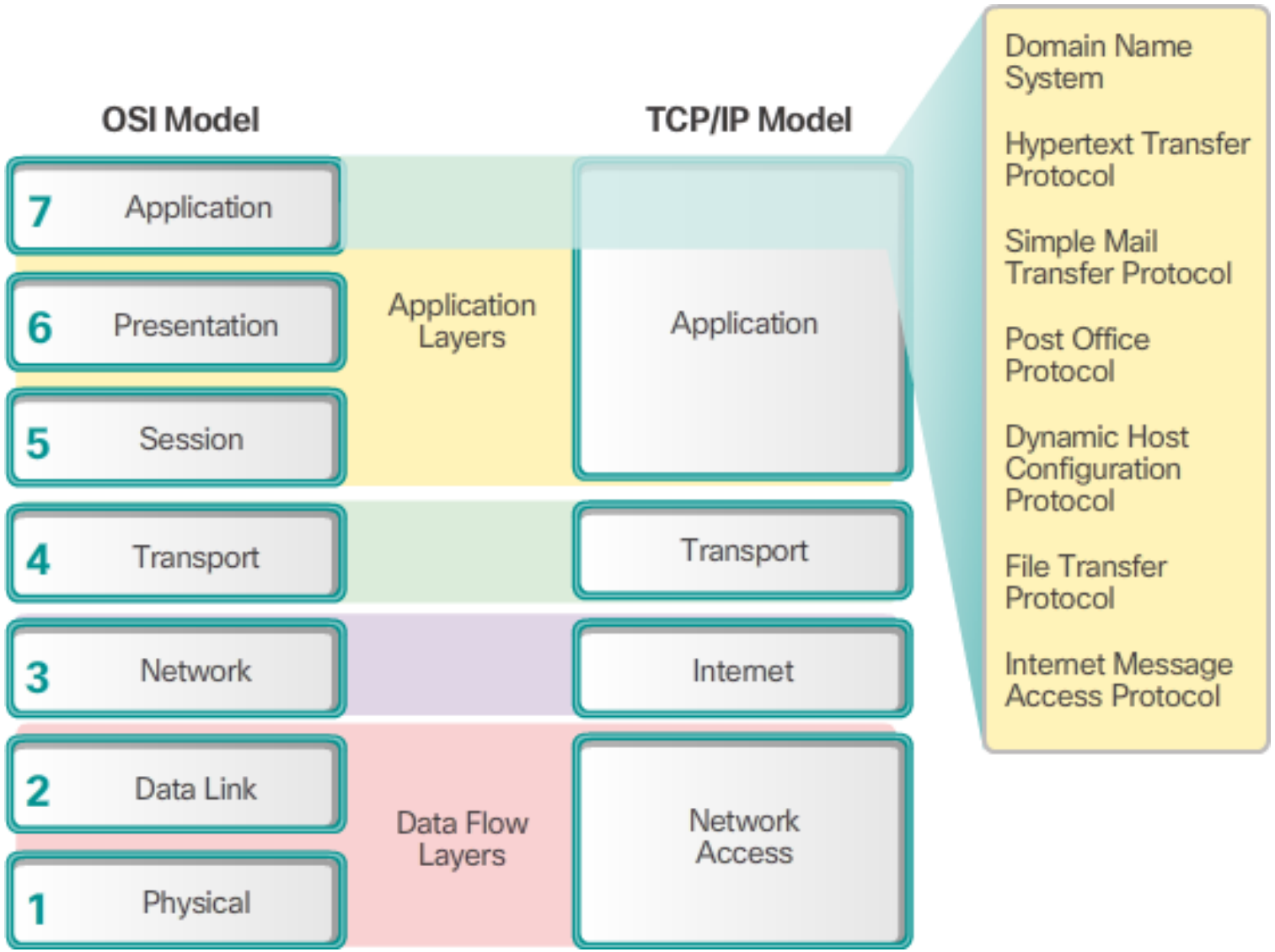
KIS FRI UNIZA – Vytvorené v rámci projektu KEGA 011STU - 4/2017.



Čo nás čaká

- Client-Server / Peer-to-Peer model
- HTTP(S)
- SMTP, POP, IMAP
- DNS
- DHCP
- FTP
- SMB
- Telnet / SSH
- SNMP

Aplikačná vrstva



Aplikačná vrstva

- Softvér pracujúci na aplikačnej vrstve môže byť dvojaký
- **Sieťové aplikácie** (Network-Aware Applications)
  - Používateľské aplikácie, s ktorými priamo pracuje používateľ
  - Webové a poštové programy, instant messaging nástroje, softvérové IP telefóny, peer-to-peer programy, ...
- **Sieťové aplikačné služby** (Application Layer Services)
  - Aplikácie, ktoré neovláda priamo používateľ, ale obvykle bežia na pozadí v operačnom systéme a poskytujú isté sieťové služby
  - Servery jednotlivých sieťových služieb, prípadne aj iné procesy bežiace v operačnom systéme, ktoré prevezmú dáta bezprostredne z aplikácie a starajú sa o ich prenos sieťou

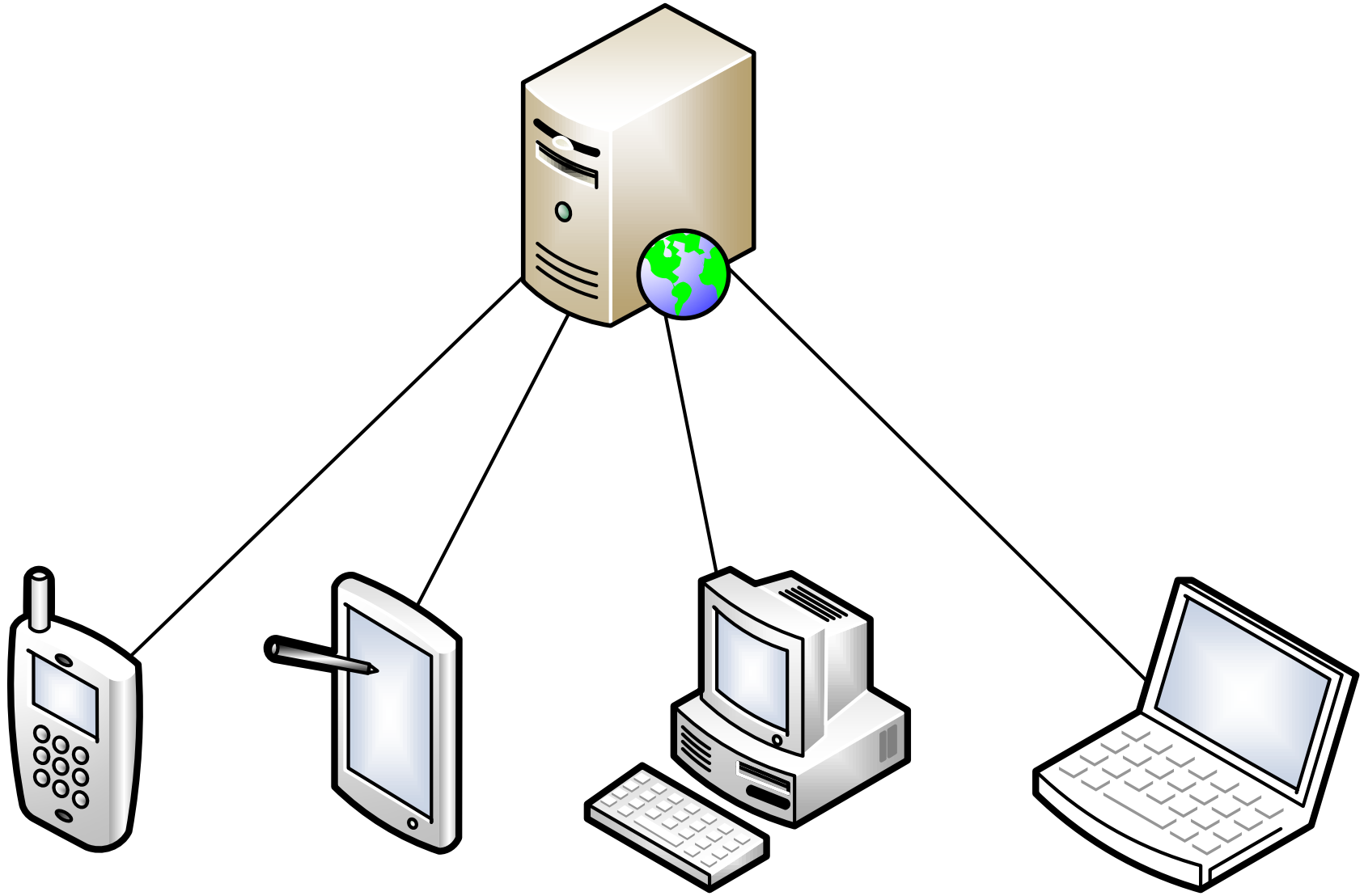
Protokoly aplikačnej vrstvy

- Aplikačné protokoly v TCP/IP sú veľmi početné
- Takmer pre každú službu používame samostatný protokol
- My sa dnes pozrieme na niektoré najbežnejšie protokoly
- Väčšina aplikačných protokolov TCP/IP je popísaná vo voľne dostupných dokumentoch s názvom Request for Comment (RFC), ktoré vytvára inštitút Internet Engineering Task Force (IETF)
  - RFC dokumentov môže byť niekoľko k jednému protokolu
  - DNS – 51 RFC (podľa wikipédie)
  - HTTP – 7 RFC
  - POP3 – 11 RFC
  - SMTP – 42 RFC

Client-Server model

- Klient je softvér, ktorý je **konzumentom** istej služby (WWW browser, poštový používateľský program, Telnet/SSH klient, FTP klient, ...)
- Server je softvér, ktorý je **producentom** istej služby (WWW server, poštový server, Telnet/SSH/FTP server, ...)
- V architektúre klient/server je poskytovanie služby centralizované
- Niektoré protokoly pracujúce na báze Client-Server
  - HTTP
  - DNS
  - DHCP
  - FTP
  - SSH
  - VNC
  - NTP

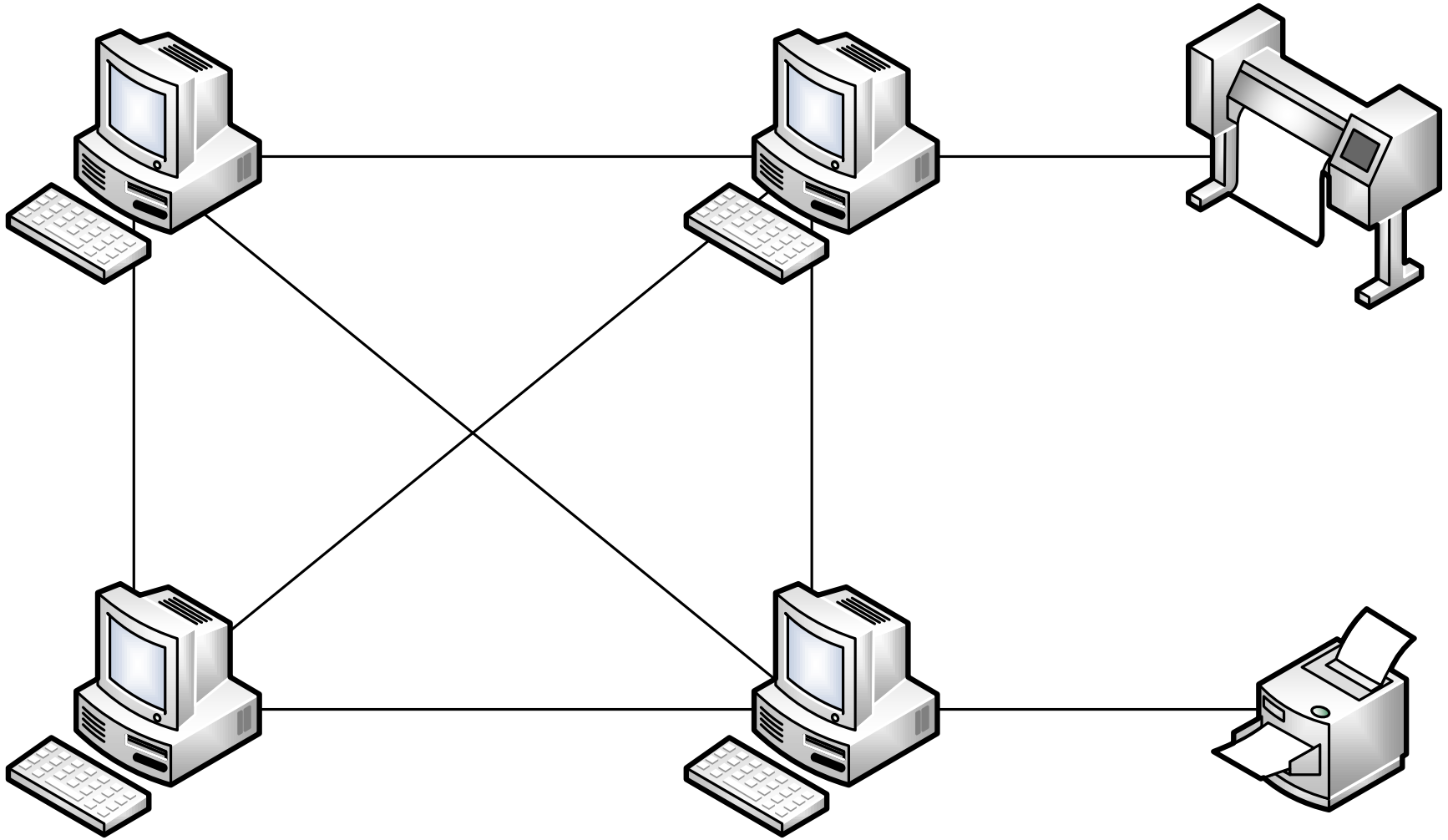
Client-Server model



Peer-to-Peer model

- Ten istý softvér je súčasne konzumentom i producentom tej istej služby, dokáže ju teda poskytnúť iným i sám využiť od iných
  - Môžeme povedať, že peer-to-peer softvér je súčasne klient i server
- Niekedy sa rozlišujú peer-to-peer siete a aplikácie
  - P2P aplikácia v sebe združuje klienta i server
  - P2P sieť je sieť, v ktorej jednotlivé uzly slúžia súčasne ako klienti i servery bez centrálneho riadiaceho prvku
- Niektoré protokoly pracujúce na báze Peer-to-Peer
  - BitTorrent
  - Bitcoin
  - Gnutella

Peer-to-Peer model



HyperText Transfer Protocol

- Protokol HTTP je dnes jedným z najpoužívanejších protokolov, vďaka ktorému existuje služba WWW a služby od nej odvodené
- HTTP umožňuje WWW klientovi
  - Adresovať vzdialený súbor
  - Požiadať server o jeho zaslanie
    - Ak sa jedná o skript (napr. PHP), klient žiada, aby mu server poslal výstup behu tohto skriptu, nie skript samotný
  - Požiadať server o prepísanie tohto súboru
- HTTP používa formát adries v tvare
  http://www.server.sk/cesta/súbor.html
  - „**http**“ – tzv. schéma, ktorá určuje použitý aplikačný protokol
  - „**www.server.sk**“ – meno servera
  - „**/cesta/súbor.html**“ – poloha požadovaného dokumentu na serveri

HyperText Transfer Protocol

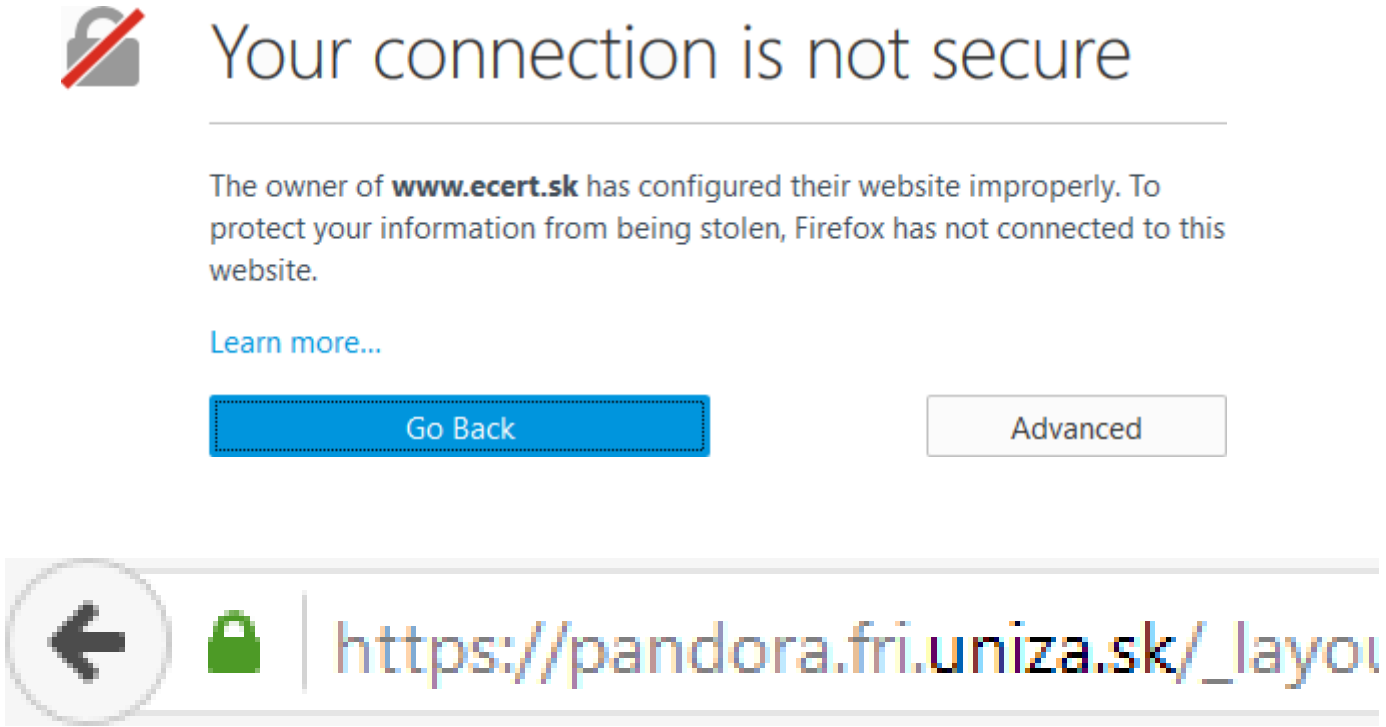
- HTTP je textový protokol, jeho príkazy sú čitateľné slová
  - HTTP nie je zabezpečený, jeho šifrovaná podoba sa volá HTTPS
- HTTP má tri základné príkazy (nazývajú sa aj metódy)
  - **GET** – žiadosť o prenos dokumentu zo servera ku klientovi
  - **POST** – žiadosť o prevzatie formulárových dát od klienta a zaslanie výsledku ich spracovania opäť klientovi
  - **PUT** – žiadosť o prenos dokumentu z klienta na server
- Odpovede servera sú identifikované číslom
  - **1xx** – spracovanie žiadosti stále prebieha
  - **2xx** – žiadosť bola spracovaná úspešne
  - **3xx** – presmerovanie, klient musí požiadať o ďalší dokument
  - **4xx** – chyba na strane klienta
  - **5xx** – chyba na strane servera

HyperText Transfer Protocol

```
GET /index.php HTTP/1.1
Host: www.kis.fri.uniza.sk
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: sk,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: __utma=82150209.352919406.1454688143.1457507625.1457518093.30; __utmz=82150209.1456150426.19.2.utmcsr=google|utmccn
__utma=55141169.1270089295.1454935745.1457598370.1457623742.11; __utmz=55141169.1454935745.1.1.utmcsr=(direct)|utmccn=(dire
__utmc=82150209; 15efd531982ff48748ecae81604c4a73=762e9e8c0582b3f16b49181ce0a58283; jfcookie[lang]=sk; __utmc=55141169; __u
Connection: keep-alive

HTTP/1.1 200 OK
Date: Thu, 10 Mar 2016 15:55:11 GMT
Server: Apache/2.2.16
Set-Cookie: lang=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/
Set-Cookie: jfcookie=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/
Set-Cookie: jfcookie[lang]=sk; expires=Fri, 11-Mar-2016 15:55:11 GMT; path=/
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Cache-Control: no-cache
Pragma: no-cache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
```

HyperText Transfer Protocol Secure

- HTTP + SSL (TLS)
- Šifrované spojenie na úrovni 4-tej vrstvy ISO OSI
- Dôveryhodnosť na základe certifikátu servera



HyperText Transfer Protocol Secure

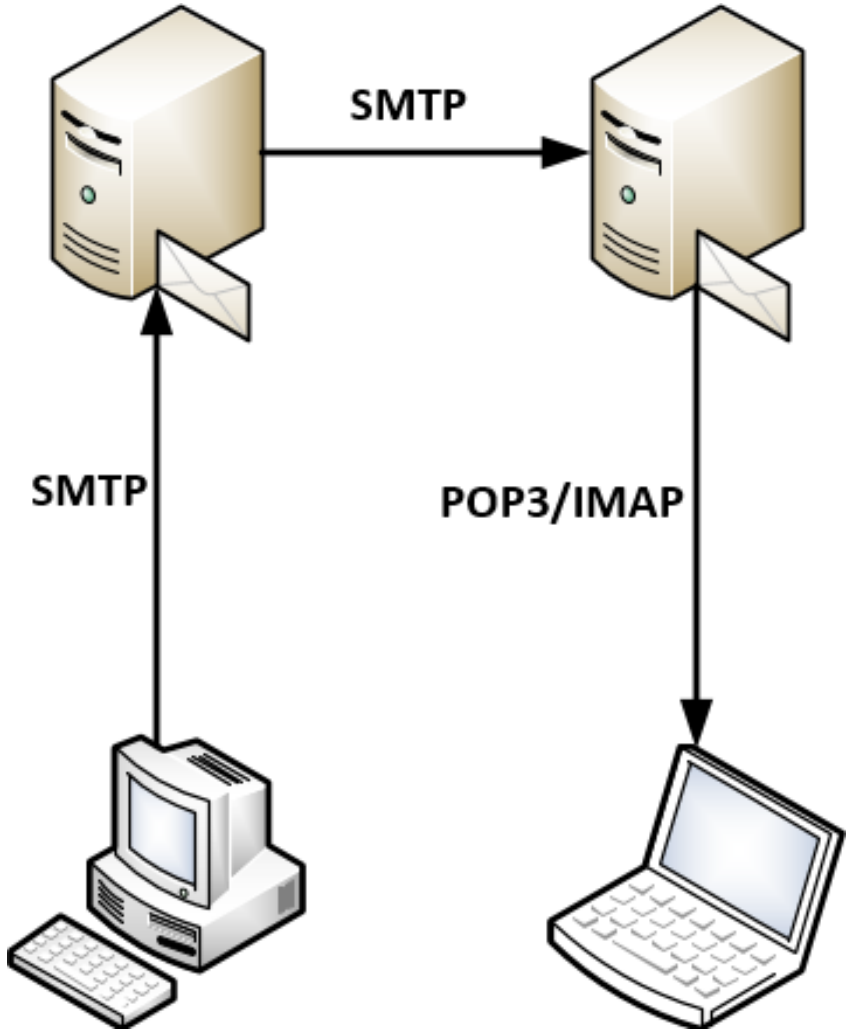
```
.................QU...Kb.k..u.=...]
...br......+./.
.          .....3.9./.5.
...z.........pandora.fri.uniza.sk......
.................#..3t.........h2.spdy/3.1.http/1.1..........
..............................M..V..6[._..g@.......
.o%2.O.....^. Z:...........K..6}.....l."....e..............r..o..l0..h0..P......
..O.....,:0
.          *.H..
.....0.1.0
..U....E-Cert0..
141203093734Z.
161202093734Z0r1.0...U.
....ilinsk.. univerzita110/..U...(FRI,Centrum informa..n..ch technol..gi..1.0...U....pandora.fri.uniza.sk0.."0
.          *.H..
..........0..
```

HTTP vs HTTPS

	HTTP	HTTPS
Šifrovanie	Nie	Áno
URL	http://	https://
L4 protokol	TCP	TLS
L4 port	80	443

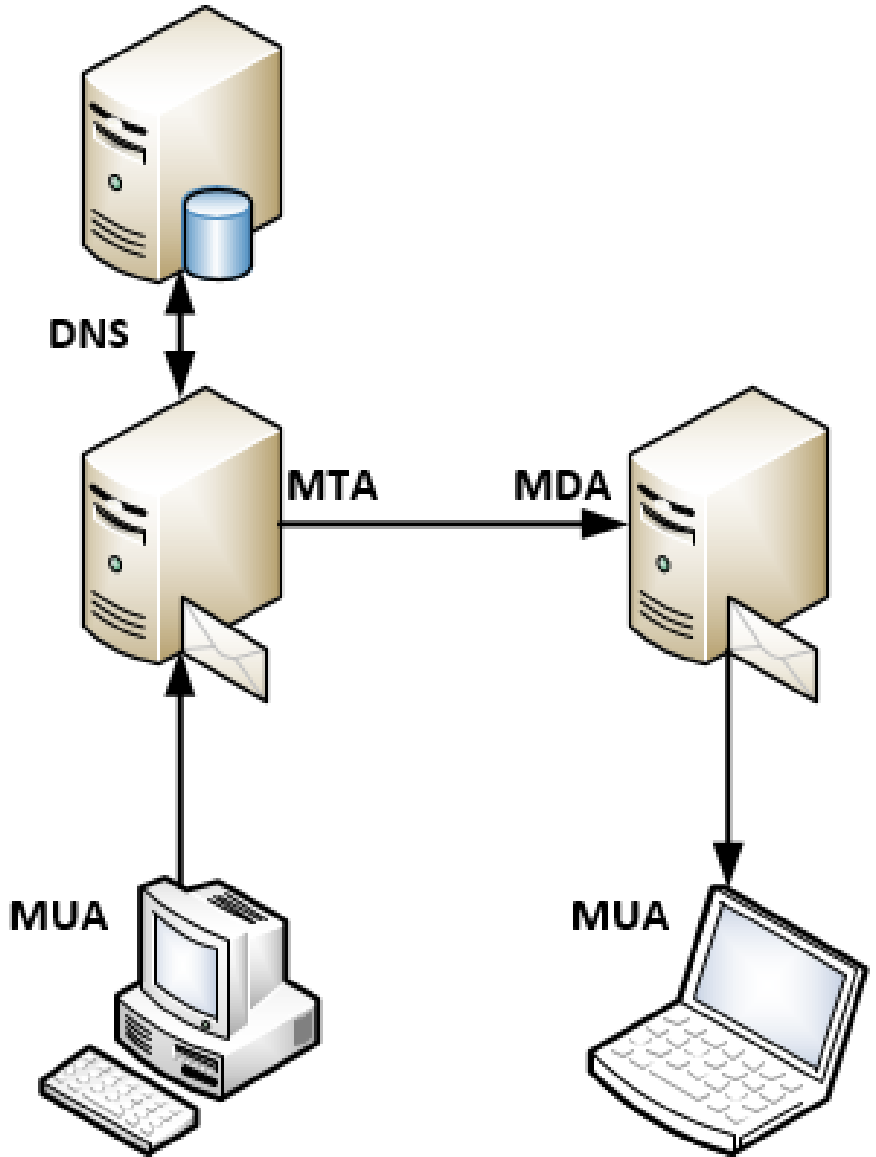
Simple Mail Transport Protocol

- Aplikačný protokol slúžiaci na odosielanie elektronickej pošty
- Správa je doručená do tzv. poštovej schránky adresáta
- Ku schránke môže používateľ ďalej pristupovať pomocou protokolov POP3/IMAP.



Simple Mail Transport Protocol

- MUA – Mail User agent
- MTA – Mail Transfer agent
- MDA – Mail Delivery agent



Simple Mail Transport Protocol

- E-mail používa formát adries v tvare **názov_používateľa@doména.sk**
  - „**názov_používateľa** “ – meno/názov používateľského konta
  - „**@**“ – oddelenie názvu používateľa od doménového mena
  - „**doména.sk**“ – doména v ktorej sa používateľ nachádza
- E-mailová správa sa delí na tzv. obálku a telo.
  - Obálka obsahuje režijné informácie potrebné na doručenie správy
    - Adresa odosielateľa
    - Adresa príjemcu
    - Kódovanie
  - Telo obsahuje vlastný text správy

Simple Mail Transport Protocol

```
220 mail.kis.fri.uniza.sk ESMTP Postfix
ehlo kis.fri.uniza.sk
250-mail.kis.fri.uniza.sk
250-PIPELINING
250-SIZE 20480000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: marek@kis.fri.uniza.sk
250 2.1.0 Ok
rcpt to: jakub.hrabovsky@fri.uniza.sk
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Tajne heslo
Ahoj Jakub,
tajne heslo je mandarinka.
Marek
.
250 2.0.0 Ok: queued as 97B77200FFD8
```

Post Office Protocol v3

- POP3 je spojovo-orientovaný textový protokol
  - POP3 nie je zabezpečený, jeho šifrovaná podoba sa volá POP3S
  - Je však autentifikovaný (vyžaduje meno a heslo)
  - Počúva na porte 110 (šifrovaný na 995)
- POP3 dialógy sa volajú transakcie, ktoré pozostávajú z týchto základných príkazov
  - **USER** – definuje meno používateľa
  - **PASS** – definuje heslo používateľa
  - **LIST** – zobrazí zoznam správ
  - **RETR** – získa správu
  - **DELE** – vymaže správu

Post Office Protocol v3

```
+OK Hello there.
user marek
+OK Password required.
pass TajneHeslo
+OK logged in.
list
+OK POP3 clients that break here, they violate STD53.
1 2518996
2 18761
3 4170
4 4170
5 3495
6 3677
7 22106
8 7276419
9 1593177
10 236371
11 24641
12 3600
13 7799
14 12443
15 4988
16 2564
17 8233089
```

Post Office Protocol v3

```
639 21494
640 5792
641 4246
642 8204
643 175227
644 5116
645 94294
646 3620
647 3168
648 6197
649 7535
650 981
651 1310
.
retr 651
+OK 1310 octets follow.
Return-Path: <marek.moravcik@fri.uniza.sk>
X-Original-To: marek@kis.fri.uniza.sk
Delivered-To: marek@kis.fri.uniza.sk
Received: from localhost (localhost [127.0.0.1])
          by mail.kis.fri.uniza.sk (Postfix) with ESMTP id AAF81200FFF8
          for <marek@kis.fri.uniza.sk>; Sun, 27 Mar 2016 16:04:10 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at kis.fri.uniza.sk
Received: from mail.kis.fri.uniza.sk ([127.0.0.1])
          by localhost (castor.kis.fri.uniza.sk [127.0.0.1]) (amavisd-new, port 10044)
          with LMTP id h6VYBhSKp7uF for <marek@kis.fri.uniza.sk>;
          Sun, 27 Mar 2016 16:04:10 +0200 (CEST)
Received: from [192.168.2.14] (unknown [188.123.100.211])
```

Post Office Protocol v3

```
From: =?UTF-8?Q?Marek_Morav=c4=8d=c3=adk?= <marek.moravcik@fri.uniza.sk>
Subject: POP3 test
Message-ID: <56F7E862.6040203@fri.uniza.sk>
Date: Sun, 27 Mar 2016 16:04:18 +0200
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101
 Thunderbird/38.7.0
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Testovacia spr..va protokolu POP3
.
dele 651
+OK Deleted.
quit
+OK Bye-bye.
```

Internet Message Access Protocol

- IMAP je klient-server textový protokol
- IMAP nie je zabezpečený, jeho šifrovaná podoba sa volá IMAPS
- Je však autentifikovaný (vyžaduje meno a heslo)
- Počúva na porte 143 (šifrovaný na 993)
- Podporuje viacnásobné prihlásenie
- Podporuje viac mailboxov (priečinky) na serveri

Internet Message Access Protocol

- IMAP používa tieto základné správy
  - **login** – prihlásenie klienta
  - **select** – vyberie požadovaný mailbox
  - **search** – hľadá správy s konkrétnymi príznakmi (flags)
  - **fetch** – preberie správu (prípadne jej časť)
  - **store** – manipulácia zo správou
  - **logout** – odhlásenie klienta
- Každá IMAP správa musí mať na začiatku identifikátor
  - Napr. a003 search unseen

Internet Message Access Protocol

```
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUO
Double Precision, Inc.  See COPYING for distribution information.
a0 login marek TajneHeslo
a0 OK LOGIN Ok.
a1 select inbox
* FLAGS (NonJunk $Forwarded /unseen \Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (NonJunk $Forwarded /unseen \* \Draft \Answered \Flagged \Deleted \Seen)] Limited
* 555 EXISTS
* 1 RECENT
* OK [UIDVALIDITY 1437044936] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
a1 OK [READ-WRITE] Ok
a2 search unseen
* SEARCH 555
a2 OK SEARCH done.
```

Internet Message Access Protocol

```
a3 fetch 555 body[]
* 555 FETCH (BODY[] {1422}
Return-Path: <marek.moravcik@fri.uniza.sk>
X-Original-To: marek@kis.fri.uniza.sk
Delivered-To: marek@kis.fri.uniza.sk
Received: from localhost (localhost [127.0.0.1])
          by mail.kis.fri.uniza.sk (Postfix) with ESMTP id 9D6A620E3732
          for <marek@kis.fri.uniza.sk>; Fri, 22 Apr 2016 16:39:34 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at kis.fri.uniza.sk
Received: from mail.kis.fri.uniza.sk ([127.0.0.1])
          by localhost (castor.kis.fri.uniza.sk [127.0.0.1]) (amavisd-new, port 10044)
          with LMTP id a4xOFW0jG5pr for <marek@kis.fri.uniza.sk>;
          Fri, 22 Apr 2016 16:39:34 +0200 (CEST)
Received: from [192.168.10.220] (unknown [192.168.10.220])
          by mail.kis.fri.uniza.sk (Postfix) with ESMTPSA id 7C83120E3730
          for <marek@kis.fri.uniza.sk>; Fri, 22 Apr 2016 16:39:34 +0200 (CEST)
Subject: Fwd: IMAP test
References: <571A3604.40906@fri.uniza.sk>
To: =?UTF-8?Q?Marek_Morav=c4=8d=c3=adk?= <marek@kis.fri.uniza.sk>
From: =?UTF-8?Q?Marek_Morav=c4=8d=c3=adk?= <marek.moravcik@fri.uniza.sk>
X-Forwarded-Message-Id: <571A3604.40906@fri.uniza.sk>
Message-ID: <571A37A7.6060606@fri.uniza.sk>
Date: Fri, 22 Apr 2016 16:39:35 +0200
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101
 Thunderbird/38.7.2
MIME-Version: 1.0
In-Reply-To: <571A3604.40906@fri.uniza.sk>
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Testovacia spr..va protokolu IMAP
)
* 555 FETCH (FLAGS (\Seen \Recent))
a3 OK FETCH completed.
```

Internet Message Access Protocol

```
a4 store 555 +flags \Deleted
* 555 FETCH (FLAGS (\Seen \Deleted \Recent))
a4 OK STORE completed.
a5 logout
* BYE Courier-IMAP server shutting down
a5 OK LOGOUT completed
```

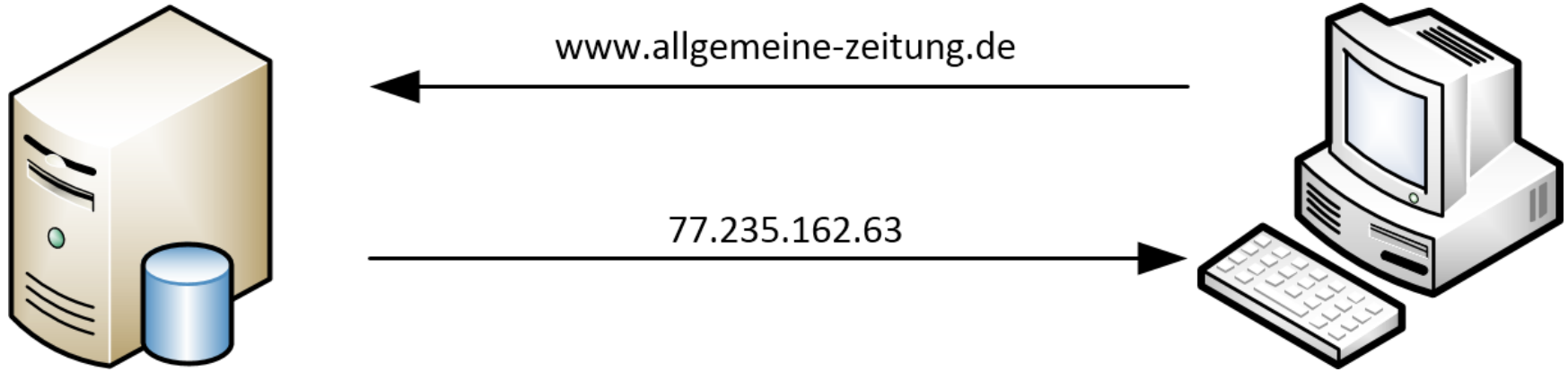
POP3 vs IMAP

	POP3	IMAP
Odosielanie/prijímanie	Prijímanie	Prijímanie
Šifrovanie	Nie/Áno	Nie/Áno
Zmazanie správy na serveri	Väčšinou	Nie
Synchronizácia klientov	Nie	Áno
L4 protokol	TCP/TLS	TCP/TLS
L4 port	110/995	143/993

Domain Name System

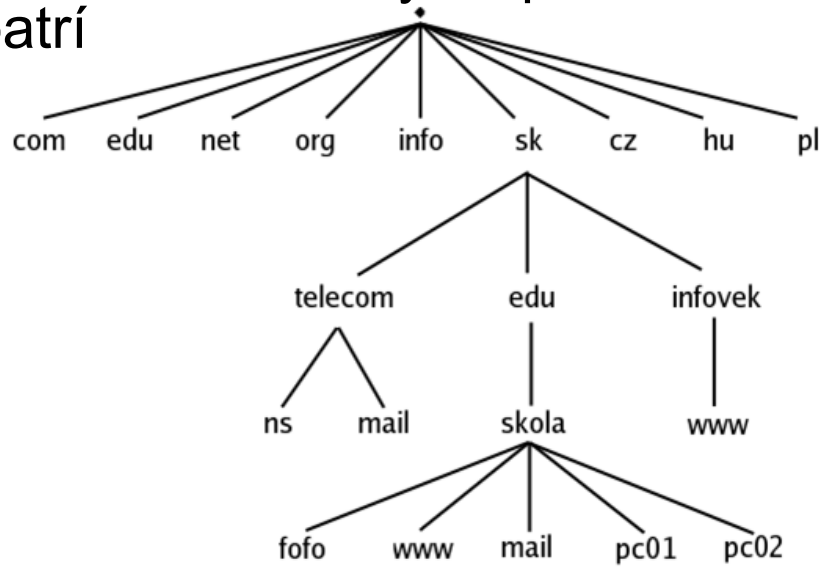
- Protokol DNS je „telefónny zoznam“ počítačov na internete
  - My používame slovné názvy počítačov
  - Počítače používajú číselné IP adresy
  - DNS slúži na vyhľadanie IP adresy počítača podľa jeho mena
- Presnejšie povedané, DNS je stromovo organizovaná databáza, ktorá obsahuje rôzne informácie o internetových menách a adresách

Domain Name System



Domain Name System

- Pojem **doména** označuje časť slovného mena počítača, ktorá istým spôsobom vyjadruje, kde sa počítač nachádza alebo komu patrí
  - V názve mail.skola.edu.sk sú 4 domény
    - **sk** – označuje Slovensko (tzv. vrcholová doména)
    - **edu** – označuje vzdelávacie inštitúcie
    - **skola** – označuje meno konkrétnej školy
    - **mail** – vlastné meno počítača
  - Úplné meno počítača so všetkými doménami sa v angličtine nazýva Fully Qualified Domain Name (FQDN)
  - Toto hierarchické usporiadanie domén vytvára tzv. doménový strom
- Žiaden DNS server neobsahuje zoznam všetkých domén
  - Každý DNS server obsluhuje iba časť doménového stromu, tzv. zónu
  - Ak hľadaný názov sám nepozná, vie aspoň zistiť, na ktorom DNS serveri sú bližšie informácie – tzv. delegovanie zón

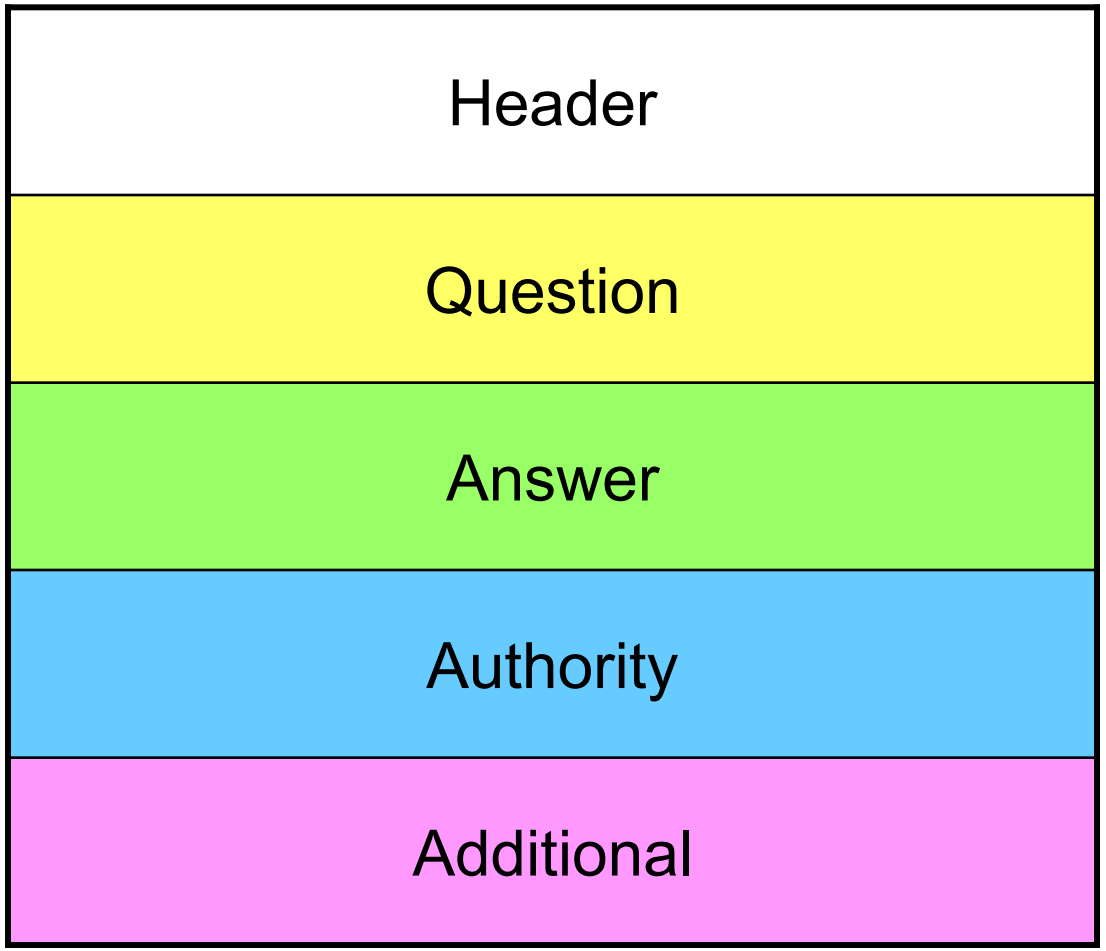


Domain Name System

- Typy záznamov v DNS sa nazývajú RR (Resource Record)
- Základné typy RR
  - A: IPv4 adresa
  - AAAA: IPv6 adresa
  - NS: name server (DNS server spravujúci doménu)
  - MX: mail exchanger (poštový server)
  - CNAME: Canonical name (alias)
  - PTR: pointer (spätný preklad z IP na meno)

- Podľa toho, aké informácie klient potrebuje, sa v DNS hľadá k danému internetovému menu záznam vhodného typu

Domain Name System



- Každá správa DNS protokolu (otázka či odpoveď) má fixnú štruktúru
  - **Header** – hlavička správy
  - **Question** – hľadaný názov
  - **Answer** – finálna odpoveď servera vo forme zdrojového záznamu
  - **Authority** – informácia o DNS serveri, ktorý má presné alebo aspoň presnejšie info o hľadanom mene
  - **Additional** – prídavné pomocné informácie

```
Internet Protocol Version 4, Src: 192.168.2.14, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 56293 (56293), Dst Port: 53 (53)
Domain Name System (query)
    [Response In: 654]
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ujszo.com: type A, class IN
```

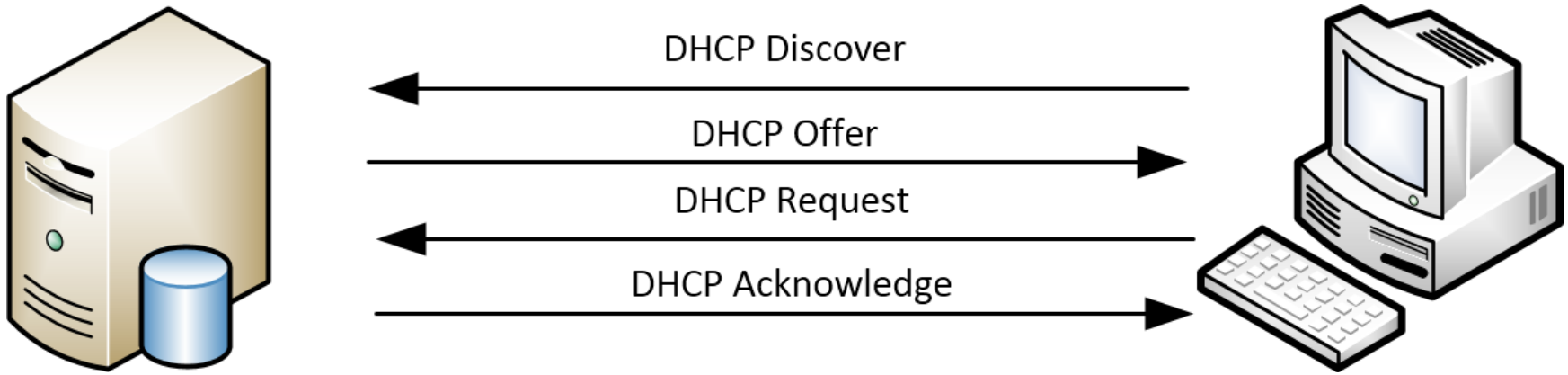
```
Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.14
User Datagram Protocol, Src Port: 53 (53), Dst Port: 56293 (56293)
Domain Name System (response)
    [Request In: 653]
    [Time: 0.113403000 seconds]
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 1
  > Queries
  v Answers
    > www.ujszo.com: type A, class IN, addr 195.146.144.223
  > Authoritative nameservers
  > Additional records
```

```
$TTL 1H
@       IN SOA  ns.kis.fri.uniza.sk. hostmaster.kis.fri.uniza.sk. (
                2015111601 ; Serial
                3H         ; Refresh
                1H         ; Retry
                2W         ; Expire
                1H         ; Negative TTL
                )

            NS  ns.kis.fri.uniza.sk.
            NS  frix.fri.uniza.sk.
            MX  10 relay.uniza.sk.
            MX  20 smtp3.uniza.sk.

mail        A   158.193.152.2
netacad     CNAME   www
nil         CNAME   www
ns          A   158.193.152.2
ns          AAAA    2001:4118:300:120::2
www         A   158.193.152.2
www         AAAA    2001:4118:300:120::2
nlab        A   158.193.152.33
voip        A   158.193.152.2
voip        AAAA    2001:4118:300:120::2
```

Dynamic Host Configuration Protocol

- Protokol DHCP slúži staniciam na automatické získanie sieťových nastavení
  - Bez DHCP by bolo potrebné všetky nastavenia konfigurovať ručne
- DHCP prideľuje staniciam rôzne konfiguračné údaje
  - IP adresu, masku siete, adresu brány, DNS server a ďalšie
- DHCP používa 4+1 základné správy
  - **Discover** – klient hľadá DHCP servery
  - **Offer** – server ponúka klientovi adresu
  - **Request** – klient žiada o konkrétnu adresu
  - **Acknowledge** – server odsúhlasuje klientovi výpožičku adresy
  - **Release** – klient sa odhlási od servera

Dynamic Host Configuration Protocol



Source	Destination	Protocol	Length	Info
192.168.2.14	192.168.2.1	DHCP	342	DHCP Release - Transaction ID 0x64d7a255
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8b4739
192.168.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x8b4739
0.0.0.0	255.255.255.255	DHCP	349	DHCP Request - Transaction ID 0x8b4739
192.168.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x8b4739

```
Hops: 0
Transaction ID: 0x008b4739
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.2.14
Next server IP address: 192.168.2.1
Relay agent IP address: 0.0.0.0
Client MAC address: CompalIn_6c:8a:c5 (f0:76:1c:6c:8a:c5)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Offer)
> Option: (54) DHCP Server Identifier
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
v Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
v Option: (3) Router
    Length: 4
    Router: 192.168.2.1
> Option: (15) Domain Name
> Option: (6) Domain Name Server
```

File Transfer Protocol

- Protokol FTP je starší protokol, ktorý slúži na prenos súborov medzi klientom a serverom
- FTP si vytvára medzi klientom a serverom až dve spojenia
  - Jedno spojenie je tzv. riadiace spojenie (control connection), ktorým sa posielajú medzi klientom a serverom príkazy
  - Druhé spojenie je tzv. dátové spojenie (data connection), ktorým sa posielajú dáta prenášaných súborov. Dátové spojenie sa vytvára len v čase, keď sa prenášajú súbory
- Protokol FTP je autentifikovaný, ale nešifrovaný
  - V súčasnosti ho nahrádza protokol SFTP (Secure FTP)
- Existuje odľahčená verzia protokolu FTP, ktorá sa volá Trivial FTP
  - TFTP má len vybranú podmnožinu operácií FTP a nie je autentifikovaný (UDP 69)

Source	Destination	Protocol	Length	Info
192.168.2.14	147.175.111.14	FTP	60	Request: PASV
147.175.111.14	192.168.2.14	FTP	106	Response: 227 Entering Passive Mode (1
192.168.2.14	147.175.111.14	FTP	71	Request: RETR HEADER.txt
147.175.111.14	192.168.2.14	FTP	122	Response: 150 Opening ASCII mode data
147.175.111.14	192.168.2.14	FTP-DATA	1281	FTP Data: 1227 bytes
147.175.111.14	192.168.2.14	FTP	77	Response: 226 Transfer complete

```
> Frame 11: 1281 bytes on wire (10248 bits), 1281 bytes captured (10248 bits) on interface 0
> Ethernet II, Src: BelkinIn_57:97:60 (94:44:52:57:97:60), Dst: CompalIn_6c:8a:c5 (f0:76:1c:6c:8a:c5)
> Internet Protocol Version 4, Src: 147.175.111.14, Dst: 192.168.2.14
> Transmission Control Protocol, Src Port: 13496 (13496), Dst Port: 5787 (5787), Seq: 1, Ack: 1, Len:
  FTP Data (##########################################################################\r\nWelcome to ftp.elf.stuba
```

```
0120  6f 3a 20 68 74 74 70 3a  2f 2f 77 77 77 2e 65 6c   o: http: //www.el
0130  66 2e 73 74 75 62 61 2e  73 6b 0d 0a 23 23 23 23   f.stuba. sk..####
0140  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23   ######## ########
0150  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23   ######## ########
0160  23 23 23 23 23 23 23 23  23 23 23 23 23 23 23 23   ######## ########
0170  23 23 23 23 23 23 23 23  23 23 0d 0a 4f 75 72 20   ######## ##..Our
0180  46 54 50 2d 73 69 74 65  20 69 73 20 6d 69 72 72   FTP-site  is mirr
0190  6f 72 65 64 20 61 74 3a  0d 0a 20 66 74 70 3a 2f   ored at: .. ftp:/
01a0  2f 66 74 70 2e 73 61 63  2e 73 6b 2f 70 75 62 2f   /ftp.sac .sk/pub/
01b0  70 63 09 09 09 20 20 20  69 6e 20 53 6c 6f 76 61   pc...    in Slova
01c0  6b 69 61 0d 0a 20 66 74  70 3a 2f 2f 73 61 63 2d   kia.. ft p://sac-
01d0  66 74 70 2e 67 72 61 74  65 78 2e 73 6b 09 09 09   ftp.grat ex.sk...
01e0  20 20 20 69 6e 20 53 6c  6f 76 61 6b 69 61 0d 0a      in Sl ovakia..
01f0  20 66 74 70 3a 2f 2f 66  74 70 2e 75 61 6b 6f 6d    ftp://f tp.uakom
0200  2e 73 6b 2f 70 75 62 2f  6d 69 72 72 6f 72 73 2f   .sk/pub/ mirrors/
0210  73 61 63 09 09 20 20 20  69 6e 20 53 6c 6f 76 61   sac..    in Slova
0220  6b 69 61 0d 0a 20 66 74  70 3a 2f 2f 66 74 70 2e   kia.. ft p://ftp.
```

Server Message Block

- Protokol slúžiaci na zdieľanie prostriedkov (súbory, tlačiarne) cez počítačovú sieť
- Client-server architektúra
- Pôvodne navrhnutý pre DOS, postupne adoptovaný inými (Apple, Unix)
- Microsoft označuje aj ako CIFS (Common Internet File System)
- Implementácia pre Unix - Samba

Server Message Block

- SMB 1.0
- SMB 2.0 alebo SMB2
  - Windows Vista – r. 2006
  - Najširšie používaná verzia
- SMB 2.1
  - Windows 7
- SMB 3.0
  - Windows 8
- SMB 3.1.1
  - Windows 10

Server Message Block

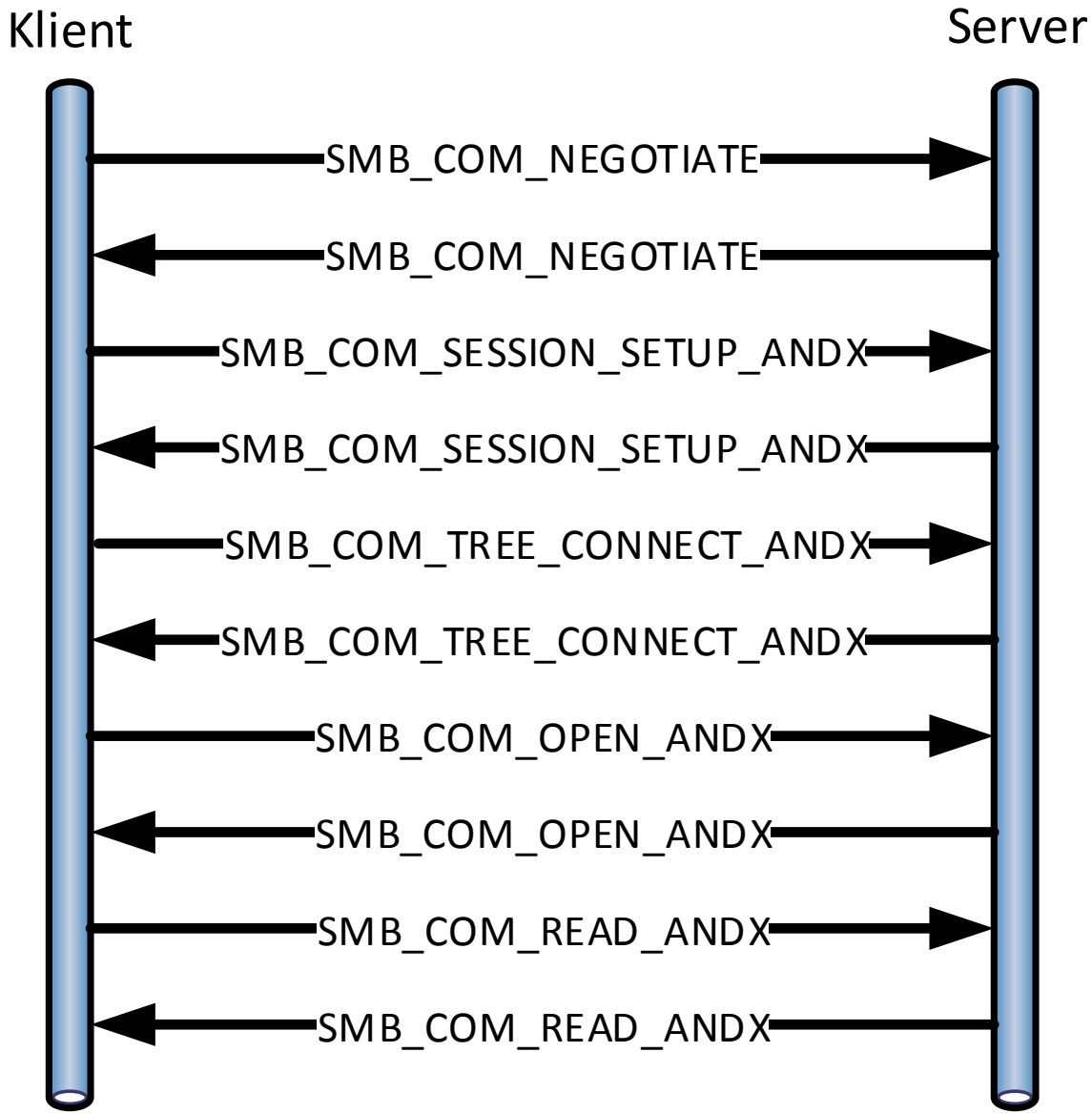
- Pracuje priamo nad TCP
  - Port 445
- Pracuje nad NetBIOS
  - TCP 137, 139
  - UDP 137, 138

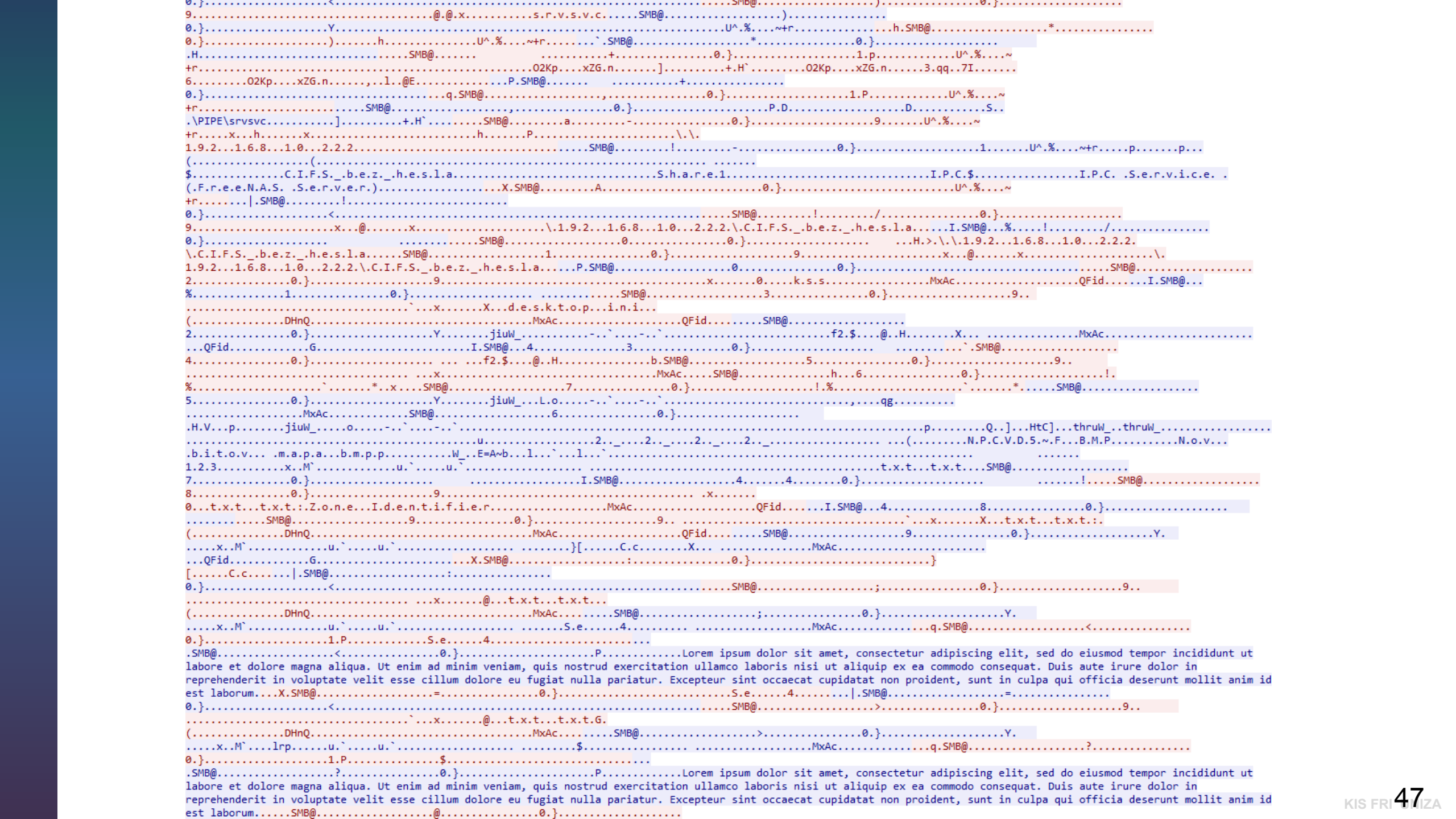
<table>
<tr><td>Application</td><td colspan="3" rowspan="2">SMB</td><td rowspan="2">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td>NetBIOS</td><td>NetBIOS</td><td></td></tr>
<tr><td>Transport</td><td rowspan="2">IPX</td><td rowspan="2">DECnet</td><td>TCP&UDP</td><td>TCP/UDP</td></tr>
<tr><td>Network</td><td>IP</td><td>IP</td></tr>
<tr><td>Link</td><td>802.2,
802.3,802.5</td><td>Ethernet V2</td><td>Ethernet V2</td><td>Ethernet or
others</td></tr>
<tr><td>Physical</td><td colspan="4"></td></tr>
</table>

Server Message Block

- SMB používa tieto základné správy:
  - SMB_COM_NEGOTIATE
    - Dohodne verziu protokolu
  - SMB_COM_SESSION_SETUP_ANDX
    - Autentifikačné údaje
  - SMB_COM_TREE_CONNECT_ANDX
    - Požiadavka na súborový podstrom
  - SMB_COM_OPEN_ANDX
    - Požiadavka na otvorenie súboru súbor
  - SMB_COM_READ_ANDX
    - Požiadavka na obsah súboru

Server Message Block





Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Telnet a Secure SHell (SSH)

- Protokoly Telnet a SSH sú určené na vzdialené ovládanie zariadenia
- Ovládajú príkazový riadok, nie grafické rozhranie
  - Grafické pripojenie je možné cez RDP a VNC

- Telnet je starší a nešifrovaný (možnosť použiť SSL)
- SSH je šifrovaný a široko používaný

```
> Internet Protocol Version 4, Src: 158.193.139.5, Dst: 192.168.10.193
> Transmission Control Protocol, Src Port: 23 (23), Dst Port: 3692 (3692), Seq: 151, Ack: 74, Len: 422
v Telnet
    Data: \r\n
    Data: Current configuration : 1355 bytes\r\n
    Data: !\r\n
    Data: version 12.1\r\n
    Data: no service pad\r\n
    Data: service timestamps debug uptime\r\n
    Data: service timestamps log uptime\r\n
    Data: service password-encryption\r\n
    Data: !\r\n
    Data: hostname 2950_B303\r\n
    Data: !\r\n
    Data: enable secret 5 $1$p.fQ$hFQbuvvIsL1CwlL5WcJ820\r\n
    Data: !\r\n
    Data: ip subnet-zero\r\n
    Data: !\r\n
    Data: !\r\n
    Data: !\r\n
    Data: spanning-tree mode rapid-pvst\r\n
```

```
> Internet Protocol Version 4, Src: 192.168.255.19, Dst: 192.168.10.193
> Transmission Control Protocol, Src Port: 22 (22), Dst Port: 3620 (3620), Seq: 321, Ack: 193, Len: 64
v SSH Protocol
    Packet Length (encrypted): b00e0a05
    Encrypted Packet: 8ae5a1994bf0db2cf413d83748bb8c2933f6bf8ff1a51fbc...
```

Simple Network Management Protocol

- Protokol umožňujúci monitorovanie a správu zariadení
- Primárne pre základné sieťové prvky
  - Smerovače
  - Prepínače
- Neskôr aj pre
  - Servery
  - Tlačiarne
  - Koncové stanice
- UDP 161 – zariadenie
- UDP 162 – monitorovací server

Simple Network Management Protocol

- SNMPv1
  - Vydaná v r. 1988
  - Autentifikácia pomocou „community string“ - plaintext
- SNMPv2c
  - Nové typy premenných
  - Rozšírená MIB
- SNMPv3
  - Vydaná v r. 2004
  - Pridaná autentifikácia

Simple Network Management Protocol

- MIB - Management information base
  - Hierarchická databáza
  - AVP – attribute value pair
  - Každý atribút má vlastné **OID**
- OID - object identifier
  - Typ (Integer, Octet String, ...) a prístup (read-only, read-write, write-only)
  - Priraďuje IANA

- Príklad: 1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3
  - Iso(1).org(3).dod(6).internet(1).private(4).transition(868).products(2).chassis(4).card(1).slotCps(2).-cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEntry(1).cpsModuleModel(3).3562.3

Simple Network Management Protocol

- Monitorovacie zariadenie (kolektor) sa vypytuje zariadenia
- Zariadenie samo pošle správu - SNMP Trap

- **GET REQUEST**: Číta informáciu z jednej alebo viacerých premenných definovaných OID
- **GETNEXT REQUEST**: Číta informáciu z jednej alebo viacerých premenných nasledujúcich po zadaných OID (vhodné napr. pri čítaní tabuliek)
- **GET BULK**: Číta informáciu z celého podstromu (od SNMPv2)
- **GET RESPONSE**: Odpoveď od agenta
- **SET**: Nastavenie jednej alebo viacerých premenných s daným OID
- **TRAP**: Spontánna správa od SNMP agenta (napr. správa o reštarte)

```
> Internet Protocol Version 4, Src: 172.31.19.54, Dst: 172.31.19.73
> User Datagram Protocol, Src Port: 15928 (15928), Dst Port: 161 (161)
v Simple Network Management Protocol
    version: version-1 (0)
    community: public
  v data: get-request (0)
    v get-request
        request-id: 50
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.2.0: Value (Null)
            Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)
            Value (Null)
```

```
> Internet Protocol Version 4, Src: 172.31.19.73, Dst: 172.31.19.54
> User Datagram Protocol, Src Port: 161 (161), Dst Port: 15928 (15928)
v Simple Network Management Protocol
    version: version-1 (0)
    community: public
  v data: get-response (2)
    v get-response
        request-id: 50
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 1 item
        v 1.3.6.1.2.1.1.2.0: 1.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1 (iso.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1)
            Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)
            Value (OID): 1.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1 (iso.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1)
```

RFC dokumenty

Protokol	RFC	Protokol	RFC
HTTP	2068 2616 7540	DNS	882 1034 1035
HTTPS	2818	DHCP	1531 1541 3736
SMTP	821 5321	Telnet	15 854
POP3	1081 1939 2449	SSH	4253 4716 6668
IMAP	1064 1203	SNMP	1213 2576 3411
FTP	114 959 2428		

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

KATEDRA INFORMAČNÝCH SIETÍ
FAKULTA RIADENIA A INFORMATIKY ŽU

cisco
Networking
Academy