

SPIS TREŚCI

O autorach	13
Przedmowa	15

■ CZĘŚĆ PIERWSZA: WPROWADZENIE

ROZDZIAŁ 1

Wprowadzenie do komunikacji danych	19
---	-----------

1.1. Wstęp	20
1.2. Sieci komunikacji danych	22
1.2.1. Komponenty sieci	25
1.2.2. Typy sieci	26
1.3. Modele sieci	28
1.3.1. Model referencyjny OSI	28
1.3.2. Model internetowy	31
1.3.3. Transmisja komunikatu przez warstwy	32
1.3.4. Zalety i wady modelu warstwowego	35
1.4. Standardy sieciowe	36
1.4.1. Znaczenie standardów	36
1.4.2. Proces standaryzacyjny	36
1.4.3. Powszechne standardy	39
1.5. Trendy przyszłościowe	40
1.5.1. Bezprzewodowe sieci LAN i BYOD	40
1.5.2. Internet rzeczy	41
1.5.3. Masywność online	43
1.6. Implikacje dla cyberbezpieczeństwa	44

■ CZĘŚĆ DRUGA: FUNDAMENTALNE KONCEPCJE

ROZDZIAŁ 2

Warstwa aplikacyjna	55
2.1. Wstęp	56
2.2. Typy architektur aplikacji	56
2.2.1. Architektura z centralnym hostem	58
2.2.2. Architektura kliencka	59
2.2.3. Odmiany architektury klient-serwer	60
2.2.4. Architektury chmurowe	64
2.2.5. Architektura peer-to-peer	67
2.2.6. Wybór właściwej architektury	68
2.3. Sieć Web	69
2.3.1. Tak działa sieć Web	69
2.3.2. Wewnątrz ządania HTTP	71
2.3.3. Wewnątrz odpowiedzi HTTP	72
2.4. Poczta elektroniczna	74
2.4.1. Tak działa poczta elektroniczna	74
2.4.2. Wewnątrz pakietu SMTP	79
2.4.3. Załączniki i MIME	79
2.5. Inne aplikacje	80
2.5.1. Telnet	80
2.5.2. Komunikatory internetowe	80
2.5.3. Wideokonferencje	82
2.6. Implikacje dla cyberbezpieczeństwa	85

ROZDZIAŁ 3

Warstwa fizyczna	97
3.1. Wstęp	98
3.2. Obwody	100
3.2.1. Konfigurowanie obwodu	100
3.2.2. Przepływ danych	101
3.2.3. Multipleksowanie	102
3.3. Nośniki transmisyjne	106
3.3.1. Skrętka	106
3.3.2. Kabel koncentryczny	107
3.3.3. Światłowód	107
3.3.4. Radio	109
3.3.5. Mikrofale	110
3.3.6. Satelity	111
3.3.7. Wybór nośnika	112

3.4. Cyfrowa transmisja danych cyfrowych	113
3.4.1. Kodowanie	114
3.4.2. Tryby transmisji	115
3.4.3. Transmisja cyfrowa	116
3.4.4. Transmisja danych przez ethernet	118
3.5. Analogowa transmisja danych cyfrowych	119
3.5.1. Modulacja	120
3.5.2. Przepustowość obwodu	122
3.5.3. Transmisja modemowa	123
3.6. Cyfrowa transmisja danych analogowych	124
3.6.1. Digitalizacja sygnału	124
3.6.2. Rozmowy telefoniczne	126
3.6.3. Komunikatory internetowe	127
3.6.4. VoIP	127
3.7. Implikacje dla cyberbezpieczeństwa	128

ROZDZIAŁ 4

Warstwa łączy danych 141

4.1. Wstęp	142
4.2. Sterowanie dostępem do nośnika	143
4.2.1. Rywalizacja	143
4.2.2. Nadzorowany dostęp	143
4.2.3. Porównanie metod	144
4.3. Kontrola błędów	145
4.3.1. Źródła błędów	146
4.3.2. Zapobieganie błędom	148
4.3.3. Wykrywanie błędów	149
4.3.4. Retransmisja pakietu	151
4.3.5. Progresywna korekcja błędów	151
4.3.6. Kontrola błędów w praktyce	153
4.4. Protokoły warstwy łączy danych	154
4.4.1. Transmisja asynchroniczna	154
4.4.2. Transmisja synchroniczna	155
4.5. Efektywność transmisji	159
4.6. Implikacje dla cyberbezpieczeństwa	162

ROZDZIAŁ 5

Warstwy sieciowa i transportowa 173

5.1. Wstęp	174
5.2. Protokoły warstw transportowej i sieciowej	176
5.2.1. TCP — protokół sterowania transmisją	177
5.2.2. IP — protokół internetowy	177

5.3. Funkcje warstwy transportowej	180
5.3.1. Łączność z warstwą aplikacyjną	180
5.3.2. Segmentacja	181
5.3.3. Zarządzanie sesjami	182
5.4. Adresowanie	187
5.4.1. Przydzielanie adresów	188
5.4.2. Rozwiązywanie adresów	195
5.5. Trasowanie	198
5.5.1. Typy trasowania	200
5.5.2. Protokoły trasowania	202
5.5.3. Multicast	206
5.5.4. Anatomia routera	207
5.6. Przykładowa sieć TCP/IP	209
5.6.1. Przypadek nr 1 — znane adresy	211
5.6.2. Przypadek nr 2 — nieznanne adresy	213
5.6.3. Połączenia TCP	214
5.6.4. TCP/IP a warstwy modelu sieciowego	215
5.7. Implikacje dla cyberbezpieczeństwa	217

■ CZĘŚĆ TRZECIA: TECHNOLOGIE SIECIOWE

ROZDZIAŁ 6

Projektowanie sieci 241

6.1. Wstęp	242
6.1.1. Komponenty architektoniczne sieci	242
6.1.2. Tradycyjny styl projektowania	244
6.1.3. Projektowanie modułowe	246
6.2. Analiza wymagań	248
6.2.1. Podział sieci na komponenty architektoniczne	249
6.2.2. Aplikacje w sieci	251
6.2.3. Użytkownicy sieci	251
6.2.4. Kategoryzacja wymagań	252
6.2.5. Dokumenty	252
6.3. Projektowanie technologiczne	254
6.3.1. Projektowanie klientów i serwerów	254
6.3.2. Projektowanie obwodów	254
6.3.3. Narzędzia wspomagające projektowanie sieci	257
6.3.4. Dokumenty	258
6.4. Szacowanie kosztów	258
6.4.1. RFP — prośba o złożenie oferty	258
6.4.2. Prezentacja na forum zarządu	260
6.4.3. Dokumenty	260
6.5. Implikacje dla cyberbezpieczeństwa	260

ROZDZIAŁ 7

Sieci lokalne — przewodowe i bezprzewodowe **267**

7.1. Wstęp	268
7.2. Komponenty sieci LAN	269
7.2.1. Karty sieciowe	270
7.2.2. Obwody sieciowe	270
7.2.3. Koncentratory, przełączniki i punkty dostępowe	272
7.2.4. Sieciowe systemy operacyjne	276
7.3. Ethernet przewodowy	277
7.3.1. Topologia	278
7.3.2. Sterowanie dostępem do nośnika	281
7.3.3. Typy ethernetu	282
7.4. Ethernet bezprzewodowy	283
7.4.1. Topologia	284
7.4.2. Sterowanie dostępem do nośnika	284
7.4.3. Format ramki bezprzewodowej	286
7.4.4. Typy bezprzewodowego ethernetu	286
7.4.5. Bezpieczeństwo	288
7.5. Zalecane praktyki w projektowaniu sieci LAN	290
7.5.1. Przewidywania dotyczące użytkowników przewodowego ethernetu	291
7.5.2. Przewidywania dotyczące użytkowników Wi-Fi	292
7.5.3. Projektowanie centrów danych	295
7.5.4. Projektowanie krawędzi e-handlu	298
7.5.5. Projektowanie środowiska SOHO	299
7.6. Polepszanie wydajności sieci LAN	301
7.6.1. Zwiększanie wydajności serwerów	302
7.6.2. Zwiększanie przepustowości obwodów	304
7.6.3. Redukowanie wymagań	304
7.7. Implikacje dla cyberbezpieczeństwa	305

ROZDZIAŁ 8

Sieci szkieletowe **317**

8.1. Wstęp	318
8.2. Przełączane sieci szkieletowe	319
8.3. Trasowane sieci szkieletowe	322
8.4. Wirtualne sieci LAN	325
8.4.1. Zalety sieci VLAN	327
8.4.2. Jak działają sieci VLAN?	328
8.5. Zalecane praktyki w projektowaniu sieci szkieletowych	332
8.6. Polepszanie wydajności sieci szkieletowych	333
8.6.1. Zwiększanie wydajności urządzeń	334
8.6.2. Zwiększanie przepustowości obwodów	334
8.6.3. Redukowanie wymagań	334
8.7. Implikacje dla cyberbezpieczeństwa	335

ROZDZIAŁ 9

Sieci rozległe 345

9.1. Wstęp	346
9.2. Sieci obwodów dedykowanych	347
9.2.1. Podstawowa architektura	347
9.2.2. Usługi T-carrier	352
9.2.3. Usługi SONET	353
9.3. Sieci komutacji pakietów	354
9.3.1. Podstawowa architektura	354
9.3.2. Usługi Frame Relay	356
9.3.3. Usługi IP	357
9.3.4. Usługi ethernetowe	357
9.4. Wirtualne sieci prywatne	358
9.4.1. Podstawowa architektura	358
9.4.2. Typy VPN	360
9.4.3. Jak działa VPN?	360
9.5. Zalecane praktyki w projektowaniu sieci WAN	363
9.6. Polepszanie wydajności sieci WAN	365
9.6.1. Zwiększanie wydajności urządzeń	366
9.6.2. Zwiększanie przepustowości obwodów	366
9.6.3. Redukowanie wymagań	367
9.7. Implikacje dla cyberbezpieczeństwa	367

ROZDZIAŁ 10

Internet 381

10.1. Wstęp	382
10.2. Jak działa internet?	383
10.2.1. Podstawowa architektura	383
10.2.2. Połączenie z dostawcą internetu	385
10.2.3. Dzisiejszy internet	387
10.3. Technologie dostępu do internetu	388
10.3.1. Cyfrowa linia abonencka (DSL)	388
10.3.2. Modem kablowy	390
10.3.3. Światłowód do domu (FTTH)	393
10.3.4. WiMax	393
10.3.5. Coraz szybciej i coraz lepiej, czyli LTE	395
10.3.6. Jeszcze szybciej i jeszcze lepiej, czyli 5G	396
10.4. Przyszłość internetu	399
10.4.1. Zarządzanie internetem	399
10.4.2. Kreowanie przyszłości	401
10.5. Implikacje dla cyberbezpieczeństwa	402

■ CZĘŚĆ CZWARTA: ZARZĄDZANIE SIECIĄ

ROZDZIAŁ 11

Bezpieczeństwo sieci **413**

11.1. Wstęp	414
11.1.1. Dlaczego w sieciach konieczne są zabezpieczenia?	416
11.1.2. Typy zagrożeń dla bezpieczeństwa	417
11.1.3. Kontrole sieciowe	419
11.2. Ocena ryzyka	420
11.2.1. Definiowanie kryteriów pomiaru ryzyka	420
11.2.2. Inwentaryzacja zasobów IT	421
11.2.3. Identyfikacja zagrożeń	425
11.2.4. Dokumentowanie istniejących kontroli	429
11.2.5. Poszukiwanie możliwości usprawnień	430
11.3. Zapewnienie ciągłości funkcjonowania	430
11.3.1. Ochrona przed złośliwym oprogramowaniem	430
11.3.2. Ochrona przed atakami DoS	432
11.3.3. Ochrona przed kradzieżą	436
11.3.4. Niwelowanie skutków awarii urządzeń	437
11.3.5. Ochrona przed skutkami katastrof	439
11.4. Zapobieganie włamaniom	443
11.4.1. Polityka bezpieczeństwa	444
11.4.2. Ochrona na granicy sieci i firewalle	444
11.4.3. Ochrona serwerów i klientów	452
11.4.4. Szyfrowanie	457
11.4.5. Uwierzytelnianie użytkowników	466
11.4.6. Obrona przed socjotechniką	471
11.4.7. Systemy zapobiegania włamaniom	474
11.4.8. Odtwarzanie po włamaniu	477
11.5. Zalecenia praktyczne	478
11.6. Implikacje dla Twojego cyberbezpieczeństwa	480

ROZDZIAŁ 12

Zarządzanie siecią **497**

12.1. Wstęp	498
12.2. Projektowanie sieci pod kątem wydajności	498
12.2.1. Sieci zarządzane	499
12.2.2. Zarządzanie ruchem sieciowym	503
12.2.3. Redukowanie ruchu sieciowego	505
12.3. Zarządzanie konfiguracją	509
12.3.1. Konfigurowanie sieci i komputerów klienckich	509
12.3.2. Dokumentowanie konfiguracji	510

12.4. Zarządzanie wydajnością i awariami 512

 12.4.1. Monitorowanie sieci 514

 12.4.2. Kontrolowanie awarii 515

 12.4.3. Statystyki wydajności i statystyki awarii 518

 12.4.4. Polepszanie wydajności 522

12.5. Wsparcie dla użytkowników 522

 12.5.1. Rozwiązywanie problemów 522

 12.5.2. Szkolenia dla użytkowników 524

12.6. Zarządzanie kosztami 525

 12.6.1. Źródła kosztów 525

 12.6.2. Redukowanie kosztów 528

12.7. Implikacje dla cyberbezpieczeństwa 530