Sieci komputerowe – wybrane zagadnienia
Wykład w ramach przedmiotu „Informatyka” (EE-DI)

Dawid Warchoł

Zakres materiału na temat sieci komputerowych

- Zagadnienia związane z sieciami komputerowymi były lub będą dość obszernie omawiane w ramach przedmiotu Technologie Informacyjne.
- W związku z tym na niniejszym wykładzie nie będzie obszernego omówienia tematyki sieci komputerowych (struktury sieci, protokoły itd.).
- Skupimy się głównie na problemie adresacji IP.
- Kilka zagadnień lub podstawowych definicji może się powtórzyć na obu przedmiotach, ale główna część tego wykładu będzie stanowić uzupełnienie materiału z TI i pomoże zrozumieć w praktyce zagadnienie adresacji IP.

Sieć komputerowa i host – definicje

- Sieć komputerowa jest **zbiorem komputerów i innych urządzeń** (smartfony, drukarki, konsole do gier, serwery, routery itp.), które są ze sobą połączone (przewodowo lub bezprzewodowo) w celu **wymiany danych i współdzielenia zasobów**.

- Urządzenia w sieci, które mogą wysyłać i odbierać dane, są nazywa **hostami**.

Adres IP – definicja

- Adres IP (Internet Protocol Address) to unikatowy identyfikator przypisany każdemu urządzeniu w sieci komputerowej (hostowi) opartej na protokole IP.
- IP służy do identyfikowania i adresowania hostów, dzięki czemu mogą się one ze sobą komunikować.
- Istnieje sześć wersji IP, ale tylko dwie przyjęły się i weszły do powszechnego użycia: IPv4 oraz IPv6.

IPv4

- Przykładowy adres IPv4: `192.168.1.10`

- Adres IPv4 jest 32-bitowy. Składa się z czterech liczb (zazwyczaj zapisywanych w systemie dziesiątkowym) z zakresu 0-255, oddzielonych kropką.

IPv6

- Przykładowy adres IPv6: `2001:db8:85a3:0:0:8a2e:370:7334`

- Adres IPv6 jest 128-bitowy. składa się z ośmiu liczb (zazwyczaj zapisywanych w systemie szesnastkowym) z zakresu 0-65535(10), czyli 0-ffff(16).
- Liczby są oddzielone dwukropkiem.
- Jeden, dowolny ciąg sąsiadujących liczb, które mają wartość zero, można zastąpić ciągiem `::`.
- Przykładowo, adres: `2001:db8:85a3:0:0:8a2e:370:7334` można zapisać jako: `2001:db8:85a3::8a2e:370:7334`.
- Można tak zrobić tylko raz w całym adresie.

Podsieć, maska podsieci

- Sieci komputerowe możemy dzielić na mniejsze segmenty (tzw. podsieci).
- Taki podział wykonuje się za pomocą maski podsieci.
- Maska podsieci ma format podobny do adresu IP; w protokole IPv4 składa się z czterech liczb z zakresu 0-255 oddzielonych kropką.
- Jeśli zapiszemy te liczby w systemie dwójkowym, to zawsze na początku będą same jedynki, a potem same zera.
- Przykłady masek podsieci:
  - 255.255.255.0 (11111111.11111111.11111111.00000000(2))
  - 255.255.255.192 (11111111.11111111.11111111.11000000(2))
  - 255.255.240.0 (11111111.11111111.11110000.00000000(2))

Maska podsieci – alternatywny zapis

- Maskę podsieci czasami zapisuje się w skrótowy sposób, podając jedynie liczbę z przedziału 0-32 na końcu adresu IP po znaku ukośnika.
- Przykładowo, jeśli mamy adres IP:

192.168.1.0

i maskę podsieci:

255.255.0.0,

to adres wraz z maską możemy zapisać w formie:

192.168.1.0/16

ponieważ 255.255.0.0 to dwójkowo 11111111.11111111.0000000.00000000(2),

a więc jest łącznie 16 jedynek w masce.

Podział sieci przy użyciu maski podsieci

- Jedynki w masce podsieci oznaczają bity odpowiadające adresowi sieci (podsieci)
- Zera oznaczają bity, które odpowiadają adresowi hosta w tej sieci.
- Przykładowo, jeśli mamy adres IP:

192.168.1.0

i maskę podsieci:

255.255.255.0,

to pierwsze trzy liczby całe liczby adresu IP odpowiadają adresowi sieci, natomiast ostatnia, czwarta, liczba odpowiada adresowi hosta.

- Jeśli jedynki w masce kończą się w środku liczby, a nie na jej końcu, to wydzielanie adresu sieci jest nieco bardziej skomplikowane.
- Takim przypadkiem zajmiemy się tym za chwilę, w ramach zadań.

Specjalne adresy IPv4

- Istnieje kilka adresów IPv4 specjalnego przeznaczenia. Oto trzy najważniejsze:
  - 127.0.0.1 – adres pętli zwrotnej (loopback).
    - Umożliwia komunikację hosta z samym sobą.
    - Za jego pomocą można np. odwołać się do serwera bazodanowego działającego na tym samym komputerze, z którego chcemy obsługiwać bazę.
    - Taki adres można zastąpić słowem *localhost*.
  - 0.0.0.0 – adres nieokreślony.
    - Może oznaczać brak adresu lub nasłuchiwanie ze wszystkich hostów.
  - Adres rozgłoszeniowy (broadcast).
    - Jest to ostatni adres możliwy do utworzenia w danej sieci.
    - Tworzy się go ustawiając wszystkie bity dotyczące hosta na jedynki.
    - Umożliwia rozgłaszanie, czyli wysyłanie danych do wszystkich komputerów w sieci, bez podawania ich konkretnych adresów.
    - Przykład adresu broadcast: 192.168.255.255 ($11000000.10101000.11111111.11111111_{(2)}$)

Zadanie 1

- Mając dany adres IP: 192.168.145.56 oraz maskę podsieci: 255.255.224.0, wyznacz adres sieci oraz adres rozgłoszeniowy w postaci dziesiątkowej. Oblicz również maksymalną możliwą liczbę hostów danej sieci. Należy zapisać obliczenia związane z zamianą systemów liczbowych oraz wyznaczeniem liczby hostów.

- UWAGA: Tego typu zadanie będzie na końcowym zaliczeniu wykładu.

Zadanie 1 – rozwiązanie

- Krok I: Zapisanie adresu IP i maski podsieci w systemie dwójkowym:

```
IP:     11000000.10101000.10010001.00111000
MASKA:  11111111.11111111.11100000.00000000
```

- Krok II: Wykonanie operacji logicznej AND na każdym bicie IP i odpowiadającym mu bicie maski.
  - Innymi słowy, przepisanie wszystkich bitów IP na lewo od granicy maski (zaznaczonej czerwoną linią) i wyzerowanie wszystkich bitów na prawo od granicy maski.
    - Uwaga: bity IP i maski muszą być do siebie dopasowane (wyrównane w poziomie).
  - Wynik tej operacji (AND) jest adresem sieci:

    `11000000.10101000.10000000.00000000`
  - Zgodnie z treścią zadania musimy go zapisać w postaci dziesiątkowej:

    `192.168.128.0` → Adres sieci – pierwszy (z trzech) wynik zadania

Zadanie 1 – rozwiązanie

```
IP:     11000000.10101000.10010001.00111000
MASKA:  11111111.11111111.11100000.00000000
```

- Krok III: Wszystkie bity IP na prawo od granicy maski należy zamienić na jedynki:
  - Wynik tej operacji jest adresem rozgłoszeniowym:

    `11000000.10101000.10011111.11111111`
  - Zgodnie z treścią zadania musimy go zapisać w postaci dziesiątkowej:

    `192.168.159.255` → Adres rozgłoszeniowy – drugi (z trzech) wynik zadania

Zadanie 1 – rozwiązanie

- Krok IV: Pozostała nam jeszcze do wyznaczenia maksymalna możliwa liczba hostów danej sieci.
- Jest ona zawsze równa $\mathbf{2^{nzm}-2}$,

  gdzie *nzm* jest liczbą zer w masce podsieci (**n**umber of **z**eros in **m**ask).
- W naszym przypadku *nzm* jest równe 13.
- A więc obliczamy $2^{13} - 2 = \underline{8190}$.

Maksymalna możliwa liczba hostów sieci – trzeci (z trzech) wynik zadania.

- Pytanie: Skąd wynika ten wzór?
- Odpowiedź:
  - 2^{nzm} oznacza liczbę wszystkich możliwych kombinacji, które można zapisać na tylu bitach, ile jest przeznaczonych na host (prawa strona maski);
  - Od całości odejmujemy 2 ze względu na to, że adresem hosta nie mogą być same zera (adres sieci) ani same jedynki (adres rozgłoszeniowy).

Zadanie 1 – rozwiązanie – przydatny trik

- Tak naprawdę na początku zadania nie musimy zapisywać wszystkich liczb (bajtów) adresu IP oraz maski w systemie dwójkowym.
- Wystarczy zapisać dwójkowo jedynie tą liczbę maski, w której następuje granica (inna liczba niż 0 i 255) i odpowiadającą jej liczbę adresu IP. W naszym przypadku jest to trzecia liczba.

```
IP:     192.168.10010001.56
MASKA: 255.255.11100000.0
```

- Dalsze obliczenia również się skrócą, ponieważ nie będziemy musieli z powrotem konwertować wszystkich liczb dwójkowych na system dziesiątkowy (jedynie trzecią).
  - Adres sieci:

    $192.168.10000000_{(2)}.0 = \underline{192.168.128.0}$
  - Adres rozgłoszeniowy:

    $192.168.10011111_{(2)}.255 = \underline{192.168.159.255}$

Co w przypadku, gdy granica jest umiejscowiona między liczbami?

- Jeśli granica w masce podsieci jest umiejscowiona między liczbami, a nie wewnątrz liczby, to mamy bardzo prostą sytuację.
- Nie trzeba w ogóle zamieniać liczb na system dwójkowy, robić podziałów, ani wykonywać operacji AND.
- Przykład:
  - IP: 192.168.85.23
  - Maska: 255.255.0.0
- Rozwiązanie:
  - Adres sieci: 192.168.0.0
  - Adres rozgłoszeniowy: 192.168.255.255
  - Maksymalna możliwa liczba hostów: $2^{16} - 2 = 65\,534$

Zadanie 2

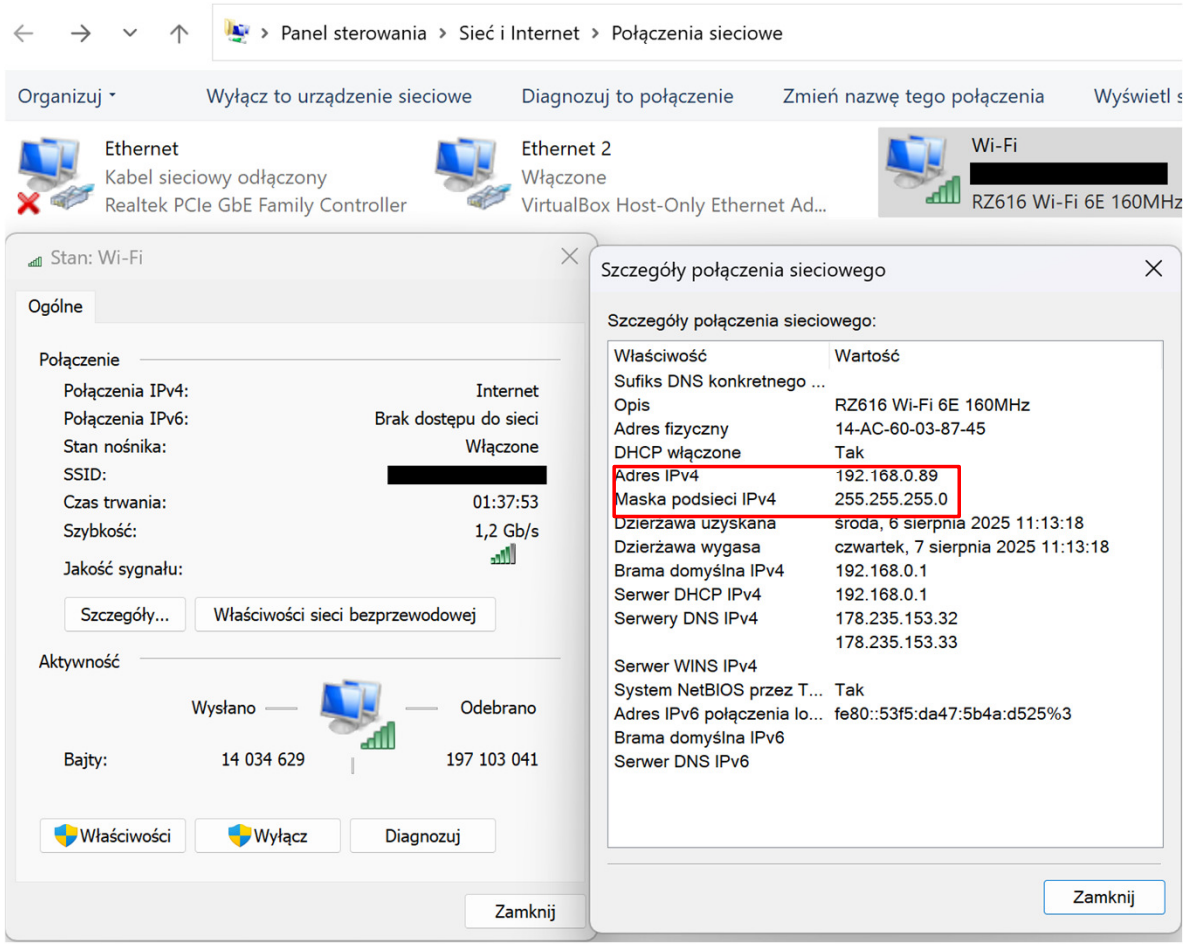
- Mając dany adres IP: 224.204.135.56 oraz maskę podsieci: 255.255.225.240, wyznacz adres sieci oraz adres rozgłoszeniowy w postaci dziesiątkowej. Oblicz również maksymalną możliwą liczbę hostów danej sieci. Należy zapisać obliczenia związane z zamianą systemów liczbowych oraz wyznaczeniem liczby hostów.

- Zadanie jest do samodzielnej realizacji.
- Rozwiązanie krok po kroku nie zostanie więc zaprezentowane, ale wyniki końcowe można odczytać na następnym slajdzie.

Zadanie 2 – wyniki

- Adres sieci: 224.204.135.48
- Adres rozgłoszeniowy: 224.204.135.63
- Maksymalna możliwa liczba hostów: 14

Jak sprawdzić adres IP i maskę przypisaną do interfejsu sieciowego (karty sieciowej w komputerze) w systemie Windows?



Wiersz polecenia (CMD):

```
C:\Users\      >ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::53f5:da47:5b4a:d525%3
   IPv4 Address. . . . . . . . . . . : 192.168.0.89
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Jak sprawdzić adres IP i maskę przypisaną do interfejsu sieciowego (karty sieciowej w komputerze) w systemach Linux i macOS?

- W systemach Linux i macOS adres IP oraz maskę podsieci możemy sprawdzić poleceniem *ifconfig* lub *ip addr* wpisując go w konsoli systemowej (wierszu poleceń).

- UWAGA: Nazwy tych poleceń w Windows i Linux/macOS są podobne, ale nie identyczne. Windows: *ipconfig*, Linux/macOS: *ifconfig*.

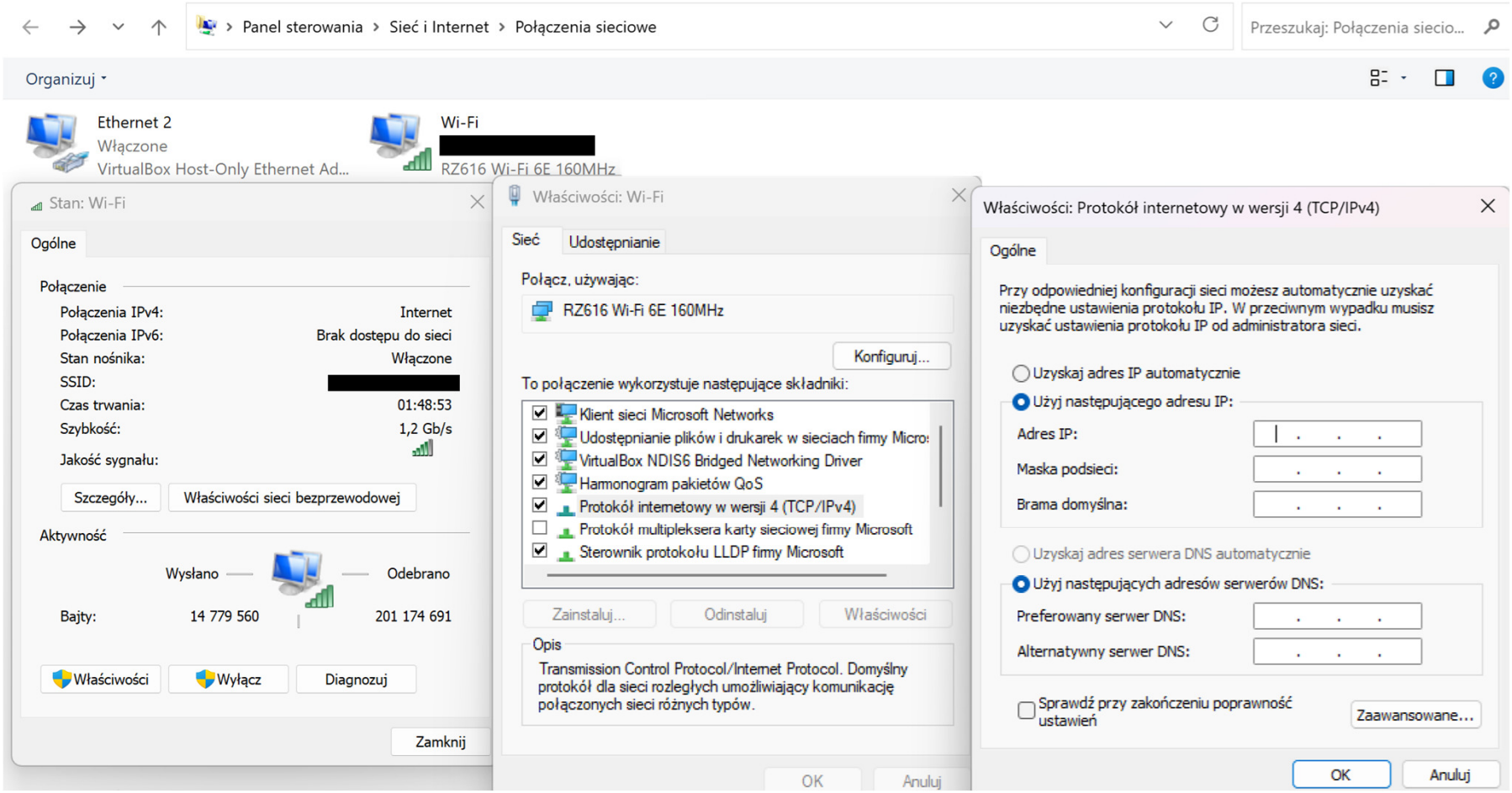
Brama domyślna

- Odczytując adres IP i maskę podsieci możemy zauważyć również dodatkowy adres IP oznaczony jako brama domyślna (ang. default gateway).
- Brama domyślna to adres urządzenia, które służy jako "wyjście" z sieci lokalnej do innych sieci, najczęściej do Internetu.
- Najczęściej rolę bramy domyślnej pełni router.
- Gdy komputer próbuje połączyć się z adresem IP, który nie należy do jego sieci lokalnej, wysyła pakiety właśnie do bramy domyślnej. Router przekazuje je dalej – na zewnątrz sieci.

Ręczna (nieautomatyczna) konfiguracja sieci

- Tworząc nową sieć lub podłączając nowego hosta do sieci zazwyczaj następuje automatyczna konfiguracja.
- Odpowiada za to serwer DHCP (Dynamic Host Configuration Protocol).
- Czasami zachodzi potrzeba ręcznego skonfigurowania sieci. Może to być konieczne np. gdy:
  - podłączamy urządzenie, które ma być zawsze dostępne pod tym samym adresem, np. drukarka, kamera sieciowa itp. (DHCP może przydzielić inny adres po ponownym połączeniu urządzenia do tej samej sieci);
  - tworzymy małą, lokalną sieć bez Internetu, np. łącząc bezpośrednio dwa komputery kablem sieciowym;
  - chcemy skomunikować urządzenia (np. mikrokomputery) z prostym systemem bez GUI (graficznego interfejsu użytkownika);
  - z jakiegoś powodu nie jest dostępny serwer DHPC (np. administrator sieci wyłączył go w routerze przez pomyłkę).

Jak skonfigurować sieć (ustawić adres IP, maskę podsieci i bramę domyślną) w systemie Windows?



Jak skonfigurować sieć (ustawić adres IP, maskę podsieci i bramę domyślną) w systemach Linux i macOS?

- W systemach Linux i macOS możemy dokonać konfiguracji w konsoli systemowej za pomocą polecenia *ifconfig* (klasyczny sposób) lub *ip addr add* (bardziej nowoczeny sposób).
- Przykład z *ifcofig*:

```
ifconfig eth0 192.168.1.10 netmask 255.255.255.0 up
route add default gw 192.168.1.1
```

- Przykład z *ip addr add*:

```
ip addr add 192.168.1.10/24 dev eth0
ip link set eth0 up
ip route add default via 192.168.1.1
```

- *eth0* oznacza nazwę interfejsu sieciowego (w tym przypadku Ethernet, czyli sieć przewodowa).

Jak skonfigurować sieć lokalną – ogólne zasady

- Należy ustalić adres IP i maskę podsieci w taki sposób, aby:
  - bity należące do adresu sieci we wszystkich komputerach były takie same;
  - Bity odpowiadające hostowi były różne (uwaga: nie może być kilku urządzeń o tym samym adresie IP w sieci).

Serwer DNS

- Na slajdzie dotyczącym konfiguracji sieci w systemie Windows można było zauważyć pole oznaczone jako serwer DNS.
- DNS (ang. Domain Name System) jest serwerem, którego głównym zadaniem jest tłumaczenie nazw stron internetowych.
- System musi znać adres tego serwera, aby był wiedział, jakie adresy IP odpowiadają wpisywanym nazwom symbolicznym (np. serwer portalu Wirtualna Polska, www.wp.pl, ma adres 212.77.100.83).
- Jeśli konfigurujemy połączenie sieciowe ręcznie i nie korzystamy z DHCP, to musimy podać adres serwera DNS. Nie zostanie on automatycznie znaleziony.
- Gdybyśmy tego nie zrobili, to wchodząc na strony internetowe musielibyśmy podawać ich adresy IP zamiast nazw symbolicznych.
- Najpopularniejsze serwery DNS mają adresy 8.8.8.8 (Google) i 1.1.1.1 (Cloudflare).

Sprawdzenie połączenia między hostami

- Jeśli chcemy sprawdzić, czy host o określonym adresie IP jest osiągalny w sieci (lokalnej lub globalnej – Internet), to możemy skorzystać z polecenia *ping* dostępnego w systemach Windows, Linux i macOS.
- Np. aby sprawdzić, czy mamy połączenie z komputerem o adresie 192.168.1.10, należy wpisać w wierszu poleceń:

```
ping 192.168.1.10
```

- Jeśli udało się nawiązać połączenie, to w systemie Windows otrzymamy cztery komunikaty podobne do tego:

```
Reply from 192.168.1.10: bytes=32 time=19ms TTL=112
```

- Jeśli nie udało się nawiązać połączenia, to otrzymamy komunikat:

```
Request timed out.
```

Jak interpretować odpowiedzi uzyskane z polecenia *ping*

```
Reply from 192.168.1.10: bytes=32 time=19ms TTL=112
```

- Ping wysyła tzw. pakiety ICMP Echo Request do hosta docelowego. W systemie Windows wysyłane są pakiety o rozmiarze 32 B (plus dodatkowe 8 B nagłówka).
- W odpowiedzi:
  - bytes – liczba bajtów pakietu, które odesłał host docelowy i które wróciły do naszego urządzenia.
  - time – czas odpowiedzi (zwany również opóźnieniem lub latencją) w milisekundach, liczony od momentu wysłania pakietu do momentu odebrania pakietu zwrotnego.
  - TTL (Time To Live) – długość „życia" pakietu. Ta wartość zmniejsza się o 1 za każdym razem, kiedy pakiet wysłany przez host docelowy przechodzi przez host pośredni (ruter). Gdy dojdzie do 0, pakiet zostaje natychmiast odrzucony, a do nadawcy wysyłany jest komunikat o błędzie. Zapobiega to krążeniu pakietu w nieskończoność.

Dodatkowe informacje na temat TTL

```
Reply from 192.168.1.10: bytes=32 time=19ms TTL=112
```

- System Windows ustawia domyślnie TTL na 128, Linux i macOS na 64, niektóre urządzenia sieciowe (np. Cisco, Juniper) na 256.

- W naszym przykładzie otrzymaliśmy wartość niewiele mniejszą niż 128. Oznacza to, że prawdopodobnie host, z którym się połączyliśmy pracuje w systemie Windows i pakiet, który został do nas odesłany przeszedł przez 128-112=16 ruterów.

ping w systemach Linux i macOS

- Polecenie *ping* w systemach Linux i macOS działa bardzo podobnie.
- Główną różnicą jest wielkość wysyłanego pakietu. W Linuksie i macOS domyślnie jest to 64 B (a nie 32 B jak w Windowsie).
- Różni się też ilość wysyłanych pakietów. W Windowsie *ping* wysyła domyślnie 4 pakiety i kończy działanie, a w Linuksie/macOS działa dopóki użytkownik nie przerwie programu (skrótem Ctrl+C).
- Komunikaty zwrotne mają trochę inny format, ale nie ma większych różnic.

Zadanie 3

- Spróbuj „zapingować” do serwera oficjalnej strony Linuksa: linux.org i sprawdź komunikaty odpowiedzi (w szczególności TTL).

Podpowiedź: można wpisać adres symboliczny hosta zamiast adresu IP.

Sprawdzanie adresu IP przez zewnętrzne strony internetowe

- Adres IP swojego komputera można również odczytać ze stron typu *www.whatismyip.com*.
- Gdybyśmy ten adres porównali z adresem odczytanym w systemie operacyjnym, to prawie zawsze okaże się, że adresy są inne. Dlaczego?
- Adres odczytany w systemie, to adres prywatny (lokalny), używany w sieci lokalnej. Można się nim komunikować z innymi urządzeniami, które połączyły się z naszą siecią (np. przez WI-FI).
- Adres ze stron typu *www.whatismyip.com*, to adres publiczny, przypisany przez dostawcę Internetu. Za jego pomocą możemy się komunikować w Internecie.

Sprawdzanie adresu IP przez zewnętrzne strony internetowe

- Najczęściej wszystkie komputery w sieci lokalnej pokazują ten sam adres IP na *www.whatismyip.com*, czyli mają przypisany ten sam adres publiczny.

- Umożliwia to mechanizm zwany NAT (Network Address Translation), który zwykle jest stosowany w routerach.

- Pełni on rolę takiej recepcjonistki, która komunikuje wszystkich pracowników ze firmy światem zewnętrznym.
- Każdy pracownik firmy (**host w sieci lokalnej**) ma na biurku telefon stacjonarny z numerem wewnętrznym (**prywatne IP**).
- Jeśli dzwoni ktoś spoza firmy (**z Internetu**), to recepcjonistka (**NAT**) odbiera telefon z numeru firmy dostępnego publicznie (**publiczne IP**) i przekazuje połączenie pracownikowi.

Sprawdzanie adresu IP przez zewnętrzne strony internetowe

- Czy jest możliwa sytuacja, w której adres IP w systemie oraz na stronie typu www.whatismyip.com będzie identyczny?

- Tak, jest możliwa, ale w szczególnych przypadkach: kiedy komputer jest bezpośrednio podłączony do Internetu bez routera z NATem.

- Możemy w swoim urządzeniu przypisać bezpośrednio adres IP publiczny i pomijać adresy prywatne (NAT). Jest to jednak możliwe tylko wtedy, gdy dostawca Internetu udostępni nam publiczny adres IP.

- Jest to przydatne np. wtedy, gdy chcemy postawić stronę internetową bezpośrednio na naszym komputerze (zrobić z niego serwer), bez korzystania z zewnętrznych serwerów, VPNów, czy tunelowania (które mają wiele ograniczeń i powodują opóźnienia).

Publiczny adres IP – bezpieczeństwo

- Używając publicznego adresu IP (z pominięciem NATu i adresów prywatnych) należy mieć koniecznie włączoną zaporę sieciową (ang. firewall) i aktualne oprogramowanie (przede wszystkim system operacyjny)!

- W przeciwnym wypadku zostaniemy ofiarą ataku hakerskiego dosłownie w kilka minut.