

Wstęp do sieci komputerowych

Arkadiusz Syta, Jacek Zaburko
Politechnika Lubelska
Katedra Informatyki Technicznej

Treści programowe:

- Historia rozwoju sieci komputerowych
- Definicje i podstawowe pojęcia z obszaru sieci komputerowych
- Typy oraz topologia sieci komputerowych



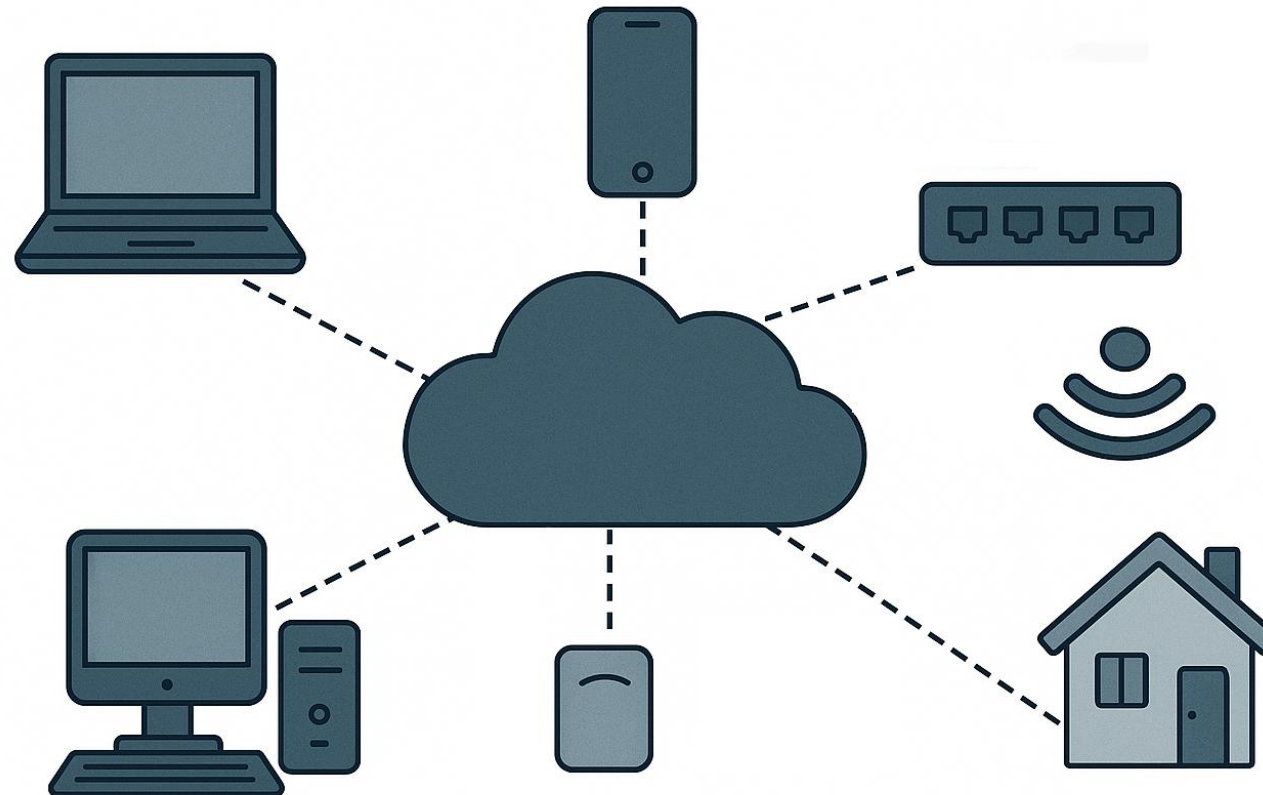
Sieć komputerowa:

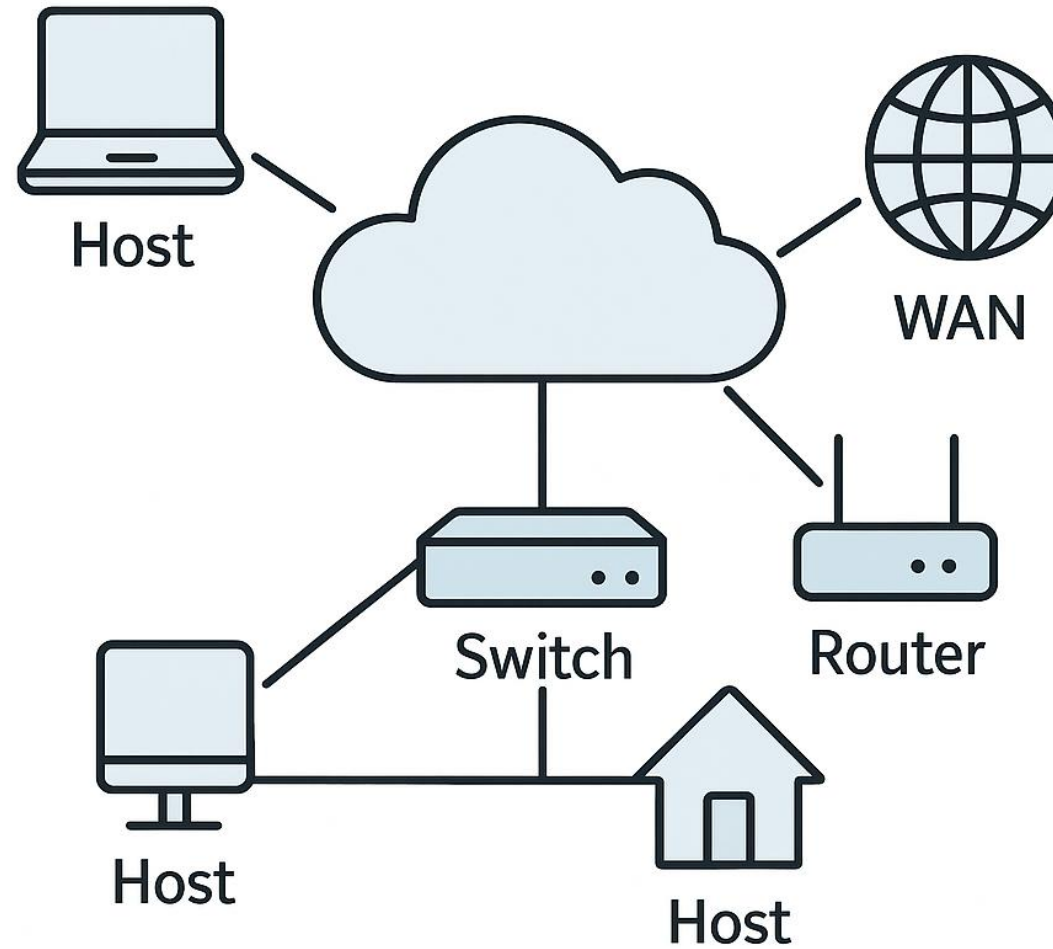
Grupa komputerów i innych urządzeń połączonych z sobą kanałami komunikacyjnymi oraz oprogramowanie wykorzystywane w tej sieci. Umożliwia ona wymianę danych lub współdzielenia różnych zasobów[*]

Zbiór zlokalizowanych oddzielnie komputerów połączonych w celu wykonania określonego zadania[**]

*Wikipedia

** Tanenbaum 1996





Szacowana liczba urządzeń sieciowych w roku 2025

- IoT Analytics:
18,8 miliarda – aktywnie połączone urządzenia
- Cisco (Annual Internet Report):
29,3 miliarda (łącznie) – wszystkie urządzenia

Podstawowe definicje

Jednostki pomiaru prędkości transmisji:
bity na sekundę (b/s) i wielokrotności

- bit (**b**) – najmniejsza jednostka informacji (wartość 0 lub 1)
- bit na sekundę (**b/s**) – ile bitów danych jest przesyłanych w ciągu 1 sekundy
- kilobit na sekundę (**Kb/s**) = 1000 b/s
- megabit na sekundę (**Mb/s**) = 1000 Kb/s = 100000 b/s
- gigabit na sekundę (**Gb/s**) = 1000 Mb/s = 1000000000 b/s

Podstawowe definicje

Jednostki pomiaru prędkości transmisji:

Mb (megabit) – prędkość transmisji danych

MB (megabajt) – pojemność pamięci i rozmiar plików

1 bajt = 8 bitów => 1 MB = 8 MB

8

Podstawowe definicje

Przykład: W jakim czasie pobierzemy plik o wielkości **4,7 GB** (obraz płyty DVD) zakładając stałą przepustowość łącza wynoszącą **100 Mb/s**

$$100 \text{ Mb/s} \div 8 = 12,5 \text{ MB/s}$$

$$4,7 \text{ GB} = 4,7 \cdot 1024 \text{ MB} = 4812,8 \text{ MB}$$

$$4812,8 \text{ MB} \div 12,5 \text{ MB/s} = 385,024 \text{ s} \approx 6,42 \text{ m}$$

Podstawowe definicje

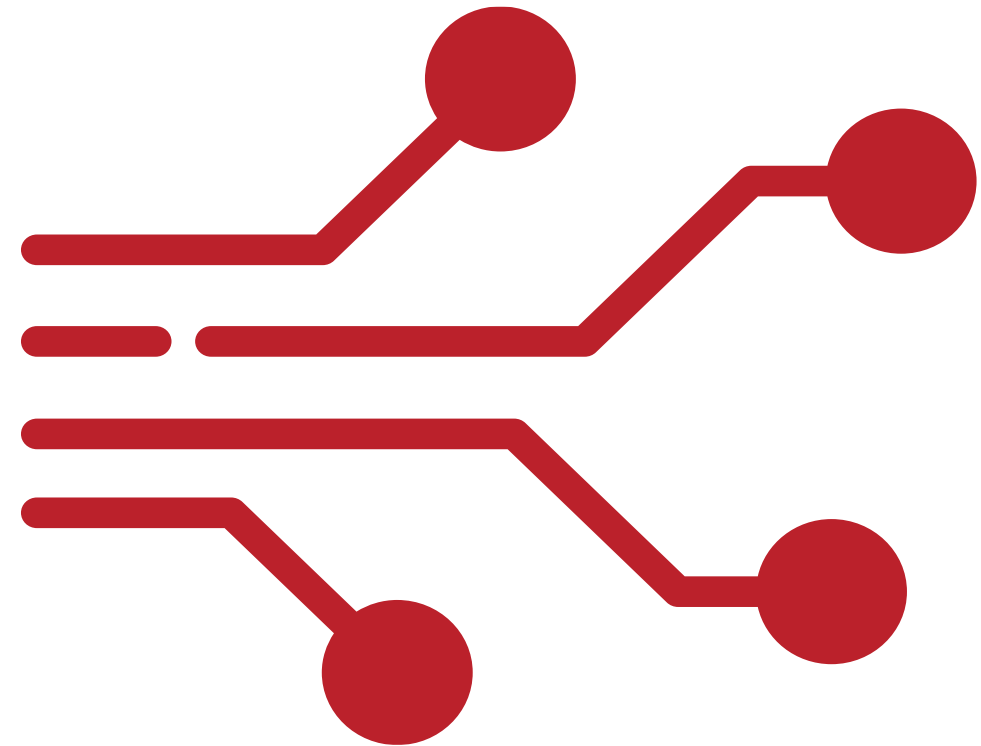
Jak sprawdzić
efektywną
przepustowość
łącza?

WYNIK SPEED TEST #451035140

PING opóźnienie w ms 2	DOWNLOAD pobieranie w Mb/s 94.09	UPLOAD wysyłanie w Mb/s 94.70



Historia rozwoju sieci komputerowych



11

Lata 50 – mainframe i terminale

Mainframe – ogromne komputery centralne

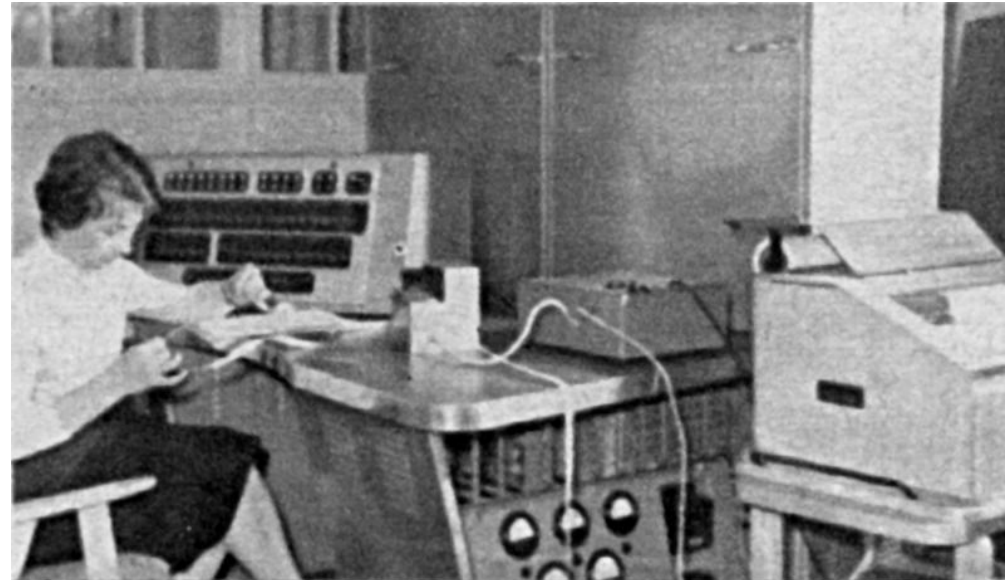
Terminal – proste urządzenia do korzystania z mainframeów (ekran + klawiatura, bez mocy obliczeniowej)

Pierwsze próby komunikacji oparte na modemach (modulator-demodulator) – zamiana sygnału cyfrowego na analogowy przesyłany liniami telefonicznymi

Sposób działania – przełączanie obwodów

Brak standardów komunikacji

12



Źródło - Wikipedia

13

Lata 60 – koncepcja sieci rozproszonych

Paul Baran (**RAND Corporation** – Research and Development - siły powietrzne Stanów Zjednoczonych)

W 1962 zaproponował koncepcję sieci rozproszonej odpornej na ataki nuklearne

Realizacja za pomocą komutacji pakietów – dane dzielone na małe porcje (**pakiety**)

Każdy pakiet posiada adres nadawcy i odbiorcy

Przesyłane różnymi trasami przez sieć i rekonstruowane u odbiorcy

14

Lata 60 – ARPAnet – pierwsza sieć komputerowa

ARPAnet (Advanced Research Projects Agency Network) - pierwsza nowoczesna sieć komputerowa łącząca ośrodki naukowe i badawcze

Finansowana przez amerykańską agencję **ARPA** (Advanced Research Projects Agency), a później **DARPA** (Defense Advanced Research Projects Agency)

29 października 1969 – przesłanie pierwszych danych między UCLA (Uniwersytet Kalifornijski w Los Angeles) a SRI (Stanford Research Institute)

Próba zakończyła się awarią po wpisaniu dwóch liter „LO” zamiast całego słowa „LOGIN” – moment ten przeszedł do historii

15

Lata 60 – ARPAnet – pierwsza sieć komputerowa

Sieć zbudowana w oparciu o przełączanie pakietów – protoplasta obecnego **internetu**

Początkowo ARPAnet miał cztery węzły:

Uniwersytet Kalifornijski, Instytut Stanforda, Uniwersytet Santa Barbara oraz Uniwersytet Utah

1972 – ARPAnet liczy już 15 węzłów

Powstała tradycja otwartych dokumentów standaryzacyjnych – **RFC** (Request for Comments), w których specyfikowano zasady działania nowych protokołów

RFC istnieją do dziś i są fundamentem Internetu

Lata 70 – aplikacje ARPAnet

1971 – Ray Tomlinson stworzył e-mail (poczta elektroniczna)

Wprowadził po raz pierwszy znak **@** oddzielający nazwę użytkownika od nazwy komputera

1973 sieć ARPAnet zostaje połączona z Europą – węzły w Norwegii i Wielkiej Brytanii

W 1972 stworzono pierwszy protokół sieciowy **NCP** (Network Control Protocol) – użyty do obsługi komunikacji pomiędzy systemami końcowymi w sieci ARPAnet [RFC001]

17

Lata 70 – protokół NCP

Protokół NCP zapewniał proste mechanizmy połączeniowe:

- otwieranie i zamykanie połączeń
- dwukierunkowe przesyłanie danych

Wady protokołu NCP:

- brak protokołów routingu i obsługi wielu sieci
- nie posiadał koncepcji adresowania między sieciami

Aplikacje zbudowane w sieci ARPAnet w oparciu o NCP:

- Telnet – zdalne logowanie
- FTP – przesyłanie plików
- SMTP (później) – poczta elektroniczna

18

Lata 70 – model OSI i protokół TCP/IP

Koncepcja modelu **OSI** (Open systems Interconnection) – podział komunikacji sieciowej na 7 warstw: od fizycznej po aplikacyjną

Model nigdy nie został w pełni wdrożony (używany w dydaktyce)

TCP/IP (Transmission Control Protocol / Internet Protocol) – podstawa działania internetu - zestaw protokołów komunikacyjnych [RFC801]

opracowany w latach 70. przez Vinta Cerfa i Boba Kahna jako rozwinięcie koncepcji NCP

1 stycznia 1983 – oficjalna migracja ARPAnet z NCP na TCP/IP
– „flag day”

19

Lata 70 – protokół TCP/IP

IP (Internet Protocol) – odpowiada za adresowanie i dostarczanie pakietów

TCP (Transmission Control Protocol) – zapewnia niezawodność i kolejność przesyłanych danych

uzupełniając **UDP** (User Datagram Protocol) – szybki, ale bez kontroli błędów

Nowy stos TCP/IP pozwolił łączyć wiele różnych sieci w jedną spójną całość – **Internet** (inter-networking = sieć sieci)

20

Lata 80 – popularyzacja sieci

1984 – powstaje **DNS** (Domain Name System) – nazwy domenowe zamiast adresów IP [RFC1034]

1985 – pierwszy komercyjny dostęp do internetu (NSFNET w USA)

Sieci lokalne (**LAN**) zdobywają popularność: **Ethernet, Token Ring, Novell NetWare**

Rozwój sieci biurowych -> komputery osobiste (IBM PC 1981, Macintosh 1984) z kartami sieciowymi

21

Lata 90 – Internet masowy

1990 – sieć ARPAnet oficjalnie wyłączona

1991 – Tim Berners-Lee (CERN) zaproponował język hipertekstu **WWW** (World Wide Web):

- **HTML** (HyperText Markup Language) – język stron internetowych
- **HTTP** (HyperText Transfer Protocol) – protokół przesyłu stron
- **URL** (Uniform Resource Locator) – jednolity system adresów

1993 – pojawia się przeglądarka Mosaic – pierwsza popularna graficzna przeglądarka

22

Lata 90 – Internet masowy

1994 – powstają kolejne przeglądarki Netscape Navigator i Internet Explorer (wojny przeglądarkowe)

pojawiają się wyszukiwarki internetowe: Yahoo, AltaVista

1998 – powstaje Google - zmiana sposobu wyszukiwania informacji

komercjalizacja Internetu, pierwsze sklepy internetowe, Amazon, eBay

Lata 90 – Internet szerokopasmowy

połowa lat 90 - Internet masowo dostępny w gospodarstwach domowych
(modemy dial-up 56 Kb/s)

koniec lat 90 – szybsze technologie:

- DSL (Digital Subscriber Line),
- ADSL (Asymmetric DSL),
- kablówka (DOCSIS – Data Over Cable Service Interface Specification),
- światłowody (FTTH – Fiber To The Home)

rozwój nowych usług: streaming wideo, telefonia **VoIP** (Voice over IP), gry online

24

Lata 90 – bezprzewodowe sieci lokalne

1997 - standard **IEEE 802.11**, znany jako **Wi-Fi** („Wireless Fidelity”)

standard określał dwie prędkości transmisji – 1 oraz 2 Mb/s

medium - promieniowanie podczerwone oraz wykorzystywany w przemyśle i medycynie zakres częstotliwości 2,4 GHz

podczerwień się nie przyjęła ze względu na konkurencję standardu **IrDA**
dalsze prace nad Wi-Fi szybko doprowadziły do powstania standardu **IEEE 802.11b** (do 11 Mb/s)

25

Ostatnie dokonania - Web 2.0

Internet społecznościowy - zmiana paradygmatu:

od statycznych stron do dynamicznych aplikacji

użytkownicy tworzą treści: blogi, fora, komentarze

powstanie portali społecznościowych:

Facebook (2004), YouTube (2005), Twitter/X (2006), Instagram (2010)

Internet jako platforma komunikacji, współpracy i reklamy

26

Ostatnie dokonania - Internet mobilny: 2G, 3G, 4G

Rozwój sieci komórkowych - zmiana sposób korzystania z Internetu:

- **2G** (GSM – Global System for Mobile Communications) – rozmowy, SMS (Short Message Service), proste transmisje danych (EDGE – Enhanced Data rates for GSM Evolution)
- **3G** (UMTS – Universal Mobile Telecommunications System) – dostęp do poczty, stron, szybkie pakietowe przesyłanie danych (HSPA – High-Speed Packet Access)
- **4G LTE** (Long Term Evolution) – szerokopasmowy Internet mobilny, videokonferencje, streaming HD

2007 - pojawił się iPhone

2008 – pojawił się Android

27

Ostatnie dokonania - Cloud Computing (chmura obliczeniowa)

Chmura obliczeniowa - zmiana sposobu korzystania z sieci
dane i aplikacje są przechowywane w centrach danych i udostępniane przez Internet
Modele:

- IaaS (Infrastructure as a Service) – infrastruktura (np. serwery, pamięć)
- PaaS (Platform as a Service) – platforma dla programistów
- SaaS (Software as a Service) – gotowe aplikacje (np. Gmail, Office 365)

2006 - Amazon uruchomił AWS (Amazon Web Services) - początek rewolucji

Pojawiają się umowy jakości usług (SLA – Service Level Agreement) i interfejsy API (Application Programming Interface)

28

Internet Rzeczy – IoT

IoT (Internet of Things) - miliardy urządzeń codziennego użytku podłączonych do Internetu

łączenie świata fizycznego i cyfrowego – inteligentne domy, miasta, fabryki

urządzenia: smartwatche, czujniki przemysłowe, AGD, samochody autonomiczne

protokoły IoT: MQTT, CoAP, Zigbee, BLELPWAN (LoRaWAN, NB-IoT, Sigfox) dla zasięgu kilometrowego

coraz częściej dane analizowane lokalnie (edge computing, MEC)

29

5G i przyszłe sieci

2019 – sieć 5G:

- przepustowość do kilku Gb/s
- opóźnienia <10 ms
- możliwość obsługi miliona urządzeń na km² (ważne dla IoT)

Zastosowania:

- samochody autonomiczne
- rozszerzona i wirtualna rzeczywistość (AR/VR)
- telemedycyna (zabiegi zdalne)

ok. 2030 – sieć 6G – planowane szybkości rzędu Tb/s, integracja z AI i siecią kwantową

30

Sztuczna inteligencja w sieciach

AI wspiera:

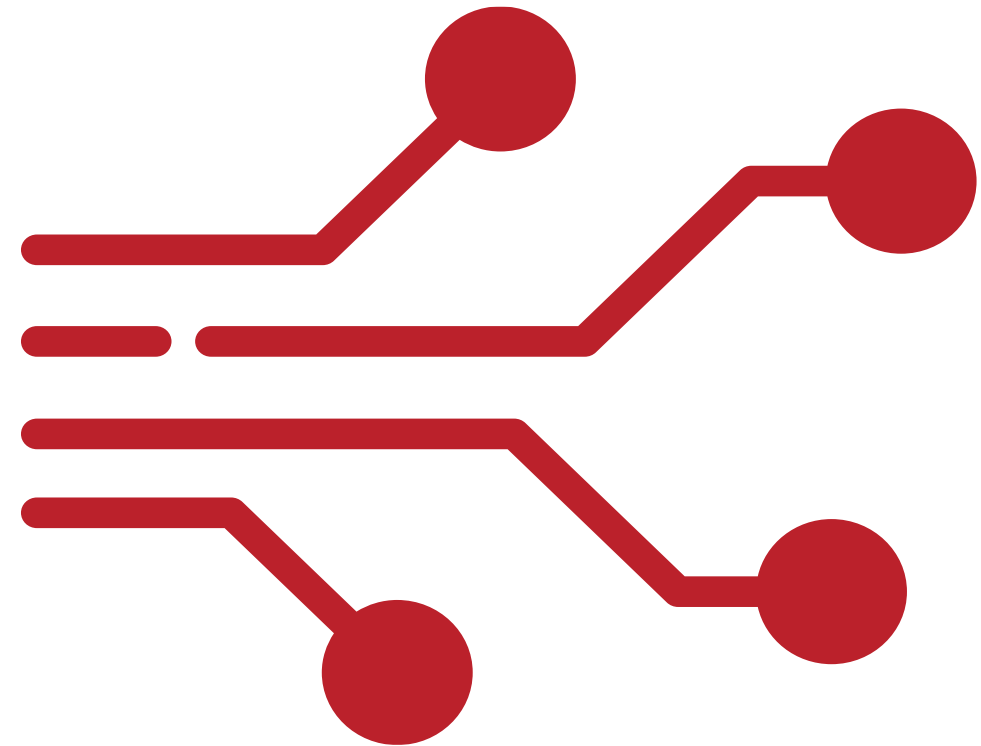
- optymalizację tras routingu
- wykrywanie ataków i anomalii w ruchu sieciowym
- zarządzanie centrami danych (oszczędność energii)

Edge AI – analiza danych bezpośrednio na urządzeniu lub przy brzegu sieci

AI + IoT + 5G = inteligentne miasta, fabryki, logistyka

31

Definicje i podstawowe pojęcia z obszaru sieci komputerowych



Podstawowe definicje

- **Host (system końcowy):** każde urządzenie końcowe podłączone do sieci, które może wysyłać i odbierać dane
- **Serwer:** komputer stale podłączony do sieci świadczący usługi innym komputerom (WWW, poczta, zasoby plikowe)
- **Klient-serwer:** model komunikacji, w którym klient żąda usługi, a serwer ją udostępnia (np. przeglądarka i serwer WWW)
- **Peer-to-peer (P2P):** model komunikacji, w którym każdy host może być zarówno klientem, jak i serwerem

33

Podstawowe definicje

- **Medium transmisyjne:** fizyczny nośnik umożliwiający przesyłanie sygnałów i danych, przewodowe (kabel miedziany, kabel światłowodowy) lub bezprzewodowe (fale radiowe, podczerwone, łączność satelitarna)
- **Sprzęt sieciowy:** urządzenia fizyczne umożliwiające komunikację w sieci

34

Podstawowe definicje – sprzęt sieciowy

- **Urządzenia aktywne:** wymagają zasilania elektrycznego do działania, potrafią przetwarzać, modyfikować lub generować sygnał sieciowy (karty sieciowe, routery, przełączniki, punkty dostępowe, zapory sieciowe, modemy, wzmacniacze)
- **Urządzenia pasywne:** nie wymagają zasilania i nie przetwarzają sygnałów, służą do fizycznego przekazywania danych (kable sieciowe, złącza np. RJ-45) oraz organizacji infrastruktury sieciowej (patch panele, szafy, splitter)

35

Podstawowe definicje – urządzenia aktywne

- **Karta sieciowa (NIC Network Interface Card):** urządzenie umożliwiające podłączenie komputera lub innego urządzenia do sieci
konwertuje dane cyfrowe na sygnały sieciowe i odwrotnie
posiada unikatowy adres **MAC**, identyfikujący urządzenie w sieci



Źródło - Wikipedia

36

Podstawowe definicje – urządzenia aktywne

- **Router:** urządzenie łączące różne sieci w celu umożliwienia im komunikacji oraz określanie tras przepływu danych pomiędzy sieciami na podstawie adresu **IP**



Źródło - Wikipedia

37

Podstawowe definicje – urządzenia aktywne

- **Przełącznik (Switch):**
urządzenie sieciowe,
które łączy urządzenia w
sieci lokalnej
decyduje o przesyłaniu
danych pomiędzy
urządzeniami na
podstawie adresu **MAC**

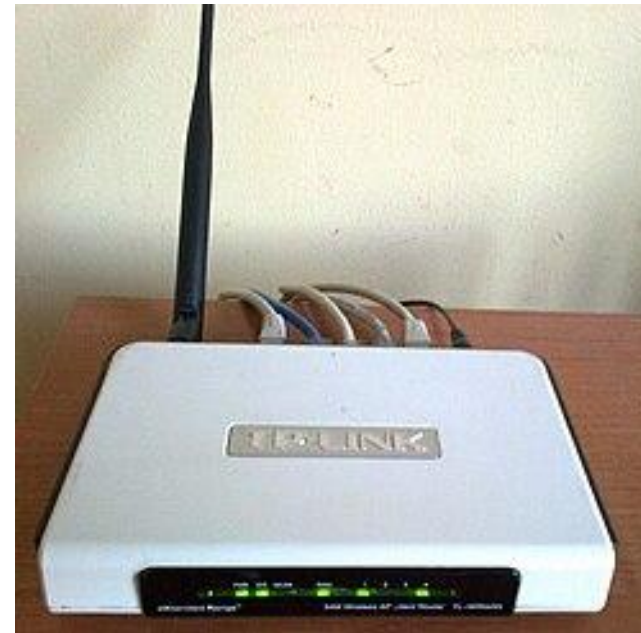


Źródło - Wikipedia

38

Podstawowe definicje – urządzenia aktywne

- **Punkt dostępowy (access point, AP):** urządzenie zapewniające hostom dostęp do sieci za pomocą bezprzewodowego nośnika transmisyjnego (fale radiowe) zazwyczaj mostem łączącym sieć WLAN z siecią LAN – posiada co najmniej dwa interfejsy sieciowe: **bezprzewodowy i przewodowy**



Źródło - Wikipedia

39

Podstawowe definicje – urządzenia aktywne

- **Modem:** urządzenie konwertujące sygnały cyfrowe na analogowe i odwrotnie, umożliwiając dostęp do Internetu (np. w technologiach DSL, kablowych lub światłowodowych)



Źródło - Wikipedia

40

Podstawowe definicje – urządzenia pasywne

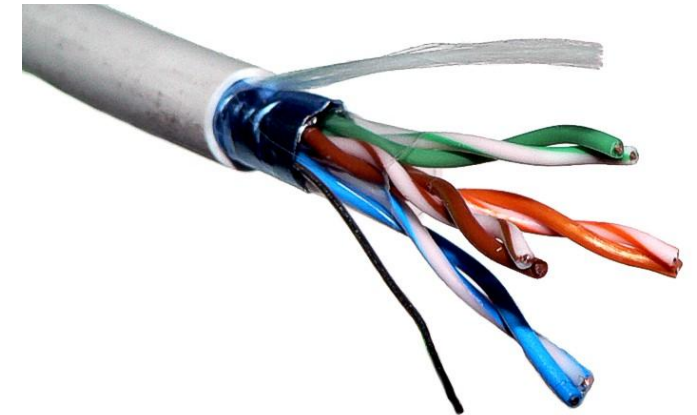
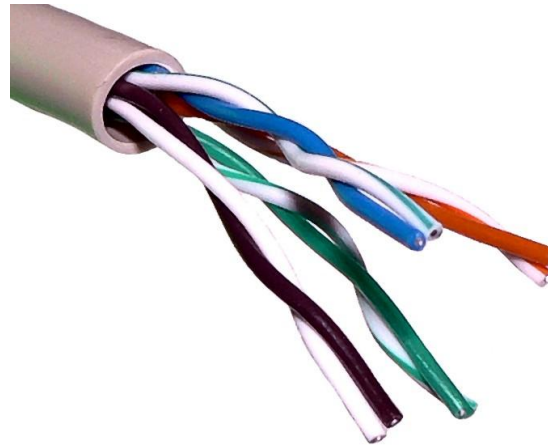
- **Skръtka miedziana**

przesył sygnałów w postaci impulsów **elektrycznych**

zbudowana z 4 par skręconych przewodów – skręcenie redukuje zakłócenia elektromagnetyczne

standardy opisane w **kategoriach (Cat)** – określają częstotliwość pracy i maksymalną przepustowość

złącza: najczęściej **RJ-45**



Źródło - Wikipedia

41

Podstawowe definicje – urządzenia pasywne

Skръtka miedziana kategorie:

- Cat5e – do 1 Gb/s, 100 MHz, powszechnie stosowana w biurach i domach
- Cat6 – do 1 Gb/s (100 m), 10 Gb/s (do 55 m), pasmo 250 MHz
- Cat6A – do 10 Gb/s (100 m), pasmo 500 MHz, lepsze ekranowanie
- Cat7 – do 10 Gb/s (100 m), pasmo 600 MHz, ekranowanie kaŹdej pary + całości, złącza GG45/Tera

42

Podstawowe definicje – urządzenia pasywne

Skръtka miedziana

Zalety: tania, łatwa w instalacji, wystarczająca dla większości LAN

Wady: ograniczony dystans (100 m), podatność na zakłócenia elektromagnetyczne, mniejsze pasmo niż światłowód

Typowe zastosowania: biura, szkoły, domy, serwerownie (połączenia krótkodystansowe)

43

Podstawowe definicje – urządzenia pasywne

• Światłowód

przesył sygnałów w postaci
impulsów świetlnych

składa się z: rdzenia, płaszczu,
powłoki ochronnej

Złącza: SC, LC, ST, MTP/MPO

bardzo duża przepustowość i
zasięg → trzon sieci
szkieletowych i centrów danych



Źródło - Wikipedia

44

Podstawowe definicje – urządzenia pasywne

• Światłowód

1977 - pierwszy na świecie światłowód telekomunikacyjny o długości 9 km łączący dwie centrale telefoniczne w Turynie (Włochy)

1978 - pierwszy w Polsce kabel światłowodowy zaprojektowany i stworzony w 1978 przez pracowników naukowych Uniwersytetu Marii Skłodowskiej-Curie w Lublinie

W Polsce najdłuższą infrastrukturą światłowodową dysponuje operator Orange Polska, który posiada ponad 80 000 km kabli optycznych (głównie sieci szkieletowej)

45

Podstawowe definicje – urządzenia pasywne

- **Światłowód typy:**

SMF (Single-Mode Fiber)

- Rdzeń $\sim 8\text{--}10\ \mu\text{m}$
- Przenosi 1 mod światła – brak efektu dyspersji
- Dystans: dziesiątki, setki kilometrów
- Zastosowania: sieci szkieletowe, operatorzy, łączy między miastami/krajami

MMF (Multi-Mode Fiber)

- Rdzeń $\sim 50/62,5\ \mu\text{m}$
- Przenosi wiele modów światła $\rightarrow$ większa dyspersja, krótsze dystanse
- Dystans: do kilkuset metrów
- Zastosowania: kampusy, serwerownie, sieci lokalne o dużej przepustowości

Podstawowe definicje – urządzenia pasywne

Światłowód

Zalety: ogromna przepustowość (Tb/s), odporność na zakłócenia, bardzo duże dystanse

Wady: wyższy koszt instalacji i sprzętu aktywnego, trudniejszy montaż (spawanie włókien)

Typowe zastosowania: transmisje szkieletowe, data center, operatorzy ISP, długodystansowe połączenia

47

Podstawowe definicje

- **Protokół sieciowy:** określony sposób wymiany komunikatów między komunikującymi się jednostkami oraz operacji w momencie wysyłania lub/i odbierania komunikatów
- **Pakiet:** podstawowa jednostka danych przesyłana w sieciach komputerowych

Powstaje w wyniku podziału większej porcji danych (np. pliku, wiadomości e-mail, strony WWW) na mniejsze fragmenty, które mogą być transmitowane przez sieć

48

Podstawowe definicje

- **Adres IP:** logiczny adres urządzenia w sieci
Identyfikuje hosta i jego lokalizację („adres ulicy”)

Wersje:

- IPv4 – 32 bity, zapis dziesiętny (np. 192.168.1.10)
- IPv6 – 128 bitów, zapis szesnastkowy (np. 2001:db8::1)

Struktura IPv4: adres sieci + adres hosta

Adresacja prywatna i publiczna:

- prywatne np. 192.168.x.x, 10.x.x.x – wewnątrz LAN, używane z NAT
- publiczne – widoczne w Internecie

49

Podstawowe definicje

- Adres IP (Windows 11): cmd / powershell : `ipconfig /all`

```
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . :  
Description . . . . . : Realtek Gaming 2.5GbE Family Controller  
Physical Address. . . . . : 9C-6B-00-94-42-BC  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::2bf4:f6e5:66c:b5e7%17(Preferred)  
IPv4 Address. . . . . : 192.168.1.144(Preferred)  
Subnet Mask . . . . . : 255.255.255.0
```

- Adres IP (Linux Ubuntu): terminal: `ip addr`

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000  
    link/ether 00:15:5d:dc:34:15 brd ff:ff:ff:ff:ff:ff  
    inet 172.28.154.23/20 brd 172.28.159.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::215:5dff:fedc:3415/64 scope link  
        valid_lft forever preferred_lft forever
```

50

Podstawowe definicje

- **DNS** (Domain Name System) – system nazw domenowych tłumaczy nazwy stron (np. example.com) na adresy IP (np. 93.184.216.34) - użytkownik wpisuje nazwę, a nie trudny do zapamiętania numer

użytkownik wpisuje adres w przeglądarce ->

komputer pyta serwer DNS o adres IP ->

serwer DNS zwraca właściwy adres IP ->

przeglądarka łączy się z serwerem docelowym

51

Podstawowe definicje

- **DHCP** (Dynamic Host Configuration Protocol) – protokół automatycznego przydzielania adresów przydziela komputerom w sieci:
- Adres IP
- Maskę podsieci
- Bramkę domyślną (router)
- Adresy serwerów DNS

52

Podstawowe definicje

- **Adres MAC** (Media Access Control) – fizyczny adres karty sieciowej

unikalny identyfikator zapisany w karcie **NIC** (Network Interface Card)

długość: 48 bitów (6 bajtów)

zapis: szesnastkowy, np. 00:1A:2B:3C:4D:5E

pierwsze 3 bajty – identyfikator producenta (OUI – Organizationally Unique Identifier)

ostatnie 3 bajty – numer seryjny karty

53

Podstawowe definicje

- Adres MAC (Windows 11): cmd / powershell : `ipconfig /all`

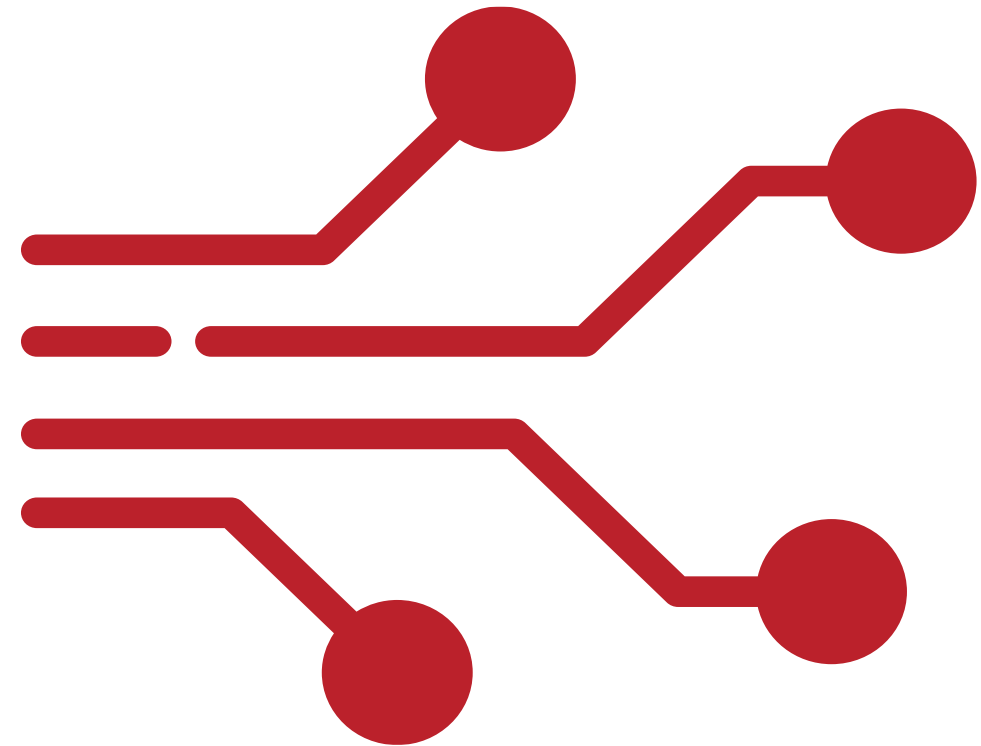
```
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . :  
Description . . . . . : Realtek Gaming 2.5GbE Family Controller  
Physical Address. . . . . : 9C-6B-00-94-42-BC  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::2bf4:f6e5:66c:b5e7%17(Preferred)  
IPv4 Address. . . . . : 192.168.1.144(Preferred)  
Subnet Mask . . . . . : 255.255.255.0
```

- Adres MAX (Linux Ubuntu): terminal: `ip addr`

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000  
    link/ether 00:15:5d:dc:34:15 brd ff:ff:ff:ff:ff:ff  
    inet 172.28.154.23/20 brd 172.28.159.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::215:5dff:fedc:3415/64 scope link  
        valid_lft forever preferred_lft forever
```

Dziękuję za uwagę

Typy sieci komputerowych



56

Rodzaje sieci

- **PAN** – Personal Area Network

sieć osobista (PAN) – najmniejsza skala, zasięg do kilku metrów

łączy urządzenia osobiste użytkownika: laptop, smartfon, tablet, słuchawki, smartwatch

najczęściej bezprzewodowa (Bluetooth, NFC, ZigBee)

57

Rodzaje sieci

- **PAN** – Personal Area Network

zasięg: 1–10 m (Bluetooth), kilka cm (NFC)

przepustowość: od kb/s (NFC) do setek Mb/s (Bluetooth 5.0+)

zalety: wygoda, mobilność

wady: mały zasięg, ograniczona przepustowość,
podatność na podsłuch

58

Rodzaje sieci

- **LAN** – Local Area Network

sieć lokalna (LAN) – obejmuje budynek, piętro, biuro, mieszkanie

łączy komputery, drukarki, serwery

umożliwia wymianę danych, dostęp do zasobów wspólnych i komunikację

najczęściej przewodowa (Ethernet) lub bezprzewodowa (Wi-Fi)

59

Rodzaje sieci

- **LAN** – Local Area Network

przepustowość: od 100 Mb/s do 10-40 Gb/s

opóźnienia: bardzo niskie (< 1 ms)

media: skrętka miedziana, światłowód, Wi-Fi

zalety: wysoka szybkość, łatwe zarządzanie

wady: ograniczony zasięg (do budynku), potrzeba zabezpieczeń

60

Rodzaje sieci

- **MAN** – Metropolitan Area Network

sieć metropolitalna (MAN) – obejmuje obszar miasta lub kampusu akademickiego

łączy wiele sieci LAN w jedną spójną infrastrukturę umożliwiając szybką wymianę danych między instytucjami, firmami czy budynkami

wykorzystuje standardy takie jak Ethernet, światłowody, MPLS (Multiprotocol Label Switching) lub technologie bezprzewodowe (np. WiMAX)

61

Rodzaje sieci

- **MAN** – Metropolitan Area Network

zasięg: kilka–kilkadzieśiat km

medium: głównie światłowody, ale też fale radiowe

przepustowość: setki Mb/s do dziesiątek Gb/s

zarządzanie: przez uczelnię, miasto lub operatora telekomunikacyjnego

zalety: szybki dostęp w dużym obszarze, integracja sieci lokalnych

wady: większe koszty wdrożenia niż LAN, potrzeba zaawansowanych zabezpieczeń

62

Rodzaje sieci

- **WAN** – Wide Area Network

sieć rozległa (WAN) – obejmuje kraje, kontynenty, cały świat
łączy sieci LAN i MAN na dużych odległościach

największa WAN na świecie = Internet

globalny dostęp do internetu, połączenia między oddziałami
firm, chmura obliczeniowa, usługi bankowe, komunikacja
międzynarodowa

63

Rodzaje sieci

- **WAN** – Wide Area Network

zasięg: setki–tysiące km.

medium: światłowody, łącza satelitarne, podmorskie kable

przepustowość: od Mb/s (użytkownik) do Tb/s (szkielet sieci)

zarządzanie: przez wielu operatorów telekomunikacyjnych

zalety: łączność globalna, dostęp wszędzie

wady: opóźnienia, ryzyko awarii węzłów, zależność od operatorów,
wysokie koszty

64

Rodzaje sieci

- **VPN** (Virtual Private Network) – technologia tworząca wirtualną, prywatną sieć w publicznym Internecie

tworzy szyfrowany tunel (np. AES-256) między urządzeniem użytkownika a serwerem VPN

widoczny jest adres IP serwera VPN, a nie prawdziwy IP użytkownika

działanie: użytkownik łączy się z serwerem VPN -> dane są szyfrowane i przesyłane w tunelu -> serwer VPN odszyfrowuje dane i przekazuje je do celu -> odpowiedź wraca tą samą drogą

65

Rodzaje sieci

- **VPN** (Virtual Private Network) – sieć wirtualna

zalety:

szyfrowanie danych -> większe bezpieczeństwo w Internecie

ochrona prywatności -> maskowanie IP

możliwość pracy zdalnej i korzystania z zasobów firmowych

wady:

spadek prędkości Internetu (szyfrowanie + dodatkowy serwer)

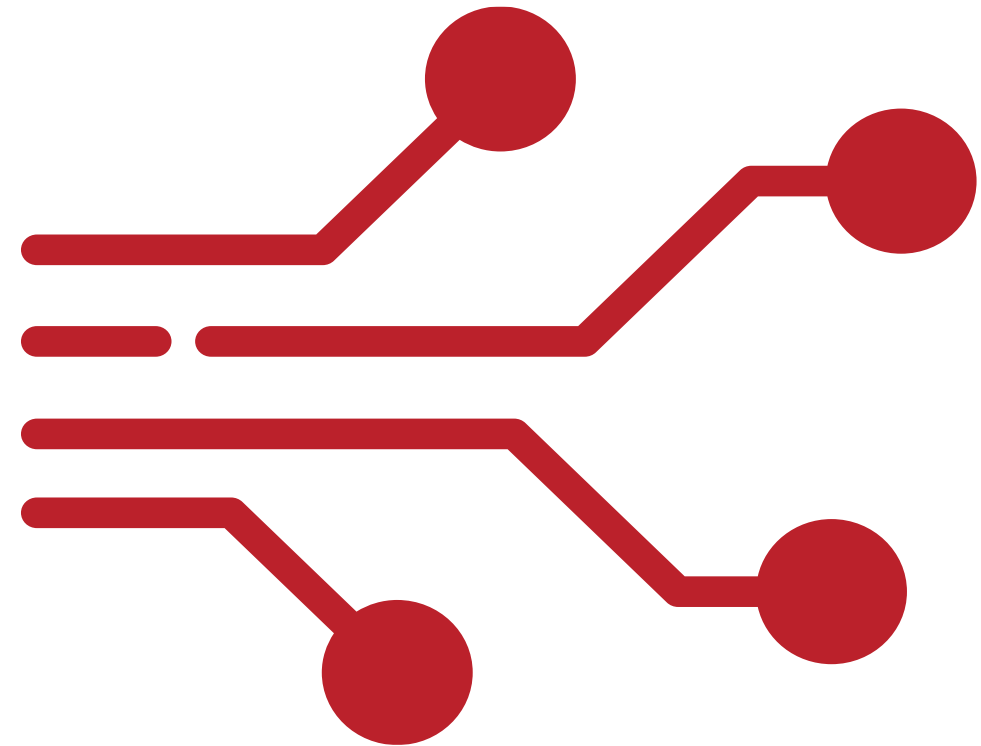
wymaga instalacji klienta VPN i konfiguracji

część serwisów blokuje ruch VPN (np. Netflix, banki)

bezpieczeństwo zależy od dostawcy - darmowe VPN mogą być ryzykowne

66

Typy transmisji



Rodzaje transmisji

Transmisję danych można klasyfikować według:

- Kierunku przepływu danych
- Trybu przesyłania sygnału (szeregową/równoległą)
- Synchronizacji (synchroniczna/asynchroniczna)
- Sposobu przesyłania w czasie (strumieniowa/pakietowa)
- Nośnika transmisji (przewodowa/bezprzewodowa – dodatkowo)

Rodzaje transmisji – kierunki przepływu

Simplex (jednokierunkowa):

Dane przesyłane tylko w jednym kierunku

Odbiorca nie ma możliwości odpowiedzi do nadawcy

Przykłady: telewizja kablowa, radio FM, ekrany informacyjne, tablice LED

Half-duplex (dwukierunkowa, naprzemienna):

Możliwa komunikacja w obie strony, ale tylko jedna strona nadaje w danej chwili

Wymaga mechanizmu przełączania nadawania/odbioru (np. przycisk PTT – „push-to-talk”)

Przykłady: krótkofalówki, CB radio, stare sieci LAN z magistralą (Ethernet na kablu koncentrycznym)

Full-duplex (dwukierunkowa, jednoczesna):

Oba urządzenia mogą nadawać i odbierać w tym samym czasie

Najbardziej wydajny tryb – brak czekania na zwolnienie medium

Przykłady: telefonia przewodowa i komórkowa, współczesne sieci LAN

Rodzaje transmisji – tryby przesyłania

Szeregowa:

Bity przesyłane jeden po drugim

Wolniejsza w teorii, ale praktycznie wydajniejsza przy dużych odległościach

Przykłady: USB, Ethernet, PCI Express

Równoległa:

Wiele bitów naraz, osobnymi liniami

Szybka na krótkich dystansach

Przykłady: magistrale komputerowe (ATA, stary PCI)

70

Rodzaje transmisji – synchronizacja

Transmisja synchroniczna:

Przesyłanie danych w takt sygnału zegara

Wymaga synchronizacji nadawcy i odbiorcy

Bardzo wydajna – brak bitów start/stop

Przykłady: SONET, SPI

Transmisja asynchroniczna:

Dane przesyłane w dowolnym momencie

Każda jednostka (np. bajt) poprzedzona bitem start i zakończona bitem stop

Prosta i tania w implementacji, mniej wydajna

Przykłady: RS-232, ATM, UART, Ethernet, USB

71

Rodzaje transmisji – sposób przesyłania

Transmisja pakietowa:

Dane dzielone na pakiety zawierające adresy, kontrolę błędów, itp.

Umożliwia multipleksację (wspólne medium dla wielu użytkowników)

Podstawa działania Internetu (TCP/IP, UDP)

Elastyczna i odporna na błędy

Transmisja strumieniowa:

Ciągły strumień danych w czasie rzeczywistym

Ważna jest minimalizacja opóźnień (latencja)

Stosowana w multimediami: VoIP, wideokonferencje, transmisje live

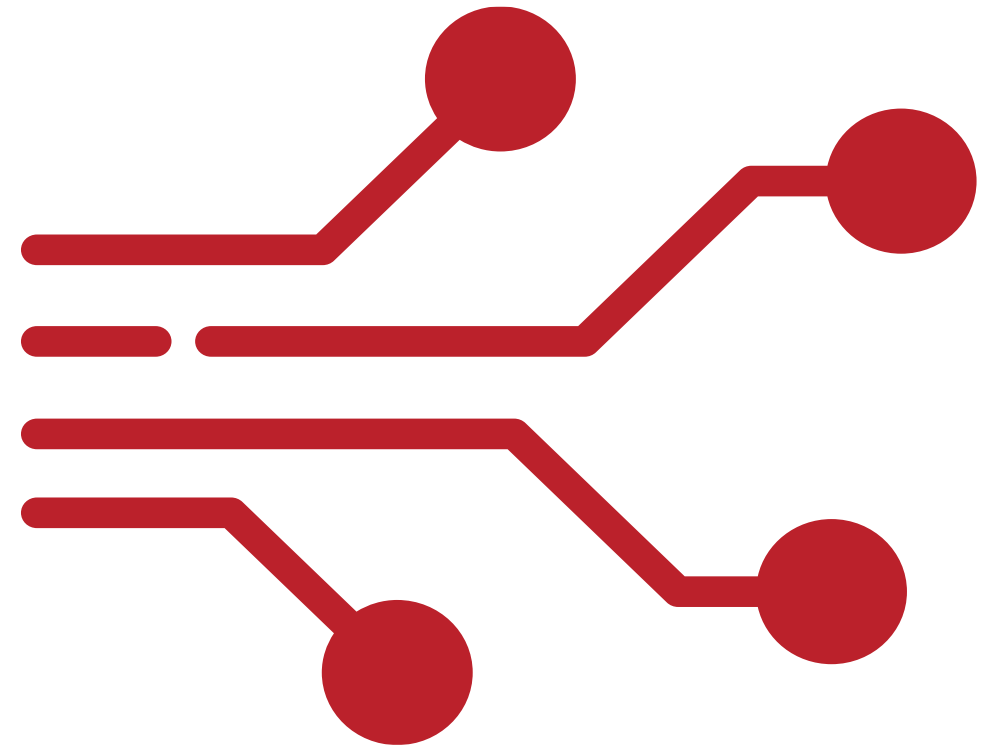
Często wymaga QoS (Quality of Service)

Tryby transmisji

Tryb transmisji	Kierunek	Adres docelowy	Przykład
Unicast	1 → 1	Pojedynczy host	WWW, e-mail, SSH
Broadcast	1 → Wszystkie	FF:FF:FF:FF:FF:FF	ARP Request, DHCP Discover
Multicast	1 → Wiele wybranych	Zakres 224.0.0.0/4 (IPv4)	IPTV, wideokonferencje
Anycast	1 → Najbliższy z wielu	Adres współdzielony	DNS, CDN, serwery routingu

73

Topologie sieci komputerowych



74

Topologia sieci komputerowej

Topologia sieci komputerowej to sposób fizycznego lub logicznego rozmieszczenia urządzeń (komputerów, serwerów, drukarek, routerów itp.) oraz sposobu ich połączenia przewodami lub sygnałem bezprzewodowym

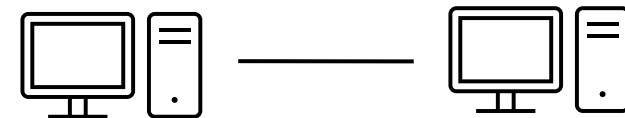
Rodzaje:

- topologia fizyczna – jak faktycznie urządzenia są połączone kablami/urządzeniami
- topologia logiczna – jak dane przepływają w sieci (np. kolejność przekazywania pakietów)

75

Topologia punkt-punkt (Point-Point)

- Najprostsza forma połączenia sieciowego
- Łączy bezpośrednio dokładnie dwa urządzenia
- Może być przewodowa lub bezprzewodowa
- Brak ryzyka kolizji – kanał używany tylko przez dwa urządzenia
- Brak skalowalności
- Awaria kable = całkowite przerwanie połączenia



76

Topologia magistrali (Bus)

- Używany jest pojedyncze medium transmisyjne – najczęściej kabel współosiowy (koncentryczny)
- Wszystkie urządzenia są podłączone do jednego kabla (równolegle) – magistrali
- Umożliwia przesyłanie danych w sieci w obu kierunkach
- Na końcach kabli – terminatory – zapobiegają odbijaniu się sygnału
- Jedno urządzenie nadaje -> sygnał dociera do wszystkich urządzeń -> odczytuje tylko adresat

77

Topologia magistrali (Bus)

Zalety:

Niska cena (małe zużycie kabla, brak urządzeń pośredniczących w dostępie do medium)

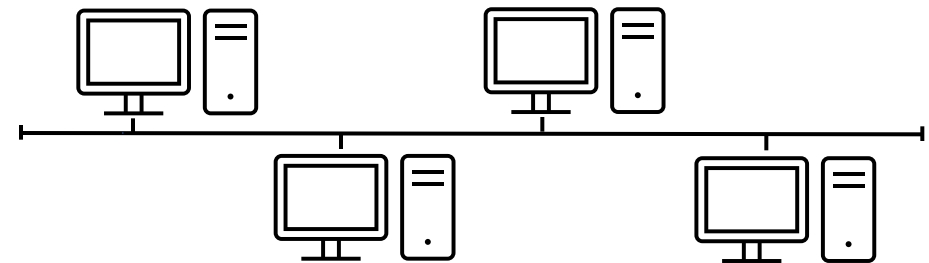
Łatwość instalacji

Wady:

Kolizje danych (gdy dwa komputery nadają jednocześnie)

Wydajność drastycznie spada przy dużej liczbie urządzeń

Wrażliwość na awarie (awaria jednego kabla = awaria całej sieci)



Topologia pierścienia (Ring)

- Bezpośrednie połączenie urządzeń (z dwoma sąsiadami) – brak koncentratora
- Całość tworzy krąg
- Dane wędrują w jedną stronę (czasem w obie – „dual ring”)
- Wykorzystuje tzw. **token** (żeton dostępu) – specjalny sygnał, który uprawnia urządzenie do nadawania
- Każde urządzenie pełni funkcję regeneratora sygnału

79

Topologia pierścienia (Ring)

Zalety:

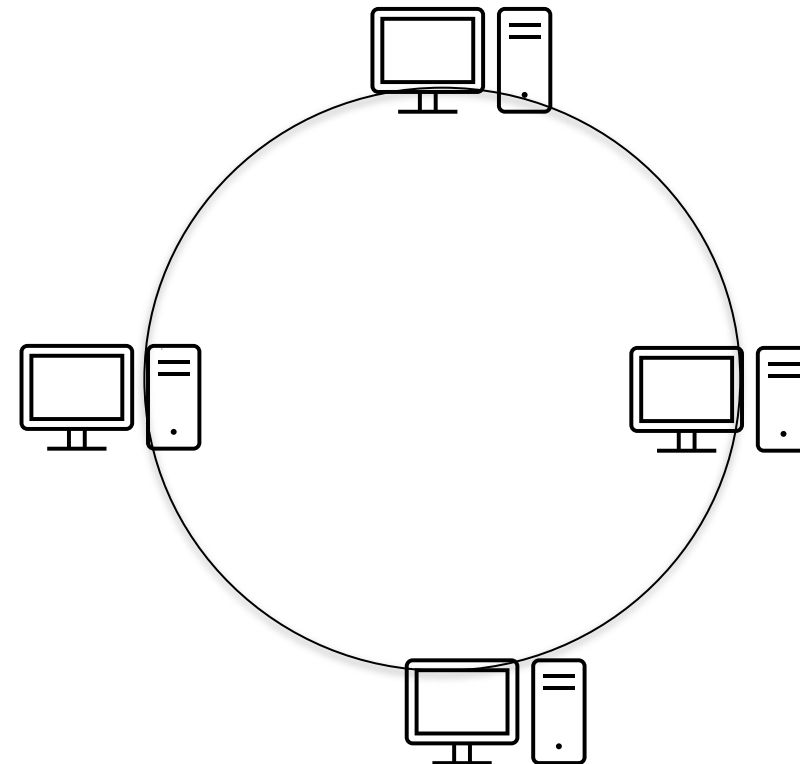
Niska cena (małe zużycie kabla, brak urządzeń pośredniczących w dostępie do medium)

Różne media transmisyjne (kabel koncentryczny, skrętka, światłowód)

Wady:

Trudności w rozbudowie i konserwacji sieci

Wrażliwość na awarie (uszkodzenie jednego z urządzeń = awaria całej sieci)



80

Topologia podwójnego pierścienia (Dual Ring)

Zasady jak w topologii pierścienia – urządzenia połączone podwójnym pierścieniem

- Pierścień główny – przesyła dane
- Pierścień zapasowy – używane w razie awarii

Oba pierścienie mogą działać równolegle (większa przepustowość) lub jeden pasywnie

W przypadku awarii jednego urządzenia sieć zachowuje możliwość działania w pełnym zakresie

81

Topologia podwójnego pierścienia (Dual Ring)

Zalety:

Wysoka niezawodność (redundancja)

Szybkie przełączanie w przypadku awarii

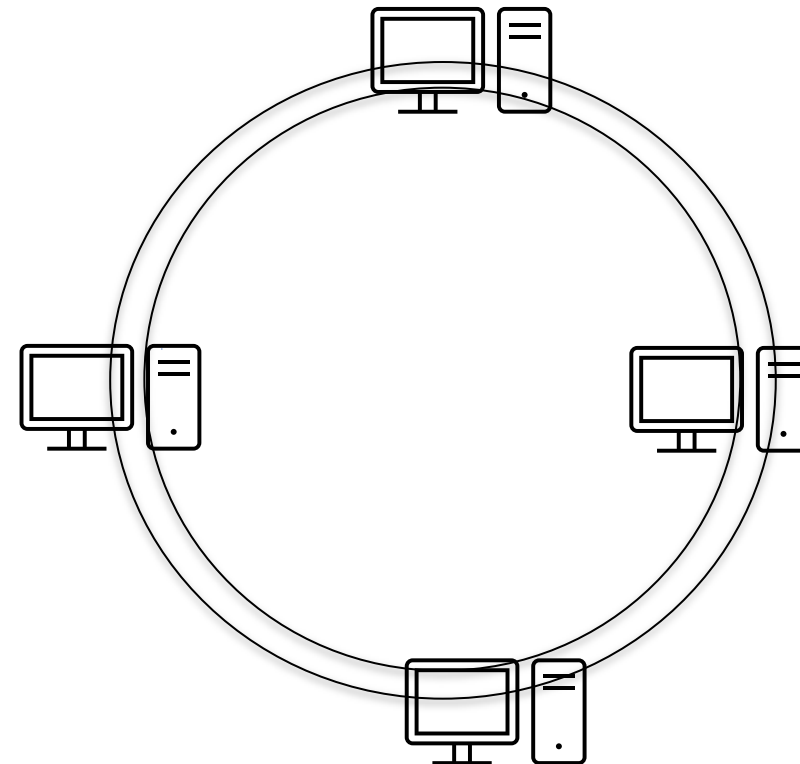
Brak pojedynczego punktu awarii jak w pojedynczym pierścieniu

Wady:

Wyższe koszty (podwójne okablowanie)

Bardziej skomplikowana konfiguracja

Zastosowania: sieci miejskie (MAN), sieci operatorskie i przemysłowe (niezawodność)



82

Topologia gwiazdy (Star)

- Podstawowa topologia w sieciach komputerowych
- Każde urządzenie jest połączone osobnym kablem do centralnego punktu – switcha lub huba
- Komunikacja odbywa się tylko poprzez centralny punkt
- Zastosowanie różnych mediów transmisyjnych
- Sieci Wi-Fi też są logiczną gwiazdą – centralny punkt to router Wi-Fi

83

Topologia gwiazdy (Star)

Zalety:

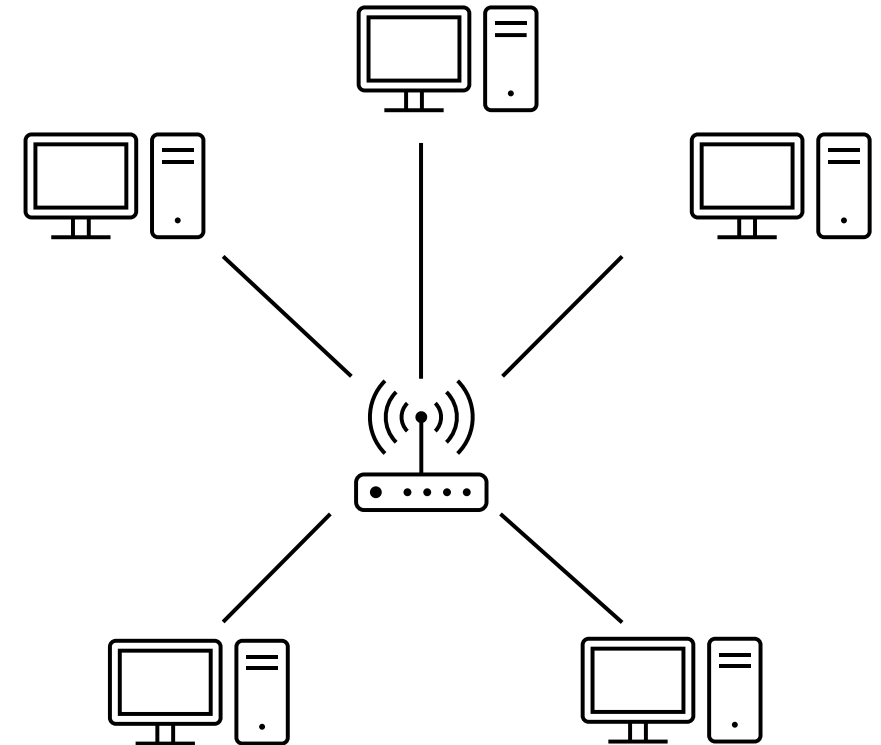
Przejrzystość konstrukcji

Odporność na awarię urządzeń oraz łączy

Wady:

Wysoki koszt okablowania (każde urządzenie potrzebuje oddzielnego przewodu)

Centralny punkt jest „single point of failure” – jeśli ulegnie awarii = cała sieć ulega awarii



84

Topologia rozszerzonej gwiazdy (Extended Star)

- Odmiana klasycznej gwiazdy, w której do centralnego urządzenia (zwykle przełącznika lub routera) nie podłączamy wszystkich komputerów bezpośrednio, tylko podgwiazdy
- W centrum sieci jest główny przełącznik - do niego podłączone są inne przełączniki, z których każdy obsługuje swoją grupę komputerów
- Układ hierarchiczny, gdzie centralny switch jest „rdzeniem”, a pozostałe przełączniki – „gałęziami”

85

Topologia rozszerzonej gwiazdy (Extended Star)

Zalety:

Bardzo dobra skalowalność – łatwo rozbudować sieć o nowe segmenty

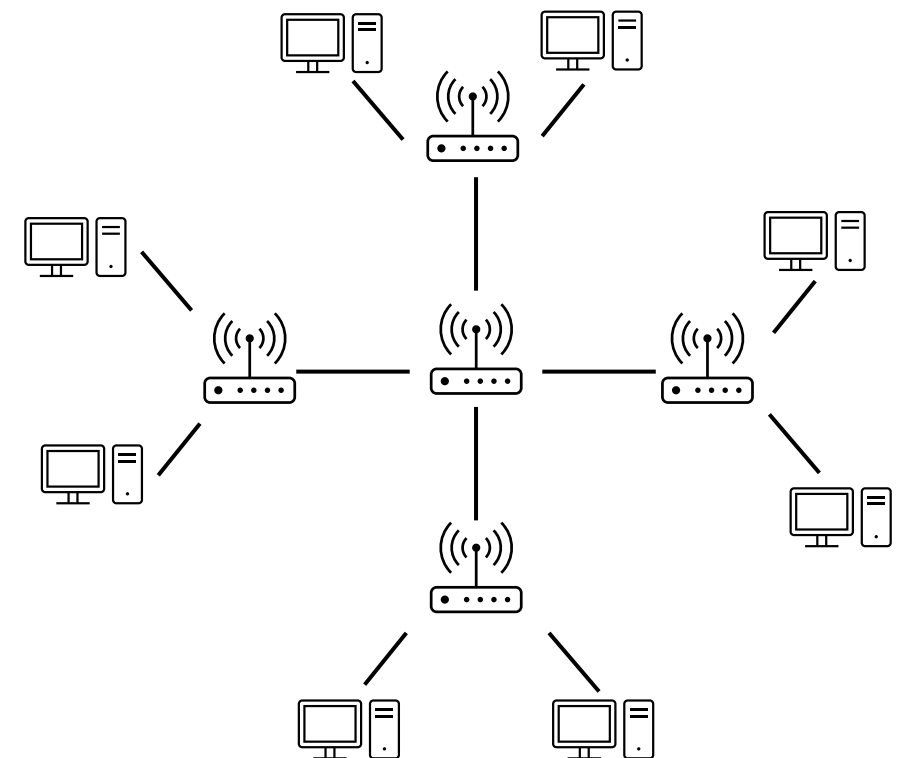
Awaria jednego przełącznika „gałęzi” nie zatrzymuje całej sieci (tylko dany segment)

Uporządkowana, hierarchiczna struktura – łatwa do zarządzania

Wady:

Awaria głównego przełącznika w centrum = awaria całej sieci

Zwiększony koszt sprzętu (wiele przełączników, więcej kabli)



86

Topologia siatki (Mesh)

- Każdy węzeł jest połączony z wieloma innymi (częściowa siatka) albo ze wszystkimi (pełna siatka)
- Istnieje wiele ścieżek przesyłania danych – jeśli jedno łącze zawiedzie, pakiet wybierze inną trasę
- Internet (trzon sieci opiera się na topologii siatki)
- Sieci wojskowe (odporność na awarie)

87

Topologia siatki (Mesh)

Zalety:

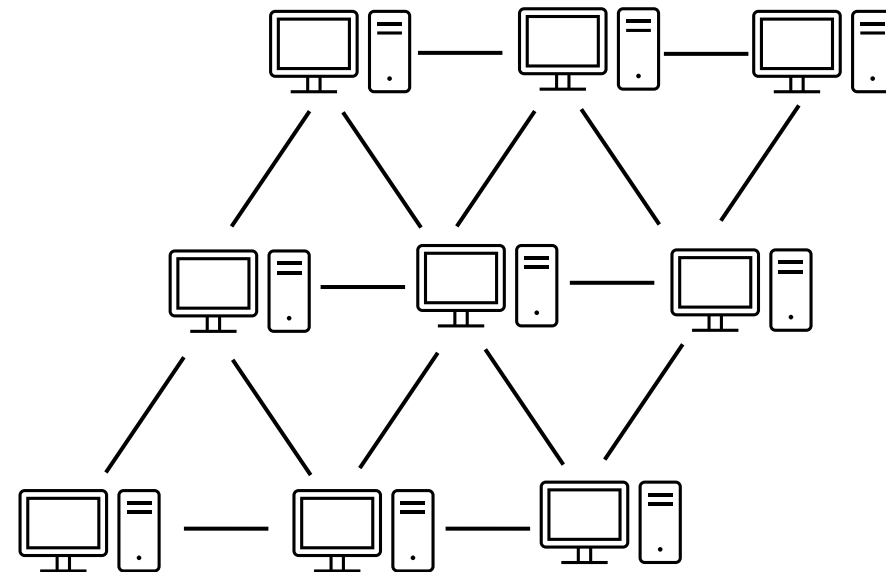
Bardzo wysoka niezawodność – awaria jednego węzła lub łącza nie powoduje przerwy w działaniu sieci (dane mogą iść inną ścieżką)

Redundancja połączeń – wiele dróg do przesyłania pakietów

Bezpieczeństwo – trudniej zakłócić lub podsłuchać całą sieć

Skalowalność logiczna – łatwo dodawać urządzenia w sieciach częściowej siatki

Wysoka wydajność – brak centralnego wąskiego gardła



Topologia siatki (Mesh)

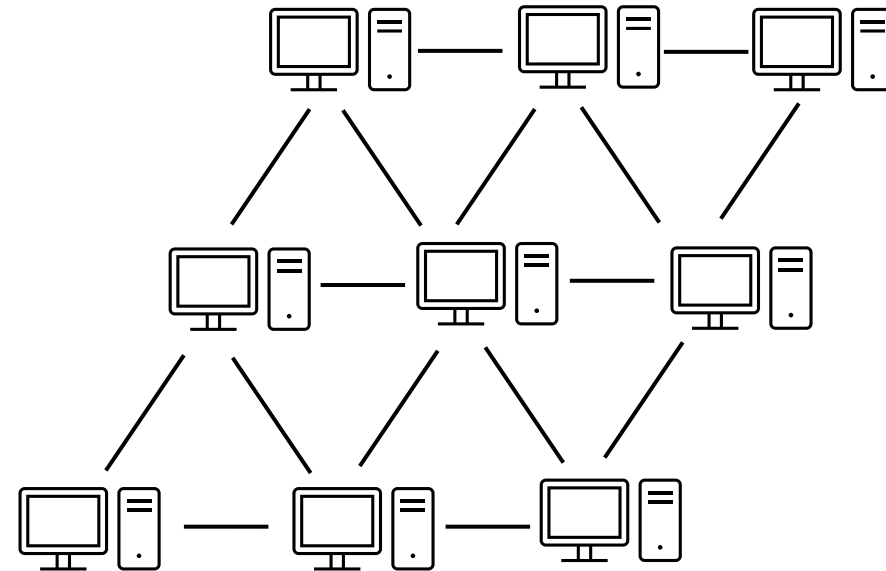
Wady:

Koszt – ogromne zużycie kabli i kart sieciowych przy pełnej siatce (dla n urządzeń liczba połączeń = $n(n-1)/2$)

Złożoność – trudna instalacja i utrzymanie, szczególnie w dużych sieciach

Nadmiarowość – wiele łączy bywa niewykorzystywanych

Nieopłacalna w małych sieciach LAN – bardziej sensowna w sieciach rozległych (WAN, sieci operatorskie)



89

Topologia hierarchiczna (Tree)

- Urządzenia są połączone w warstwach
- Na samej górze znajduje się urządzenie główne (np. router lub centralny switch)
- Pod nim znajdują się kolejne przełączniki, które łączą się z urządzeniami końcowymi (komputery, serwery)
- Struktura przypomina drzewo odwrócone:

korzeń (root) → gałęzie → liście

W praktyce jest to rozwinięcie topologii gwiazdy - gwiazdy połączone między sobą w większą strukturę

Topologia hierarchiczna (Tree)

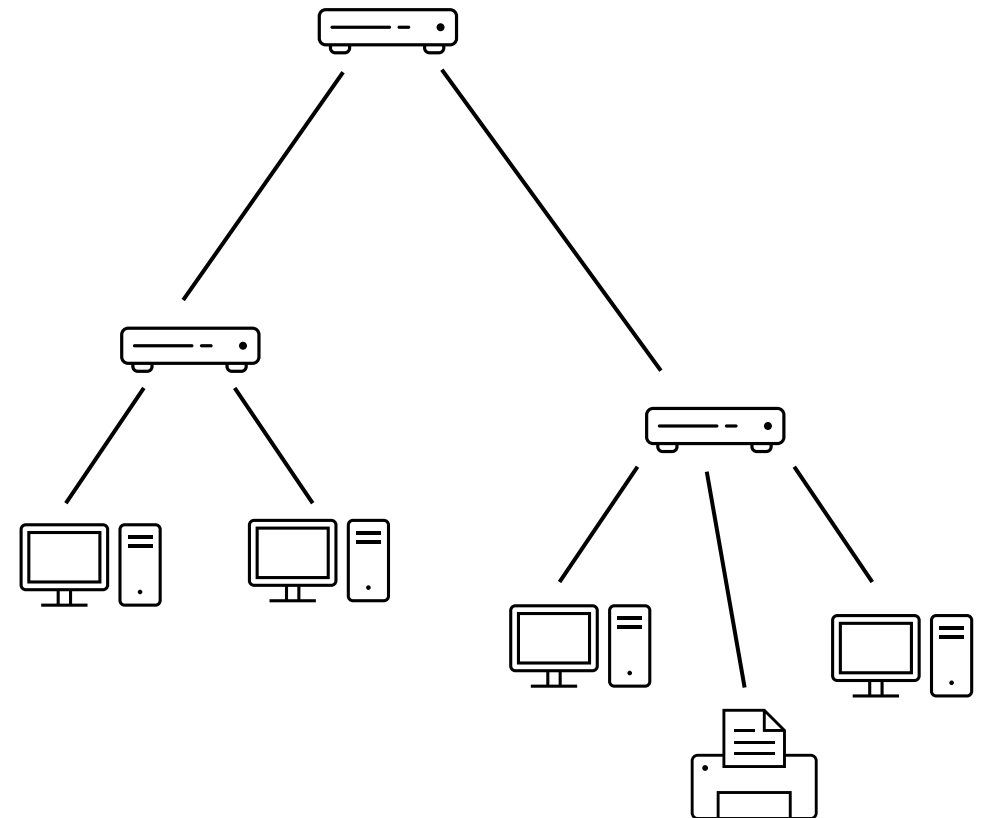
Zalety:

Łatwa rozbudowa – można dodawać kolejne gałęzie drzewa (np. nowe przełączniki z komputerami)

Uporządkowana struktura – dobrze odwzorowuje hierarchię sieci (rdzeń -> dystrybucja -> dostęp)

Izolacja awarii – problem w jednej gałęzi nie zatrzymuje całej sieci

Skalowalność – można obsługiwać bardzo duże sieci



91

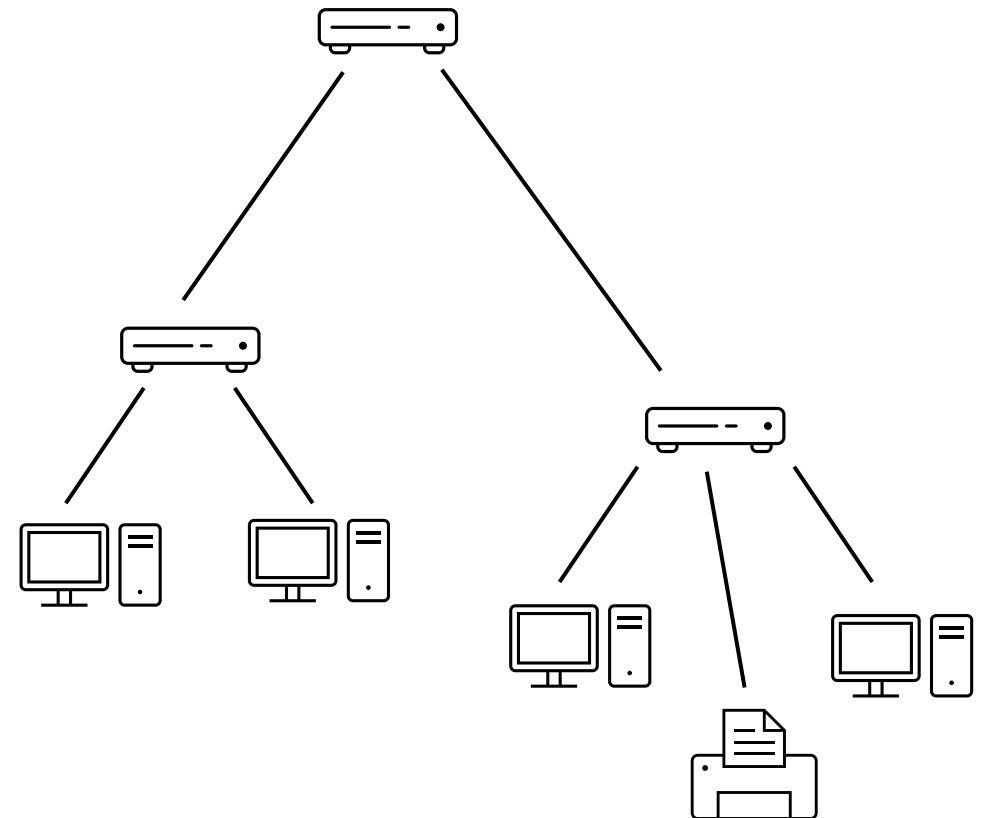
Topologia hierarchiczna (Tree)

Wady:

Awaria głównego urządzenia (korzenia drzewa, np. routera) = awaria sieci

Złożona administracja – wymaga planowania hierarchii i konfiguracji wielu przełączników

Duża zależność od jakości kabli i sprzętu – aby utrzymać wydajność na całej głębokości drzewa



92

Topologia hybrydowa

- Łączy różne topologie, aby wykorzystać ich zalety
- Przykład: sieć firmowa, gdzie biura w budynku są połączone w gwiazdy, a budynki łączy pierścień lub siatka
- Zastosowania:
 - Sieci korporacyjne
 - Duże centra danych
 - Infrastruktury miejskie

Wady:

Złożona, wymaga starannego projektowania

Kosztowna

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

93

Dofinansowane przez
Unię Europejską



Topologia sieci

Topologia	Zalety	Wady
Punkt-punkt	Prosta, niezawodna	Brak skalowalności
Magistrala	Tania, łatwa w instalacji	Kolizje, awaria kabla = awaria sieci
Gwiazda	Łatwa rozbudowa, niezależność hostów	Awaria węzła centralnego = brak działania
Pierścień	Brak kolizji, uporządkowany dostęp	Awaria jednego węzła = awaria całej sieci
Siatka	Bardzo odporna na awarie	Kosztowna, trudna w budowie
Drzewo	Skalowalna, hierarchiczna	Awaria wyższych poziomów = awaria sieci
Hybrydowa	Elastyczne, praktyczne	Większa złożoność i koszt

94

Dziękuję za uwagę

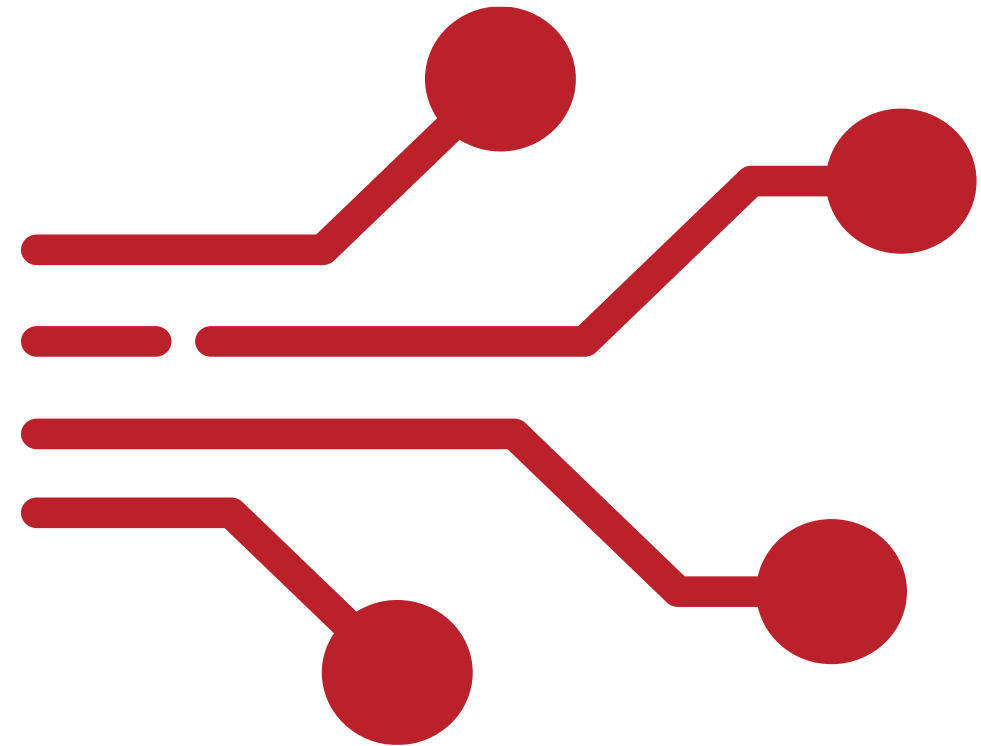
Treści programowe:

- Modele sieciowe: model TCP/IP, model OSI. Warstwy i ich funkcje
- Przykłady protokołów w różnych warstwach (np. HTTP, TCP, IP, Ethernet)



96

Modele sieciowe



97

Modele sieciowe

Komunikacja urządzeń w sieci komputerowej składa się z kilku etapów (elementów)

Każdy z nich realizuje inne zadania niezbędne do poprawnej komunikacji

Etapy określone są przez **modele warstwowe**

Istnieją dwa modele warstwowe:

Model protokołów **TCP/IP**

Model odniesienia **ISO/OSI**

98

Modele sieciowe

Korzyści z podziału procesu komunikacji sieciowej na warstwy:

- łatwiejsze określenie reguł i zasad komunikacji:
protokoły komunikacyjne
- Możliwość współdziałania urządzeń sieciowych i oprogramowania różnych producentów
- Logiczna struktura procesu komunikacji
- Zarządzanie i kontrola poprawności komunikacji

99

Modele sieciowe

Model **TCP/IP**:

- Model protokołów
- Każda z warstw wykonuje konkretne zadania za pomocą odpowiednich protokołów

Model **ISO/OSI**:

- Model odniesienia
- Stosowany do analizy w celu zrozumienia procesów komunikacyjnych

100

Model TCP/IP

- **Warstwa aplikacji**
- **Warstwa transportowa**
- **Warstwa internetowa**
- **Warstwa dostępu do sieci**

APLIKACJI

TRANSPORTOWA

INTERNETOWA

DOSTĘPU DO SIECI

101

Model TCP/IP – Warstwa aplikacji

- Najbliższa użytkownikowi – definiuje sposób w jaki aplikacje korzystają z sieci
- Pakiety danych w warstwie aplikacji – **komunikaty**
- Protokoły usług sieciowych:
 - **HTTP/HTTPS** (strony WWW)
 - **SMTP, IMAP, POP3** (poczta e-mail)
 - **FTP, SFTP** (przesył plików)
 - **DNS** (rozwiązywanie nazw)
 - **SSH, Telnet** (zdalne logowanie)

102

Model TCP/IP – Warstwa transportowa

- Przesyła komunikaty warstwy aplikacyjnej między urządzeniami
- Pakiety danych w warstwie transportowej – **segmenty, datagramy**
- Protokoły usług sieciowych:
 - **TCP** – usługa połączeniowa, niezawodność transmisji, kontrola przepływu, dzieli długie komunikaty na krótsze segmenty i zapewnia mechanizm kontroli przeciążenia sieci
 - **UDP** - usługa bezpołączeniowa – szybka transmisja, bez zapewnienia niezawodności ani kontroli przepływu i przeciążenia
- Przykład: TCP (strony WWW), UDP (gry online)

103

Model TCP/IP – Warstwa internetowa

- Przesyła pakiety od jednego hosta do drugiego
- Pakiety danych w warstwie internetowej – **pakiety**
- Obejmuje protokół IP (adres logiczny) oraz protokoły **routingu** (wyznaczania trasy dla datagramów)
- Protokoły usług sieciowych:
 - **IP (IPv4, IPv6)** – adresacja logiczna i trasowanie pakietów
 - **ICMP** – komunikaty kontrolne i diagnostyczne (ping, traceroute)
 - **IGMP** – obsługa **multicastu** (transmisja grupowa)
 - **ARP** – tłumaczenie adresów IP -> MAC

104

Model TCP/IP – Warstwa dostępu do sieci

- Odpowiada za fizyczne przesyłanie danych przez medium transmisyjne (kable, fale radiowe)
- Pakiety danych w warstwie dostępu do sieci – **ramki**
- Zawiera mechanizmy adresowania MAC, wykrywanie błędów i kontroli dostępu do medium
- Protokoły usług sieciowych:
 - **Ethernet** – sieci przewodowe (LAN)
 - **Wi-Fi (IEEE 802.11)** – sieci bezprzewodowe LAN (WAN)
 - **PPP** – połączenie punkt-punkt (modemy DSL)

105

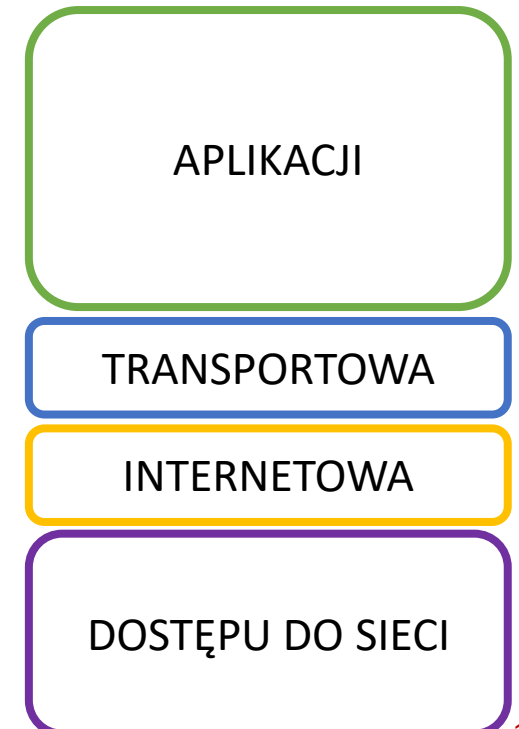
Model ISO/OSI

- Warstwa aplikacji
- Warstwa prezentacji
- Warstwa sesji
- Warstwa transportowa
- Warstwa sieci
- Warstwa łącza danych
- Warstwa fizyczna

ISO/OSI



TCP/IP



106

Model ISO/OSI – Warstwa prezentacji

- Tłumaczy dane na format zrozumiały dla aplikacji
- Odpowiada za formatowanie, szyfrowanie i kompresję danych
- Zapewnia, że dane są zrozumiałe dla obu stron (np. kodowanie znaków ASCII/UTF-8)
- Funkcje: translacja danych, kompresja, szyfrowanie (SSL/TLS)

107

Model ISO/OSI – Warstwa sesji

- Kontrola dialogu między aplikacjami
- Zarządza sesjami komunikacyjnymi między aplikacjami
- Umożliwia ich otwieranie, utrzymywanie i zamykanie
- Przykład: logowanie do serwera, utrzymywanie połączenia w wideokonferencji

108

Model ISO/OSI – Warstwa łączy danych

- Zajmuje się transmisją ramek w obrębie jednej sieci lokalnej (LAN)
- Odpowiada za adresy MAC, detekcję i korekcję błędów
- Podwarstwy: **LLC** (Logical Link Control) i **MAC** (Media Access Control)
- Protokoły usług sieciowych:
 - **Ethernet** – sieci przewodowe (LAN)
 - **Wi-Fi (IEEE 802.11)** – sieci bezprzewodowe LAN (WAN)
 - **PPP** – połączenie punkt-punkt (modemy DSL)
 - **ARP** – tłumaczenie adresów IP -> MAC

109

Model ISO/OSI – Warstwa fizyczna

- Zamiana danych na sygnały elektryczne/światłne/radiowe i odwrotnie
- Najniższa warstwa – odpowiada za fizyczne przesyłanie bitów w medium transmisyjnym
- Określa standardy: kable, fale radiowe, napięcia, złącza, sygnały
- Przykłady: kabel miedziany, światłowód, Bluetooth, USB

110

Warstwa aplikacji – model TCP/IP

- Zapewnia usługi sieciowe dla użytkownika i aplikacji
- Umożliwia działanie programów korzystających z sieci (np. przeglądarki, poczta, komunikatory)
- Definiuje protokoły aplikacyjne – np. HTTP, HTTPS, FTP, SMTP, DNS.
- Z punktu widzenia aplikacji – sieć jest przezroczysta, hosty „rozmawiają bezpośrednio”
- Współpracuje z warstwą transportową, która dodaje porty i zapewnia dostarczenie
- Jednostki danych: **komunikaty**

Warstwa aplikacji – model TCP/IP

Rodzaje architektury aplikacji:

- **Klient – Serwer** – zawsze występuje host (**serwer**), który obsługuje żądania przychodzące od wielu hostów (**klientów**)
- **P2P** – bezpośrednie połączenie pomiędzy parami tymczasowo połączonych hostów (**węzły**)
- Architektura hybrydowa – połączenie powyższych: np. serwer śledzący adresy IP hostów, a dane przekazywane bezpośrednio pomiędzy nimi (bez przechodzenia przez serwery)

112

Warstwa aplikacji – model TCP/IP

Komunikacja aplikacji odbywa się za pomocą komunikacji procesów – programów uaktywnionych w systemie operacyjnym końcowego użytkownika

Reguły komunikacji określa system operacyjny hosta

Komunikacja procesów dwóch różnych systemów końcowych – wymiana komunikatów za pośrednictwem sieci komputerowej

Proces nadawczy – tworzy komunikaty i umieszcza je w sieci

Proces odbiorczy – otrzymuje te komunikaty i ewentualnie odpowiada własnymi komunikatami

113

Warstwa aplikacji – model TCP/IP

Każdy komunikat wysłany przez jeden proces do drugiego jest umieszczany w gnieździe i przebywa drogę przez sieć

Gniazdo – interfejs używany przez program w warstwie aplikacji w celu wysłania / odebrania danych

Gniazdo określa się też mianem

API (Application Programming Interface) – interfejs programowania pośredniczący pomiędzy aplikacją a siecią

114

Warstwa aplikacji – model TCP/IP

Wybrane aplikacje sieciowe i ich protokoły warstwy aplikacji

<i>Zastosowanie</i>	<i>Protokół warstwy aplikacji</i>	<i>Architektura</i>
Poczta elektroniczna	SMTP (RFC 5321)	klient - serwer
Zdalny dostęp terminalowy	Telnet (RFC 854)	klient - serwer
Technologia WWW	HTTP (RFC 2616)	klient - serwer
Transfer plików	FTP (RFC 959)	klient - serwer
Telefonia internetowa	SIP (RFC 3261), RTP (RFC 3550) lub niestandardowy (np. Skype)	hybryda

115

Warstwa aplikacji - HTTP

HTTP (Hypertext Transfer Protocol) – podstawowy składnik technologii WWW

Wykorzystywany w aplikacji zarówno klienta (wysyła żądanie), jak i serwera (zwraca odpowiedź)

HTTP jest bezstanowy - każde żądanie jest niezależne

Strona WWW – dokument złożony z obiektów

Obiekt – plik HTML, plik graficzny JPEG, aplik apletu JAVA, plik audio MP3, itd.

116

Warstwa aplikacji - HTTP

Specyfikacja HTTP określa 2 typy komunikatów:

- Komunikat żądania – wysyłany do serwera
- Komunikat odpowiedzi – zwracany przez serwer do klienta

Obydwa zapisane w formacie ASCII

117

Warstwa aplikacji - HTTP

Komunikat żądania - przykład

GET /index.html HTTP/1.1

Host: www.przyklad.pl

User-Agent: Mozilla/5.0

Accept: text/html

Accept-language: pl

- wiersz żądania
- wiersz nagłówka
- wiersz nagłówka
- wiersz nagłówka
- wiersz nagłówka

118

Warstwa aplikacji - HTTP

Komunikat żądania - przykład

GET /index.html HTTP/1.1

- Wiersz żądania – 3 pola:

- Pole metody:
- Pole adresu URL:
- Pole wersji protokołu HTTP:

GET
/index.html
HTTP/1.1

119

Warstwa aplikacji - HTTP

Dostępne metody:

GET – pobranie zasobu

POST – przesłanie danych (np. formularz)

PUT – aktualizacja zasobu

DELETE – usunięcie zasobu

HEAD – tylko nagłówki odpowiedzi (bez treści)

OPTIONS – zapytanie o dostępne metody

120

Warstwa aplikacji - HTTP

Host: www.przyklad.pl - obowiązkowy w HTTP/1.1

Informuje, do której domeny kierowane jest żądanie - jeden serwer może obsługiwać wiele domen (tzw. virtual hosting)

User-Agent: Mozilla/5.0 - identyfikuje klienta (przeglądarkę, wersję, system)

Serwer może używać tej informacji np. do dostosowania treści

121

Warstwa aplikacji - HTTP

Accept: text/html - jakie typy treści (MIME types) klient akceptuje w odpowiedzi

Przeglądarka prosi o stronę w formacie HTML

Accept-language: pl – negocjowanie treści - preferowany język odpowiedzi

Klient woli wersję polską strony, jeśli serwer ją posiada

122

Warstwa aplikacji - HTTP

Komunikat żądania - przykład

HTTP/1.1 200 OK

Date: Wed, 03 Sep 2025 12:00:00 GMT

Server: Apache/2.4.57 (Unix)

Content-Type: text/html; charset=UTF-8

Content-Length: 137

<html> ... </html>

123

Warstwa aplikacji - HTTP

Komunikat żądania - przykład

HTTP/1.1 200 OK – wersja protokołu, kod statusu (sukces), testowy opis kodu

Date: Wed, 03 Sep 2025 12:00:00 GMT – kiedy serwer wygenerował odpowiedź

Server: Apache/2.4.57 (Unix) – identyfikacja oprogramowania serwera WWW

124

Warstwa transportowa – model TCP/IP

- Zapewnia **logiczną komunikację** między procesami aplikacji uruchomionymi na różnych hostach
- Z punktu widzenia aplikacji – hosty połączone ze sobą bezpośrednio
- Zapewnia podział danych na **segmenty** i ich poprawne złożenie
- Dodaje **numery portów** – dane trafiają do właściwego procesu
- Odpowiada za niezawodność i kontrolę przepływu (**TCP**)
- Jednostki danych: **segmenty (TCP)** lub **datagramy (UDP)**

125

Warstwa transportowa – model TCP/IP

Numery portów = numery identyfikujące aplikacje

Zakres: 0 – 65535 – w nagłówku TCP i UDP pole numeru portu nadawcy i odbiorcy ma 16 bitów

Liczba możliwych kombinacji = $2^{16} = 65535$

Porty:

0 – formalnie zarezerwowany, zwykle nie używany jako port docelowy

1–1023 – porty dobrze znane (systemowe)

1024–49151 – porty zarejestrowane

49152–65535 – porty dynamiczne

Warstwa transportowa - TCP

Przykład działania:

1. Przeglądarka chce pobrać stronę:
2. Serwer WWW nasłuchuje na porcie **80** (HTTP)
3. System operacyjny klienta przydziela losowy port dynamiczny (**51532**)
4. **Segment TCP:**

Źródło:	192.168.1.10:51532
Cel:	203.0.113.5:80
5. Dane HTTP przesyłane w segmentach TCP
6. Po zakończeniu transmisji – zamknięcie połączenia

127

Warstwa transportowa

<i>Zastosowanie</i>	<i>Protokół warstwy aplikacji</i>	<i>Protokół warstwy transportowej</i>	<i>Porty (domyślne)</i>
HTTP	Strony WWW	TCP	80
HTTPS	Strony WWW (szyfrowane TLS)	TCP	443
FTP	Transfer plików	TCP	21 (sterowanie) 20 (dane)
SMTP	Wysyłanie poczty	TCP	25 465, 587 (szyfrowany)
POP3	Pobieranie poczty	TCP	110 995 (szyfrowany)
IMAP	Pobieranie poczty (zaawansowany)	TCP	143 993 (szyfrowany)

Warstwa transportowa

<i>Zastosowanie</i>	<i>Protokół warstwy aplikacji</i>	<i>Protokół warstwy transportowej</i>	<i>Porty (domyślne)</i>
DNS	Tłumaczenie nazw – IP	UDP/TCP	53
DHCP	Przydzielanie adresów IP	UDP	67 (klient) 68 (serwer)
SSH	Zdalne logowanie (szyfrowane)	TCP	22
Telnet	Zdalne logowanie (nieszyfrowane)	TCP	23
SNMP	Zarządzanie usługami sieciowymi	UDP	161 (zapytania) 162 (pułapki)

129

Warstwa transportowa

<i>Zastosowanie</i>	<i>Protokół warstwy aplikacji</i>	<i>Protokół warstwy transportowej</i>	<i>Porty (domyślne)</i>
RDP	Zdalny pulpit Windows	UDP/TCP	3389
NTP	Synchronizacja czasu	UDP	123
TFTP	Prosty transfer plików	UDP	69

130

Warstwa transportowa – protokół TCP

Protokół **TCP (Transmission Control Protocol)**

Połączeniowy – wymaga nawiązania sesji (3-way handshake)

Niezawodny – retransmisje, potwierdzenia (ACK)

Uporządkowany – zachowana kolejność danych (numery sekwencji)

Kontrola przepływu – „okno” TCP (window size)

Kontrola przeciążenia – algorytmy (slow start, congestion avoidance)

Bardziej rozbudowany – nagłówek minimum 20 bajtów

131

Warstwa transportowa – protokół TCP

Połączeniowy – wymaga nawiązania sesji (3-way handshake)

Proces nawiązywania połączenia składa się z 3 kroków:

1. SYN (SYNCHRONIZE) – klient prosi o połączenie, wysyła swój początkowy numer sekwencji (ISN)

„Zacznijmy wymianę danych, mój numer startowy to 1001”

2. SYN+ACK(ACKNOWLEDGMENT) – serwer potwierdza i podaje swój własny ISN

„OK, mój numer startowy to 5000, potwierdzam twój 1001”

3. ACK – klient potwierdza numer serwera

„Potwierdzam twój 5001, zaczynamy wymianę danych”

132

Warstwa transportowa – protokół TCP

Niezawodny – retransmisje, potwierdzenia (ACK)

Każdy segment danych jest potwierdzany:

„Otrzymałem dane do bajtu nr X, czekam na kolejny”

Dzięki temu:

nadawca wie, że dane dotarły

w razie braku ACK → retransmisja

TCP może wysyłać ACK skumulowane – jedno potwierdzenie obejmuje wiele segmentów

133

Warstwa transportowa – protokół UDP

Protokół **UDP** (User Datagram Protocol)

Bezpołączeniowy – brak zestawiania sesji

Niezawodność NIE jest gwarantowana – brak ACK, brak retransmisji

Prostota i szybkość – mały nagłówek (8 bajtów)

Możliwe zgubione lub zdublowane pakiety

134

Warstwa transportowa - UDP

Przykład działania:

1. Klient chce zapytać serwer DNS o adres example.com
2. Serwer DNS nasłuchuje na porcie **53** (UDP)
3. System operacyjny klienta przydziela losowy port dynamiczny (**51532**)
4. **Datagram UDP:**
Źródło: 192.168.1.10:51532
Cel: 203.0.113.5:53
5. Serwer DNS odsyła odpowiedź w kolejnym datagramie UDP
6. Brak handshake, brak ACK

135

Warstwa internetowa – model TCP/IP

- Zapewnia adresację i trasowanie pakietów między hostami w różnych sieciach
- Odpowiada za dostarczenie pakietu IP z hosta źródłowego do docelowego
- Każdy pakiet zawiera adres źródłowy i docelowy IP
- Współpracuje z routerami, które wybierają najlepszą drogę (routing)
- Wykorzystuje protokoły pomocnicze: ICMP (komunikaty o błędach, ping), ARP/NDP (mapowanie IP ↔ MAC)
- Jednostka danych: **pakiet IP**

Warstwa internetowa – model TCP/IP

Główne protokoły:

- **IP (Internet Protocol)** – podstawowy protokół dostarczania pakietów
- **ICMP (Internet Control Message Protocol)** – komunikaty o błędach i diagnostyka
- **ARP (Address Resolution Protocol)** – mapowanie IP → MAC (IPv4)
- **NDP (Neighbor Discovery Protocol)** – mapowanie i konfiguracja w IPv6
- **IPsec (Internet Protocol Security)** – rozszerzenie IP zapewniające szyfrowanie

137

Warstwa internetowa – protokół IP

Odpowiada za adresację i trasowanie pakietów

IPv4: 32-bitowe adresy (np. 192.168.1.10)

IPv6: 128-bitowe adresy (np. 2001:db8::1)

Pola nagłówka IP:

Adres źródłowy i docelowy

TTL (Time To Live)

Protocol (TCP, UDP, ICMP...)

Checksum

138

Warstwa internetowa – protokół ICMP

Protokół wspierający działanie IP

Służy do raportowania błędów i testowania łączności

Typowe komunikaty:

Echo Request / Echo Reply → ping

Destination Unreachable – host/port niedostępny

Time Exceeded – TTL = 0

Redirect – informacja o lepszej trasie

139

Warstwa internetowa – protokół ARP

Służy do zamiany adresu IP → MAC w sieci lokalnej

Działa na zasadzie rozgłaszania (broadcast):

„Kto ma IP 192.168.1.1?”

Router odpowiada:

„Ja – mój MAC to 00:1A:2B:3C:4D:5E”

Niezbędny do komunikacji w Ethernet/Wi-Fi przy IPv4

140

Warstwa internetowa – protokół NDP (IPv6)

Zastępuje ARP w IPv6

Wykorzystuje ICMPv6

Funkcje:

- Mapowanie adresów IPv6 → MAC

- Autokonfiguracja adresów (stateless)

- Znajdowanie routerów i sąsiadów

- Wykrywanie duplikatów adresów

141

Warstwa internetowa – protokół IPsec

Rozszerzenie protokołu IP zapewniające bezpieczeństwo komunikacji

Funkcje:

Szyfrowanie (poufność)

Uwierzytelnianie (pewność źródła)

Integralność (ochrona przed modyfikacją)

Stosowany w: VPN, zabezpieczonych tunelach, komunikacji między routerami

142

Warstwa dostępu do sieci – model TCP/IP

- Zapewnia fizyczny przesył pakietów IP przez konkretne medium transmisyjne
- Odpowiada za:
 - adresację sprzętową (MAC)
 - format ramek (frames)
 - dostęp do medium (Ethernet, Wi-Fi, itp.)
 - wykrywanie błędów transmisji
- Jednostka danych: **ramka**

143

Warstwa dostępu do sieci – model TCP/IP

Adres MAC (Media Access Control) = sprzętowy adres karty sieciowej

Nadawany fabrycznie przez producenta

Długość: 48 bitów (6 bajtów)

Zapis szesnastkowy, np. 00:1A:2B:3C:4D:5E

Unikalny w skali całego świata

Pierwsze 24 bity – OUI (Organizationally Unique Identifier) - identyfikator producenta

Ostatnie 24 bity – numer karty nadany przez producenta

144

Warstwa dostępu do sieci – model TCP/IP

Bity specjalne:

I/G – unicast (0) / multicast (1)

U/L – globalny (0) / lokalny (1)

Unicast – do jednego odbiorcy

Broadcast – do wszystkich w sieci (FF:FF:FF:FF:FF:FF)

Multicast – do wybranej grupy odbiorców

145

Warstwa dostępu do sieci – model TCP/IP

Adres MAC:

Identyfikuje urządzenie w sieci lokalnej (LAN, Wi-Fi)

Konkretny host - ramka Ethernet

Routery zmieniają adresy MAC na każdym przeskoku, ale adresy IP zostają stałe

Powiązanie IP $\leftrightarrow$ MAC realizowane przez ARP (IPv4) lub NDP (IPv6)

146

Warstwa dostępu do sieci – model TCP/IP

Protokoły warstwy dostępu

Ethernet (IEEE 802.3) – najpopularniejszy w sieciach przewodowych

Wi-Fi (IEEE 802.11) – sieci bezprzewodowe

PPP (Point-to-Point Protocol) – łączy punkt–punkt (np. modem, WAN)

Frame Relay, ATM – starsze technologie WAN

Bluetooth (802.15) – krótkie zasięgi

147

Warstwa dostępu do sieci – protokół Ethernet

Sieci przewodowe

Ramka Ethernet zawiera:

- MAC źródłowy i docelowy
- pole EtherType (np. IPv4, IPv6, ARP)
- dane (pakiet IP)
- sumę kontrolną (CRC)

Szybkości: od 10 Mb/s do nawet 400 Gb/s i więcej

Wersje: Fast Ethernet, Gigabit Ethernet, 10/40/100 Gigabit Ethernet

148

Warstwa dostępu do sieci – protokół Wi-fi

Sieci bezprzewodowe

Obsługuje roaming (przenoszenie urządzeń), autoryzację (WPA2, WPA3), szyfrowanie

Ramka Wi-Fi ma strukturę podobną do Ethernetu, ale z dodatkowymi polami (np. identyfikator punktu dostępowego)

Wersje: 802.11b/a/g/n/ac/ax/be (Wi-Fi 4/5/6/7)

149

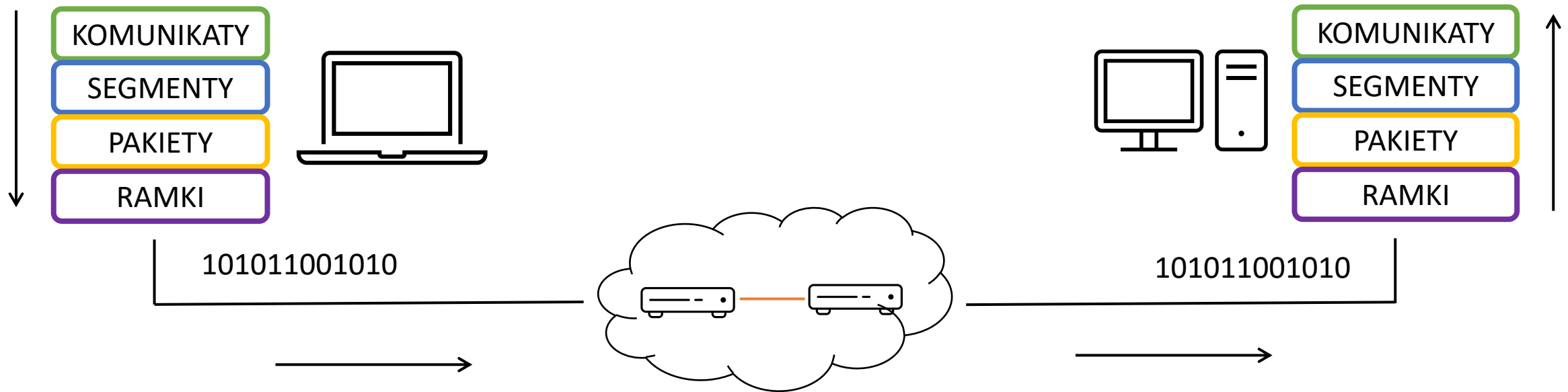
Warstwa dostępu do sieci – protokół Wi-fi

Wersje Wi-fi (IEEE):

802.11b	– 11 Mb/s, 2,4 GHz
802.11a	– 54 Mb/s, 5 GHz
802.11g	– 54 Mb/s, 2,4 GHz, zgodny z b
802.11n (Wi-Fi 4)	– do 600 Mb/s, 2,4 i 5 GHz
802.11ac (Wi-Fi 5)	– do kilku Gb/s, 5 GHz
802.11ax (Wi-Fi 6 / 6E)	– wyższa wydajność, 2,4 / 5 / 6 GHz
802.11be (Wi-Fi 7)	– w trakcie wdrażania, prędkości 30–40 Gb/s

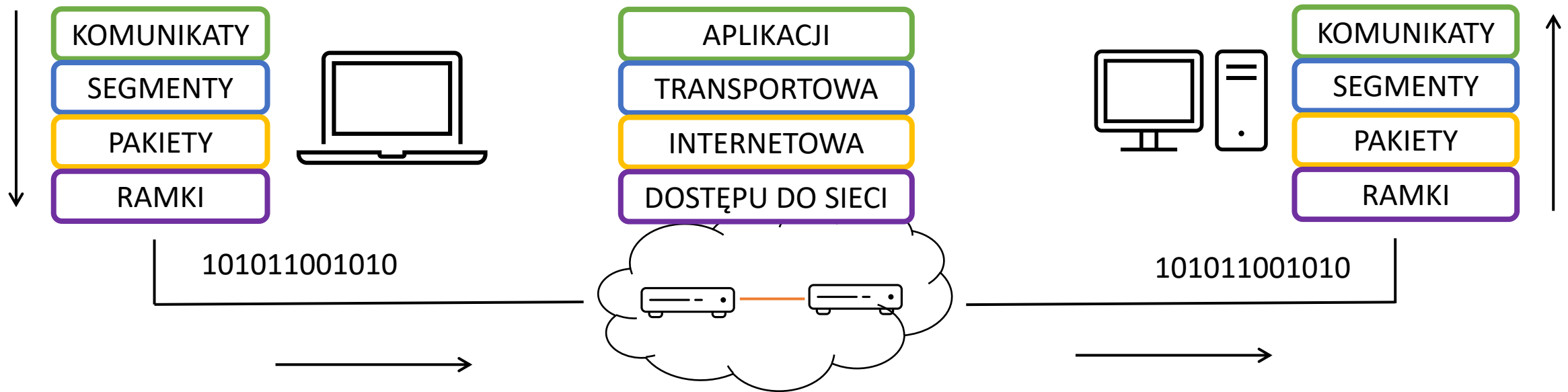
150

Enkapsulacja i dekapulacja



151

Enkapsulacja i dekapulacja



152

Enkapsulacja – wysyłanie danych

Proces „opakowywania” danych przy przechodzeniu w dół stosu protokołów TCP/IP

Każda warstwa dodaje własne informacje sterujące (nagłówki, stopki)

Enkapsulacja:

komunikat → segment/datagram → pakiet → ramka → bity

153

Enkapsulacja – wysyłanie danych

1. Warstwa aplikacji – tworzy komunikat (np. żądanie HTTP)
2. Warstwa transportowa – dodaje nagłówek TCP/UDP (porty, niezawodność) → powstaje segment (TCP) lub datagram (UDP)
3. Warstwa internetowa – dodaje nagłówek IP (adresy źródłowy i docelowy) → powstaje pakiet IP
4. Warstwa dostępu do sieci – dodaje nagłówek i stopkę ramki (MAC, CRC) → powstaje ramka Ethernet/Wi-Fi

Ramka zamieniana na bity i wysyłana przez medium

154

Dekapsulacja – odbieranie danych

Proces „odpakowywania” danych przy przechodzeniu w górę stosu protokołów TCP/IP

Każda warstwa usuwa swój nagłówek

Dekapsulacja:

bity → ramka → pakiet → segment/datagram → komunikat

155

Dekapsulacja – odbieranie danych

1. Warstwa dostępu do sieci – odbiera ramkę, sprawdza adres MAC i CRC, usuwa nagłówki i przekazuje dalej
2. Warstwa internetowa – analizuje nagłówki IP (adresy, TTL), usuwa go i przekazuje dane dalej
3. Warstwa transportowa – analizuje nagłówki TCP/UDP (porty, numery sekwencji, ACK), usuwa go i przekazuje dalej
4. Warstwa aplikacji – otrzymuje komunikat (np. strona WWW w przeglądarce)

156

Dziękuję za uwagę

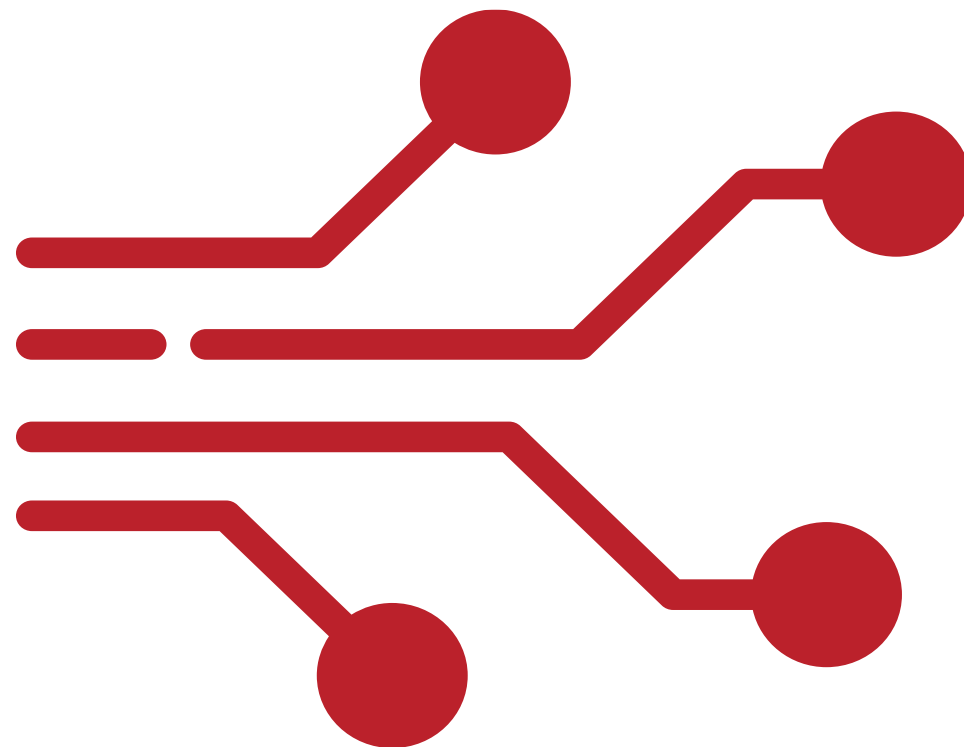
Treści programowe:

- Adresacja IP i podstawy podsieci
- Struktura adresów IPv4: klasy adresów, sieci prywatne i publiczne
- Podstawy IPv6: format, struktura i zastosowania
- Koncepcja maski podsieci i obliczanie zakresów adresów.
- Podział na podsieci (subnetting) – metody i przykłady



158

Aderesacja IP (IPv4)



Adres IP

- IP (Internet Protocol) – podstawowy protokół warstwy sieciowej w modelu TCP/IP
- Adres IP identyfikuje jednoznacznie urządzenie w sieci
- Funkcje adresu:
 - Identyfikacja hosta (komputera, routera, telefonu itp.)
 - Określenie lokalizacji w sieci (do jakiej sieci należy host)

160

Rodzaje adresów IP

IPv4

- 32 bity → zapis dziesiętny, 4 oktety: 192.168.1.10
- Zakres: ok. 4,3 mld adresów
- Problem: wyczerpywanie się puli adresów → NAT, prywatne adresy

IPv6

- 128 bitów → zapis szesnastkowy: 2001:0db8:85a3::8a2e:0370:7334
- Zakres: praktycznie niewyczerpywalny
- Rozwiązania wbudowane: autokonfiguracja, lepsze wsparcie multicast

161

Struktura adresu IP

Każdy adres IPv4 składa się z dwóch części:

1. Część sieciowa (Network ID)
 - Wskazuje, do której sieci należy host
 - Dzięki niej routery mogą podejmować decyzje, jak przesłać pakiet
 - Wszystkie hosty w tej samej sieci mają identyczny Network ID
2. Część hosta (Host ID)
 - Identyfikuje konkretne urządzenie w obrębie sieci
 - Musi być unikalny w danej sieci (nie mogą istnieć dwa takie same Host ID)

Granicę między Network ID a Host ID wyznacza maska podsieci

162

System binarny – adres IP

Komputery operują na bitach: 0 i 1

Adres IP (v4) to ciąg 32 bitów zapisanych w 4 oktetach:
każdy po 8 bitów (każdy po 1 bajcie)

Dla czytelności zapisujemy je w postaci dziesiętnej kropkowanej (np. 192.168.1.10), ale w rzeczywistości komputer widzi je jako binarne

Wszystkie hosty w tej samej sieci mają ten sam Network ID, ale różne Host ID

163

System binarny

Stosuje tylko cyfr 0 i 1

Każda pozycja ma wagę będącą kolejną potęgą liczby 2

Przykład: liczba binarna 1011:

1	0	1	$1 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 2 + 1 = 11_{10}$
2^3	2^2	2^1	2^0

164

System binarny

Stosuje tylko cyfr 0 i 1

Każda pozycja ma wagę będącą kolejną potęgą liczby 2

Przykład: liczba binarna 11111000 :

1	1	1	1	1	0	0	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

165

System binarny

Stosuje tylko cyfr 0 i 1

Każda pozycja ma wagę będącą kolejną potęgą liczby 2

Przykład: liczba binarna 11111000 :

1	1	1	1	1	0	0	0	$= 128+64+32+16+8 = 248_{10}$
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	

166

System binarny – wybrane działania

- Suma logiczna:

OR	0	1
0	0	1
1	1	1

- Iloczyn logiczny:

AND	0	1
0	0	0
1	0	1

167

System binarny

Zamiana na system dziesiętny może się odbywać na kilka sposobów:

1. Dzielenie liczby dziesiętnej przez 2 i zapisywanie reszty
2. Suma wag bitów
3. Kalkulator – np. wbudowany w Windows

168

System binarny

Dzielenie liczby dziesiętnej przez 2 i zapisywanie reszty

168 / 2	= 84	reszta 0
84 / 2	= 42	reszta 0
42 / 2	= 21	reszta 0
21 / 2	= 10	reszta 1
10 / 2	= 5	reszta 0
5 / 2	= 2	reszta 1
2 / 2	= 1	reszta 0
1 / 2	= 0	reszta 1

Zapisujemy bity od końca: $168_{10} = 10101000_2$

169

System binarny

Suma wag bitów

Każdy bit w bajcie (8 bitów) ma określoną wagę:

Bit	7	6	5	4	3	2	1	0
Waga	128	64	32	16	8	4	2	1

$168 > 128 \rightarrow$ zaznaczamy bit 7 = 1 pozostało $168 - 128 = 40$

$40 < 64 \rightarrow$ bit 6 = 0

$40 \geq 32 \rightarrow$ bit 5 = 1 pozostało $40 - 32 = 8$

$8 < 16 \rightarrow$ bit 4 = 0

$8 \geq 8 \rightarrow$ bit 3 = 1 pozostało $8 - 8 = 0$

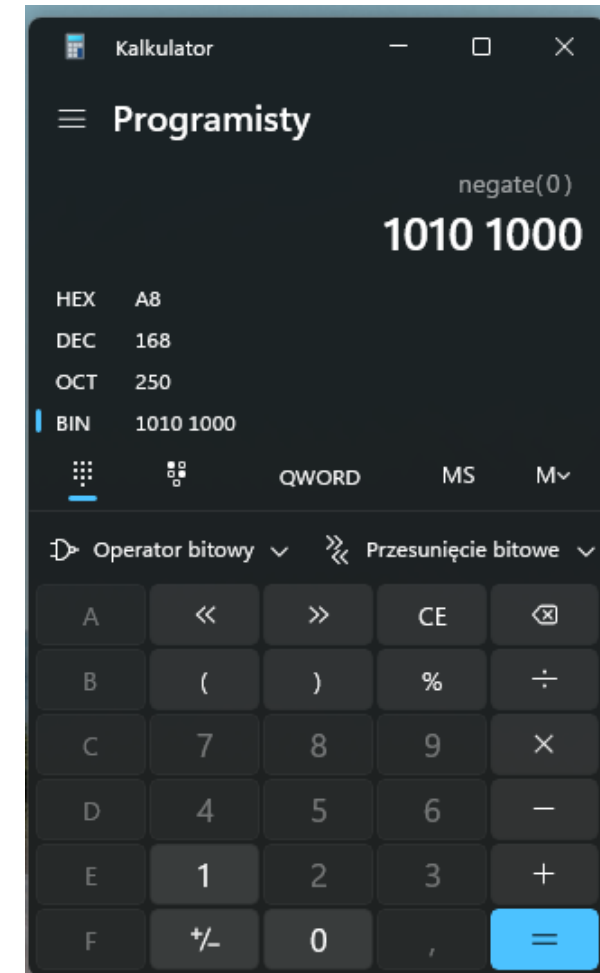
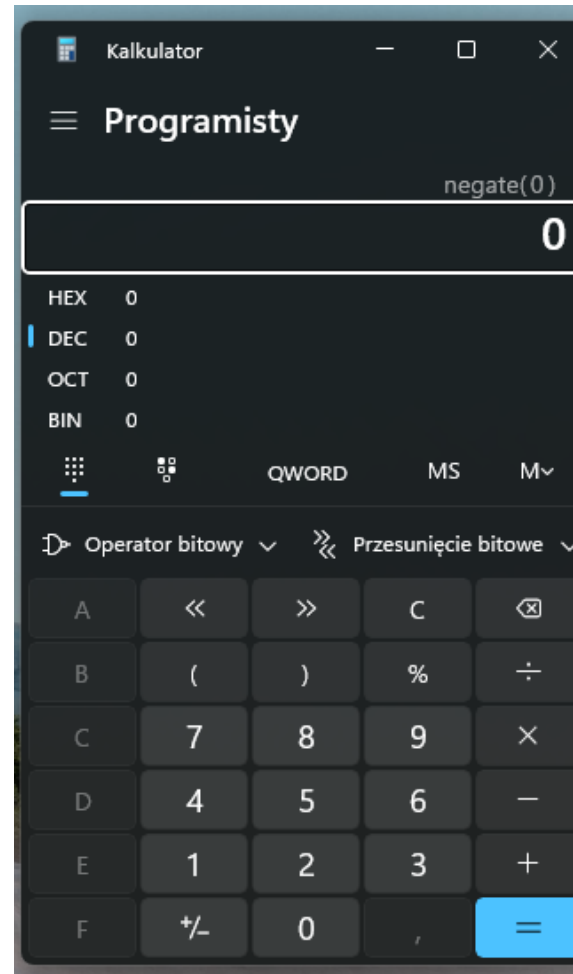
Pozostałe bity (2, 1, 0) = 0

Zapisujemy bity: $168_{10} = 10101000_2$

170

System binarny

Windows 11 – Kalkulator
w trybie Programisty



System binarny – adres IP

Przykład: adres IP 192.168.1.10:

192 = 11000000

168 = 10101000

1 = 00000001

10 = 00001010

192.168.1.10 = 11000000.10101000.00000001.00001010

172

Maska podsieci

Wszystkie hosty w tej samej sieci mają ten sam Network ID, ale różne Host ID

Maska podsieci (ang. *subnet mask*) to 32-bitowa liczba, która określa, gdzie kończy się część sieciowa adresu, a zaczyna część hosta

- Bity ustawione na 1 → należą do części sieciowej
- Bity ustawione na 0 → należą do części hosta

173

Maska podsieci

Sam adres IP nie wystarcza do określenia maski!

Maska jest ustawiana razem z adresem IP

Adres IP: 192.168.1.10 →

11000000.10101000.00000001.00001010

Maska: 255.255.255.0 →

11111111.11111111.11111111.00000000

174

Część sieciowa i część hosta

Adres IP: 192.168.1.10 → 11000000.10101000.00000001.00001010

Maska: 255.255.255.0 → 11111111.11111111.11111111.00000000

Mnożenie logiczne (bit po bicie):

11000000 AND 11111111 = 11000000 = 192

10101000 AND 11111111 = 10101000 = 168

00000001 AND 11111111 = 00000001 = 1

00001010 AND 00000000 = 00000000 = 0

Network ID = 192.168.1.0

175

Część sieciowa i część hosta

Adres IP: 192.168.1.10 →

11000000.10101000.00000001.00001010

Maska: 255.255.255.0 →

11111111.11111111.11111111|00000000

11000000.10101000.00000001|00001010



część sieciowa



część hosta

Część sieciowa (Network ID): 192.168.1.0

Część hosta (Host ID): 10

Adres sieci (Network Address)

Pierwszy adres w podsieci →

wszystkie bity hosta ustawione na 0

Identyfikuje całą sieć – nie przypisuje się go do hostów

Adres IP: 192.168.1.10

Maska: 255.255.255.0

Adres sieci: 192.168.1.0

177

Adres rozgłoszeniowy (Broadcast Address)

Ostatni adres w podsieci →
wszystkie bity hosta ustawione na 1

Służy do wysyłania pakietów do wszystkich urządzeń w tej sieci

Adres IP: 192.168.1.10

Maska: 255.255.255.0

Adres sieci: 192.168.1.0

Adres rozgłoszeniowy: 192.168.1.255

178

Zakres hostów

Hosty to wszystkie adresy pomiędzy:

192.168.1.1 → adres pierwszego hosta

192.168.1.254 → adres ostatniego hosta

Liczba hostów

Liczbę hostów wyznacza liczba bitów przeznaczonych na część hosta → bity w masce ustawione na 0

$$\text{Liczba hostów} = 2^n - 2$$

n = liczba bitów hosta

odejmujemy 1 adres sieci (bity hosta = 0) i 1 adres broadcast (bity hosta = 1)

180

Liczba i zakres hostów

Adres IP: 192.168.1.10 - 32 bity

Maska: 255.255.255.0

Adres sieci: 192.168.1.0 - 24 bity

Adres rozgłoszeniowy: 192.168.1.255

32 bity (adres IP) – 24 bity (adres sieci) = 8 bitów hosta

$2^8 - 2 = 256 - 2 = 254$ hosty – typowa sieć LAN

Liczba hostów: 254

Zakres hostów: 192.168.1.1 – 192.168.1.254

CIDR – Classless Inter-Domain Routing

Na początku Internetu (lata 80) cały zakres IPv4

0.0.0.0 – 255.255.255.255 podzielono na klasy

Każda klasa miała domyślną maskę i określoną liczbę hostów:

Klasa A:

- Zakres: **0.0.0.0 – 127.255.255.255**
- Maska: **255.0.0.0 (/8)**
- Hostów: ~16 milionów w jednej sieci

182

CIDR – Classless Inter-Domain Routing

Na początku Internetu (lata 80) cały zakres IPv4

0.0.0.0 – 255.255.255.255 podzielono na klasy

Każda klasa miała domyślną maskę i określoną liczbę hostów:

Klasa B:

- Zakres: **128.0.0.0 – 191.255.255.255**
- Maska: **255.255.0.0 (/16)**
- Hostów: ~65 tys. w jednej sieci

183

CIDR – Classless Inter-Domain Routing

Na początku Internetu (lata 80) cały zakres IPv4

0.0.0.0 – 255.255.255.255 podzielono na klasy

Każda klasa miała domyślną maskę i określoną liczbę hostów:

Klasa C:

- Zakres: **192.0.0.0 – 223.255.255.255**
- Maska: **255.255.255.0 (/24)**
- Hostów: 254 w jednej sieci

184

CIDR – Classless Inter-Domain Routing

Na początku Internetu (lata 80) cały zakres IPv4

0.0.0.0 – 255.255.255.255 podzielono na klasy

Każda klasa miała domyślną maskę i określoną liczbę hostów:

Klasa D:

- Zakres: **224.0.0.0 – 239.255.255.255** (multicast)

Klasa E:

- Zakres: **240.0.0.0 – 255.255.255.255** (eksperymentalne, zarezerwowane)

185

CIDR – Classless Inter-Domain Routing

Wystarczyło znać adres IP, żeby „zgadnąć” maskę → była sztywno powiązana z klasą

- Marnowanie adresów – ktoś potrzebował np. 1000 hostów:
 - Klasa C (254 hosty) → za mała
 - Klasa B (65 tys. hostów) → ogromna, większość się marnowała
- Zbyt duże sieci → problem z routingiem (tablice tras były ogromne)
- Bardzo szybko zaczęło brakować wolnych adresów

186

CIDR – Classless Inter-Domain Routing

W latach 90. wprowadzono CIDR (bezklasowe trasowanie międzydomenowe)

Najważniejsze cechy:

- Brak klas – sieć można podzielić dowolnie za pomocą maski
- Zapis:

adres_sieci/maska

187

CIDR – Classless Inter-Domain Routing

Adres: 192.168.1.10/24

Adresacja klasowa (klasa C):

- Domyślna maska: /24 (255.255.255.0)
- Hostów: 254

Adresacja CIDR:

- Różne maski np. /26 (62 hosty), /28 (14 hostów), /30 (2 hosty)
- Sieć staje się elastyczna, nic się nie marnuje

188

CIDR – Classless Inter-Domain Routing

Dlaczego CIDR jest ważny?

- Pozwala dzielić sieci (subnetting)
- Pozwala łączyć sieci w większe bloki (supernetting)
- Zmniejsza rozmiar tablic routingu w Internecie
- Umożliwił przedłużenie życia IPv4, mimo że pula adresów i tak zaczęła się wyczerpywać (IPv6)

189

Przykłady dla adresu 192.168.1.10

Maska /24 → 255.255.255.0

IP: 192.168.1.10

Maska: 255.255.255.0

Network ID: 192.168.1.0

Broadcast: 192.168.1.255

Hosty: 192.168.1.1 – 192.168.1.254

Liczba hostów: 254

190

Przykłady dla adresu 192.168.1.10

Maska /25 → 255.255.255.128

25 bitów – część sieciowa | 32 bitów – 25 bitów = **7 bitów** – część hosta

IP: 192.168.1.10 = 11000000.10101000.00000001.0**0001010**

Maska: 255.255.255.128 = **11111111.11111111.11111111.1**0000000

Network ID: 192.168.1.0 = 11000000.10101000.00000001.0**0000000**

Broadcast: 192.168.1.127 = 11000000.10101000.00000001.0**1111111**

Hosty: 192.168.1.1 – 192.168.1.126

Liczba hostów: 126 = $2^7 - 2$

191

Przykłady dla adresu 192.168.1.10

Maska /26 → 255.255.255.192

26 bitów – część sieciowa | 32 bitów – 26 bitów = **6 bitów** – część hosta

IP: 192.168.1.10 = 11000000.10101000.00000001.00**001010**

Maska: 255.255.255.192 = **11111111.11111111.11111111.11**000000

Network ID: 192.168.1.0 = 11000000.10101000.00000001.00**000000**

Broadcast: 192.168.1.63 = 11000000.10101000.00000001.00**111111**

Hosty: 192.168.1.1 – 192.168.1.62

Liczba hostów: 62 = $2^6 - 2$

192

Przykłady dla adresu 192.168.1.10

Maska /30 → 255.255.255.252

30 bitów – część sieciowa | 32 bitów – 30 bitów = **2 bity** – część hosta

IP: 192.168.1.10 = 11000000.10101000.00000000.000010**10**

Maska: 255.255.255.252 = **11111111.11111111.11111111.11111100**

Network ID: 192.168.1.8 = 11000000.10101000.00000000.000010**00**

Broadcast: 192.168.1.11 = 11000000.10101000.00000000.000010**11**

Hosty: 192.168.1.9 – 192.168.1.10

Liczba hostów: 2 = $2^2 - 2$

193

Przykład → 10.0.5.20/24

Maska /24 → 255.255.255.0

24 bitów – część sieciowa | 32 bitów – 24 bitów = **8 bitów** – część hosta

IP: 10.0.5.20 = 00001010.00000000.00000101.**00010100**

Maska: 255.255.255.0 = **11111111.11111111.11111111.00000000**

Network ID: 10.0.5.0 = 00001010.00000000.00000101.**00000000**

Broadcast: 10.0.5.255 = 00001010.00000000.00000101.**11111111**

Hosty: 10.0.5.1 – 10.0.5.254

Liczba hostów: 254 = $2^8 - 2$

194

Przykład → 172.16.45.200/26

Maska /26 → 255.255.255.192

26 bitów – część sieciowa | 32 bitów – 26 bitów = **6 bitów** – część hosta

IP: 172.16.45.200 = 10101100.00010000.00101101.11**001000**

Maska: 255.255.255.192 = **11111111.11111111.11111111.11**000000

Network ID: 172.16.45.192 = 10101100.00010000.00101101.11**000000**

Broadcast: 172.16.45.255 = 10101100.00010000.00101101.11**111111**

Hosty: 172.16.45.193 – 172.16.45.192.254

Liczba hostów: 62 = $2^6 - 2$

195

Przykład → 192.168.100.130/28

Maska /28 → 255.255.255.240

28 bitów – część sieciowa | 32 bitów – 28 bitów = **4 bity** – część hosta

IP: 192.168.100.130

Maska: 255.255.255.240

Kiedy maska nie kończy się równo po 8 bitach (np. /28), część bitów w **ostatnim okcie** należy do sieci, a część do hostów

To właśnie w tym ostatnim okcie tworzą się **podziały – bloki**

196

Przykład → 192.168.100.130/28

Maska /28 → 255.255.255.240

28 bitów – część sieciowa | 32 bitów – 28 bitów = **4 bity** – część hosta

IP: 192.168.100.130

Maska: 255.255.255.240

Wyznamy wielkość bloku: $256 - 240 = 16$ – każda podsieć: 16 adresów,
granice między nimi: co 16

0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240

197

Przykład → 192.168.100.130/28

Maska /28 → 255.255.255.240

28 bitów – część sieciowa | 32 bitów – 28 bitów = **4 bity** – część hosta

IP: 192.168.100.130

Maska: 255.255.255.240

Ostatni oktet = 130 → sprawdzamy do którego bloku należy:

$$128 \leq 130 < 144$$

Network ID: 192.168.100.128

198

Przykład → 192.168.100.130/28

Maska /28 → 255.255.255.240

28 bitów – część sieciowa | 32 bitów – 28 bitów = **4 bity** – część hosta

IP: 192.168.100.130

Maska: 255.255.255.240

Network ID: 192.168.100.128

Broadcast: 192.168.100.143 → ostatni adres w bloku 128+16-1=143

199

Przykład → 192.168.100.130/28

Maska /28 → 255.255.255.240

28 bitów – część sieciowa | 32 bitów – 28 bitów = **4 bity** – część hosta

IP: 192.168.100.130

Maska: 255.255.255.240

Network ID: 192.168.100.128

Broadcast: 192.168.100.143

Hosty: 192.168.100.129 – 192.168.100.142 – od pierwszego po adresie sieci do ostatniego przed adresem rozgłoszeniowym

200

Przykład → 192.168.100.130/28

Maska /28 → 255.255.255.240

28 bitów – część sieciowa | 32 bitów – 28 bitów = **4 bity** – część hosta

IP: 192.168.100.130

Maska: 255.255.255.240

Network ID: 192.168.100.128

Broadcast: 192.168.100.143

Hosty: 192.168.100.129 – 192.168.100.142

Liczba hostów: $14 = 2^4 - 2$

Przykład → 10.23.45.67/12

1. Wyznaczamy ostatni oktet maski:
2. Liczba bitów hosta: $32 - 12 = 20$
3. Ostatni oktet maski ze wzoru: $256 - 2^n$, gdzie n oznacza liczbę bitów w ostatnim oktecie maski, w naszym przypadku $n = (12 - 8) = 4$

$$256 - 2^4 = 256 - 16 = 240$$

4. Maska: 255.240.0.0 = **11111111.1111**0000.00000000.00000000

5. Wyznaczamy wielkość bloku: $256 - 240 = 16$ – sieci co 16

6. Drugi oktet IP: $16 \leq 23 < 32$

202

Przykład → 10.23.45.67/12

7. Wyznaczamy Network ID – niższe oktety na 0, a drugi na początek bloku

8. Network ID: 10.16.0.0 – początek bloku, następny blok: 10.32.0.0

9. Wyznaczamy Broadcast – drugi oktet = koniec bloku (32-1), niższe oktety = 255

10. Broadcast: 10.31.255.255

11. Zakres hostów: 10.16.0.1 – 10.31.255.254

12. Liczba hostów: $2^{20} - 2 = 1\,048\,574$

203

Przykład → 10.23.45.67/12

Maska /12 → 255.240.0.0

12 bitów – część sieciowa | 32 bitów – 12 bitów = **20 bitów** – część hosta

IP: 10.23.45.67

Maska: 255.240.0.0

Network ID: 10.16.0.0

Broadcast: 10.31.255.255

Hosty: 10.16.0.1 – 10.31.255.254

Liczba hostów: $1\ 048\ 574 = 2^{20} - 2$

Przykład → 212.10.20.130/27

205

Przykład → 212.10.20.130/27

IP: 212.10.20.130

Maska /27 → 11111111.11111111.11111111.11100000

Maska /27 → 255.255.255.224

Blok: $256 - 224 = 32$ – sieci co 32; $128 < 130 < 160$

Network ID: 212.10.20.128

Broadcast: 212.10.20.159

Hosty: 212.10.20.129 – 212.10.20.158

Liczba hostów: $2^5 - 2 = 30$

206

Klasy adresów IPv4 (adresacja klasowa – historyczna)

Klasa	Zakres pierwszego oktetu	Maska domyślna	Liczba sieci	Liczba hostów w sieci	Zastosowania
A	0 – 127	255.0.0.0 (/8)	128	ok. 16 mln	Bardzo duże sieci
B	128 – 191	255.255.0.0 (/16)	16 tys	ok. 65 tys.	Średnie sieci
C	192 – 223	255.255.255.0 (/24)	2 mln	254	Małe sieci
D	224 – 239	-	-	-	Multicast
E	240 – 255	-	-	-	Eksperymentalne

207

Sieci prywatne i publiczne

Sieci prywatne (RFC 1918) – adresy zarezerwowane do użytku wewnętrznego: LAN, firmy, domy, itp.

Nie są routowane w Internecie

- 10.0.0.0 – 10.255.255.255 (/8)
- 172.16.0.0 – 172.31.255.255 (/12)
- 192.168.0.0 – 192.168.255.255 (/16)

Typowy domowy router dostaje adres z zakresu **192.168.x.x**

208

Sieci prywatne i publiczne

Sieci publiczne – pozostałe adresy (unikalne) – mogą być używane w Internecie – routowane

Przydzielane przez organizacje zarządzające adresacją (np. IANA, RIPE, ARIN)

Przykład publicznego IP

8.8.8.8

Klasa

A

Opis

Serwer DNS Google

212.182.16.104

C

Publiczny adres PL

209

Adresy specjalne

- Adres sieci, np. 192.168.1.0 – wszystkie bity hosta = 0, oznacza samą sieć – nie można przypisać do host
- Adres rozgłoszeniowy, np. 192.168.1.255/24 – wszystkie bity hosta = 1, stosowany do wysyłania pakietów do wszystkich urządzeń w danej sieci, w IPv6 nie istnieje – zastąpiony multicastem
- Adres 0.0.0.0 – ma różne znaczenia:
 - 1.w routingu – default route (trasa domyślna)
 - 2.przy uruchamianiu hosta – brak jeszcze własnego adresu IP

Nie można go przypisać do urządzenia sieciowego

210

Adresy specjalne

- Adres loopback – 127.0.0.0/8 – najczęściej używany, służy do testowania stosu TCP/IP na własnym komputerze, każdy adres z zakresu: 127.0.0.1 do 127.255.255.254
- Adresy prywatne:
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- Adresy automatyczne APIPA (169.254.0.0/16) - w przypadku braku adresu z DHCP - automatyczna konfiguracja 169.254.x.x - umożliwia to komunikację tylko w lokalnym segmencie sieci

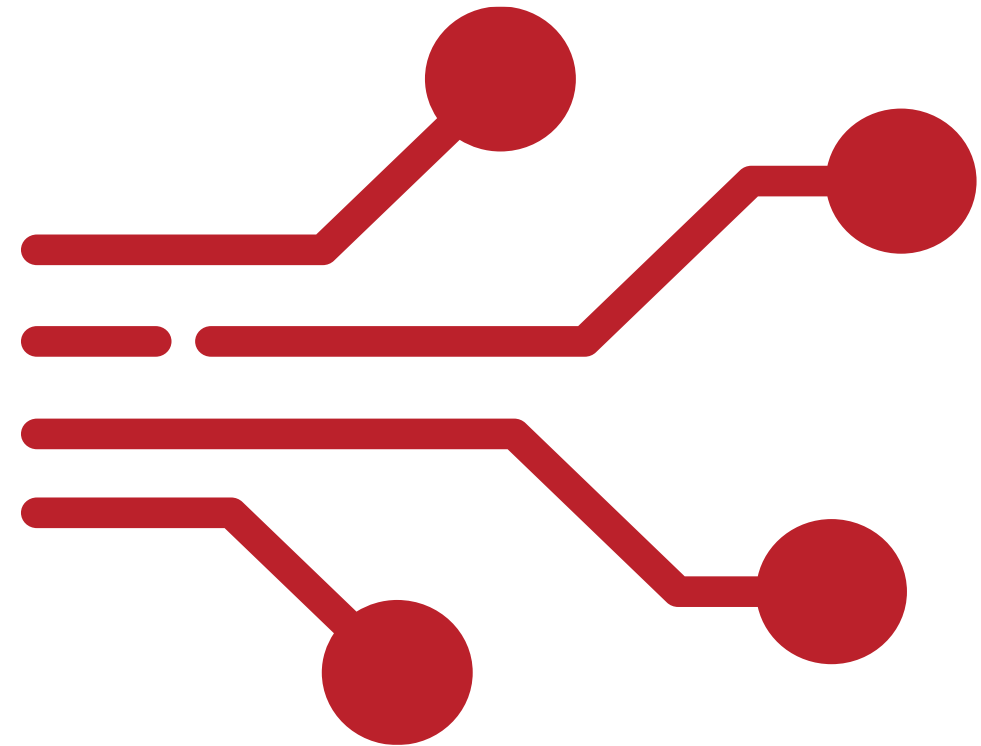
211

Adresy specjalne

- Adresy multicastowe (224.0.0.0 – 239.255.255.255) - używane do wysyłania pakietów do grupy hostów (np. transmisja wideo, routing protokołów jak OSPF)
- Adresy zarezerwowane i eksperymentalne:
 - 240.0.0.0 – 255.255.255.254 – zarezerwowane do badań i testów, nie używane w Internecie
 - 255.255.255.255 → broadcast ogólny (wysłanie do wszystkich w lokalnym segmencie sieci)

212

Subnetting



213

Subnetting

Subnetting = dzielenie większej sieci IP na mniejsze, logiczne podsieci

Każda podsieć ma:

- własny adres sieci
- własny adres rozgłoszeniowy
- własny zakres hostów

Dzięki temu sieć jest bardziej uporządkowana i łatwiejsza w zarządzaniu

214

Subnetting przykład

Firma dostaje pulę: 192.168.1.0/24 (256 adresów)

Bez podziału: wszystkie hosty w jednej sieci

Z podziałem: można stworzyć np. 4 podsieci po 62 hosty

Każdy dział firmy ma osobny segment sieci

215

Dlaczego subnetting jest ważny?

Oszczędność adresów – nie marnujemy dużej przestrzeni na małe grupy hostów

Bezpieczeństwo – podsieci izolują ruch (np. księgowość od gości Wi-Fi)

Wydajność – mniej broadcastów w jednej podsieci = szybsza sieć

Zarządzanie – łatwiej lokalizować problemy

216

Subnetting – główne podejścia

FLSM (Fixed Length Subnet Mask) – stałe rozmiary podsieci

- Wszystkie podsieci są tej samej wielkości
- Łatwość planowania i prosty routing
- Mniej elastyczne – marnowanie adresów

VLSM (Variable Length Subnet Mask) – różne rozmiary podsieci

- Podział sieci na podsieci o różnych wielkościach
- Elastyczność dopasowana do potrzeb działów/oddziałów
- Wymaga dokładnego planowania

217

Subnetting – procedura podziału

Podział na podsieci wykonuje się w kilku krokach:

- Określenie potrzeb (ile podsieci, ile hostów)
- Dobranie liczby bitów do „pożyczenia” z części hosta
- Obliczenie nowej maski podsieci
- Wyznaczenie adresów sieci, hostów i rozgłoszeniowych

218

Subnetting – przykład

Analiza wymagań

Ile podsieci jest potrzebnych?

Ile urządzeń (hostów) musi działać w każdej podsieci?

Przykład:

firma ma 3 działy:

- A – 100 komputerów
- B – 50 komputerów
- C – 10 komputerów

Subnetting – przykład

Sieć początkowa: 192.168.1.0/24 → 256 adresów ($2^8 = 256$)

Do dyspozycji: 254 hosty (dwa adresy odpadają: sieci i broadcast)

Z sieci /24 mamy 8 bitów na część hosta

Musimy policzyć:

$2^m - 2 \geq \text{liczba hostów}$

gdzie m – liczba pozostałych bitów na część hosta

220

Subnetting – przykład

- Dział A: 100 hostów $\rightarrow 2^7 - 2 = 126 \geq 100 \rightarrow 7$ bitów na hosta
Maska: /25 (bo $32 - 7 = 25$)
- Dział B: 50 hostów $\rightarrow 2^6 - 2 = 62 \geq 50 \rightarrow 6$ bitów na hosta
Maska: /26 (bo $32 - 6 = 26$)
- Dział C: 10 hostów $\rightarrow 2^4 - 2 = 14 \geq 10 \rightarrow 4$ bity na hosta
Maska: /28 (bo $32 - 4 = 28$)

221

Subnetting – przykład

Metoda bloku (skoku):

Wybieramy oktet, w którym maska nie jest pełna (255)

Obliczamy skok: $256 - \text{wartość maski w tym oktecie}$

Network ID to kolejne bloki zaczynając od 0 (0, skok, $2 \times \text{skok}$,...)

Broadcast = „następny network ID” – 1

Zakres hostów = od (network + 1) do (broadcast – 1)

222

Subnetting – przykład

- Dział A: Maska: /25 ($32 - 7 = 25$)

255.255.255.128

- Dział B: Maska: /26 ($32 - 6 = 26$)

255.255.255.192

- Dział C: Maska: /28 ($32 - 4 = 28$)

255.255.255.240

223

Subnetting – przykład

- Dział A: Maska: /25 → 255.255.255.128 – blok co 256 - 128 = 128

Network ID: 192.168.1.0

Broadcast ID: 192.168.1.127 (128-1)

Zakres hostów: 192.168.1.1 - 192.168.1.126

Liczba hostów: $2^7 - 2 = 126$

224

Subnetting – przykład

- Dział B: Maska: /26 → 255.255.255.192 – blok co 256 – 192 = 64

Network ID: 192.168.1.128

Broadcast ID: 192.168.1.191 (192-1)

Zakres hostów: 192.168.1.129 - 192.168.1.190

Liczba hostów: $2^6 - 2 = 62$

225

Subnetting – przykład

- Dział C: Maska: /28 → 255.255.255.240 – blok co 256 – 240 = 16

Network ID: 192.168.1.192

Broadcast ID: 192.168.1.207 (208-1)

Zakres hostów: 192.168.1.193 - 192.168.1.206

Liczba hostów: $2^4 - 2 = 14$

226

Subnetting – liczba podsieci i hostów

1. Sprawdzamy maskę początkową (np. /24)
2. Określamy, ile bitów będzie przeznaczonych na podsieci (pożyczonych z bitów hostów)
3. Stosujemy wzór:
 - **Liczba podsieci:** 2^n , n – liczba pożyczonych bitów
 - **Liczba hostów:** $2^m - 2$, m – bity hostów

227

Subnetting – przykład

Mając dany adres Network IP: 172.16.0.0/16 podziel na 64 podsieci i
wyznacz liczbę hostów w sieci

Maska: /16 $\rightarrow 2^{16} - 2 = 65536 - 2 = 65534$ hostów

Potrzebujemy 64 podsieci: $2^n \geq 64 \rightarrow n = 6$, bo $2^6 = 64$

Należy pożyczyć **6 bitów z części hostów**

Nowa maska /22 (16 + 6)

Liczba podsieci: 64

Liczba hostów: $2^{(32-22)} - 2 = 2^{10} - 2 = 1022$

228

Subnetting – przykład

Mając dany adres Network IP: 192.168.10.0/24 podziel na 6 podsieci i
wyznacz liczbę hostów w sieci

229

Subnetting – przykład

Mając dany adres Network IP: 192.168.10.0/24 podziel na 6 podsieci i
wyznacz liczbę hostów w sieci

Maska: /24 $\rightarrow 2^8 - 2 = 256 - 2 = 254$ hostów

Potrzebujemy 8 podsieci: $2^n \geq 8 \rightarrow n = 3$, bo $2^3 = 8$

Należy pożyczyć **3 bity z części hostów**

Nowa maska /27 (24 + 3)

Liczba podsieci: 8

Liczba hostów: $2^{(32-27)} - 2 = 2^5 - 2 = 30$

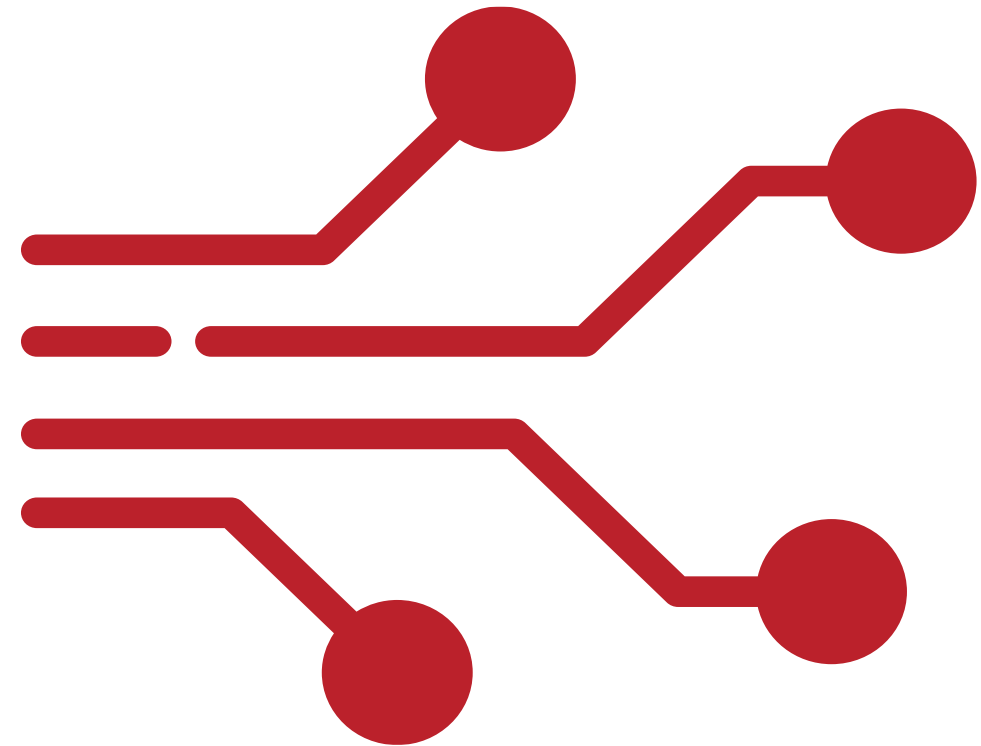
230

Subnetting – tabela podsieci klasy C

Maska (CIDR)	Maska dziesiętna	Liczba podsieci	Liczba hostów w podsieci
/24	255.255.255.0	1	254
/25	255.255.255.128	2	126
/26	255.255.255.192	4	62
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14
/29	255.255.255.248	32	6
/30	255.255.255.252	64	2

231

Aderesacja IP (IPv6)



232

IPv6 struktura

Długość adresu: 128 bitów (16 bajtów)

Zapis: osiem grup czterech cyfr szesnastkowych (0-F)

np. 2001:0db8:0000:0000:0000:ff00:0042:8329

Usuwanie zer na początku grupy: 2001:db8:0:0:0:ff00:42:8329

Skracanie – zastąpienie ciągu zer podwójnym dwukropkiem:

2001:db8::ff00:42:8329

Łączna liczba adresów: $2^{128} \approx 3,4 \times 10^{38}$ (praktycznie „nieskończoność”)

233

IPv6 rodzaje adresów

Typ	Zakres / Prefiks	Opis
Global Unicast	2000::/3	publiczne adresy routowalne w Internecie
Link-Local	fe80::/10	działają tylko w lokalnej sieci (np. do komunikacji routerów)
Unique Local (ULA)	fc00::/7	odpowiednik prywatnych IPv4 (10.0.0.0/8, 192.168.x.x)
Multicast	ff00::/8	wysyłanie do grup hostów
Loopback	::1	odpowiednik 127.0.0.1 w IPv4
Unspecified	::	brak adresu (np. w konfiguracji początkowej)

234

IPv6 prefix sieci i hosta

IPv6 także używa maski - notacja z ukośnikiem /:

Przykład: 2001:db8:abcd:1234::1/64

- /64 oznacza, że pierwsze 64 bity to część sieciowa, pozostałe 64 bity — identyfikator hosta
- standardowa długość w IPv6 dla większości sieci LAN

Network ID 2001:db8:abcd:1234::/64

Host 1 2001:db8:abcd:1234::1

Host 2 2001:db8:abcd:1234::2

Router 2001:db8:abcd:1234::fe

Broadcast brak (IPv6 nie ma broadcastu – używa multicastu)

235

IPv6 automatyczne adresowanie

IPv6 został zaprojektowany tak, by urządzenia mogły same się konfigurować, bez potrzeby ręcznego przypisywania adresów czy serwera DHCP (tak jak w IPv4)

Urządzenie, gdy „zobaczy” sieć IPv6 — potrafi samo wygenerować swój adres IPv6

Główne sposoby konfiguracji IPv6:

- SLAAC (Stateless Address Autoconfiguration)
- DHCPv6 (Stateful lub Stateless)
- Ręczne (manualne) przypisanie

236

IPv6 automatyczne adresowanie

SLAAC (Stateless Address Autoconfiguration) — najczęstszy, „automatyczny” sposób

Działanie:

1. Urządzenie nasłuchuje komunikatu Router Advertisement (RA), który wysła router
2. Z komunikatu pobiera prefiks sieci (np. 2001:db8:abcd:1234::/64)
3. Samo dodaje do tego swój unikalny identyfikator interfejsu (64 bity)
 - może go stworzyć na podstawie adresu MAC
 - albo losowo (tzw. privacy extension)
4. Pełny adres IPv6

237

IPv6 automatyczne adresowanie

SLAAC (Stateless Address Autoconfiguration) — najczęstszy, „automatyczny” sposób

Działanie:

1. Urządzenie nasłuchuje komunikatu Router Advertisement (RA), który wysyła router
2. Z komunikatu pobiera prefiks sieci (np. 2001:db8:abcd:1234::/64)
3. Samo dodaje do tego swój unikalny identyfikator interfejsu (64 bity)
 - może go stworzyć na podstawie adresu MAC
 - albo losowo (tzw. privacy extension)
4. Pełny adres IPv6

Prefiks z routera: 2001:db8:abcd:1234::/64

Adres hosta: 2001:db8:abcd:1234:1a2b:3c4d:5e6f:7890

238

IPv6 automatyczne adresowanie

DHCPv6 (Stateful lub Stateless)

Podobnie jak klasyczny DHCP w IPv4, ale w wersji IPv6

- Stateful DHCPv6 – serwer przydziela adres i pamięta, komu go dał
- Stateless DHCPv6 – host sam ustawia adres (SLAAC), a DHCPv6 podaje tylko dodatkowe dane (DNS, domena itd.)

Stosowany tam, gdzie administrator chce mieć pełną kontrolę nad adresacją (np. sieci korporacyjne)

Ręczne (manualne) przypisanie

Można oczywiście wpisać adres IPv6 ręcznie – np. dla routerów, serwerów czy testów labowych:

```
ip -6 addr add 2001:db8:abcd:1234::1/64 dev eth0
```

239

IPv6 adresy lokalne (Link-local)

Każde urządzenie w IPv6 zawsze automatycznie tworzy adres link-local, nawet bez routera

Ten adres działa tylko w obrębie lokalnego segmentu sieci (LAN) – służy np. do komunikacji routerów (protokół NDP) – nie jest routowalny w Internecie

Ten adres zawsze zaczyna się od fe80::

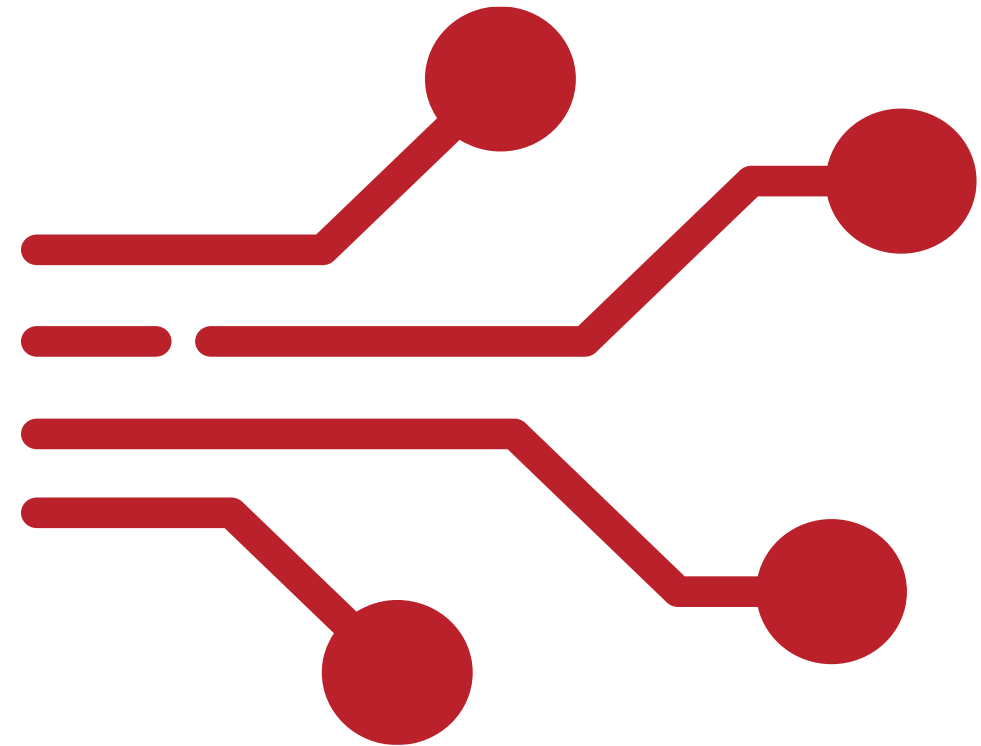
IPv4	IPv6	
192.168.1.144	fe80::1979:7a93:e8d:4e58%8	– Windows
192.168.1.144	fe80::1979:7a93:e8d:4e58%eth0	– Linux

IPv6 może mieć ten sam adres fe80:: na różnych interfejsach

Wi-Fi (wlan0)	fe80::1979:7a93:e8d:4e58%3
Ethernet (eth0)	fe80::1979:7a93:e8d:4e58%8
VirtualBox (vboxnet0)	fe80::1979:7a93:e8d:4e58%12

240

IPv4 vs IPv6



241

IPv4 struktura

Długość adresu: 32 bity (4 bajty)

Zapis: dziesiętny - cztery liczby dziesiętne oddzielone kropkami

Podział: każda liczba 0–255 to 8 bitów

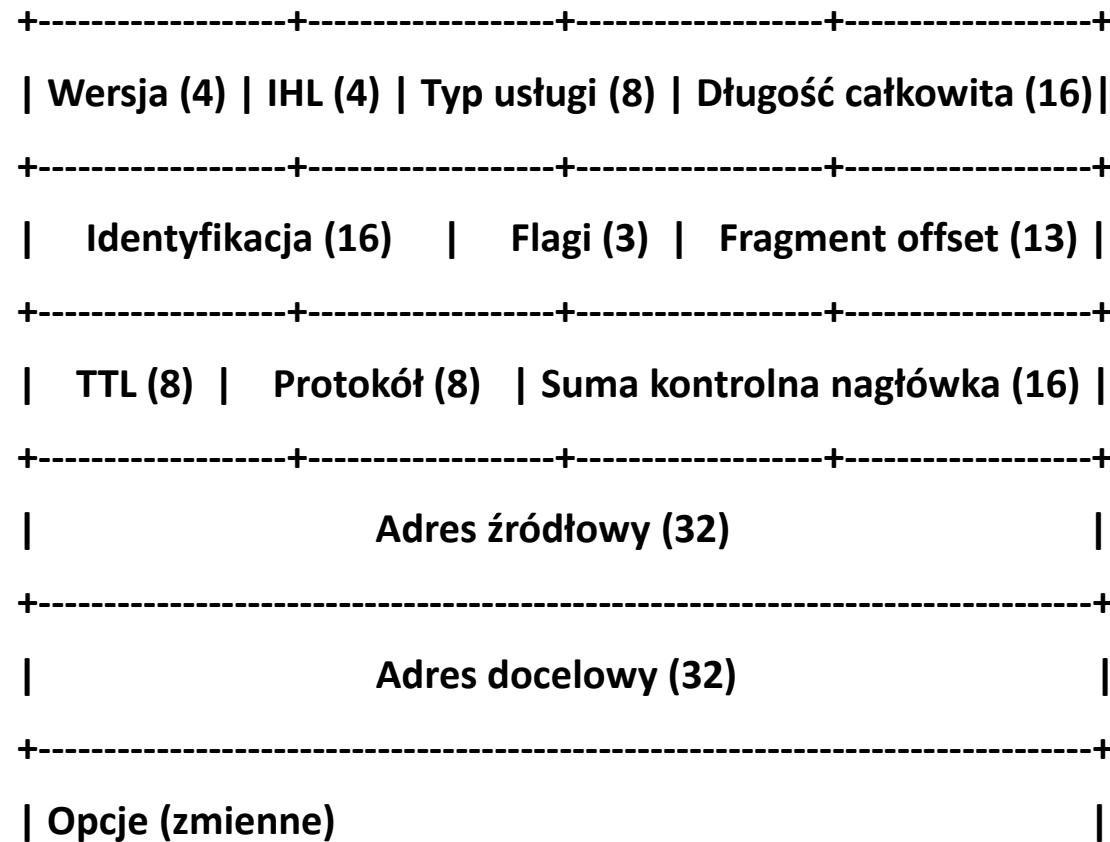
Łączna liczba adresów: ok. 4,3 miliarda (2^{32})

Nagłówek pakietu (header):

wersja (4 bity), długość nagłówka, typ usługi (ToS/DSCP), długość całkowita, identyfikacja, flagi, fragmentacja, czas życia (TTL), protokół (TCP, UDP, ICMP...), suma kontrolna nagłówka, adres źródłowy, adres docelowy, opcje (opcjonalnie)

242

IPv4 struktura nagłówka



243

IPv6 struktura

Długość adresu: 128 bitów (16 bajtów)

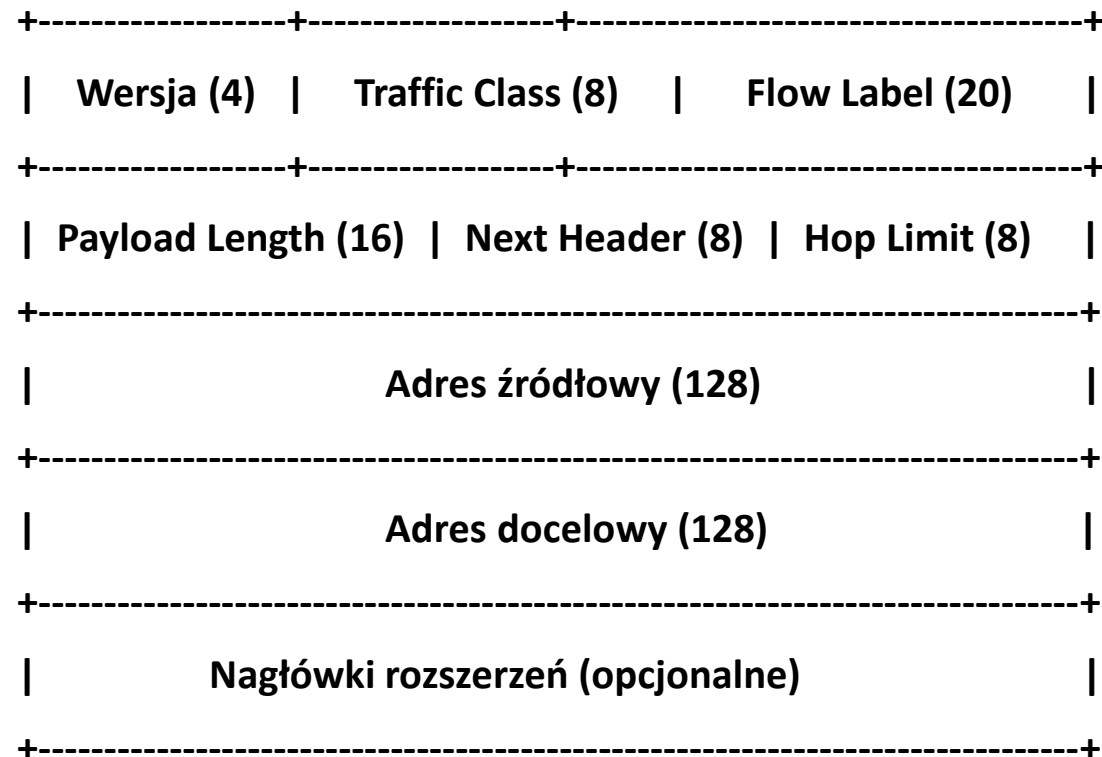
Zapis: osiem grup czterech cyfr szesnastkowych,
np. 2001:0db8:85a3:0000:0000:8a2e:0370:7334 – skracanie – zera można pominąć
łączna liczba adresów: $2^{128} \approx 3,4 \times 10^{38}$ (praktycznie „nieskończoność”)

Nagłówek pakietu:

wersja (6), priorytet (Traffic Class), etykieta przepływu (Flow Label), długość ładunku, następny nagłówek (Next Header), limit skoków (Hop Limit), adres źródłowy (128 bitów), adres docelowy (128 bitów)

244

IPv6 struktura nagłówka



245

IPv4 – IPv6

Obecnie oba protokoły są w użyciu jednocześnie – trwa tzw. okres współistnienia IPv4 i IPv6

IPv4:

- Wciąż dominuje w Internecie, bo większość starszej infrastruktury i urządzeń działa na IPv4
- Problemem jest brak wolnych adresów – oficjalnie pula IPv4 wyczerpała się:
 - w regionie APNIC (Azja-Pacyfik) już w 2011
 - RIPE NCC (Europa) – w 2019
 - ARIN (Ameryka Północna) – w 2015

246

IPv4 – IPv6

IPv6:

- Stopniowo wdrażany od ok. 2012 roku
- Wprowadza ogromną przestrzeń adresową i prostsze mechanizmy routingu
- Według danych Google (wrzesień 2025), około 45–50% użytkowników na świecie korzysta z IPv6 – ale różni się to w zależności od kraju i operatora (np. w Indiach, Belgii czy USA adopcja przekracza 60–70%, w Polsce ok. 15–25%)

Nie da się przełączyć całego Internetu - dual stack (urządzenia działają jednocześnie na IPv4 i IPv6)

Istnieją też translacje, np. NAT64/DNS64, aby umożliwić komunikację między IPv4 i IPv6

247

Dziękuję za uwagę

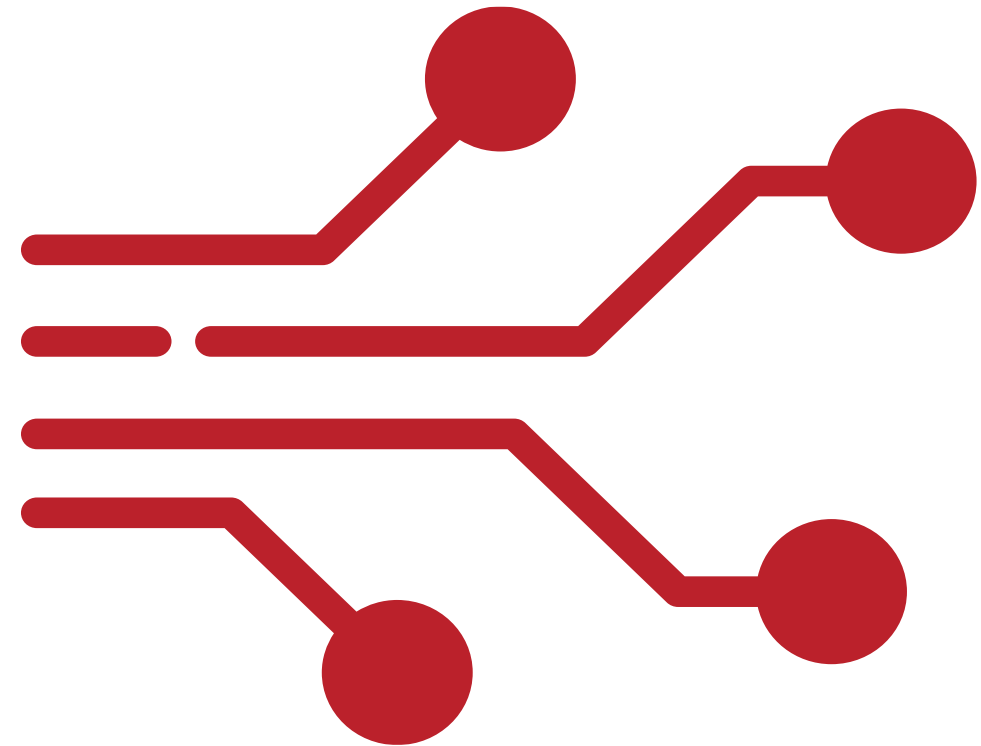
Treści programowe:

- Urządzenia sieciowe
- Routery: funkcje i zastosowanie w przesyłaniu danych między sieciami
- Przełączniki: działanie, różnice między hubem a przełącznikiem
- Punkty dostępu bezprzewodowego (AP): zastosowanie i konfiguracja
- Inne urządzenia sieciowe



249

Urządzenia sieciowe



250

Urządzenia sieciowe

Sprzęt wykorzystywany do budowy, łączenia i zarządzania sieciami komputerowymi

Mogą pełnić różne funkcje:

- kierowanie ruchem (routing)
- łączenie wielu urządzeń w jednej sieci (switch, hub)
- zapewnianie dostępu do Internetu
- umożliwianie komunikacji przewodowej i bezprzewodowej
- zabezpieczanie i monitorowanie ruchu

251

Routery

Urządzenia pracujące głównie w warstwie sieciowej (3) modelu ISO/OSI

Odpowiadają za kierowanie pakietów danych między różnymi sieciami (przekazywanie/routing)

Przekazywanie – lokalna operacja routera polegająca na przesłaniu pakietu z interfejsu łącza wejściowego do interfejsu odpowiedniego łącza wyjściowego – realizowane sprzętowo, odbywa się błyskawicznie (nanosekundy)

Routing – proces sieciowy określający ścieżki między węzłami, którymi pakiet podąża od miejsca źródłowego do docelowego – implementowany programowo, trwa znacznie dłużej (sekundy)

252

Routery

Każdy router posiada **tablicę przekazywania** – wewnętrzną bazę danych na podstawie której router podejmuje decyzje, do którego interfejsu przekazać pakiet, zawiera: sieć docelową, maskę podsieci, next hop (kolejny router), interfejs wyjściowy

Algorytm routingu - sposób, w jaki router wybiera najlepszą trasę do przesyłania pakietów między sieciami

- Statyczny routing:
Trasy są wprowadzane ręcznie przez administratora - brak automatycznego dostosowania w razie awarii, stosowany w małych sieciach lub do specjalnych zastosowań
- Dynamiczny routing:
Routery automatycznie wymieniają się informacjami o trasach i wybierają najlepszą, dostosowują się do zmian w sieci (awarie, nowe połączenia), wykorzystują protokoły routingu (np. RIP, OSPF, EIGRP, BGP)

253

Routery

Uogólniony schemat działania:

1. Router odbiera informacje o sieci od sąsiadów (lub administratora w przypadku tras statycznych)
2. Tworzy/aktualizuje tablicę routingu
3. Dla każdego pakietu sprawdza adres docelowy IP
4. Szuka najlepszego dopasowania w tablicy routingu
5. Wysyła pakiet przez odpowiedni interfejs do następnego routera (next hop)

254

Routery

Metryki w algorytmach routingu:

Routery wybierają trasę na podstawie tzw. metryki – kosztu danej ścieżki

Metryka może oznaczać:

- liczbę przeskoków (hop count) – ile routerów trzeba przejść (RIP)
- przepustowość łącza
- opóźnienie (delay)
- obciążenie (load)
- koszt administracyjny (np. ustalony ręcznie)

255

Routery

Model usług sieciowych:

Gwarancja dostarczenia – pakiety dotrą do miejsca docelowego (kolejkowanie, buforowanie)

Gwarancja dostarczenia z ograniczonym opóźnieniem – pakiety dotrą i nie zajmie to więcej czasu niż określone opóźnienie międzywęzłowe (prioryteryzacja ruchu – QoS)

Dostarczenie pakietu zgodnie z kolejnością wysyłania – pakiety dotrą do miejsca przeznaczenia w kolejności wysyłania (kolejki FIFO, buforowanie)

Gwarantowana minimalna przepustowość – dopóki host nadawczy transmituje bity z szybkością mniejszą od określonej – wszystkie pakiety dotrą na miejsce (rezerwacja pasma)

Bezpieczeństwo – warstwa sieciowa może zaszyfrować treści datagramów po stronie nadawcy i odszyfrować po stronie odbiorcy (tunelowanie VPN)

256

Routery - architektura

Porty wejściowe (Input Ports) – odbierają pakiety z sieci, wstępnie je analizują i kierują do przełącznicy

Struktura przełączająca (Switching Fabric) – serce routera, przenosi pakiety z portów wejściowych do odpowiednich portów wyjściowych

Porty wyjściowe (Output Ports) – kolejkują pakiety i wysyłają je dalej do sieci docelowej

Procesor obsługujący routing (Control Plane CPU)– „mózg” routera: utrzymuje tablice routingu, uruchamia protokoły routingu, decyduje o trasach

257

Routery - architektura

Porty wejściowe (input ports) - interfejsy, przez które router odbiera pakiety

Składają się z:

- fizycznej warstwy – np. Ethernet, światłowód, DSL
- bufora wejściowego – przechowuje pakiety, gdy ruch jest większy niż przepustowość dalszej części routera
- funkcji wstępnej analizy nagłówka – sprawdzają adres docelowy (IP), TTL, błędy

Często już tutaj wykonywane jest dopasowanie do tablicy routingu (fast path)

Jeśli bufor wejściowy jest pełny → pakiety są odrzucane (drop) → zjawisko input queuing

258

Routery - architektura

Struktura przełączająca (switching fabric) – odpowiada za przeniesienie pakietu z portu wejściowego do odpowiedniego portu wyjściowego, musi być bardzo szybka, żeby nie tworzyć wąskiego gardła

Metody przełączania:

- Memory-based (przez pamięć) - port wejściowy zapisuje pakiet w pamięci, a port wyjściowy odczytuje, działa jak klasyczny komputer (CPU obsługuje przełączanie) – proste rozwiązanie, ale wolne przy dużym ruchu
- Bus-based (przez magistralę) - pakiety przesyłane przez wspólną magistralę systemową, tylko jeden transfer na raz → możliwe wąskie gardło
- Crossbar / Fabric (przełącznica krzyżowa) - bardzo szybkie połączenia równoległe między portami, używane w nowoczesnych routerach szkieletowych i switchach

259

Routery - architektura

Porty wyjściowe (output ports) - interfejsy, przez które pakiety wychodzą z routera do kolejnej sieci

Składają się z:

- bufora wyjściowego – przechowuje pakiety, gdy link wyjściowy jest zajęty
- scheduler (planista) – decyduje, które pakiety wyjść jako pierwsze (np. priorytety QoS)
- modułu transmisyjnego – wysyła pakiety w odpowiednim formacie (Ethernet, MPLS, ATM...)

Jeśli bufor wyjściowy się przepełni → pakiety tracone (output queuing)

260

Routery - architektura

Procesor obsługujący routing (route processor / control plane CPU) - „mózg” routera

Odpowiedzialny za:

- utrzymywanie tablicy routingu
- uruchamianie protokołów routingu (RIP, OSPF, BGP)
- aktualizację tablicy FIB (Forwarding Information Base) używanej do szybkiego przekazywania pakietów
- zarządzanie systemem operacyjnym routera

Control plane (procesor) – decyduje o trasach, uczy się od innych routerów

Data plane (fast path) – przekazuje pakiety na podstawie tablic FIB → odbywa się bez udziału CPU, na poziomie sprzętowym (ASIC) 261

Przełączniki (switch)

Urządzenia pracujące głównie w warstwie łącza danych (2) modelu ISO/OSI
łączą urządzenia w jednej sieci lokalnej (LAN), przesyłają ramki do hostów

Przekazywanie – lokalna operacja przełącznika polegająca na przesłaniu ramki z portu wejściowego do odpowiedniego portu wyjściowego na podstawie adresu MAC odbiorcy, proces realizowany sprzętowo (ASIC), co zapewnia jego błyskawiczne działanie (w skali nanosekund)

Przełączanie – proces sieciowy warstwy łącza danych, polegający na podejmowaniu decyzji, do którego portu wyjściowego należy przesłać ramkę na podstawie adresu MAC odbiorcy, obejmuje: uczenie się adresów MAC urządzeń podłączonych do portów, tworzenie i utrzymywanie tablicy MAC (CAM table), kierowanie ramek tylko do właściwego odbiorcy, w razie braku wpisu – rozgłaszanie (broadcast)

262

Przełączniki – tablica MAC

1. Początek – pusta tablica

- Po włączeniu switch nie zna żadnych adresów MAC
- Wszystkie ramki, których odbiorcy nie zna, rozsyła w trybie broadcast (do wszystkich portów)

2. Uczenie się adresów (MAC learning)

- Gdy ramka trafia na port wejściowy, switch odczytuje adres MAC źródłowy z nagłówka
- Dzięki temu „wie”, że urządzenie o danym MAC jest podłączone do konkretnego portu

3. Budowanie tablicy

- Switch wykonuje ten proces dla wszystkich ramek, które odbiera

263

Przełączniki – tablica MAC

4. Przekazywanie ramek (Forwarding)

- Gdy przychodzi ramka z adresem docelowym:
 - Jeśli adres MAC docelowy jest w tablicy → ramka trafia tylko na ten port
 - Jeśli adresu brak → ramka jest rozgłaszana (broadcast)

5. Starzenie się wpisów (Aging)

- Jeśli przez pewien czas (np. 300 sekund) switch nie widzi ruchu z danego adresu MAC, usuwa wpis
- Dzięki temu tablica nie jest przepełniona i odzwierciedla aktualny stan sieci

6. Przepełnienie tablicy MAC

- Jeśli w sieci działa bardzo dużo urządzeń, tablica może się zapełnić
- Wtedy switch działa jak hub → rozsyła ruch do wszystkich portów
- To może być wykorzystane w atakach typu MAC flooding

Przełączniki – zasada działania

1. Urządzenie (np. komputer A) wysyła ramkę
2. Switch odbiera ramkę na porcie wejściowym
3. Switch sprawdza adres MAC źródła i zapisuje go w swojej tablicy MAC (adres → port)
4. Switch sprawdza adres MAC docelowy:
 - jeśli adres jest w tabeli → ramka idzie tylko na właściwy port
 - jeśli adresu brak → ramka jest rozgłaszana (broadcast)
5. Odbiorca (np. komputer B) odpowiada, a switch zapamiętuje jego adres MAC i port
6. W kolejnych transmisjach ruch trafia już bezpośrednio, bez rozgłaszania

265

Przełączniki – tryby przełączania ramek

- Store-and-Forward – switch buforuje całą ramkę, sprawdza sumę kontrolną CRC i dopiero wysyła dalej (bezpieczne, ale wolniejsze)
- Cut-Through – przełącza ramkę natychmiast po odczytaniu adresu MAC docelowego (szybkie, ale mniej bezpieczne)
- Fragment-Free – kompromis – przechowuje pierwsze 64 bajty (eliminuje kolizje), potem przekazuje dalej

266

Przełączniki – główne funkcje

Łączenie urządzeń w sieci LAN– komputery, drukarki, serwery, punkty dostępowe

Przekazywanie ramek na podstawie adresów MAC– wysyła dane tylko do właściwego portu, a nie do wszystkich (jak hub)

Tworzenie tabeli MAC (CAM table)– zapamiętuje, które urządzenie jest podłączone do którego portu

Redukcja kolizji – każdy port = osobna domena kolizji → lepsza wydajność

Obsługa VLAN (w switchach zarządzalnych) – logiczne podziały sieci dla bezpieczeństwa i organizacji

QoS (Quality of Service) – priorytetyzacja ruchu (np. VoIP, wideokonferencje)

Port Security– możliwość blokady nieznanych urządzeń na danym porcie

PoE (Power over Ethernet)– przesyłanie danych i zasilania jednym kablem (dla kamer IP, AP)

267

Koncentratory (hub)

Urządzenia sieciowe działające w warstwie fizycznej (1) modelu OSI

Łączą wiele urządzeń w sieci lokalnej, ale nie rozpoznają odbiorców ramek

Jego zadaniem jest powielanie sygnału odebranego na jednym porcie i przesyłanie go do wszystkich pozostałych portów

Nie ma tablicy MAC

Tworzy jedną domenę kolizji

Właściwie nie stosowany obecnie

268

Koncentratory – zasada działania

1. Komputer A wysyła ramkę Ethernet
2. Hub odbiera sygnał na jednym porcie
3. Hub powiela sygnał i wysyła go na wszystkie inne porty
4. Wszystkie komputery odbierają ramkę, ale tylko komputer docelowy reaguje (na podstawie adresu MAC)

Hub nie analizuje ani adresów MAC, ani IP – „rozgłasza” ruch do wszystkich

269

Domena kolizji

Domena kolizji to fragment sieci komputerowej, w którym może dojść do kolizji pakietów (ramek Ethernet), jeśli dwa lub więcej urządzeń spróbują wysyłać dane w tym samym czasie

Kolizja = dwa sygnały nakładają się na siebie → dane zostają uszkodzone i muszą być ponownie wysłane

W starszych sieciach Ethernet (CSMA/CD, half-duplex):

- wszystkie urządzenia w danym segmencie „słyszają się nawzajem”, jeśli dwa hosty wyślą ramki jednocześnie → kolizja

Rozwiązanie: wykrywanie kolizji (Collision Detection) i ponowna transmisja po losowym czasie

270

Domena kolizji a urządzenia sieciowe

Hub (koncentrator):

- wszystkie porty należą do jednej domeny kolizji
- więcej urządzeń = więcej kolizji = spadek wydajności

Switch (przełącznik):

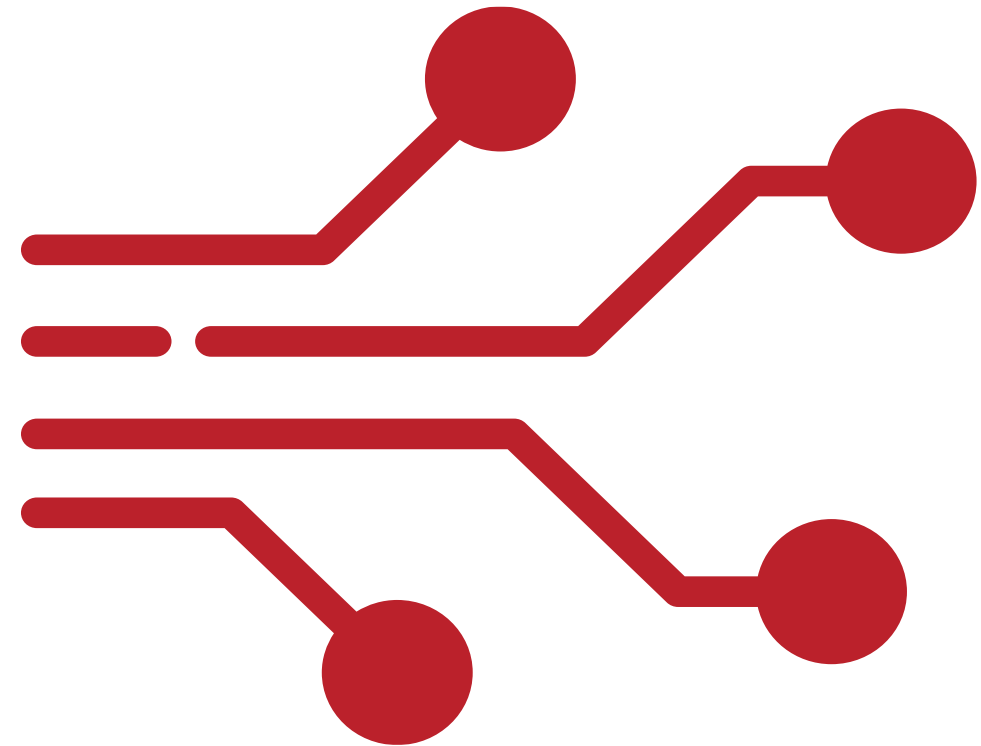
- każdy port = osobna domena kolizji
- urządzenia podłączone do różnych portów nie zakłócają się nawzajem

Router:

- oddziela sieci → każda sieć podłączona do routera ma własną domenę kolizji

271

Punkty dostępu bezprzewodowego (AP)



272

Access Points (AP) – punkt dostępowy Wi-Fi

Urządzenia pracujące głównie w warstwie łącza danych (2) modelu ISO/OSI

łączą urządzenia bezprzewodowe z siecią przewodową

Przekazywanie – lokalna operacja przełącznika polegająca na przesłaniu ramki z portu wejściowego do odpowiedniego portu wyjściowego na podstawie adresu MAC odbiorcy, proces realizowany sprzętowo (ASIC), co zapewnia jego błyskawiczne działanie (w skali nanosekund)

Przełączanie – proces sieciowy warstwy łącza danych, polegający na podejmowaniu decyzji, do którego portu wyjściowego należy przesłać ramkę na podstawie adresu MAC odbiorcy, obejmuje: uczenie się adresów MAC urządzeń podłączonych do portów, tworzenie i utrzymywanie tablicy MAC (CAM table), kierowanie ramek tylko do właściwego odbiorcy, w razie braku wpisu – rozgłaszanie (broadcast)

Access Points (AP) – zasada działania

1. Klient (np. laptop, telefon) wysyła ramkę Wi-Fi z adresem MAC
2. AP odbiera ramkę i tłumaczy ją na standard Ethernet
3. Ramka trafia do sieci LAN (np. switcha lub routera)
4. W drugą stronę – dane przewodowe są zamieniane przez AP na sygnał radiowy i wysyłane do klienta

Dla użytkownika wygląda to tak, jakby był „wpięty kablem do switcha”, tylko że bezprzewodowo

274

Access Points (AP) – funkcje

Zapewnienie dostępu do sieci urządzeniom Wi-Fi

Konwersja sygnałów przewodowy ↔ bezprzewodowy

Obsługa wielu standardów IEEE 802.11 (a/b/g/n/ac/ax – Wi-Fi 6)

Autoryzacja użytkowników (hasło, 802.1X)

Szyfrowanie ruchu (WEP – przestarzałe, WPA2, WPA3)

Możliwość ograniczania przepustowości i liczby użytkowników

Obsługa QoS (priorytetyzacja pakietów np. dla VoIP)

Obsługa VLAN – przypisywanie różnych SSID do różnych podsieci

275

Access Points (AP) – rodzaje

Samodzielne AP:

Działają indywidualnie, konfiguracja oddzielna

Dobre do małych sieci (dom, małe biuro)

AP zarządzane kontrolerem:

W dużych sieciach (firmy, szkoły, uczelnie)

Wiele AP podłączonych do jednego kontrolera, który zarządza całą siecią Wi-Fi

AP wbudowane w routery domowe:

Najczęstsze rozwiązanie w domach

Router = router (warstwa 3) + switch (warstwa 2) + AP (warstwa 2)

Access Points (AP) – rodzaje

Repeater / Extender Wi-Fi:

Specjalny rodzaj AP służący do rozszerzania zasięgu istniejącej sieci Wi-Fi

Mesh AP:

Tworzą sieć kratową (mesh) – wiele punktów współpracuje, dając pełny zasięg

Umożliwia płynny roaming (np. w biurach, domach piętrowych)

277

Access Points (AP) – konfiguracja

SSID (Service Set Identifier) – nazwa sieci Wi-Fi

Kanał radiowy – unikanie zakłóceń (np. wybór wolniejszego kanału w paśmie 2,4 GHz)

Pasmo częstotliwości – 2,4 GHz (większy zasięg, mniejsza prędkość) lub 5 GHz / 6 GHz (mniejszy zasięg, większa prędkość)

Szyfrowanie i hasło – WPA2 / WPA3 dla bezpieczeństwa

Moc nadawania – dostosowanie zasięgu

VLAN – przypisywanie różnych SSID do różnych podsieci (np. pracownicy, goście)

278

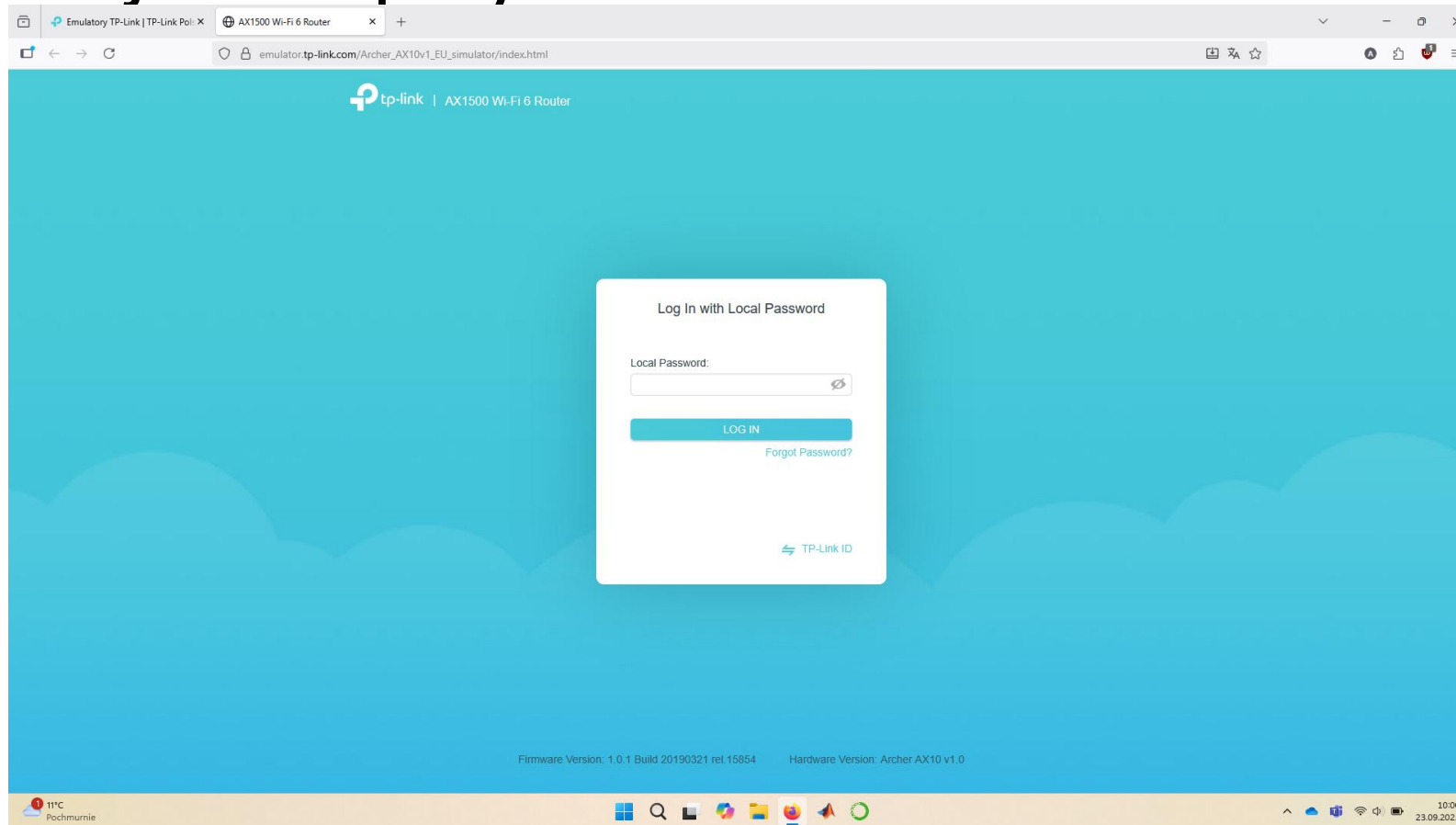
Access Points (AP) – konfiguracja

Dostęp do panelu AP

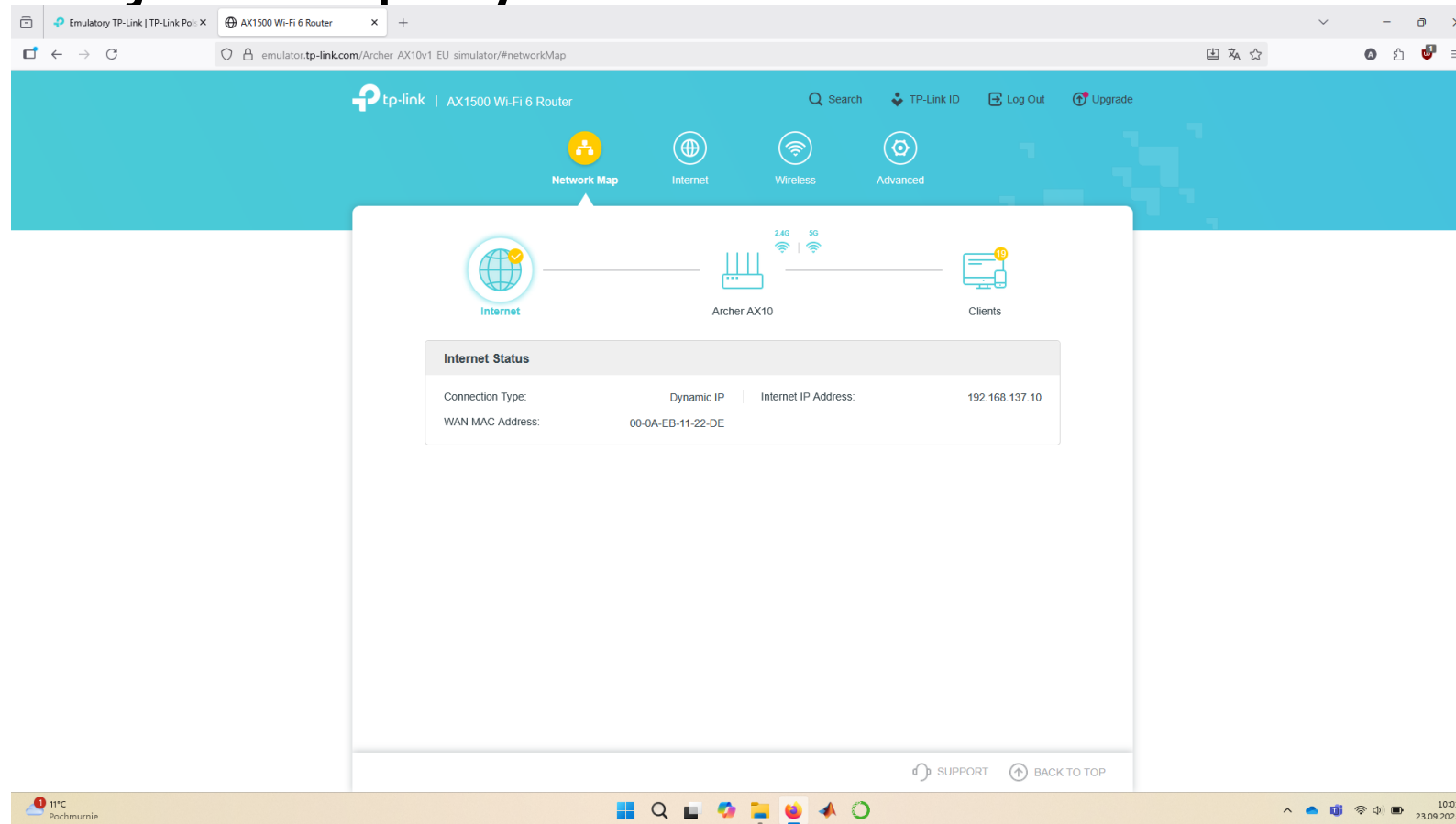
- Podłącz AP do routera/switcha przewodowego
- Na komputerze ustaw uzyskiwanie adresu IP automatycznie (DHCP)
- W przeglądarce wpisz adres AP (np. 192.168.0.254 – typowe dla TP-Link)
- Zaloguj się (domyślne: login admin, hasło admin – do zmiany przy pierwszym logowaniu)

279

Konfiguracja AP - przykład



Konfiguracja AP - przykład



281

Access Points (AP) – konfiguracja

Tryb pracy

Access Point (AP) - Tworzy nowy punkt dostępu do istniejącej sieci LAN, łączy urządzenia bezprzewodowe (laptop, telefon) z siecią przewodową (Ethernet), Działa jak „switch bezprzewodowy”

Repeater (Wzmacniacz Wi-Fi) - Powiela sygnał Wi-Fi z istniejącej sieci i retransmituje go dalej, nie tworzy nowej sieci przewodowej, tylko rozszerza zasięg

282

Access Points (AP) – konfiguracja

Wybór pasma

Pasmo 2,4 GHz

Zasięg: większy (lepiej przenika ściany)

Prędkość: niższa (do ok. 300–600 Mb/s w Wi-Fi 4, do 1 Gb/s w Wi-Fi 6)

Zakłócenia: duże (kuchenki mikrofalowe, Bluetooth, inne sieci Wi-Fi)

Kanały: tylko 3 niekolidujące (1, 6, 11)

Zastosowanie: urządzenia daleko od AP, starsze urządzenia

283

Access Points (AP) – konfiguracja

Wybór pasma

Pasma 5 GHz

Zasięg: mniejszy (gorzej przechodzi przez ściany)

Prędkość: wyższa (nawet 3–4 Gb/s w Wi-Fi 6)

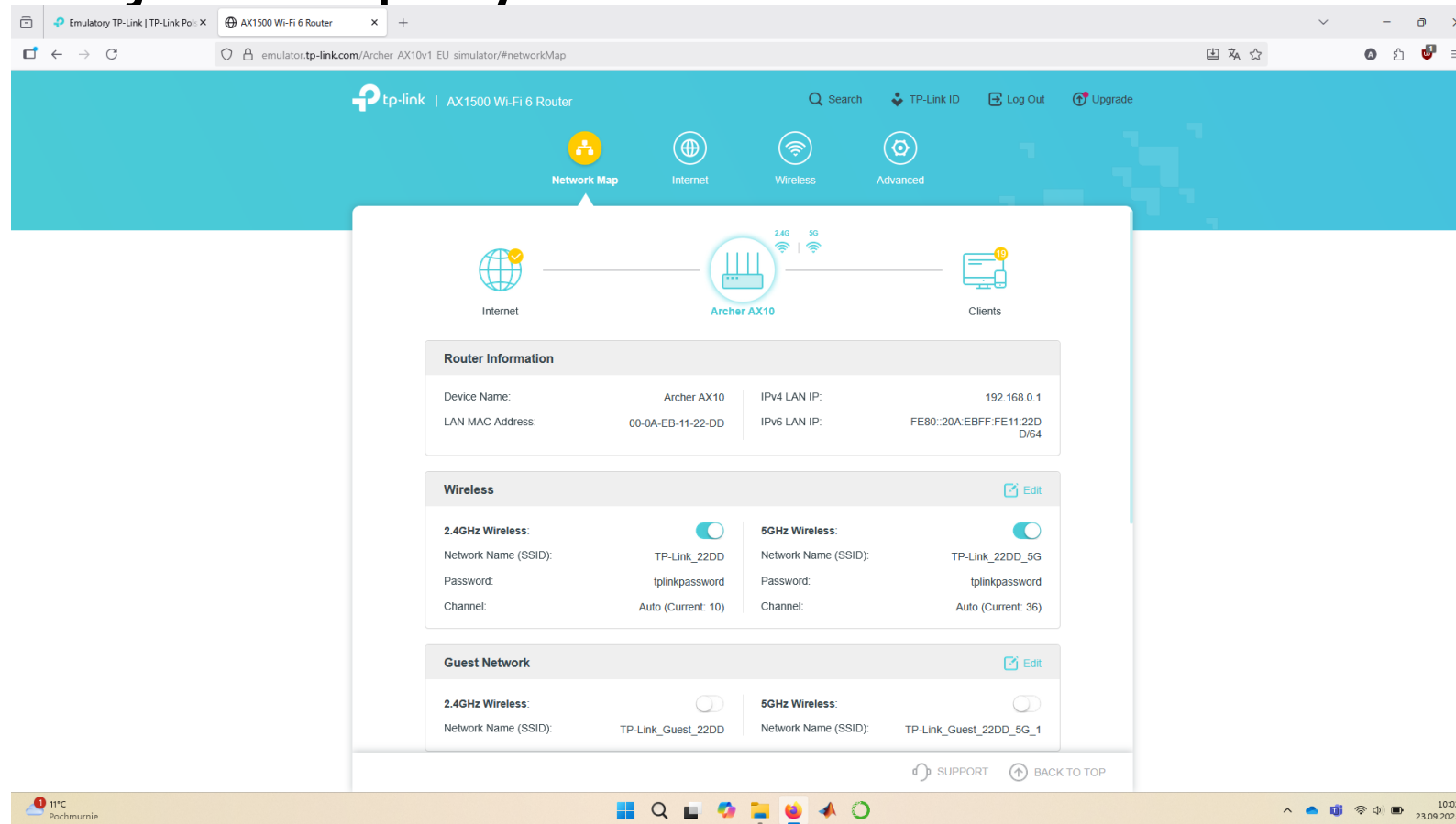
Zakłócenia: mniejsze (więcej wolnych kanałów)

Kanały: kilkanaście niekolidujących

Zastosowanie: szybki Internet, gry online, multimedia, streaming

284

Konfiguracja AP - przykład



285

Access Points (AP) – konfiguracja

Zabezpieczenia

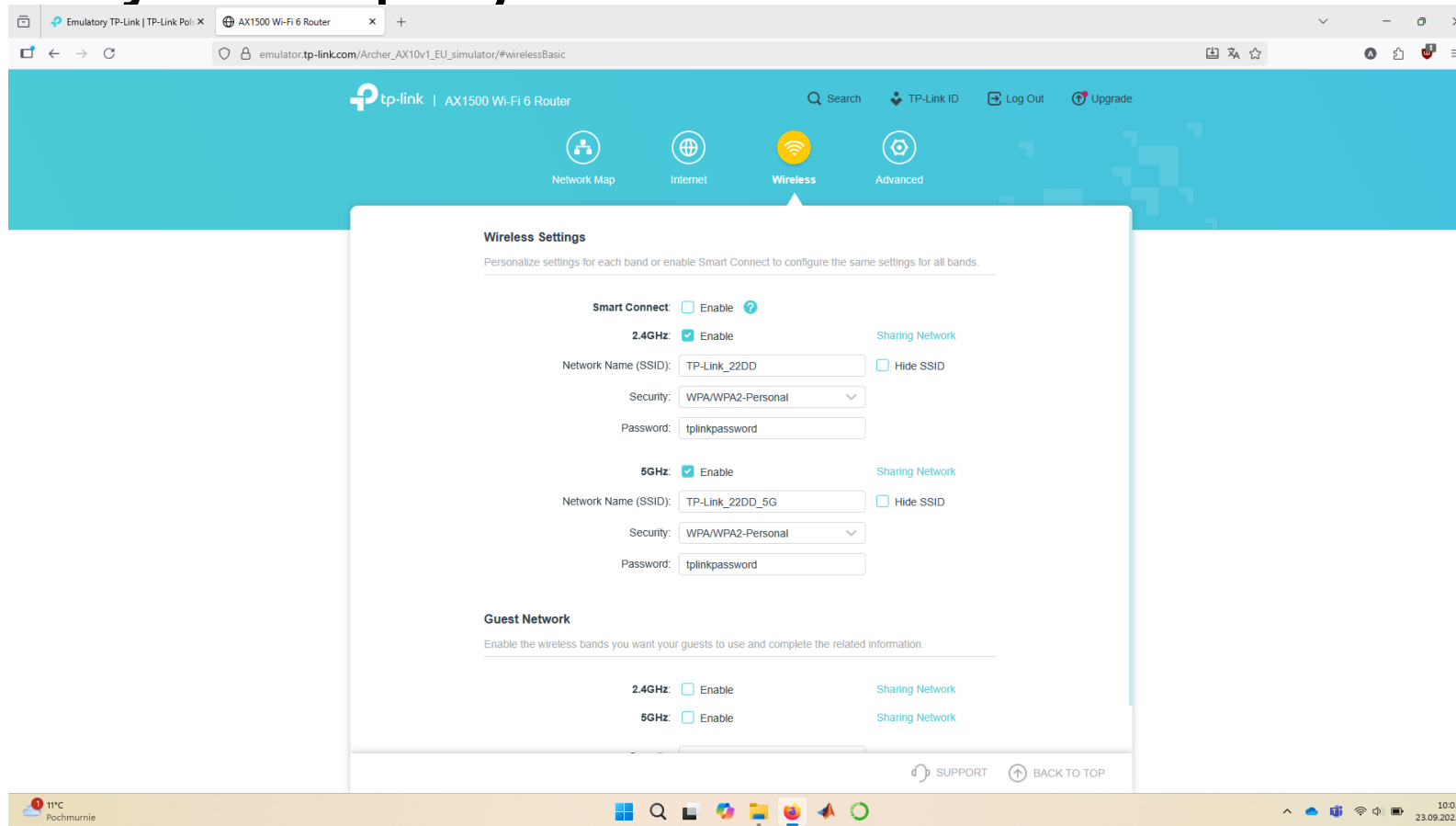
WEP (Wired Equivalent Privacy) – stary standard, bardzo słabe szyfrowanie, łatwe do złamania → NIE stosować

WPA (Wi-Fi Protected Access) – następca WEP, poprawione bezpieczeństwo, ale dziś również przestarzałe

WPA2 – standard od 2004 r., używa szyfrowania AES – wciąż najpopularniejsze zabezpieczenie w sieciach Wi-Fi

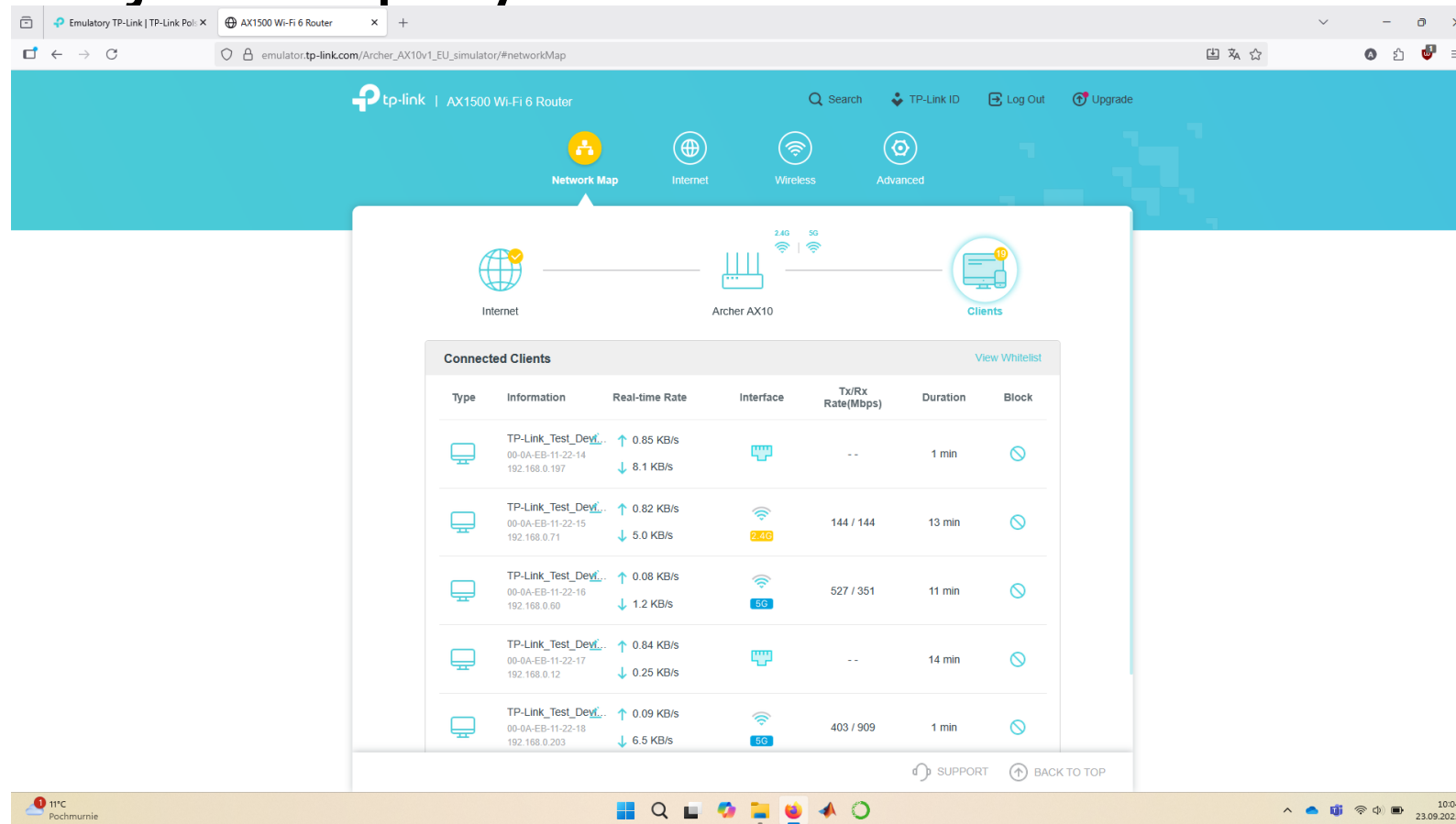
WPA3 – najnowszy standard (od 2018 r.) – jeszcze silniejsze szyfrowanie, ochrona przed atakami słownikowymi – wymaga nowszego sprzętu

Konfiguracja AP - przykład



287

Konfiguracja AP - przykład



tp-link | AX1500 Wi-Fi 6 Router

Search TP-Link ID Log Out Upgrade

Network Map Internet Wireless Advanced

Internet Archer AX10 Clients

Connected Clients View Whitelist

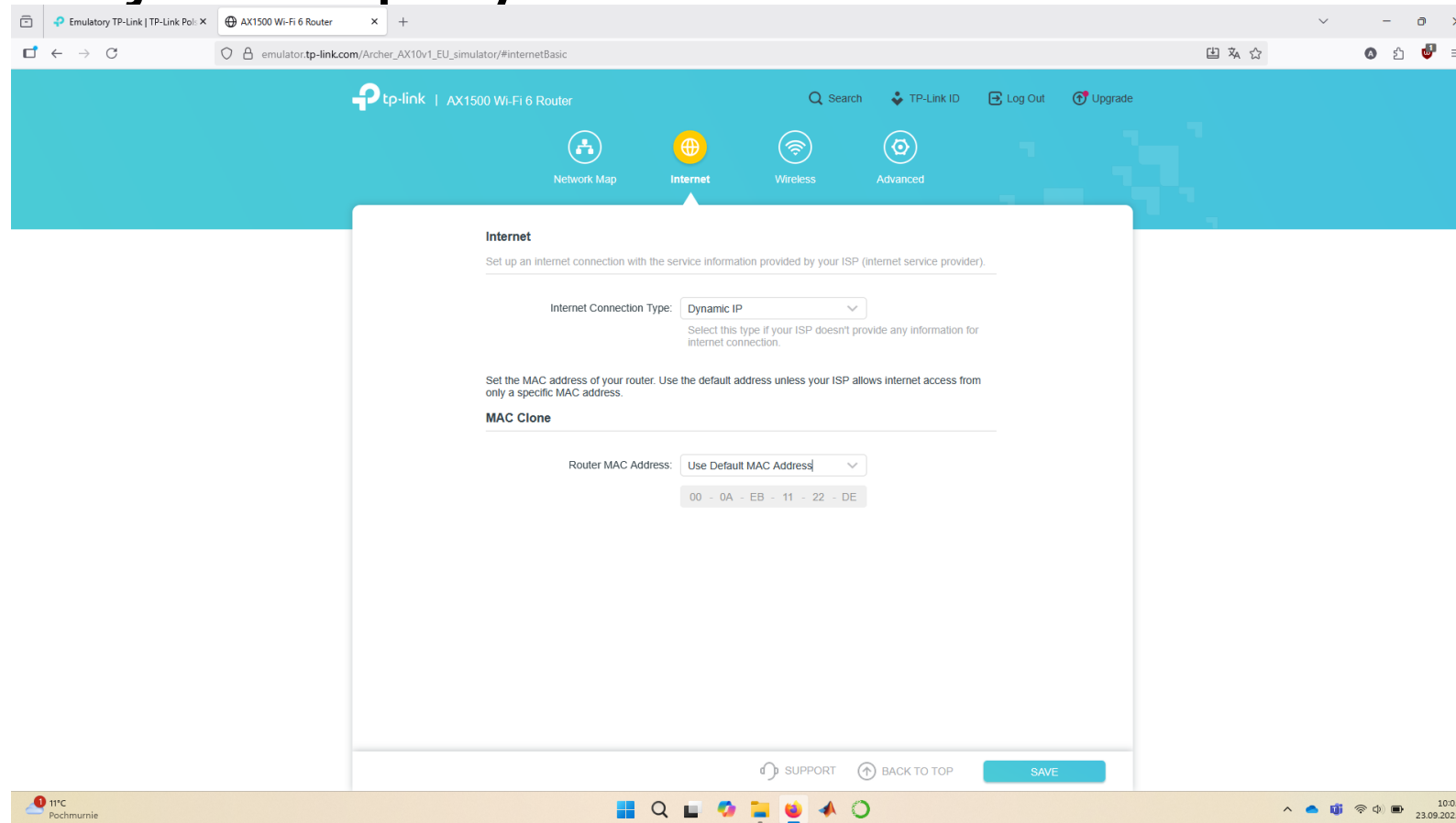
Type	Information	Real-time Rate	Interface	Tx/Rx Rate(Mbps)	Duration	Block
TP-Link_Test_Dev...	00-0A-EB-11-22-14 192.168.0.197	↑ 0.85 KB/s ↓ 8.1 KB/s		--	1 min	ⓘ
TP-Link_Test_Dev...	00-0A-EB-11-22-15 192.168.0.71	↑ 0.82 KB/s ↓ 5.0 KB/s	2.4G	144 / 144	13 min	ⓘ
TP-Link_Test_Dev...	00-0A-EB-11-22-16 192.168.0.60	↑ 0.08 KB/s ↓ 1.2 KB/s	5G	527 / 351	11 min	ⓘ
TP-Link_Test_Dev...	00-0A-EB-11-22-17 192.168.0.12	↑ 0.84 KB/s ↓ 0.25 KB/s		--	14 min	ⓘ
TP-Link_Test_Dev...	00-0A-EB-11-22-18 192.168.0.203	↑ 0.09 KB/s ↓ 6.5 KB/s	5G	403 / 909	1 min	ⓘ

SUPPORT BACK TO TOP

11°C Pochmurnie 10:04 23.09.2025

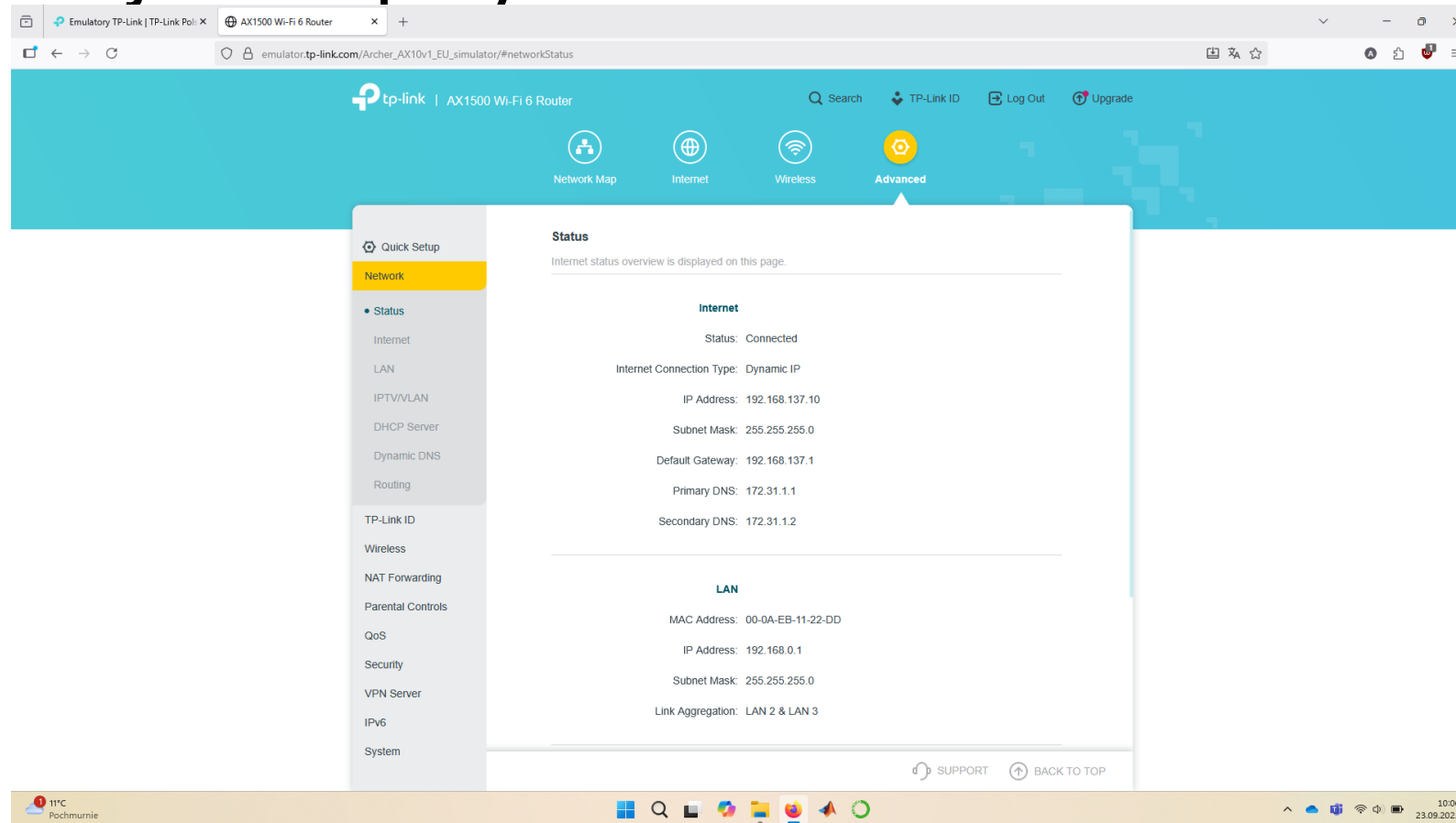
288

Konfiguracja AP - przykład



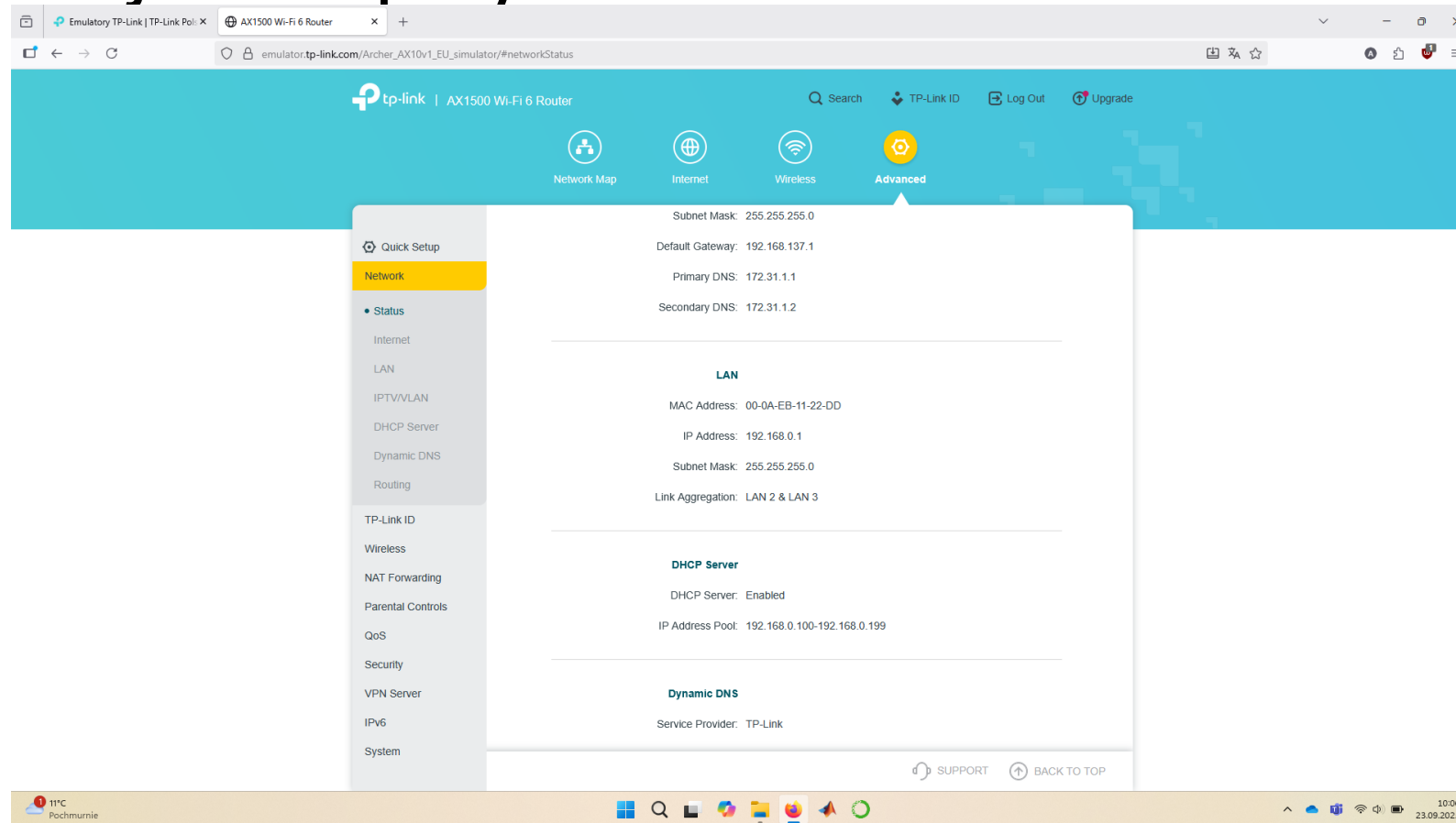
289

Konfiguracja AP - przykład



290

Konfiguracja AP - przykład



291

Access Points (AP) – konfiguracja

VLAN (Virtual LAN) - logiczny podział jednej fizycznej sieci na wiele mniejszych segmentów (podsieci)

Każdy VLAN działa jak osobna sieć LAN

Przykład: VLAN 10 (pracownicy), VLAN 20 (księgowość), VLAN 30 (goście)

Bezpieczeństwo – odseparowanie ruchu różnych grup użytkowników

Lepsza organizacja – łatwe zarządzanie ruchem w sieci

Redukcja broadcastów (mniej niepotrzebnego ruchu)

W AP: można przypisać różne SSID (nazwy Wi-Fi) do różnych VLAN-ów

292

Access Points (AP) – konfiguracja

Guest Network (Sieć gościnna) - wydzielona sieć Wi-Fi dla gości

Tworzona w AP/routerze jako osobne SSID

Zwykle odseparowana od głównej sieci LAN → goście mają tylko dostęp do Internetu, a nie do komputerów firmowych

Bezpieczeństwo (goście nie „widzą” urządzeń wewnętrznych)

Łatwość konfiguracji – często kilka kliknięć w panelu AP

Możliwość ograniczenia pasma lub liczby podłączonych urządzeń

293

Access Points (AP) – konfiguracja

QoS – Quality of Service – mechanizmy w sieci, które priorytetyzują ruch, aby ważne aplikacje miały zapewnioną jakość transmisji (przepustowość, opóźnienia, utrata pakietów)

Główne funkcje QoS:

Priorytetyzacja ruchu (VoIP, wideo, gry online > zwykłe pobieranie plików)

Rezerwacja pasma – gwarantowana minimalna przepustowość

Kontrola opóźnień (latency) – ważne dla rozmów i transmisji wideo

Kolejkowanie i limitowanie – różne typy ruchu w osobnych kolejkach

294

Access Points (AP) – przykład

Konfiguracja sieci bezprzewodowej w routerze/AP:

tworzenie sieci głównej (SSID, hasło WPA2/WPA3)

dodanie sieci gościnnej (Guest Network)

włączenie izolacji gości (tylko Internet, brak dostępu do LAN)

zastosowanie QoS (Quality of Service) do ograniczania pasma i priorytetyzacji ruchu

295

Dziękuję za uwagę

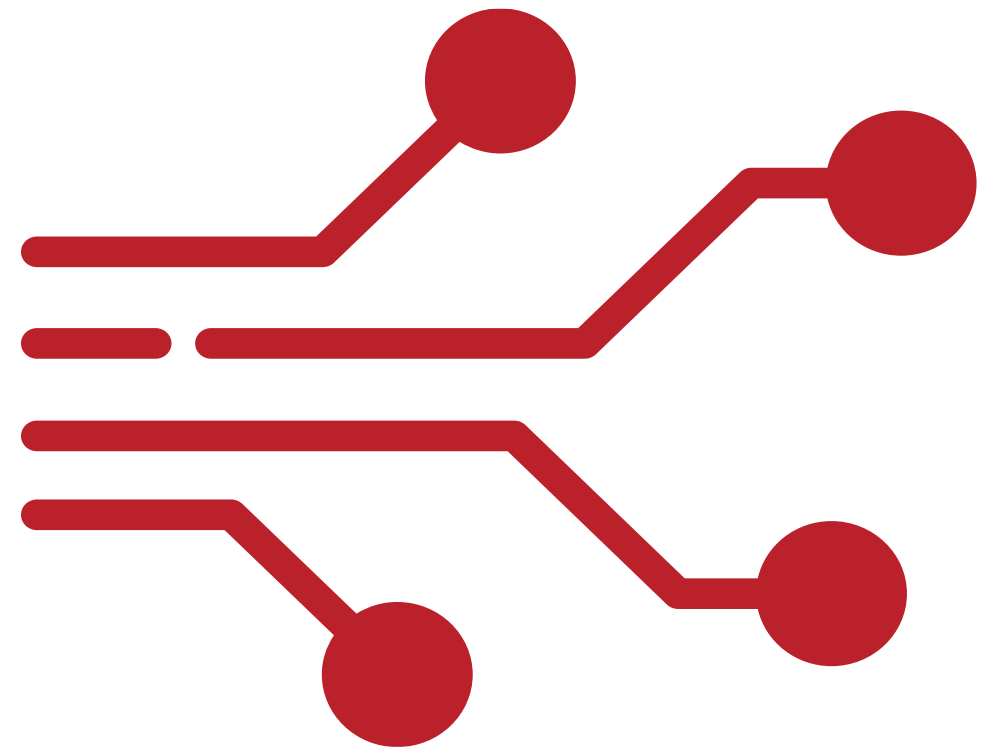
Treści programowe:

- Protokoły sieciowe. Protokół IP: funkcje, różnice między IPv4 a IPv6
- Protokoły transportowe: TCP i UDP – różnice i zastosowania
- Protokoły sieciowe: DHCP (przydzielanie adresów IP), DNS (tłumaczenie nazw na adresy IP)
- Protokoły aplikacyjne: HTTP/HTTPS, FTP, SMTP, POP3, IMAP
- Protokół ARP i ICMP: mechanizmy działania i zastosowania



297

Protokoły sieciowe. Protokół IP: funkcje, różnice między IPv4 a IPv6



298

Protokoły sieciowe

Protokół = zestaw reguł komunikacji między urządzeniami

Określa:

- format danych
- sposób adresowania
- kolejność komunikatów
- zachowanie przy błędach

Przykład: rozmowa w jednym języku – obie strony muszą znać te same zasady

299

Dlaczego protokoły sieciowe są ważne?

Umożliwiają komunikację między różnymi urządzeniami (np. PC z Windows, serwer Linux, telefon Android)

Zapewniają zgodność i interoperacyjność – każdy producent stosuje te same standardy (RFC)

Bez protokołów komunikacja w sieci byłaby niemożliwa

300

Protokoły sieciowe - Model TCP/IP

Model warstwowy TCP/IP:

Każda warstwa ma swoje protokoły i zadania:

- **Dostępu do sieci:** Ethernet, Wi-Fi – przesyłają ramki w sieci lokalnej
- **Sieciowa:** IP, ICMP, ARP – adresuje hosty i dostarcza pakiety między sieciami
- **Transportowa:** TCP, UDP – dostarcza dane do odpowiednich aplikacji
- **Aplikacyjna:** HTTP, DNS, FTP, SMTP – to, czego używa użytkownik

301

Protokoły sieciowe

Protokoły współpracują **pionowo** (warstwa wyższa korzysta z usług warstwy niższej) oraz **poziomo** (host A komunikuje się z hostem B za pomocą tego samego protokołu)

Każdy protokół wykonuje swoje odrębne zadanie ale dopiero razem tworzą pełen model komunikacji: od nazwy domenowej, przez adres IP, aż po np. otwarcie strony w przeglądarce

302

Przykład – otwarcie strony w przeglądarce

1. **DNS (UDP/53)** – komputer pyta serwer DNS o adres IP www.pollub.pl
2. **IP** – zna już IP serwera, więc wysyła pakiet IP z adresem docelowym
3. **TCP (port 80/443)** – przeglądarka zestawia połączenie TCP z serwerem WWW (3-way handshake)
4. **HTTP/HTTPS** – przesyła żądanie GET: „daj mi stronę główną”
5. **ARP (w LAN)** – jeśli komputer nie zna adresu MAC routera, używa ARP, aby wysłać pakiet w sieci lokalnej
6. **ICMP** – gdy coś nie działa (np. TTL=0), routery zwracają komunikat ICMP, dzięki czemu można diagnozować trasę (ping, traceroute)

303

Przykład – otwarcie strony w przeglądarce

Jak wygląda to w warstwach (enkapsulacja):

Aplikacja (HTTP) → dane użytkownika

Transport (TCP) → dzieli na segmenty, dodaje numery portów

Sieciowa (IP) → dodaje adres źródłowy i docelowy

Dostępu do sieci (Ethernet/Wi-Fi) → dodaje adresy MAC

Każda warstwa dokłada swoją „kopertę” → tworzy się kapsuła danych

Na końcu odbiorca otwiera te koperty w odwrotnej kolejności

304

Protokół IP

Pełna nazwa: Internet Protocol

Rola: Dostarczanie pakietów danych między urządzeniami w sieci

Warstwa: sieciowa

Wersje:

IPv4 (starsza, szeroko stosowana, RFC 791, 1981)

IPv6 (nowsza, stopniowo wdrażana, RFC 8200, 2017)

Zadania: Adresacja hostów, routing, enkapsulacja danych w pakiety, fragmentacja pakietów, TTL (Time To Live)

305

Protokół IPv4

Format: 32 bity, 4 oktety (np. 192.168.1.1)

Klasy adresów: A (duże sieci), B, C (małe), D (multicast), E (rezerwowane)

CIDR: Classless Inter-Domain Routing (np. /24 dla podsieci)

Pola nagłówka:

Wersja, IHL (długość nagłówka), TOS (typ usługi), długość pakietu, ID, flagi, offset, TTL, protokół, suma kontrolna, adres źródłowy/docelowy, opcje

Zmienna długość: 20-60 bajtów

306

Protokół IPv4

Zalety: powszechna stosowalność, kompatybilność, prostota wdrożenia

Ograniczenia: 4,3 mld adresów (wyczerpane w 2011 przez IANA),
fragmentacja w routerach, brak wbudowanego bezpieczeństwa

Niezbędny NAT (Network Address Translation):

- Tłumaczenie prywatnych adresów IP (RFC 1918) na publiczne adresy IP
- Statyczny, dynamiczny, PAT (Port Address Translation)
- Oszczędność adresów, podstawowa ochrona
- Komplikuje komunikację P2P, śledzenie połączeń

307

Protokół IPv4 - NAT

Hosty używają adresów IP z zakresów prywatnych (np. 192.168.x.x), które nie są rutowane w Internecie

Router ma jeden publiczny adres IP przypisany przez dostawcę Internetu

Translacja wychodząca (SNAT) - Kiedy urządzenie z sieci lokalnej wysyła pakiet do Internetu, router zmienia prywatny adres źródłowy na swój publiczny adres IP

Tabela NAT - router zapisuje informacje o tej zmianie w tabeli NAT, łącząc prywatny adres i port z publicznym adresem i innym portem

308

Protokół IPv4 - NAT

Translacja przychodząca (SNAT) - gdy odpowiedź wraca z Internetu, router używa tabeli NAT, aby zidentyfikować, do którego urządzenia w sieci lokalnej ma przesłać pakiet, zamieniając publiczny adres z powrotem na prywatny adres docelowy

Zalety:

Oszczędność adresów IPv4: jednoczesne połączenie wielu urządzeń z Internetem przy użyciu tylko jednego publicznego adresu IPv4

Bezpieczeństwo: ukrywanie wewnętrznej struktury sieci i adresów IP urządzeń

309

Protokół IPv4 – format datagramu

Pole numeru wersji	Pole długości nagłówka	Pole typu usługi	Pole długości datagramu
Pole 16-bitowego identyfikatora		Pole znaczników	Pole 13-bitowej pozycji fragmentów
Pole wartości TTL	Pole protokołu wyższej warstwy	Pole sumy kontrolnej nagłówka	
Pole 32-bitowego źródłowego adresu IP			
Pole 32-bitowego docelowego adresu IP			
Pole opcji (o ile występują)			
Pole danych			

310

Protokół IPv4 – format datagramu

Pole numeru wersji:

4-bitowe pole określające numer wersji protokołu IP – wartość 4
Sprawdzając numer wersji router może stwierdzić w jaki sposób
interpretować resztę datagramu IP – IPv4 lub IPv6

Pole długości nagłówka:

4-bitowe pole oznaczające od którego miejsca zaczynają się dane
datagramu IP – liczba opcji może być zmienna – zwykle 20 bajtów
(jeżeli nie ma opcji)

311

Protokół IPv4 – format datagramu

Pole typu usługi:

Umożliwia odróżnienie różnych typów datagramów IP, np. telefonii internetowej od klienta FTP

Pole długości datagramu:

Określa całkowitą długość datagramu w bajtach = nagłówek + dane

Pole 16 bitowe – maksymalny rozmiar datagramu IP = 65535 bajtów

Zazwyczaj długość datagramu nie przekracza 1500 bajtów

312

Protokół IPv4 – format datagramu

Pola identyfikatorów, znaczników i pozycji fragmentów:

Określają fragmentację datagramu IP – wersja IPv6 nie zezwala na fragmentację

Pole wartości TTL (Time To Live):

Pole zapobiega krążeniu bez końca datagramów w sieci (długotrwała pętla routingu)

Wartość pola jest zmniejszana o jeden każdorazowo po przetworzeniu przez router, wartość TTL = 0 – odrzucenie datagramu

313

Protokół IPv4 – format datagramu

Pole protokołu wyższej warstwy:

Używane tylko wtedy, gdy datagram IP dotrze do miejsca docelowego

Wartość identyfikuje określony protokół warstwy transportowej, do której powinny zostać dostarczone dane, np. wartość 6 – TCP, wartość 17 - UDP

Pole sumy kontrolnej:

Pomaga wykrywać routerowi błędy bitów w odebranym datagramie

Obliczane jako suma liczbowa każdych dwóch bajtów nagłówka

314

Protokół IPv4 – format datagramu

Pola źródłowego i docelowego adresu IP:

Węzeł tworząc datagram IP umieszcza swój adres IP (źródło) oraz adres IP przeznaczenia (docelowy)

Pole opcji:

Umożliwia rozszerzenie nagłówka datagramu IP – rzadko stosowane

Nagłówki datagramów mogą mieć różną długość – nie można określić gdzie rozpoczyna się pole danych, część datagramów może wymagać opcji – czas przetwarzania przez router może się różnić

315

Protokół IPv4 – format datagramu

Pole danych (treść zasadnicza):

Ostatnie i najważniejsze pole – powód istnienia datagramu IP

W większości sytuacji pole danych zawiera segment warstwy transportowej (segment TCP lub UDP) przesyłany w miejsce docelowe

Może przechowywać też dane innego typu, np. komunikaty protokołu ICMP

316

Protokół IPv6

Format: 128 bitów, 8 grup heksadecymalnych

(np. 2001:0db8:85a3:0000:0000:8a2e:0370:7334)

Skróty: Pomijanie zer wiodących, :: dla ciągów zer

Niedobór adresów IPv4, wzrost urządzeń mobilnych/IoT

Masowa adopcja od 2010+

Adopcja w 2025: Ok. 40-50% ruchu internetowego (na podstawie danych Google)

317

Protokół IPv6

Typy adresów:

- Unicast – unikalny adres hosta
- Multicast – dla grup hostów
- Anycast – wysyłanie do najbliższego hosta
- Link-local – fe80::, do komunikacji w LAN

Pola nagłówka: Wersja, klasa ruchu, etykieta przepływu, długość ładunku, następny nagłówek, limit skoków, adres źródłowy/docelowy

Stała długość: 40 bajtów + rozszerzenia

318

Protokół IPv6

Cechy:

- Autokonfiguracja (SLAAC)
- Wbudowane bezpieczeństwo (IPsec)
- Uproszczony nagłówek → szybsze przetwarzanie
- Brak NAT – każdy host ma globalny adres
- Privacy Extensions: Tymczasowe adresy dla anonimowości
- Neighbor Discovery Protocol (NDP): Zastępuje ARP w IPv6

319

Protokół IPv6 – najważniejsze zmiany

- Rozszerzone możliwości adresowania – 32 bity (IPv4) vs 128 bitów (IPv6), nowy typ adresu – adres anycast – umożliwia dostarczenie datagramów do dowolnej grupy hostów
- Udoskonalony 40-bajtowy nagłówek – rezygnacja z kilku pól (jako opcje) w porównaniu z IPv4 – stała długość umożliwia szybsze przetwarzanie datagramu IP
- Oznaczenie przepływu – nowa definicja – umożliwia oznaczanie pakietów należących do przepływu (niestandardowe usługi lub różne priorytety)

320

Protokół IPv6 – format datagramu

Pole numeru wersji	Pole kategorii danych sieciowych	Pole etykiety przepływu	
Pole rozmiaru danych		Pole nagłówka kolejnego protokołu	Pole maksymalnej liczby routerów
Pole 128-bitowego źródłowego adresu IP			
Pole 128-bitowego docelowego adresu IP			
Pole danych			

321

Protokół IPv6 – format datagramu

Pole numeru wersji:

4-bitowe pole określające numer wersji protokołu IP – wartość 6
Umieszczenie wartości 4 nie spowoduje utworzenia poprawnego datagramu IPv4

Pole kategorii danych sieciowych:

8-bitowe pole podobne do pola typu usługi IPv4

Może być wykorzystywane do priorytetowego traktowania datagramów z określonej aplikacji (np. telefonia VoIP) względem innych datagramów (np. poczta elektroniczna SMTP)

322

Protokół IPv6 – format datagramu

Pole etykiety przepływu:

20-bitowe pole służące do identyfikowania przepływu datagramów

Pole rozmiaru danych:

16-bitowe pole zawierające wartość (liczba całkowita) określającą liczbę bajtów danych znajdujących się za 40-bitowym nagłówkiem (niezmienna długość) datagramu IPv6

323

Protokół IPv6 – format datagramu

Pole nagłówka kolejnego protokołu:

Pole identyfikujące protokół do którego zostanie dostarczona zawartość datagramu (TCP lub UDP)

Przechowuje takie same wartości, co pole protokołu wyższej warstwy zawarte w nagłówku IPv4

Pole maksymalnej liczby routerów:

Wartość pola zmniejszana o jeden przez kolejne routery przekazujące datagram, wartość 0 – odrzucenie datagramu

324

Protokół IPv6 – format datagramu

Pola źródłowego i docelowego adresu IP:

Węzeł tworząc datagram IP umieszcza swój adres IP (źródło) oraz adres IP przeznaczenia (docelowy)

Pole danych:

Dane datagramu IPv6 – po dotarciu do miejsca przeznaczenia zostają wyodrębnione i przekazane protokołowi określonymu w polu nagłówka kolejnego protokołu

325

Protokół IPv4 vs IPv6

Cecha	IPv4	IPv6
Adres	32 bity, dziesiętny	128 bitów, heksadecymalny
Pula adresów	~ 4,3 mld	~ nieskończona (przeliczalna)
NAT	Wymagany	Opcjonalny
Fragmentacja	Nadawca/routery	Tylko nadawca
Bezpieczeństwo	Opcjonalne	Wbudowane (IPsec)
Autokonfiguracja	DHCP	SLAAC + DHCPv6

326

Przejsie na IPv6 - mechanizmy

Dual Stack:

Polega na jednoczesnym uruchomieniu protokołu IPv4 i IPv6 na tych samych urzadzeniach i interfejsach

Dzieki temu hosty i routery moga komunikowac sie zarowno po IPv4, jak i po IPv6, w zaleznosci od tego, ktory protokol jest obslugiwany przez druga strone

Jest to najprostsza i najbardziej naturalna metoda migracji, ale wymaga podwojnej konfiguracji i utrzymywania obu protokolow

327

Przejsie na IPv6 - mechanizmy

Tunelowanie:

Stosowane, gdy sieć IPv6 musi przesyłać dane przez infrastrukturę, która wspiera tylko IPv4

Mechanizm ten opakowuje pakiety IPv6 w pakiety IPv4 (enkapsulacja)

6to4 – automatyczne tworzenie tuneli IPv6 przez sieć IPv4, używane w scenariuszach połączenia różnych wysp IPv6

Teredo – umożliwia przesyłanie ruchu IPv6 przez translacje NAT w sieciach IPv4, szczególnie przydatne dla użytkowników domowych

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) – stosowany wewnątrz organizacji, do tworzenia tuneli IPv6 w ramach infrastruktury IPv4

328

Przejsie na IPv6 - mechanizmy

Translacja:

Umożliwia komunikację między hostami IPv6 a IPv4

Polega na tłumaczeniu nagłówek pakietów i adresów, podobnie jak w klasycznym NAT

NAT64 – pozwala urządzeniom z IPv6 na dostęp do usług działających tylko w IPv4 poprzez translację adresów

DNS64 – uzupełnia NAT64, generując rekordy AAAA (IPv6) na podstawie rekordów A (IPv4), aby hosty IPv6 mogły odnaleźć serwery IPv4

329

Przejsie na IPv6 - wyzwania

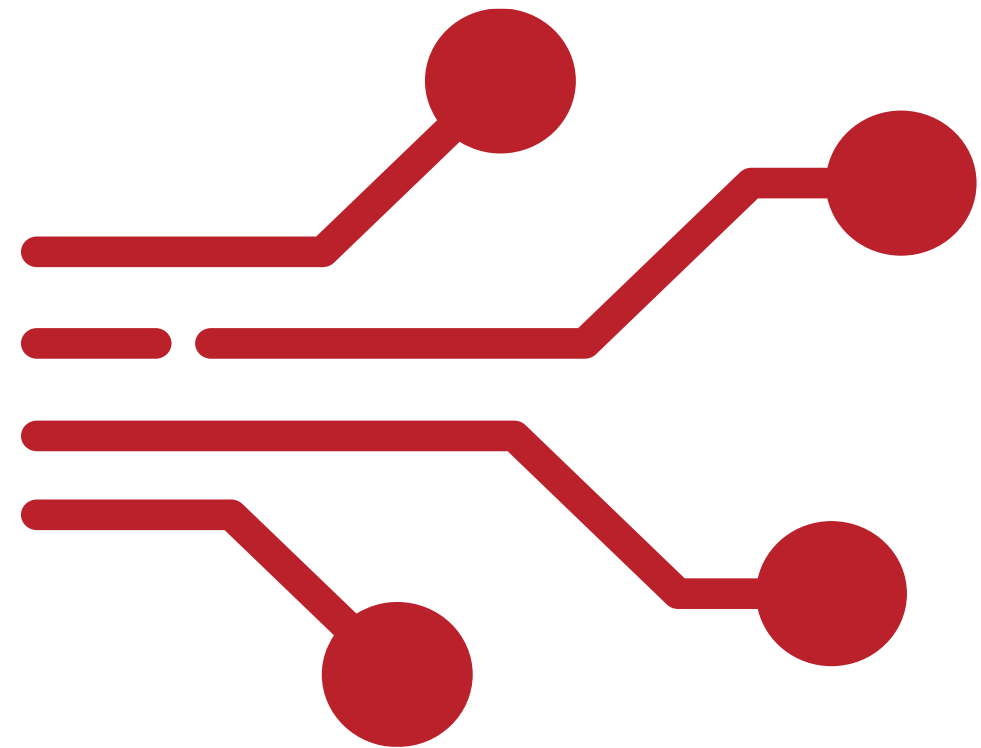
Koszty migracji – konieczność modernizacji infrastruktury, oprogramowania i szkoleń dla administratorów

Kompatybilność starszego sprzętu – wiele starszych urządzeń nie wspiera IPv6 i wymaga wymiany lub dodatkowej konfiguracji

Złożoność przejściowa – okres równoległego działania IPv4 i IPv6 oznacza dodatkowe obciążenia administracyjne, testowanie aplikacji i rozwiązywanie problemów związanych z bezpieczeństwem

330

Protokoły transportowe: TCP i UDP – różnice i zastosowania



331

Protokoły transportowe

Protokoły transportowe odpowiadają za komunikację między aplikacjami na różnych hostach, a nie tylko między urządzeniami sieciowymi

Kluczową rolę pełnią porty, które pozwalają rozróżniać różne procesy działające na tym samym komputerze (np. serwer WWW na porcie 80, poczta na 25)

Zapewniają też kontrolę błędów i niezawodność transmisji (np. TCP), albo szybkie, bezpołączeniowe przesyłanie danych (UDP)

332

Protokół TCP

TCP (Transfer Control Protocol) – protokół zorientowany na połączenie – przed wysłaniem danych musi być ustanowione połączenie – proces negocjacji

Protokół TCP funkcjonuje tylko w systemach końcowych – routery i przełączniki nie utrzymują stanu połączenia – rozpoznają datagramy

Połączenie TCP działa w trybie pełnego duplexu – dane mogą być przesyłane niezależnie w obydwie strony

Połączenie TCP jest połączeniem typu punkt-punkt – jeden nadawca i jeden odbiorca

333

Protokół TCP – porty i gniazda

TCP jak punkty końcowe połączeń wykorzystuje gniazda

Gniazdo (Socket) - unikalny identyfikator połączenia: zestaw **IP + numer portu**

Na jednym komputerze może działać wiele usług naraz (np. strona WWW na porcie 80 i poczta na porcie 25)

Porty:

0–1023 → tzw. well-known ports (np. 80 HTTP, 443 HTTPS, 53 DNS)

1024–49151 → registered ports (np. 3306 MySQL)

49152–65535 → dynamic/ephemeral ports – używane tymczasowo przez klienta do zestawiania połączeń

334

Protokół TCP – porty i gniazda

Multipleksowanie - ten sam adres IP może obsłużyć wiele jednoczesnych połączeń, bo każde ma inny zestaw (IP źródłowy, port źródłowy, IP docelowy, port docelowy)

Umożliwia to np. wielu klientom korzystanie z jednej strony WWW równocześnie

Klient1: 192.168.1.10:50432 → 93.184.216.34:80

Klient2: 192.168.1.10:50433 → 93.184.216.34:80

Proces klienta – nawiązujący połączenie

Proces serwera – nasłuchujący połączeń

335

Protokół TCP – połączenie

Proces klienta – nawiązujący połączenie

- Inicjuje połączenie z serwerem (wysyła żądanie), korzysta z tymczasowego (dynamicznego) portu źródłowego
- Wysyła pierwszy segment SYN w ramach trójfazowego uzgadniania połączenia
- Oczekuje potwierdzenia od serwera
- Po zestawieniu połączenia wymienia dane z serwerem

Proces serwera – nasłuchujący połączeń

- Otwiera gniazdo i nasłuchuje na określonym porcie (np. 80 dla HTTP)
- Oczekuje przychodzących żądań od klientów, Po odebraniu:
 - potwierdza nawiązanie połączenie,
 - czeka na ostateczne potwierdzenie od klienta
- Po pełnym uzgodnieniu tworzy nowe gniazdo dedykowane danemu połączeniu
- Dalej przesyła dane, zapewniając niezawodność i kontrolę przepływu

336

Protokół TCP - połączenie

Nawiązywanie połączenia – tzw. 3-way handshake (flagi):

1. **Klient → SYN** – klient prosi o rozpoczęcie połączenia i wysyła swój numer sekwencyjny
2. **Serwer → SYN-ACK** – serwer potwierdza prośbę i wysyła swój numer sekwencyjny
3. **Klient → ACK** – klient potwierdza i połączenie jest gotowe

Zamykanie połączenia – tzw. 4-way handshake (flagi):

1. **Klient → FIN** – klient informuje, że nie ma więcej danych do wysłania
2. **Serwer → ACK** – serwer potwierdza odebranie żądania zamknięcia
3. **Serwer → FIN** – serwer po przesłaniu danych wysyła sygnał zakończenia
4. **Klient → ACK** – klient potwierdza i połączenie zostaje całkowicie zamknięte

337

Protokół TCP - flagi

SYN (Synchronize) - inicjuje połączenie (synchronizacja numerów sekwencyjnych) – początek 3-way handshake

ACK (Acknowledgment) - potwierdza odbiór danych/segmentów, obecna w większości pakietów po nawiązaniu sesji

FIN (Finish) - zamknięcie połączenia przez jedną stronę – początek 4-way handshake

RST (Reset) - nagłe zerwanie połączenia (np. błąd, brak usługi na porcie)

PSH (Push) - wymusza natychmiastowe przekazanie danych do aplikacji (bez buforowania)

URG (Urgent) - informuje, że dane w segmencie są priorytetowe i powinny być obsłużone od razu

338

Protokół TCP - nagłówek

Numer portu źródłowego					Numer portu docelowego				
Pole wartości sekwencyjnej									
Pole wartości potwierdzenia									
Pole długości nagłówka	Nie używane	URG	ACK	PSH	RST	SYN	FIN	Pole okna odbiorczego	
Pole internetowej sumy kontrolnej					Pole wskaźnika „pilnych” danych				
Pole opcji									
Pole danych									

339

339

Protokół TCP – nagłówek

Port źródłowy (16 bitów) - numer portu aplikacji wysyłającej dane

Port docelowy (16 bitów) - numer portu aplikacji odbierającej dane

Pole wartości sekwencyjnej (32 bity) - określa, od którego bajtu danych zaczyna się ten segment - TCP układa dane w odpowiedniej kolejności

Pole wartości potwierdzenia (Acknowledgment Number, 32 bity) - informuje, który bajt danych odbiorca oczekuje jako następny – czyli „potwierdzenie” odbioru poprzednich bajtów

Pole długości nagłówka (4 bity) – określa, ile słów 32-bitowych zajmuje nagłówek (minimum 20 bajtów) – informuje gdzie znajduje się właściwa treść danych

340

Protokół TCP - nagłówek

Zarezerwowane (6 bitów) - przeznaczone do przyszłego użytku (powinny być zerami)

Flagi (6 bitów najczęściej używanych, w rzeczywistości jest ich więcej): URG, ACK, PSH, RST, SYN, FIN

Pole okna odbiorczego (Window Size, 16 bitów) - informuje, ile bajtów odbiorca może jeszcze przyjąć bez potwierdzenia – mechanizm kontroli przepływu

Pole internetowej sumy kontrolnej (Checksum, 16 bitów) - sprawdza poprawność nagłówka i danych segmentu

Pole wskaźnika „pilności” danych (Urgent Pointer, 16 bitów) - używany razem z flagą URG – wskazuje ostatni bajt danych pilnych

341

Protokół TCP - nagłówek

Pole opcji (zmienna długość) – umożliwia rozszerzenie TCP

Typowe opcje:

- MSS (Maximum Segment Size)
- Window Scale (okno skalujące)
- Znaczniki czasu

Pole danych - właściwa treść przesyłana przez TCP – dane aplikacji (np. strona WWW, e-mail, plik), zmienna długość, segment TCP może być pusty (np. przy SYN lub ACK)

342

Protokół TCP – kontrola błędów i przepływu

TCP zapewnia niezawodność poprzez potwierdzanie każdego segmentu (ACK)

Jeśli pakiet zaginie:

- następuje retransmisja po przekroczeniu limitu czasu
- albo szybciej – przy wykryciu kilku duplikatów ACK (tzw. fast retransmit)

Okno przesuwne (sliding window) umożliwia wysyłanie wielu segmentów bez czekania na każde potwierdzenie – zwiększa to wydajność, ale jednocześnie pozwala regulować tempo transmisji (aby nie „zalać” odbiorcy ani sieci)

343

Protokół TCP – kontrola błędów i przepływu

Różne algorytmy TCP sterują zachowaniem w przypadku strat pakietów i przeciążeń:

Tahoe:

- Pierwszy algorytm kontroli przeciążenia TCP
- Gdy wykryje stratę pakietu (brak ACK lub timeout), resetuje rozmiar okna do 1 MSS (Maximum Segment Size)
- Następnie stosuje fazę slow start – powoli zwiększa wielkość okna, aż osiągnie tzw. Threshold
- Jest bardzo konserwatywny – po błędzie mocno zwalnia, co w nowoczesnych sieciach bywa nieefektywne

344

Protokół TCP – kontrola błędów i przepływu

Różne algorytmy TCP sterują zachowaniem w przypadku strat pakietów i przeciążeń:

Reno:

- Rozwinięcie Tahoe – wprowadza mechanizm:
 - **Fast retransmit** – szybsze ponowne wysłanie segmentu, gdy pojawią się 3 duplikaty ACK (nie trzeba czekać na timeout)
 - **Fast recovery** – zamiast resetować całe okno, Reno zmniejsza je o połowę i od razu próbuje wrócić do wyższego tempa transmisji
- Dzięki temu Reno lepiej radzi sobie w praktyce niż Tahoe, ale wciąż słabo wykorzystuje łącza o dużej przepustowości

345

Protokół TCP – kontrola błędów i przepływu

Różne algorytmy TCP sterują zachowaniem w przypadku strat pakietów i przeciążeń:

Cubic:

- Standardowy algorytm w **Linuksie** i wielu nowoczesnych systemach
- Używa **funkcji sześciennej (cubic)** do obliczania tempa wzrostu okna – dzięki temu szybciej odzyskuje wydajność po błędach
- Stabilny w sieciach o dużej przepustowości i wysokich opóźnieniach (tzw. high-speed networks)
- Lepsze wykorzystanie łącza w porównaniu z Reno czy Tahoe

346

Protokół TCP – przykłady

Usługi WWW

- HTTP (HyperText Transfer Protocol) – port 80
- HTTPS (HTTP Secure) – port 443

Poczta elektroniczna

- SMTP (Simple Mail Transfer Protocol) – port 25 (wysyłka poczty)
- IMAP (Internet Message Access Protocol) – port 143 / 993 (z SSL/TLS)
- POP3 (Post Office Protocol v3) – port 110 / 995 (z SSL/TLS)

347

Protokół TCP – przykłady

Transfer plików

- FTP (File Transfer Protocol) – porty 20 (dane) i 21 (kontrola)
- SFTP (SSH File Transfer Protocol) – działa w oparciu o SSH (port 22)
- FTPS – FTP przez SSL/TLS

Bazy danych i zdalny dostęp

- MySQL – port 3306
- PostgreSQL – port 5432
- MSSQL – port 1433
- Oracle DB – port 1521
- SSH (Secure Shell) – port 22 (tunelowanie, zdalny dostęp)

Protokół TCP – przykłady

Inne

- Telnet – port 23 (starszy, niezabezpieczony dostęp do terminala)
- LDAP (Lightweight Directory Access Protocol) – port 389 / 636 (LDAPS)
- IRC (Internet Relay Chat) – port 6667

349

Protokół UDP

UDP (User Datagram Protocol) nie tworzy sesji między hostami

Każdy wysyłany pakiet (datagram) jest niezależny od poprzednich i kolejnych

UDP jest szybsze i mniej obciążające niż TCP, ale mniej niezawodne

Nagłówek: **8 bajtów** – znacznie mniejszy niż TCP (od 20 bajtów do 60 bajtów)

Brak gwarancji transmisji: Pakiety mogą zostać zgubione, zdublowane lub dostarczone w innej kolejności

UDP nie retransmituje danych, nie potwierdza odbioru i nie zapewnia kontroli przeciążenia - odpowiedzialność za poprawność transmisji spada na aplikację (np. RTP w VoIP sam radzi sobie z jitterem (zmienne opóźnienie) i brakami)

350

Protokół UDP - nagłówek

Numer portu źródłowego	Numer portu docelowego
Pole długości	Pole sumy kontrolnej
Dane aplikacji (komunikat)	

351

Protokół UDP - nagłówek

Numer portu źródłowego (16 bitów) – identyfikuje aplikację wysyłającą dane

Numer portu docelowego (16 bitów) – identyfikuje aplikację odbierającą dane

Pole długości (16 bitów) – rozmiar całego datagramu (nagłówkek + dane), minimalna długość 8 bajtów – brak danych

Pole sumy kontrolnej (16 bitów) – prosta metoda sprawdzania poprawności danych (ale nie retransmisja)

352

Protokół UDP – przykłady

Rozdzielanie adresów i nazwy domen

- DHCP (Dynamic Host Configuration Protocol) – porty 67 (serwer) i 68 (klient)
- DNS (Domain Name System) – port 53 (zwykle UDP, ale TCP też bywa używany np. przy dużych strefach)

Usługi sieciowe

- SNMP (Simple Network Management Protocol) – port 161 (agent), 162 (trap)
- TFTP (Trivial File Transfer Protocol) – port 69
- Syslog – port 514

353

Protokół UDP – przykłady

Multimedia i komunikacja czasu rzeczywistego

- VoIP (Voice over IP) – np. SIP, RTP, RTCP (najczęściej UDP)
- Online gaming – wiele gier korzysta z UDP do szybkiej wymiany danych
- Streaming audio/video – np. IPTV, aplikacje live streaming

Inne przykłady

- NTP (Network Time Protocol) – port 123
- RIP (Routing Information Protocol) – port 520
- mDNS (Multicast DNS) – port 5353 (np. w Apple Bonjour)

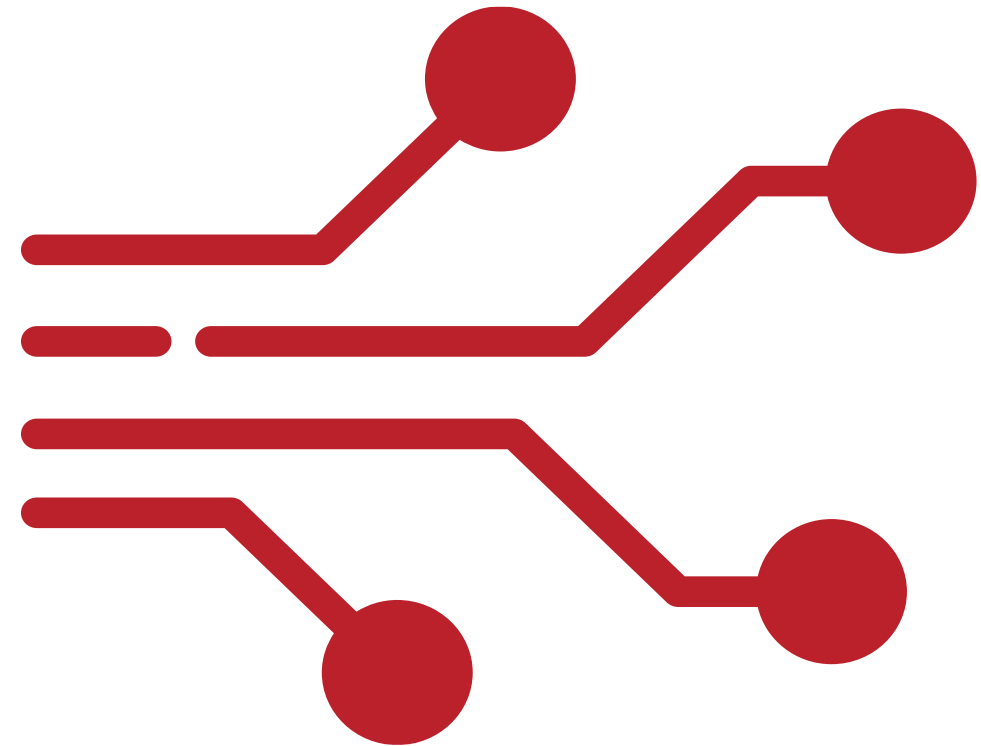
354

Protokół TCP vs UDP

Cecha	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Typ połączenia	Połączeniowy (3-way handshake)	Bezpołączeniowy (brak handshake)
Niezawodność	Gwarantuje dostarczenie i kolejność	Brak gwarancji, brak retransmisji
Nagłówek	20–60 bajtów (rozbudowany)	8 bajtów (prosty)
Kontrola przepływu	Tak (okno przesuwne, algorytmy)	Nie
Opóźnienia	Większe (potwierdzenia, retransmisje)	Małe (brak kontroli, szybki)
Zastosowania	WWW (HTTP/HTTPS), e-mail, FTP, bazy danych	DNS, DHCP, VoIP, streaming, gry

355

Protokoły sieciowe: DHCP (przydzielanie adresów IP), DNS (tłumaczenie nazw na adresy IP)



356

Usługi sieciowe - DHCP

DHCP (Dynamic Host Configuration Protocol) – protokół odpowiedzialny za automatyczne przydzielanie adresów IP i innych parametrów sieciowych eliminując ręczną konfigurację hostów

Działa w warstwie aplikacyjnej – używa UDP (67 - serwer, 68 - klient)

RFC 2131 (1997) – główny dokument definiujący DHCP

Rozszerzenie protokołu BOOTP (Bootstrap Protocol)

Obecnie stosowane także w IPv6 (DHCPv6 – RFC 8415)

357

Usługi sieciowe - DHCP

Automatyczne przydzielanie:

- Adresów IP
- Maski podsieci
- Bramy domyślnej - router przekazujący ruch z sieci lokalnej do innych sieci
- Adresu DNS (Domain Name System) - serwer tłumaczący nazwy domen na adresy IP
- Adresu NTP (Network Time Protocol) - serwer synchronizacji czasu

358

Usługi sieciowe - DHCP

Komponenty:

- *Klient DHCP* – host dołączany do sieci (PC, telefon, drukarka)
- *Serwer DHCP* – zarządza pulą adresów, przydziela adres i parametry
- *Relay agent* – w dużych sieciach przekazuje komunikaty DHCP między podsieciami – UDP broadcast nie przechodzi przez routery

359

Usługi sieciowe - DHCP

Proces DORA (Discover–Offer–Request–Acknowledge):

- *Wykrywanie serwera DHCP* (Discover) – komunikat wykrywania serwera DHCP: klient pyta „kto może mi dać IP?” – rozgłaszanie do wszystkich hostów w sieci – adres rozgłaszania 255.255.255.255, adres źródłowy to 0.0.0.0
- *Oferta DHCP* (Offer) – serwer przesyła klientowi komunikat oferty DHCP (adres IP + konfiguracja) oraz okres dzierżawy adresu IP (czas, przez który adres IP jest prawidłowy) – przekazywany do wszystkich węzłów w sieci
- *Żądanie DHCP* (Request) – klient wybiera ofertę (może być jedna z wielu) i prosi o przydzielenie – komunikat żądania DHCP z powtórzonymi parametrami konfiguracji
- *Potwierdzenie DHCP* (Acknowledge) – serwer odpowiada wysłaniem komunikatu potwierdzenia DHCP – potwierdza żądane parametry

360

Usługi sieciowe - DHCP

DHCP jest w modelu warstwy aplikacji, ale to nie oznacza, że działa dopiero po uruchomieniu aplikacji użytkownika – nie musi działać w pełnym systemie operacyjnym ładowanie systemu operacyjnego:

1. Kernel startuje stos TCP/IP
2. Startuje usługa klienta DHCP na wstępnym etapie uruchamiania systemu i automatycznie wysyła zapytania o konfigurację
3. Proces DORA: Discover → Offer → Request → Acknowledge
4. Serwer DHCP przydziela adres IP, maskę, bramę, DNS, NTP itd.

Sieć działa jeszcze zanim użytkownik się zaloguje – aplikacje mogą korzystać z Internetu 361

Usługi sieciowe – DHCP i NAT

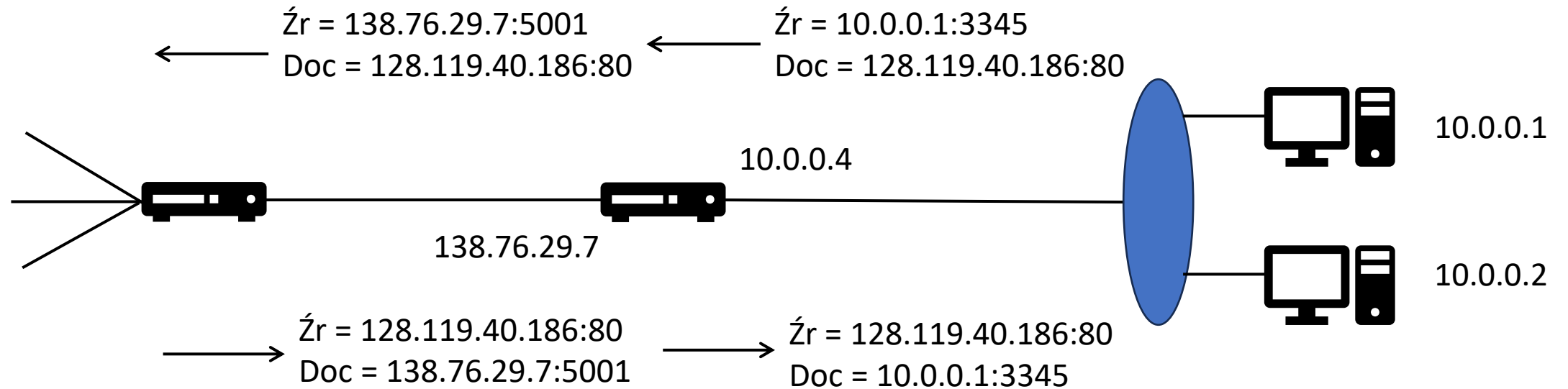


Tabela funkcji NAT	
Sieć rozległa	Sieć lokalna
138.76.29.7:5001	10.0.0.1:3345

362

Usługi sieciowe – DHCP i NAT

Router z funkcją NAT może otrzymywać zewnętrzny (publiczny) adres IP z serwera DHCP dostawcy Internetu (ISP)

Router pełni funkcję serwera DHCP w sieci lokalnej (LAN), przydzielając hostom adresy z puli prywatnych IP

Router prowadzi tablicę translacji NAT, w której zapisane są powiązania:

adres prywatny + port źródłowy $\leftrightarrow$ adres publiczny + port zewnętrzny

Numery portów identyfikują procesy lub usługi w obrębie hosta, a nie same hosty

Router pracuje w warstwie sieciowej (L3) modelu TCP/IP – przetwarza pakiety na poziomie adresów IP i trasowania

363

Usługi sieciowe - DHCP

Nagłówek DHCP: 236 bajtów (część stała) + maksymalnie 576 bajtów (część zmienna):

Pola nagłówka:

- op – typ wiadomości (1 = request, 2 = reply)
- xid – ID transakcji (identyfikator sesji)
- ciaddr / yiaddr / siaddr / giaddr – adresy (klienta, przydzielony, serwera, relay)
- chaddr – adres sprzętowy klienta (MAC)
- sname / file – nazwa serwera, plik startowy (PXE)
- options – parametry konfiguracyjne (IP, maska, gateway, DNS, NTP, lease time)

364

Usługi sieciowe - DNS

DNS (Domain Name System) – protokół odpowiedzialny za tłumaczenie nazwy domenowe na adresy IP

Działa w warstwie aplikacyjnej – używa UDP (53) lub/i TCP(53)

RFC 1034 i RFC 1035 (1987) – główne dokumenty definiujące DNS

- Użytkownicy pamiętają nazwy, nie adresy IP
- Adresy IP mogą się zmieniać
- DNS zapewnia mapowanie nazwa ↔ adres IP
- Umożliwia działanie usług sieciowych (WWW, e-mail, FTP)

365

Usługi sieciowe - DNS

Struktura DNS jest rozproszona i hierarchiczna (struktura drzewa)

- Root servers – początek hierarchii (13 logicznych grup)
- TLD (Top-Level Domain) – np. .com, .pl, .org, .edu
- Autorytatywne serwery (domena drugiego poziomu) – rzeczywiste rekordy domen (np. example.com)
- Subdomena/host (Recursive resolver) – pośredniczy, odpytuje kolejne serwery, przechowuje wyniki w cache – przyspiesza zapytania

www.cyber.edu.pl → pl → edu.pl → cyber.edu.pl

366

Usługi sieciowe - DNS

Proces:

- Klient pyta resolver (nie pyta bezpośrednio wszystkich serwerów), np. www.example.com -
- Zapytania trafiają do lokalnego serwera (sprawdza cache)
- Resolver kontaktuje się z:
 - Root DNS → wskazuje TLD: .com
 - TLD DNS → wskazuje serwer autorytatywny: example.com
 - Serwer autorytatywny → zwraca adres IP
- Wynik wraca do klienta i trafia do cache (czas określony w TTL)

367

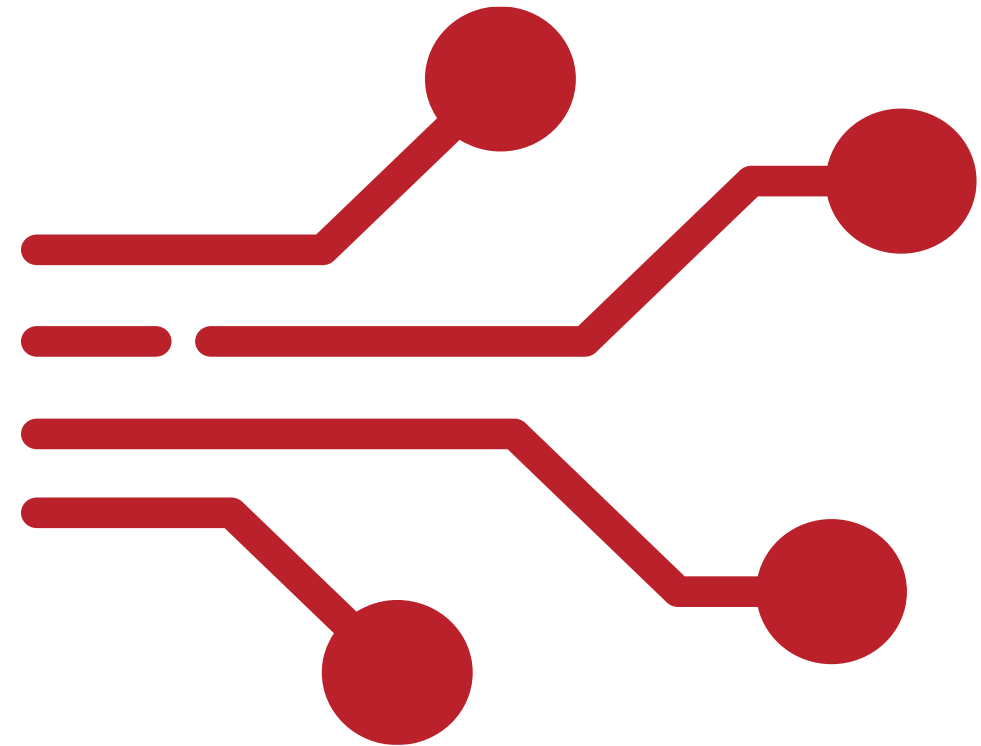
Usługi sieciowe - DNS

Nagłówek DNS (12 bajtów):

- ID – identyfikator zapytania : para zapytanie - odpowiedź
- Flags – bity kontrolne (Q/R, recursion, authoritative)
- QDCOUNT – liczba pytań
- ANCOUNT – liczba odpowiedzi
- NSCOUNT – rekordy Authority
- ARCOUNT – rekordy Additional

368

Protokoły aplikacyjne



369

Protokoły aplikacyjne

Protokoły aplikacyjne to zestaw reguł umożliwiających komunikację między aplikacjami w sieci (warstwa aplikacyjna modelu OSI/ISO lub TCP/IP)

Rola:

- Umożliwiają wymianę danych między klientami a serwerami (np. przeglądarki, aplikacje mobilne, serwery)
- Obsługują specyficzne zadania, takie jak przeglądanie stron, wysyłanie e-maili, przesyłanie plików

370

Protokoły aplikacyjne

Przykłady protokołów aplikacyjnych:

- **HTTP/HTTPS:** Przeglądanie stron WWW, API (np. REST, GraphQL)
- **FTP/SFTP:** Przesyłanie plików (File Transfer Protocol, Secure FTP)
- **SMTP/IMAP/POP3:** Wysyłanie i odbieranie e-maili
- **DNS:** Rozwiązywanie nazw domen na adresy IP
- **WebSocket:** Komunikacja dwukierunkowa w czasie rzeczywistym (np. czaty, gry online)
- **SNMP:** Zarządzanie urządzeniami sieciowymi
- **Telnet/SSH:** Zdalny dostęp do systemów

371

Protokoły aplikacyjne

Cechy wspólne:

- Działają na wyższym poziomie niż protokoły transportowe (TCP, UDP)
- Zorientowane na konkretne zastosowania użytkownika
- Często bezstanowe (np. HTTP) lub stanowe (np. WebSocket)

Znaczenie:

- Podstawa funkcjonowania aplikacji internetowych i usług sieciowych
- HTTPS jako standard dla bezpieczeństwa w Internecie
- Rozwój nowych protokołów (np. QUIC dla HTTP/3) poprawia wydajność i niezawodność

372

Protokół HTTP/HTTPS

HTTP (Hypertext Transfer Protocol) – główny protokół komunikacji w Internecie, umożliwia przesyłanie hipertekstu

Historia:

- Powstał w 1991 r. wraz z WWW, stworzony przez Tima Bernersa-Lee w CERN
- Rozwój: od prostego protokołu do zaawansowanego standardu

Model klient–serwer:

- **Klient:** przeglądarka (Chrome, Firefox), aplikacje mobilne, skrypty.
- **Serwer WWW:** Apache, Nginx, Microsoft IIS, serwery chmurowe

Domyślny port: 80 dla HTTP, 443 dla HTTPS

373

Protokół HTTP/HTTPS

Standaryzacja:

- **HTTP/1.0** – RFC 1945 (1996): jedno żądanie = jedna odpowiedź – każde żądanie wymaga nowego połączenia TCP
- **HTTP/1.1** – RFC 7230–7235 (1999): wprowadzenie persistent connections (keep-alive), pipelining – wiele żądań może być wysłanych bez czekania na odpowiedzi
- **HTTP/2** – RFC 7540 (2015): multiplexing (wiele żądań w jednym połączeniu), kompresja nagłówek, format binarny zamiast tekstowego
- **HTTP/3** – RFC 9114 (2020): oparty na protokole QUIC (UDP), szybsze zestawianie połączeń, mniejsze opóźnienia, odporność na utratę pakietów, wbudowane szyfrowanie

374

Protokół HTTP/HTTPS

Bezstanowy protokół (stateless): każde żądanie (request) jest niezależne, brak pamięci kontekstu

Sesje utrzymywane przez cookies, tokeny lub identyfikatory w URL

Komunikacja: Klient wysyła żądanie (request): metoda, URL, nagłówki, ciało (body)

Serwer odpowiada odpowiedzią (response): kod statusu, nagłówki, treść

Metody HTTP:

GET: pobranie zasobu (np. strona HTML, obraz), POST: przesłanie danych (np. formularze, upload plików), PUT: aktualizacja zasobu, DELETE: usunięcie zasobu, HEAD: pobranie tylko nagłówek (metadane), OPTIONS: sprawdzenie dostępnych metod i możliwości serwera

375

Protokół HTTP/HTTPS

Struktura danych:

Nagłówki: metadane (np. Content-Type: application/json, Authorization)

Ciało (body): dane właściwe (np. HTML, JSON, XML, obrazy)

Sesje i uwierzytelnianie:

Cookies: przechowywanie stanu (np. logowanie)

Tokeny: JWT, OAuth dla API

Identyfikatory w URL (rzadziej, mniej bezpieczne)

376

Protokół HTTP/HTTPS

Cookies :

Małe pliki tekstowe (zazwyczaj 4 KB) przechowywane po stronie klienta (przeglądarka), służą do utrzymania stanu sesji, np. logowania użytkownika, przesyłane w nagłówku HTTP (Cookie: sessionId=abc123 lub Set-Cookie w odpowiedzi)

Atrybuty cookies:

HttpOnly: chroni przed dostępem przez JavaScript (zabezpieczenie przed XSS)

Secure: przesyłanie tylko przez HTTPS

SameSite: ogranicza przesyłanie cookies między domenami

377

Protokół HTTP/HTTPS

Tokeny:

JWT (JSON Web Token): Samowystarczalny token w formacie JSON, składający się z Header, Payload i Signature przesyłany w nagłówku Authorization: Bearer <token>, zawiera informacje o użytkowniku (np. ID, role) i czas ważności

OAuth:

Protokół autoryzacji, umożliwia dostęp do zasobów bez udostępniania hasła, używa tokenów (access token, refresh token) przesyłanych w nagłówku Authorization, popularny w integracji z zewnętrznymi usługami (np. logowanie przez Google, Facebook)

378

Protokół HTTP/HTTPS

HTTPS = HTTP + TLS/SSL (Transport Layer Security/Secure Sockets Layer)

Domyślny port: 443

Główne cechy:

Poufność: szyfrowanie (np. AES) chroni przed podsłuchem

Integralność: zabezpieczenie przed modyfikacją danych w transzycie

Uwierzytelnienie: certyfikaty potwierdzają tożsamość serwera

Certyfikaty cyfrowe: wydawane przez CA (Certificate Authority), np. DigiCert, Sectigo

379

Protokół HTTP/HTTPS

Nagłówki HTTP: metadane przesyłane w żądaniach i odpowiedziach HTTP

Umożliwiają kontrolę nad komunikacją między klientem a serwerem

Przekazują informacje o formacie danych, uwierzytelnianiu, cache'owaniu, itp.

Struktura: klucz-wartość, np. Content-Type: application/json

Występują w żądaniach (Request Headers) i odpowiedziach (Response Headers)

Kategorie nagłówków:

General Headers: ogólne informacje (np. Date, Connection)

Request Headers: dane od klienta (np. Accept, Authorization)

Response Headers: dane od serwera (np. Content-Length, Server)

Entity Headers: opis treści (np. Content-Type, Content-Encoding)

Protokół FTP

FTP (File Transfer Protocol):

Protokół aplikacyjny do przesyłania plików w sieciach TCP/IP (RFC 959)

Działa w modelu klient – serwer

Standardowy port: 21/TCP

- Przesyłanie plików w obie strony (upload / download)
- Przeglądanie katalogów na serwerze
- Tworzenie, usuwanie, zmiana nazw plików i katalogów
- Obsługa uprawnień i kont użytkowników
- Możliwość wznowiania przerwanych transferów

381

Protokół FTP

FTP wykorzystuje dwa połączenia TCP:

1. Control Connection (port 21) – polecenia i odpowiedzi
2. Data Connection (port 20 lub dynamiczny) – przesył danych

Użytkownik loguje się do serwera (login + hasło lub anonimowo)

Komunikacja odbywa się tekstowo (komendy ASCII)

Może również działać w trybie anonimowym (anonymous FTP) – umożliwia pobieranie plików bez logowania

382

Protokół FTP

FTP może działać w dwóch trybach, które różnią się sposobem nawiązywania połączenia danych:

- **Active mode (PORT):**

Serwer łączy się z klientem na losowym porcie (>1023) – problem z zaporą sieciową klienta

- **Passive mode (PASV):**

klient inicjuje oba połączenia (control i data) – bezpieczniejsze, używane w praktyce (np. w FileZilla)

383

Protokół FTP

Client → Server : CONNECT port 21

Server → Client : 220 Service ready

Client → Server : USER student

Server → Client : 331 Password required

Client → Server : PASS ***

Server → Client : 230 Logged in

Client → Server : LIST

Server → Client : Data connection opened

Server → Client : Directory listing

Client → Server : RETR file.txt

Server → Client : File transferred

Client → Server : QUIT

Server → Client : 221 Goodbye

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

384



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Protokół FTP

Dane (łącznie z hasłami) przesyłane jawnie (bez szyfrowania)

Protokół FTP uznaje się za niebezpieczny w Internecie

Rozszerzenia zapewniające bezpieczeństwo:

- FTPS – FTP over SSL/TLS – FTP zabezpieczony protokołem TLS
- SFTP – SSH File Transfer Protocol (inny protokół, korzysta z portu 22) – nie jest połączeniem protokołu FTP z SSL

385

Protokół FTP

Wady i ograniczenia FTP:

- Brak szyfrowania (plaintext)
- Problemy z firewallami (tryb aktywny)
- Użycie wielu portów
- Brak kompresji
- Trudna automatyzacja bez dodatkowych narzędzi

386

Protokół FTP

SFTP (SSH File Transfer Protocol):

- Działa w oparciu o protokół SSH (port 22)
- Cała komunikacja szyfrowana – dane, hasła, polecenia
- Zapewnia funkcje podobne do FTP (upload, download, lista plików)
- Uwierzytelnianie: hasło lub klucze kryptograficzne
- Wspierany przez narzędzia: sftp, WinSCP, FileZilla

FTPS (FTP Secure – TLS/SSL):

- Klasyczny FTP rozszerzony o szyfrowanie SSL/TLS – kompatybilność
- Działa na portach 21 (control) i dynamicznych (data)
- Tryb Implicit FTPS – szyfrowanie wymuszone (z góry)
- Tryb Explicit FTPS – negocjowane przez klienta (STARTTLS)

Protokół FTP

SCP (Secure Copy Protocol)

- Bardzo prosty protokół oparty na SSH (port 22)
- Umożliwia kopiowanie plików między hostami
- Szyfrowanie i uwierzytelnianie takie jak w SSH
- Brak zaawansowanych funkcji zarządzania plikami

```
scp plik.txt user@host:/ścieżka/docelowa
```

HTTP/HTTPS File Transfer

- Wykorzystuje protokoły HTTP / HTTPS - Popularne w usługach chmurowych i REST API
- Transfer plików przez przeglądarkę lub narzędzia CLI (np. curl, wget)
- HTTPS zapewnia szyfrowanie (TLS)
- Porty: 80 (HTTP), 443 (HTTPS)

```
wget https://example.com/file.zip
```

388

Protokół FTP

- rsync (Remote Synchronization)
- Narzędzie do synchronizacji plików i katalogów
- Działa przez SSH – szyfrowanie i autoryzacja
- Kopiuje tylko zmienione fragmenty plików – porównuje sumy kontrolne
- Może działać lokalnie lub zdalnie – kopie lustrzane, synchronizacja serwerów
- Parametry:
 - -a – tryb archiwalny (zachowuje uprawnienia, daty itp.)
 - -v – tryb szczegółowy (verbose)
 - -z – kompresja w locie

```
rsync -avz user@server:/etc/./backup/
```

389

Protokoły pocztowe

Poczta elektroniczna (e-mail) - najważniejsze protokoły:

SMTP (Simple Mail Transfer Protocol) – wysyłanie i przekazywanie wiadomości między serwerami

POP3 (Post Office Protocol v3) – odbiór i przechowywanie poczty z serwera na host

IMAP (Internet Message Access Protocol) – zaawansowany dostęp do poczty

Protokoły pocztowe działają w oparciu o protokół TCP (niezawodność, kontrola błędów)

Działają w modelu klient-serwer

Nadawca (SMTP) → Serwer pocztowy → Odbiorca (POP3/IMAP)

390

Protokoły pocztowe

SMTP protokół SMTP – protokół do wysyłania poczty elektronicznej

Umożliwia przesyłanie wiadomości:

- od klienta pocztowego (MUA – Mail User Agent) do serwera wysyłającego (MSA – Mail Submission Agent)
- oraz między serwerami pocztowymi (MTA – Mail Transfer Agent)

Standard określony w RFC 5321

Dodatkowe rozszerzenia opisują:

- ESMTP (Extended SMTP) – RFC 5321
- AUTH – RFC 4954 (uwierzytelnianie)
- STARTTLS – RFC 3207 (szyfrowanie)

391

Protokoły pocztowe

SMTP model działania: push – nadawca aktywnie przesyła dane do odbiorcy

Porty TCP:

- 25 – standardowa komunikacja serwer–serwer
- 587 – wysyłanie przez klienta (submission)
- 465 – szyfrowany kanał (SMTPS, TLS/SSL)

SMTP obsługuje tylko tekst ASCII – przesyłanie plików binarnych (np. załączników) odbywa się poprzez kodowanie Base64 w standardzie MIME

Przesyłane są dwa typy danych:

1. Nagłówki wiadomości (headers) – np. From, To, Subject, Date
2. Treść wiadomości (body) – tekst i załączniki zakodowane

392

Protokoły pocztowe

SMTP model połączenia

Ustanowienie połączenia (handshake):

- Klient łączy się z serwerem na porcie 25 lub 587
- Serwer odpowiada kodem powitalnym (np. 220 mail.example.com ESMTP)
- Klient identyfikuje się poleceniem HELO lub EHLO

Wymiana komend i danych (przesyłanie wiadomości):

- MAIL FROM:<nadawca@domena.pl> – adres nadawcy
- RCPT TO:<odbiorca@domena.pl> – adres odbiorcy
- DATA – rozpoczęcie przysyłania treści wiadomości
- Po zakończeniu treści – linia z samą kropką (.)

Zamknięcie sesji:

- QUIT – zakończenie połączenia
- Serwer potwierdza kodem 221 i zamyka sesję TCP

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

393



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Protokoły pocztowe

220 mail.server.com ESMTP Ready

C: EHLO pc.student.edu

S: 250-mail.server.com Hello pc.student.edu

C: MAIL FROM:<jan@edu.pl>

S: 250 OK

C: RCPT TO:<anna@uczelnia.pl>

S: 250 Accepted

C: DATA

S: 354 End data with <CR><LF>.<CR><LF>

C: Subject: Test

C: Hello Anna, this is a test email.

C: .

S: 250 Message accepted for delivery

C: QUIT

S: 221 Goodbye

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

394



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Protokoły pocztowe

Wszystkie komendy SMTP są tekstowe i kończą się sekwencją CRLF (Carriage Return + Line Feed)

Serwer odpowiada kodami trzycyfrowymi:

- 2xx – sukces (np. 250 OK)
- 3xx – kontynuacja (np. 354 – oczekiwanie na dane)
- 4xx – błąd tymczasowy
- 5xx – błąd trwały (np. 550 – odbiorca nie istnieje)

SMTP nie potwierdza odebrania wiadomości przez odbiorcę końcowego – tylko dostarczenie do kolejnego serwera

395

Protokoły pocztowe

Ograniczenia oryginalnego SMTP (1982):

- Brak szyfrowania – dane przesyłane jawnym tekstem
- Brak uwierzytelniania – dowolny host mógł wysyłać e-maile w cudzym imieniu
- Brak ochrony przed spamem i spoofingiem

396

Protokoły pocztowe

Rozszerzenia ESMTP (Extended SMTP)

- **STARTTLS** – umożliwia szyfrowanie sesji SMTP przy użyciu TLS (Transport Layer Security)
 - Po komendzie STARTTLS strony przechodzą w tryb szyfrowany
- **AUTH LOGIN / PLAIN / CRAM-MD5** – różne metody logowania użytkowników
- **SIZE** – informuje o maksymalnym dopuszczalnym rozmiarze wiadomości
- **8BITMIME** – pozwala przesyłać znaki spoza ASCII (np. polskie znaki)
- **DSN (Delivery Status Notification)** – raporty doręczenia

Protokoły pocztowe

Mechanizmy bezpieczeństwa domenowego

SPF (Sender Policy Framework) – określa, które serwery mogą wysyłać pocztę w imieniu danej domeny

DKIM (DomainKeys Identified Mail) – podpis cyfrowy w nagłówku wiadomości (weryfikacja autentyczności)

DMARC (Domain-based Message Authentication, Reporting and Conformance) – łączy SPF i DKIM – reguły określające co zrobić z wiadomościami, które nie przejdą weryfikacji

398

Protokoły pocztowe

POP3 (Post Office Protocol version 3) – protokół służący do pobierania wiadomości e-mail z serwera pocztowego na komputer użytkownika

Zdefiniowany w RFC 1939 (1996)

Używa protokołu TCP:

- Port 110 – standardowy POP3
- 995 – szyfrowany POP3S (TLS/SSL)

Działa w modelu store-and-forward:

Wiadomości są przechowywane na serwerze →

Klient (np. Outlook, Thunderbird) łączy się, pobiera pocztę →

Po pobraniu – opcjonalnie usuwa wiadomości z serwera

Sesja POP3 jest prosta – komunikacja w postaci tekstowej ASCII

Protokoły pocztowe

Fazy działania POP3:

1. Autoryzacja (logowanie):

- USER – nazwa użytkownika
- PASS – hasło

2. Transakcja (operacje na wiadomościach):

- STAT – liczba wiadomości i łączny rozmiar skrzynki
- LIST – lista wiadomości z ich rozmiarami
- RETR <nr> – pobierz wiadomość
- DELE <nr> – oznacz wiadomość do usunięcia
- NOOP – brak operacji (utrzymanie sesji)

3. Aktualizacja (zakończenie sesji):

- QUIT – kończy połączenie i usuwa wiadomości oznaczone przez DELE

400

Protokoły pocztowe

```
S: +OK POP3 server ready
C: USER jan
S: +OK
C: PASS haslo123
S: +OK User successfully logged in
C: STAT
S: +OK 3 2450
C: LIST
S: +OK
1 850
2 760
3 840
C: RETR 1
S: [treść wiadomości...]
C: DELE 1
S: +OK marked for deletion
C: QUIT
S: +OK Goodbye
```

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"Goodbye z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

401



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

401

Dofinansowane przez
Unię Europejską



Protokoły pocztowe

Zalety:

- Prosty i mało zasobożerny
- Możliwość pracy **offline** (wiadomości lokalnie)
- Szybki przy małych skrzynkach
- Nie wymaga stałego połączenia z serwerem

Wady:

- Brak synchronizacji między urządzeniami
- Domyślnie usuwa wiadomości po pobraniu
- Brak folderów i etykiet
- Nie obsługuje wyszukiwania po stronie serwera

402

Protokoły pocztowe

IMAP (Internet Message Access Protocol) – protokół do zdalnego dostępu do wiadomości e-mail przechowywanych na serwerze

Standard: RFC 3501

Porty TCP:

- 143 – IMAP (nieszyfrowany)
- 993 – IMAPS (TLS/SSL)

Działa w modelu online – wiadomości pozostają na serwerze

Klient pobiera jedynie nagłówki lub wybrane fragmenty wiadomości

Umożliwia zarządzanie folderami i synchronizację wielu urządzeń

403

Protokoły pocztowe

Podstawowe komendy IMAP:

LOGIN	– Logowanie użytkownika
SELECT <folder>	– Wybór folderu (np. INBOX)
FETCH <nr>	– Pobranie wiadomości lub fragmentu
STORE	– Ustawienie flag (np. \Seen, \Deleted)
SEARCH	– Wyszukiwanie wiadomości wg kryteriów
EXPUNGE	– Usunięcie wiadomości oznaczonych do kasacji
LOGOUT	– Zakończenie sesji

404

Protokoły pocztowe

```
S: * OK IMAP4rev1 Service Ready
C: A001 LOGIN student haslo123
S: A001 OK LOGIN completed
C: A002 SELECT INBOX
S: * 3 EXISTS
S: A002 OK [READ-WRITE] SELECT completed
C: A003 FETCH 1 BODY[HEADER.FIELDS (SUBJECT FROM)]
S: * 1 FETCH (BODY[HEADER.FIELDS (SUBJECT FROM)] {45}
From: admin@uczelnia.pl
Subject: Egzamin sieci
)
S: A003 OK FETCH completed
C: A004 LOGOUT
S: * BYE Logging out
S: A004 OK LOGOUT completed
```

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

405



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Protokoły pocztowe

Zalety:

- Pełna synchronizacja poczty między urządzeniami
- Wiadomości pozostają na serwerze – dostęp z dowolnego miejsca
- Obsługa folderów, etykiet i flag wiadomości
- Możliwość pracy w trybie online lub częściowym offline
- Wsparcie dla powiadomień w czasie rzeczywistym (IDLE)

Wady:

- Większe obciążenie serwera i większe zużycie pasma
- Konieczność stałego połączenia z Internetem
- Potencjalne kwestie prywatności – dane przechowywane w chmurze
- Bardziej złożona implementacja niż POP3

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU Społecznego 2011-2020 (PFR)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00



Fundusze Europejskie
dla Rozwoju Społecznego



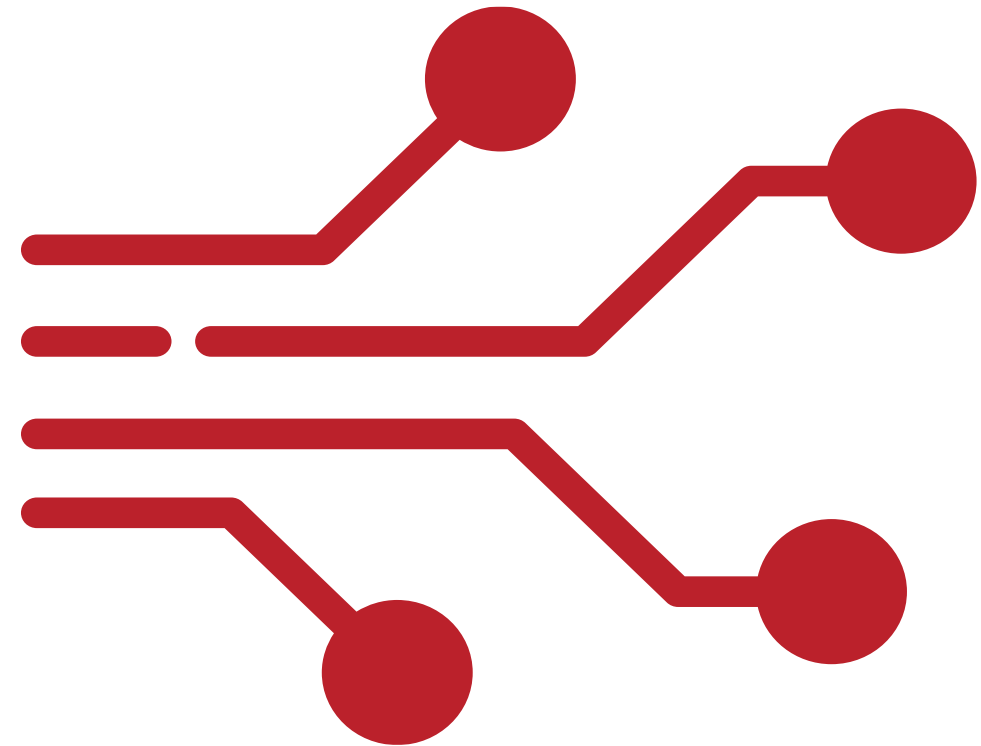
Rzeczpospolita
Polska

406

Dofinansowane przez
Unię Europejską



Protokół ARP i ICMP: mechanizmy działania i zastosowania



407

Protokół ARP

ARP (Address Resolution Protocol) – protokół warstwy łącza danych (adresy MAC) oraz warstwy sieciowej (adresy IP), który umożliwia mapowanie adresów logicznych IP na adresy fizyczne MAC

Stosowany w sieciach IPv4 (dla IPv6 odpowiednikiem jest NDP – Neighbor Discovery Protocol)

Używany lokalnie w ramach jednej sieci LAN – nie jest przekazywany przez routery

Określony w standardzie RFC 826 (1982)

Działa automatycznie i dynamicznie – bez udziału użytkownika (PnP – Plug and Play)

408

Protokół ARP

Adres IP (np. 192.168.1.10) – logiczny, używany przez warstwę sieci

Adres MAC (np. 00:1B:44:11:3A:B7) – fizyczny, używany przez warstwę łącza danych

Aby wysłać ramkę Ethernet, komputer musi znać MAC adres odbiorcy

ARP tłumaczy adresy IP → MAC

Proces:

- Komputer sprawdza, czy zna adres MAC dla danego IP (ARP Cache)
- Jeśli nie – wysyła zapytanie ARP Request w trybie *broadcast* (do wszystkich urządzeń w sieci)
- Urządzenie z pasującym adresem IP odpowiada ARP Reply w trybie *unicast* (do konkretnego odbiorcy)
- Adres MAC zostaje zapisany w **tabeli ARP** (cache) na pewien czas (np. 60–120 s)

409

Protokół ARP

Nagłówek ARP (28 bajtów) – pola protokołu:

Pole	Rozmiar	Opis
Hardware Type (HTYPE)	2 bajty	Typ warstwy łącza – dla Ethernetu: 1
Protocol Type (PTYPE)	2 bajty	Typ protokołu warstwy sieci – dla IPv4: 0x0800
Hardware Size (HLEN)	1 bajt	Długość adresu MAC (dla Ethernetu: 6)
Protocol Size (PLEN)	1 bajt	Długość adresu IP (dla IPv4: 4)
Opcode	2 bajty	Typ komunikatu: 1 – Request, 2 – Reply
Sender MAC Address	6 bajtów	Adres MAC nadawcy
Sender IP Address	4 bajty	Adres IP nadawcy
Target MAC Address	6 bajtów	Adres MAC odbiorcy (zerowy w zapytaniu)
Target IP Address	4 bajty	Adres IP odbiorcy

410

Protokół ARP – krok po kroku

Komputer A (192.168.1.10) chce wysłać pakiet IP do Komputera B (192.168.1.20)

1. Sprawdzanie własnej tablicy ARP:

- System sprawdza, czy zna adres MAC dla IP 192.168.1.20
- Jeśli nie – przechodzi do następnego kroku

2. Wysłanie zapytania ARP (ARP Request):

- Ramka broadcast do adresu MAC FF:FF:FF:FF:FF:FF
- Zawiera: „Kto ma 192.168.1.20? Odpowiedz 192.168.1.10”

3. Odpowiedź ARP (ARP Reply):

- Host B odpowiada unicastem: „192.168.1.20 ma MAC 00:1B:44:11:3A:B7”

4. Aktualizacja tablicy ARP:

- Host A zapisuje parę IP–MAC w swojej tablicy ARP
- Kolejne pakiety mogą być wysyłane bez dodatkowych zapytań

Projekt współfinansowany ze środków Unii Europejskiej w ramach:
FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS)
"POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

411

Dofinansowane przez
Unię Europejską



Protokół ARP – krok po kroku

Tablica ARP (ARP Cache) – lokalna pamięć odwzorowań IP ↔ MAC

Przechowuje dynamiczne wpisy (uzyskane z zapytań ARP) oraz statyczne (wprowadzone ręcznie)

Przykład (Windows/Linux):

Internet Address	Physical Address	Type
192.168.1.1	00-14-22-01-23-45	dynamic
192.168.1.20	00-1b-44-11-3a-b7	dynamic

Rodzaje wpisów:

Dynamiczne – dodawane automatycznie, wygasają po czasie

Statyczne – dodawane przez administratora, trwałe do restartu systemu

Protokół ARP – krok po kroku

Tablica ARP (ARP Cache) – lokalna pamięć odwzorowań IP ↔ MAC

Przechowuje dynamiczne wpisy (uzyskane z zapytań ARP) oraz statyczne (wprowadzone ręcznie)

Przykład (Windows/Linux):

Internet Address	Physical Address	Type
192.168.1.1	00-14-22-01-23-45	dynamic
192.168.1.20	00-1b-44-11-3a-b7	dynamic

Rodzaje wpisów:

Dynamiczne – dodawane automatycznie, wygasają po czasie

Statyczne – dodawane przez administratora, trwałe do restartu systemu

413

Protokół ARP – gdzie znajduje się tablica ARP

W hoście końcowym (liczba tablic = 1) – czas życia 1-5 min:

- Każdy host IP utrzymuje własną tablicę ARP (ARP Cache)
- Służy ona do mapowania adresów IP sąsiadów w sieci lokalnej (LAN) na ich adresy MAC
- Host używa tej tablicy, gdy chce wysłać pakiet IP do innego urządzenia w tej samej sieci

W routerze (liczba tablic = liczba interfejsów) – czas życia 4-20 min:

- Router ma własną tablicę ARP dla każdego interfejsu sieciowego (np. LAN, DMZ, WAN)
- Router działa na warstwie 3 (IP), ale do wysyłania pakietów potrzebuje znać adresy warstwy 2 (MAC) swoich sąsiadów
- Dla każdego interfejsu utrzymuje oddzielny ARP Cache

414

Protokół ICMP

ICMP (Internet Control Message Protocol)

– protokół sieciowy używany do wymiany komunikatów kontrolnych i diagnostycznych w sieciach IP

Nie służy do przesyłania danych użytkowych, lecz do informowania o błędach i monitorowania działania sieci

- Standard: RFC 792 (IPv4), RFC 4443 (IPv6)
- ICMP jest integralną częścią warstwy sieciowej (IP) w modelu TCP/IP
- Używa protokół IP (numer 1) w polu *Protocol* nagłówka IP
- Nie korzysta z portów (w odróżnieniu od TCP/UDP)

415

Protokół ICMP

ICMP działa razem z IP, nie zamiast niego – nie ma własnego portu źródłowego ani docelowego

Jest enkapsulowany wewnątrz pakietu IP tak jak TCP czy UDP – każdy komunikat ICMP jest traktowany jako specjalny pakiet IP o protokole nr 1

Używany przez urządzenia warstwy 3 (routery, hosty) do komunikacji o stanie sieci – automatyczna interpretacja komunikatów ICMP

W odpowiedziach ICMP (np. błędach) często zwracany jest fragment oryginalnego pakietu IP, który spowodował problem – nadawca wie, którego pakietu dotyczył komunikat

416

Protokół ICMP

Nagłówek ICMP (8 bajtów) – pola protokołu:

Pole	Rozmiar	Opis
Type	1 bajt	Określa rodzaj komunikatu (np. 0 – Echo Reply, 8 – Echo Request)
Code	2 bajt	Dodatkowe informacje o typie błędu
Checksum	2 bajty	Suma kontrolna ICMP
Pozostałe	4 bajy	Zależne od typu komunikatu (np. identyfikator, numer sekwencji, dane IP)

417

Protokół ICMP – najważniejsze komunikaty (IPv4)

Typ	Kod	Nazwa komunikatu	Znaczenie
0	0	Echo Reply	Odpowiedź na ping
3	0-15	Destination Unreachable	Host, sieć lub port nieosiągalny
4	0	Source Quench (<i>przestarzały</i>)	Redukcja prędkości wysyłania
5	0-3	Redirect	Informacja o lepszej trasie
8	0	Echo Request	Żądanie ping
11	0-1	Time Exceeded	TTL przekroczony – używany w traceroute
12	0-2	Parameter Problem	Błąd w nagłówku IP

418

Protokół ICMP – przykład (ping)

Polecenie:

```
ping 192.168.1.1
```

Sekwencja zdarzeń:

- Host wysyła ICMP Echo Request (typ 8) do adresu 192.168.1.1
- Router lub host docelowy odpowiada ICMP Echo Reply (typ 0)
- Na podstawie czasu odpowiedzi (RTT – Round Trip Time) mierzona jest dostępność i opóźnienie

Wynik:

```
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.12 ms
```

```
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.10 ms
```

419

Protokół ICMP – ICMPv6

ICMPv6 – odpowiednik ICMP dla IPv6

Standard: RFC 4443

Pełni wszystkie funkcje ICMPv4, ale zawiera dodatkowe mechanizmy:

- Neighbor Discovery Protocol (NDP) – zastępuje ARP (odkrywanie sąsiadów)
- Router Solicitation / Advertisement – automatyczna konfiguracja adresów IPv6
- Multicast Listener Discovery (MLD) – zarządzanie multicastem

W odróżnieniu od ICMPv4, komunikaty ICMPv6 są zabezpieczane protokołem IPsec

420

Dziękuję za uwagę

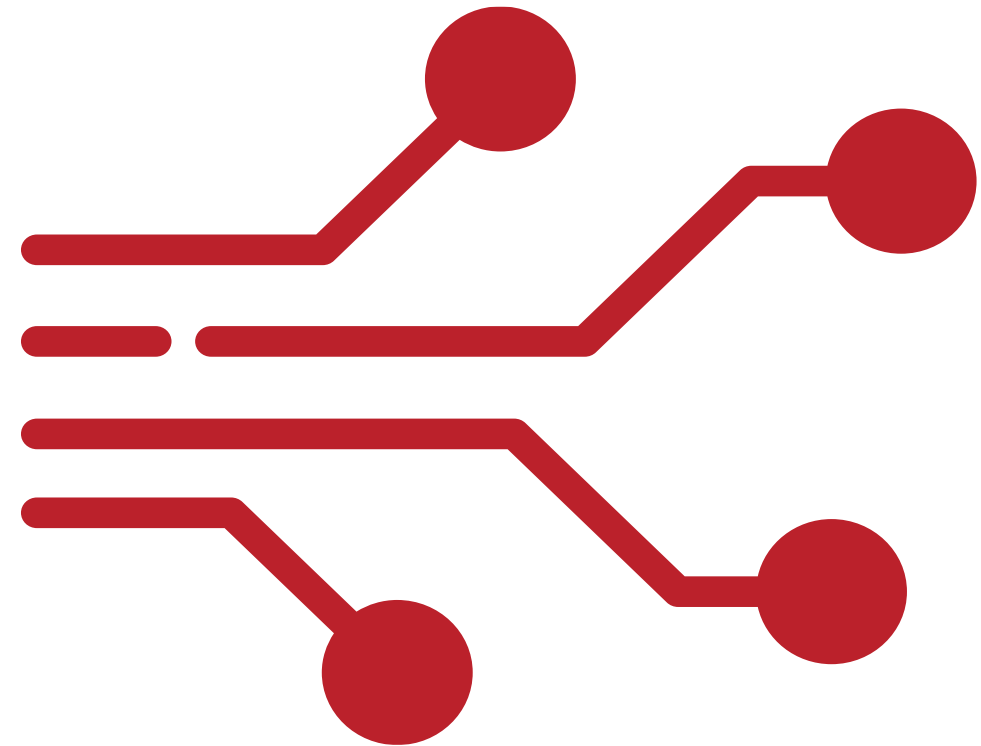
Treści programowe:

- Komunikacja w sieciach lokalnych i bezprzewodowych
- Media transmisyjne w sieciach LAN: przewodowe (Ethernet) i światłowodowe
- Podstawy działania Ethernetu
- Standardy Wi-Fi: 802.11, działanie i konfiguracja
- Zabezpieczenia sieci bezprzewodowych: szyfrowanie



422

Komunikacja w sieciach lokalnych i bezprzewodowych



423

Komunikacja w sieciach LAN

Technologie komunikacji LAN: Token Ring, FDDI, ATM, Wi-Fi, Ethernet

Token Ring – sieć z żetonem

- Token Ring (IEEE 802.5) – technologia IBM z lat 80
- Urządzenia połączone logicznie w pierścień
- W sieci krąży token (żeton) – prawo do nadawania
- Brak kolizji, deterministyczny czas dostępu
- Prędkości: 4 Mb/s, 16 Mb/s (rzadko 100 Mb/s)
- Topologia fizyczna: gwiazda z koncentratorom MAU (Multistation Access Unit)

424

Komunikacja w sieciach LAN

Technologie komunikacji LAN: Token Ring, FDDI, ATM, Wi-Fi, Ethernet

FDDI – światłowodowy pierścień

- FDDI (Fiber Distributed Data Interface) – sieć światłowodowa LAN/MAN
- Standard ANSI X3T9.5, lata 80
- Prędkość: 100 Mb/s
- Medium: światłowód (rzadziej miedź – CDDI)
- Struktura: podwójny pierścień – pierścień główny i zapasowy
- Mechanizm transmisji: token passing
- Zasięg: do 200 km, do 500 urządzeń

425

Komunikacja w sieciach LAN

Technologie komunikacji LAN: Token Ring, FDDI, ATM, Wi-Fi, Ethernet

ATM – Asynchronous Transfer Mode

- Technologia łącząca cechy LAN i WAN
- Transmisja danych, głosu i wideo w czasie rzeczywistym
- Oparta na komutacji połączeń wirtualnych (VC).
- Dane dzielone na komórki o stałej długości 53 bajty
- Prędkości: od 25 Mb/s do 622 Mb/s (i więcej)
- Zapewnia QoS (Quality of Service) – kontrolę jakości transmisji

426

Komunikacja w sieciach LAN

Technologie komunikacji LAN: Token Ring, FDDI, ATM, Wi-Fi, Ethernet

Wi-Fi – bezprzewodowy LAN

- Wi-Fi (IEEE 802.11) to bezprzewodowa technologia LAN
- Umożliwia łączność radiową między urządzeniami bez kabli
- Standardy: 802.11a/b/g/n/ac/ax (Wi-Fi 6 i 6E)
- Prędkości: od 11 Mb/s (802.11b) do ponad 9 Gb/s (Wi-Fi 6E)
- Pasma: 2,4 GHz, 5 GHz, 6 GHz
- Urządzenia: Access Point (AP), klient Wi-Fi, SSID (nazwa sieci), szyfrowanie WPA2/WPA3

427

Komunikacja w sieciach LAN

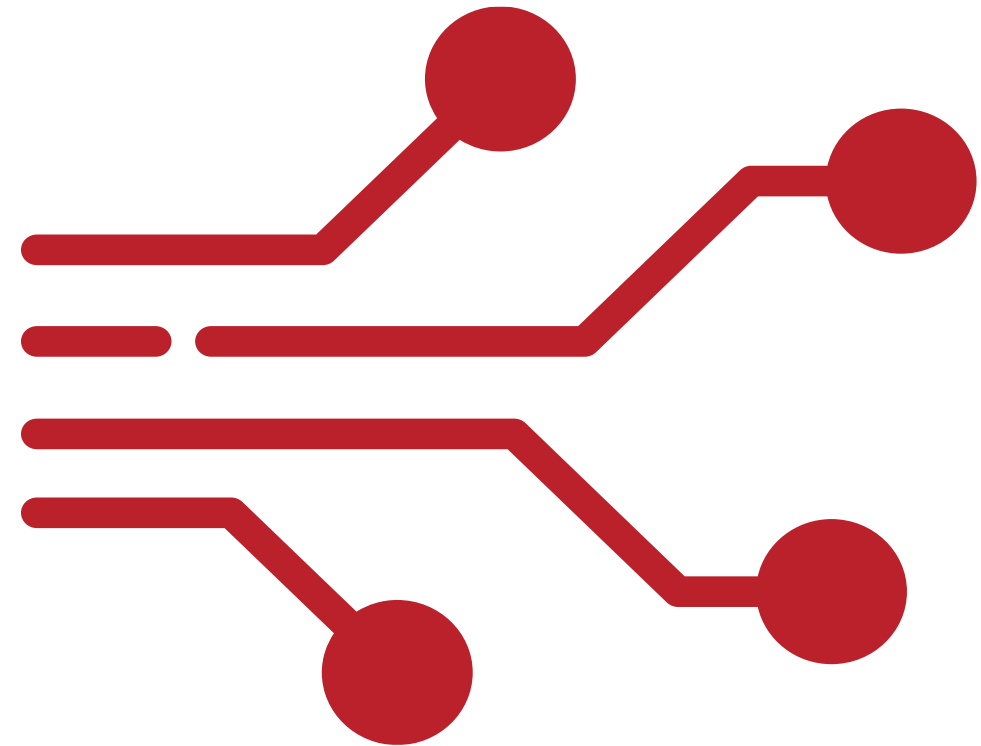
Technologie komunikacji LAN: Token Ring, FDDI, ATM, Wi-Fi, Ethernet

Ethernet – podstawowa technologia LAN

- Ethernet (IEEE 802.3) to dominujący standard przewodowej komunikacji LAN
- Opracowany w latach 70. przez firmę Xerox, następnie rozwijany przez IEEE
- Wykorzystuje ramki Ethernet do przesyłania danych między urządzeniami
- Każde urządzenie ma unikalny adres MAC (48-bitowy identyfikator)
- Obecne wersje działają z prędkościami od 10 Mb/s do 400 Gb/s
- Topologia fizyczna: gwiazda (z przełącznikiem), logiczna: punkt–punkt

428

Media transmisyjne w sieciach LAN: przewodowe (Ethernet) i światłowodowe



429

Ethernet

Ethernet – rodzina technologii sieciowych służących do transmisji ramek danych w sieciach lokalnych (LAN), działa w warstwie łącza danych modelu OSI oraz częściowo w warstwie fizycznej

Główne zadanie – **ramkowanie, adresowanie i dostarczanie danych między urządzeniami** w obrębie tej samej sieci lokalnej

Architektura otwarta i standaryzowana – rozwijana przez IEEE w ramach 802.3 – interoperacyjność sprzętu i oprogramowania wielu producentów

Ekonomiczna efektywność – prosty model transmisji i tania infrastruktura (skrętka, przełączniki, karty NIC)

Ewolucyjny rozwój – kolejne generacje (Fast, Gigabit, 10/40/100G Ethernet) zachowały zgodność wsteczną i ten sam format ramki

Integracja z TCP/IP – naturalne dopasowanie do warstwy sieciowej Internetu uczyniło Ethernet podstawą komunikacji w systemach IP

Elastyczność mediów transmisyjnych – wsparcie dla skrętki, światłowodu i łączy bezprzewodowych (Ethernet over WLAN)

Bezpieczeństwo i zarządzanie – rozszerzenia standardu (802.1X, VLAN, QoS, PoE) pozwoliły na budowę sieci o kontrolowanym dostępie i wysokiej niezawodności

430

Ethernet - początki

Lata 70: Ethernet opracowany w Xerox PARC (1973–1976) przez Roberta Metcalfe'a

Pierwotny prototyp: prędkość 2,94 Mb/s

medium: kabel koncentryczny, topologia magistrali

Zasada działania: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – urządzenia dzielą wspólne medium i wykrywają kolizje

W 1980 r. opracowano pierwszą specyfikację DIX Ethernet (Digital, Intel, Xerox) → później standard IEEE 802.3 (1983)

Lata 80–90: standaryzacja i popularyzacja

Ethernet staje się otwartym standardem – rozwijanym przez IEEE

Wersje 10BASE-2 i 10BASE-T: tanie, oparte na skrętce, topologia gwiazdy

W 1995 – pojawia się Fast Ethernet (100BASE-TX) – 10× szybszy, ale w pełni zgodny z wcześniejszymi wersjami

431

Ethernet - początki

Lata 2000–2010: Gigabit i Ethernet przełączany

Gigabit Ethernet (1000BASE-T) – standard 1999, masowo wdrażany od 2000

Switche zastępują huby → sieci bez kolizji, segmentacja ruchu, lepsze bezpieczeństwo

Pojawiają się technologie: VLAN (802.1Q), PoE (802.3af), link aggregation, QoS

Ethernet staje się podstawą sieci kampusowych, korporacyjnych i centrów danych

Lata 2010–2020: Ethernet światłowodowy i mobilny 10GBASE-T, 40GBASE, 100GBASE – wprowadzenie światłowodu do sieci LAN i MAN

Wsparcie dla wirtualizacji i centrów danych (DC Ethernet, VXLAN, EVPN)

Rozwój Industrial Ethernet – zastosowania w automatyce, SCADA, IoT

Pojawienie się Ethernet over Wireless – integracja z Wi-Fi i sieciami 5G

432

Ethernet - początki

Aktualne standardy: 400GBASE, 800GBASE – sieci operatorów, data center, HPC

Ethernet rozszerzony o mechanizmy bezpieczeństwa:

802.1X – uwierzytelnianie portów

802.1AE (MACsec) – szyfrowanie ramek w warstwie 2

VLAN, ACL, segmentacja mikrosieciowa

Ethernet obsługuje wiele rodzajów mediów transmisyjnych, które różnią się budową fizyczną, zasięgiem, odpornością na zakłócenia i zastosowaniem

Wybór medium wpływa bezpośrednio na wydajność, bezpieczeństwo i niezawodność sieci

Ethernet to rodzina standardów sieci lokalnych (LAN), które łączą:

media transmisyjne fizyczne – przewody, światłowody, złącza

protokoły dostępu do medium (MAC) – reguły określające podział kanału transmisyjnego

433

Ethernet – media transmisyjne

Skrętka miedziana (Twisted Pair): najpowszechniejsze medium transmisyjne w sieciach Ethernet

Transmisja odbywa się przy użyciu par przewodów miedzianych skręconych ze sobą w celu redukcji zakłóceń elektromagnetycznych (EMI) i przesłuchów (crosstalk)

Każda para przewodów przenosi sygnały różnicowe – informacja jest reprezentowana przez różnicę potencjałów między przewodami, a nie względem masy

Budowa i kategorie przewodów (kategorie Cat):

Kategoria	Maks. prędkość	Pasmo	Typowe zastosowanie
Cat 5e	1 Gb/s	100 MHz	Sieci biurowe, domowe
Cat 6	1–10 Gb/s	250 MHz	Nowoczesne sieci LAN
Cat 6a	10 Gb/s	500 MHz	Infrastruktura korporacyjna
Cat 7/7a	10–40 Gb/s	600–1000 MHz	Centra danych
Cat 8	do 40 Gb/s	2000 MHz	Sieci serwerowe, HPC

Ethernet – media transmisyjne

Standard Ethernet ogranicza długość przewodu do 100 metrów

W zależności od potrzeb i środowiska elektromagnetycznego stosuje się różne rodzaje ekranowania:

Oznaczenie	Opis	Zastosowanie
UTP (Unshielded Twisted Pair)	brak ekranowania	typowe biura, niskie zakłócenia
FTP (Foiled Twisted Pair)	ekran foliowy wokół wszystkich par	sieci z umiarkowanymi zakłóceniami
STP (Shielded Twisted Pair)	ekran wokół każdej pary	laboratoria, serwerownie
S/FTP	ekran ogólny + folie dla każdej pary	infrastruktura krytyczna, przemysł

Złącza wykorzystywane w skrętce to RJ-45 (8P8C), a w nowszych implementacjach – także GG45 lub TERA (dla Cat 7/8)

435

Ethernet – media transmisyjne

Nazwy standardów Ethernetu (np. 100BASE-TX) mają ściśle określoną strukturę i niosą informacje o prędkości, rodzaju transmisji i medium

Każda nazwa Ethernetu ma trzy części: [PRĘDKOŚĆ][BASE/BROAD][SUFIKS MEDIUM]

Składnik

Znaczenie

Liczba (np. 10, 100, 1000, 10G)

Nominalna przepustowość w megabitach lub gigabitach na sekundę

BASE / BROAD

Rodzaj sygnału:

BASE (baseband) – transmisja cyfrowa, pojedynczy kanał danych (Ethernet)

BROAD (broadband) – modulacja analogowa, wiele kanałów (np. Ethernet po kablu TV – rzadko używany)

Sufiks (np. T, TX, FX, LX, SR, LR)

Typ medium transmisyjnego i wariant fizyczny

436

Ethernet – media transmisyjne

Sufiks	Rozwinięcie	Medium / technologia	Przykładowe zastosowanie
T	Twisted Pair	Skrętka miedziana (UTP/STP)	10BASE-T
TX	Twisted Pair – Transmit/Receive	Skrętka (2 pary, Cat 5)	100BASE-TX
FX	Fiber Optic – Short-range Multimode	Światłowód MMF (850 nm)	100BASE-FX
SX / SR	Short / Short-Range	Światłowód MMF (850 nm)	1000BASE-SX
LX / LR	Long / Long-Range	Światłowód SMF (1310 nm lub 1550 nm)	1000BASE-LX
EX / ER	Extended / Extended-Reach	Światłowód SMF, większy zasięg (kilka km)	1000BASE-EX
CX	Copper – Shielded Twinax	Krótkie łącza miedziane ekranowane (DAC)	10GBASE-CX4
CR	Copper – Direct-Attach Twinax	Kable DAC w centrach danych (≤ 7 m)	10GBASE-CR
KX / KR	Backplane Copper / Backplane Reach	Połączenia wewnętrzne (np. switchy)	10GBASE-KR
BZ /-T1	Base-T1 Automotive / Industrial	Jednoparowy Ethernet (automotive, IoT)	1000BASE-T1

437

Ethernet – media transmisyjne

100BASE-TX

- 100 → prędkość 100 Mb/s
- BASE → transmisja cyfrowa (baseband)
- TX → skrętka miedziana (Cat 5), oddzielne linie TX/RX

Standard Fast Ethernet 100 Mb/s na skrętce UTP/STP

1000BASE-T

- 1000 → 1 Gb/s
- BASE → baseband
- T → skrętka miedziana (Cat 5e)

Gigabit Ethernet na czterech parach skrętki

438

Ethernet – media transmisyjne

10BASE-T (klasyczny Ethernet)

Rok standaryzacji: 1990 (IEEE 802.3i)

Prędkość: 10 Mb/s

Medium: skrętka UTP, kategoria 3

Liczba par: 2 (1 para nadawcza, 1 odbiorcza)

Długość segmentu: 100 m

Kodowanie: Manchester

Topologia: gwiazda (z hubem lub przełącznikiem w środku)

Znaczenie: zastąpił kable koncentryczne (10BASE-2, 10BASE-5), uprościł instalację sieci

Aspekt bezpieczeństwa: sieci 10BASE-T korzystały z hubów, które rozgłaszały ruch do wszystkich portów — umożliwiało to podsłuch ramek (sniffing)

switche eliminują to ryzyko — kierują ruch wyłącznie do właściwego portu

439

Ethernet – media transmisyjne

100BASE-TX (Fast Ethernet)

Rok standaryzacji: 1995 (IEEE 802.3u)

Prędkość: 100 Mb/s

Medium: skrętka UTP/STP, kategoria 5

Liczba par: 2

Długość segmentu: 100 m

Topologia: gwiazda (z hubem lub przełącznikiem w środku)

Kodowanie: 4B/5B + MLT-3 (Multi-Level Transmission – 3 poziomy sygnału)

Znaczenie: 10 –krotne zwiększenie przepustowości – istniejące okablowanie, autonegocjacja prędkości, pełny duplex, eliminacja kolizji

Aspekt bezpieczeństwa: większa stabilność połączeń, redukcja błędów transmisji – mniejsze szanse na fault injection

440

Ethernet – media transmisyjne

1000BASE-T (Gigabit Ethernet)

Rok standaryzacji: 1999 (IEEE 802.3ab)

Prędkość: 1 Gb/s

Medium: skrętka kategoria 5e, 6

Liczba par: 4 (transmisja równoczesna w obu kierunkach – full duplex)

Długość segmentu: 100 m

Kodowanie: PAM-5 (Pulse Amplitude Modulation – 5 poziomów)

Topologia: gwiazda (z hubem lub przełącznikiem w środku)

Znaczenie: wykorzystuje wszystkie 4 pary przewodów jednocześnie – efektywność

Aspekt bezpieczeństwa: zwiększona przepustowość – wdrażanie systemów monitoringu ruchu w czasie rzeczywistym (IDS/IPS) oraz szyfrowanie warstwy 2 (MACsec) bez utraty wydajności – wymaga wysokiej jakości okablowania (błędy transmisji mogą być wykorzystane do ataków na integralność danych) ⁴⁴¹

Ethernet – media transmisyjne

10GBASE-T (10 Gigabit Ethernet)

Rok standaryzacji: 2006 (IEEE 802.3an)

Prędkość: 10 Gb/s

Medium: skrętka ekranowana (Cat 6a, 7, 8)

Liczba par: 4 (transmisja równoczesna w obu kierunkach – full duplex)

Długość segmentu: 100 m

Kodowanie: PAM-16 (16 poziomów sygnału)

Topologia: gwiazda (z hubem lub przełącznikiem w środku)

Znaczenie: wdrożenie szybkiego Ethernetu w warstwie dostępowej bez konieczności wymiany całej infrastruktury, kodowanie PAM-16 i korekcja błędów zapewnia stabilną transmisję przy bardzo wysokich częstotliwościach

Aspekt bezpieczeństwa: MACsec (IEEE 802.1AE) – szyfrowanie ramek Ethernet w czasie rzeczywistym, 802.1X – uwierzytelnianie urządzeń przy użyciu EAP, izolacja VLAN i segmentacja ruchu – podwyższony poziom bezpieczeństwa (np. data center, instytucje rządowe)

442

Ethernet – media transmisyjne

100BASE-FX — Fast Ethernet na światłowodzie

Rok standaryzacji: 1995 (IEEE 802.3u)

Prędkość: 100 Mb/s

Medium: światłowód MMF (Multi-Mode Fiber)

Długość segmentu: do 2 km

Kodowanie: 4B/5B + NRZI

Topologia: gwiazda (z przełącznikiem w środku) lub pierścień

Znaczenie: odporność na zakłócenia elektromagnetyczne

Aspekt bezpieczeństwa: trudności w podsłuchu – niezbędny fizyczny dostęp i specjalny sprzęt optyczny, podwyższony poziom bezpieczeństwa (np. data center, instytucje rządowe)

443

Ethernet – media transmisyjne

1000BASE-LX — Gigabit Ethernet światłowodowy

Rok standaryzacji: 1999 (IEEE 802.3z)

Prędkość: 1 Gb/s

Medium: światłowód SMF (Single-Mode Fiber) lub MMF

Długość segmentu: do 5 km

Kodowanie: 8B/10B

Topologia: gwiazda (z przełącznikiem w środku) lub pierścień

Znaczenie: stosowany w sieciach szkieletowych – połączenie sieci lokalnych z rozległymi

Aspekt bezpieczeństwa: trudności w podsłuchu – niezbędny fizyczny dostęp i specjalny sprzęt optyczny, zabezpieczenia logiczne: 802.1X, VLAN, MACsec, podwyższony poziom bezpieczeństwa (np. data center, instytucje rządowe)

444

Ethernet – media transmisyjne

10GBASE-SR / LR — 10 Gigabit Ethernet światłowodowy

Rok standaryzacji: 2002 (IEEE 802.3ae)

Prędkość: 10 Gb/s

Medium: SR – światłowód MMF (Multi-Mode Fiber), długość fali 850 nm
LR – światłowód SMF (Single-Mode Fiber), długość fali 1310 nm

Długość segmentu: SR: do 300 m
LR: do 10 Km (SMF)

Kodowanie: 64B/66B

Topologia: gwiazda lub szkielet światłowodowy

Znaczenie: pierwszy szeroko stosowany w sieciach szkieletowych – niski poziom opóźnień i odporność na zakłócenia EMI

Aspekt bezpieczeństwa: trudności w podsłuchu – niezbędny fizyczny dostęp i specjalny sprzęt 445
optyczny, zabezpieczenia logiczne: 802.1X (EAP), VLAN i ACL, MACsec, fizyczny system detekcji naruszenia toru optycznego

Ethernet – media transmisyjne

40GBASE-SR4 — 40 Gigabit Ethernet światłowodowy

Rok standaryzacji: 2010 (IEEE 802.3ba)

Prędkość: 40 Gb/s

Medium: światłowód MMF (Multi-Mode Fiber)

Długość segmentu: do 150 m (klasa OM3) lub 400 m (klasa OM4)

Kodowanie: 64B/66B

Topologia: gwiazda lub szkielet data center

Znaczenie: 4 krotnie zwiększona przepustowość przy zachowaniu niskich opóźnień, kluczowy standard w centrach danych, wspiera technologię link aggregation i redundancję ścieżek

Aspekt bezpieczeństwa: trudności w podsłuchu – niezbędny fizyczny dostęp i specjalny sprzęt optyczny, zabezpieczenia logiczne: 802.1X (EAP), VLAN i ACL, MACsec, fizyczny system

detekcji naruszenia toru optycznego, architektura leaf-spline zwiększa odporność na awarie i ataki DoS w warstwie fizycznej

Ethernet – media transmisyjne

100GBASE-SR4 — 100 Gigabit Ethernet światłowodowy

Rok standaryzacji: 2010 (IEEE 802.3ba)

Prędkość: 100 Gb/s

Medium: światłowód SMF (Single-Mode Fiber)

Długość segmentu: do 10 km

Kodowanie: 64B/66B

Topologia: gwiazda lub szkielet data center

Znaczenie: standard sieci szkieletowych – łączy węzły sieci operatorskich i korporacyjnych, wprowadza technologię WDM – wiele strumieni danych jednym włóknem

Aspekt bezpieczeństwa: trudności w podsłuchu – niezbędny fizyczny dostęp i specjalny sprzęt optyczny, zabezpieczenia logiczne: (802.1AE) – szyfrowanie w warstwie 2 dla 100Gb/s, BFD, OAM – monitorowanie integralności połączeń, 802.1X – kontrola dostępu do portów, DWDM 447
– alarmowanie przy naruszeniu włókna, ISP, obronność, bankowość, sektor energetyczny

Ethernet – protokoły wielodostępu

W sieciach komputerowych wiele urządzeń (hostów) może chcieć jednocześnie wysyłać dane przez wspólne medium transmisyjne – kabel, światłowód lub fale radiowe
Aby zapobiec kolizjom i zapewnić sprawiedliwy dostęp, w warstwie MAC (Media Access Control) stosuje się protokoły wielodostępu

Każdy protokół określa, jak urządzenia „dogadują się” co do tego, kto może nadawać w danym momencie

Protokoły MAC można podzielić na trzy główne grupy:

- Protokoły dzielące kanał (Channel Partitioning Protocols)
- Protokoły dostępu losowego (Random Access Protocols)
- Protokoły cykliczne / deterministyczne (Taking-Turns Protocols)

448

Ethernet – protokoły wielodostępu

Protokoły dzielące kanał (Channel Partitioning Protocols)

Każdy użytkownik ma zagwarantowaną część medium – czas, pasmo częstotliwości lub unikalny kod

Medium jest podzielone statycznie – kolizje nie występują, ale efektywność spada, jeśli nie wszystkie stacje nadają

Metoda

Opis

FDM (Frequency Division Multiplexing)

Każda stacja używa innego zakresu częstotliwości

DSLTD (Time Division Multiplexing)

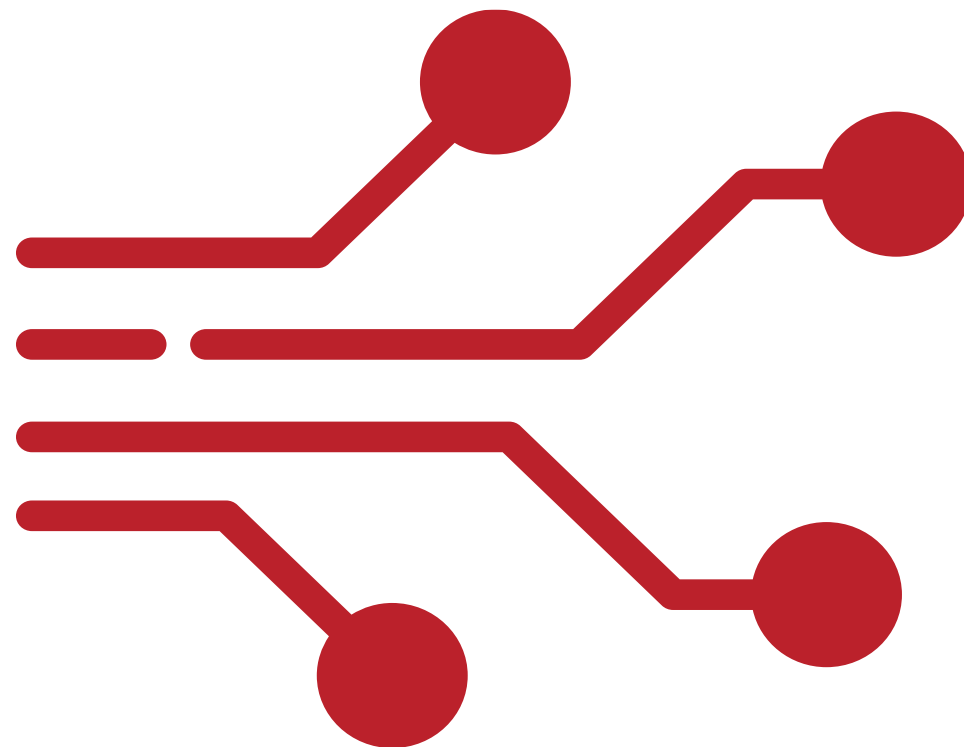
Każda stacja nadaje w przydzielonym przedziale czasowym (slot)

CDMA (Code Division Multiple Access)

Każda stacja używa innego kodu – transmisje się nakładają, ale są rozróżnialne

449

Podstawy działania Ethernetu



450

Ethernet – podstawy działania

Technologia sieci LAN stworzona w latach 70 – Bob Metcalfe i David Boggs

Na początku – węzły połączone magistralą za pomocą kabla koncentrycznego

Topologia stosowana w latach 80 – lokalne sieci rozgłaszające – wszystkie karty sieciowe odbierają i przetwarzają każdą wysłaną ramkę danych

W latach 90 większość firm i uniwersytetów wdrożyła w sieciach lokalnych sieci ethernetowe w topologii gwiazdy z koncentratorem za pomocą miedzianej skrętki

Koncentrator (hub) – urządzenie działające na poszczególnych bitach (nie ramkach):

Jeśli do jednego interfejsu koncentratora trafi bit o wartości 0 lub 1 – powieli bit, wzmacnia sygnał i przekazuje do wszystkich interfejsów

451

Ethernet – podstawy działania

Na początku tego wieku – topologia gwiazdy – centralny koncentrator zastąpiono przełącznikiem

Przełącznik – urządzenie odbierające ramki danych warstwy łącza danych i przekazujące je do łączy wychodzących

Jest przełącznikiem pakietów działającym w trybie przechowywania i przekazywania

Działa tylko do poziomu warstwy 2 (łącza danych) w przeciwieństwie do routerów – działają do poziomu warstwy 3 (sieci)

Przełącznik jest niewidoczny dla hostów i routerów:

host lub router umieszcza w ramce adres innego węzła (nie przełącznika) → przesyła do sieci lokalnej → przełącznik odbiera ramkę → przekazuje innym węzłom

452

Ethernet – ramka

Preambuła	Adres docelowy	Adres źródłowy	Typ	Dane	CRC

Pole preambuły (8 bajtów) – każdy z pierwszych 7 bajtów ma wartość 10101010 – sekwencja synchronizująca odbiornik (zegary), ostatni bajt ma wartość 10101011 – wskazuje początek ramki (dane)

Pole adresu docelowego (6 bajtów) – adres MAC karty sieciowej docelowego węzła – jeżeli karta odbierze ramkę ze swoim adresem docelowym lub adresem rozgłaszania – przekaże dalej, w przeciwnym wypadku - odrzuca

Pole adresu źródłowego (6 bajtów) – adres MAC karty sieciowej węzła umieszczającego ramkę w sieci lokalnej

453

Ethernet – ramka

Preambuła	Adres docelowy	Adres źródłowy	Typ	Dane	CRC

Pole typu (2 bajty) – typ protokołu warstwy wyższej (np. IPv4 = 0800, ARP = 00806) – umożliwia multipleksowanie protokołów warstwy sieciowej – odpowiada polu protokołu datagramu warstwy sieciowej i polu numeru portu warstwy transportowej

Pole danych (od 46 do 1500 bajtów) – datagram IP – wartość MTU (Maximum Transfer Unit) = 1500 bajtów

Pole kodu CRC (4 bajty) – umożliwia sprawdzenie błędów związanych z bitami za pomocą sumy kontrolnej

454

Ethernet – przełącznik

Przełącznik – urządzenie odbierające ramki danych warstwy łącza danych i przekazujące je do łączy wychodzących (portów) w obrębie jednej sieci lokalnej

Działa na podstawie adresów MAC zapisanych w tablicy przełączania (MAC Table)

Działają w trybie pełnego duplexu – przesył danych w obydwu kierunkach

Urządzenia typu PnP (Plug and Play) – nie wymagają interwencji administratora – podłączanie segmentów sieci LAN

Główne zadania:

przełączanie ramek, uczenie się adresów MAC, przekazywanie i filtrowanie, segmentacja kolizji, obsługa sieci VLAN

455

Ethernet – przełącznik

Przełączanie ramek

Analiza docelowego adresu MAC znajdującego się w nagłówku ramki Ethernet

Przekierowanie ramki do odpowiedniego portu wyjściowego – zamiast rozgłaszania do wszystkich urządzeń w sieci

1. Odbiór ramki (Frame Reception) - odbiera ramkę z jednego ze swoich portów i odczytuje adres MAC źródłowy i zapisuje go w tablicy MAC (tzw. Learning)
2. Decyzja przełączania (Forwarding Decision) - analizuje adres MAC docelowy ramki i sprawdza swoją tablicę MAC (MAC Address Table), czy zna port, na którym znajduje się adres odbiorcy
3. Przekazanie ramki (Frame Forwarding) - jeśli adres docelowy jest znany → przesyła ramkę tylko na właściwy port (unicast), Jeśli adres nieznany → ramka jest rozgłaszana (flooding) do wszystkich portów oprócz źródłowego, Jeśli adres jest rozgłoszeniowy (broadcast) lub grupowy (multicast) → switch rozsyła ramkę do wszystkich odpowiednich portów VLAN-u
4. Odrzucenie / filtrowanie (Filtering) - ramka może zostać odrzucona, jeśli jest skierowana do nadawcy (loop prevention), pochodzi z nieautoryzowanego portu, lub narusza reguły bezpieczeństwa (Port Security, VLAN ACL)

456

Ethernet – przełącznik

Tryby przełączania ramek

Tryb	Opis	Zalety	Wady
Store-and-Forward	Switch buforuje całą ramkę, sprawdza błędy CRC, a następnie przesyła dalej	Wysoka dokładność, brak błędów transmisji	Większe opóźnienie
Cut-Through	Switch przesyła ramkę natychmiast po odczytaniu adresu docelowego MAC (bez sprawdzania CRC)	Bardzo niskie opóźnienie	Możliwe błędy transmisji
Fragment-Free	Hybrydowy — odczytuje pierwsze 64 bajty ramki (gdzie zwykle występują kolizje) i dopiero wtedy przekazuje dalej	Kompromis między szybkością a jakością	Używany głównie w sieciach Fast Ethernet

457

Ethernet – przełącznik

Uczenie się adresów

Uczenie się (Learning) to proces, w którym przełącznik Ethernet buduje mapę sieci lokalnej na podstawie adresów MAC urządzeń końcowych

Switch analizuje każdą przychodzącą ramkę i zapisuje w swojej tablicy MAC (MAC Address Table) informację, który adres MAC znajduje się na którym porcie fizycznym

Dzięki temu kolejne ramki mogą być precyzyjnie przekazywane tylko do odpowiedniego portu, zamiast rozgłaszania ich w całej sieci

Tabela przełączania tworzona jest automatycznie, dynamicznie i autonomicznie – bez udziału administratora lub protokołu komunikacyjnego

458

Ethernet – przełącznik

Uczenie się adresów

1. Początkowo tablica przełączania jest pusta
2. Dla każdej ramki odebranej przez interfejs przełącznik tworzy w tabeli wpis przechowujący:
 - Adres MAC zawarty w polu adresu źródłowego ramki
 - Numer interfejsu, który otrzymał ramkę
 - Aktualny czas
3. Adresy w tabeli zostaną usunięte, jeżeli po upływie pewnego czasu (czas starzenia) nie zostaną odebrane żadne ramki z tym adresem źródłowym

459

Ethernet – przełącznik

Uczenie się adresów

Adres MAC	Interfejs	Czas ostatniej aktywności
00:11:22:33:44:55	1	12:31:04
00:11:22:AA:BB:CC	2	12:31:06
00:11:22:DD:EE:FF	3	12:31:08

460

Ethernet – przełącznik

Przekazywanie i filtrowanie

Po odebraniu ramki Ethernet z portu wejściowego, przełącznik analizuje jej nagłówek, a konkretnie adres docelowy MAC (Destination MAC)

Na tej podstawie decyduje, czy i dokąd przekazać ramkę – czyli wykonuje tzw. decyzję przełączania (switching decision)

Proces ten obejmuje dwa podstawowe mechanizmy:

- **Forwarding** – przekazanie ramki do odpowiedniego portu
- **Filtering** – odrzucenie lub zablokowanie ramki w określonych warunkach

461

Ethernet – przełącznik

Przekazywanie i filtrowanie – Etapy podejmowania decyzji

1. Odbiór ramki (Frame Reception)
2. Sprawdzenie tablicy MAC (MAC Address Table Lookup)\
3. Decyzja:
 - Jeśli adres jest znany (Unicast) → ramka trafia tylko do jednego portu (precyzyjny forwarding)
 - Jeśli adres nieznany (Unknown Unicast) → switch rozgłasza (flooding) ramkę do wszystkich portów w tym samym VLAN-ie (oprócz źródłowego)
 - Jeśli adres docelowy = adres źródłowy → ramka jest odrzucana (filtering), aby uniknąć powstania pętli logicznej

462

Ethernet – przełącznik

Przekazywanie i filtrowanie – Etapy podejmowania decyzji

4. Dodatkowe decyzje – filtracja na podstawie polityk

Filtrowanie ruchu (czyli nie przekazywanie ramek):

- ramka pochodzi z nieautoryzowanego urządzenia (Port Security)
- przekracza limity (Storm Control)
- należy do innego VLAN-u (VLAN Isolation)
- zawiera błędy (CRC Error)
- lub narusza reguły ACL (Access Control List)

463

Ethernet – przełącznik

Typ	Opis	Przykład
Unicast	Ramka skierowana do jednego konkretnego odbiorcy (znany adres MAC)	Komputer → drukarka
Unknown Unicast	Odbiorca nieznany – switch rozsyła ramkę do wszystkich portów VLAN-u	Nowe urządzenie w sieci
Broadcast	Ramka z adresem FF:FF:FF:FF:FF:FF – trafia do wszystkich portów VLAN	ARP Request
Multicast	Ramka do określonej grupy urządzeń (MAC grupowy)	Transmisja wideo, IPv6 ND
Filtering	Ramka odrzucona, np. z powodu błędu lub pętli	Ramka z tym samym źródłem i celem

464

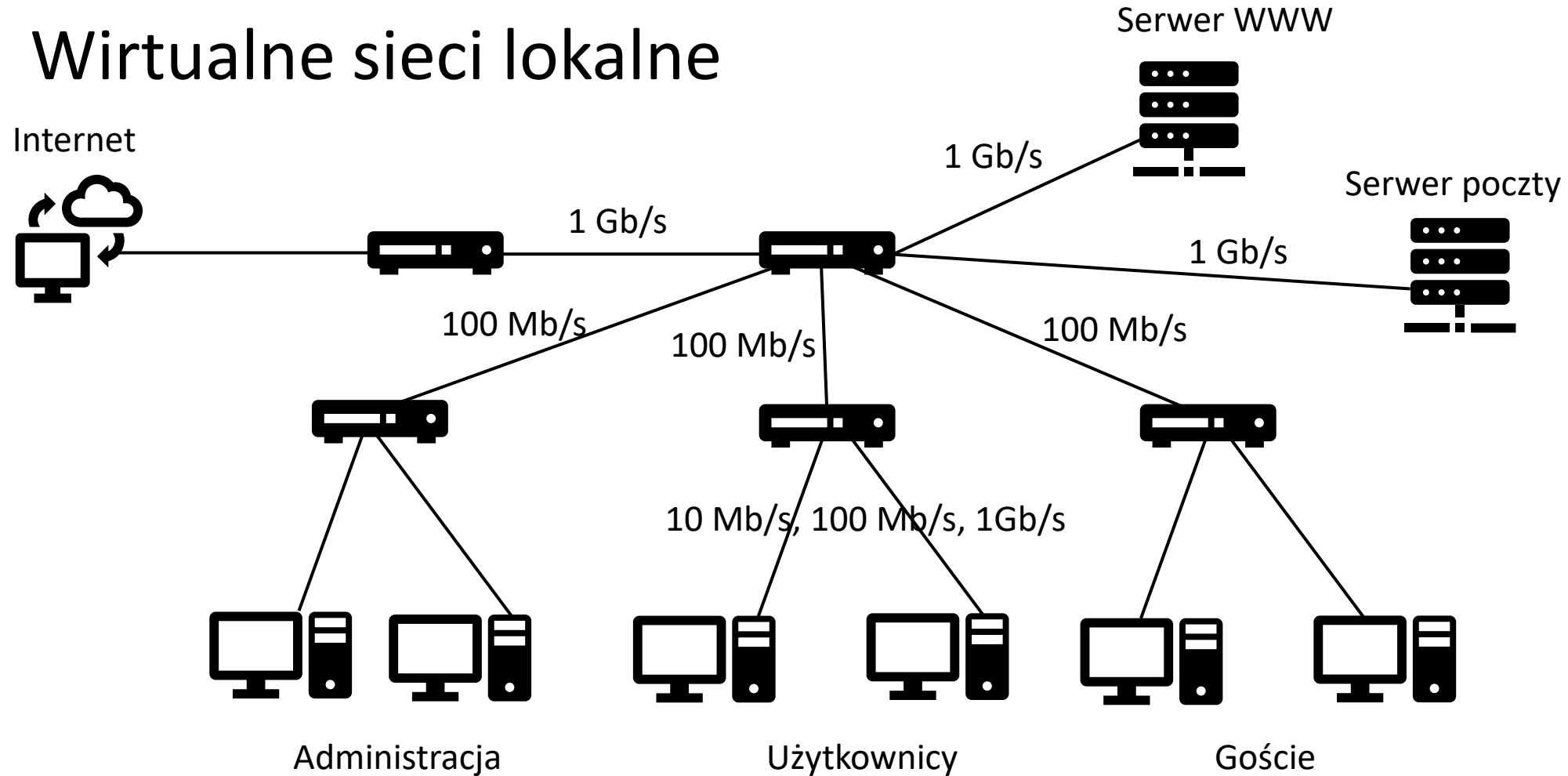
Ethernet – przełącznik

Mechanizmy filtracji i zapobiegania pętlom:

1. Spanning Tree Protocol (STP, RSTP, MSTP) – zapobiega powstawaniu pętli w topologiach z redundantnymi połączeniami, automatycznie blokuje część portów, pozostawiając tylko jedno aktywne łącze między przełącznikami (jeśli aktywne łącze ulegnie awarii – STP aktywuje zapasowe)
2. Filtering na podstawie VLAN (VLAN Separation) – ramki są przekazywane tylko w obrębie tego samego VLAN, odrzuca (filteruje) ramki z identyfikatorem VLAN, który nie jest dozwolony na danym porcie (dotyczy portów trunk)
3. Storm Control / Broadcast Suppression – chroni sieć przed przeciążeniem spowodowanym nadmiarem ramek broadcast lub multicast, automatycznie blokuje port lub ogranicza przepływ ramek po przekroczeniu progu (np. 20% pasma)
4. Access Control Lists (ACL) – pozwalają zdefiniować dokładnie, które ramki mogą być przekazane lub odrzucone, Filtracja odbywa się według: adresu MAC, VLAN, protokołu, a nawet typu EtherType

465

Wirtualne sieci lokalne



466

Wirtualne sieci lokalne

Hierarchiczna architektura sieci LAN

Sieć lokalna w dużych organizacjach jest zbudowana warstwowo (hierarchicznie)

Każda grupa robocza lub dział posiada własny przełącznik dostępu (Access Switch), który jest połączony z przełącznikami dystrybucyjnymi i rdzeniowymi (Core)

Ruch wewnątrz danej grupy jest lokalny, natomiast komunikacja między działami odbywa się przez warstwy wyższe

Wady sieci bez segmentacji:

- Wszystkie urządzenia znajdują się w jednej domenie rozgłoszeniowej
- Komunikaty typu ARP, DHCP Discover czy broadcast są rozsyłane do wszystkich hostów
- Powoduje to:
 - zwiększone obciążenie sieci (broadcast stormy),
 - brak izolacji ruchu między działami (np. Administracja ↔ Użytkownicy ↔ Goście)
 - ryzyko podsłuchu i ataków wewnętrznych
 - trudności w zarządzaniu bezpieczeństwem

467

Wirtualne sieci lokalne

VLAN (Virtual Local Area Network) to logiczny podział jednej fizycznej sieci LAN na wiele niezależnych, odizolowanych segmentów, VLAN działa w warstwie 2, ale wymaga warstwy 3 do komunikacji między segmentami

Każdy VLAN ma:

- własną domenę rozgłoszeniową
- własną tablicę adresów MAC
- często także osobną podsieć IP (np. VLAN 10 → 192.168.10.0/24)

Dzięki temu możliwe jest:

- oddzielenie ruchu działów lub systemów
- zwiększenie bezpieczeństwa (mniej powierzchni ataku)
- lepsze zarządzanie ruchem i priorytetami

468

Wirtualne sieci lokalne

Jak działa VLAN w praktyce

- Każdy port przełącznika jest przypisany do VLAN-u (w trybie Access lub Trunk):
 - Port typu Access – przypisany do jednego VLAN-u (np. komputer w VLAN 20)
 - Port typu Trunk – przenosi wiele VLAN-ów między przełącznikami (ramki tagowane)
 - Przełącznik wie, do którego VLAN-u należy dany port i kieruje ruch tylko w jego obrębie
- Ramki Ethernet zawierają znacznik VLAN (802.1Q Tag)
 - W polu nagłówka Ethernet dodawane są 4 bajty informacji (VID – VLAN ID)
 - Ten znacznik informuje inne przełączniki, do którego VLAN-u należy dana ramka
 - Zakres ID VLAN: 1–4094 (standard IEEE 802.1Q)
- Przełącznik przekazuje ramki tylko w obrębie tego samego VLAN-u
 - Hosty w różnych VLAN-ach nie mogą się komunikować bezpośrednio
 - Pełna izolacja logiczna między grupami urządzeń - ruch broadcast (np. ARP, DHCP Discover) nie wychodzi poza VLAN

469

Wirtualne sieci lokalne

Jak działa VLAN w praktyce

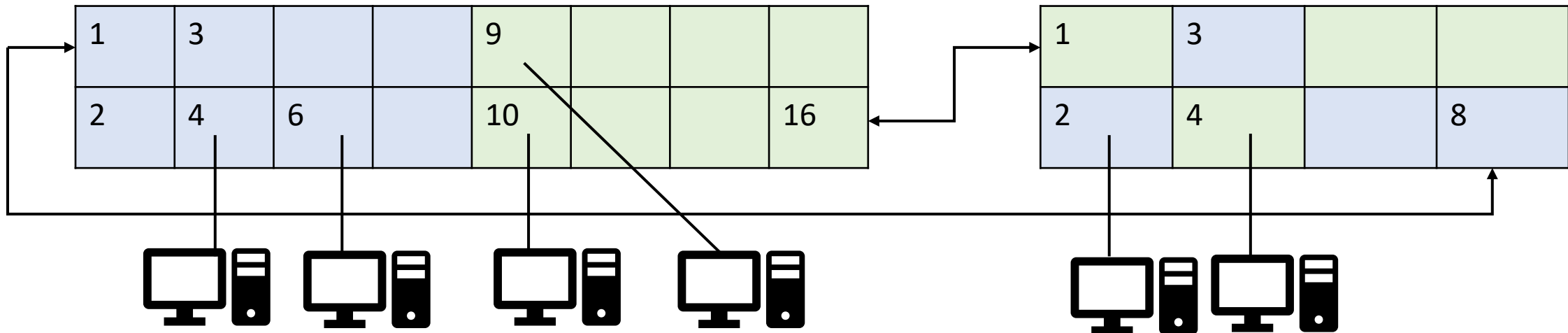
Komunikacja między VLAN-ami (Inter-VLAN Routing)

- Aby przesłać dane między VLAN-ami, potrzebne jest urządzenie warstwy 3:
 - Router (Router-on-a-stick) – klasyczne rozwiązanie
 - Przełącznik warstwy 3 (L3 Switch) – szybsze, nowoczesne rozwiązanie
- Router analizuje nagłówki IP i decyduje, które pakiety mogą przechodzić między VLAN-ami
- Można też stosować reguły ACL, aby ograniczyć komunikację między segmentami

Co jeżeli jest potrzebny kolejny przełącznik z tymi samymi sieciami VLAN?

470

Wirtualne sieci lokalne



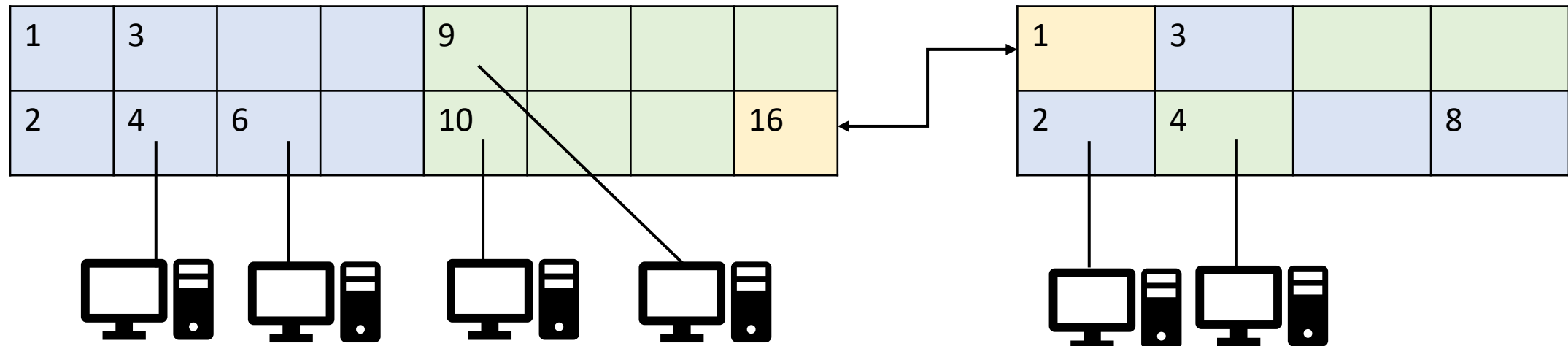
Określamy porty należące do danej sieci VLAN i łączymy je ze sobą

N sieci VLAN wymaga N portów w każdym przełączniku

Brak skalowalności

471

Wirtualne sieci lokalne



Określamy w każdym przełączniku port przełączający (Trunk port)
 Pozwala przesyłać ruch wielu sieci VLAN jednym fizycznym łączem
 Wysoka skalowalność

472

Wirtualne sieci lokalne

- Port typu Access – przypisany do jednego VLAN-u (np. komputer w VLAN 20)
- Port typu Trunk – przenosi wiele VLAN-ów między przełącznikami (ramki tagowane)

Jak przełącznik określa które ramki docierające do portu przełączającego mają trafić do których sieci VLAN?

Nowy format ramki ethernetowej wzbogacony o 4 bitowy znacznik sieci VLAN (wstawiany pomiędzy adres MAC a pole EtherType) – dodawany do ramki przez przełącznik po stronie nadawczej portu przełączającego - przetwarzany i usuwany przez przełącznik po stronie odbiorcy

Standard IEEE 802.1Q

473

Wirtualne sieci lokalne

Standardowa ramka ethernetowa

Preambuła	Adres docelowy	Adres źródłowy	Typ	Dane	CRC

Ramka ethernetowa 802.1Q z oznaczeniem sieci VLAN

Preambuła	Adres docelowy	Adres źródłowy	TPID	TCI	Typ	Dane	CRC

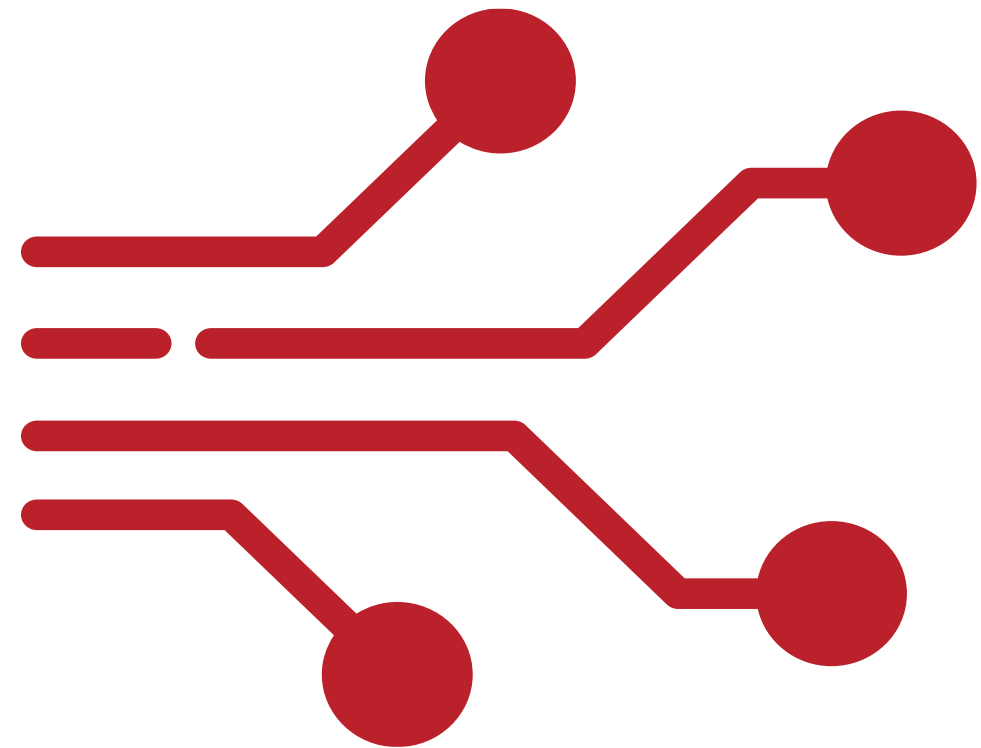
474

Wirtualne sieci lokalne

- Pole TPID (Tag Protocol Identifier) – 16 bitów (2 bajty) – wartość 0x8100 – ramka zawiera tag VLAN
- Pole TCI (Tag Control Information) – 16 bitów (2 bajty) – zawiera:
 - PRI (3 bity) – priorytet ramki w mechanizmach QoS (0-7)
 - CFI (1 bit) – sposób kodowania adresów MAC w ramce: 0 – kanoniczny (Ethernet), 1 – niekanoniczny (dawniej Token Ring), aktualnie CFI = 0 – inaczej brak przekazywania
 - VID – Vlan Identifier (12 bitów) – identyfikuje logiczny segment VLAN danej ramki:
 - 0 – ramka bez przypisanego VLAN – używana przy QoS (priorytety bez segmentacji)
 - 1 – domyślny VLAN (Native VLAN, zalecana zmiana)
 - 2–1005 – VLAN-y standardowe (legacy / Cisco)
 - 1006–4094 – VLAN-y rozszerzone (IEEE 802.1Q)
 - 4095 – zarezerwowane

475

Standardy Wi-Fi 802.11: działanie i konfiguracja



476

Bezprzewodowe sieci lokalne

Kiedy stosujemy sieci bezprzewodowe?

- Gdy brak fizycznej możliwości ułożenia okablowania (zabytki, duże hale, obiekty tymczasowe)
- W miejscach, gdzie mobilność użytkowników jest kluczowa (biura, uczelnie, magazyny, IoT)
- Ze względów ekonomicznych – niższy koszt wdrożenia w porównaniu z siecią przewodową
- W środowiskach wymagających elastycznej rekonfiguracji (sieci tymczasowe, eventy, systemy awaryjne)

477

Bezprzewodowe sieci lokalne - zalety

Obszar

Opis

Dostępność

Łatwy dostęp do medium transmisyjnego (powietrza) bez potrzeby kabli

Zasięg

Możliwość pokrycia dużych obszarów – od pomieszczeń po kampusy

Mobilność

Użytkownicy mogą się przemieszczać, zachowując połączenie z siecią

Skalowalność

Prosta rozbudowa poprzez dodanie punktów dostępowych (AP)

Elastyczność

Różnorodne topologie (Ad-Hoc, BSS, ESS, Mesh)

Ekonomia

Niższe koszty instalacji i utrzymania w porównaniu z siecią przewodową

478

Bezprzewodowe sieci lokalne - wady

Kategoria	Opis
Zakłócenia i tłumienie	Fale radiowe ulegają odbiciu, pochłanianiu i zakłóceniom od innych urządzeń (Bluetooth, mikrofalówki, 5G)
Zasięg i przepustowość	Wraz z odległością maleje siła sygnału i efektywna prędkość transmisji
Bezpieczeństwo	Ryzyko podsłuchu, zagłuszania, spoofingu, ataków typu <i>evil twin</i> (fałszywy punkt dostępowy)
Stabilność	Wrażliwość na warunki środowiskowe (wilgoć, ściany, metalowe powierzchnie)
Zarządzanie częstotliwościami	Ograniczona liczba kanałów w paśmie ISM, konieczność planowania kanałów
Energochłonność	Urządzenia mobilne szybciej zużywają baterię podczas transmisji radiowej

479

Bezprzewodowe sieci lokalne - topologia

Topologia

Charakterystyka

Ad-Hoc

Połączenia bez punktu dostępowego (peer-to-peer)

BSS (Basic Service Set)

Jeden punkt dostępowy (AP) i klienci – najczęstsza forma Wi-Fi

ESS (Extended Service Set)

Wiele punktów AP połączonych siecią przewodową (LAN) – sieci kampusowe

Mesh (802.11s)

Wiele punktów AP tworzących dynamiczną, samonaprawialną sieć

480

Bezprzewodowe sieci lokalne - elementy

- Hosty bezprzewodowe – urządzenia końcowe, w których działają aplikacje sieciowe
- Łącza bezprzewodowe – host łączy się z:
 - Stacją bazową - w trybie infrastruktury
 - Innym hostem – w trybie ad-hoc (peer-to-peer)Podstawowe cechy: zasięg i prędkość
- Stacja bazowa – urządzenie pośredniczące między hostami a siecią przewodową (Ethernet), realizuje transmisję ramek 802.11 oraz funkcje warstwy łącza i sieci, wysyła i odbiera dane (pakiety) od hostów znajdujących się w jej zasięgu
Zapewnia usługi sieciowe: przydzielanie adresów IP (DHCP), uwierzytelnianie (802.1X / WPA2-Enterprise), translację adresów (NAT), routing między sieciami

481

Bezprzewodowe sieci lokalne - tryby

Infrastruktura sieci bezprzewodowej (Infrastructure Mode):

Hosty są powiązane z konkretną stacją bazową (AP)

Cała komunikacja między hostami przechodzi przez AP

AP pośredniczy w połączeniu z siecią lokalną (LAN) lub Internetem

W ramach infrastruktury funkcjonują:

BSS (Basic Service Set) – pojedynczy AP i jego hosty

ESS (Extended Service Set) – wiele AP połączonych siecią przewodową (np. w kampusie)

482

Bezprzewodowe sieci lokalne - elementy

Sieć doraźna (Ad-Hoc Mode – IBSS):

Hosty komunikują się bezpośrednio, bez punktu dostępowego.

Tworzą tymczasową sieć peer-to-peer, np. między laptopami lub urządzeniami mobilnymi.

Każdy host realizuje podstawowe usługi sieciowe samodzielnie:

- przekazywanie ramek

- adresowanie

- wybór trasy (routing ad hoc)

483

Bezprzewodowe sieci lokalne – zasada działania

Nadajniki konwertują sygnał elektryczny na fale elektromagnetyczne (radiowe)

Prąd zmienny w antenie nadajnika generuje zmienne pole elektryczne i magnetyczne, które propaguje się w przestrzeni jako fala radiowa

Odbiornik dokonuje odwrotnego procesu – przekształca falę radiową z powrotem w sygnał elektryczny

Im wyższa częstotliwość – tym większe tłumienie i krótszy zasięg

484

Bezprzewodowe sieci lokalne – propagacja fal

Tłumienie sygnału (attenuation):

- energia fali maleje w miarę oddalania się od anteny
- siła sygnału spada proporcjonalnie do kwadratu odległości (prawo odwrotności kwadratu):
- w odległości 10 m sygnał ma ok. 1/100 pierwotnej mocy
- **Pochłanianie i odbicia:**
 - fala traci energię przy przechodzeniu przez przeszkody (ściany, szkło, drzewa, ciało ludzkie)
 - odbicia od metalowych powierzchni powodują wielodrogowość (multipath) – kilka kopii sygnału dociera z opóźnieniem, co zniekształca odbiór
- **Załamanie (refrakcja):**
 - zmiana kierunku fali przy przechodzeniu między ośrodkami o różnej gęstości (np. powietrze–ściana)
- **Rozpraszanie (scattering):**
 - fale odbijają się od małych obiektów (np. kropli deszczu, liści), co prowadzi do utraty energii i interferencji

485

Bezprzewodowe sieci lokalne – konfiguracja antenowa

W sieciach bezprzewodowych jakość i przepustowość połączenia zależą nie tylko od mocy nadajnika, ale także od liczby anten po stronie nadawczej i odbiorczej

Typ systemu	Nazwa	Liczba anten	Charakterystyka	Przykłady
SISO	<i>Single Input, Single Output</i>	1 Tx – 1 Rx	Klasyczny system z jedną anteną nadawczą i jedną odbiorczą	Stare Wi-Fi (802.11b), Bluetooth
SIMO	<i>Single Input, Multiple Output</i>	1 Tx – wiele Rx	Jedna antena nadaje, kilka odbiera – poprawa czułości i odporności na zakłócenia	Odbiorniki diversity w telefonach
MISO	<i>Multiple Input, Single Output</i>	Wiele Tx – 1 Rx	Wiele anten nadających zwiększa siłę i niezawodność sygnału w kierunku odbiorcy	Transmit Beamforming w Wi-Fi 5/6
MIMO	<i>Multiple Input, Multiple Output</i>	Wiele Tx – wiele Rx	Wiele anten nadaje i odbiera równolegle — wzrost przepustowości (równoległe strumienie danych)	Wi-Fi 5/6, LTE, 5G

486

Bezprzewodowe sieci lokalne – propagacja fal

Tłumienie sygnału (attenuation):

- energia fali maleje w miarę oddalania się od anteny
- siła sygnału spada proporcjonalnie do kwadratu odległości (prawo odwrotności kwadratu):
- w odległości 10 m sygnał ma ok. 1/100 pierwotnej mocy
- **Pochłanianie i odbicia:**
 - fala traci energię przy przechodzeniu przez przeszkody (ściany, szkło, drzewa, ciało ludzkie)
 - odbicia od metalowych powierzchni powodują wielodrogowość (multipath) – kilka kopii sygnału dociera z opóźnieniem, co zniekształca odbiór
- **Załamanie (refrakcja):**
 - zmiana kierunku fali przy przechodzeniu między ośrodkami o różnej gęstości (np. powietrze–ściana)
- **Rozpraszanie (scattering):**
 - fale odbijają się od małych obiektów (np. kropli deszczu, liści), co prowadzi do utraty energii i interferencji

487

Bezprzewodowe sieci lokalne – propagacja fal

Zysk dywersyfikacji (Diversity Gain) - *wyższa niezawodność połączenia*

- Wiele anten odbiorczych lub nadawczych = różne ścieżki propagacji sygnału
- Sygnały docierają różnymi drogami → mniejsze ryzyko zaniku (fading)
- System wybiera lub łączy najlepsze sygnały (ang. *selection combining / maximal ratio combining*)

Zysk odbioru zbiorczego (Array Gain / SNR Gain) - *poprawa jakości połączenia i zasięgu*

- Wiele anten odbiorczych sumuje energię odebranych sygnałów → wzrost **SNR (Signal-to-Noise Ratio)**
- Lepszy stosunek sygnału do szumu = mniejszy błąd transmisji, większa odległość między urządzeniami

Zysk multipleksacji przestrzennej (Spatial Multiplexing Gain) - *wielokrotny wzrost przepustowości bez zwiększania pasma*

- Strumień danych jest **dzielony na niezależne podstrumienie**, transmitowane równolegle różnymi antenami
- Każdy odbiornik odbiera unikalne kombinacje sygnałów i rekonstruuje pełny strumień dzięki różnicom w propagacji

488

Bezprzewodowe sieci lokalne – SNR

SNR – Signal-to-Noise Ratio (stosunek sygnału do szumu) - miara jakości połączenia radiowego, określająca, jak silny jest sygnał użyteczny w porównaniu z zakłóceniami (szumem tła)

$$SNR = P_{\text{sygnału}} - P_{\text{szumu}} [dB]$$

Im wyższy SNR, tym lepsza jakość połączenia i mniejsza liczba błędów transmisji

- Wpływa bezpośrednio na prędkość i stabilność transmisji
- Określa, jakie modulacje i kody korekcyjne (MCS) może zastosować urządzenie
- Niski SNR → więcej błędów ramek, retransmisje, spadek przepustowości
- Wysoki SNR → możliwość użycia wyższych modulacji

SNR jest kluczowym wskaźnikiem jakości połączenia w Wi-Fi – bardziej miarodajnym niż sam poziom sygnału

489

Bezprzewodowe sieci lokalne – SNR

Jakość połączenia	SNR [dB]	Możliwa modulacja	Prędkość (przykładowo)
Doskonała	> 40 dB	256-QAM / 1024-QAM	600 Mb/s – 9,6 Gb/s (Wi-Fi 6)
Dobra	25–40 dB	64-QAM / 256-QAM	150–600 Mb/s
Średnia	15–25 dB	16-QAM	54–150 Mb/s
Słaba	10–15 dB	QPSK	< 54 Mb/s
Bardzo słaba	< 10 dB	BPSK / brak łączności	Niestabilna transmisja

Aby utrzymać stabilne połączenie Wi-Fi, minimalny SNR powinien wynosić **15–20 dB**

490

Bezprzewodowe sieci lokalne – BER

BER – Bit Error Rate - miara błędów transmisji w kanale komunikacyjnym

Określa, jaki procent bitów został odebrany niepoprawnie w stosunku do liczby wszystkich przesłanych bitów:

$$BER = \frac{N_{\text{błędnych bitów}}}{N_{\text{wszystkich bitów}}}$$

Im niższy BER → tym bardziej niezawodne połączenie

Zależny od: SNR, modulacji, kodowania korekcyjnego (FEC) i warunków środowiskowych

Wysoki BER : retransmisja ramek (CSMA/CA → ponowne nadanie), spadek efektywnej przepustowości, większe opóźnienia i utrata pakietów

Wi-Fi obniża szybkość transmisji, gdy BER przekracza próg błędów dla danej modulacji

491

Bezprzewodowe sieci lokalne – SNR

Modulacja	Wymagany SNR	Typowy BER (dla niskiego SNR)	Odporność na błędy	
BPSK	> 7 dB	$10^{-3} - 10^{-4}$	bardzo wysoka	
QPSK	> 10 dB	$10^{-4} - 10^{-5}$	wysoka	
16-QAM	> 16 dB	$10^{-5} - 10^{-6}$	średnia	
64-QAM	> 24 dB	$10^{-6} - 10^{-7}$	niska	
256-QAM / 1024-QAM	> 30–35 dB	$< 10^{-8}$ (przy idealnym kanale)	bardzo niska odporność	492

Bezprzewodowe sieci lokalne – zasięg

Czynniki wpływające na zasięg

1. Pasma częstotliwości:

1. 2.4 GHz → większy zasięg, mniejsza prędkość
2. 5 GHz → krótszy zasięg, większa przepustowość
3. 6 GHz (Wi-Fi 6E) → bardzo szybkie, ale najmniejszy zasięg

2. Moc nadawcza routera (Transmit Power) – typowo 15–20 dBm

3. Rodzaj anteny – wewnętrzne (krótszy zasięg) vs zewnętrzne (lepsze pokrycie)

4. Materiały budowlane – ściany z cegły lub betonu tłumią sygnał 10–20 dB

5. Zakłócenia elektromagnetyczne – mikrofalówki, Bluetooth, inne Wi-Fi

493

Bezprzewodowe sieci lokalne – zasięg

Pasmo	Zasięg w otwartej przestrzeni	Wewnątrz budynku (przez 2 ściany)	Typowe zastosowanie
2.4 GHz	ok. 45–50 m	ok. 20–25 m	urządzenia IoT, smartfony, drukarki
5 GHz	ok. 25–30 m	ok. 10–15 m	laptopy, TV 4K, konsole
6 GHz	ok. 15–20 m	ok. 5–10 m	urządzenia Wi-Fi 6E

494

Bezprzewodowe sieci lokalne – siła sygnału (RSSI)

- **RSSI (Received Signal Strength Indicator)** – wskaźnik siły odbieranego sygnału radiowego Wi-Fi wyrażany w dBm (decybelach miliwata)
- Im bliżej zera, tym mocniejszy sygnał
- Im bardziej ujemna wartość, tym słabsze połączenie

Poziom sygnału	Zakres (dBm)	Jakość połączenia	Wpływ na działanie
Bardzo silny	-30 do -50	★★★★★	idealny – pełna prędkość
Dobry	-51 do -60	★★★★	stabilne połączenie, streaming 4K
Średni	-61 do -67	★★★	przeglądanie stron, gry jeszcze działają
Słaby	-68 do -75	★★	spadki prędkości, lagi w grach 495
Bardzo słaby	< -75	★	częste rozłączenia, brak Internetu

Bezprzewodowe sieci lokalne – siła sygnału (RSSI)

Jak zmierzyć siłę sygnału

- Na laptopie:
 - Windows: `netsh wlan show interfaces`
 - Mac/Linux: `iwconfig` lub `airport -s`
- Na smartfonie: aplikacje WiFi Analyzer, NetSpot, TP-Link Tether
- W interfejsie routera – często dostępny w sekcji Wireless Statistics

496

Bezprzewodowe sieci lokalne

Wszystkie wersje 802.11 (a/b/g/n/ac/ax) korzystają z tego samego mechanizmu dostępu do medium:

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance → urządzenia nasłuchują kanał i unikają kolizji, rezerwując medium za pomocą ramek RTS/CTS

Transmisja odbywa się w pasmach ISM (2,4 GHz / 5 GHz / 6 GHz) – bez konieczności licencji

Struktura ramki warstwy łącza danych (MAC) jest zgodna między wszystkimi wersjami standardu

Urządzenia Wi-Fi są kompatybilne wstecz – nowsze punkty dostępowe (AP) mogą obsługiwać starsze standardy

Standardy mogą dynamicznie zmniejszać prędkość transmisji, aby zwiększyć zasięg (mechanizm rate adaptation)

497

Bezprzewodowe sieci lokalne - standardy

Standard	Pasmo	Modulacja	Przepustowość	Rok	Uwagi
802.11b	2,4 GHz	DSSS	do 11 Mb/s	1999	tanie, długi zasięg, duże zakłócenia
802.11a	5 GHz	OFDM	do 54 Mb/s	1999	krótszy zasięg, mniej zakłóceń
802.11g	2,4 GHz	OFDM	do 54 Mb/s	2003	kompatybilny z 802.11b
802.11n (Wi-Fi 4)	2,4 / 5 GHz	MIMO-OFDM	do 600 Mb/s	2009	transmisja wieloantenowa
802.11ac (Wi-Fi 5)	5 GHz	MU-MIMO, 256-QAM	do 6,9 Gb/s	2013	duża przepustowość
802.11ax (Wi-Fi 6)	2,4 / 5 / 6 GHz	OFDMA	do 9,6 Gb/s	2019	wysoka efektywność, mniejsze opóźnienia
802.11be (Wi-Fi 7)	6 GHz	4096-QAM	> 30 Gb/s	2024	niskie opóźnienia, real-time, VR/IoT

498

Bezprzewodowe sieci lokalne - kanały

Kanał Wi-Fi to wydzielony fragment pasma częstotliwości, w którym może pracować sieć bezprzewodowa IEEE 802.11

Każdy kanał ma określoną szerokość (MHz) i środek częstotliwości

Kanały umożliwiają równoległe działanie wielu sieci w tym samym obszarze bez wzajemnego zakłócania się

Pasmo Wi-Fi	Zakres częstotliwości	Typowe zastosowanie	Uwaga
2,4 GHz	2,400 – 2,4835 GHz	domowe sieci Wi-Fi	duże zasięgi, zakłócenia
5 GHz	5,150 – 5,875 GHz	Wi-Fi 5 / 6	większa przepustowość, krótszy zasięg
6 GHz	5,925 – 7,125 GHz	Wi-Fi 6E / 7	duża liczba kanałów, mało interferencji

499

Bezprzewodowe sieci lokalne - kanały

Kanały w paśmie 2,4 GHz (802.11b/g/n)

- Szerokość kanału: 22 MHz
- Odstęp między kanałami: 5 MHz
- Dostępnych kanałów: 13 (w Europie)
- Kolidujące kanały: większość nakłada się na siebie – oddzielone mniej niż 4 kanałami
- Aby uniknąć interferencji, używa się tylko trzech niepokrywających się kanałów: 1, 6 i 11

Wspólne kanały to główna przyczyna zakłóceń w sieciach domowych i biurowych

500

Bezprzewodowe sieci lokalne - kanały

- Kanały w paśmie 5 GHz (802.11a/n/ac/ax)
- Szerokości kanałów: 20 / 40 / 80 / 160 MHz
- Kanały są niekolidujące, co umożliwia dużą liczbę jednoczesnych sieci
- Kanały dzielą się na grupy:
 - UNII-1 (5150–5250 MHz) – do użytku wewnętrznego,
 - UNII-2 / UNII-2e – wymagają DFS (Dynamic Frequency Selection) – wykrywanie radarów,
 - UNII-3 – do zastosowań zewnętrznych

DFS chroni pasmo radarowe – router musi przełączyć kanał, jeśli wykryje sygnał radarowy

DFS (Dynamic Frequency Selection) – to mechanizm automatycznego wyboru kanału radiowego w paśmie 5 GHz (i częściowo 6 GHz), który chroni systemy radarowe i wojskowe działające na tych samych częstotliwościach

501

Bezprzewodowe sieci lokalne - kanały

- Kanały w paśmie 6 GHz (Wi-Fi 6E / 7)
- Dostępne kanały: 59 (20 MHz)
- Możliwe łączenie w 40 / 80 / 160 / 320 MHz
- Brak wymogu DFS – czyste pasmo, niskie opóźnienia
- Wi-Fi 6E i 7 działają wyłącznie w trybie WPA3, co podnosi poziom bezpieczeństwa

Pasmo 6 GHz = przyszłość sieci korporacyjnych i kampusowych (duże bezpieczeństwo + prędkość)

502

Bezprzewodowe sieci lokalne - AP

SSID (Service Set Identifier) – nazwa sieci Wi-Fi (do 32 znaków), która identyfikuje logicznie daną sieć bezprzewodową

BSSID (Basic Service Set Identifier) – unikalny identyfikator punktu dostępowego (AP) w sieci Wi-Fi, jest to adres MAC interfejsu radiowego Access Pointa, nadawany w każdej ramce rozgłaszanej w sieci

ESSID (Extended Service Set Identifier) – nazwa logiczna sieci Wi-Fi, która obejmuje wiele punktów dostępowych (AP) pracujących wspólnie (jedna sieć bezprzewodową)

Uzyskanie dostępu do Internetu – stacja bezprzewodowa musi połączyć się z dokładnie jedną podsiecią – dokładnie jednym punktem dostępowym

Cały proces odbywa się w warstwie łącza danych (MAC) – jeszcze przed uzyskaniem adresu IP

503

Bezprzewodowe sieci lokalne – etapy połączenia

1. Skanowanie (Discovery / Scanning)

- Urządzenie szuka dostępnych sieci w swoim zasięgu
- Tryby skanowania:
 - Pasywny (Passive Scan):
Klient tylko nasłuchuje ramek Beacon (ramka identyfikacyjna) wysyłanych przez AP (co 100 ms)
→ Niskie zużycie energii, wolniejsze wykrywanie
 - Aktywny (Active Scan):
Klient wysyła ramki Probe Request (ramka próbna żądania), a AP odpowiada ramkami Probe Response (ramka próbna odpowiedzi)
→ Szybsze wykrywanie, ale więcej ruchu w eterze

Ramki te zawierają SSID, BSSID, kanał, poziom sygnału i informacje o zabezpieczeniach (WPA2/WPA3)

504

Bezprzewodowe sieci lokalne – etapy połączenia

2. Autentykacja (Authentication)

- Klient wysyła do AP ramkę Authentication Request (zawiera identyfikator sieci (SSID) i informację o rodzaju autentykacji), a AP odpowiada Authentication Response (potwierdza: kod 0 – sukces lub odrzuca: inny kod) próbę połączenia
- Rodzaje autentykacji:
 - Open System Authentication - klient wysyła prośbę o autentykację, a AP zawsze odpowiada „OK”, standardowe sieci Wi-Fi (WPA2, WPA3, hotspoty), brak weryfikacji na tym etapie (dopiero później – handshake WPA)
 - Shared Key Authentication - używa mechanizmu WEP, AP wysyła wyzwanie (challenge text), które klient szyfruje współdzielonym kluczem WEP i odsyła, stare sieci WEP (obecnie nieużywane), można łatwo odtworzyć klucz WEP analizując odpowiedzi
 - SAE (Simultaneous Authentication of Equals) - mechanizm w WPA3 – oparty na kryptografii krzywych eliptycznych (ECDH), nowoczesne sieci WPA3-Personal, odporność na ataki słownikowe i podszywania

505

To nie jest jeszcze logowanie do sieci – to tylko uwierzytelnienie na poziomie MAC (warstwy 2)

Bezprzewodowe sieci lokalne – etapy połączenia

3. Asocjacja (Association)

- Po pomyślnej autentykacji klient prosi o dołączenie do sieci
- Ramki:
- Wysyłane przez klienta do AP - Association Request:
zawiera SSID, obsługiwane szybkości transmisji, adres MAC klienta, parametry QoS i bezpieczeństwa
- Wysyłane przez AP do klienta - Association Response:
AP potwierdza przyjęcie i przypisuje Association ID (AID) klientowi w tabeli AP
zawiera: status przyjęcia, AID (Association ID), parametry kanału i mocy, ewentualne limity (np. liczba asocjowanych stacji)

Od tego momentu klient i AP tworzą logiczne połączenie w warstwie 2

506

Bezprzewodowe sieci lokalne – etapy połączenia

4. Uwierzytelnianie (Authentication / Security Handshake)

To właściwy etap bezpieczeństwa – ustanowienie kluczy szyfrowania transmisji

Po autentykacji (MAC) i asocjacji następuje właściwe uwierzytelnienie — czyli sprawdzenie tożsamości użytkownika i ustanowienie kluczy szyfrowania transmisji

To moment, w którym sieć przechodzi z trybu „otwartego” do „bezpiecznego” – dane są szyfrowane i chronione przed podsłuchem

Etapy bezpieczeństwa (warstwa 2):

- Asocjacja – urządzenie zostaje przyjęte do sieci (bez szyfrowania)
- Uwierzytelnienie (Authentication) – weryfikacja tożsamości użytkownika/urządzenia
- Szyfrowanie (Encryption) – generacja i wymiana kluczy (np. WPA2 4-Way Handshake)
- Ochrona transmisji – ruch danych szyfrowany AES-CCMP (WPA2) lub AES-GCMP (WPA3)

507

Bezprzewodowe sieci lokalne – etapy połączenia

4. Uwierzytelnianie (Authentication / Security Handshake)

To właściwy etap bezpieczeństwa – ustanowienie kluczy szyfrowania transmisji

Typ sieci Wi-Fi	Metoda uwierzytelniania	Mechanizm szyfrowania	Charakterystyka / Zastosowanie
Open / Captive Portal	brak (lub logowanie HTTP po połączeniu)	brak szyfrowania ramek	sieci publiczne (hotele, kawiarnie, uczelnie) – niski poziom bezpieczeństwa
WPA2-PSK (Personal)	hasło sieciowe (Pre-Shared Key)	4-Way Handshake → klucz PTK (Pairwise Transient Key)	sieci domowe i małe biura, łatwe w konfiguracji, podatne na ataki słownikowe
WPA2-Enterprise (802.1X)	serwer RADIUS, protokoły EAP / PEAP / TLS	dynamiczne klucze sesji (PMK, PTK, GTK)	sieci korporacyjne, uczelnie, instytucje – wysoka kontrola i logowanie
WPA3-SAE (Simultaneous Authentication of Equals)	wymiana kluczy oparta na Diffie-Hellman (ECDH)	AES-GCMP, odporność na ataki offline i podsłuch	najnowszy standard – sieci nowej generacji, IoT, instytucje publiczne

Bezprzewodowe sieci lokalne – uwierzytelnianie

Sieci otwarte (Open System) — nie używają szyfrowania na poziomie warstwy 2 (MAC)

Dostęp może być kontrolowany dopiero później — przez przeglądarkę WWW (Captive Portal) lub inny system autoryzacji, sieci publiczne (hotele, kawiarnie, lotniska)

Proces uwierzytelniania:

1. Klient łączy się z siecią (SSID, brak hasła)
2. Punkt dostępowy (AP) przyznaje adres IP z DHCP
3. Pierwsze żądanie HTTP użytkownika zostaje przekierowane (HTTP redirect) do strony logowania Captive Portal
4. Użytkownik wpisuje dane logowania (login, hasło, token)
5. Serwer autoryzacyjny (np. RADIUS, captive gateway) weryfikuje danei przekazuje pozwolenie do AP / routera
6. Po autoryzacji ruch użytkownika zostaje przepuszczony do Internetu

Mechanizm zabezpieczeń: Brak szyfrowania ramek 802.11 – transmisja w eterze jest w pełni otwarta, autoryzacja aplikacyjna (HTTP / HTTPS) – tylko na poziomie warstwy 7, dane w sieci lokalnej (ARP, DHCP, DNS) nadal są nieszyfrowane

509

Bezprzewodowe sieci lokalne – uwierzytelnianie

WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key) – najczęściej używany standard w sieciach domowych i małych firmach

Uwierzytelnianie odbywa się poprzez statyczne hasło PSK (Pre-Shared Key), a szyfrowanie – przez mechanizm 4-Way Handshake

Proces uwierzytelniania (4-Way Handshake):

1. Klient → AP: prośba o rozpoczęcie handshake'u
2. AP → Klient: wysyła losowy ANonce (liczbę jednorazową)
3. Klient tworzy własny SNonce i oblicza klucz sesji PTK (Pairwise Transient Key)= funkcja(PSK, ANonce, SNonce, MAC_AP, MAC_Klienta)
4. Obie strony wymieniają MIC (Message Integrity Code), potwierdzając, że znają ten sam klucz PTK
5. Po handshake'u dane są szyfrowane AES-CCMP (Counter Mode + CBC-MAC)

PSK musi być długi i losowy → minimalnie 20+ znaków, handshake można przechwycić i poddać atakowi słownikowemu (offline), brak indywidualnego logowania – wszyscy znają to samo hasło

510

Bezprzewodowe sieci lokalne – uwierzytelnianie

WPA2-Enterprise (IEEE 802.1X + RADIUS) – standard korporacyjny, zapewniający indywidualne uwierzytelnianie użytkowników dynamiczne przydzielanie kluczy szyfrowania

Wykorzystuje serwer RADIUS i protokół EAP (Extensible Authentication Protocol)

Stosowany w sieciach uczelnianych, instytucjach rządowych, bankach

Proces uwierzytelniania (EAP over LAN – EAPOL):

1. Klient nawiązuje połączenie z AP (EAPOL-Start)
2. AP przekazuje dane logowania do serwera RADIUS
3. Serwer weryfikuje użytkownika (np. EAP-TLS, PEAP, TTLS)
4. Po sukcesie generowany jest klucz PMK (Pairwise Master Key)
5. AP inicjuje 4-Way Handshake → tworzy PTK / GTK

Każdy użytkownik ma unikalne klucze szyfrowania – pełna separacja sesji

WPA2-Enterprise zapewnia najwyższy poziom bezpieczeństwa i pełną kontrolę dostępu

Wymaga serwera RADIUS i poprawnej konfiguracji certyfikatów

511

Bezprzewodowe sieci lokalne – uwierzytelnianie

WPA3-SAE (Simultaneous Authentication of Equals) – najnowszy standard (IEEE 802.11-2018), zastępujący WPA2-PSK

Wprowadza mechanizm SAE (Simultaneous Authentication of Equals) – eliminuje ataki słownikowe offline i zapewnia Forward Secrecy, tzw. handshake równych – obie strony uwierzytelniają się symetrycznie, bez przesyłania hasła

Proces uwierzytelniania (SAE Handshake):

1. Klient i AP wymieniają publiczne klucze (commit messages) wykorzystując kryptografię ECDH (Elliptic Curve Diffie-Hellman)
2. Obie strony obliczają wspólny tajny klucz sesji (shared secret) na podstawie hasła
3. Generują klucz PMK (Pairwise Master Key) z tajnego sekretu
4. Następuje potwierdzenie tożsamości (confirm messages)
5. Po pomyślnej wymianie → 4-Way Handshake ustanawia PTK i GTK
6. Dane są szyfrowane AES-GCMP-128 / GCMP-256 (większa szybkość i odporność)

WPA3-SAE – obecnie najbezpieczniejszy standard Wi-Fi, zapewnia odporność na podsłuch, ataki słownikowe i przechwycenie sesji, oferując pełną ochronę kryptograficzną w warstwie 2

512

Bezprzewodowe sieci lokalne – kontrola dostępu

Protokół MAC (Media Access Control) określa sposób, w jaki urządzenia bezprzewodowe współdzielą wspólne medium radiowe – tak, by unikać kolizji i zapewnić sprawiedliwy dostęp do kanału transmisyjnego

W sieciach Wi-Fi wszystkie urządzenia korzystają z jednego pasma częstotliwości, więc dostęp do medium musi być ściśle kontrolowany

Charakterystyka dostępu w Wi-Fi

- Transmisja odbywa się w pasmie radiowym (Half-duplex), które nie pozwala na jednoczesne nadawanie i odbiór (Full-duplex nie jest możliwy w klasycznym 802.11)
- Medium jest współdzielone (shared medium) — każdy host musi sprawdzać, czy kanał jest wolny
- Sieci Wi-Fi korzystają z mechanizmu wielodostępu z unikaniem kolizji – CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*)
- CSMA/CD – Ethernet 802.3 – wykrywanie kolizji
- CSMA/CA – Wi-Fi 802.11 – unikanie kolizji

513

Bezprzewodowe sieci lokalne – unikanie kolizji

- W sieciach radiowych:
- Urządzenie nie może jednocześnie nadawać i odbierać – sygnał własny zagłuszyłby odbiór
- Kolizje nie są bezpośrednio wykrywalne, ponieważ:
 - nie wiadomo, czy sygnał nie dotarł z powodu kolizji, tłumienia czy zakłóceń
 - urządzenia mogą być poza zasięgiem wzajemnym (hidden node problem)
 - kanał radiowy ma zmienną charakterystykę propagacji (odbicia, wielodrożność)

Detekcja kolizji (CD) wymaga ciągłego nasłuchu własnej transmisji — w radiu to fizycznie niemożliwe

802.11 stosuje mechanizm unikania kolizji (CA) oparty na nasłuchu kanału i rezerwacji czasu transmisji

514

Bezprzewodowe sieci lokalne – unikanie kolizji

CSMA/CA to protokół dostępu wielodostępowego, który minimalizuje ryzyko kolizji ramek w środowisku bezprzewodowym

Ponieważ urządzenia Wi-Fi nie mogą wykrywać kolizji (jak w CSMA/CD), protokół unika ich poprzez:

- nasłuchiwanie medium przed nadawaniem
- odczekiwanie losowego czasu (backoff)
- opcjonalną rezerwację kanału (RTS/CTS)
- potwierdzenie odbioru (ACK)

Dzięki CSMA/CA wiele urządzeń może współdzielić to samo pasmo radiowe bez chaosu transmisji

515

Bezprzewodowe sieci lokalne – unikanie kolizji

1. Nasłuchiwanie medium (Carrier Sense)

Każda stacja Wi-Fi (STA)

- nasłuchuje kanału radiowego, aby sprawdzić, czy jest on zajęty
- sprawdza poziom sygnału (RSSI) i analizuje, czy inne urządzenie nadaje
- wykorzystuje do tego fizyczną warstwę, która informuje o stanie kanału (Clear Channel Assessment – CCA)

Jeśli kanał jest zajęty → transmisja zostaje odroczone

516

Bezprzewodowe sieci lokalne – unikanie kolizji

2. Okres ciszy i priorytety czasowe – DIFS i SIFS

- zanim jakkolwiek stacja zacznie nadawać, musi odczekać określony interwał czasowy po zakończeniu poprzedniej transmisji
- SIFS – Short Interframe Space (Krótka przerwa międzyramkowa) - najkrótszy czas przerwy między dwiema powiązаныmi ramkami, zastosowanie SIFS: odpowiedź (np. ACK lub CTS) musi zostać wysłana natychmiast, zanim inne stacje zdążą zareagować
- DIFS – Distributed Interframe Space (Rozproszona przerwa międzyramkowa) - czas oczekiwania, jaki musi zachować każda stacja przed rozpoczęciem nowej transmisji, zastosowanie DIFS: przed każdą nową transmisją danych (DATA), po wykryciu, że kanał jest wolny przez określony czas, daje pierwszeństwo odpowiedziom typu ACK/CTS (wysyłanym po SIFS) i dopiero potem pozwala innym stacjom rozpocząć rywalizację o medium

517

Bezprzewodowe sieci lokalne – unikanie kolizji

2. Okres ciszy i priorytety czasowe – DIFS i SIFS

RÓŻNE STANDARDY - RÓŻNE CZASY

Standard	SIFS	DIFS
Wi-Fi 4 (b/g)	10μs	50μs
Wi-Fi 5 (a)	16μs	34μs
Wi-Fi 6 (ax)	16μs	34μs

Najpopularniejsze:

SIFS = 10μs – krótka pauza dla WAŻNYCH ramek

DIFS = 50μs – dłuższa pauza dla NORMALNYCH ramek

518

Bezprzewodowe sieci lokalne – unikanie kolizji

3. Backoff – losowe opóźnienie transmisji

- Jeśli kanał jest zajęty, urządzenie losuje czas opóźnienia (backoff time) z przedziału:
 $0 \dots (CW - 1)$, gdzie CW (Contention Window) to okno rywalizacji (np. 0–15 slotów)

Mechanizm:

- licznik backoffu odlicza w dół tylko, gdy kanał jest wolny
- jeśli w trakcie odliczania ktoś inny zacznie nadawać → licznik się zatrzymuje
- po zwolnieniu medium licznik jest kontynuowany
- gdy osiągnie 0 → stacja rozpoczyna nadawanie

Dzięki backoffowi różne urządzenia losują inne momenty startu – zmniejsza to prawdopodobieństwo kolizji

519

Bezprzewodowe sieci lokalne – unikanie kolizji

4. Rezerwacja medium – RTS/CTS

- w celu uniknięcia problemów ukrytych węzłów (Hidden Node Problem), stacje mogą użyć mechanizmu RTS/CTS (Request to Send / Clear to Send)
- sekwencja:
 1. Nadawca wysyła ramkę RTS (Request to Send) – prośbę o zgodę na nadawanie.
 2. Odbiorca (np. Access Point) odpowiada CTS (Clear to Send) – przydziela kanał na określony czas.
 3. Wszystkie inne stacje, które usłyszą CTS, wstrzymują swoje transmisje (NAV – Network Allocation Vector)

To rodzaj „rezerwacji kanału” – stacja ma zagwarantowany dostęp do medium przez ustalony czas

520

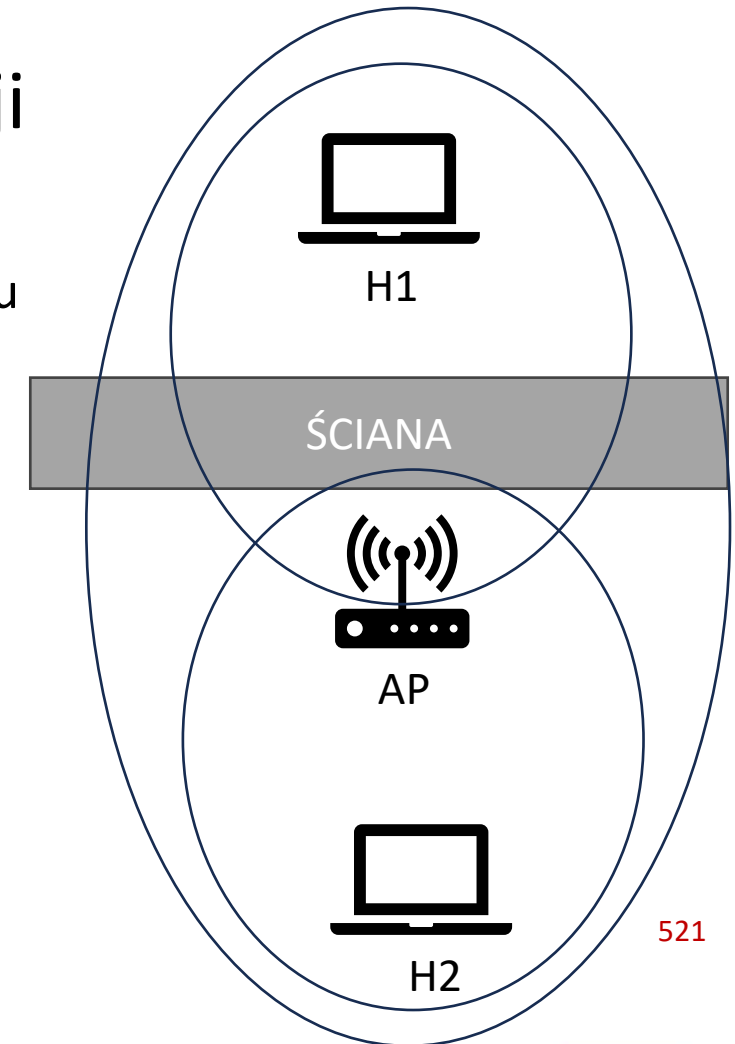
Bezprzewodowe sieci lokalne – unikanie kolizji

4. Rezerwacja medium – RTS/CTS (problem ukrytych węzłów):

- hosty H1 i H2 mogą znajdować się poza zasięgiem wzajemnego odbioru sygnału, ale w zasięgu wspólnego punktu dostępowego (AP)
- nie słyszą nawzajem swoich transmisji — nie wiedzą, że medium jest zajęte
- efekt: kolizje ramek w punkcie dostępowym, mimo że każda stacja uważa, że kanał jest wolny

Rozwiązanie – mechanizm RTS/CTS:

1. Host H1 przed nadawaniem wysyła RTS do AP
2. AP odpowiada CTS, które słyszą wszystkie hosty w zasięgu (H1 i H2)
3. Hosty, które odbiorą CTS, wstrzymują transmisję (NAV = czas)
4. Host H1 ma zarezerwowany kanał na czas przesyłania danych



Bezprzewodowe sieci lokalne – unikanie kolizji

5. Transmisja danych (DATA)

- po uzyskaniu dostępu do medium stacja wysyła dane:
 - ramka danych (DATA) zawiera identyfikatory MAC nadawcy i odbiorcy, numer sekwencyjny oraz dane użytkowe
 - odbiorca (np. AP) buforuje ramkę i przygotowuje potwierdzenie

6. Potwierdzenie odbioru – ACK (Acknowledgment)

- odbiorca (AP lub inna stacja) wysyła **ramkę ACK** po czasie **SIFS**
ACK potwierdza, że ramka została poprawnie odebrana i zdekodowana
- brak ACK → retransmisja po kolejnym okresie backoff

7. Retransmisja (w razie braku ACK)

- jeśli nadawca nie otrzyma ACK w określonym czasie:
 - przyjmuje, że nastąpiła kolizja lub zakłócenie
 - zwiększa okno rywalizacji CW (np. 2× poprzednia wartość)
 - ponownie losuje czas backoffu i próbuje nadać ponownie

Bezprzewodowe sieci lokalne – ramka IEEE 802.11

Podobieństwo do ramki ethernetowej 802.3 – specyficzne pola dla łączności bezprzewodowej

2	2	6	6	6	2	6	0-2312	2
Kontrola ramki	Okres	Adres 1	Adres 2	Adres 3	Numer sekwencyjny	Adres 4	Treść	CRC

2	2	4	1	1	1	1	1	1	1	1
Wersja protokołu	Typ	Podtyp	Do PD	Od PD	Więcej fragmentów	Ponowna prośba	Zarządzanie zasilaniem	Więcej danych	WEP	Zarezerwowane

523

Bezprzewodowe sieci lokalne – ramka IEEE 802.11

Opisy pól:

Kontrola ramki – określa typ ramki:

- Ramki zarządzające (typ 00) – zapytania, odpowiedzi, Beacon, zerwania, uwierzytelnienie
- Ramki kontroli (typ 01) – RTS, CST, ACK, tryb oszczędzania energii, bez rywalizacji dostępu (CF)
- Ramki danych (typ 01) – dane, brak danych

Okres – określa:

- Długość trwania rezerwacji kanału – ustawia NAV (Network Allocation Vector) – monitorowany przez wszystkie stacje
- Wspomaga zarządzanie energią (PS-poll)
- Wspomaga przesyłanie danych bez rywalizacji (gdy stacja nie otrzymała ramki Beacon)

Pola adresowe:

Adresowanie multicast i unicast

Pozwalają rozróżnić stacje Ethernet i bezprzewodowe

Zwykle wykorzystywane 3 pierwsze: adres docelowy (0 – unicast, 1 – multicast), adres źródłowy, adres odbiornika (BSSID), opcjonalnie 4: adres nadajnika - używany w trybie WDS (most Wi-Fi ↔ Wi-Fi)

524

Bezprzewodowe sieci lokalne – ramka IEEE 802.11

Opisy pól:

Numer sekwencji – numer sekwencji i fragmentacji ramki:

- Wspomaga obsługę fragmentacji
- Przenosi numery sekwencji z warstw wyższych
- Wspomaga wykrywanie zduplikowanych ramek

Treść – dane użytkowe lub ramki zarządzające (Beacon, Auth, Assoc) – w przypadku dużych zakłóceń – mniejsze ramki

CRC – suma kontrolna błędów (jak w Ethernet) – taki sam algorytm, musi być przeliczona ze względu na inną budowę ramki

525

Bezprzewodowe sieci lokalne – ramka IEEE 802.11 vs 802.3

Obszar	Ethernet (802.3)	Wi-Fi (802.11)
Protokół dostępu	CSMA/CD (Collision Detection)	CSMA/CA (Collision Avoidance)
Tryb pracy	Full-duplex	Half-duplex
Liczba adresów	2	Do 4
Rodzaje ramek	Dane	Dane, sterujące, zarządzające
Kontrola błędów	CRC (FCS)	CRC + retransmisje + ACK
Potwierdzenie transmisji	Brak	Obowiązkowe (ACK)
Rezerwacja kanału	Nie	Tak (NAV)
Szyfrowanie	Brak (opcjonalne wyżej, np. IPsec)	Tak (WPA2/WPA3 – bit „Protected Frame”)
Fragmentacja	Warstwa IP	Warstwa MAC
Bezpieczeństwo	Na poziomie aplikacji (TLS/VPN)	Na poziomie MAC (WPA, EAP)

526

Bezprzewodowe sieci lokalne – konfiguracja

1. Analiza wymagań:

- liczba użytkowników i urządzeń (telefony, laptopy, IoT)
- wymagania przepustowości (np. 4K video, VoIP, przeglądanie www)
- zasięg — liczba i układ pomieszczeń
- środowisko (dom, biuro, hala, uczelnia)

2. Wybór pasma częstotliwości

Standard	Pasmo	Prędkość teoretyczna	Zastosowanie
802.11n (Wi-Fi 4)	2.4 / 5 GHz	do 600 Mb/s	domowe sieci
802.11ac (Wi-Fi 5)	5 GHz	do 3.5 Gb/s	biura, multimedia
802.11ax (Wi-Fi 6/6E)	2.4 / 5 / 6 GHz	do 9.6 Gb/s	gęste sieci, IoT
802.11be (Wi-Fi 7)	2.4 / 5 / 6 GHz	> 30 Gb/s	przyszłościowe rozwiązania

527

Bezprzewodowe sieci lokalne – konfiguracja

3. Kanały i ich rozmieszczenie

- Unikać nakładania się kanałów (w 2.4 GHz używać 1, 6, 11)
- W 5 GHz kanały są niepokrywające się – można dobrać dynamicznie

4. Szyfrowanie i bezpieczeństwo

- WPA3 – najlepsze, aktualny standard bezpieczeństwa
- WPA2 – używać tylko gdy urządzenia nie obsługują WPA3
- Unikać WEP / otwartych sieci

5. Nazwa sieci (SSID)

- Krótka, jednoznaczna, bez danych osobowych (np. „LabWiFi”, nie „JanKowalskiWiFi”)
- Można rozdzielić SSID na różne VLAN-y (np. WiFi-Student, WiFi-Admin)

528

Bezprzewodowe sieci lokalne – konfiguracja

6. Moc nadawcza i zasięg

- Zbyt duża moc → interferencje i przeciążenie kanału
- Zbyt mała moc → martwe strefy
- Dla domów zwykle 15–20 dBm, dla biur 10–15 dBm

7. DHCP i adresacja

- Router rozdaje adresy z określonej puli
- Warto zarezerwować adresy statyczne dla AP / serwerów

8. VLAN-y i segmentacja sieci

- Oddziel sieć dla gości, pracowników i urządzeń IoT
- Izolacja ruchu → większe bezpieczeństwo i stabilność

529

Bezprzewodowe sieci lokalne – konfiguracja przykład

Router: TP-Link Archer AX55 Pro

Zastosowanie: 4K streaming, gry online, Internet

Dom: 3 pomieszczenia, ściany z cegły / betonu

Urządzenia: TV 4K, konsola, 2 laptopy, 3 smartfony

Cel: wysoka prędkość, niski ping, stabilny zasięg w całym mieszkaniu

Standard: IEEE 802.11ax (Wi-Fi 6) - duża przepustowość (do 9.6 Gb/s), niższe opóźnienia (gry online), lepsza obsługa wielu urządzeń (OFDMA, MU-MIMO)

Zalecane pasma: Dual Band (2.4 + 5 GHz) aktywne jednocześnie

Rozmieszczenie routera: centralne miejsce w mieszkaniu, najlepiej w środkowym pokoju, nie za meblami ani w rogu, unikać mikrofalówek i metalowych powierzchni

530

Bezprzewodowe sieci lokalne – konfiguracja przykład

Kanały i szerokość pasma: 2.4 GHz → kanały 1 / 6 / 11, 5 GHz → *Auto* lub ręcznie,

- Szerokość pasma:
 - 2.4 GHz → 20/40 MHz – stabilność, mniejsze zakłócenia
 - 5 GHz → 80 MHz (dla gier i 4K) – wysoka przepustowość, idealne do 4K/gier

SSID: DomWiFi_5G / DomWiFi_2G, Hasło: min. 12 znaków, np. *MojeWiFi_2025!*

Szyfrowanie: WPA3-Personal

WPS – wyłączony, firmware – zaktualizowany

DHCP: włączony, zakres: 192.168.0.100–199

rezerwacje: TV – 192.168.0.101, konsola – 192.168.0.102, laptop – 192.168.0.103

531

Bezprzewodowe sieci lokalne – konfiguracja przykład

QoS i priorytety: włącz QoS (Quality of Service):

priorytet „High” dla: konsoli do gier, TV (4K streaming),laptopa

priorytet „Normal/Low” dla: pozostałe urządzenia

Zasięg i moc: Transmit Power: Medium / High

Sprawdź zasięg w 3 pomieszczeniach:

Salon: -40 dBm (idealnie)

Gabinet: -55 dBm (OK)

Sypialnia: -65 dBm (granicznie, można dodać repeater)

532

Dziękuję za uwagę

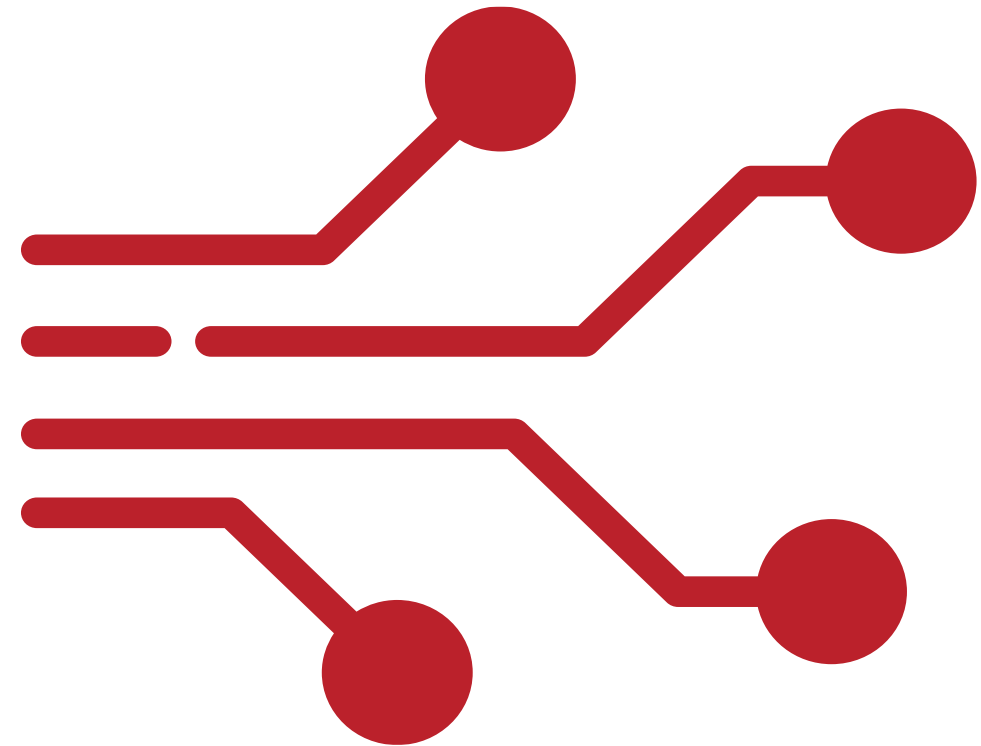
Treści programowe:

- Analiza ruchu sieciowego
- Narzędzia do analizy: Wireshark, tcpdump – podstawowe zastosowania
- Diagnostyka połączeń: ping, traceroute, netstat
- Identyfikacja i rozwiązywanie problemów sieciowych



534

Analiza ruchu sieciowego - narzędzia



535

Analiza ruchu sieciowego

Cel analizy ruchu sieciowego

Zrozumienie, co dzieje się w sieci:

- identyfikacja błędów transmisji
- rozwiązywanie problemów z połączeniem
- wykrywanie przeciążeń i anomalii
- analiza protokołów (Ethernet, IP, TCP, UDP, HTTP itd.)
- kontrola bezpieczeństwa i audyt ruchu

536

Analiza ruchu sieciowego

Ruch sieciowy = ciąg ramek, pakietów i segmentów przesyłanych między urządzeniami, każdy pakiet zawiera:

- nagłówek (adresy MAC, IP, porty, numery sekwencji)
- dane
- sumy kontrolne

Poziom

Warstwa 2

Warstwa 3

Warstwa 4

Warstwa 7

Co analizujemy

ramki Ethernet

pakiety IP

segmenty TCP/UDP

dane aplikacji

Przykład

adresy MAC

adresy źródłowe i docelowe

numery portów

HTTP, DNS, SMTP, itp.

537

Analiza ruchu sieciowego

Narzędzia do analizy ruchu - dwa najpopularniejsze:

Wireshark – graficzne narzędzie do przechwytywania i analizy pakietów:

<https://www.wireshark.org/>

tcpdump – konsolowe narzędzie do przechwytywania i filtrowania ruchu

<https://www.tcpdump.org/>

538

Analiza ruchu sieciowego - Wireshark

Wireshark – darmowy, open-source’owy analizator pakietów sieciowych

Pozwala na:

- przechwytywanie i analizę pakietów w czasie rzeczywistym
- filtrowanie ruchu po protokołach, adresach, portach
- wielowymiarową analizę ruchu sieciowego
- wizualizację struktury pakietu (od warstwy 2 do 7)
- zapis i odczyt plików .pcap (np. z tcpdumpa)

Obsługuje setki protokołów: Ethernet, Wi-Fi, IP, TCP, UDP, ARP, DNS, HTTP, HTTPS, ICMP, DHCP, itp.

539

Analiza ruchu sieciowego - Wireshark

Instalacja i uruchomienie

- Dostępny dla **Windows, macOS, Linux, UNIX**
- Pobierz ze strony: <https://www.wireshark.org/>
- Wymaga sterownika przechwytywania: Npcap (Windows) lub libpcap (Linux)
- Uruchamiaj z uprawnieniami administratora, by przechwytywać cały ruch

Wireshark instaluje też narzędzie konsolowe tshark – tekstowy odpowiednik

540

Analiza ruchu sieciowego - Wireshark

Instalacja Windows 11:

1. Wybierz przycisk Download Now
2. Wybierz właściwą wersję instalacyjną: Windows x64 Installer
3. Uruchom instalator – zaznacz instalator Npcap – niezbędny! USBPcap – jeżeli chcesz analizować USB
4. Przeczytaj i zaakceptuj zgody
5. Uruchom jako Administrator

Sterownik: Npcap

Format pliku: .pcapng, pcap

541

Analiza ruchu sieciowego - Wireshark

Instalacja Ubuntu:

Program znajduje się w repozytoriach

```
sudo apt install wireshark -y
```

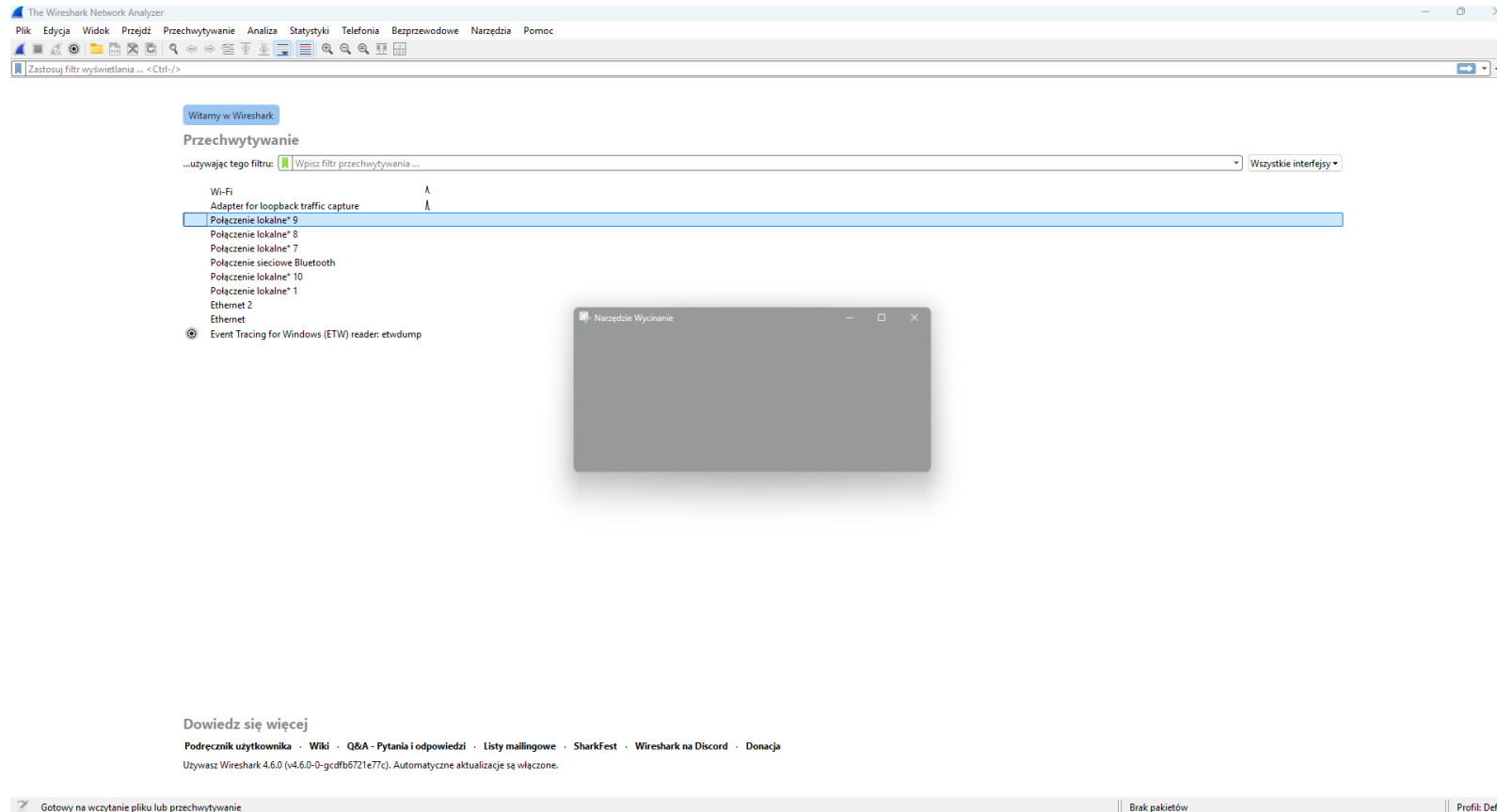
Czy nieuprzywilejowani użytkownicy powinni mieć możliwość przechwytywania pakietów? - Jeśli chcesz móc korzystać z Wiresharka bez używania sudo, wybierz "Tak" (Yes), W przeciwnym wypadku, tylko użytkownik root będzie mógł przechwytywać pakiety

Jeśli wybrałeś "Tak", musisz dodać swojego użytkownika do grupy wireshark:

```
sudo usermod -aG wireshark $USER
```

Wymagane wylogowanie i ponowne zalogowanie

Analiza ruchu sieciowego - Wireshark



543

Analiza ruchu sieciowego - Wireshark

Po uruchomieniu zobaczysz listę interfejsów sieciowych (np. eth0, wlan0, lo)

- Kliknij dwukrotnie interfejs, który chcesz analizować (np. Wi-Fi → wlan0)
- Wireshark zacznie przechwytywanie pakietów w czasie rzeczywistym
- Każdy przechwycony pakiet pokazuje się w tabeli:
- No. – numer pakietu
- Time – czas od rozpoczęcia przechwytywania
- Source – adres źródłowy
- Destination – adres docelowy
- Protocol – użyty protokół (np. TCP, UDP, HTTP, DNS)
- Info – krótki opis zdarzenia

544

Analiza ruchu sieciowego - Wireshark

Filtry wyświetlania (Display Filters):

Cel

Tylko ruch HTTP

Tylko ruch DNS

Tylko TCP

Tylko UDP

Tylko pakiety z IP źródłowym 192.168.1.10

Tylko pakiety do IP 8.8.8.8

Ruch z/do portu 80

Ruch HTTP zawierający "login,,

Filtr

http

dns

tcp

udp

ip.src == 192.168.1.10

ip.dst == 8.8.8.8

tcp.port == 80

http contains "login"

545

Analiza ruchu sieciowego - Wireshark

Aby zapisać przechwycone dane:

- Wybierz: Plik → Zapisz jako
- Format domyślny: .pcapng (czytelny dla Wiresharka i innych narzędzi, np. tshark)

Analiza sesji i statystyki

Menu Statystyki zawiera przydatne narzędzia:

- Szczegóły pliku przechwytywania – podstawowe informacje o aktualnym pliku .pcapng
- Rozwiązane adresy – lista wszystkich przetłumaczonych adresów IP i MAC
- Hierarchia protokołów – statystyczne drzewo protokołów
- Conversations – lista wszystkich „rozmów” (połączeń) między adresami IP
- Punkty końcowe – lista wszystkich indywidualnych urządzeń (adresów) występujących w przechwyceniu
- Wykresy we./wy. – wykresy aktywności sieciowej w czasie

546

Analiza ruchu sieciowego - tcpdump

tcpdump – narzędzie wiersza poleceń do przechwytywania i analizy ruchu sieciowego

Działa podobnie do Wiresharka, ale:

- działa z konsoli (bez GUI)
- jest lekki i szybki
- idealny do pracy na serwerach lub przy automatycznym logowaniu ruchu

Przechwycone dane można oglądać w terminalu lub zapisać do pliku .pcap i później otworzyć (np. w Wiresharku)

547

Analiza ruchu sieciowego - tcpdump

- Dostępny na platformy uniksowe: **Linux, Solaris, BSD, UNIX**
- Wymaga sterownika przechwytywania: libpcap (Linux)
- Uruchamiaj z uprawnieniami administratora, by przechwytywać cały ruch

Wersja przeniesiona na system Windows – WinDump, współpracuje z biblioteką WinPcap:

<https://www.winpcap.org/windump/>

548

Analiza ruchu sieciowego - tcpdump

Instalacja Ubuntu:

Program znajduje się w repozytoriach, jeżeli nie jest zainstalowany:

```
sudo apt install tcpdump -y
```

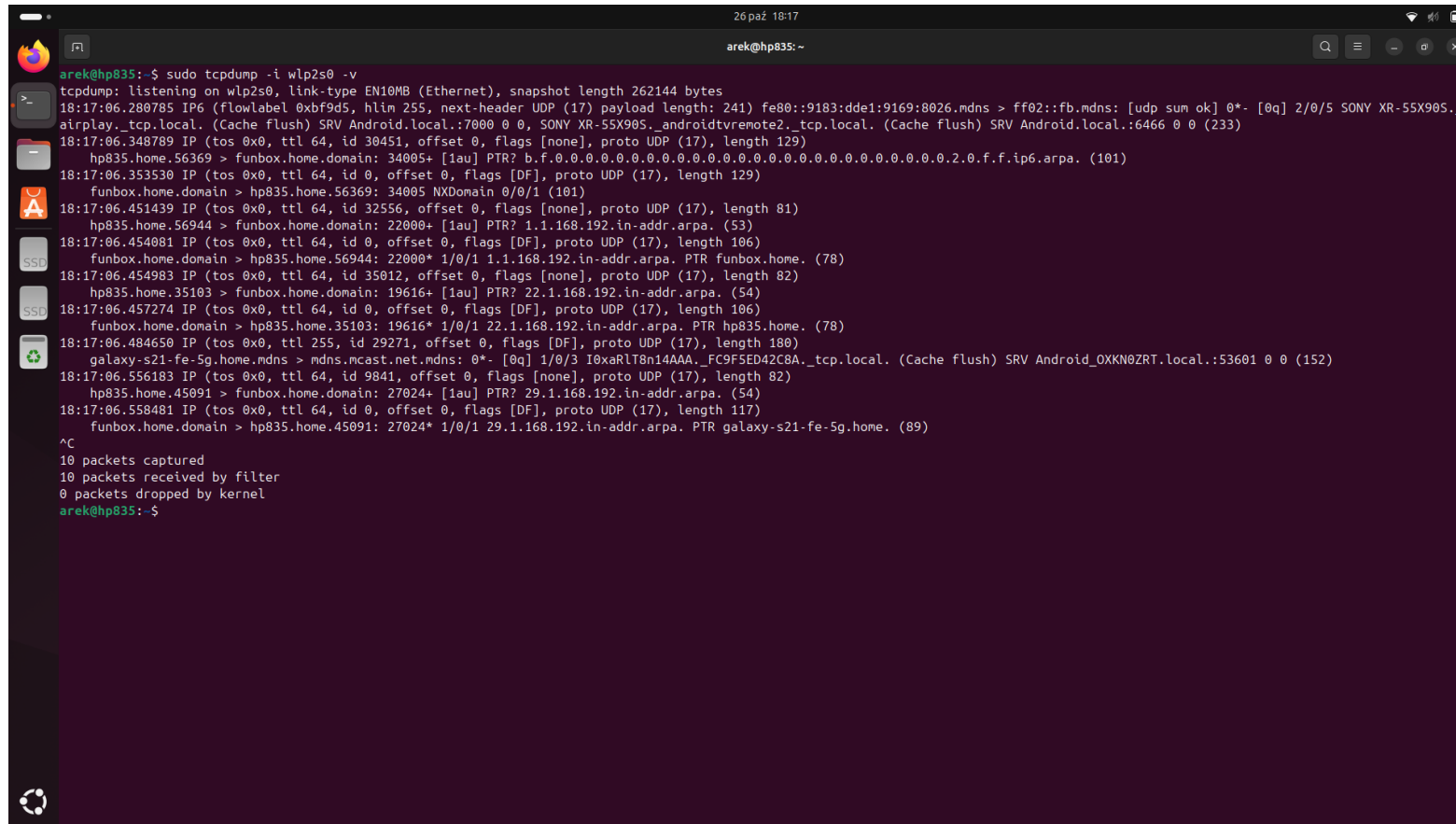
Uruchamiany w środowisku konsolowym jako super użytkownik (sudo)

Podstawowa składnia:

```
sudo tcpdump [opcje] [filtr]
```

Definicje filtrów – podobnie jak w Wireshark

549



Analiza ruchu sieciowego - tcpdump

Podstawowa składnia:

```
sudo tcpdump -D – lista wszystkich interfejsów
```

```
sudo tcpdump -i wlan0 – przechwytuje pakiety w czasie rzeczywistym korzystając z interfejsu wlan0
```

```
Ctrl + c – zatrzymuje działanie
```

```
sudo tcpdump -i eth0 -w capture.pcap – zapis do pliku capture.pcap
```

```
tcpdump -r capture.pcap – odczyt zapisanego pliku
```

```
sudo tcpdump -n – tylko nagłówki – nie tłumaczy adresów IP na adresy hostów
```

```
sudo tcpdump -i eth0 -c 10 – ogranicza zapis do liczby pakietów = 10
```

```
sudo tcpdump -i eth0 -w /tmp/capture -C 10 -W 5 – maksymalny rozmiar pliku = 10MB, tylko ostatnie 5 plików
```

```
sudo tcpdump -i eth0 tcp – filtrowanie według protokołu (tcp, udp, icmp, dhcp, itd.)
```

```
sudo tcpdump -i eth0 host 192.168.1.10 – filtrowanie według adresu IP (host, src, dst)
```

```
sudo tcpdump -i eth0 tcp port 443 – filtrowanie według portu
```

551

Analiza ruchu sieciowego - tcpdump

`sudo tcpdump -i eth0 -A -s 0 tcp port 80` – przechwytywanie tylko pakietów HTTP, w postaci ASCII (-A), pełnej długości (-s 0)

`sudo tcpdump net 192.168.1.0/24` – przechwytywanie pakietów w podsieci

Przykładowe połączenia tcpdump z poleceniami powłoki:

`sudo tcpdump -i eth0 icmp and host 8.8.8.8` – przechwytuje tylko pakiety icmp z/do danego hosta (np. ping)

`sudo tcpdump -n -i eth0 | grep 8.8.8.8` – pokazuje tylko pakiety związane z DNS Googla

`sudo tcpdump -i eth0 tcp | wc -l` – zlicza ile pakietów przechwycono

`sudo timeout 10 tcpdump -i eth0 icmp -w capture.pcap` – tcpdump automatycznie się zatrzyma po 10 sekundach

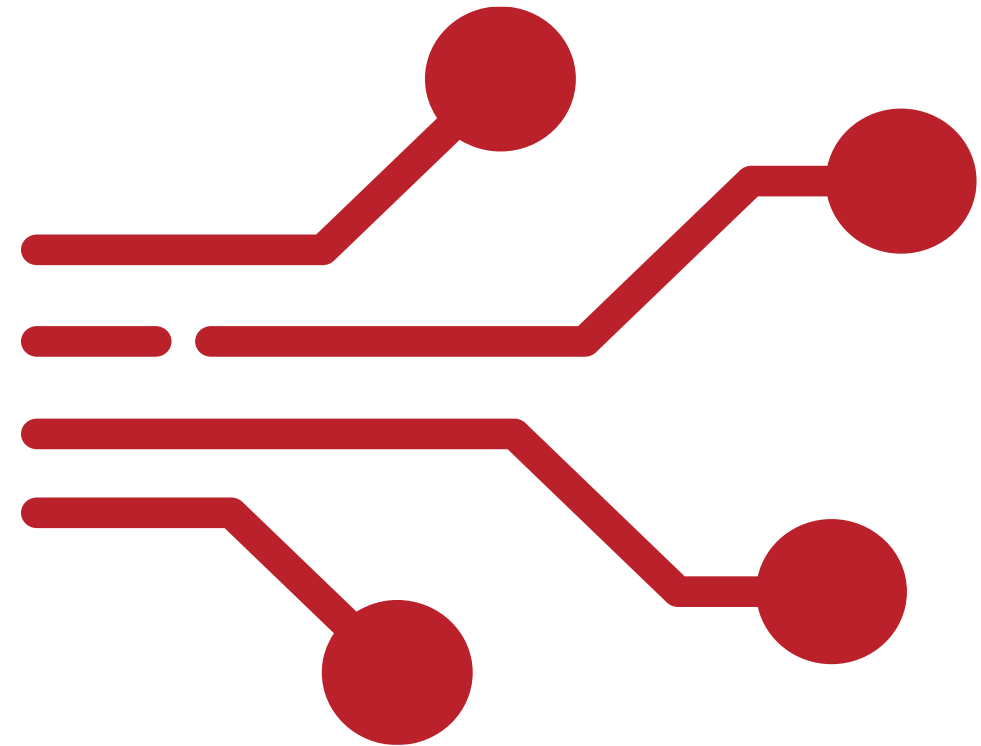
`sudo timeout 30 tcpdump -i eth0 icmp -c 100` – automatyczne zatrzymanie po 10 sekundach lub 100 pakietach (co pierwsze)

`sudo tcpdump -i eth0 -w - | gzip > /tmp/capture.pcap.gz` – zapis skompresowany do pliku

`sudo tcpdump -i eth0 -w - | ssh user@remotehost "cat > ~/capture_$(hostname).pcap"` – wysyłanie przechwytywania na zdalny host przez SSH (stream pcap)

552

Diagnostyka połączeń: ping, traceroute, netstat



553

Diagnostyka połączeń

Narzędzia konsolowe dostępne zarówno w Ubuntu Linux jak i Windows 11:

ping (Ubuntu/Windows) – test osiągalności hosta

tracert / traceroute (Ubuntu/Windows) – śledzenie trasy pakietów

netstat (Ubuntu/Windows) – analiza połączeń i portów

554

Diagnostyka połączeń - ping

Zadanie: Sprawdza, czy host jest osiągalny (ICMP Echo Request / Reply)

System	Polecenie	Uwagi
Ubuntu	ping -c 4 8.8.8.8	-c = liczba pakietów, Ctrl + C - przerywa
Windows 11	ping -n 4 8.8.8.8	-n = liczba pakietów, kończy automatycznie

Interpretacja wyniku:

- time= – opóźnienie (RTT)
- TTL – czas życia pakietu (liczba skoków pozostałych)
- packet loss – utracone pakiety

555

Diagnostyka połączeń - ping

Funkcja	Ubuntu / Linux	Windows 11	Uwagi
Liczba wysłanych pakietów	-c <liczba>	-n <liczba>	Najczęstsza różnica — c = count, n = number
Czas między pakietami	-i <sekundy>	-w <milisekundy>	W Linuxie – odstęp między pakietami, w Windows – timeout
Rozmiar pakietu	-s <bajty>	-l <bajty>	W Linuxie – size, w Windows – length
TTL (czas życia pakietu)	-t <wartość>	-i <wartość>	Odwrotnie niż w nazwach 😊
Timeout odpowiedzi	-W <sekundy>	-w <milisekundy>	Linux: w sekundach; Windows: w ms
Tryb ciągły	ping adres (Ctrl+C żeby przerwać)	ping -t adres	Domyślnie w Linux ciągły, w Windows – trzeba wymusić
DNS reverse lookup (nazwa hosta)	-n (wyłącza)	brak	W Linuxie -n = nie rozwiązuje DNS (szybciej) 556

Diagnostyka połączeń – traceroute/tracert

Zadanie: Pokazuje trasę pakietów do hosta (każdy „hop” = kolejny router)

System	Polecenie	Uwagi
Ubuntu	traceroute 8.8.8.8	Domyślnie UDP, opcje -I (ICMP), -T (TCP)
Windows 11	tracert 8.8.8.8	Używa ICMP Echo Request (zawsze)

Interpretacja:

- każdy wiersz = kolejny skok (router)
- * * * – brak odpowiedzi (np. firewall lub limit TTL)

557

Diagnostyka połączeń – traceroute/tracert

Funkcja	Ubuntu / Linux (traceroute)	Windows 11 (tracert)	Uwagi
Liczba prób na hop	-q <liczba>	-q <liczba>	Działa podobnie
Maksymalna liczba hopów	-m <liczba>	-h <liczba>	m = max TTL (Linux), h = hops (Windows)
Brak rozwiązywania DNS	-n	-d	Linux: -n = no DNS, Windows: -d = don't resolve
Protokół ICMP	-I	(domyślny)	W Windows tracert zawsze używa ICMP
Protokół TCP	-T	brak	Linux potrafi użyć TCP (np. na porcie 80)
Zmiana portu UDP	-p <port>	brak	Tylko Linux
Timeout na odpowiedź	-w <sekundy>	-w <milisekundy>	Linux – sekundy, Windows – ms

558

Diagnostyka połączeń – netstat

Zadanie: Pokazuje aktywne połączenia, porty i trasy routingu

System	Polecenie	Opis
Ubuntu	netstat -tuln	wymaga pakietu net-tools; alternatywa:
	netstat -antp	ss -tuln
Windows 11	netstat -ano	pokazuje PID procesu, adresy lokalne i zdalne

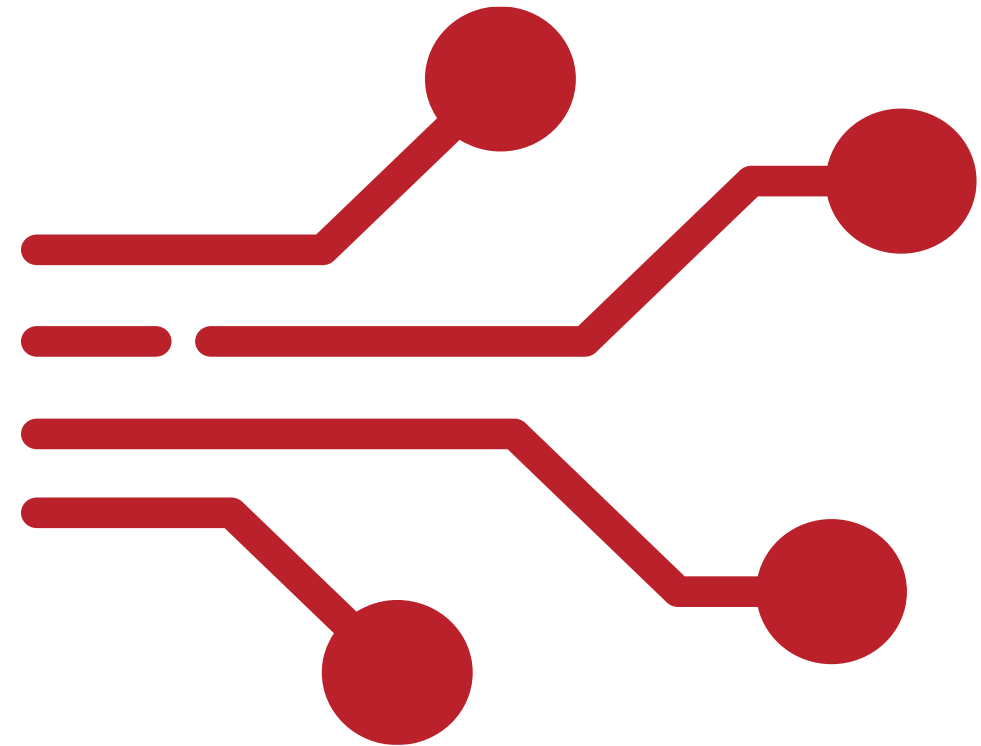
559

Diagnostyka połączeń – netstat

Funkcja	Ubuntu / Linux	Windows 11	Uwagi
Pokaz portów nasłuchujących	<code>-tuln</code>	<code>-a</code>	Linux rozróżnia TCP/UDP (t/u)
Pokaz aktywnych połączeń	<code>-antp</code>	<code>-b lub -o</code>	Linux: p = proces; Windows: b = program, o = PID
Tablica routingu	<code>-r</code>	<code>-r</code>	Identyczne w obu
Statystyki protokołów	<code>-s</code>	<code>-s</code>	Identyczne
Nazwy hostów (DNS)	<code>-n = wyłącz</code>	<code>-n = wyłącz</code>	Tu akurat ta sama opcja
IPv6	<code>-6</code>	<code>-6</code>	Działa w obu
Czas odświeżania (ciągły podgląd)	brak	<code>-t <sekundy></code>	Windows może odświeżać co X sekund
Filtr po PID	automatycznie w <code>-p</code>	<code>-o + tasklist</code>	W Windows wymaga dodatkowego polecenia

560

Identyfikacja i rozwiązywanie problemów sieciowych



561

Identyfikacja i rozwiązywanie problemów

Diagnozowanie sieci to proces wykrywania przyczyn problemów z łącznością lub wydajnością

Celem jest określenie, *gdzie* leży problem – w komputerze użytkownika, routerze, kablu, DNS-ie, czy po stronie dostawcy internetu

W tym module skupiamy się na praktycznym wykorzystaniu narzędzi takich jak:

`ping`, `tracert`, `netstat`, `ip`, Wireshark i `tcpdump`

Zrozumienie ich wyników pozwala na szybsze podejmowanie decyzji naprawczych

Diagnozowanie sieci to nie tylko znajomość komend, ale też umiejętność logicznego łączenia objawów z przyczyną

562

Identyfikacja i rozwiązywanie problemów

Proces diagnozy warto prowadzić metodycznie, według schematu krok po kroku:

Pierwszy etap to identyfikacja objawów – co dokładnie nie działa: przeglądarka, e-mail, cały Internet?

Drugi etap to analiza warstw modelu OSI – od fizycznej po aplikacyjną

Trzeci etap to testy łączności i adresacji (ping, traceroute, ipconfig)

Czwarty – izolacja problemu: czy dotyczy pojedynczego urządzenia, całej sieci, czy konkretnego protokołu

Na końcu – wdrożenie rozwiązania i weryfikacja efektów testami

Taka struktura pozwala uniknąć przypadkowego działania i błędnych wniosków.

563

Identyfikacja i rozwiązywanie problemów

W każdej z siedmiu warstw modelu OSI mogą pojawić się inne rodzaje błędów:

- Na warstwie fizycznej to np. odłączony kabel, przerwany światłowód lub brak sygnału
- W warstwie łącza danych – błędy adresów MAC, kolizje, problemy z kartą sieciową
- W warstwie sieciowej – błędna konfiguracja IP, brak bramy lub błędny routing
- Na warstwie transportowej – blokady portów przez firewall, zbyt duże opóźnienia TCP
- Na poziomie aplikacji – nieprawidłowa konfiguracja DNS, serwera HTTP, czy proxy

Zrozumienie, w której warstwie szukać, znacznie przyspiesza rozwiązanie problemu

564

Identyfikacja i rozwiązywanie problemów

Najczęstsze objawy to całkowity brak dostępu do Internetu lub sporadyczne zrywanie połączenia

Czasami problem objawia się wolnym ładowaniem stron, dużym opóźnieniem w grach lub błędami DNS

W sieciach lokalnych użytkownicy mogą mieć problem z widocznością serwerów lub drukarek

Przy połączeniach zdalnych – zbyt długi czas odpowiedzi (timeout)

Inne objawy to np. komunikaty o konflikcie adresów IP, błędy w DHCP, lub niemożność połączenia z określonym portem

Warto rozróżnić objawy stałe (ciągłe) od okresowych, bo to często wskazuje, czy problem jest fizyczny, czy konfiguracyjny

565

Diagnostyka: Warstwa 1 - Fizyczna

Sprawdzamy, czy urządzenie jest fizycznie podłączone do sieci i aktywne

Błędy na tym etapie to: odłączony kabel, brak sterownika, wyłączona karta sieciowa

```
ip link show → 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ...
```

```
Get-NetAdapter →
```

Name	Status	MacAddress
Ethernet	Up	00-1A-2B-3C-4D-5E

Włączamy adapter, jeżeli nie jest włączony:

```
sudo ip link set eth0 up
```

```
Enable-NetAdapter -Name "Ethernet"
```

- brak błędu = interfejs włączony
- Status zmienia się z Disabled → Up

566

Diagnostyka: Warstwa 2 - łączy danych

Jeśli karta sieciowa działa (warstwa 1), ale:

- nie widzi żadnych innych urządzeń w LAN
- tablica ARP jest pusta
- ping do lokalnego routera nie działa

to znaczy, że ramki Ethernet nie docierają = problem jest na warstwie 2:

- błędny VLAN
- uszkodzony kabel
- zła konfiguracja switcha
- filtracja MAC

567

Diagnostyka: Warstwa 2 - łączy danych

```
ip neigh show → 192.168.0.1 dev eth0 lladdr 00:11:22:33:44:55 REACHABLE
```

```
arp -a          → 192.168.0.1    00-11-22-33-44-55    dynamic
```

Host z IP 192.168.0.1 odpowiedział na ARP → karta działa w warstwie 2

Test komunikacji lokalnej (ping LAN):

```
ping -c 4 192.168.0.1 →
```

```
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1.23 ms
```

```
ping 192.168.0.1 →
```

```
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
```

Odpowiedź oznacza działającą łączność w sieci lokalnej

568

Diagnostyka: Warstwa 3 - Sieciowa

Odpowiada za adresację IP i routing - sprawdzamy adres IP, maskę, bramę i trasy routingu

Adres IP (Linux):

```
ip addr show → inet 192.168.0.105/24 brd 192.168.0.255 ...
```

Brama (Linux):

```
ip route show → default via 192.168.0.1 dev eth0
```

Adres IP (Windows):

```
ipconfig /all → IPv4 Address: 192.168.0.105
```

Brama (Windows):

```
route print → Default Gateway: 192.168.0.1
```

569

Diagnostyka: Warstwa 3 - Sieciowa

Odpowiada za adresację IP i routing - sprawdzamy adres IP, maskę, bramę i trasy routingu

Ping do Internetu po IP (Linux):

```
ping -c 4 8.8.8.8 → time=20.1 ms = połączenie działa
```

Ping do Internetu po IP (Windows):

```
ping 8.8.8.8 time → Reply from 8.8.8.8 = połączenie z Internetem aktywne
```

570

Diagnostyka: Warstwa 4 - Transportowa

Odpowiada za połączenia TCP/UDP - sprawdzamy, czy porty są otwarte i nasłuchujące i ruch jest kierowany prawidłowo

Linux: `netstat -tuln`

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
udp	0	0	0.0.0.0:68	0.0.0.0:*	

tcp ... :22 LISTEN → serwer SSH nasłuchuje na porcie 22

udp ... :68 → klient DHCP działa

0.0.0.0 → port jest dostępny na wszystkich interfejsach

571

Diagnostyka: Warstwa 4 - Transportowa

Odpowiada za połączenia TCP/UDP - sprawdzamy, czy porty są otwarte i nasłuchujące i ruch jest kierowany prawidłowo

Windows: netstat -ano

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1234
UDP	0.0.0.0:68	*:*		520

port 80 → serwer WWW działa

port 68 → klient DHCP

kolumna PID pozwala sprawdzić, która aplikacja korzysta z danego portu (tasklist | find "1234")

572

Diagnostyka: Warstwa 7 - Aplikacyjna

Testujemy działanie protokołów aplikacyjnych - sprawdzenie działania usług (DNS, HTTP, SSH)

Najczęstsze problemy: błędna konfiguracja DNS lub usługi

Sprawdzamy, czy DNS działa i zwraca poprawne adresy IP (Linux/Windows):

```
nslookup google.com →
```

Name: google.pl

Address: 216.58.208.195

DNS odpowiada – rozwiązywanie nazw działa poprawnie

573

Diagnostyka: Warstwa 7 - Aplikacyjna

Objaw	ping 8.8.8.8	ping google.com	nslookup google.com	Diagnoza
✗ Oba nie działają	✗	✗	✗	Brak Internetu (routing)
✗ Działa tylko IP	✓	✗	✗	Problem z DNS
⚠ Działa tylko czasem	✓	⚠	⚠	Niestabilny DNS lub cache
✓ Wszystko działa	✓	✓	✓	DNS i sieć OK

Jeśli działa ping 8.8.8.8, ale nie ping google.com → wina DNS

574

Diagnostyka: Warstwa 7 - Aplikacyjna

Testujemy działanie protokołów aplikacyjnych - sprawdzenie działania usług (DNS, HTTP, SSH)

Najczęstsze problemy: błędna konfiguracja DNS lub usługi

Sprawdzamy, czy działa komunikacja HTTP/HTTPS (Linux/Windows):

```
curl -I http://example.com → HTTP/1.1 200 OK
```

Serwer WWW działa i odpowiada – warstwa aplikacyjna (HTTP) jest poprawna

```
curl -I https://example.com → HTTP/1.1 200 OK
```

```
schannel: SSL/TLS connection renegotiated
```

Połączenie zostało zabezpieczone protokołem TLS — szyfrowanie działa w pełni poprawnie

575

Dziękuję za uwagę

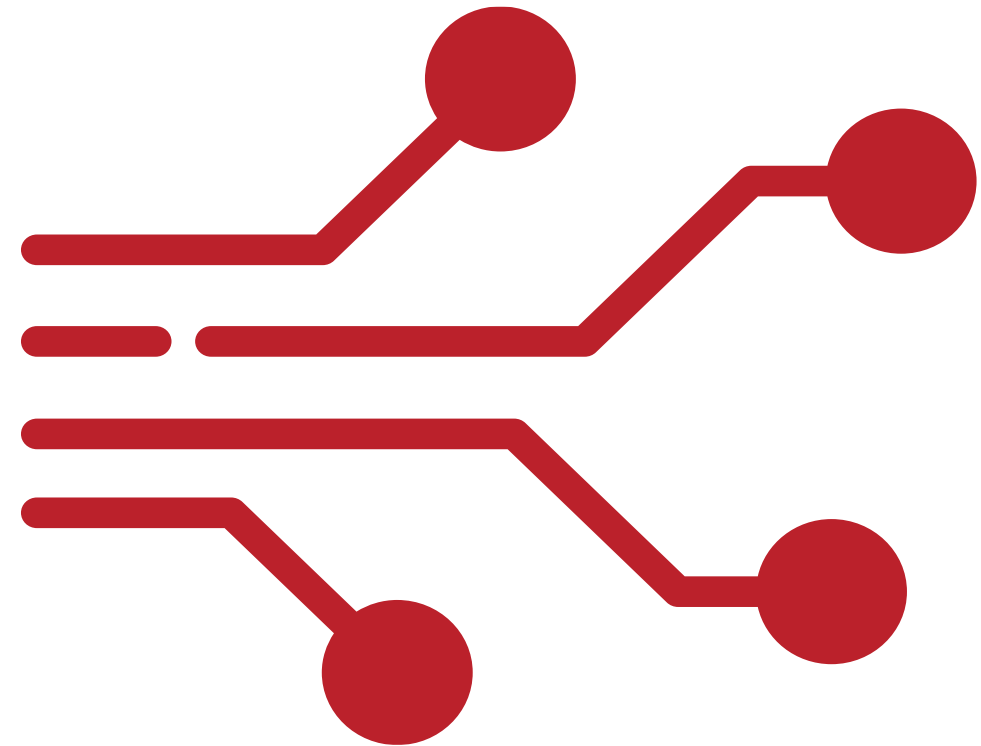
Treści programowe:

- Podstawy bezpieczeństwa sieci komputerowych
- Typowe zagrożenia sieciowe: sniffing, spoofing, ataki DoS, phishing
- Rola firewalli i systemów IDS/IPS w ochronie sieci
- Podstawy szyfrowania danych w sieci (SSL/TLS)
- Dobre praktyki w konfiguracji urządzeń sieciowych



577

Podstawy bezpieczeństwa sieci komputerowych - typowe zagrożenia



578

Podstawy bezpieczeństwa sieci komputerowych

Statystyki: Według raportów Cybersecurity Ventures, w 2025 r. globalne koszty cyberprzestępczości przekroczą 10,5 biliona USD rocznie; ataki sieciowe wzrosły o 30% w porównaniu do 2024 r., z dominacją ransomware i DDoS. W Polsce: Dane NASK wskazują na 20% wzrost incydentów w sektorze publicznym

Konsekwencje: Utrata poufnych danych (np. RODO/GDPR kary do 4% obrotu), przestoje biznesowe (średnio 4,45 mln USD na incydent wg IBM), reputacyjne szkody, ryzyko prawne

579

Modele sieciowe a bezpieczeństwo

Modele sieciowe – każda warstwa ma swoje zadania i inne podatności:

Warstwa fizyczna: przesyłanie bitów przez media transmisyjne (kable, światłowody, fale radiowe)

Zagrożenia: tapping (podśluch), uszkodzenia mechaniczne, zakłócenia

Zabezpieczenia: ekranowanie kabli, szyfrowanie transmisji optycznych, ochrona fizyczna dostępu

580

Modele sieciowe a bezpieczeństwo

Modele sieciowe – każda warstwa ma swoje zadania i inne podatności:

Warstwa łączy danych: komunikacja między sąsiednimi węzłami (adresy MAC)

Zagrożenia: MAC spoofing, ARP poisoning

Zabezpieczenia: Filtrowanie MAC, Dynamic ARP Inspection, segmentacja VLAN

581

Modele sieciowe a bezpieczeństwo

Modele sieciowe – każda warstwa ma swoje zadania i inne podatności:

Warstwa sieciowa: Adresacja IP, routing, zarządzanie ruchem

Zagrożenia: IP spoofing DoS / DDoS Routing attacks

Zabezpieczenia: Firewall, IPsec / VPN, Filtrowanie pakietów

582

Modele sieciowe a bezpieczeństwo

Modele sieciowe – każda warstwa ma swoje zadania i inne podatności:

Warstwa transportowa: Niezawodność połączenia (TCP/UDP)

Zagrożenia: SYN floods, Port scanning Session hijacking

Zabezpieczenia: TLS, Stateful firewalls, Rate limiting

583

Modele sieciowe a bezpieczeństwo

Modele sieciowe – każda warstwa ma swoje zadania i inne podatności:

Warstwa sesyjna: Zarządza sesjami komunikacyjnymi

Zagrożenia: przejęcie sesji, błędne uwierzytelnienie

Zabezpieczenia: SSL/TLS, bezpieczne logowanie

Warstwa prezentacji: Formatuje i szyfruje dane

Zagrożenia: błędy w dekodowaniu, ataki na kryptografię

Zabezpieczenia: sprawdzone biblioteki kryptograficzne

584

Modele sieciowe a bezpieczeństwo

Modele sieciowe – każda warstwa ma swoje zadania i inne podatności:

Warstwa aplikacyjna: Interfejs użytkownika (HTTP, FTP, SMTP itd.)

Zagrożenia: SQL injection, XSS, CSRF, Malware

Zabezpieczenia: WAF (Web Application Firewall), Walidacja danych wejściowych, Regularne aktualizacje aplikacji

585

Podstawowe pojęcia bezpieczeństwa sieci

Triada **CIA** – podstawa bezpieczeństwa:

1. Poufność (**Confidentiality**):

Dane dostępne tylko dla uprawnionych

Przykład: szyfrowanie transmisji (SSL/TLS, VPN)

2. Integralność (**Integrity**):

Dane nie mogą być zmieniane bez autoryzacji

Przykład: użycie funkcji skrótu (hashing: MD5, SHA-256)

3. Dostępność (**Availability**):

Systemy i dane muszą być dostępne, gdy są potrzebne

Przykład: redundancja, load balancing, ochrona przed DoS/DDoS

586

Podstawowe pojęcia bezpieczeństwa sieci

AAA – Authentication, Authorization, Accounting

1. Autentykacja (Authentication):

Sprawdzenie tożsamości użytkownika

Przykład: hasło, karta, biometryka, 2FA / MFA

2. Autoryzacja (Authorization):

Określenie, do czego użytkownik ma dostęp

Przykład: uprawnienia w systemie, kontrola ról (RBAC)

3. Audyt / Rozliczalność (Accounting):

Rejestrowanie działań użytkownika – kto, co, kiedy zrobić

Przykład: logi systemowe, RADIUS, TACACS+

587

Ewolucja bezpieczeństwa sieci

Lata 1980–1990: Początki bezpieczeństwa IT:

Proste zabezpieczenia oparte na hasłach, brak szyfrowania ruchu sieciowego, zaufanie w sieciach lokalnych (LAN)

Lata 1990–2000: Narodziny firewalli:

Pojawienie się pierwszych zapór sieciowych (np. Check Point Firewall-1), segmentacja sieci i kontrola ruchu, wzrost znaczenia polityk bezpieczeństwa

Lata 2000–2010: Monitorowanie i detekcja zagrożeń:

Rozwój IDS/IPS (Intrusion Detection/Prevention Systems) – np. Snort, wzrost liczby ataków z Internetu, początki automatyzacji w reakcji na incydenty

Lata 2010–2020: Chmura i mobilność:

Pojawia się cloud security i ochrona SaaS, wzrost znaczenia zarządzania tożsamością (IAM), początki modelu Zero Trust (weryfikuj zawsze, nigdy nie ufaj domyślnie)

Lata 2020–2025: Era sztucznej inteligencji i zaufania zerowego:

AI/ML w detekcji zagrożeń (behavioral analysis, SIEM z ML), Zero Trust Architecture (NIST SP 800-207) jako standard, większy nacisk na ochronę danych w ruchu, chmurze i na brzegu sieci

588

Ewolucja bezpieczeństwa sieci

Lata 1980–1990: Początki bezpieczeństwa IT:

Proste zabezpieczenia oparte na hasłach, brak szyfrowania ruchu sieciowego, zaufanie w sieciach lokalnych (LAN)

Lata 1990–2000: Narodziny firewalli:

Pojawienie się pierwszych zapór sieciowych (np. Check Point Firewall-1), segmentacja sieci i kontrola ruchu, wzrost znaczenia polityk bezpieczeństwa

Lata 2000–2010: Monitorowanie i detekcja zagrożeń:

Rozwój IDS/IPS (Intrusion Detection/Prevention Systems) – np. Snort, wzrost liczby ataków z Internetu, początki automatyzacji w reakcji na incydenty

Lata 2010–2020: Chmura i mobilność:

Pojawia się cloud security i ochrona SaaS, wzrost znaczenia zarządzania tożsamością (IAM), początki modelu Zero Trust (weryfikuj zawsze, nigdy nie ufaj domyślnie)

Lata 2020–2025: Era sztucznej inteligencji i zaufania zerowego:

AI/ML w detekcji zagrożeń (behavioral analysis, SIEM z ML), Zero Trust Architecture (NIST SP 800-207) jako standard, większy nacisk na ochronę danych w ruchu, chmurze i na brzegu sieci

Wstęp do zagrożeń sieciowych

Czym są zagrożenia sieciowe?

- Każde działanie, które narusza poufność, integralność lub dostępność danych
- Zagrożenia mogą pochodzić z zewnątrz (external) lub wewnątrz organizacji (insider)
- Niektóre są ciche i trudne do wykrycia, inne – agresywne i destrukcyjne

590

Klasyfikacja zagrożeń sieciowych

Pasywne (Passive)

- Obserwacja ruchu bez ingerencji
- Celem jest **pozyskanie informacji**, nie uszkodzenie systemu
- Przykłady: Sniffing (podśluchiwanie pakietów w sieci)

Aktywne (Active)

- Atakujący modyfikuje, przerywa lub przeciąża komunikację
- Celem jest **zakłócenie** lub **przejęcie systemu**
- **Przykłady:** DoS/DDoS (atak na dostępność)

591

Klasyfikacja zagrożeń sieciowych

Typ ataku	Charakterystyka	Przykład
Insider	Osoba z dostępem wewnętrznym, nadużywa uprawnień	pracownik kopiujący dane firmowe
External	Atak spoza organizacji, często przez Internet	haker włamujący się do systemu

592

Wektory ataku (Attack Vectors)

Ludzie – Social Engineering (74% ataków, Verizon DBIR 2025)

- Najłabsze ogniwo to człowiek
- Techniki: phishing, pretexting, baiting, smishing
- **Cel:** skłonić ofiarę do ujawnienia informacji lub kliknięcia w złośliwy link

Oprogramowanie

- Luki w systemach i aplikacjach (CVE – *Common Vulnerabilities and Exposures*):
exploity zero-day, błędy konfiguracyjne, niezaktualizowane systemy

Sprzęt (Hardware)

- Ataki na poziomie łańcucha dostaw (*supply chain attacks*): manipulacja komponentów routerów, chipów, BIOS-u

593

Sniffing (Podśluchiwanie) - działanie

Cel: przechwycenie pakietów przesyłanych w sieci lokalnej (LAN)

Mechanizm: karta sieciowa pracuje w trybie **promiscuous**, odbierając wszystkie ramki Ethernet, nie tylko te adresowane do niej

Protokoły podatne:

- **HTTP, FTP, Telnet** – dane przesyłane w postaci *plaintext* (czytelne loginy, hasła)
- **SMTP, POP3** – jeśli bez SSL/TLS, również podatne na podsłuch
- **Typy sieci:**
 - **Hub-based LAN:** wszystkie pakiety są rozgłaszane – łatwe do podsłuchania
 - **Switch-based LAN:** trudniejsze, ale nadal możliwe przy wykorzystaniu ARP spoofingu lub port mirroringu

Spoofing (Podszywanie się) - działanie

Atak polegający na **fałszowaniu tożsamości w sieci**, by zdobyć zaufanie systemu lub użytkownika

Cel: wprowadzenie fałszywych danych do komunikacji lub przekierowanie ruchu sieciowego

Mechanizm: miana nagłówków pakietów lub odpowiedzi sieciowych (np. z użyciem narzędzi takich jak **Scapy**)

Efekt: system ofiary wierzy, że komunikacja pochodzi z zaufanego źródła

596

Spoofing (Podszywanie się) - działanie

Rodzaj	Opis	Skutek
IP spoofing	Fałszowanie adresu źródłowego IP w pakiecie	Trudność w identyfikacji źródła ataku (DoS, DDoS)
ARP spoofing	Wysyłanie fałszywych odpowiedzi ARP – zatrutowanie cache'u	Przekierowanie ruchu w LAN (MITM)
DNS spoofing	Fałszywe rekordy DNS (cache poisoning)	Użytkownik trafia na złośliwą stronę

597

Spoofing (Podszywanie się) - przykład

Atak: Man-in-the-Middle (MITM) przez ARP Spoofing

Scenariusz:

Atakujący w sieci LAN wysyła fałszywe odpowiedzi ARP do ofiary i routera
→ Oba urządzenia myślą, że adres MAC atakującego to adres drugiego hosta → Cały ruch przechodzi przez atakującego

Atakujący może: podsłuchiwać pakiety (sniffing), modyfikować dane, przekierować użytkownika na fałszywą stronę

Efekt: Atakujący staje się „przezroczystym routerem” w komunikacji

598

Spoofing (Podszywanie się) - obrona

Obszar	Technologia	Działanie
Warstwa łącza danych	Dynamic ARP Inspection (DAI)	Weryfikuje odpowiedzi ARP z tablic DHCP, blokuje fałszywe wpisy
Warstwa sieciowa	IPsec	Uwierzytelnia źródło i integralność pakietów IP
Warstwa aplikacyjna / DNS	DNSSEC	Weryfikuje podpisy cyfrowe rekordów DNS
Routing (warstwa 3/4)	BGPsec	Chroni wymianę tras między routerami, zabezpiecza przed route hijacking

DoS / DDoS – działanie

DoS (Denial of Service): atak polegający na przeciążeniu usługi lub zasobu tak, by stał się niedostępny dla użytkowników

DDoS (Distributed Denial of Service): ten sam mechanizm, ale wykonywany z wielu rozproszonych źródeł – np. tysiące zainfekowanych urządzeń (botnet)

2018: Atak na GitHub – 1.3 Tbps (rekordowy wówczas)

2025: Hipotetyczny rekord – 3 Tbps atak wymierzony w infrastrukturę Azure (IoT botnet + amplifikacja)

Trend: rosnąca przepustowość sieci = większe możliwości ataków

600

DoS / DDoS – działanie

Typ	Opis	Przykład
SYN Flood	Zalewanie serwera nieukończonymi połączeniami TCP („half-open”)	Fałszywe żądania SYN, brak ACK
UDP Flood	Wysyłanie masowych pakietów UDP bez kontekstu	Brak odpowiedzi = zasobowość CPU
Reflection Attack	Wysyłanie pakietów z fałszywym IP ofiary	Serwery (np. NTP, DNS) odpowiadają na ofiarę
Amplification Attack	Użycie protokołów z dużym ratio odpowiedzi	NTP/DNS amplification – małe zapytanie → duża odpowiedź

601

DoS / DDoS – obrona

Technika

Rate Limiting

Blackholing / Sinkholing

Scrubbing Centers

CDN (Content Delivery Network)

Anomaly Detection (AI/ML)

Opis

Ograniczanie liczby żądań na sekundę

Przekierowanie ruchu na „czarną dziurę” lub honeypot

Dedykowane centra czyszczące ruch (analiza, filtracja, przekazanie czystych danych)

Rozproszenie ruchu na wiele serwerów brzegowych

Automatyczne wykrywanie anomalii w ruchu

Zastosowanie

W serwerach HTTP, API gateways

Tymczasowa ochrona infrastruktury

W dużych firmach i ISP

Absorpcja dużych wolumenów DDoS

W systemach typu Cloudflare Magic Transit, AWS Shield

Advanced
602

Phishing – działanie

Atak wykorzystujący socjotechnikę – manipulowanie użytkownikiem, by podał dane, kliknął link lub pobrał złośliwy plik

Cel: kradzież danych uwierzytelniających, numerów kart, dostępów administracyjnych lub zainstalowanie malware

Według badań – aż 90% naruszeń bezpieczeństwa zaczyna się od phishingu

300% wzrost ataków phishingowych w ciągu roku

1,5 mln nowych stron phishingowych miesięcznie

Najczęściej celem: Microsoft 365, Google Workspace, bankowość online

603

Phishing – działanie

Typ	Opis	Przykład
Spear phishing	Spersonalizowany atak na konkretną osobę lub firmę	Mail z prawdziwym imieniem i nazwiskiem adresata
Whaling	Atak na osoby na wysokich stanowiskach (CEO, CFO)	„Pilne przelewy” z rzekomego konta prezesa
Vishing	Voice phishing – telefoniczne podszywanie się pod bank, IT	Fałszywe połączenia z „działu bezpieczeństwa”
Smishing	Phishing przez SMS	Link do „aktualizacji przesyłki” z fałszywej strony

604

Phishing – przykład

Case study: Atak na Twitter (2020, obecnie X)

1. Atakujący dzwonili do pracowników Twittera, podszywając się pod dział IT
2. Uzyskali dostęp do panelu administracyjnego i przejęli konta znanych osób (Elon Musk, Obama, Gates)
3. Wykorzystali je do publikowania wiadomości o „szybkich inwestycjach w kryptowaluty”

Klucz: nie technologia, a socjotechnika – przekonali człowieka

605

Phishing – obrona

Edukacja użytkowników

- Regularne szkolenia z rozpoznawania phishingu
- Symulacje phishingowe – testowanie reakcji zespołu

Uwierzytelnianie wieloskładnikowe (2FA/MFA)

- Nawet jeśli hasło zostanie przejęte – brak drugiego czynnika blokuje dostęp

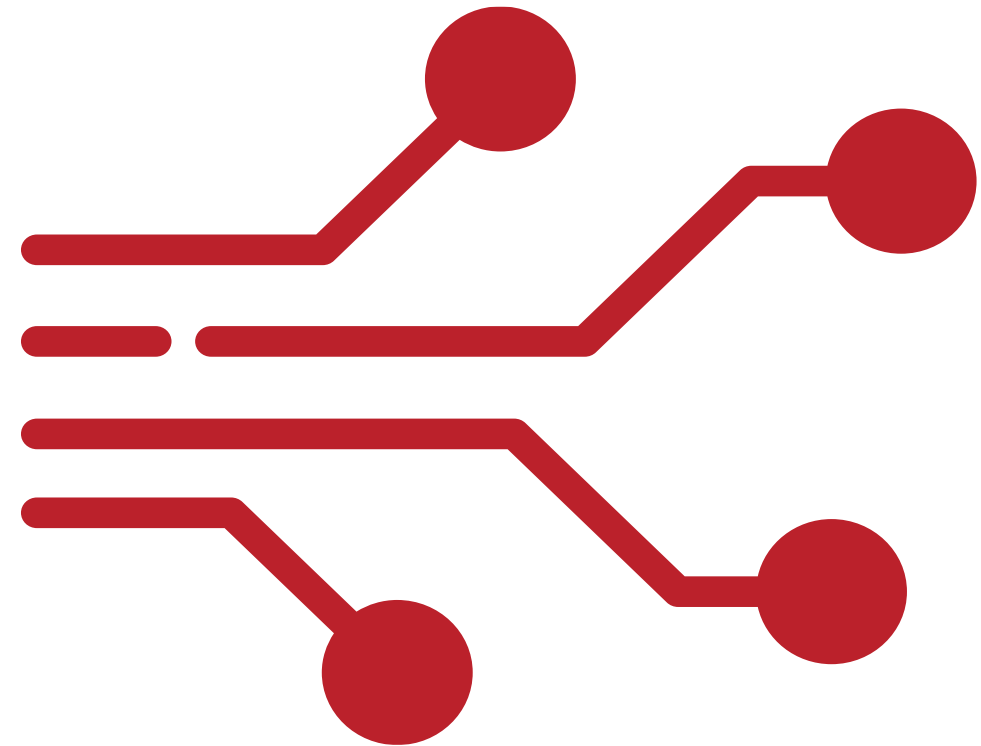
Filtrowanie wiadomości (SPF, DKIM, DMARC)

- **SPF** – weryfikuje serwer wysyłający
- **DKIM** – podpisy cyfrowe wiadomości
- **DMARC** – polityka reagowania (blokuje, kwarantanna, raportuj)

Ochrona po stronie użytkownika

- Rozszerzenia przeglądarek: uBlock, Netcraft, Guard.io
- Nie klikać linków z nieznanych źródeł, zawsze sprawdzać domene

Rola firewalli i systemów IDS/IPS w ochronie sieci



607

Wstęp do firewalli

Firewall:

Bariera między siecią zaufaną (LAN) a niezaufaną (Internet)

Filtruje ruch zgodnie z regułami bezpieczeństwa (**ACL – Access Control Lists**)

Typ	Opis	Zastosowanie
Packet filtering (Stateless)	Sprawdza nagłówki pakietów (IP, port, protokół), nie pamięta stanu połączenia	Szybki, prosty, warstwa 3 (OSI)
Stateful inspection	Analizuje kontekst połączenia – utrzymuje tablicę stanów	Standard w nowoczesnych zaporach
Application-layer firewall (proxy)	Analiza treści aplikacyjnych (HTTP, SMTP) – DPI (Deep Packet Inspection)	Ochrona aplikacji i API

608

Firewall – zasada działania

Firewall podejmuje decyzję dla każdego pakietu na podstawie zestawu reguł

Każda reguła określa kogo wpuścić, a kogo zablokować, analizując:

- **IP źródłowy / docelowy** (skąd i dokąd idzie pakiet)
- **Port źródłowy / docelowy** (jaki serwis – np. 80 = HTTP, 443 = HTTPS)
- **Protokół** (TCP / UDP / ICMP)

Reguły definiują akcję:

- **PERMIT / ALLOW** – przepuść ruch
- **DENY / DROP / REJECT** – zablokuj ruch

Kolejność ma znaczenie: listy ACL są przetwarzane od góry do dołu, sekwencyjnie:

1. Firewall czyta pierwszą regułę → sprawdza, czy pasuje do pakietu
2. Jeśli tak → wykona akcję (permit/deny) i nie sprawdza dalszych reguł
3. Jeśli nie → przechodzi do kolejnej reguły

Ostatnia reguła (niewidoczna) zwykle jest „implicit deny all” — blokuje wszystko, co nie zostało jawnie dopuszczone

Firewall – przykład listy iptables

1 Zezwól na ruch HTTPS (port 443/TCP) do serwera
`iptables -A INPUT -p tcp --dport 443 -j ACCEPT`

2 Zablokuj ruch HTTP (port 80/TCP)
`iptables -A INPUT -p tcp --dport 80 -j DROP`

3 Blokuj wszystko inne (implicit default deny)
`iptables -A INPUT -j DROP`

Kolejność ma znaczenie! Przeniesienie reguły 3 (`iptables -A INPUT -j DROP`) na samą górę - blokuje cały ruch!

610

Systemy IDS/IPS

System	Funkcja	Tryb działania	Zachowanie w przypadku zagrożenia	Przykłady technologii
IDS – Intrusion Detection System	Wykrywa podejrzany ruch i generuje alerty	Passive (off-path / mirror port)	<i>Alertuje administratora, ale nie blokuje ruchu</i>	Snort, Zeek, Suricata (IDS mode)
IPS – Intrusion Prevention System	Wykrywa i aktywnie blokuje ataki w czasie rzeczywistym	Inline (pakiety przechodzą przez IPS)	<i>Blokuje pakiet, resetuje sesję, modyfikuje ACL</i>	Palo Alto NGFW IPS, Cisco Firepower, Suricata (IPS mode)

611

Systemy IDS/IPS

IDS – Intrusion Detection System („detektyw”)

Pracuje **pasywnie**, analizuje ruch z mirror/SPAN portu

Nie ingeruje w pakiety — „**widzi wszystko, niczego nie zmienia**”

Tworzy **logi** i wysyła **alerty** (np. do SIEM)

Idealny do: **analizy incydentów, wykrywania anomalii**

Przykład: wykrywa próbę **SQL Injection**, tworzy alert dla administratora

IPS – Intrusion Prevention System („policjant”)

Pracuje **aktywnie**, jest **inline** (ruch przepływa przez niego)

Może **zatrzymać pakiet**, zresetować sesję lub zmienić reguły firewalla

Chroni aplikacje i usługi **w czasie rzeczywistym**

Przykład: zobaczy SQL Injection → **blokuje pakiet i rozłącza połączenie**

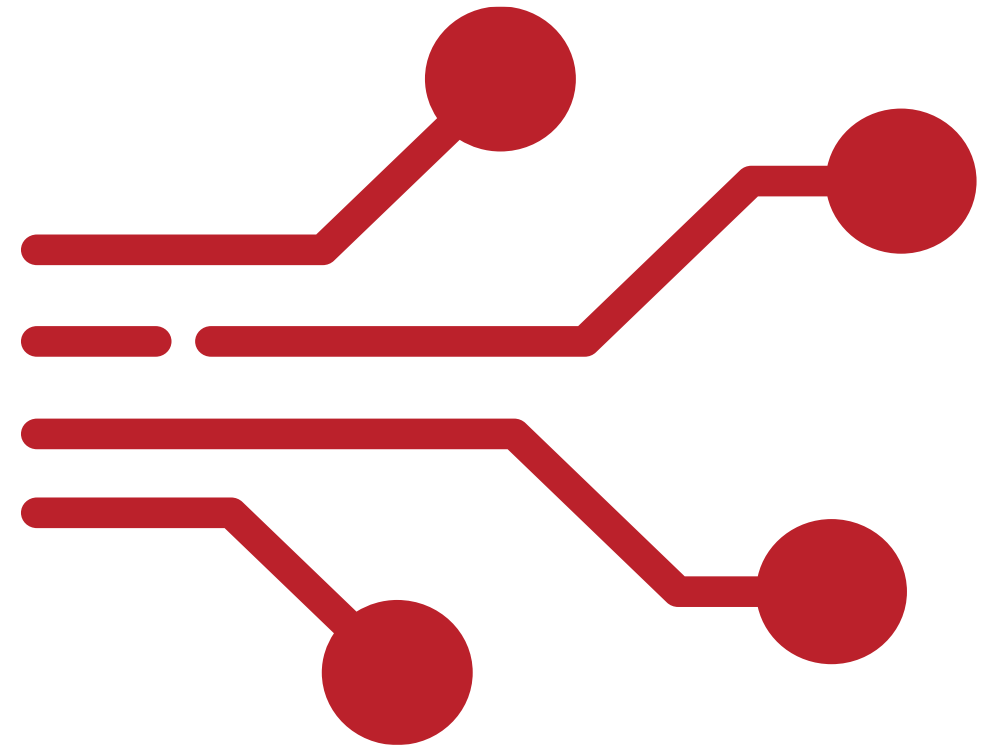
612

Systemy IDS/IPS – typy detekcji i narzędzia

Typ analizy	Jak działa?	Zalety	Wyzwania
Signature-based detection	Porównuje ruch do bazy znanych sygnatur ataków (jak „antywirus dla sieci”)	Skuteczne na znane ataki	Nie wykryje zero-day
Anomaly-based detection (ML)	Uczy się „normalnego ruchu” i wykrywa odchylenia (baseline)	Wykrywa nowe, nieznane ataki	False positives (fałszywe alarmy)
Narzędzie	Typ	Charakterystyka	
Snort	IDS / IPS	Open-source, reguły sygnaturowe (Snort rules language)	
Suricata	IDS / IPS	Lepsza wydajność, automatyczna analiza TLS/HTTP	
Zeek (Bro)	IDS (analiza behawioralna)	Tworzy logi zdarzeń w oparciu o zachowanie	

613

Podstawy szyfrowania danych w sieci (SSL/TLS)



614

Dlaczego szyfrowanie jest niezbędne

Szyfrowanie = ochrona danych przed osobami nieuprawnionymi

- Chroni przed:
- **podśluchem (sniffingiem)** — ktoś przechwytuje ruch w sieci
- **atakiem typu MITM (Man-in-the-Middle — człowiek pośrodku)** — ktoś próbuje zmodyfikować dane
- Zapewnia:
- **poufność** — dane są nieczytelne bez klucza
- **integralność** — dane nie mogą zostać zmienione
- **uwierzytelnienie serwera** — mamy pewność, że łączymy się z właściwą stroną
- Szyfrowanie jest obowiązkowe w systemach:
- logowanie użytkowników
- dane osobowe (RODO — *Rozporządzenie o Ochronie Danych Osobowych*)
- płatności (PCI DSS — *Payment Card Industry Data Security Standard*)

Szyfrowanie symetryczne vs asymetryczne

Szyfrowanie symetryczne

- używa **jednego klucza** do szyfrowania i odszyfrowania danych
- **bardzo szybkie** — idealne do dużej ilości danych
- Przykład: **AES** — *Advanced Encryption Standard (standard szyfrowania używany w TLS i VPN)*

Szyfrowanie asymetryczne

- używa **pary kluczy**: klucz publiczny — do szyfrowania, klucz prywatny — do odszyfrowania
- wolniejsze, używane głównie do: wymiany klucza sesyjnego, podpisów cyfrowych (uwierzytelnianie)
- Przykłady:
- **RSA** — Rivest Shamir Adleman
- **ECC** — Elliptic Curve Cryptography (kryptografia krzywych eliptycznych)

616

Mechanizm TLS Handshake

Powitanie klienta

→ Klient wysyła listę obsługiwanych metod szyfrowania

Powitanie serwera + certyfikat

→ Serwer wybiera metodę szyfrowania i przesyła swój certyfikat

Wymiana klucza

→ Klient i serwer wymieniają dane potrzebne do ustalenia wspólnego klucza sesyjnego

Weryfikacja certyfikatu

→ Klient sprawdza certyfikat: jego ważność, wystawcę oraz zgodność z domeną

Zakończenie negocjacji

→ Obie strony przechodzą na szyfrowaną komunikację.

617

Certyfikaty i CA (urząd certyfikacji)

Certyfikat TLS (Transport Layer Security) lub SSL (Secure Sockets Layer) to **cyfrowy dowód tożsamości serwera lub użytkownika**

1. Zapewnia trzy podstawowe funkcje bezpieczeństwa:
Uwierzytelnienie (ang. authentication) → Potwierdza, że strona, z którą się łączymy, naprawdę jest tym, za kogo się podaje
Przykład: certyfikat bank.pl potwierdza, że łączymy się z prawdziwym bankiem, a nie fałszywą stroną phishingową
2. Szyfrowanie (ang. encryption) → Dane przesyłane między przeglądarką a serwerem są zaszyfrowane i nikt nie może ich podsłuchać (sniffing, MITM – Man in the Middle)
3. Integralność danych (ang. integrity) → Chroni przed modyfikacją danych po drodze – jeśli ktoś zmieni bajt w transmisji, zostanie to wykryte

618

Certyfikaty i CA (urząd certyfikacji)

Certyfikat wydaje Urząd certyfikacji (CA) - **zaufana instytucja**, która:

- potwierdza tożsamość właściciela domeny lub organizacji
- **podpisuje cyfrowo certyfikat**, aby inni mogli mu zaufać

Przykłady znanych CA:

- **Let's Encrypt** – darmowy, automatyczny, najczęściej używany na stronach WWW
- **DigiCert, GlobalSign, Sectigo, GoDaddy** – komercyjne, oferują certyfikaty firmowe (OV, EV)
- **CERTUM (Asseco)** – polski urząd certyfikacji

Jak działa zaufanie (model PKI – Public Key Infrastructure):

PKI to system, który zarządza wydawaniem i weryfikacją certyfikatów

619

Certyfikat X.509 (standardowy format certyfikatów)

Pole	Znaczenie
Subject (Podmiot)	Domena lub organizacja, dla której wydano certyfikat
Issuer (Wystawca)	Urząd certyfikacji (CA), który podpisał certyfikat
Validity (Ważność)	Okres ważności – „Not Before” / „Not After”
Public Key (Klucz publiczny)	Klucz używany do szyfrowania i podpisywania
Signature (Podpis)	Cyfrowy podpis CA potwierdzający autentyczność
SAN (Subject Alternative Names)	Lista domen objętych certyfikatem (np. <code>www.example.com</code>) 620

Typy certyfikatów (według poziomu walidacji)

Typ	Nazwa (ang.)	Co sprawdza urząd	Przykład zastosowania
DV	Domain Validation	Czy właściciel kontroluje domenę	Blog, sklep online
OV	Organization Validation	Czy firma istnieje i jest legalna	Strony firmowe
EV	Extended Validation	Pełna weryfikacja tożsamości prawnej i adresowej	Banki, instytucje finansowe

621

TSL – znane ataki

Nazwa ataku	Co oznacza skrót / identyfikator	Co się dzieje
Heartbleed	CVE-2014-0160 (<i>CVE = Common Vulnerabilities and Exposures — publiczna baza podatności</i>)	Luka w bibliotece OpenSSL — umożliwiała podejrzenie pamięci RAM serwera, w tym haseł i kluczy prywatnych
POODLE	<i>Padding Oracle On Downgraded Legacy Encryption</i>	Atak wymuszał, aby serwer zamiast TLS użył starego i słabego SSL 3.0, co pozwalało na odszyfrowanie części danych

Posiadanie TLS nie wystarczy – ważna jest wersja i konfiguracja

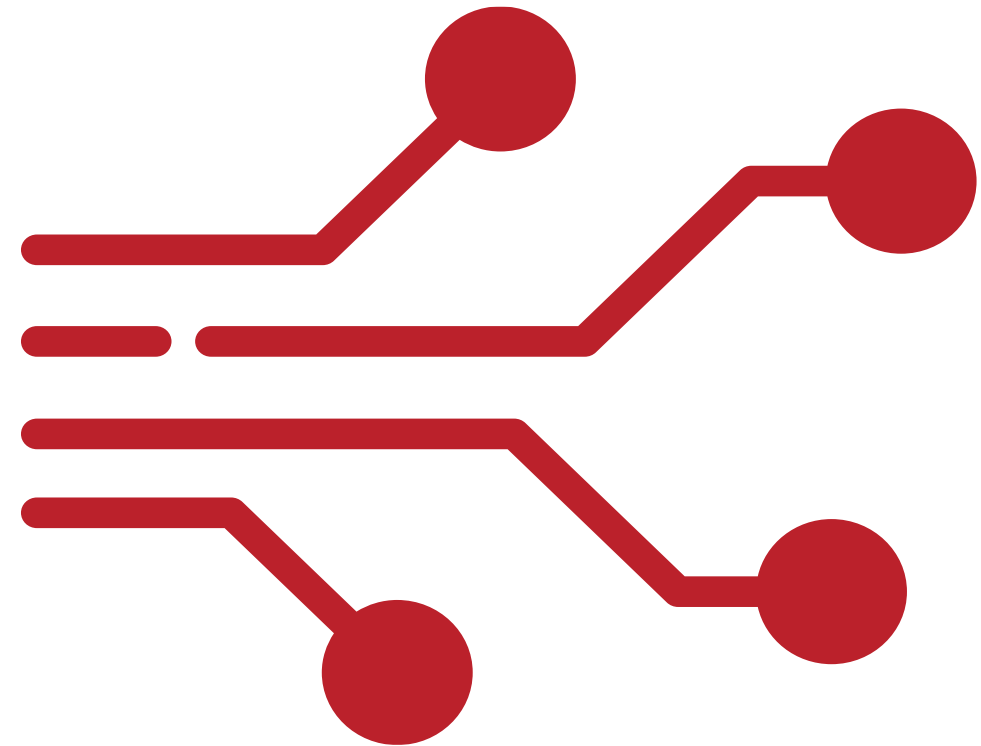
622

TSL – obrona

Mechanizm	Co oznacza	Jak chroni
HSTS – <i>HTTP Strict Transport Security</i>	Mechanizm wymuszający HTTPS	Przeglądarka nigdy nie pozwoli cofnąć się do HTTP ani SSL
Certificate pinning (<i>przypinanie certyfikatu</i>)	Przeglądarka pamięta konkretny certyfikat lub klucz publiczny	Utrudnia ataki MITM z fałszywym certyfikatem
Expect-CT	<i>Certificate Transparency enforcement</i> — wymóg jawności certyfikatu	Certyfikaty muszą być w publicznych logach, co pozwala wykrywać fałszywe certyfikaty

623

Dobre praktyki w konfiguracji urządzeń sieciowych



624

Podstawowe dobre praktyki bezpieczeństwa urządzeń sieciowych

Cel: Zmniejszyć powierzchnię ataku

- Zmień domyślne hasła (np. admin/root → **łatwe do zgadnięcia**)
- Wyłącz nieużywane usługi:
 - **Telnet (nieszyfrowane zarządzanie)** → wyłączyć
 - **SSH – Secure Shell (szyfrowane zarządzanie)** → używać
- Regularne kopie konfiguracji (backup)
- Ogranicz dostęp administracyjny tylko do sieci wewnętrznej

625

Dobre praktyki – konfiguracja routerów i switchy

1. Zmieniaj hasła administratora

- Domyślne loginy typu admin/admin, admin/password są publicznie znane
- Używaj długich, unikalnych haseł (min. 12 znaków)
- Przechowuj hasła w menedżerze haseł (np. KeePass, Bitwarden)

2. Zarządzanie tylko przez SSH (Secure Shell)

- **SSH – Secure Shell = szyfrowane połączenie do zarządzania urządzeniem**
- Alternatywa: Telnet
Telnet = dane (hasła!) lecą bez szyfrowania → łatwe do podsłuchania (sniffing)

3. Wyłącz dostęp administracyjny z Wi-Fi gości (Wi-Fi ogólnie)

- Router nie powinien pozwalać na logowanie z sieci, której nie kontrolujesz
- Dostęp administracyjny tylko z LAN / sieci administratorów

Dobre praktyki – bezpieczeństwo komputerów użytkowników

Endpoint = komputer użytkownika końcowego:

Najczęstszy punkt wejścia dla ataków (phishing, malware)

- Aktualizacje oprogramowania (patching):
 - Windows Update / **WSUS — Windows Server Update Services**
 - Linux: **sudo apt update && sudo apt upgrade**
- EDR — Endpoint Detection and Response (Wykrywanie i reagowanie na zagrożenia na stacjach roboczych) = „Nowoczesny antywirus” + analiza zachowania systemu: nie tylko skanuje pliki, monitoruje procesy, wykrywa podejrzane działania
- Host-based IDS — Intrusion Detection System (System wykrywania włamań na poziomie jednego komputera) = Analiza logów i zdarzeń na konkretnym urządzeniu (host = komputer)

627

Dobre praktyki – silne hasła

Hasło to **pierwsza linia obrony** przed przejęciem konta

- **Zasady tworzenia bezpiecznego hasła:**
 - minimum **12–16 znaków**
 - używaj **wielkich i małych liter, cyfr i znaków specjalnych**
 - **nie używaj tego samego hasła w wielu serwisach**
 - unikaj danych osobowych (imię, data urodzenia, nazwa psa)
 - Przykład złego hasła: Janek2024
 - Przykład dobrego hasła (łatwego do zapamiętania): Kot#Na_Kawie!7
- **Hasło ma być długie, nie skomplikowane**

628

Segmentacja sieci (VLAN – Virtual LAN)

VLAN — Virtual Local Area Network (wirtualny podział sieci)

Rozdzielanie różnego typu ruchu:

VLAN pracowników

VLAN gości (tylko Internet)

VLAN IoT (drukarki, kamery — ryzykowne)

Segmentacja = **mniej szkody przy incydencie**

Łączenie subnettingu z VLANem — jeden VLAN = jedna podsieć IP

Segmentacja VLAN (Warstwa 2) ≠ Subnetting (Warstwa 3)

VLAN fizycznie izoluje ruch na switchu, zanim dojdzie do IP/routingu

629

Zasada najmniejszych uprawnień (PoLP)

PoLP — Principle of Least Privilege → każdy użytkownik, urządzenie i aplikacja ma mieć tylko minimalne uprawnienia, potrzebne do wykonania zadania:

Minimalizuje skutki błędu użytkownika

Ogranicza rozprzestrzenianie się malware (np. ransomware nie zaszyfruje całej firmy)

Chroni dane przed nieuprawnionym dostępem

Im mniejsze uprawnienia, tym mniejsze ryzyko

RBAC — Role-Based Access Control = nadawanie uprawnień według ról (stanowiska), a nie według osoby (Zmieniasz rolę → zmieniają się uprawnienia)

Przykłady ról: użytkownik (dostęp do własnych dokumentów), kierownik (dostęp do dokumentów działu), administrator (pełny dostęp do systemu) 630

Aktualizacje i kopie bezpieczeństwa

Aktualizacje usuwają znane luki bezpieczeństwa

Luki są katalogowane jako CVE — Common Vulnerabilities and Exposures (publiczny identyfikator podatności, np. CVE-2024-12345)

Jeśli system nie jest aktualizowany → jest podatny na ataki już opisane i znane

Planowanie aktualizacji (harmonogram, okno serwisowe)

Testowanie aktualizacji na małej grupie urządzeń i wdrażaj na pozostałych komputerach/serwerach

Regularne kopie konfiguracji i danych przechowywane w innym miejscu niż dane produkcyjne

Testowanie przywracania — backup bez testu = backup, który nie istnieje

631

Monitorowanie i logowanie

Monitorowanie sieci:

- Pozwala wiedzieć co się dzieje w sieci i na urządzeniach
- Pozwala wykryć incydent, zanim zrobi szkody
- Pozwala posiadać dowody w przypadku naruszenia bezpieczeństwa

Co zbierać:

Logi z firewalla: informacje o blokowanym ruchu, próbach skanowania, podejrzanych połączeniach

IDS (system wykrywania włamań): podejrzane zdarzenia i alerty

logi systemowe (Syslog): z systemów operacyjnych, usług, aplikacji

632

Logi systemowe – Linux / Windows

System operacyjny	Nazwa logów / sekcja	Miejsce / ścieżka	Co tam znajdziesz?
Linux (Ubuntu)	syslog	/var/log/syslog	główne logi systemu (usługi, błędy, sieć)
	auth.log	/var/log/auth.log	logowania, SSH, błędne próby logowania
	kern.log	/var/log/kern.log	logi jądra systemu
	dmesg	/var/log/dmesg	informacje sprzętowe (uruchamianie systemu)
Windows 11	System	Event Viewer (Podgląd zdarzeń) → <i>Windows Logs</i> → <i>System</i>	logi systemu Windows, błędy usług
	Security	Event Viewer → Windows Logs → Security	logowania, nieudane logowania, zmiany uprawnień
	Application	Event Viewer → Windows Logs → Application	logi programów i aplikacji
	Pliki fizyczne	C:\Windows\System32\winevt\Logs\	logi w formacie .evtx

633

Dziękuję za uwagę