

# Obsah

<b>Úvod</b> .....	<b>13</b>
-------------------	-----------

## **Kapitola 1**

<b>Síťové protokoly</b> .....	<b>15</b>
-------------------------------	-----------

Jaké protokoly se používají na Internetu? .....	17
Fyzická vrstva .....	18
Lokální síť (LAN) .....	19
Linková vrstva .....	20
IP vrstva .....	21
Vrstva TCP/UDP .....	22
Aplikační vrstva .....	23
Způsoby přenosu informací .....	25
Synchronní přenos .....	25
Paketový přenos .....	26
Asynchronní přenos .....	26
Virtuální okruh .....	26
Pevné a komutované virtuální okruhy .....	28

## **Kapitola 2**

<b>Nástroje pro sledování a zkoumání sítě</b> .....	<b>29</b>
---	-----------

Packet driver .....	30
Promiskuitní mód .....	30
Program Wireshark .....	31
Začínáme s Wiresharkem .....	32
Filtry .....	33
Colorig rules .....	36
Follow TCP stream .....	36
Statistiky .....	37
Tisk a Export .....	37
Další utility .....	39
Domácí cvičení .....	39
Program nmap .....	40
Co program nmap dělá? .....	40
První fáze: Vyhledávání připojených systémů .....	40
Druhá fáze: Scanování portů .....	41
Další zajímavé přepínače .....	42
zenmap GUI .....	42
Domácí cvičení .....	42

## Kapitola 3

### Fyzická vrstva .....45

Sériová rozhraní .....	46
Sériový a paralelní přenos dat.....	46
Symetrický a asymetrický signál.....	47
Synchronní nebo asynchronní přenos .....	47
Normy V.24, V.35 a X.21 .....	48
Nulový modem.....	51
Modemy .....	52
Analogová linka .....	52
Modem je „automatický“.....	53
AT-příkazy .....	53
Synchronní přenos .....	55
ISDN .....	55
Basic Rate .....	56
Základní pásmo a telefonní (hlasové) pásmo .....	57
ADSL .....	57
Přenosové rychlosti modemů.....	59
Strukturovaná kabeláž.....	60
Měděné rozvody .....	61
Optická vlákna.....	62
IEEE 802 .....	64
Ethernet, FastEthernet a Gigabitový Ethernet .....	65
Bezdrátové lokální sítě WLAN .....	69
Typické WLAN-konfigurace .....	71
Antény .....	71
Sledování WiFi .....	72

## Kapitola 4

### Linková vrstva .....75

SLIP .....	75
HDLC .....	76
Křídlová značka (Flag).....	77
Adresní pole.....	78
Datové pole a typ přenášeného protokolu .....	78
Řídicí pole.....	78
Kontrolní součet (Frame Check Sequence – FCS).....	81
Základní vlastnosti protokolu HDLC .....	81
Cisco HDLC (cHDLC).....	81
PPP.....	82
Vytáčení telefonní linky .....	84
Protokol LCP.....	85
Autentizace.....	90
Protokol řízení zpětného volání .....	95
Další protokoly .....	96
Protokol IPCP.....	101
Frame Relay .....	103

Rámec protokolu Frame relay .....	106
IP přes Frame Relay .....	109
LMI .....	110
Závěr k protokolu Frame Relay .....	111
Ethernet .....	111
Bezdrátové lokální síť WLAN – IEEE 802.11 .....	114
Obecný formát rámce .....	116
Ovládací rámce .....	117
Řídicí rámce .....	118
Datové rámce .....	122
WEP .....	123
IEEE 802.1X .....	124
IEEE 802.11i .....	124
LLC (IEEE 802.2) .....	124
Domácí cvičení .....	126

## Kapitola 5

### **IPv4..... 127**

IP datagram .....	131
Protokol ICMP .....	135
Echo .....	137
Nedoručitelný IP datagram .....	138
Sniž rychlost odesílání .....	138
Změň směrování (Redirect) .....	138
Žádost o směrování .....	139
Čas vypršel (time exceeded) .....	139
Žádost o masku .....	141
Časová synchronizace .....	141
Fragmentace .....	142
Volitelné položky IP záhlaví .....	145
Zaznamenávej směrovače .....	147
Zaznamenávej čas .....	149
Explicitní směrování .....	150
Upozornění pro směrovač (IP Router Alert Option) .....	152
Protokoly ARP a RARP .....	153
Filtrace ARP .....	156
Proxy ARP .....	156
RARP .....	157
IGMP .....	158
Oběžníky a linkový protokol .....	161
QoS .....	162
ECN .....	164
Domácí cvičení .....	165

## Kapitola 6

### IPv4 – adresa ..... 167

Síť – historická epocha I .....	168
Speciální IP adresy.....	169
Síťová maska .....	170
Síť – historická epocha II.....	171
Subsítě a supersítě.....	172
Supersítě a autonomní systémy.....	176
IP adresy v intranetu.....	181
Nečíslované síť .....	181
Dynamicky přidělované adresy .....	182
Adresní plán .....	183
Více než 254 rozhraní na LAN.....	184
Domácí cvičení.....	184

## Kapitola 7

### Směrování..... 185

Předávání (forwarding) a filtrace (filtering).....	187
Směrování (routing) .....	187
Zpracování .....	189
Manipulace se směrovacími tabulkami.....	190
Výpis obsahu směrovací tabulky .....	190
Výpis obsahu směrovací tabulky v UNIXu/Linuxu.....	190
Výpis v operačních systémech Microsoft.....	191
Výpis obsahu směrovací tabulky na směrovačích CISCO.....	192
Naplnění směrovací tabulky a rušení položek .....	193
Směrovací protokoly.....	194
Princip Routing Vector Protocols (RVP).....	195
RIP, RIP2 a RIPng .....	198
Princip Link State Protocols (LSP) .....	198
OSPF .....	203
Redistribuce.....	204
Domácí cvičení.....	205

## Kapitola 8

### IPv6..... 207

Další hlavičky v IP datagramu .....	210
Informace pro směrovače.....	210
Směrovací informace .....	212
Záhlaví fragmentu.....	213
Autentizační hlavička (protokol AH).....	215
Bezpečnostní hlavička (protokol ESP) .....	215
ICMPv6.....	216
Překlad IP adres na linkové adresy.....	218
Zjištění adresy směrovače na LAN .....	221

Změň směrování .....	223
IPv6 – adresa .....	224
Zápis adresy .....	225
Oběžníky (Multicasts) .....	226
Jednoznačné adresy .....	226
Identifikátor (index) síťového rozhraní .....	228
Domácí cvičení .....	228

## Kapitola 9

### Protokol TCP (Transmission Control Protocol) ..... 229

TCP segment .....	231
Volitelné položky TCP záhlaví .....	234
Příklad výpisu TCP segmentu .....	234
Navázání a ukončení spojení protokolem TCP .....	236
Navazování spojení .....	236
Ukončování spojení .....	240
Odmítnutí spojení .....	242
Zjištění stavu spojení .....	242
Technika zpoždění odpovědi .....	243
Technika okna .....	245
Zahlcení sítě .....	247
Pomalý start .....	247
Vyhýbání se zahlcení .....	248
Ztráta segmentu .....	248
Volba zvětšení okna .....	249
Domácí cvičení .....	250

## Kapitola 10

### Protokol UDP (User Datagram Protocol) ..... 251

Fragmentace .....	252
Příklad UDP datagramu .....	253
Oběžníky .....	253
Domácí cvičení .....	253

## Kapitola 11

### DNS ..... 255

Domény a subdomény .....	256
Syntaxe jména .....	257
Reverzní domény .....	258
Doména 0.0.127.in-addr.arpa .....	259
Zóna .....	259
Speciální zóny .....	259
Rezervované domény a pseudodomény .....	260

Dotazy (překlady).....	260
Round Robin .....	263
Konfigurace resolveru .....	264
Konfigurace resolveru v Unixu .....	264
Konfigurace resolveru ve Windows .....	265
Jmenné servery .....	267
Předávání dotazů DNS .....	270
Věty RR.....	271
Databáze DNS.....	273
SOA .....	274
Záznamy typu A.....	276
CNAME.....	276
HINFO a TXT.....	277
NS.....	277
MX.....	278
PTR.....	279
Věta typu SRV .....	280
\$ORIGIN .....	282
\$INCLUDE .....	283
Rozšíření DNS pro IP verze 6 .....	283
Záznam typu AAAA .....	283
Záznam typu A6.....	283
Reverzní domény .....	285
Záznam typu DNAME.....	285
Nástroje pro sledování DNS.....	286
Program nslookup.....	286
Domácí cvičení: .....	288
Ladící režim .....	289
Ladící úroveň debug.....	289
Ladící úroveň d2.....	290
Změna implicitního jmenného serveru .....	291
Dig.....	291
Domácí cvičení.....	292

## Kapitola 12

### Protokol DNS..... 293

DNS QUERY .....	293
Formát paketu DNS query .....	294
Záhlaví paketu DNS query .....	294
Sekce dotaz (Question section) .....	296
Sekce odpověď, autoritativní servery a doplňující informace .....	298
Komprese .....	298
Domácí cvičení.....	299
Inverzní dotaz .....	299
DNS UPDATE .....	299
Sekce záhlaví .....	300
Sekce zóny .....	301
Sekce předpokladů.....	301
Sekce update.....	302

Sekce doplňujících informací .....	303
Soubor žurnál .....	303
DNS Notify .....	303
Zpráva Notify .....	304
Inkrementální zone transfer .....	305
Formát dotazu .....	306
Formát odpovědi .....	306
Strategie čištění (purging) .....	306
Negativní caching (DNS NCACHE) .....	307
Jaké negativní odpovědi ukládat do paměti? .....	307
Jak dlouho udržovat negativní odpovědi v paměti? .....	308
Pole MINIMUM ve větě SOA .....	308
Pravidla ukládání negativních odpovědí .....	309
Domácí cvičení .....	309

## Kapitola 13

### Mezinárodní a národní organizace Internetu ..... 311

ICANN .....	312
RIR .....	312
Národní organizace .....	313
O sdružení CZ.NIC .....	313
Protokol whois .....	314
TLD .....	315
Adresní prostor IPv4 .....	324
Adresní prostor IPv6 .....	328
Domácí cvičení .....	330

## Kapitola 14

### Telnet ..... 331

Charakteristika protokolu .....	331
Bezpečnost .....	332
Protokol Virtuální terminál (NVT) .....	332
Příkazy protokolu Telnet .....	334
Příklad komunikace klienta z Windows .....	340
Příklad komunikace klienta z Unixu .....	342
Domácí cvičení .....	344

## Kapitola 15

### FTP ..... 345

Charakteristika .....	345
Architektura .....	345
Aktivní režim komunikace protokolu FTP .....	348
Pasivní režim komunikace protokolu FTP .....	350

Příkazy FTP .....	353
Proxy .....	355
Návratové kódy .....	357
Abnormální ukončení příkazu .....	357
Anonymní FTP.....	358
Domácí cvičení.....	359

## Kapitola 16

### **HTTP..... 361**

Klient-server.....	361
Domácí cvičení.....	364
Proxy.....	364
Brána.....	367
Tunel.....	368
Více mezilehlých uzlů.....	369
URI.....	370
Schéma http.....	370
Schéma ftp.....	371
Schéma mailto.....	372
Schéma nntp:.....	372
Schéma Telnet.....	372
Schéma file.....	372
Schéma pop.....	372
Relativní URI.....	372
HTTP dotaz.....	373
Metoda GET.....	374
Metoda POST.....	377
Metoda HEAD.....	378
Metoda TRACE.....	378
Metoda OPTIONS.....	379
HTTP odpověď.....	380
Přehled výsledkových kódů.....	381
Ostatní hlavičky.....	381
Hlavičky Accept.....	381
Autorizace klienta.....	382
Proxy autentizace.....	383
Hlavičky Content.....	384
Přesměrování a dočasná nedostupnost.....	384
Hlavička Upgrade.....	385
Cache.....	385
Informace o softwaru.....	387
Cookie.....	387
Hlavička Set-Cookie2.....	389
Hlavička Cookie.....	389
Domácí cvičení.....	389



## Kapitola 17

### **Elektronická pošta ..... 391**

Elektronická pošta a DNS .....	397
Formát poštovní zprávy.....	397
Přehled základních hlaviček z RFC-822 .....	398
SMTP .....	400
ESMTP .....	403
VERB.....	403
BITMIME .....	404
SIZE .....	404
ETRN .....	405
Potvrzení o doručení zprávy .....	405
DSN (Delivery Status Notifications).....	406
POP3 .....	408
IMAP4 .....	411
Neautentizovaný stav.....	413
Autentizovaný stav .....	414
Otevřená schránka.....	418
Domácí cvičení.....	423

## Kapitola 18

### **Filtrace, proxy a NAT ..... 425**

Filtrace .....	425
Filtrace na úrovni protokolu IP .....	427
Filtrace na úrovni TCP.....	432
Reflexivní filtry.....	436
Filtrace protokolů UDP, ICMP a případně dalších protokolů.....	440
Zakázané adresy.....	440
Aplikační protokoly a filtrace.....	440
Závěr k filtraci.....	445
Proxy .....	445
Klasická proxy .....	447
Generická proxy .....	448
Transparentní proxy .....	449
Autentizace.....	451
SOCKS.....	451
Skryté sítě .....	453
NAT .....	455
Jednoduchý NAT .....	455
Rozšířený NAT .....	457
Dvojitý NAT.....	458
Rozložení výkonu.....	459
ALG .....	459
Domácí cvičení.....	460

## Kapitola 19

<b>Firewall .....</b>	<b>461</b>
Architektura firewallů .....	462
TIS Firewall Toolkit .....	463
SEAL .....	463
Jednopočítačové firewally s dvěma síťovými rozhraními .....	465
Firewalling .....	465
Personální firewall .....	466
Demilitarizované zóny (DMZ) .....	466
Firewall on Firewall .....	467
Extranet .....	467
Viruswall a antispamový filter .....	469
DNS .....	470
DNS v uzavřených podnikových sítích .....	470
DNS a firewall .....	472
Společné DNS pro Internet i intranet .....	473
Na firewallu je jen jmenný server pro Internet, a nikoliv pro intranet .....	476
Duální DNS .....	477
Ostatní aplikační protokoly a firewall .....	479
HTTP a FTP .....	479
SSL/TLS .....	479
Telnet či SSH .....	479
Elektronická pošta .....	479
NTP (Network Time Protocol) .....	480
<b>Rejstřík .....</b>	<b>483</b>

# Úvod

Vážený čtenáři,

dostává se vám do rukou poslední, zcela přepracované vydání Velkého průvodce TCP/IP. Jedná se o originální českou příručku a učebnici TCP/IP, která nejenom vychází v 5. českém vydání, ale mezi tím vyšla anglicky, rusky a druhý díl dokonce polsky. Díky aktualizacím v jednotlivých vydáních došlo k takovým změnám, že z prvního vydání toho zbylo opravdu málo (třeba příklad na str. 399).

## Velký průvodce TCP/IP má nyní 19 kapitol:

1. **Síťové protokoly** – v této kapitole jsem s gusem vypustil model ISO OSI a jeho sedm vrstev na důkaz definitivního vítězství rodiny TCP/IP nad protokoly ISO OSI. Víím, že spíše došlo ke zkřížení obou rodin protokolů, ale pro mne, který zažil v první polovině 90. let minulého století monopol sítí ISO OSI (X.25) stvrzený tehdy ještě československým státem, který zakazoval veřejné využívání TCP/IP, to navždy bude vítězstvím.
2. **Nástroje pro sledování a zkoumání sítě** – tato kapitola byla přepracována a nyní je postavena na bázi programu Wireshark a byla dopracována část zabývající se sledováním sítí programem nmap.
3. **Fyzická vrstva** – z nostalgických důvodů jsem ponechal sériová rozhraní, modemy, strukturovanou kabeláž a dokonce i ISDN, protože mi stále připadá, že to patří k všeobecnému vzdělání. Dopracováno bylo ADSL a bezdrátové sítě.
4. **Linková vrstva** – byla vypuštěna obtížná část o van Jacobsonově kompresi IP a TCP záhlaví. Ponechány byly protokoly HDLC, PPP, Ethernet a dokonce i Frame Relay. Dopracovány byly části o WiFi a vrstvě LLC.
5. **IPv4** – všimněte si, že tato kapitola už má ve svém názvu v4. Protokol IPv4 je dnes sice na svém vrcholu, ale z vrcholu jdou cesty jen dolů.
6. **IPv4 adresa** – tato kapitola popisuje tvar IP adres. Kapitola zůstává bez zásadních změn.
7. **Směrování** – tato kapitola se asi nejvíce liší od předchozích vydání. Popisuje detailně nejenom Bellman-Fordův algoritmus, ale i Dijkstrův algoritmus.
8. **IPv6** – kapitola o IP protokolu verze 6 již uvádí příklady z Microsoft Windows Vista, protože od verze Vista je IPv6 standardní součástí Windows.
9. **Protokol TCP** – zde byly zásadně přepracovány obrázky, které byly údajně málo demonstrativní. Doufám, že tentokrát bude laskavý čtenář spokojen.
10. **Protokol UDP** – tento protokol je tak jednoduchý, že toho k němu už mnoho nelze dodat.
11. **DNS** – tato kapitola objasňuje principy a základní termíny DNS.
12. **Protokol DNS** – obsahuje vlastní popis protokolu DNS.
13. **Mezinárodní a národní organizace internetu** – zde čtenář najde informace, jak jsou celosvětově rozděleny internetové IP adresy a domény a kdo je přidělováním těchto světových zdrojů pověřen.
14. **Telnet** – popisuje stejnojmenný aplikační protokol, který je jedním z nejstarších protokolů Internetu.

15. **FTP** – popisuje protokol FTP.
16. **HTTP** – popisuje protokol HTTP.
17. **Elektronická pošta** – tato kapitola objasňuje principy elektronické pošty a následně popisuje protokoly POP3, IMAP4 a SMTP.
18. **Filtrace, proxy a NAT** – popisuje některé bezpečnostní mechanismy TCP/IP.
19. **Firewall** – popisuje využití uvedených bezpečnostních mechanismů TCP/IP pro ochranu vnitřních sítí.

Jak jste si asi všimli, byla přepracována i skladba kapitol. Přibyly kapitoly o filtraci, proxy a firewallu, které původně byly součástí až 2. dílu. Druhý díl se tak zabývá výhradně PKI a tak mohl vyjít pod názvem „Velký průvodce PKI a technologií elektronického podpisu“.

Zatímco první vydání sloužila zejména jako příručky TCP/IP, tak v poslední době se Velký průvodce TCP/IP hojně využívá jako učebnice na vysokých, a dokonce i na středních školách. Proto téměř za každou kapitolou přibily náměty na domácí cvičení.

Českým čtenářům bych chtěl poděkovat za vesměs kladné ohlasy na tuto publikaci. Nemohu ale nevzpomenou na extrémně negativní reakci jednoho australského čtenáře. Velice jej totiž rozlítilo, že to je už myslím 12. učebnice TCP/IP, kterou si koupil, a zase to TCP/IP nepochopil. Pokaždé, když si na tuto zlostnou reakci vzpomenu, tak mi to zlepší náladu. Dokonce mě to povzbudilo, abych připravil toto 5. české vydání. A aby se ten Australan už tolik nezlobil, tak mu posílám klokana – třeba aspoň pozná, co to je za zvíře, i když neumí česky.

Závěrem bych chtěl poděkovat Haně Strakové a Janu Říhovi za velice zodpovědnou revizi a podnětné připomínky. Dále děkuji Vilému Sládkovi, který doplnil informace o sdružení CZ.NIC.

From: Neposílejte mi spamy <[libor.dostalek@siemens.com](mailto:libor.dostalek@siemens.com)>

Date: Mon, 11 Aug 2008 17:17:48 +0200

