

Spis treści

Wstęp	13
Rozdział 1. Sieci komputerowe	25
1.1. Podział sieci komputerowych w zależności od rozmiaru	25
1.2. Topologie sieci komputerowych	26
Topologia sieci	26
Topologia fizyczna	26
Topologia logiczna	27
1.3. Model ISO/OSI	28
1.4. Model protokołu TCP/IP	30
Rozdział 2. Rodzaje nośników	35
2.1. Najważniejsze technologie	35
2.2. Przewód koncentryczny	38
Zastosowania sieci 10Base-2	40
2.3. Skrętka UTP	41
Wymagania dla instalacji spełniającej założenia CAT-5	47
Cat-5e — parametry	48
2.4. Światłowód	52
Budowa światłowodu	53
Zasada działania światłowodu	53
Światłowód wielomodowy	53
Światłowód jednomodowy	54
Złącza światłowodowe	55
Standardy transmisji światłowodowych	57
2.5. Okablowanie strukturalne	59
Definicje	59
Normy	60
Projekt i definicje	61
Zalecenia	65
Telefonia	66
Serwerownia	68
Rozdział 3. Warstwa dostępu do sieci — standard Ethernet	73
3.1. Historia	73
3.2. Działanie protokołu	74
Metody transmisji	74
Norma IEEE 802.3	74
Wydajność sieci Ethernet 10 Mb/s	77

3.3. Budowa ramki Ethernet	78
Protokół LLC	80
3.4. Zasady konstruowania sieci Ethernet	82
Reguły dla Ethernetu (10 Mb/s)	82
Reguły dla Fast Ethernetu (100 Mb/s)	86
Reguły dla Gigabit Ethernetu (1 000 Mb/s)	87
3.5. Technologie	88
Full-duplex	88
MAC Control	89
Automatyczne negocjowanie parametrów łącza	89
1000Base-T	90
VLAN — IEEE 802.1q	91
QoS — 802.1p	94
STP (Spanning Tree Protocol)	95
Power over Ethernet	101
Sygnały i kodowanie	102
3.6. Protokół ARP — protokół określania adresów	104
Proxy-ARP	105
Reverse-ARP	105
Zapobieganie zdublowaniu adresów IP	106
Pakiet protokołu ARP	106
Polecenia do manipulacji tablicą ARP	108
3.7. Urządzenia sieciowe działające w warstwie dostępu do sieci	110
Karta sieciowa	110
Modem	110
Transceiver	111
Konwerter nośników	111
Regenerator (repeater)	112
Koncentrator (hub)	112
Most (bridge)	117
Przełącznik (switch)	117

Rozdział 4. Sieci bezprzewodowe	123
802.11	124
802.11b	125
Kanały (channel)	125
802.11a	126
802.11g	126
802.11n	127
Standaryzacja	127
4.1. Struktura sieci WLAN	128
4.2. Kontrola dostępu do medium	130
Mechanizmy transmisji	131
4.3. Ramka 802.11	133
4.4. Działanie protokołu 802.11	138
Skanowanie	138
Przyłączanie	139
Uwierzytelnianie	139
Kojarzenie (powiązanie)	140
Roaming — proces kojarzenia ponownego	141
Oszczędzanie energii	142
Transmisja radiowa	142

4.5. WEP i bezpieczeństwo	143
Problemy z WEP	144
Nowe protokoły bezpieczeństwa WLAN	146
4.6. Pozostałe projekty WLAN	148
4.7. Projektowanie sieci radiowych	149
Rodzaje anten	151
Obliczenia	151
Zalecenia	156
4.8. Konfigurowanie urządzeń	157
Konfiguracja sieciowej karty bezprzewodowej	157
Punkt dostępowy (Access Point)	161
4.9. Kismet	165
4.10. WiMax — 802.16	166

Rozdział 5. Warstwa Internetu 169

5.1. Protokół IP	169
Zadania spełniane przez protokół IP	170
Cechy protokołu IP	170
Budowa datagramu IP	170
5.2. Adresowanie IP	173
Klasy adresów w TCP/IP	177
Bezklasowe routowanie międzydomenowe (CIDR)	178
Adresy specjalne i klasy nieroutowalne	183
Nadawanie adresów IP interfejsowi sieciowemu	184
5.3. Routowanie datagramów IP	188
Tablica routingu	191
Polecenia służące do manipulacji tablicą routingu	193
Routing źródłowy	195
5.4. Protokół ICMP	196
Zadania protokołu ICMP	197
Format nagłówka ICMP	198
Pola Typ i Kod komunikatu ICMP	199
Polecenia wykorzystujące protokół ICMP	202
5.5. IPv6 — wersja szоста protokołu IP	205
Nagłówek IPv6	206
Adres IPv6	207
5.6. Protokoły routingu dynamicznego	208
Protokoły wektora odległości (Distance Vector)	208
Protokoły stanu łącza (Link State)	209
Jak zbudowany jest Internet?	209
5.7. Urządzenia pracujące w warstwie Internetu	214
Router	214

Rozdział 6. Warstwa transportowa 217

6.1. Port, gniazdo	217
6.2. Protokół UDP	219
6.3. Protokół TCP	220
tcpdump	223
netstat	228

Rozdział 7. Usługi warstwy aplikacji 233

7.1. DNS	233
Rejestrowanie własnej domeny	236
Ogólne informacje o serwerach DNS	238

Jak to w rzeczywistości działa?	239
Konfiguracja hosta	240
Rekordy zasobów	244
Serwery DNS	246
Konfiguracja serwera BIND	247
Sterowanie demonem named	255
Kwestie bezpieczeństwa	258
Format komunikatu DNS	262
Programy użytkowe — diagnostyka	264
7.2. SMTP	272
Serwery SMTP	272
Sprawdzanie działania serwera	275
Protokół MIME	282
Bezpieczeństwo	283
7.3. POP	284
Sprawdzanie działania serwera	285
Serwery POP	286
7.4. IMAP	287
Sprawdzanie działania serwera	287
Serwery IMAP	289
7.5. FTP	290
Tryby pracy FTP	290
Komunikacja z serwerem	292
Obsługa programu ftp	293
Serwery	295
Bezpieczeństwo	296
7.6. HTTP	297
Protokół HTTP	297
Sprawdzanie działania serwera HTTP	298
Serwery	299
Bezpieczeństwo	301
7.7. SSL	302
Certyfikaty	303
Uproszczona zasada działania SSL	303
Długość klucza	304
Pakiet stunnel	304
7.8. Telnet	305
7.9. SSH	306
7.10. Finger	307
7.11. Auth	308
7.12. NNTP	308
7.13. SNMP	309
Różnice pomiędzy wersjami SNMP	313
RMON	314
Bezpieczeństwo	316
Testowanie	316
7.14. IRC	318
7.15. Whois	318
7.16. NTP	321
7.17. Syslog	322
7.18. Bootps, DHCP	324
Nagłówki DHCP	325
Pola i ich opisy	325

Proces uzyskiwania konfiguracji	327
Konfiguracja klientów DHCP	328
Serwery DHCP	330
7.19. NetBIOS	334
Wyszukiwanie nazw NetBIOS	337
Optymalizacja	338
Bezpieczeństwo	339
7.20. VoIP	339
SIP	339
H.323	343
7.21. Urządzenia sieciowe pracujące w warstwie aplikacji	344
Komputer	344
Serwer	345

Rozdział 8. Inne protokoły 347

8.1. Token Ring	347
8.2. FDDI	348
8.3. IPX/SPX	351
Budowa pakietu IPX	351
Adresy IPX	353
Protokoły używane w IPX	353
8.4. ISDN	354
8.5. PPP	357
Ramka PPP	358
Dodatkowe możliwości PPP	359
Konfiguracja PPP w Linuksie	359
8.6. xDSL	365
ADSL	366
RADSL	367
SDSL	368
HDSL	368
VDSL	368
IDSL	368
8.7. Frame Relay	368
Opis technologii Frame Relay	369
Zasada działania FR	370
Format ramki Frame Relay	371
Mechanizmy sieci FR	372
Parametry transmisji FR	374
8.8. ATM	375
Właściwości standardu ATM	376
Interfejsy ATM	376
Rodzaje połączeń w sieciach ATM	376
Komórka ATM	377
Usługi ATM	379
Model ATM	380
Klasy ruchu	381
Trasowanie ATM	383
Dodatkowe możliwości sieci ATM	383
8.9. Sieci w gniazdku zasilającym — PLC	384
Topologia sieci PLC	384
Standardy PLC	385
Wady PLC	386

8.10. Sieci telewizji kablowych	387
Standard MCSN/DOCSIS	388
Rozdział 9. Administracja siecią LAN	389
9.1. Projektowanie sieci LAN	390
Struktura fizyczna sieci	390
Struktura logiczna sieci	393
9.2. Rozwiązywanie problemów	396
Poważna awaria	396
Użytkownik	396
Rady	397
Problemy	398
9.3. Narzędzia administratora sieci	401
Sniffery	402
Analizatory sieci	409
Testowanie dostępności usług	418
Skanery bezpieczeństwa	422
Inne narzędzia	429
9.4. Wykorzystanie protokołu SNMP	434
Konfiguracja agenta snmpd	435
Konfiguracja menedżera MRTG	437
9.5. Zarządzalne urządzenia aktywne	441
Rozdział 10. Bezpieczeństwo	443
10.1. Polityka bezpieczeństwa	445
10.2. Najważniejsze pojęcia	449
Firewall	449
NAT	451
Kryptografia	454
VPN	459
IDS	461
Wirusy	466
10.3. Konstrukcja sieci	467
10.4. Rozpoznanie terenu	474
Zbieranie danych	475
Skanowanie	477
Metody ukrywania skanowania	480
Identyfikacja systemu operacyjnego	484
10.5. Metody włamań	489
Uzyskanie dostępu	490
Destabilizacja pracy	497
10.6. Zagrożenia wewnętrzne	502
Wykrywanie snifferów	502
Sposoby omijania przełączników	504
Zasoby	507
10.7. Podsumowanie	508
Zachowanie podczas włamania	508
Rozdział 11. Firewall	511
11.1. Rodzaje firewalli	511
Tradycyjne proxy (Traditional proxies)	511
Przezroczyste proxy (Transparent proxies)	512
Tłumaczenie adresów IP (NAT)	512
Filtrowanie pakietów	512

11.2. Obsługa filtrowania pakietów w Linuksie	513
Rozwiązania komercyjne	515
Ipchains — Linux 2.2	517
Składnia polecenia ipchains	518
Iptables — Linux 2.4	520
11.3. Tworzymy firewall	522
Podstawy	523
Konfiguracja	525
Logi systemowe	531
Problemy z działaniem firewalla	532
Wyłączanie firewalla	532
11.4. Dodatkowe funkcje	533
Ograniczenia na ICMP	533
Jak przepuścić nową usługę	534
Ustawianie priorytetów pakietów	535
Wykrywanie skanowania za pomocą firewalla	537
Wykrywanie NAT	538