



Sieci przewodowe

Sieć przewodowa to rodzaj **sieci komputerowej**, w której **urządzenia są połączone za pomocą fizycznych kabli** — najczęściej **miedzianych (Ethernet)** lub **światłowodowych (fiber optic)**.

 **Najprościej mówiąc:**

Sieć przewodowa = połączenie komputerów, drukarek, routerów itp. **za pomocą kabli**, a nie przez Wi-Fi.



Główne cechy:

- **Przesył danych:** Dane są transmitowane przez przewodniki, co zapewnia stabilne i szybkie połączenie, zazwyczaj z mniejszą podatnością na zakłócenia niż w sieciach bezprzewodowych.
- **Przykłady zastosowań:** Sieci LAN w domach, biurach, centrach danych czy systemy monitoringu CCTV.



Przykłady sieci przewodowych

Ethernet (LAN) — najczęściej spotykana sieć przewodowa w domach i firmach.

- używa kabli **RJ-45 (skrętka)**,
- prędkości np. **100 Mb/s, 1 Gb/s, 10 Gb/s**,
- łączy komputery, routery, switchy.

Światłowód (Fiber Optic) — sieć zbudowana z kabli światłowodowych.

- bardzo duża prędkość transmisji,
- stosowana w łączach między miastami, serwerowniach lub w nowoczesnych domach (FTTH – Fiber To The Home).

Połączenia szeregowo / przemysłowe — np. RS-232, RS-485 — używane w automatyce i systemach przemysłowych.



Jak działa sieć przewodowa

1. Każde urządzenie ma **kartę sieciową (NIC)**.
2. Kable łączą urządzenia poprzez **switch, router** lub **hub**.
3. Dane przesyłane są w postaci **sygnałów elektrycznych lub optycznych** przez przewody.
4. Komunikacja odbywa się według określonych **protokołów sieciowych** (np. TCP/IP, Ethernet).



Zalety sieci przewodowej

- ✓ **Szybka transmisja danych** – stabilniejsze połączenie niż Wi-Fi.
- ✓ **Niskie opóźnienia (ping)** – ważne np. w grach i serwerach.
- ✓ **Bezpieczeństwo** – trudniej podsłuchać połączenie fizyczne.
- ✓ **Odporność na zakłócenia radiowe** – nie zależy od zasięgu Wi-Fi.



Wady sieci przewodowej

- ✗ **Trudniejszy montaż** – trzeba prowadzić kable w ścianach lub po podłodze.
- ✗ **Mniejsza mobilność** – urządzenia muszą być fizycznie podłączone.
- ✗ **Koszty instalacji** – więcej sprzętu (kable, gniazda, przełączniki).



Sieć bezprzewodowa

Sieć komputerowa, w której urządzenia **łączą się ze sobą bez użycia kabli**, wykorzystując fale radiowe, podczerwień lub mikrofale do przesyłania danych.

✚ Najprościej mówiąc:

Sieć bezprzewodowa = połączenie komputerów, telefonów, tabletów i innych urządzeń bez kabli, np. przez **Wi-Fi** lub **Bluetooth**.



Przykłady sieci bezprzewodowych

- **Wi-Fi (WLAN – Wireless Local Area Network)**
 - najpopularniejsza sieć domowa lub biurowa,
 - wykorzystuje fale radiowe (częstotliwości 2,4 GHz i 5 GHz),
 - umożliwia łączenie komputerów, smartfonów i innych urządzeń z routerem bez kabli.
- **Bluetooth**
 - służy do połączenia urządzeń na krótką odległość (np. telefon ↔ słuchawki).
- **Sieć komórkowa (LTE, 5G)**
 - zapewnia dostęp do Internetu przez operatorów sieci komórkowych,
 - obejmuje duże obszary (miasta, regiony).
- **Hotspot Wi-Fi**
 - punkt dostępu umożliwiający innym urządzeniom korzystanie z Internetu bezprzewodowo.



Jak działa sieć bezprzewodowa

1. Urządzenie (np. laptop, telefon) ma **kartę sieciową Wi-Fi**.
2. Wysyła i odbiera dane przez **antnę**, która komunikuje się z **routerem (punktem dostępowym)**.
3. Router przekazuje dane dalej – np. do Internetu przez kabel (światłowód lub Ethernet).
4. Komunikacja odbywa się wg ustalonych **protokołów sieciowych** (np. 802.11).



Zalety sieci bezprzewodowej

- Mobilność Można się łączyć z dowolnego miejsca w zasięgu sygnału
- Brak kabli Nie trzeba prowadzić przewodów przez ściany
- Łatwość instalacji Wystarczy router i urządzenia z Wi-Fi
- Wiele urządzeń Może łączyć laptopy, smartfony, drukarki itd.



Wady sieci bezprzewodowej

- **Mniejsza stabilność** Sygnał może zanikać przez ściany lub zakłócenia
- **Bezpieczeństwo** Łatwiej podsłuchać lub włamać się niż w sieci przewodowej
- **Niższa prędkość** Wolniejsza transmisja niż przez kabel Ethernet
- **Zużycie energii** Urządzenia mobilne szybciej rozładowują baterię



Polityka bezpieczeństwa w sieci

Polityka bezpieczeństwa sieci (Network Security Policy) to zbiór zasad, procedur i **wytocznych**, które określają:

- jak chronić dane i zasoby sieciowe,
- kto i w jaki sposób może korzystać z sieci,
- jakie działania są dozwolone, a jakie zabronione,
- jak reagować w razie incydentów bezpieczeństwa.

Innymi słowy: to **plan działania**, który pomaga organizacji **utrzymać poufność, integralność i dostępność danych (zasada CIA: Confidentiality, Integrity, Availability)**.



Główne cele polityki bezpieczeństwa

1. **Poufność (Confidentiality)** – ochrona danych przed nieautoryzowanym dostępem.
👉 np. szyfrowanie, uwierzytelnianie użytkowników.
2. **Integralność (Integrity)** – zapobieganie nieautoryzowanym zmianom danych.
👉 np. sumy kontrolne, kopie zapasowe.
3. **Dostępność (Availability)** – zapewnienie, że dane i usługi są dostępne, gdy są potrzebne.
👉 np. ochrona przed atakami DDoS, redundancja serwerów.



Rodzaje polityk bezpieczeństwa w sieci

1. **Polityka dostępu do sieci (Access Control Policy)**

Określa, kto może korzystać z sieci i w jakim zakresie.

- ♦ *Przykład:* pracownicy działu finansowego mają dostęp do serwera księgowego, ale nie do serwera HR.

2. **Polityka haseł (Password Policy)**

Ustala reguły dotyczące złożoności, długości i zmiany haseł.

- ♦ *Przykład:* hasło musi mieć min. 10 znaków, zawierać litery, cyfry i znaki specjalne, zmiana co 90 dni.

3. **Polityka korzystania z Internetu (Acceptable Use Policy)**

Określa, w jaki sposób można korzystać z Internetu w pracy.

- ♦ *Przykład:* zakaz wchodzenia na strony o treści niezgodnej z prawem lub niezwiązanej z pracą.



Rodzaje polityk bezpieczeństwa w sieci c.d.

4. **Polityka zapory sieciowej (Firewall Policy)**

Definiuje, które połączenia są dozwolone, a które blokowane.

- ♦ *Przykład:* ruch przychodzący na port 22 (SSH) dozwolony tylko z sieci firmowej.

5. **Polityka aktualizacji i łatania systemów (Patch Management Policy)**

Określa zasady instalowania poprawek bezpieczeństwa.

- ♦ *Przykład:* wszystkie serwery muszą być aktualizowane co najmniej raz w miesiącu.

6. **Polityka tworzenia kopii zapasowych (Backup Policy)**

Wskazuje, jak i kiedy wykonywać backupy danych.

- ♦ *Przykład:* codzienna kopia danych na serwer zewnętrzny, przechowywana przez 30 dni.

7. **Polityka reagowania na incydenty (Incident Response Policy)**

Opisuje procedury w razie włamania, ataku lub awarii.

- ♦ *Przykład:* po wykryciu ataku DDoS administrator odłącza serwer i powiadamia zespół SOC.



Praktyczne zastosowania

Pracownik loguje się do sieci VPN z domu

Zastosowana polityka: Polityka dostępu + polityka haseł (Efekt: Bezpieczny, uwierzytelniony dostęp)

Firma blokuje porty 21 (FTP) i 23 (Telnet)

Zastosowana polityka: Polityka zapory sieciowej (Efekt: Ochrona przed niebezpiecznymi protokołami)

Użytkownicy mają ograniczony dostęp do pendrive'ów

Zastosowana polityka: Polityka dostępu do urządzeń (Efekt: Zapobieganie wyciekom danych)

Codzienne kopie zapasowe serwerów

Zastosowana polityka: Polityka backupu (Efekt: Ochrona przed utratą danych)

Pracownicy nie mogą instalować oprogramowania

Zastosowana polityka: Polityka uprawnień użytkownika (Efekt: Redukcja ryzyka złośliwego oprogramowania)



Polityka haseł

Polityka haseł określa, jak **trudne powinny być hasła** i jak często trzeba je **zmieniać**.

Ma to chronić konta użytkowników przed włamaniami.

Hasło **powinno mieć duże i małe litery, cyfry i znaki specjalne**.

Nie powinno się używać tego samego hasła w kilku miejscach.

W firmach często **wymaga się zmiany hasła co kilka miesięcy**.

To **pomaga zwiększyć bezpieczeństwo** danych i systemów.



Polityka korzystania z Internetu

Ta polityka mówi, jak **pracownicy mogą używać Internetu w pracy.**

Na przykład **zabrania wchodzenia na strony niezwiązane z obowiązkami służbowymi.**

Chroni to firmę przed wirusami i stratą czasu w pracy.

Dzięki niej **administratorzy mogą łatwiej monitorować ruch sieciowy.**

W szkole taka **zasada też może obowiązywać** – np. nie wolno grać online podczas lekcji.

To **pomaga utrzymać porządek i bezpieczeństwo w sieci.**



Polityka zapory sieciowej (Firewall)

Zapora sieciowa **to program lub urządzenie, które blokuje niebezpieczne połączenia z Internetu.**

Polityka określa, które **połączenia są dozwolone, a które zablokowane.**

Na przykład może **pozwalać tylko na strony firmowe, a blokować porty używane przez hakerów.**

Dzięki temu **wirusy i nieautoryzowani użytkownicy nie dostają się do sieci.**

Firewall działa jak **strażnik** pilnujący bramy do firmy.

To jedna z podstawowych metod ochrony sieci komputerowych.



Polityka tworzenia kopii zapasowych (Backup)

Ta polityka mówi, **jak często trzeba robić kopie danych**, żeby ich nie stracić.

Backupy mogą być zapisywane na dysku zewnętrznym lub w **chmurze**.

W razie awarii, **ataku lub błędu można łatwo odzyskać dane**.

Firmy często robią kopie codziennie lub co tydzień.

W domu też warto robić kopie zdjęć czy **dokumentów**.

Dzięki temu nawet po awarii komputera dane nie przepadają.



Polityka reagowania na incydenty

Ta polityka określa, co robić, gdy **dojdzie do ataku lub problemu z bezpieczeństwem**.

Na przykład: kto ma zostać powiadomiony, jak zabezpieczyć dane i jak naprawić system.

Pomaga **szybko zareagować, zanim szkody będą duże**.

W firmach często **tworzy się specjalne zespoły reagowania (tzw. CERT lub SOC)**.

Dzięki tej **polityce każdy wie, jakie są jego obowiązki**.

To pozwala **utrzymać spokój i porządek w sytuacjach kryzysowych**.



Programowanie rozproszone

to sposób tworzenia oprogramowania, w którym **program (system)** nie działa na jednym komputerze, tylko na **wielu połączonych ze sobą komputerach (w sieci)**.

Każda z tych maszyn wykonuje część zadań, a razem tworzą jeden wspólny system.



Rodzaje (modele) progr. rozproszonego c.d.

Rodzaj:

Klient-serwer (Client-Server) - Klient wysyła żądania, serwer odpowiada.

Przykład: Strona WWW (przeglądarka ↔ serwer)

Wielowarstwowe (n-warstwowe) - System podzielony na warstwy: prezentacji, logiki i danych.

Przykład: Aplikacja webowa: frontend – backend – baza danych

Peer-to-Peer (P2P) - Każdy komputer (węzeł) może być klientem i serwerem jednocześnie.

Przykład: Torrent, komunikatory (np. Skype, BitTorrent)



Rodzaje (modele) programow. rozproszonego

Zdalne wywołania procedur (RPC) - Program na jednym komputerze wywołuje funkcję na innym.

Przykład: Java RMI, gRPC

Systemy oparte o komunikaty (Message-Oriented) - Komputery komunikują się przez kolejki wiadomości.

Przykład: RabbitMQ, Apache Kafka

Mikroserwisowe (Microservices) - System składa się z wielu małych usług, które komunikują się przez sieć.

Przykład: Aplikacje w chmurze (np. Netflix, Amazon)

Grid Computing / Cloud Computing - Wiele serwerów współdzieli zasoby obliczeniowe lub pamięć.

Przykład: AWS, Azure, Google Cloud



Technologie używane w progr. rozproszonym

Obszar:

Przykłady

Backend

Java (Spring Cloud), .NET, Node.js

Komunikacja

REST API, gRPC, WebSocket, message queues (RabbitMQ, Kafka)

Bazy danych

MongoDB, Cassandra, PostgreSQL Cluster

Architektura

mikroserwisy, chmura (AWS, Azure, GCP)



Cechy systemów rozproszonych

Cecha

Znaczenie

Współbieżność

wiele komputerów działa jednocześnie

Komunikacja przez sieć

wymiana danych np. przez HTTP, TCP/IP

Niezależność sprzętowa

różne komputery i systemy operacyjne mogą współpracować

Odporność na awarie

gdy jeden element padnie, reszta może działać dalej

Skalowalność

łatwo dodać więcej maszyn, żeby system działał szybciej



Przykład z życia

Wyobraź sobie aplikację bankową:

- Serwer A obsługuje logowanie,
- Serwer B zapisuje dane klientów w bazie,
- Serwer C przetwarza płatności.

Współpracują razem w sieci — **to właśnie programowanie rozproszone.**