

Obsah

O autorech	9
Jim Kurose	9
Keith Ross	9
Předmluva	13
Co je nového v tomto vydání?	13
Cílová skupina čtenářů	14
Čím je tato učebnice jedinečná?	14
Přístup shora dolů	14
Zaměření na Internet	15
Výuka síťových principů	15
Webová stránka	15
Pedagogické funkce	16
Kapitola Závislosti	17
Zpětná vazba	17
Errata	18
Poděkování	18

KAPITOLA 1

Počítačové sítě a Internet	23
1.1 Co je Internet?	24
1.1.1 Popis základních součástí	24
1.1.2 Popis služeb	27
1.1.3 Co je protokol?	28
1.2 Okraj sítě	29
1.2.1 Přístupové sítě	30
1.2.2 Fyzická média	37
1.3 Jádro sítě	39
1.3.1 Přepínání paketů	39
1.3.2 Přepínání okruhů	43
1.3.3 Síť sítí	46
1.4 Zpoždění, ztráta, a propustnost v sítích s přepínáním paketů	49
1.4.1 Přehled zpoždění v sítích s přepínáním paketů	49
1.4.2 Zpoždění fronty a ztráta paketů	52
1.4.3 Zpoždění mezi koncovými uzly	54
1.4.4 Propustnost v počítačových sítích	55
1.5 Vrstvy protokolů a jejich modely služeb	58
1.5.1 Vrstvená architektura	58
1.5.2 Zapouzdření	62
1.6 Sítě pod útokem	64
1.7 Historie počítačových sítí a Internetu	67
1.7.1 Vývoj přepínání paketů: 1961–1972	67
1.7.2 Vlastnické sítě a propojení Internetu: 1972–1980	68

1.7.3 Rozšíření sítí: 1980–1990	69
1.7.4 Internetová exploze: Devadesátá léta	70
1.7.5 Nové tisíciletí	71
1.8 Shrnutí	71

KAPITOLA 2

Aplikační vrstva	85
2.1 Principy síťových aplikací	86
2.1.1 Architektury síťových aplikací	87
2.1.2 Komunikace mezi procesy	89
2.1.3 Transportní služby dostupné aplikacím	91
2.1.4 Transportní služby poskytované Internetem	93
2.1.5 Protokoly aplikační vrstvy	95
2.1.6 Síťové aplikace, zahrnuté v této knize	96
2.2 Web a HTTP	96
2.2.1 Obecný přehled protokolu HTTP	97
2.2.2 Dočasná a trvalá spojení	98
2.2.3 Formát zprávy HTTP	100
2.2.4 Interakce uživatele a serveru: Cookies	104
2.2.5 Webová mezipaměť	106
2.2.6 Podmíněná metoda GET	109
2.3 Přenos souborů: FTP	110
2.3.1 FTP příkazy a odpovědi	111
2.4 Elektronická pošta v Internetu	112
2.4.1 SMTP	113
2.4.2 Srovnání s HTTP	115
2.4.3 Formáty poštovních zpráv	116
2.4.4 Protokoly pro přístup k poště	116
2.5 DNS – internetová adresářová služba	120
2.5.1 Služby poskytované systémem DNS	120
2.5.2 Přehled funkce DNS	122
2.5.3 DNS záznamy a zprávy	126
2.6 Aplikace Peer-to-Peer	130
2.6.1 Distribuce souborů P2P	130
2.6.2 Distribuované hašovací tabulky (DHT)	135
2.7 Programování soketů: Vytváření síťových aplikací	139
2.7.1 Programování soketů s UDP	140
2.7.2 Programování soketů s TCP	143
2.8 Shrnutí	147

KAPITOLA 3

Transportní vrstva	159
3.1 Úvod a služby transportní vrstvy	160
3.1.1 Vztah mezi transportní a síťovou vrstvou	160
3.1.2 Přehled transportní vrstvy na Internetu	162
3.2 Multiplexing a demultiplexing	164
3.3 Nespojovaný transport: UDP	169
3.3.1 Struktura segmentu UDP	171
3.3.2 Kontrolní součet UDP	172
3.4 Principy spolehlivého přenosu dat	173
3.4.1 Budování protokolu pro spolehlivý přenos dat	174
3.4.2 Proudové rotokoly pro spolehlivý přenos dat	181

3.4.3 Go-Back-N (GBN - Opakování s návratem)	183
3.4.4 Selektivní opakování (Selective Repeat, SR)	187
3.5 Přenos orientovaný na spojení: TCP	192
3.5.1 TCP spojení	192
3.5.2 Struktura TCP segmentu	194
3.5.3 Odhad obousměrné cesty (round-trip time, RTT) a timeout	198
3.5.4 Spolehlivý přenos dat	200
3.5.5 Řízení datového toku	207
3.5.6 Správa TCP spojení	208
3.6 Principy kontroly přetížení	213
3.6.1 Příčiny a náklady plynoucí z přetížení	214
3.6.2 Přístupy ke kontrole přetížení	218
3.6.3 Příklad kontroly přetížení pomocí sítě: Kontrola přetížení ATM ABR	219
3.7 Kontrola přetížení TCP	221
3.7.1 Spravedlnost	228
3.8 Shrnutí	230

 KAPITOLA 4

Síťová vrstva	247
4.1 Úvod	248
4.1.1 Předávání a směrování	249
4.1.2 Modely služeb síťové vrstvy	251
4.2 Síť virtuálních okruhů a datagramů	253
4.2.1 Síť virtuálních okruhů	254
4.2.2 Datagramové sítě	256
4.2.3 Počátky VC a datagramových sítí	258
4.3 Co je uvnitř routeru?	258
4.3.1 Vstupní zpracování	260
4.3.2 Přepínání	262
4.3.3 Zpracování výstupu	263
4.3.4 Kdy se provádí řazení do fronty?	264
4.3.5 Řídící úroveň směrování	267
4.4 Internet Protocol (IP): Předávání a adresování v Internetu	267
4.4.1 Formát datagramů	268
4.4.2 Adresování v protokolu IPv4	272
4.4.3 Internet Control Message Protocol (ICMP)	283
4.4.4 IPv6	285
4.4.5 Stručný úvod do zabezpečení IP	289
4.5 Směrovací algoritmy	290
4.5.1 Směrovací algoritmus podle stavu linky (Link-State, LS)	293
4.5.2 Směrovací algoritmus vektoru vzdálenost (Distance-Vector, DV)	296
4.5.3 Hierarchické směrování	302
4.6 Směrování v Internetu	305
4.6.1 Směrování mezi AS v Internetu: RIP	305
4.6.2 Vnitřní směrování AS v Internetu: OSPF	308
4.6.3 Směrování mezi AS: BGP	310
4.7 Skupinové a všesměrové vysílání	316
4.7.1 Všesměrové směrovací algoritmy	316
4.7.2 Multicast (skupinové vysílání)	321
4.8 Shrnutí	327

KAPITOLA 5

Linková vrstva:	
Linky, přístupové sítě a síť LAN	343
5.1 Úvod do linkové vrstvy	344
5.1.1 Služby poskytované linkovou vrstvou	345
5.1.2 Kde je linková vrstva implementována?	346
5.2 Techniky detekce a korekce chyb	347
5.2.1 Kontrola parity	348
5.2.2 Metody kontrolních součtů	350
5.2.3 Cyklická kontrola redundance (CRC)	351
5.3 Linky a protokoly pro vícenásobný přístup	352
5.3.1 Protokoly s dělením kanálu	354
5.3.2 Protokoly s náhodným přístupem	355
5.3.3 Protokoly se střídavým přístupem	362
5.3.4 DOCSIS: The Link-Layer Protocol for Cable Internet Access (Protokol linkové vrstvy pro kabelový přístup k Internetu)	363
5.4 Přepínané lokální sítě	364
5.4.1 Adresování linkové vrstvy a protokol ARP	365
5.4.2 Ethernet	369
5.4.3 Přepínače linkové vrstvy	374
5.4.4 Virtuální lokální sítě (VLAN)	378
5.5 Virtualizace linky: Síť jako linková vrstva	380
5.5.1 Multiprotocol Label Switching (MPLS)	381
5.6 Sítě datových center	383
5.7 Retrospektiva: Den v životě požadavku na webovou stránku	387
5.7.1 Začínáme: DHCP, UDP, IP a Ethernet	388
5.7.2 Stále začínáme: DNS a ARP	389
5.7.3 Stále začínáme: Vnitřní doménové směrování na serveru DNS	390
5.7.4 Interakce webového klienta a serveru: TCP a HTTP	390
5.8 Shrnutí	391

KAPITOLA 6

Bezdrátové a mobilní sítě	401
6.1 Úvod	402
6.2 Charakteristiky bezdrátových linek a sítí	406
6.2.1 Protokol CDMA	408
6.3 WiFi: Bezdrátové síť LAN 802.11	411
6.3.1 Architektura 802.11	411
6.3.2 Protokol MAC 802.11	414
6.3.3 Rámec IEEE 802.11	419
6.3.4 Mobilita v rámci stejné IP podsítě	421
6.3.5 Pokročilé funkce 802.11	422
6.3.6 Osobní síť (Personal Area Networks): Bluetooth a ZigBee	423
6.4 Mobilní přístup k Internetu	425
6.4.1 Přehled architektury mobilních sítí	426
Mobilní datové síť 3G: Rozšíření Internetu na mobilní předplatitele	428
6.4.3 K sítím 4G: LTE	429
6.5 Správa mobility: Principy	431
6.5.1 Adresování	433
6.5.2 Směrování do mobilního uzlu	434
6.6 Mobilní IP	438

6.7 Správa mobility v mobilních sítích	441
6.7.1 Směrování hovorů na mobilní uživatele	442
6.7.2 Předávání řízení v sítích GSM	443
6.8 Bezdrátové sítě a mobilita: Dopad na protokoly vyšší vrstvy	445
6.9 Shrnutí	447

KAPITOLA 7

Multimédia v počítačových sítích **455**

7.1 Multimediální aplikace	456
7.1.1 Vlastnosti videa	456
7.1.2 Vlastnosti zvuku (audio)	457
7.1.3 Typy multimediálních síťových aplikací	458
7.2 Streaming uloženého videa	460
7.2.1 UDP streaming	461
7.2.2 HTTP streaming	462
7.2.3 Adaptivní streaming a DASH	466
7.2.4 Síť pro distribuci obsahu	467
7.2.5 Případové studie: Netflix, YouTube a Kankan	471
7.3 Voice-over-IP	474
7.3.1 Limity služby nejlepší snahy protokolu IP	474
7.3.2 Odstranění chvění na straně příjemce pro přenos zvuku	476
7.3.3 Obnovení po ztrátě paketu	478
7.3.4 Případová studie: VoIP s programem Skype	481
7.4 Protokoly aplikací pro konverzaci v reálném čase	483
7.4.1 RTP	483
7.4.2 SIP	485
7.5 Síťová podpora multimédií	489
7.5.1 Dimenzování sítí se službou nejlepší snahy	491
7.5.2 Poskytování více tříd obsluhy	492
7.5.3 Architektura Diffserv	500
Záruky Quality-of-Service (QoS) pro připojení: Rezervace zdrojů a přijetí volání	503
7.6 Shrnutí	506

KAPITOLA 8

Bezpečnost v počítačových sítích **517**

8.1 Co je to síťová bezpečnost?	518
8.2 Principy kryptografie	520
8.2.1 Kryptografie se symetrickým klíčem	521
8.2.2 Šifrování s veřejným klíčem	526
8.3 Integrita zpráv a digitální podpisy	530
8.3.1 Kryptografické hašovací funkce	531
8.3.2 Ověřovací kód zprávy (Message Authentication Code)	532
8.3.3 Digitální podpisy	533
8.4 Ověřování koncového bodu	538
8.4.1 Autentizační protokol ap1.0	539
8.4.2 Autentizační protokol ap2.0	539
8.4.3 Autentizační protokol ap3.0	540
8.4.4 Autentizační protokol ap3.1	541
8.4.5 Autentizační protokol ap4.0	541
8.5 Zabezpečení e-mailu	542
8.5.1 Bezpečný e-mail	543
8.5.2 PGP	545

8.6 Zabezpečení TCP spojení: SSL	546
8.6.1 Celkový obraz	547
8.6.2 Ještě úplnější obraz	550
8.7 Zabezpečení síťové vrstvy: Protokol IPsec a virtuální privátní síť	551
8.7.1 Protokol IPsec a virtuální privátní síť (VPN)	552
8.7.2 Protokoly AH a ESP	553
8.7.3 Bezpečnostní asociace	553
8.7.4 Datagram protokolu IPsec	554
8.7.5 IKE: Správa klíčů protokolu IPsec	556
8.8 Zabezpečení bezdrátových sítí LAN	557
8.8.1 Wired Equivalent Privacy (WEP)	558
8.8.2 IEEE 802.11i (WPA2)	559
8.9 Provozní bezpečnost: Firewally a systémy detekce průniku	561
8.9.1 Firewally	562
8.9.2 Systémy detekce průniku	567
8.10 Shrnutí	570

 KAPITOLA 9

Správa sítě	581
9.1 Co je to vlastně správa sítě?	582
9.2 Infrastruktura pro správu sítě	585
9.3 Rámec pro správu internetových standardů	588
9.3.1 Struktura informací pro správu (Structure of Management Information, SMI):	589
9.3.2 Informační základna pro správu (Management Information Base, MIB)	591
9.3.3 Provozní a transportní mapování protokolu SNMP	593
9.3.4 Správa zabezpečení	596
9.4 ASN.1	598
9.5 Závěr	600
Webová stránka	605
Rejstřík	607