

Spis treści

Słowo wstępne	19
Przedmowa do wydania drugiego	21
Przedmowa do wydania pierwszego	27
Rozdział 1. Wprowadzenie	31
1.1. Założenia architektoniczne	32
1.1.1. Pakiety, połączenia i datagramy	33
1.1.2. Zasady „end-to-end argument” i „fate sharing”	35
1.1.3. Kontrola błędów i sterowanie przepływem	37
1.2. Projekt i implementacje	38
1.2.1. Architektura warstwowa	38
1.2.2. Multipleksowanie, demultipleksowanie i enkapsulacja w implementacjach warstwowych	40
1.3. Architektura i protokoły zestawu TCP/IP	43
1.3.1. Model odniesienia ARPANET	43
1.3.2. Multipleksowanie, demultipleksowanie i enkapsulacja w protokołach TCP/IP	46
1.3.3. Numery portów	47
1.3.4. Nazwy, adresy i usługa DNS	49
1.4. Internety, intranety i ekstranety	50
1.5. Projektowanie aplikacji	51
1.5.1. Architektura klient-serwer	51
1.5.2. Architektura peer-to-peer	52
1.5.3. Interfejsy programisty (API)	52
1.6. Procesy standaryzacyjne	53
1.6.1. Dokumenty RFC (Request for Comments)	54
1.6.2. Inne standardy	54
1.7. Implementacje TCP/IP i ich dystrybucja	55
1.8. Ataki wymierzone w architekturę Internetu	55
1.9. Podsumowanie	57
1.10. Bibliografia	59
Rozdział 2. Architektura adresów internetowych	63
2.1. Wprowadzenie	63
2.2. Zapisywanie adresów IP	64
2.3. Podstawowa struktura adresu IP	66
2.3.1. Klasy adresów IP	66
2.3.2. Adresowanie podsieci	68
2.3.3. Maski podsieci	70

2.3.4.	Zmienna długość maski podsieci (VLSM)	72
2.3.5.	Adresy rozgłoszeniowe (broadcast)	73
2.3.6.	Adresy IPv6 i identyfikatory interfejsów	74
2.4.	CIDR i agregacja	77
2.4.1.	Prefiksy	77
2.4.2.	Agregowanie prefiksów	78
2.5.	Adresy specjalnego znaczenia	81
2.5.1.	Translatory IPv4/IPv6	83
2.5.2.	Adresy grupowe (multicast)	84
2.5.3.	Multicasting w IPv4	85
2.5.4.	Multicasting w IPv6	87
2.5.5.	Adresy anycast	92
2.6.	Przydzielanie adresów IP	93
2.6.1.	Adresy unicast	93
2.6.2.	Adresy multicast	96
2.7.	Przypisywanie adresów unicast do węzłów sieci	96
2.7.1.	Jeden dostawca, jeden komputer, jeden adres	97
2.7.2.	Jeden dostawca, jedna sieć, jeden adres	97
2.7.3.	Jeden dostawca, wiele sieci, wiele adresów	98
2.7.4.	Wielu dostawców, wiele sieci, wiele adresów (multihoming)	99
2.8.	Ataki z wykorzystaniem adresów IP	101
2.9.	Podsumowanie	102
2.10.	Bibliografia	103
Rozdział 3.	Warstwa łącza danych	109
3.1.	Wprowadzenie	109
3.2.	Ethernet i standardy IEEE 802 LAN/MAN	109
3.2.1.	Standardy sieci LAN/MAN IEEE 802	112
3.2.2.	Format ramki ethernetowej	114
3.2.3.	802.1p/Q sieci wirtualne i znaczniki QoS	119
3.2.4.	802.1AX: agregowanie łączy (dawniej 802.3ad)	122
3.3.	Pełny duplex, oszczędzanie energii, autonegociowanie i sterowanie przepływem 802.1X	123
3.3.1.	Niezgodność duplexowa	125
3.3.2.	Wybudzanie przez sieć (WoL), oszczędzanie energii i magiczne pakiety	126
3.3.3.	Sterowanie przepływem w warstwie łącza danych	126
3.4.	Mostki a przełączniki	128
3.4.1.	Protokół drzewa rozpinającego (STP)	131
3.4.2.	802.1ak: protokół wielorejestacyjny (MRP)	140
3.5.	Bezprzewodowe sieci LAN — IEEE 802.11 (Wi-Fi)	141
3.5.1.	Ramki standardu 802.11	142
3.5.2.	Tryb oszczędzania energii i funkcja synchronizacji czasu (TSF)	148
3.5.3.	Sterowanie dostępem do nośnika w sieciach 802.11	149
3.5.4.	Parametry warstwy fizycznej: szybkości, kanały i częstotliwości	153
3.5.5.	Bezpieczeństwo Wi-Fi	159
3.5.6.	802.11s — sieci kratowe Wi-Fi	161
3.6.	Protokół „punkt-punkt” (PPP)	161
3.6.1.	Protokół sterowania łączem (LCP)	162
3.6.2.	Wielołączone PPP (Multilink PPP)	169
3.6.3.	Protokół sterowania kompresją (CCP)	171
3.6.4.	Uwierzytelnianie PPP	172

	3.6.5. Protokoły sterowania siecią (NCP)	173
	3.6.6. Kompresja nagłówków	174
	3.6.7. Przykład	175
	3.7. Pętla zwrotna	177
	3.8. MTU protokołu i MTU ścieżki (PMTU)	180
	3.9. Podstawy tunelowania	180
	3.9.1. Łączy jednokierunkowe	185
	3.10. Ataki na warstwę łącza danych	186
	3.11. Podsumowanie	188
	3.12. Bibliografia	190
Rozdział 4.	Protokół ARP	197
	4.1. Wprowadzenie	197
	4.2. Przykład	198
	4.2.1. Dostarczanie bezpośrednie i ARP	198
	4.3. Tablice ARP cache	200
	4.4. Format ramki ARP	201
	4.5. Przykłady użycia ARP	203
	4.5.1. Typowy przypadek	203
	4.5.2. Zapytanie ARP o nieistniejący host	205
	4.6. Przetknięcie danych ARP	205
	4.7. Proxy ARP	206
	4.8. Gratuitous ARP i wykrywanie konfliktu adresów IP	206
	4.9. Polecenie arp	209
	4.10. Przypisywanie adresów IPv4 za pomocą ARP	209
	4.11. Ataki sieciowe z użyciem ARP	210
	4.12. Podsumowanie	210
	4.13. Bibliografia	211
Rozdział 5.	Protokół internetowy (IP)	213
	5.1. Wprowadzenie	213
	5.2. Nagłówki IPv4 i IPv6	215
	5.2.1. Pola nagłówków IP	215
	5.2.2. Internetowa suma kontrolna	219
	5.2.3. Pola DS i ECN (dawniej ToS i Klasa ruchu)	221
	5.2.4. Opcje IP	225
	5.3. Nagłówki rozszerzeń IPv6	228
	5.3.1. Opcje IPv6	230
	5.3.2. Nagłówek trasowania	234
	5.3.3. Nagłówek fragmentacji	237
	5.4. Forwardowanie datagramów IP	242
	5.4.1. Tablica forwardowania	243
	5.4.2. Szczegóły forwardowania	244
	5.4.3. Przykłady	244
	5.4.4. Dyskusja	249
	5.5. Mobilny IP	249
	5.5.1. Model podstawowy — tunelowanie dwukierunkowe	250
	5.5.2. Optymalizacja trasy (RO)	251
	5.5.3. Dyskusja	254
	5.6. Przetwarzanie datagramów IP przez host	254
	5.6.1. Modele hosta	254
	5.6.2. Selekcja adresów	256

5.7.	Ataki wykorzystujące protokół IP	260
5.8.	Podsumowanie	261
5.9.	Bibliografia	262
Rozdział 6.	Konfigurowanie systemu: DHCP i autokonfiguracja	267
6.1.	Wprowadzenie	267
6.2.	Dynamic Host Configuration Protocol (DHCP)	268
6.2.1.	Pule i dzierżawienie adresów	269
6.2.2.	Format komunikatów DHCP i BOOTP	270
6.2.3.	Opcje DHCP i BOOTP	272
6.2.4.	Operacje protokołu DHCP	274
6.2.5.	DHCPv6	285
6.2.6.	Przełączniki DHCP	298
6.2.7.	Uwierzytelnianie DHCP	303
6.2.8.	Rozszerzenie rekonfiguracji	304
6.2.9.	Opcja Rapid Commit	305
6.2.10.	Informacja o lokalizacji	305
6.2.11.	Informacje dla urządzeń mobilnych (MoS i ANDSF)	306
6.2.12.	Podsłuchiwanie DHCP	307
6.3.	Bezstanowe konfigurowanie adresów (SLAAC)	307
6.3.1.	Dynamiczne konfigurowanie adresów IPv4 lokalnych dla łącza	308
6.3.2.	Procedura SLAAC dla adresów IPv6 lokalnych dla łącza	308
6.4.	Współdziałanie DHCP i DNS	315
6.5.	PPP przez Ethernet (PPPoE)	316
6.6.	Ataki ukierunkowane na konfigurowanie systemu	321
6.7.	Podsumowanie	322
6.8.	Bibliografia	323
Rozdział 7.	Firewalles i translacja adresów sieciowych (NAT)	329
7.1.	Wprowadzenie	329
7.2.	Firewalles	330
7.2.1.	Firewalles filtrujące pakiety	330
7.2.2.	Firewalles proxy	331
7.3.	Translacja adresów sieciowych	333
7.3.1.	NAT podstawowe i NAPT	335
7.3.2.	Klasy behawioralne translacji adresów i portów	341
7.3.3.	Zachowanie filtracyjne NAT	344
7.3.4.	Serwery w lokalnej domenie adresowej	345
7.3.5.	Upinanie ruchu — pętla zwrotna NAT	345
7.3.6.	Edytory NAT	346
7.3.7.	SPNAT — NAT w infrastrukturze dostawcy	347
7.4.	Omijanie NAT	347
7.4.1.	Otworki i wybijanie dziur	348
7.4.2.	Jednostronne fiksowanie adresów (UNSAF)	349
7.4.3.	Omijanie NAT za pomocą STUN	350
7.4.4.	Omijanie NAT z użyciem przełączników (TURN)	356
7.4.5.	ICE — interaktywne nawiązywanie połączenia	362
7.5.	Konfigurowanie NAT i firewali filtrujących	364
7.5.1.	Reguły firewala	364
7.5.2.	Reguły NAT	366
7.5.3.	Bezpośrednia interakcja z NAT i firewallami — UPnP, NAT-PMP i PCP	368

7.6.	Migracja na adresy IPv6 i współistnienie adresów IPv4/IPv6 z wykorzystaniem NAT	369
7.6.1.	Dualny stos TCP/IP (DS-Lite)	369
7.6.2.	Translacja między IPv4 a IPv6 przy użyciu NAT i ALG	370
7.7.	Ataki na firewallo i NAT	375
7.8.	Podsumowanie	376
7.9.	Bibliografia	378
Rozdział 8.	ICMPv4 i ICMPv6 — Internet Control Message Protocol	383
8.1.	Wprowadzenie	383
8.1.1.	Encapsulowanie komunikatów ICMP w datagramach IPv4 i IPv6	384
8.2.	Komunikaty ICMP	386
8.2.1.	Komunikaty ICMPv4	386
8.2.2.	Komunikaty ICMPv6	388
8.2.3.	Przetwarzanie komunikatów ICMP	391
8.3.	Komunikaty ICMP o błędach	392
8.3.1.	Rozszerzenia ICMP i komunikaty wieloczęściowe	394
8.3.2.	Komunikat Destination Unreachable (typ 3 w ICMPv4, typ 1 w ICMPv6)	395
8.3.3.	Komunikat Redirect (typ 5 w ICMPv4, typ 137 w ICMPv6)	403
8.3.4.	Komunikat ICMP Time Exceeded (typ 11 w ICMPv4, typ 3 w ICMPv6)	406
8.3.5.	Komunikat Parameter Problem (typ 12 w ICMPv4, typ 4 w ICMPv6)	408
8.4.	Komunikaty informacyjne ICMP	410
8.4.1.	Komunikaty Echo Request/Reply (ping) (typy 0/8 w ICMPv4, typy 129/128 w ICMPv6)	411
8.4.2.	Odnajdywanie routerów: komunikaty Router Solicitation i Router Advertisement (typy 9 i 10 w ICMPv4)	413
8.4.3.	Komunikaty Home Agent Address Discovery Request/Reply (typy 144/145 w ICMPv6)	416
8.4.4.	Komunikaty Mobile Prefix Solicitation/Advertisement (typy 146/147 w ICMPv6)	416
8.4.5.	Komunikaty szybkiego przełączenia w mobilnych IPv6 (typ 154 w ICMPv6)	417
8.4.6.	Komunikaty Multicast Listener Query/Report/Done (typy 130/131/132 w ICMPv6)	418
8.4.7.	Wersja 2 komunikatu Multicast Listener Discovery (MLDv2) (typ 143 w ICMPv6)	420
8.4.8.	Komunikaty Multicast Router Discovery (MRD) (typy 48/49/50 w IGMP, typy 151/152/153 w ICMPv6)	423
8.5.	Odnajdywanie sąsiadów w IPv6	425
8.5.1.	Komunikaty ICMPv6 Router Solicitation i Router Advertisement (typy 133 i 134)	426
8.5.2.	Komunikaty ICMPv6 Neighbor Solicitation i Neighbor Advertisement (typy 135 i 136)	428
8.5.3.	Komunikaty ICMPv6 Inverse Neighbor Discovery Solicitation/Advertisement (typy 141 i 142)	431
8.5.4.	Wykrywanie nieosiągalności sąsiadów (NUD)	432
8.5.5.	Bezpieczne odnajdywanie sąsiadów (SEND)	433
8.5.6.	Opeje komunikatów odnajdywania sąsiadów	438
8.6.	Translacja komunikatów między ICMPv4 a ICMPv6	454
8.6.1.	Translacja z ICMPv4 na ICMPv6	454
8.6.2.	Translacja z ICMPv6 na ICMPv4	457

	8.7. Ataki wykorzystujące ICMP	459
	8.8. Podsumowanie	461
	8.9. Bibliografia	462
Rozdział 9.	Broadcasting i lokalny multicasting	467
	9.1. Wprowadzenie	467
	9.2. Broadcasting	468
	9.2.1. Adresy rozgłoszeniowe	468
	9.2.2. Rozsyłanie datagramów rozgłoszeniowych	470
	9.3. Multicasting	472
	9.3.1. Konwersja adresów grupowych IP na adresy MAC IEEE-802	473
	9.3.2. Przykłady	475
	9.3.3. Rozsyłanie datagramów multicastingu	477
	9.3.4. Odbieranie datagramów multicastingu	478
	9.3.5. Filtrowanie adresów przez host	480
	9.4. Protokoły IGMP i MLD	482
	9.4.1. Przetwarzanie komunikatów IGMP i MLD przez hosty	486
	9.4.2. Funkcjonowanie routerów multicast	488
	9.4.3. Przykłady	491
	9.4.4. Protokoły LW-IGMPv3 i LW-MLDv2	495
	9.4.5. Niezawodność IGMP i MLD	496
	9.4.6. Zmienne i liczniki protokołów IGMP i MLD	498
	9.4.7. Podshuchiwanie IGMP/MLD w warstwie 2	498
	9.5. Ataki wykorzystujące IGMP i MLD	500
	9.6. Podsumowanie	501
	9.7. Bibliografia	502
Rozdział 10.	Protokół datagramów użytkownika (UDP) oraz fragmentacja IP ...	505
	10.1. Wprowadzenie	505
	10.2. Nagłówki UDP	506
	10.3. Suma kontrolna	507
	10.4. Przykłady	510
	10.5. Datagramy UDP w sieciach IPv6	513
	10.5.1. Teredo — tunelowanie datagramów IPv6 w sieciach IPv4	514
	10.6. UDP-Lite	519
	10.7. Fragmentacja	520
	10.7.1. Przykład — fragmentacja datagramów UDP/IPv4	521
	10.7.2. Maksymalny czas odtwarzania datagramu	524
	10.8. Ustalanie parametru MTU trasy w protokole UDP	525
	10.8.1. Przykład	525
	10.9. Zależność między fragmentacją IP i procesem ARP/ND	528
	10.10. Maksymalny rozmiar datagramu UDP	529
	10.10.1. Ograniczenia implementacyjne	529
	10.10.2. Obcinanie datagramów	530
	10.11. Budowa serwera UDP	530
	10.11.1. Adresy IP i numery portów UDP	531
	10.11.2. Ograniczenie użycia lokalnych adresów IP	532
	10.11.3. Wykorzystanie wielu adresów	533
	10.11.4. Ograniczenie zdalnych adresów IP	534
	10.11.5. Wiele serwerów na jednym porcie	535
	10.11.6. Objęcie dwóch rodzin adresów — IPv4 i IPv6	536
	10.11.7. Brak mechanizmów sterowania przepływem i przeciążeniami	536

10.12.	Translacja datagramów UDP/IPv4 i UDP/IPv6	537
10.13.	UDP w Internecie	538
10.14.	Ataki z użyciem protokołu UDP i fragmentacji IP	539
10.15.	Podsumowanie	540
10.16.	Bibliografia	540
Rozdział 11.	Odwzorowanie nazw i system nazw domenowych (DNS)	543
11.1.	Wprowadzenie	543
11.2.	Przebieg 11.2.1. Składnia nazw DNS	544
11.3.	Serwery nazw i strefy	548
11.4.	Buforowanie	549
11.5.	Protokół DNS	551
11.5.1.	Format komunikatu DNS	553
11.5.2.	Format rozszerzenia DNS (EDNS0)	557
11.5.3.	Protokół UDP czy TCP?	557
11.5.4.	Format sekcji zapytania i sekcji strefy	558
11.5.5.	Format odpowiedzi, pełnomocnictw oraz informacji dodatkowych	559
11.5.6.	Typy rekordów zasobów	560
11.5.7.	Dynamiczne aktualizacje DNS	587
11.5.8.	Transfer strefy i operacja DNS NOTIFY	590
11.6.	Listy sortowania, algorytm karuzelowy i dzielony DNS	597
11.7.	Otwarte serwery DNS i system DynDNS	598
11.8.	Przezroczystość i rozszerzalność	599
11.9.	Translacja komunikatów DNS IPv4 na IPv6 (DNS64)	600
11.10.	Protokoły LLMNR i mDNS	601
11.11.	Usługa LDAP	601
11.12.	Ataki na usługi DNS	602
11.13.	Podsumowanie	603
11.14.	Bibliografia	604
Rozdział 12.	TCP — protokół sterowania transmisją (zagadnienia wstępne)	611
12.1.	Wprowadzenie	611
12.1.1.	ARQ i retransmisja	612
12.1.2.	Okna pakietów i okna przesuwne	614
12.1.3.	Okna o zmiennym rozmiarze: sterowanie przepływem i kontrola przeciążenia	615
12.1.4.	Ustalanie czasu oczekiwania na retransmisję	616
12.2.	Wprowadzenie do TCP	617
12.2.1.	Model usług TCP	617
12.2.2.	Niezawodność w TCP	618
12.3.	Nagłówek TCP i enkapsulacja	620
12.4.	Podsumowanie	623
12.5.	Bibliografia	624
Rozdział 13.	Zarządzanie połączeniem TCP	627
13.1.	Wprowadzenie	627
13.2.	Ustanawianie i kończenie połączenia TCP	627
13.2.1.	Częściowe zamknięcie połączenia TCP	630
13.2.2.	Jednoczesne otwarcie i jednoczesne zamknięcie	631
13.2.3.	Początkowy numer sekwencyjny (ISN)	633
13.2.4.	Przykład	634
13.2.5.	Wygaśnięcie czasu oczekiwania na ustanowienie połączenia	636
13.2.6.	Połączenia a translatory adresów	637

	13.3. Opcje TCP	637
	13.3.1. Opcja maksymalnego rozmiaru segmentu (MSS)	639
	13.3.2. Opcje selektywnego potwierdzenia (SACK)	639
	13.3.3. Opcja skalowania rozmiaru okna (WSCALE lub WSOPT)	640
	13.3.4. Opcja znaczników czasu i ochrona przed przepelnieniem numeru sekwencyjnego (PAWS)	641
	13.3.5. Opcja czasu oczekiwania użytkownika (UTO)	643
	13.3.6. Opcja uwierzytelniania (TCP-AO)	644
	13.4. Odkrywanie MTU ścieżki w protokole TCP	645
	13.4.1. Przykład	646
	13.5. Przejścia między stanami protokołu TCP	649
	13.5.1. Diagram stanów protokołu TCP	649
	13.5.2. Stan TIME_WAIT (oczekiwanie 2MSL)	651
	13.5.3. Pojęcie czasu ciszy	657
	13.5.4. Stan FIN_WAIT	657
	13.5.5. Przejścia odpowiadające jednoczesnemu otwarciu i jednoczesnemu zamknięciu	658
	13.6. Segmenty RST	658
	13.6.1. Żądanie połączenia z nieistniejącym hostem	658
	13.6.2. Przerwanie połączenia	659
	13.6.3. Połączenia częściowo otwarte	661
	13.6.4. TIME_WAIT Assassination (TWA)	663
	13.7. Działanie serwera TCP	664
	13.7.1. Numery portów TCP	664
	13.7.2. Ograniczanie lokalnych adresów IP	666
	13.7.3. Ograniczanie obcych punktów końcowych	667
	13.7.4. Kolejka połączeń przychodzących	668
	13.8. Ataki związane z zarządzaniem połączeniem TCP	672
	13.9. Podsumowanie	675
	13.10. Bibliografia	676
	Rozdział 14. Przerwanie i retransmisja w TCP	679
	14.1. Wprowadzenie	679
	14.2. Prosty przykład przerwania i retransmisji	680
	14.3. Ustalanie czasu oczekiwania na retransmisję (RTO)	682
	14.3.1. Metoda klasyczna	683
	14.3.2. Metoda standardowa	684
	14.3.3. Metoda systemu Linux	689
	14.3.4. Działanie estymatorów RTT	693
	14.3.5. Odporność procedury RTTM na utratę i zmianę kolejności pakietów	694
	14.4. Retransmisje na podstawie licznika czasu	696
	14.4.1. Przykład	697
	14.5. Szybka retransmisja	698
	14.5.1. Przykład	699
	14.6. Retransmisja z potwierzzeniami selektywnymi	703
	14.6.1. Zachowanie odbiorcy obsługującego opcję SACK	704
	14.6.2. Zachowanie nadawcy obsługującego opcję SACK	704
	14.6.3. Przykład	705
	14.7. Falszywe przerwanie i zbędne retransmisje	708
	14.7.1. Rozszerzenie Duplicate SACK (DSACK)	709
	14.7.2. Algorytm wykrywania Eifel	710
	14.7.3. Odtwarzanie Forward-RTO (F-RTO)	711
	14.7.4. Algorytm odpowiedzi Eifel	712

14.8.	Zmiana kolejności i powielanie pakietów	714
14.8.1.	Zmiana kolejności pakietów	714
14.8.2.	Powielanie pakietów	716
14.9.	Mierniki punktu docelowego	717
14.10.	Przepakietowanie	718
14.11.	Ataki związane z mechanizmem retransmisji protokołu TCP	719
14.12.	Podsumowanie	720
14.13.	Bibliografia	721
Rozdział 15.	Przepływ danych i zarządzanie oknem w protokole TCP	723
15.1.	Wprowadzenie	723
15.2.	Komunikacja interaktywna	724
15.3.	Potwierdzenia opóźnione	727
15.4.	Algorytm Nagle'a	728
15.4.1.	Interakcja opóźnionych potwierdzeń ACK i algorytmu Nagle'a	731
15.4.2.	Wyłączenie algorytmu Nagle'a	731
15.5.	Stercowanie przepływem i zarządzanie oknem	732
15.5.1.	Okna przesuwne	733
15.5.2.	Okna zerowe i licznik czasu przetrwania w protokole TCP	736
15.5.3.	Syndrom głupiego okna (SWS)	739
15.5.4.	Duże bufor i automatyczne dostrajanie okna	747
15.6.	Mechanizm pilnych danych	751
15.6.1.	Przykład	752
15.7.	Ataki dotyczące zarządzania oknem	754
15.8.	Podsumowanie	755
15.9.	Bibliografia	756
Rozdział 16.	Kontrola przeciążenia w protokole TCP	759
16.1.	Wprowadzenie	759
16.1.1.	Wykrywanie przeciążenia w protokole TCP	760
16.1.2.	Spowolnienie nadawcy w protokole TCP	761
16.2.	Algorytmy klasyczne	762
16.2.1.	Powolny start	764
16.2.2.	Unikanie przeciążenia	766
16.2.3.	Wybór między algorytmami powolnego startu i unikania przeciążenia	769
16.2.4.	Algorytmy Tahoe, Reno i szybkie odtwarzanie	770
16.2.5.	Standardowy protokół TCP	771
16.3.	Ewolucja algorytmów standardowych	772
16.3.1.	NewReno	772
16.3.2.	Kontrola przeciążenia w TCP z użyciem opcji SACK	773
16.3.3.	Potwierdzenie generowane w przód (FACK) i zmniejszanie szybkości transmisji o połowę	774
16.3.4.	Algorytm ograniczonej transmisji	776
16.3.5.	Walidacja okna przeciążenia (CWV)	776
16.4.	Obsługa zbędnych retransmisji — algorytm odpowiedzi Eifel	777
16.5.	Rozszerzony przykład	779
16.5.1.	Działanie procedury powolnego startu	783
16.5.2.	Przerwa w działaniu nadawcy i lokalne przeciążenie (zdarzenie 1.)	784
16.5.3.	Przeciągnięte potwierdzenia ACK i odtwarzanie po lokalnym przeciążeniu	789
16.5.4.	Szybka retransmisja i odtwarzanie z wykorzystaniem opcji SACK (zdarzenie 2.)	792

	16.5.5. Kolejne zdarzenia lokalnego przeciężenia i szybkiej retransmisji	795
	16.5.6. Przerzucenie stanu, retransmisje i wycofywanie zmian okna cwnd	797
	16.5.7. Zakończenie połączenia	801
	16.6. Współdzielenie stanu przeciężenia	802
	16.7. Przyjazność protokołu TCP	802
	16.8. TCP w szybkich środowiskach	804
	16.8.1. Protokół HighSpeed TCP (HSTCP) i ograniczony powolny start	805
	16.8.2. Kontrola przeciężenia z binarnym zwiększaniem okna (BIC i CUBIC)	807
	16.9. Kontrola przeciężenia oparta na opóźnieniu	811
	16.9.1. Vegas	812
	16.9.2. FAST	813
	16.9.3. Protokoły TCP Westwood i TCP Westwood+	814
	16.9.4. Protokół Compound TCP	814
	16.10. Rozdzielenie buforów	816
	16.11. Aktywne zarządzanie kolejkami i znacznik ECN	818
	16.12. Ataki związane z kontrolą przeciężenia protokołu TCP	820
	16.13. Podsumowanie	822
	16.14. Bibliografia	824
	Rozdział 17. Mechanizm podtrzymania aktywności w protokole TCP	829
	17.1. Wprowadzenie	829
	17.2. Opis	831
	17.2.1. Przykłady dotyczące podtrzymania aktywności	833
	17.3. Ataki związane z mechanizmem podtrzymania aktywności protokołu TCP	838
	17.4. Podsumowanie	839
	17.5. Bibliografia	839
	Rozdział 18. Bezpieczeństwo — EAP, IPsec, TLS, DNSSEC oraz DKIM	841
	18.1. Wprowadzenie	841
	18.2. Bezpieczeństwo informacji — podstawowe założenia	842
	18.3. Zagrożenia w komunikacji sieciowej	843
	18.4. Podstawowe mechanizmy kryptograficzne i zabezpieczające	845
	18.4.1. Systemy kryptograficzne	845
	18.4.2. Szyfrowanie RSA — Rivest, Shamir i Adleman	848
	18.4.3. Metoda uzgadniania kluczy Diffie-Hellman-Merkle (znana również jako algorytm Diffiego-Hellmana lub DH)	849
	18.4.4. Szyfrowanie z uwierzytelnieniem i kryptografia krzywych eliptycznych (ECC)	850
	18.4.5. Wyznaczanie kluczy i doskonała poufność przekazu (PFS)	851
	18.4.6. Liczby pseudolosowe, generatory i rodziny funkcji	851
	18.4.7. Wartości jednorazowe i zaburzające	852
	18.4.8. Kryptograficzne funkcje skrótu	853
	18.4.9. Kody uwierzytelniania wiadomości (MAC, HMAC, CMAC i GMAC)	854
	18.4.10. Zestawy algorytmów kryptograficznych	855
	18.5. Certyfikaty, urzędy certyfikacji (CA) i infrastruktura PKI	858
	18.5.1. Certyfikaty kluczy publicznych, urzędy certyfikacji i standard X.509	859
	18.5.2. Walidacja i unieważnianie certyfikatów	865
	18.5.3. Certyfikaty atrybutów	868
	18.6. Protokoły bezpieczeństwa stosu TCP/IP i podział na warstwy	868
	18.7. Kontrola dostępu do sieci — 802.1X, 802.1AE, EAP i PANA	870
	18.7.1. Metody EAP i wyznaczanie klucza	874
	18.7.2. Protokół ponownego uwierzytelnienia (ERP)	876

18.7.3. Protokół przenoszenia danych uwierzytelniających w dostępie do sieci (PANA)	876
18.8. Bezpieczeństwo warstwy 3. (IPsec)	877
18.8.1. Protokół wymiany kluczy w Internecie (IKEv2)	880
18.8.2. Protokół AH	892
18.8.3. Protokół ESP	896
18.8.4. Multiemisja	902
18.8.5. Protokoły L2TP/IPsec	903
18.8.6. IPsec i funkcja NAT	904
18.8.7. Przykład	906
18.9. Bezpieczeństwo warstwy transportowej (TLS i DTLS)	915
18.9.1. TLS 1.2	916
18.9.2. Protokół TLS do obsługi datagramów (DTLS)	929
18.10. Bezpieczeństwo protokołu DNS (DNSSEC)	934
18.10.1. Rekordy zasobów DNSSEC	935
18.10.2. Działanie mechanizmu DNSSEC	941
18.10.3. Uwierzytelnianie transakcji (TSIG, TKEY oraz SIG(0))	950
18.10.4. DNSSEC z protokołem DNS64	953
18.11. Identyfikowanie poczty za pomocą kluczy domenowych (DKIM)	954
18.11.1. Sygnatury DKIM	954
18.11.2. Przykład	955
18.12. Ataki na protokoły zabezpieczeń	957
18.13. Podsumowanie	958
18.14. Bibliografia	961

Słownik akronimów	973
--------------------------------	------------

Skorowidz	1013
------------------------	-------------

Czytając kolejno rozdziały tej książki, nie sposób oprzeć się wrażeniu podziwu wywołującego z faktu, że początkowo niewielki zbiór usługowa przetrwał koncepcji, wykorzystywanych w świecie sieciach, ewoluowała i jako rezultat spełnienia szeregu nowych wymagań, przetrwała aż do lat czterdziestych, kiedy to...

