

ADAM JÓZEFIOK



Zostań inżynierem sieci

100 PYTAŃ

DO PRZYSZŁEGO SIECIOWCA

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: helion@helion.pl
WWW: helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/zosinz
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-2643-1

Copyright © Helion S.A. 2025

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wprowadzenie	7
ROZDZIAŁ 1. Podstawy sieci komputerowych i modele warstwowe	11
Wprowadzenie	11
Pytanie 1. Jak działa komunikacja w modelu klient-serwer i modelu peer-to-peer?	11
Pytanie 2. Co to jest adres MAC i jakie ma znaczenie w sieci?	18
Pytanie 3. Z ilu warstw składa się model OSI? Opisz je i podaj przykłady	20
Pytanie 4. Czym różni się model OSI od modelu TCP/IP?	23
Pytanie 5. W której warstwie modelu OSI działa router? Wyjaśnij dlaczego	24
Pytanie 6. W której warstwie modelu OSI działa przełącznik? Wyjaśnij dlaczego	25
Pytanie 7. Co to jest adres IP i jak działa brama domyślna?	28
Pytanie 8. Jaka jest różnica między adresem IPv4 a adresem IPv6?	29
Pytanie 9. Co to jest maska podsieci i jak obliczyć liczbę hostów w podsieci dla adresu IPv4?	30
Pytanie 10. Ile urządzeń możemy zaadresować w sieci /22? Zaprezentuj przykład dla sieci 172.16.0.0 pokazujący również pulę adresową	32
Pytanie 11. Jaki jest ostatni użyteczny adres IP w sieci 192.168.0.0/24?	33
Pytanie 12. Co oznaczają 127.0.0.1 i localhost?	34
Pytanie 13. Jaka jest różnica pomiędzy komunikacją unicast, multicast i broadcast?	35
Pytanie 14. Co to jest numer portu w kontekście TCP/UDP i do czego służy?	38
Pytanie 15. Jakie są dobrze znane numery portów dla HTTP, HTTPS, FTP, SSH i Telnetu? Za co odpowiedzialne są te protokoły?	39
ROZDZIAŁ 2. Protokół IP i mechanizmy sieciowe	46
Wprowadzenie	46
Pytanie 16. Co to jest mechanizm DAD?	46
Pytanie 17. Jak działa SLAAC i czym różni się od DHCPv6?	48
Pytanie 18. Co to jest IPv6 anycast?	51
Pytanie 19. Czym są NAT i PAT oraz jak działają?	52
Pytanie 20. Co to jest DHCP i jak działa proces przydziału adresu IP?	59
Pytanie 21. Co to jest DNS i jak działa proces rozwiązywania nazw w DNS?	64
Pytanie 22. Co to jest protokół ARP i jak działa proces ARP?	72
Pytanie 23. Co to jest agent przekazywania w DHCP i jak działa?	75
Pytanie 24. Co to jest proxy ARP i jak działa?	77
Pytanie 25. Jak działa protokół ICMP i do czego jest wykorzystywany?	78

Pytanie 26. Co to jest i jak działa TLS 1.3 0-RTT?	80
Pytanie 27. Co to jest PoE i jakie są jego zastosowania?	82
Pytanie 28. Jak działa mechanizm TTL w pakietach IP i dlaczego jest ważny?	84
Pytanie 29. Co to jest protokół UDP i jakie są jego cechy?	86
Pytanie 30. Jak działa protokół QUIC?	88
Pytanie 31. Co to jest protokół TCP i jakie są jego cechy?	89
Pytanie 32. Na czym polega mechanizm fragmentacji pakietów IP i jakie mogą być jego konsekwencje?	94

ROZDZIAŁ 3. Segmentacja sieci i routing98

Wprowadzenie	98
Pytanie 33. Co to jest VLAN i jakie są zalety jego stosowania?	98
Pytanie 34. Co to jest trunk i jakie protokoły wykorzystuje?	102
Pytanie 35. Co to jest VTP i do czego służy? Podaj różnice wersji	104
Pytanie 36. Co to jest SVI? Co jest potrzebne, aby interfejs SVI był w statusie UP/UP?	107
Pytanie 37. Jak działa metoda router-on-a-stick?	108
Pytanie 38. Co to jest ACL?	112
Pytanie 39. Jakie są różnice między standardową a rozszerzoną listą ACL?	114
Pytanie 40. Czym są routing statyczny i dynamiczny?	116
Pytanie 41. Czym różni się protokół wektora odległości od protokołu stanu łączy?	121
Pytanie 42. Co to jest protokół RIPv2, jak działa i jakie są jego ograniczenia?	123
Pytanie 43. Jak działa protokół OSPF i jakie są jego zalety?	124
Pytanie 44. Co to jest obszar w OSPF?	127
Pytanie 45. Czym jest BGP i gdzie się go stosuje?	128
Pytanie 46. Jak działa protokół BGP?	130
Pytanie 47. Co to jest EIGRP i jak działa?	134
Pytanie 48. Jakich metryk używa EIGRP?	135
Pytanie 49. Czym jest successor w EIGRP?	138
Pytanie 50. Czym są DR i BDR w OSPF?	139
Pytanie 51. Co to jest EtherChannel i jakie protokoły są używane w tej technologii?	142
Pytanie 52. Co to jest MPLS i jakie są zalety jego stosowania?	145
Pytanie 53. Jak działa atak na podstawie podwójnego DHCP spoofingu?	149
Pytanie 54. Jak można wykryć obecność sniffiera w sieci lokalnej?	151

ROZDZIAŁ 4. Bezpieczeństwo sieci i mechanizmy ochrony 152

Wprowadzenie	152
Pytanie 55. Co to jest DHCP snooping?	153
Pytanie 56. Jak działa Port Security na przełączniku Cisco?	157
Pytanie 57. Jakie są zagrożenia związane z VLAN hopping i jakie są metody ochrony?	161
Pytanie 58. Co to jest BPDU Guard?	162
Pytanie 59. Do czego służy Root Guard?	166
Pytanie 60. Jakie są różnice między BPDU Guard a BPDU Filter?	167
Pytanie 61. Co to jest Dynamic ARP Inspection (DAI)?	167

Pytanie 62. Co to jest PortFast?	169
Pytanie 63. Jakie są najczęstsze ataki na sieć Wi-Fi?	171
Pytanie 64. Jakie są zalety i wady WEP, WPA, WPA2 i WPA3?	173
Pytanie 65. Jak działa model AAA?	175
Pytanie 66. Czym są TACACS+ i RADIUS i jakie są różnice między nimi?	177
Pytanie 67. Co to jest NetFlow i jak działa?	178
Pytanie 68. Jak działa port SPAN na przełączniku Cisco?	180
Pytanie 69. Jak działa ERSPAN i jakie są jego zalety?	184
Pytanie 70. Co to jest syslog i jak go używać?	186
Pytanie 71. Jak działa NTP?	192
Pytanie 72. Jakie są różnice między NTP a PTP?	199
Pytanie 73. Co to jest SNMP?	200
Pytanie 74. Jakie są różnice między SNMPv1, SNMPv2 i SNMPv3?	205
Pytanie 75. Co to jest XDR w kontekście bezpieczeństwa sieci?	206
Pytanie 76. Mechanizm CSMA/CA	207
Pytanie 77. Co to jest Cisco DNA?	208
ROZDZIAŁ 5. Zaawansowane technologie sieciowe i konfiguracja	212
Wprowadzenie	212
Pytanie 78. Jakie są podstawowe komendy konfiguracji routera Cisco i jak sprawdzić jego aktualną konfigurację?	213
Pytanie 79. Jak działa konfiguracja SSH na urządzeniu Cisco?	218
Pytanie 80. Co to jest HSRP?	221
Pytanie 81. Co to jest VRRP?	225
Pytanie 82. Co to jest GLBP?	228
Pytanie 83. Co to jest VPN? Wymień jego rodzaje	231
Pytanie 84. Co to jest IPsec i jak działa?	233
Pytanie 85. Co to jest GRE?	236
Pytanie 86. Co to jest SD-WAN?	239
Pytanie 87. Co to jest Intent-Based Networking (IBN)?	243
Pytanie 88. Jakie są różnice między IPv4 a IPv6 w kontekście routingu?	243
Pytanie 89. Czym są i jak działają SR oraz SRv6?	244
Pytanie 90. Co to jest IoT i jakie są jego zastosowania?	245
Pytanie 91. Co to jest network slicing?	247
Pytanie 92. Jak działa cloud networking?	248
Pytanie 93. Jak skonfigurować route-map w Cisco IOS?	249
Pytanie 94. Jak działa filtracja tras za pomocą prefix-list?	252
Pytanie 95. Co to jest i jak działa sumaryzacja tras?	255
Pytanie 96. Co to jest QoS i jakie są jego podstawowe mechanizmy?	257
Pytanie 97. Jak działa CoPP (Control Plane Policing) i do czego służy?	265
Pytanie 98. Co to jest VXLAN i jak działa?	268
Pytanie 99. Co to jest EVPN?	275
Pytanie 100. Co to jest MPLS i jak działa?	276
Zakończenie	288

Wprowadzenie

W świecie, w którym niemal każda sfera życia zależy od stabilnego i bezpiecznego dostępu do sieci komputerowej — począwszy od zakupów internetowych, przez komunikację, po krytyczne systemy medyczne, finansowe i przemysłowe — zrozumienie zasad działania sieci komputerowych staje się nie tylko domeną specjalistów, ale także ważną umiejętnością dla każdego świadomego użytkownika technologii. Książka, którą trzymasz w rękach, powstała z potrzeby zebrania w jednym miejscu najważniejszych zagadnień sieciowych i przedstawienia ich w formie przystępnych odpowiedzi na konkretne pytania.

Książka ta nie jest zbiorem encyklopedycznych definicji. To praktyczny przewodnik, który krok po kroku przeprowadzi Cię przez fundamenty działania współczesnych sieci komputerowych, z uwzględnieniem ewolucji technologii, najlepszych praktyk oraz rzeczywistych scenariuszy wykorzystywanych przez administratorów i inżynierów sieci.

Jest to pozycja będąca również uzupełnieniem kursu wideo pt. „Zostań inżynierem sieci. Kurs video. 100 pytań do przyszłego sieciowca”. Kurs odpowiada również na 100 pytań. Opanowanie jego tematyki pozwala na zapoznanie się z wieloma definicjami obecnych sieci komputerowych. Umożliwia bezproblemowe przejście przez niemal każdą rozmowę kwalifikacyjną.

Ze względu na to, że sieci komputerowe to bardzo obszerny materiał, książka rozwija niektóre tematy oraz uzupełnia te, które na szkoleniu nie zostały poruszone, a również są istotne.

Dla kogo jest ta książka?

Dla osób, które chcą zacząć przygodę w świecie sieci komputerowych i aplikują na stanowisko inżyniera sieci. Ale nie tylko, bo zarówno początkujący pasjonat sieci, jak i student kierunków technicznych, specjalista IT czy kandydat przygotowujący się do certyfikacji znajdzie tutaj coś dla siebie. Książka została napisana prostym, zrozumiałym językiem, przy zachowaniu technicznej precyzji i zgodności z aktualnym stanem wiedzy. Każde pytanie i odpowiedź zostały opracowane tak, aby można było z nich korzystać niezależnie. Możesz przeczytać książkę od początku do końca, ale równie dobrze sięgnąć tylko po interesujący Cię temat.

Publikacja została podzielona na pięć logicznych rozdziałów:

Rozdział 1. „Podstawy sieci komputerowych i modele warstwowe”

W tym rozdziale poznasz absolutne fundamenty: modele odniesienia OSI i TCP/IP, różnice między komunikacją klient-serwer a peer-to-peer, pojęcia takie jak adres IP, adres MAC, brama domyślna czy maska podsieci. Zrozumiesz, czym jest adres 127.0.0.1, czym różni się IPv4 od IPv6 oraz jak działa routing w podstawowej formie. Ten rozdział to solidny start, bez którego nie da się skutecznie przejść dalej.

Rozdział 2. „Protokół IP i mechanizmy sieciowe”

To serce logicznego działania sieci. Opisuję tu m.in. działanie DHCP, DNS, NAT, ARP, ICMP, TLS 1.3 czy protokołów transportowych TCP i UDP. Omawiam również nowoczesne podejścia, jak QUIC czy PoE, oraz mechanizmy bezpieczeństwa i wydajności, takie jak TTL czy fragmentacja pakietów. Rozdział ten stanowi pomost między teorią a praktyką, zrozumienie tych mechanizmów to podstawa przy każdej konfiguracji.

Rozdział 3. „Segmentacja sieci i routing”

To obszar skupiający się na tym, jak zorganizować duże sieci w mniejsze logiczne fragmenty (VLAN-y, trunking, ACL), jak działa routing dynamiczny i statyczny oraz jakie protokoły pomagają w efektywnym wyznaczaniu tras (OSPF, EIGRP, BGP). Znajdziesz tu również tematy takie jak MPLS, EtherChannel, router-on-a-stick czy metody wykrywania ataków trzeciej warstwy.

Rozdział 4. „Bezpieczeństwo sieci i mechanizmy ochrony”

Dobrze zaprojektowana sieć to nie tylko wydajność, ale też odporność na ataki. W tym rozdziale omawiam mechanizmy ochrony stosowane na przełącznikach i routerach Cisco, takie jak DHCP snooping, Port Security, DAI, BPDU Guard, Root Guard czy AAA. Zawarto tu także popularne zagrożenia, w tym ataki na sieci Wi-Fi oraz różnice między protokołami SNMP, NTP czy TACACS+ i RADIUS. To kompletny zbiór narzędzi i koncepcji dla osób chcących zabezpieczyć infrastrukturę.

Rozdział 5. „Zaawansowane technologie sieciowe i konfiguracja”

To rozdział dla tych, którzy chcą iść dalej — znaleźć się o krok bliżej technologii klasy korporacyjnej. Opisuję tutaj konfiguracje takich funkcji jak VPN, IPsec, SSH, GRE, SD-WAN, SRv6, CoPP, VXLAN oraz technologie klasy service provider, takie jak MPLS czy EVPN. Znajdziesz tu również wyjaśnienia dotyczące Cloud Networking, Intent-Based Networking oraz Internetu rzeczy (IoT).

Książka jest napisana w formie pytanie – odpowiedź, co umożliwia szybkie odnajdywanie informacji i wykorzystywanie treści w praktyce. To format szczególnie przydatny dla osób przygotowujących się do egzaminów i rozmów kwalifikacyjnych, administratorów sieci szukających szybkich odpowiedzi na konkretne pytania, nauczycieli i wykładowców szukających uporządkowanych treści do zajęć.

Zachęcam Cię do tego, aby nie tylko czytać, ale także testować przedstawione rozwiązania w praktyce — na symulatorach, takich jak Cisco Packet Tracer, GNS3 czy nawet w realnych środowiskach testowych.

Na pewno nie jest to książka encyklopedyczna. Nie znajdziesz tu suchych definicji ani kopiowanych opisów z dokumentacji producentów. Znajdziesz za to zrozumiałe odpowiedzi na rzeczywiste pytania. To książka o tym, co naprawdę działa w sieci, co warto wiedzieć i co często sprawia problem, a co łatwo wyjaśnić, jeśli tylko ktoś Ci to dobrze wytłumaczy.

Mam nadzieję, że pozycja ta stanie się Twoim osobistym przewodnikiem po świecie sieci komputerowych — nie tylko dziś, ale i w przyszłości. A jeśli zdecydujesz się sięgnąć również do wcześniejszego kursu video, to gwarantuję, że każda rozmowa kwalifikacyjna będzie dla Ciebie formalnością.

ROZDZIAŁ 1.

Podstawy sieci komputerowych i modele warstwowe

Wprowadzenie

Sieci komputerowe we współczesnym świecie zajęły pierwsze miejsce pod względem ważności i wpływu na życie ludzkości. Bez komunikacji współczesny świat nie mógłby funkcjonować. Sieci komputerowe to fundament nowoczesnej komunikacji, która w każdej chwili jest na świecie wykorzystywana. Sieci te nie odpoczywają i nie idą spać, mało tego — każdego dnia eksploatowane są coraz bardziej.

Pierwszy rozdział tej książki jest poświęcony kilkunastu pytaniom związanym z podstawami działania sieci komputerowych.

Pytanie 1. Jak działa komunikacja w modelu klient-serwer i modelu peer-to-peer?

Na początku należy zaznaczyć, że oba wspomniane modele to podstawowe architektury komunikacji w sieciach komputerowych. Ze względu na złożoność sieci komputerowych często komunikacja oparta jest na różnych modelach architektonicznych. Tymi dwoma najczęściej stosowanymi są klient-serwer (ang. *client-server*) oraz peer-to-peer (P2P). Nie można o tych modelach powiedzieć, że jeden jest lepszy od drugiego, gdyż po prostu każdy z nich posiada swoje własne cechy, a w tym wady i zalety. Działają w różnych warunkach, a to je odróżnia od siebie już na samym wstępie. W pierwszej kolejności przyjrzyjmy się komunikacji w modelu klient-serwer.

Podczas korzystania z sieci komputerowej możesz zauważyć, że występuje w niej szereg różnego rodzaju urządzeń. Podstawowym urządzeniem jest komputer, zwany często urządzeniem końcowym. To na nim wykonujesz czynności wymagające dostępu do sieci komputerowej. Może to być na przykład związane z chęcią skorzystania z Internetu. Ze względu na to, że urządzenia sieciowe pełnią odmienne funkcje, przydziela się zadania wielu różnym sprzętom.

W modelu klient-serwer następuje określony rodzaj komunikacji, mający na celu to, aby jedno urządzenie mogło wykorzystać zasoby drugiego. I tak na przykład serwer FTP (ang. *File Transfer Protocol*) jest urządzeniem dostarczającym usługi innym urządzeniom, klientom. Serwer FTP centralizuje dane, a klienci przesyłają zapytania, aby uzyskać do nich dostęp. Za chwilę pokażę to na konkretnym przykładzie. Chciałbym, abyś na razie

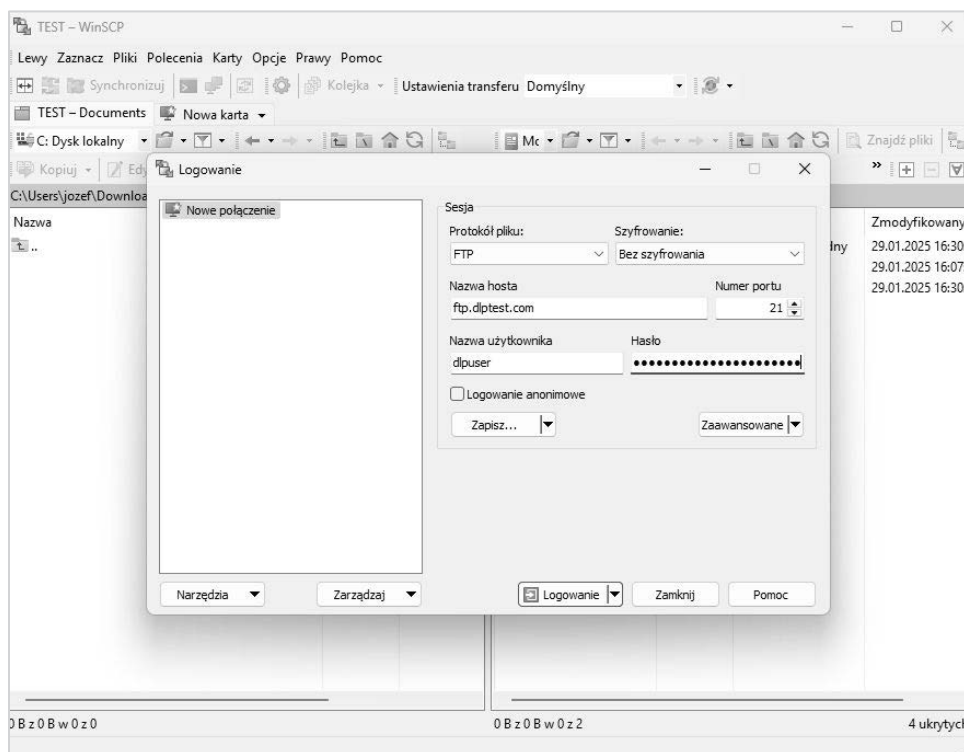
wiedział, że podczas połączenia w modelu klient-serwer to klient inicjuje połączenie. Robi to poprzez wysłanie żądania do serwera. Żądanie ma określoną postać i zależy od protokołu. Protokół zaś jest ustalony na podstawie tego, co chcesz uzyskać z serwera. Jeśli ma to być plik, to protokołem będzie FTP, jeżeli natomiast chcesz wyświetlić stronę WWW, wówczas zostanie użyty protokół HTTP lub HTTPS. Inny protokół będzie używany do serwera pocztowego, jeszcze inny do serwera wydruku itd.

Tuż po wysłaniu przez klienta żądania serwer je odbiera. Następnie musi je przetworzyć i uzyskać wymagane informacje. W kolejnym kroku serwer wysyła odpowiedź, w której tak naprawdę znajdują się wyniki jego działania. Odpowiedzią może być plik, o który prosił klient, strona WWW lub coś innego.

Model klient-serwer posiada szereg zalet, z których najważniejszymi są centralizacja zasobów wraz z danymi i łatwy do nich dostęp. Inną zaletą jest skalowalność, czyli łatwa rozbudowa istniejącej infrastruktury. Model posiada oczywiście wady, z których najpoważniejszą jest słaby punkt w postaci serwera. Jeśli ten ulegnie awarii, wszystkie usługi przestają działać. Drugą wadą jest wydajność samego serwera. Jeżeli ten nie będzie wystarczająco wydajny, wówczas stanie się wąskim gardłem całej sieci.

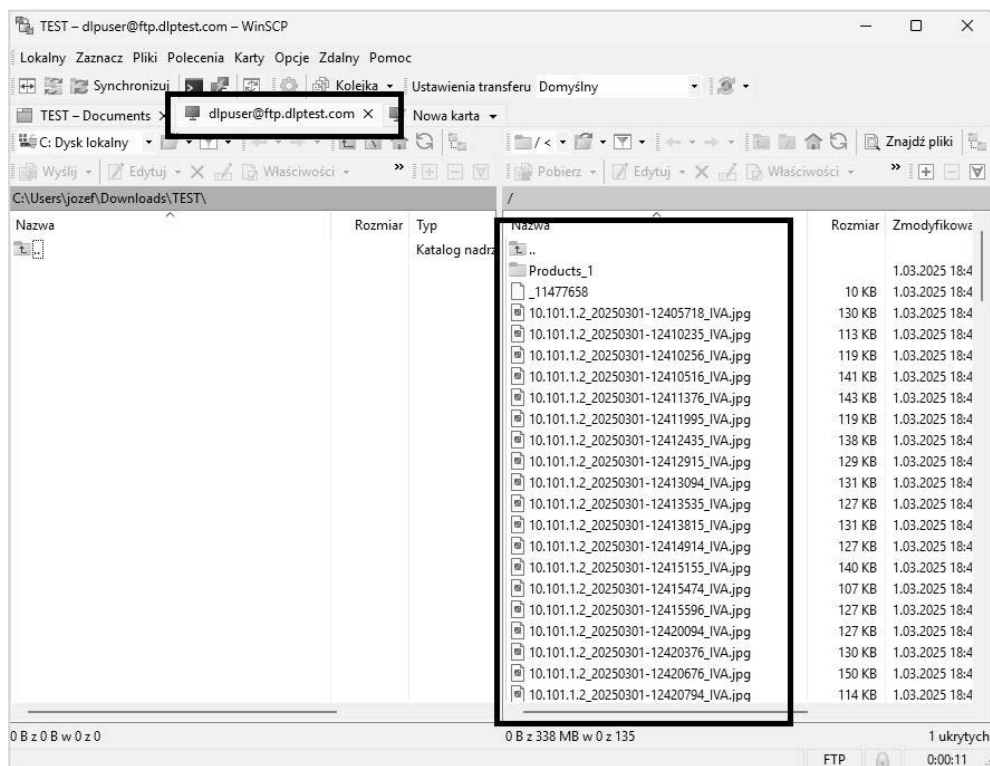
Zobaczmy, jak prezentuje się to w praktyce.

Pokażę Ci, jak wygląda transmisja klient-serwer na przykładzie darmowego serwera FTP. W pierwszej kolejności należy zainstalować klienta FTP, na przykład darmowy program **WinSCP**. Następnie należy podać dane dostępowe do serwera, co obrazuje rysunek 1.1.



RYСУNEK 1.1. Wprowadzanie danych logowania do serwera FTP

Po wprowadzeniu danych logowania i kliknięciu przycisku *Logowanie* zostaniesz połączony z zasobami serwera. Zauważ, że na rysunku 1.2 pokazana jest zawartość folderu głównego serwera FTP.



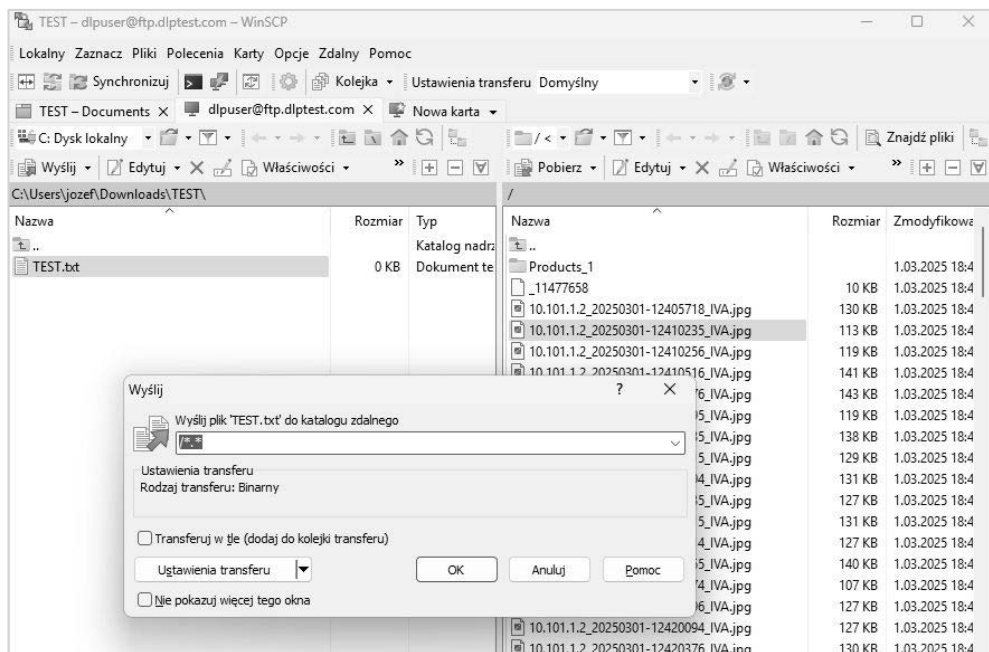
RYСУNEK 1.2. Nawiązane połączenie z serwerem FTP

Teraz skopiujemy wybrany plik na serwer FTP, aby potem wykorzystać tę przykładową transmisję do sprawdzenia właściwości modelu klient-serwer. Po wybraniu dowolnego pliku po lewej stronie okna programu kopiujemy go na serwer FTP, co obrazuje rysunek 1.3.

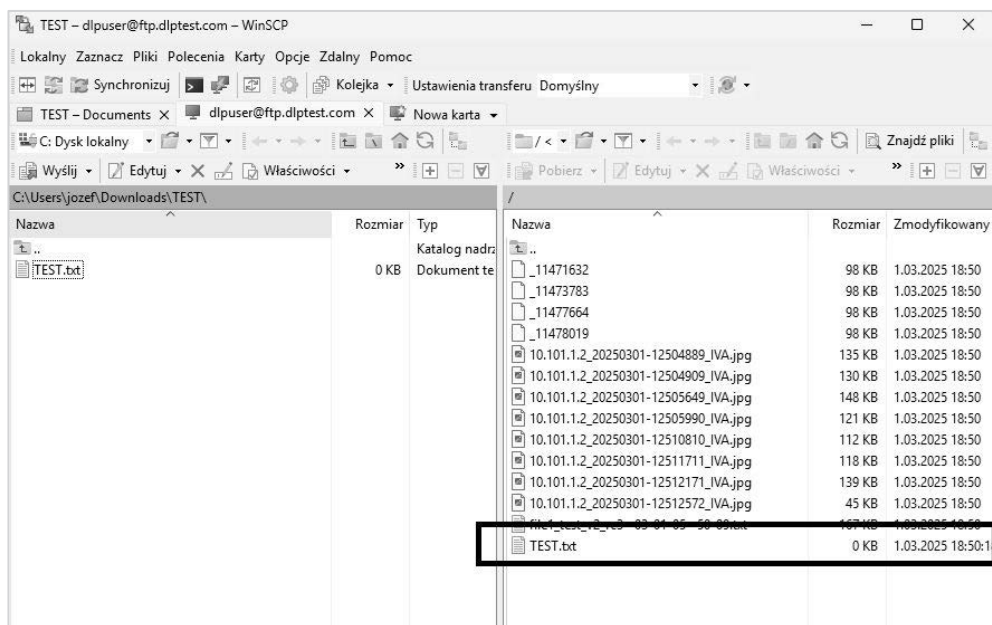
Jak widać na rysunku 1.4, plik został skopiowany na serwer. Jest to przykład transmisji klienta do serwera FTP. Teraz możemy przejść dalej, aby sprawdzić, czy faktycznie model klient-serwer zawiera tylko te dwie stacje.

W czasie kiedy transmitowany był plik tekstowy, za pomocą programu Wireshark została przechwycona transmisja pomiędzy klientem a serwerem. Spójrz na rysunek 1.5, który przedstawia kilka istotnych ramek potwierdzających to, co napisałem wcześniej.

Zanim przejdę do omawiania przesłanych danych, pragnę wspomnieć, że program Wireshark jest snifferem, czyli programem umożliwiającym przechwytywanie danych oraz ich późniejszą analizę. Program przydaje się, jeśli chcesz przejrzeć, co dokładnie przesyłane jest na wybranym interfejsie lub łączu sieciowym. Będę w dalszej części książki często sięgał do tego programu, aby pokazać Ci w praktyce działanie omawianych rzeczy. Dzięki temu uzyskasz praktyczne potwierdzenie teoretycznych informacji.



RYSUNEK 1.3. Kopiowanie pliku TEST.txt na serwer FTP



RYSUNEK 1.4. Skopiowany na serwer FTP plik tekstowy widoczny jest w folderze głównym

The screenshot displays the Wireshark interface with the following details:

- Packet List:** Shows a series of FTP packets. Packet 1830 is highlighted, corresponding to the selected packet details.
- Packet Details:**
 - Ethernet II:** Src: ASUSTekCOMPU_63:b0:02 (60:cf:84:63:b0:02), Dst: Routerbo...
 - Internet Protocol Version 4:** Src: 172.30.100.14, Dst: 44.241.66.173
 - Transmission Control Protocol:** Src Port: 64003, Dst Port: 21, Seq: 381, Ac...
 - File Transfer Protocol (FTP):**
 - Request command: STOR
 - Request arg: TEST.txt
 - [Current working directory: /]
 - [Command response frames: 0]
 - [Command response bytes: 0]
 - [Command response first frame: 0]
 - [Command response last frame: 0]
 - [Setup frame: 0]
- Packet Bytes:** Shows the raw data of the selected packet, including the command 'STOR TEST.txt'.

RYSunek 1.5. Przechwycona transmisja danych pomiędzy serwerem FTP a klientem

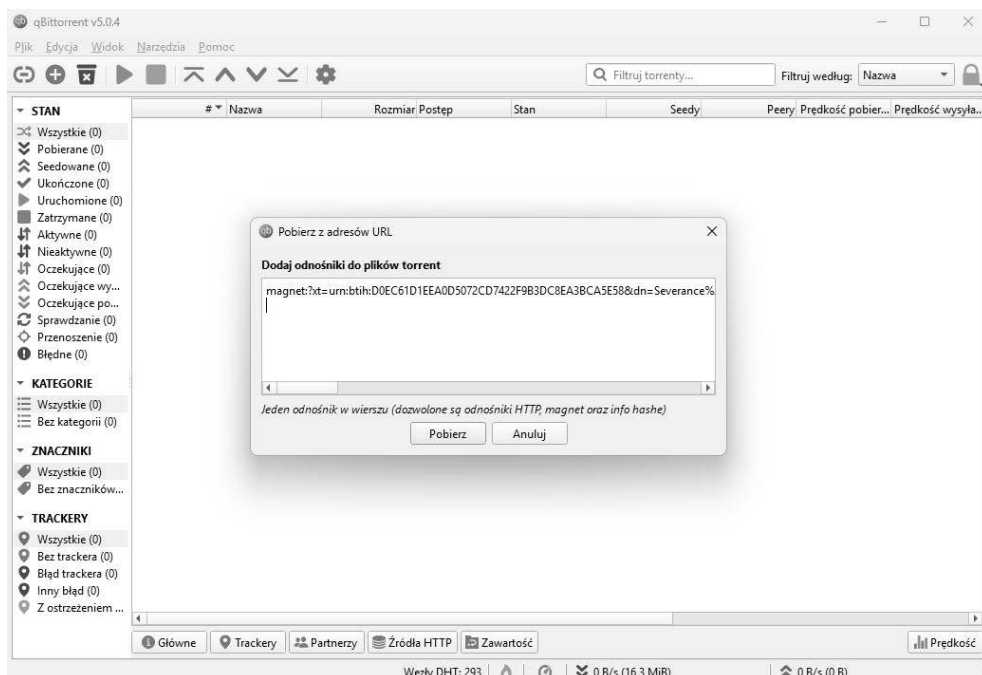
Zauważ, że w górnym polu okna widocznego na rysunku 1.5 wpisałem **ftp**, aby przefiltrować przechwycony ruch. Interesuje nas tylko transmisja FTP. Pamiętajsz zapewne, że charakterystyczny dla komunikacji klient-serwer jest centralny punkt oraz to, że transmisja odbywa się faktycznie pomiędzy dwiema stacjami. Rysunek 1.5 potwierdza to, gdyż jeśli w polu *Source* pojawia się adres IP serwera FTP, a jest nim *44.241.66.173*, to w polu *Destination* pokazuje się adres klienta, czyli *172.30.100.14*. Na odwrót jest w przypadku żądania klienta. Inny adres w tej transmisji się nie pokazuje.

Zauważ również, że zaznaczona ramka *1830* pokazuje wartość *STOR TEST.txt* — jest to właśnie próba przesłania pliku o tej nazwie. Transmisja odbywa się od klienta (IP *172.30.100.14*), bo to klient ją rozpoczyna, a celem jest serwer FTP. Potem serwer odpowiada komunikatem *150 Ok to send data*. Jest to nic innego, jak gotowość serwera do odbioru pliku. Ze względu na to, że plik jest niewielkich rozmiarów, po błyskawicznej transmisji serwer od razu odpowiada komunikatem *226 Transfer complete*, oznaczającym zakończenie transmisji. Dalej następuje przesłanie informacji o metadanych oraz innych, o których nie będę tutaj wspominał. Natomiast na koniec transmisji pojawia się ostatnia ramka, z numerem *1869* i komunikatem *226 Directory send OK*, oznaczająca zakończenie transferu i pomyślne przesłanie pliku.

Jak więc można było się przekonać, jest to typowa komunikacja klient-serwer i na tym ona polega w praktyce. Oczywiście, w zależności od protokołu dodatkowych informacji będzie pojawiać się więcej, natomiast zawsze będzie to komunikacja jeden do jednego.

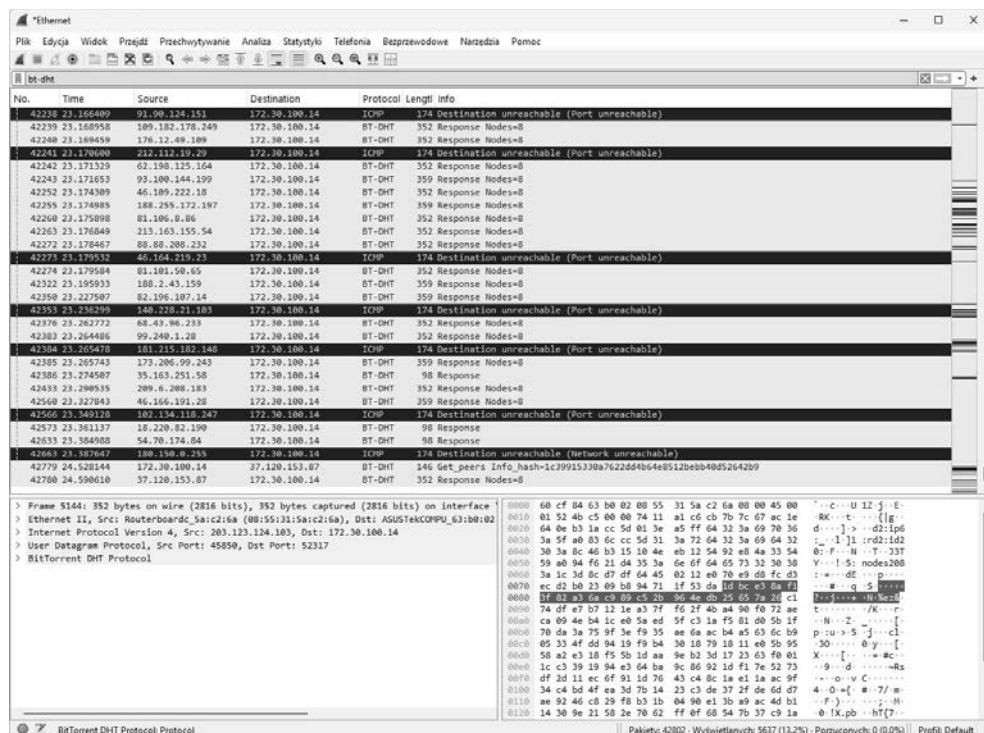
Drugim modelem jest model zwany peer-to-peer (P2P). Jest to architektura, która działa nieco inaczej i charakteryzuje się innymi cechami niż klient-serwer. Przede wszystkim P2P jest architekturą zdecentralizowaną. Tym, co wyróżnia ten model, jest to, że każdy host (nazywany często węzłem) może być klientem, ale również serwerem. Można powiedzieć, że komunikacja za pomocą tego modelu odbywa się bezpośrednio pomiędzy klientami. Jeśli takie połączenie zostanie zrealizowane, to na jego czas wybrany host przyjmuje rolę serwera. W tym modelu urządzenia podczas transmisji mogą odbierać oraz wysyłać dane, są równorzędne. Czasem, aby zwiększyć odporność na awarie, pliki, usługi lub inne zasoby są przechowywane na wielu klientach. Tak więc w razie konieczności dostępu do zasobów mogą one być pobierane z różnych serwerów jednocześnie. W taki sposób działają właśnie usługi typu BitTorrent czy eMule. Zaletami tego modelu są bez wątpienia: brak w nim centralnego punktu oraz bardzo duża skalowalność. Wadą są bardzo duże problemy w zarządzaniu zasobami, które mają być dostępne. Inną wadą jest niestabilność działania tego typu sieci.

Nadszedł teraz czas, aby sprawdzić, jak wygląda w praktyce komunikacja P2P. Aby wygenerować ruch, użyta została aplikacja **qBittorrent**, która pozwala na pobieranie plików torrent z sieci P2P. Jest to klasyczny przykład tego typu sieci. Na rysunku 1.6 widać wklejony link do odnośnika pliku torrent (tzw. magnet link). Po kliknięciu przycisku *Pobierz* we wspomnianej aplikacji rozpocznie się pobieranie pliku na dysk, za pomocą sieci P2P.



RYSUNEK 1.6. Rozpoczęcie pobierania pliku torrent

Podobnie jak poprzednio, uruchomiony został program Wireshark, aby rejestrował wszystkie pakiety przesyłane w trakcie transmisji. Rysunek 1.7 przedstawia przechwycone dane pomiędzy klientem i pozostałymi serwerami.



RYСУNEK 1.7. Przechwycona transmisja P2P

Napisałem „serwerami”, ponieważ — jak możesz zauważyć na rysunku 1.7 — w kolumnach *Source* oraz *Destination* jest już wiele adresów IP. Nie jest to już tylko adres klienta i serwera, jak miało to miejsce w modelu klient-serwer. W Wiresharku widać wiele połączeń pomiędzy różnymi węzłami, wymieniającymi fragmenty pliku. Mało tego, w trakcie transmisji można zauważyć, że nasza stacja również staje się klientem, gdyż w polu *Source* pojawia się adres 172.30.100.14. Tak działa sieć P2P w praktyce.

Podsumowując, oba modele — klient-serwer i peer-to-peer — są fundamentalnymi architekturami komunikacji w sieciach komputerowych. Wybór odpowiedniego zależy od rodzaju usługi, wymaganej skalowalności, poziomu centralizacji oraz potrzeb w zakresie bezpieczeństwa i zarządzania.

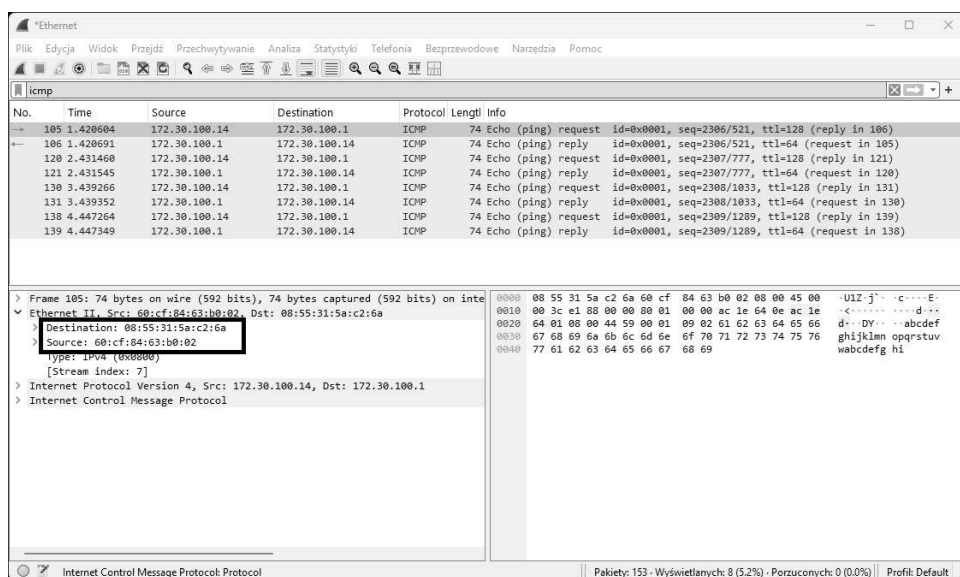
Pytanie 2. Co to jest adres MAC i jakie ma znaczenie w sieci?

Adres MAC to wartość liczbową, zapisana w formacie szesnastkowym, który oprócz liczb od 0 do 9 wykorzystuje również litery od A do F. Tak więc 0 to najniższa wartość adresu MAC, a F to wartość najwyższa. Użyty skrót MAC to tak naprawdę Media Access Control i pełni funkcję unikatowego identyfikatora, który jest przypisany do każdej karty sieciowej działającej w standardzie Ethernet.

Identyfikator ten jest zapisany na stałe w chipie karty sieciowej przez producenta. Adres MAC może mieć postać na przykład 1A:B2:3C:D4:5E:FF. Jego długość wynosi więc 48 bitów. Warto w tym miejscu wspomnieć, że adres karty sieciowej można podzielić na dwie równe części. Pierwsza, 24-bitowa część (OUI) oznacza kod producenta karty, a druga część to unikatowy numer karty. Taki schemat został wymyślony z tego względu, że na świecie nie mogą pojawić się dwie karty sieciowe o tych samych adresach MAC. Mogłoby to spowodować błędy w transmisji danych lub całkowicie uniemożliwić komunikację. Pomimo tego, że adres MAC kojarzony jest zwykle z kartą sieciową, to unikatowe adresy MAC mają również porty przełącznika, porty routera, port sieciowy drukarki czy karta bezprzewodowa Ethernet. Każdy smart zegarek, smartfon czy inne urządzenie, wykorzystując dostęp do sieci, posiada taki adres.

Tak więc adres MAC ma ogromne znaczenie w sieciach komputerowych, które w większości są oparte na technologii Ethernet. Adres MAC identyfikuje w sieci konkretne urządzenie. Zobaczmy to na przykładzie prostej komunikacji pomiędzy stacją roboczą a routerem dostępowym.

Rysunek 1.8 przedstawia zarejestrowaną za pomocą programu Wireshark komunikację pomiędzy stacją roboczą a routerem.



RYСУNEK 1.8. Przechwycona komunikacja protokołu ICMP pomiędzy stacją roboczą a routerem

Ze stacji roboczej z adresem IP 172.30.100.14 został wysłany komunikat ICMP (potocznie ping) do routera z adresem IP 172.30.100.1. Mamy na rysunku cztery żądania (ang. *request*) oraz cztery odpowiedzi (ang. *reply*). Komunikacja działa więc prawidłowo. Jednak spójrz na zaznaczony fragment, w którym znajdują się pola *Destination* i *Source*. Tam właśnie jest adres MAC routera, czyli adres docelowy 08:55:31:5a:c2:6a. Adres źródłowy to właśnie adres MAC karty sieciowej stacji roboczej, czyli 60:cf:84:63:b0:02.

W sieciach komputerowych dane wysyłane są na konkretny adres komputera lub innego urządzenia pracującego w sieci. Adresem tym w sieci Ethernet jest właśnie adres MAC. Adresy MAC źródłowy i docelowy są konieczne do tego, aby komunikacja pomiędzy dwoma urządzeniami mogła działać prawidłowo.

Gdybyś chciał sprawdzić w systemie Windows, gdzie znajduje się adres MAC Twojej karty sieciowej, możesz użyć komendy `ipconfig -all`, tak jak pokazano to na rysunku 1.9. Znajdują się tam dwa adresy MAC. Pierwszy jest adresem karty sieciowej kablowej, a drugi adresem karty bezprzewodowej.

```

Wiersz polecenia
C:\Users\jozef>ipconfig -all

Windows IP Configuration

Host Name . . . . . : IGOR
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No


Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek Gaming 2 5GbE Family Controller
Physical Address. . . . . : 60-CF-84-63-B0-02
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 172.30.100.14(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : poniedziałek, 3 marca 2025 18:29:26
Lease Expires . . . . . : poniedziałek, 3 marca 2025 19:59:24
Default Gateway . . . . . : 172.30.100.1
DHCP Server . . . . . : 172.30.100.1
DNS Servers . . . . . : 178.235.153.32
                        178.235.153.33
NetBIOS over Tcpip. . . . . : Enabled


Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card
Physical Address. . . . . : 58-CD-C9-D6-F7-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
    
```

RYSUNEK 1.9. Adresy MAC w systemie Windows możesz sprawdzić za pomocą komendy `ipconfig`

Adres MAC odgrywa kluczową rolę w komunikacji lokalnej w sieciach Ethernet, pozwalając na jednoznaczną identyfikację urządzeń. To dzięki niemu ramki danych trafiają do właściwego odbiorcy. Jego zrozumienie jest fundamentem do dalszego poznawania działania sieci komputerowych.

PROGRAM PARTNERSKI

— GRUPY HELION —

- 
1. ZAREJESTRUJ SIĘ
 2. PREZENTUJ KSIĄŻKI
 3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion 

Wszystko, co powinien wiedzieć przyszły inżynier sieci

Książka, którą trzymasz w rękach, powstała z potrzeby zebrania w jednym miejscu najważniejszych zagadnień dotyczących sieci komputerowych i przedstawienia tej wiedzy w formie przystępnych odpowiedzi na konkretne pytania. Ten praktyczny przewodnik krok po kroku przeprowadzi Cię przez fundamenty działania współczesnych sieci komputerowych z uwzględnieniem ewolucji technologii, najlepszych praktyk, a także rzeczywistych scenariuszy stosowanych przez administratorów. Planujesz karierę jako inżynier sieci? Koniecznie sięgnij po tę książkę. Przy czym skorzystają z niej nie tylko przyszli inżynierowie — również pasjonaci sieci, studenci kierunków technicznych, specjaliści IT i osoby przygotowujące się do certyfikacji znajdą tu wiele cennych informacji.

Podręcznik został napisany prostym, zrozumiałym językiem przy zachowaniu technicznej precyzji i zgodności z aktualnym stanem wiedzy. Pytania i odpowiedzi opracowano tak, aby można było z nich korzystać niezależnie. Książkę możesz przeczytać od początku do końca, ale równie dobrze możesz sięgnąć tylko po tematy z interesującego Cię obszaru.

Pytania zostały podzielone na pięć sekcji:

- **Podstawy sieci komputerowych i modele warstwowe**
- **Protokół IP i mechanizmy sieciowe**
- **Segmentacja sieci i routing**
- **Bezpieczeństwo sieci i mechanizmy ochrony**
- **Zaawansowane technologie sieciowe i konfiguracja Cisco**

Adam Józefiok

Ukończył studia doktora na Politechnice Śląskiej w Gliwicach, na Wydziale Automatyki, Elektroniki i Informatyki. Specjalizuje się w tematyce sieci komputerowych (przełączanie, routing, bezpieczeństwo i projektowanie). Jest autorem publikacji polskich i zagranicznych z tej dziedziny. Brał udział w konferencjach naukowych (krajowych i międzynarodowych) dotyczących sieci komputerowych. Jest pracownikiem naukowym Katedry Sieci i Systemów Komputerowych Politechniki Śląskiej. Na co dzień administruje również bezpieczeństwem urządzeń sieciowych, konfiguruje między innymi urządzenia sieciowe (Cisco, HP), utrzymuje sieci WAN. Przez siedem lat kierował komórką realizacji wsparcia usług IT. Ma wieloletnie doświadczenie w pracy jako administrator sieci i projektant sieci komputerowych. Przez lata projektował serwery i tworzył projekty okablowania. Opracowywał procedury i dokumentację projektowe. Na koncie ma wiele zrealizowanych projektów w zakresie zakupu sprzętu IT wraz z prowadzeniem procedur przetargowych, wdrożeniem, wykonaniem dokumentacji i testami. Posiada certyfikaty: CCNA Security, CCNP Routing and Switching, Cisco CCDP, CCNAV, jak również certyfikat instruktorski Cisco CCAI, certyfikaty ITIL i PRINCE2. Jego pasją jest pisanie książek, praca ze studentami i szeroko rozumiana dydaktyka.

	KOD KORZYŚCI Sięgnij po więcej! 
 helion.pl	ISBN 978-83-289-2643-1
 HELION S.A. ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	 9 788328 926431
Cena: 89,00 zł	