WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

KURS WSTĘPNY: PODSTAWY SIECI KOMPUTEROWYCH

ZARYS WYKŁADU

- Wprowadzenie do sieci komputerowych
- Sprzęt sieciowy
- Adresowanie urządzeń sieciowych
- Protokoły sieciowe i komunikacja

WPROWADZENIE DO SIECI KOMPUTEROWYCH

KRÓTKA HISTORIA KOMUNIKACJI KOMPUTEROWEJ

Rozwój komunikacji komputerowej rozpoczął się w latach pięćdziesiątych XX wieku i od tego czasu postępuje w szybkim tempie

Lata 1950-te	Rozwój zapoczątkowany w armii USA
Lata 1960-te	Poszukiwania i rozwijanie przez instytucje akademickie
Lata 1970-te	Pierwsze podstawowe zastosowanie w kilku branżach
1973	Firma Xerox opracowała Ethernet
Lata 1980-te	Rozwój sieci LAN, powszechna dostępność usług, m.in. poczty e-mail
Lata 1990-te	HTTP i pojawienie się stron internetowych
1996	Powstanie firmy Google
…	…

INTERNET

Ogromny, rozproszony system informatyczny, działający głównie w architekturze klient-serwer

Uważany za „sieć sieci”

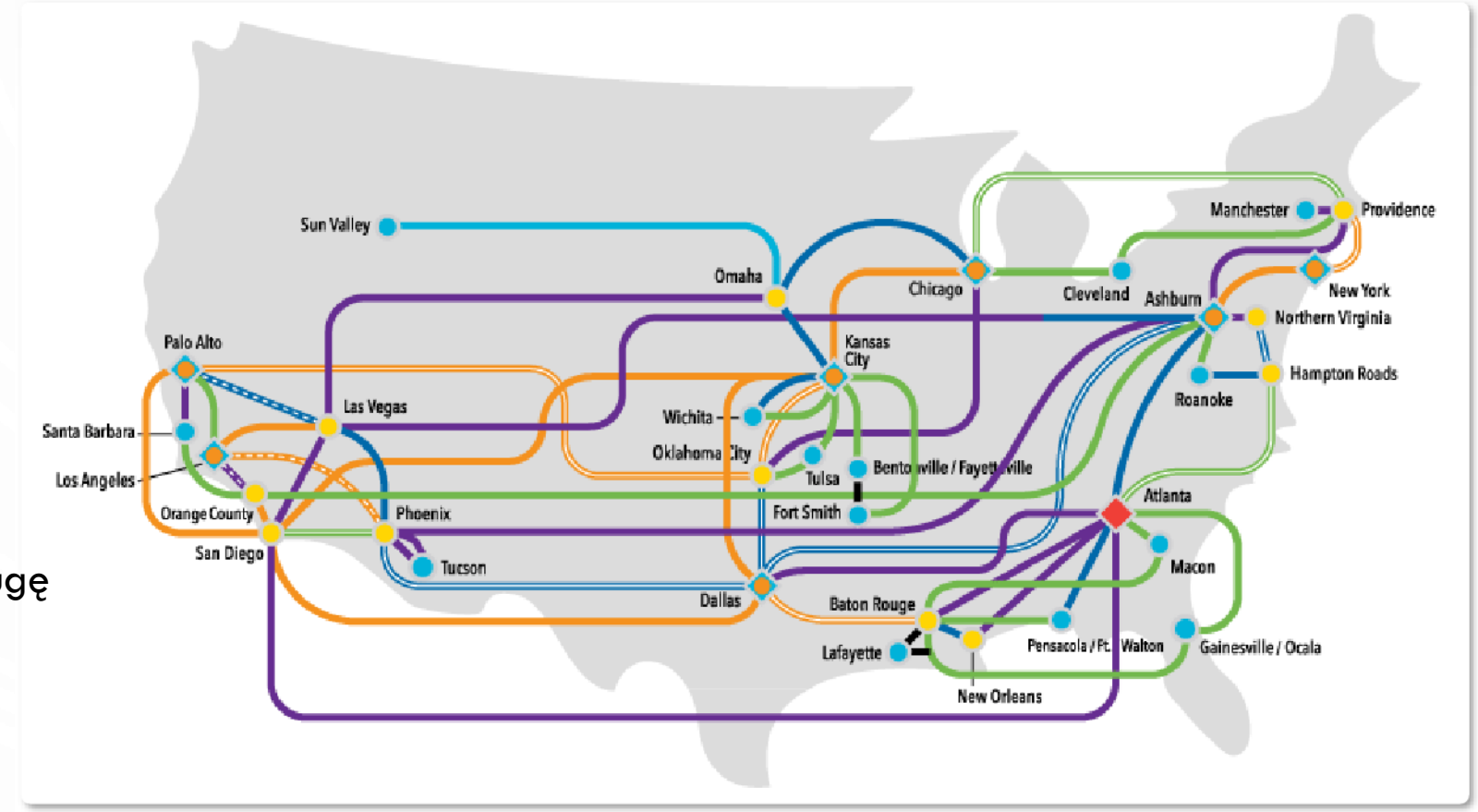
Wykorzystuje wiele typów protokołów komunikacyjnych

„SZKIELET” INTERNETU

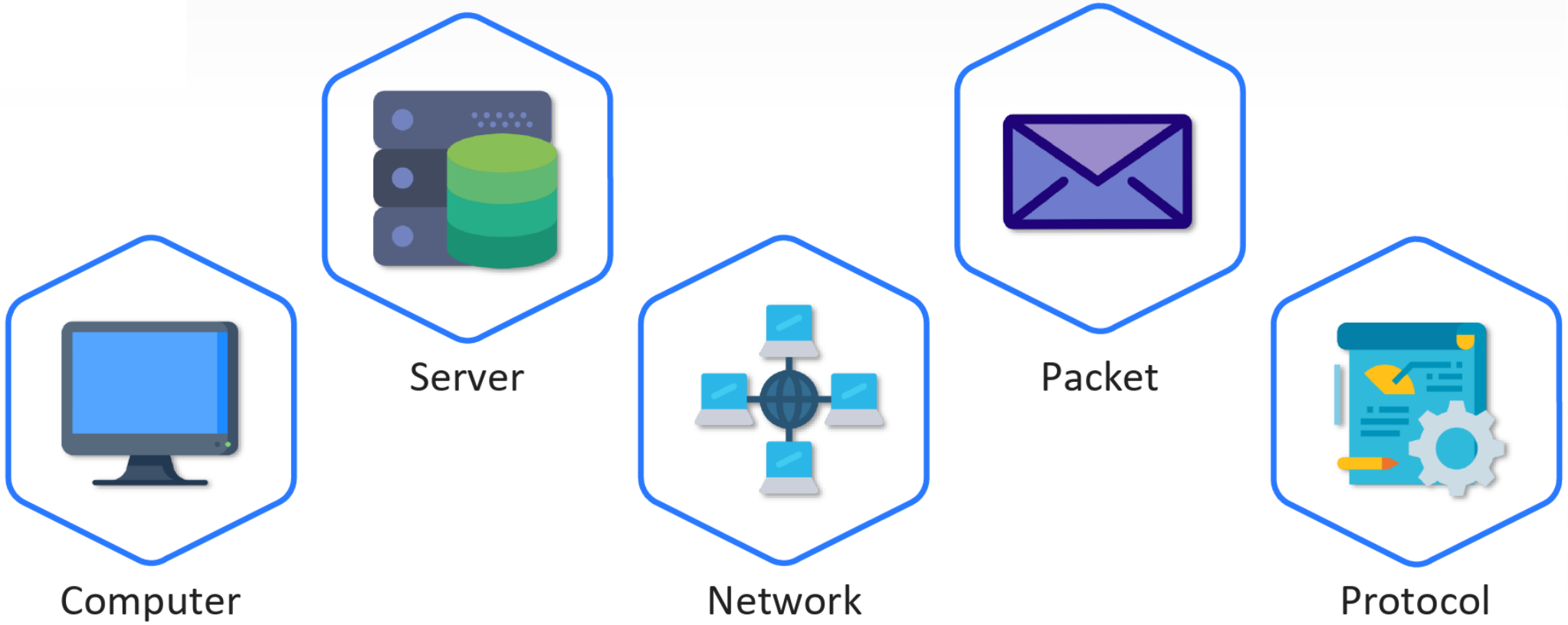
Główne trasy pomiędzy dużymi, strategicznie połączonymi sieciami komputerowymi

Jest własnością zarówno firm prywatnych, jak i rządów

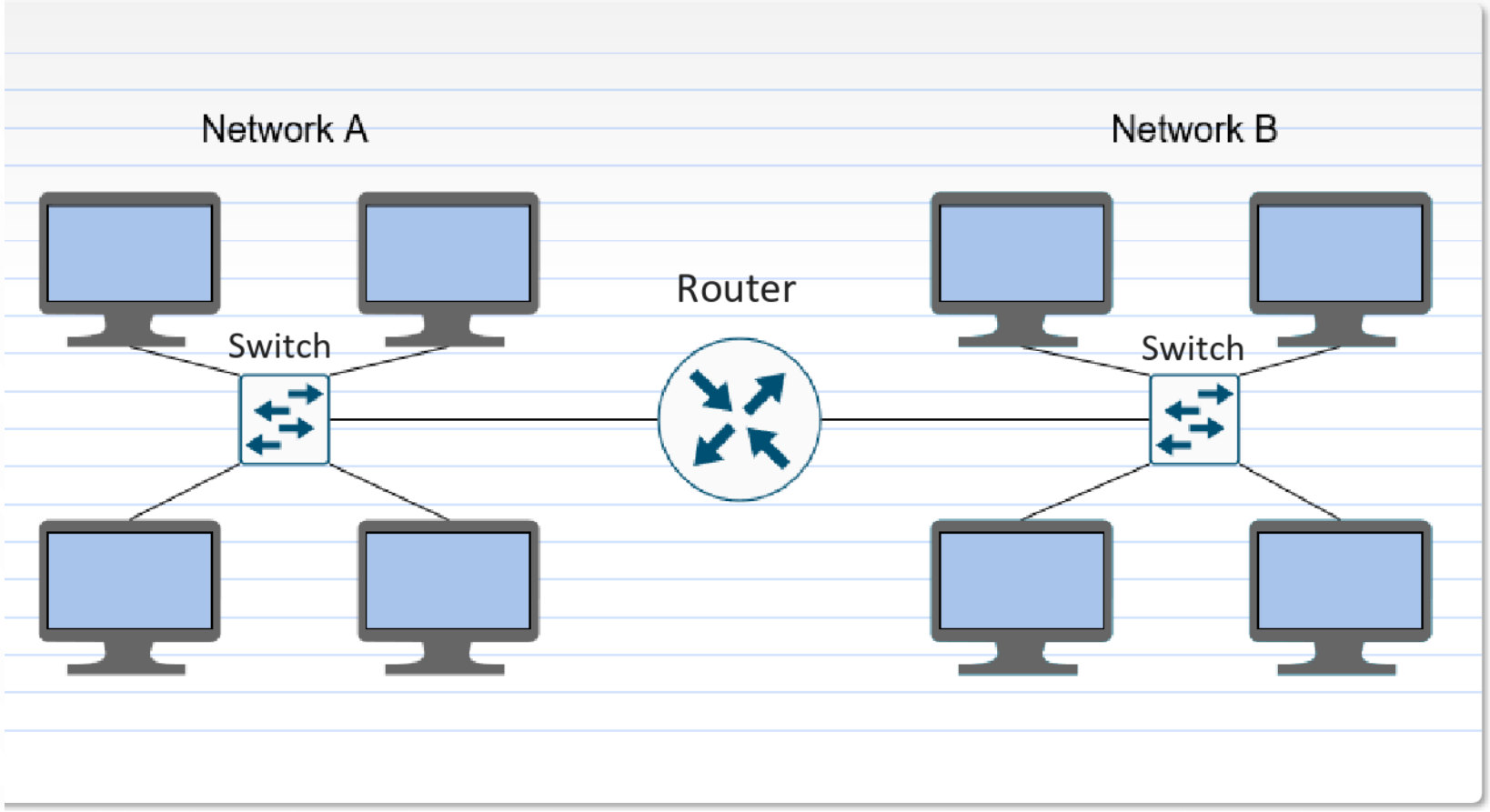
CenturyLink, Comcast i XO Communications to tylko niektóre z firm świadczących tę usługę



TERMINOLOGIA

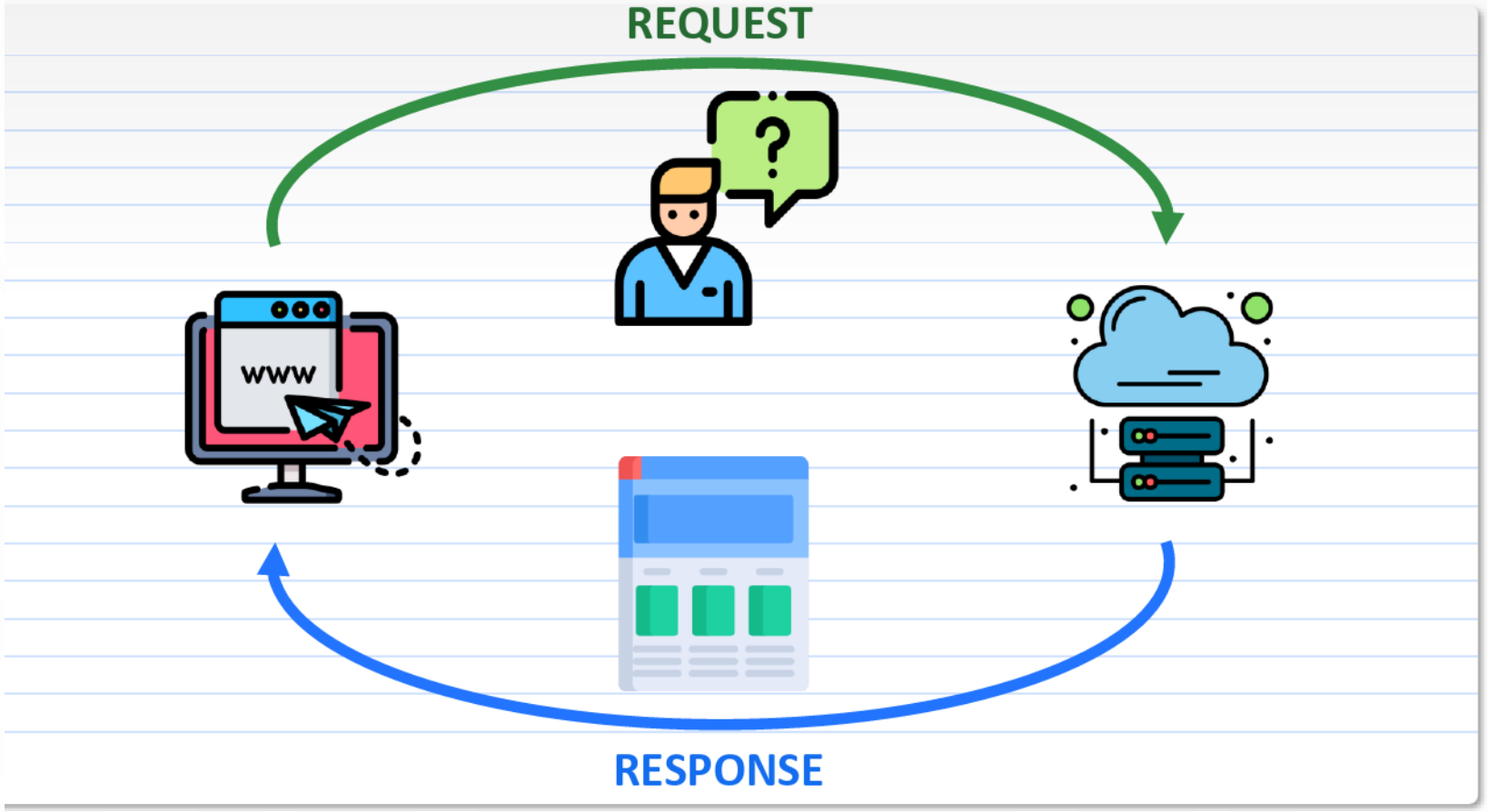


PODSTAWOWA STRUKTURA SIECI KOMPUTEROWEJ



Powyższa ilustracja przedstawia prostą sieć z trzema urządzeniami sieciowymi do zarządzania ruchem pakietów

KOMUNIKACJA W ARCHITEKTURZE KLIENT-SERWER



Ilustracja przedstawia podstawowy proces komunikacji pomiędzy klientem a serwerem

ĆWICZENIE

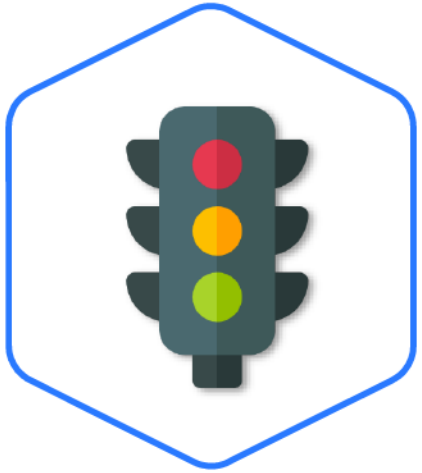
Zapoznaj się z narzędziem do konfiguracji sieci w systemie Windows, macOS lub Linux.

- Otwórz narzędzie do konfiguracji interfejsu sieciowego
- Przestudiuj panel konfiguracyjny

SPRZĘT SIECIOWY

RUCH W SIECI KOMPUTEROWEJ

Pakiety danych
Sieć przypomina system drogowy.
Pakiety danych to pojazdy.



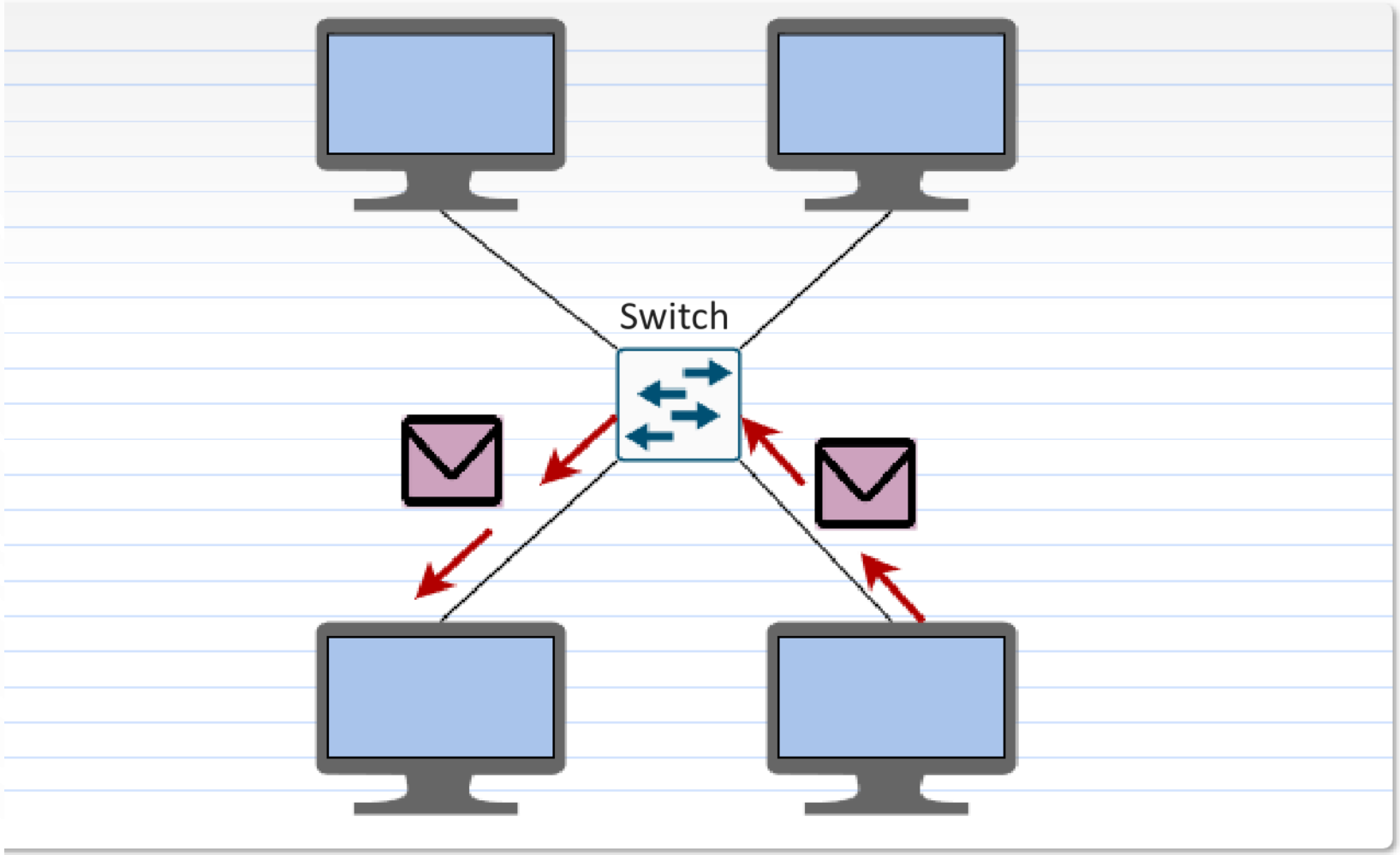
Routery i przełączniki
Kontrolują ruch w taki sam sposób, jak skrzyżowania i sygnalizacja świetlna na drodze.

PRZEŁĄCZNIK SIECIOWY (SWITCH)

Urządzenie sieciowe przekazujące ruch **w obrębie jednej sieci.**

Przekazywanie ruchu w oparciu o adresy MAC (fizyczne).

Przełączniki **nie korzystają** z informacji o adresie IP.

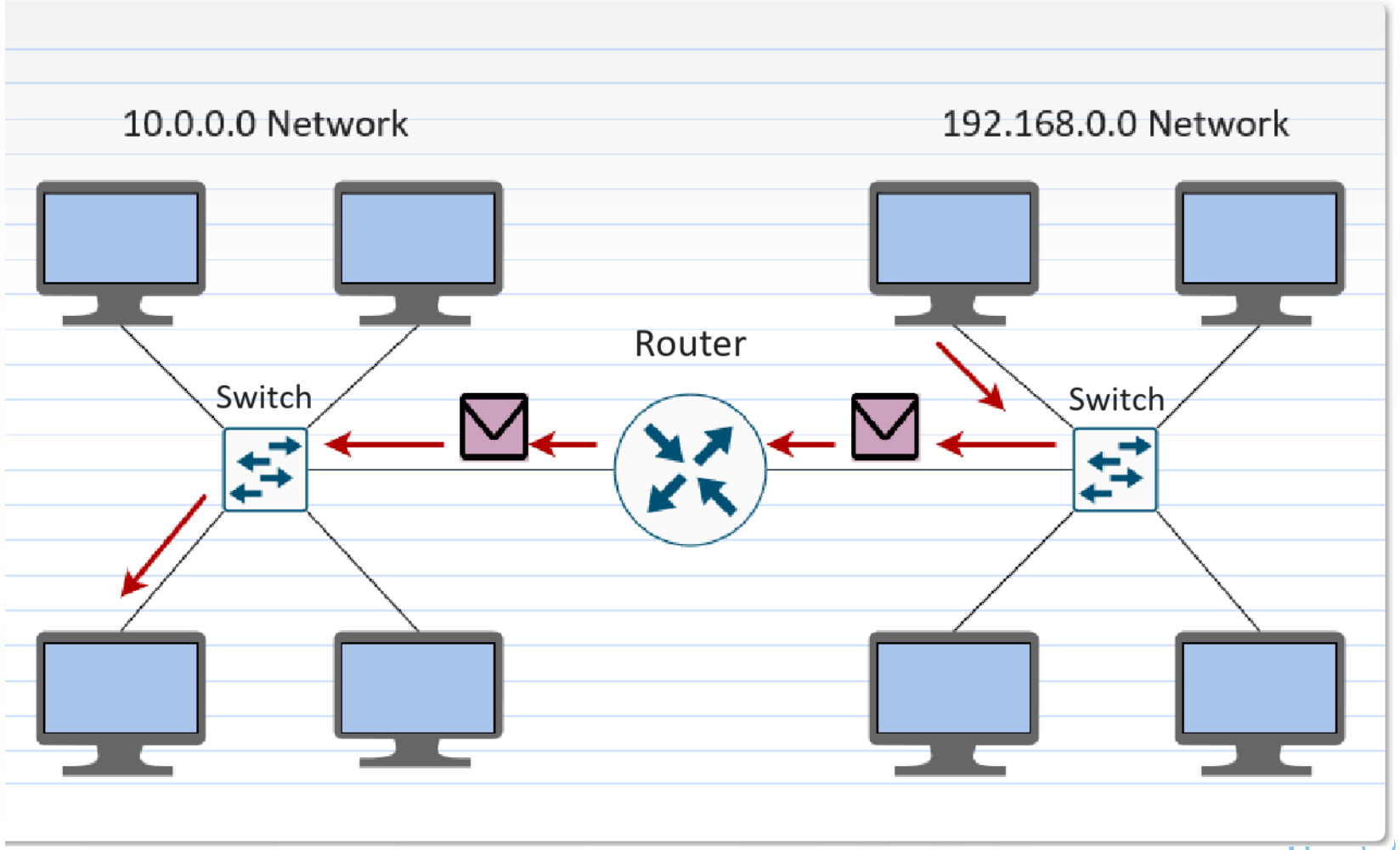


ROUTER

Urządzenie sieciowe przekazujące ruch **pomiędzy sieciami**.

Używa adresów IP do identyfikacji nadawcy i odbiorcy.

Używa tablic routingu
do kierowania ruchem danych.



OCHRONA ROUTERÓW I PRZEŁĄCZNIKÓW

Mechanizm „port security” w przełączniku
Chroni przełącznik przed nieuprawnionymi adresami MAC.

Lista kontroli dostępu (ACL) w routerze
Oparta na regułach funkcja podstawowego filtrowania ruchu.

ADRESOWANIE URZĄDZEŃ SIECIOWYCH

ADRES IP (INTERNET PROTOCOL)

- Identyfikator urządzenia w sieci (np. interfejsu sieciowego komputera)
- Dwie wersje: IPv4 i IPv6
- Służy do komunikacji pomiędzy urządzeniami w różnych sieciach
- Adres logiczny (zmienny)
- Zapisywany w postaci dziesiętnej (v4) lub szesnastkowej (v6)

WERSJE ADRESÓW IP

IPv4
Przykład w notacji dziesiętnej:
192.168.1.1

IPv6
Przykład w notacji szesnastkowej:
2001:0db8:0000:0042:0000:8a2e:0370:7334

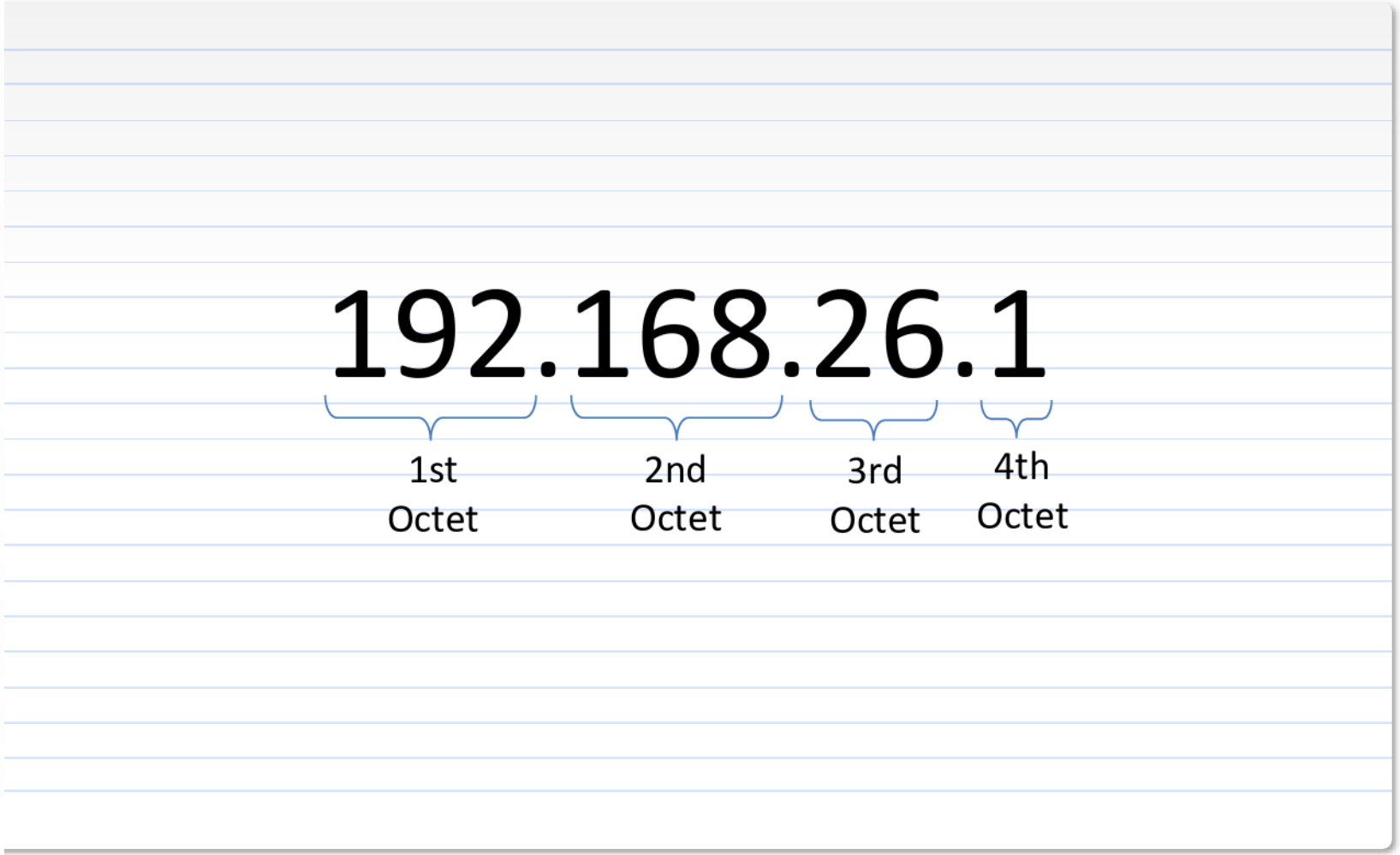
Każde urządzenie końcowe, które może połączyć się z siecią, posiada adres IP

FORMAT ADRESU IPV4

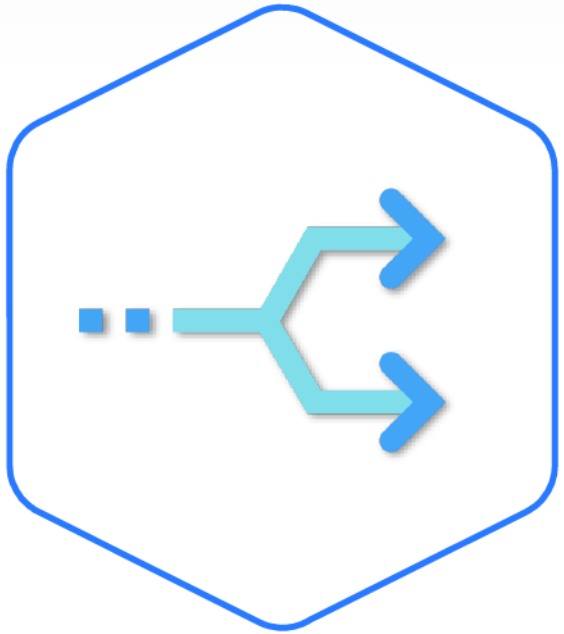
Składa się z czterech liczb oddzielonych kropkami

Każda liczba nazywana jest **oktetem**

Zakres (dziesiętnej) wartości oktetu wynosi od 0 do 255

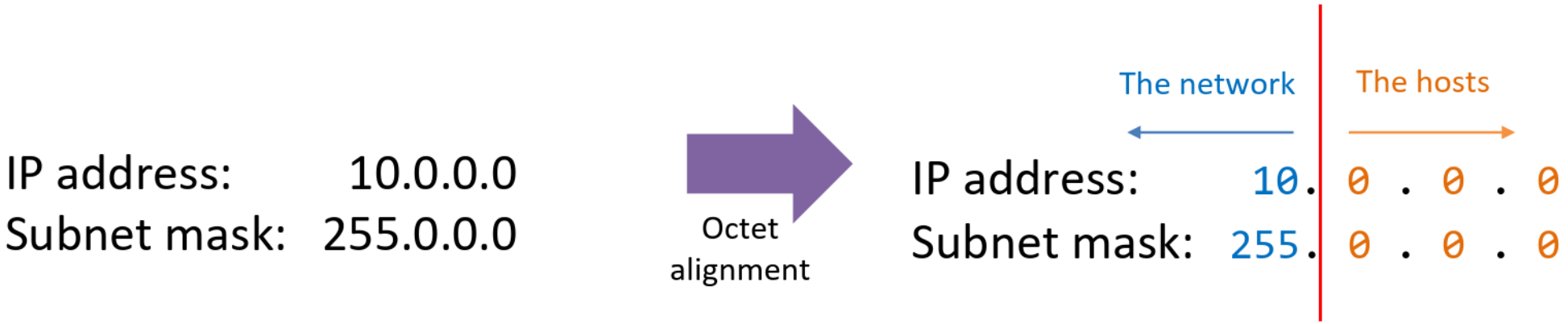


PODSIECI



- Logiczny sposób grupowania adresów IP
- Pomaga określić zasięg sieci
- Historyczny podział na trzy klasy podsieci: A, B, C

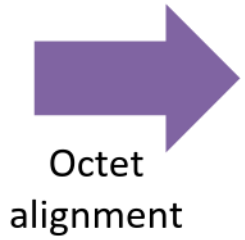
PODSIECI KLASY A

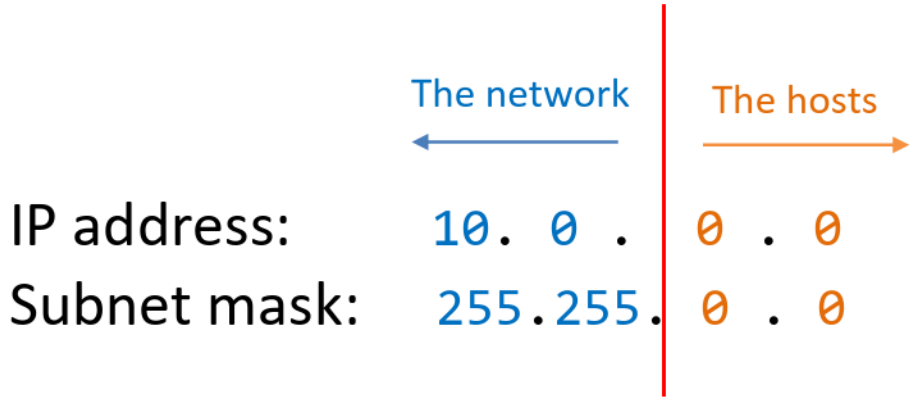


Ilustracja przedstawia maskę podsieci klasy A **255.0.0.0** dla przykładowego adresu IP.

PODSIECI KLASY B

IP address: 10.0.0.0
Subnet mask: 255.255.0.0



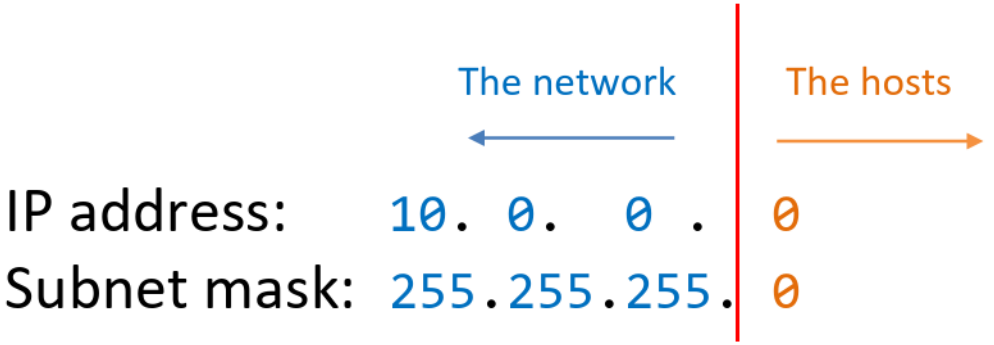


Ilustracja przedstawia maskę podsieci klasy B **255.255.0.0** dla przykładowego adresu IP.

PODSIECI KLASY C

IP address: 10.0.0.0
Subnet mask: 255.255.255.0

Octet alignment



Ilustracja przedstawia maskę podsieci klasy C **255.255.255.0** dla przykładowego adresu IP.

MASKA PODSIECI

Każdy oktet jest reprezentowany przez osiem cyfr binarnych.

/8 reprezentuje pierwszy oktet od lewej.

/16 wskazuje pierwszy i drugi oktet.

/24 wskazuje pierwszy, drugi i trzeci oktet.

255. 0. 0. 0 /8

11111111.00000000.00000000.00000000

255. 255. 0. 0 /16

11111111.11111111.00000000.00000000

255. 255. 255. 0 /24

11111111.11111111.11111111.00000000

PRYWATNE ADRESY IP

Zdefiniowane w dokumencie RFC 1918
dla sieci wewnętrznych/prywatnych

Określone aby opóźnić tempo
wyczerpywania adresów IPv4

Nie można ich używać
do komunikacji w Internecie

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Adresy IP spoza wyżej wymienionych zakresów nazywane są adresami publicznymi.

SPOSOBY KONFIGUROWANIA ADRESÓW IP

Tryb konfiguracji statycznej
Adres IP konfigurowany ręcznie
w panelu konfiguracji interfejsu sieciowego

Tryb konfiguracji dynamicznej
Automatyczna konfiguracja adresu IP.
Adres IP może być używany przez ograniczony czas

Serwery protokołu dynamicznej konfiguracji hosta (Dynamic Host Configuration Protocol - DHCP) mogą przydzielać adresy IP.
Niektóre routery, w tym routery domowe, mają wbudowaną obsługę protokołu DHCP.

ADRESY FIZYCZNE (MEDIA ACCESS CONTROL – MAC)

Unikalny identyfikator sprzętu

Adres fizyczny zapisany w formie szesnastkowej

Przypisany **na stałe** do interfejsu komunikacyjnego urządzenia, które może połączyć się z siecią

ADRES LOCALHOST

- Komputer może komunikować się sam ze sobą.
- Domyślny adres IP to 127.0.0.1; jednakże może to być
- dowolny adres w postaci 127.x.x.x.
- Jego maska podsieci to 255.0.0.0.
- Jest przydatny do testowania systemów i środowisk.

ĆWICZENIE

Ujawnij adresy IP i MAC komputera.

1. Otwórz CMD lub terminal
2. W systemie Windows uruchom polecenie **ipconfig /all**
3. Na komputerze z systemem macOS lub Linux uruchom **ifconfig**
4. Zanotuj adresy IP i MAC.
5. Jaki to rodzaj adresu IP: publiczny czy prywatny?

PROTOKOŁY SIECIOWE I KOMUNIKACJA

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

- ICMP to protokół służący do diagnostyki sieci.
- Określa parametry wydajności sieci.
- Zawiera wiele typów żądań i odpowiedzi.
- Używany przez różne narzędzia sieciowe, takie jak **ping**

PING

Używa żądania „echo” protokołu ICMP

Używany do testowania dostępności hostów i wydajności sieci

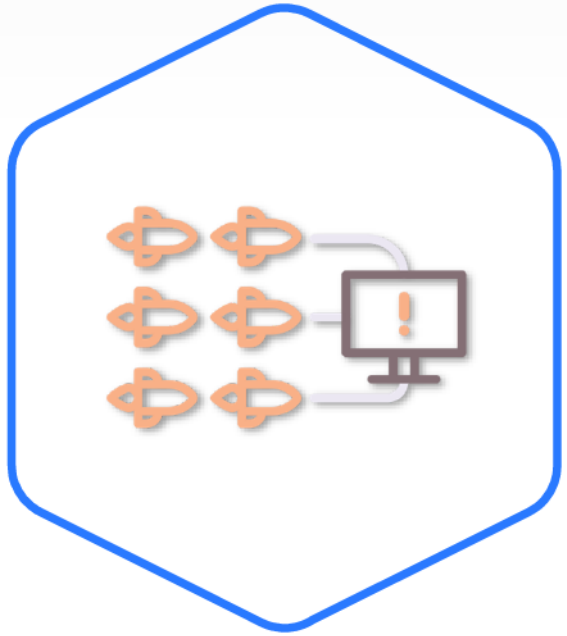
Można go używać do testowania łączności z hostami i adresami witryn internetowych.

```
C:\Users\John>ping 10.21.0.210

Pinging 10.21.0.210 with 32 bytes of data:
Reply from 10.21.0.210: bytes=32 time<1ms TTL=128
Reply from 10.21.0.210: bytes=32 time<1ms TTL=128
Reply from 10.21.0.210: bytes=32 time<1ms TTL=128
Reply from 10.21.0.210: bytes=32 time<1ms TTL=128

Ping statistics for 10.21.0.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

„POWÓDŹ PINGÓW” – PING FLOOD



- Znany również jako „powódź ICMP”
- Obejmuje dużą liczbę żądań ICMP
- Powoduje atak typu Denial of Service (DoS) wygenerowany przy użyciu podstawowych narzędzi

Ping Flood jest potencjalnym zagrożeniem, gdy składa się z bardzo dużych woluminów danych, na przykład w przypadku ataku typu Distributed Denial of Service (DDoS)

TRACEROUTE

- Służy do mapowania sieci
- Używany również do diagnozowania niektórych problemów z komunikacją w sieci
- Pozwala określić trasę do celu
- Może ujawniać informacje o usługach

TRACEROUTE

Traceroute to narzędzie uruchamiane w wierszu poleceń, które wyświetla ścieżkę pakietu do miejsca przeznaczenia

Podobnie jak ping, używa protokołu ICMP, ale mierzy każdy adres IP na ścieżce i czas potrzebny na każdy „przeskok”

```
C:\>tracert cisco.com

Tracing route to cisco.com [72.163.4.185]
over a maximum of 30 hops:

  1     9 ms     5 ms     5 ms  Docsis-Gateway.hsd1.co.comcast.net [10.1.10.1]
  2    15 ms    16 ms    15 ms  cm-1-acr02.englewood.co.denver.comcast.net [96.120.13.65]
  3    20 ms    15 ms    14 ms  ae-252-1210-rur102.englewood.co.denver.comcast.net
[96.110.242.129]
  4    24 ms    13 ms    13 ms  ae-2-rur01.englewood.co.denver.comcast.net [68.86.104.69]
  5    13 ms    15 ms    18 ms  ae-27-ar01.denver.co.denver.comcast.net [68.86.128.5]
  6    18 ms    21 ms    36 ms  ae-13.edge8.Denver1.Level3.net [4.68.63.165]
  7    29 ms    30 ms    35 ms  ae-4-15.edge5.Dallas3.Level3.net [4.69.208.233]
  8    33 ms    35 ms    29 ms  CISCO-SYSTE.edge5.Dallas3.Level3.net [4.59.34.66]
  9    29 ms    32 ms    28 ms  rcdn9-cd1-cbb-gw1-ten0-0-0-12.cisco.com [72.163.0.5]
 10    32 ms    35 ms    31 ms  72.163.0.102
 11    30 ms    31 ms    29 ms  rcdn9-cd1-dmzdcc-gw1-por2.cisco.com [72.163.0.186]
 12    32 ms    32 ms    29 ms  rcdn9-16b-dcz05n-gw2-por1.cisco.com [72.163.2.102]
 13    32 ms    31 ms    30 ms  redirect-ns.cisco.com [72.163.4.185]
```

DOMAIN NAME SYSTEM (DNS)

- Ułatwia korzystanie z Internetu
- Zapewnia translację nazwy na adres IP
- Eliminuje potrzebę zapamiętywania adresów IP

USŁUGI DNS

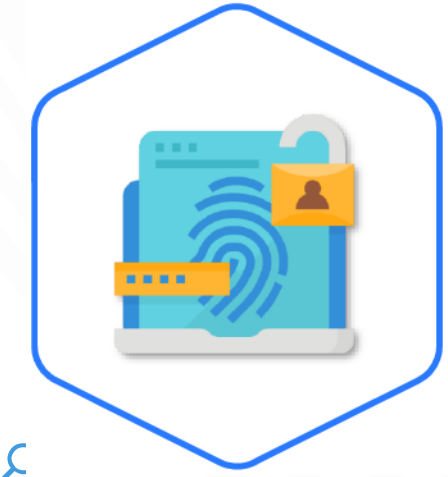
Komputery w domu komunikują się z serwerami DNS dostawcy usług internetowych za pośrednictwem routerów domowych, które mogą nie być chronione.

Wiele firm oferuje usługi związane z bezpieczeństwem w oparciu o publiczny system DNS

Usługi filtrują żądania DNS w celu wykrywania i blokowania niepożądanych i/lub podejrzanych działań.

OCHRONA USŁUG DNS

„Zatruwanie” DNS
Zapytania i rekordy DNS mogą być manipulowane w złośliwych celach.



Domain Name System Security Extensions (DNSSEC)
Zapewnia bezpieczeństwo uwierzytelniania wymienianych danych.

ĆWICZENIE

Użyj poleceń ping i traceroute w kilku scenariuszach

Poćwicz pracę z poleceniem **ping**
Poćwicz pracę z funkcją **traceroute** (**tracert** w systemie Windows)

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

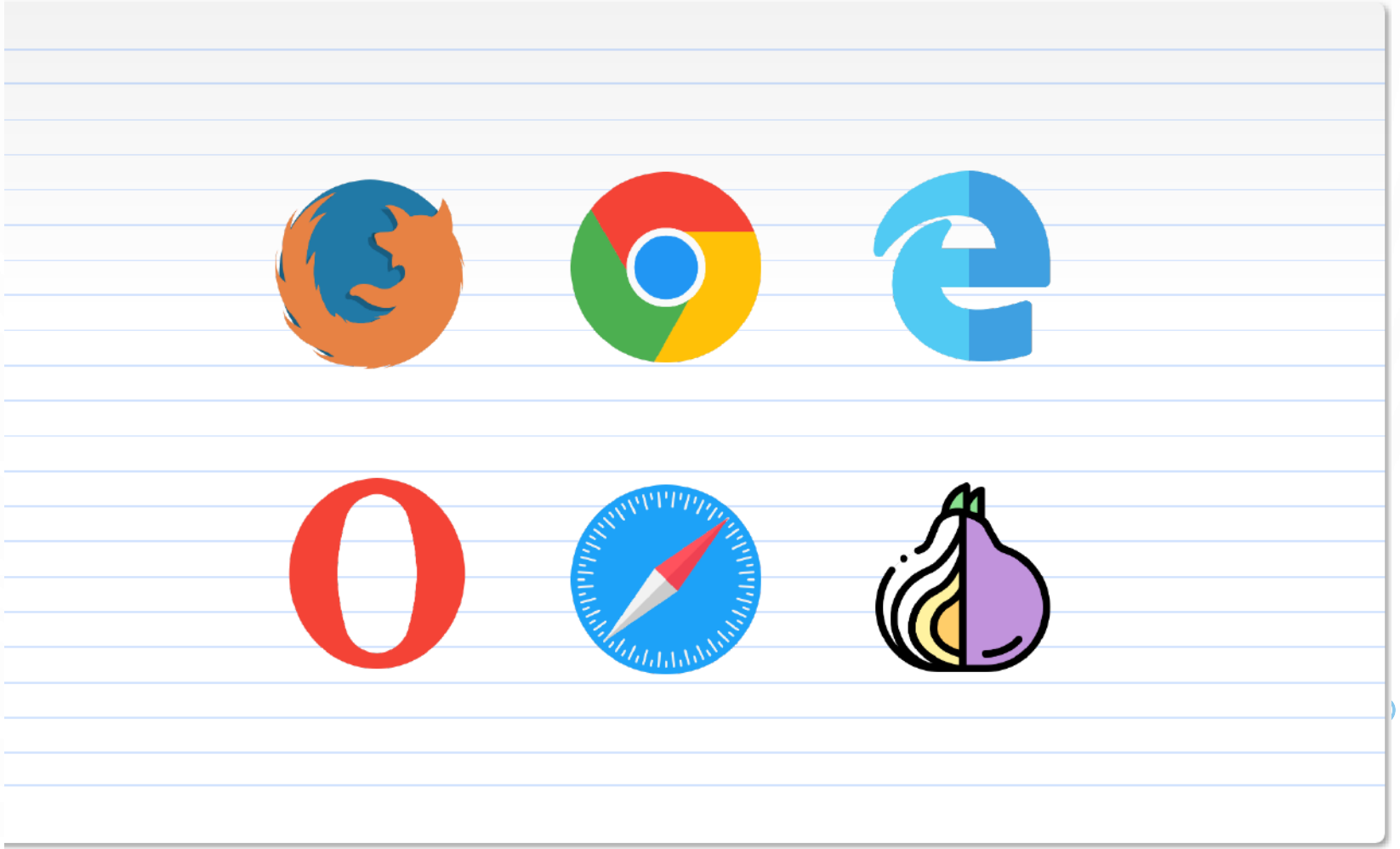
- Ułatwia komunikację w sieci
- Przypisuje interfejsom sieciowym adresy IP, maski podsieci i adres bramy domyślnej
- Eliminuje potrzebę ręcznej konfiguracji ustawień sieciowych

PRZEGLĄDARKA INTERNETOWA

Interaktywny program żądający informacji z serwerów internetowych

Używa adresów URL i IP do kontaktowania się z serwerami

Do wymiany informacji wykorzystuje protokoły HTTP lub HTTPS



UNIFORM RESOURCE LOCATOR (URL)

Adres URL jednoznacznie identyfikuje zasób w sieci

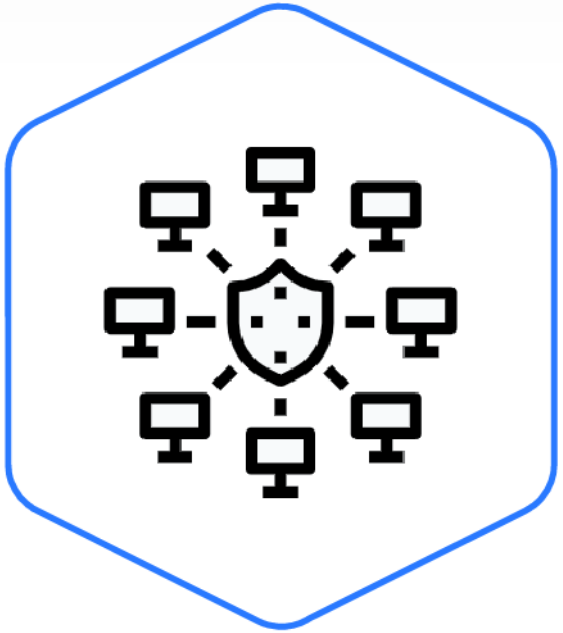
Format adresu URL:
protokół://host:port/scieżka-i-nazwa-pliku

Adresy URL mogą być wykorzystywane do szkodliwych celów, takich jak **phishing**. Złośliwe adresy URL można próbować ukryć (**Faceb00k.com**)

HYPERTEXT TRANSFER PROTOCOL/SECURE

- Określa sposób wymiany danych treści internetowych
- Komunikacja pomiędzy klientem HTTP a serwerem HTTP
- HTTPS dodaje warstwę szyfrowania do danych

IP SECURITY



- Można przeglądać informacje przesyłane przez sieci komputerowe
- Protokoły IPsec i HTTPS zapewniają dosyć bezpieczny sposób komunikacji poprzez zapewnienie uwierzytelniania i szyfrowania

DODATKOWE POLECENIA SIECIOWE

arp -a: Wyświetla listę nauczonych maszynowo odwzorowań adresu MAC na adres IP

nslookup: Używa skonfigurowanego głównego serwera DNS do rozpoznawania, rozwiązywania problemów i sprawdzania różnych typów rekordów DNS

pathping: połączenie polecenia **ping** i polecenia **tracert;**
polecenie pathping służy do śledzenia trasy do określonego miejsca docelowego podczas testowania połączenia z każdym „przeskokiem”

DZIĘKUJĘ ZA UWAGĘ!

MACIEJ.RYBCZYNSKI@UJK.EDU.PL