Zadanie: Konfiguracja podstawowa i testowanie sieci

Autor (Michał, Gebel, 229879):
Data: 24.10.2020r.
Przedmiot: Podstawy sieci komputerowych

Zadanie: Konfiguracja podstawowa i testowanie sieci

Cele:

- **Konfiguracja sieciowa stacji roboczej z systemem operacyjnym Windows**
- **Konfiguracja sieciowa stacji roboczej z systemem operacyjnym Linux**
- **Testowanie łączności pomiędzy hostami w sieci IP**
- **Kontrola ustawień zapory sieciowej (*firewall*) na stacji roboczej z systemem Windows**
- **Wyznaczanie tras pakietów w sieci IP**

Opis środowiska laboratoryjnego

Aby możliwa była pełna kontrola konfiguracji sieciowej stacji roboczych, zadanie wykonywane jest przy wykorzystaniu maszyn wirtualnych, na których zainstalowany jest odpowiedni system operacyjny – Windows 10 lub Linux (dystrybucja Fedora). W obu przypadkach użytkownik ma możliwość działania z poziomu konta administratora (w systemie Linux określanego jako root). Maszyny wirtualne działają w środowisku wirtualizacji tworzonym przez program VirtualBox, zainstalowany w systemie operacyjnym maszyny fizycznej (czyli po prostu komputera) – a więc w tzw. systemie gospodarza. W tym przypadku system operacyjny zainstalowany w maszynie wirtualnej (Windows lub Linux) jest więc systemem gościa.

Przynajmniej jeden z interfejsów sieciowych maszyny wirtualnej działa w tzw. trybie zmostkowanym (*bridged*) z fizyczną kartą sieciową systemu gospodarza. Oznacza to, że interfejs ten zachowuje się tak, jakby był bezpośrednio podłączony do sieci lokalnej – z punktu widzenia komunikacji sieciowej taką maszynę wirtualną można traktować identycznie jak maszyny fizyczne (komputery) podłączone do tej sieci.

Obie maszyny wirtualne mogą być zlokalizowane na tej samej maszynie fizycznej (komputerze) lub też na różnych, podłączonych do tej samej sieci lokalnej.

Część 1: Konfiguracja sieciowa stacji roboczej z systemem operacyjnym Windows

Część 1 zadania polega na weryfikacji konfiguracji sieciowej stacji roboczej z systemem operacyjnym Windows 10 oraz zweryfikowaniu działania dynamicznego przydziału tej konfiguracji za pomocą protokołu DHCP.

Etap 1: Weryfikacja podstawowej konfiguracji sieciowej stacji roboczej z systemem Windows

Uruchom interfejs wiersza poleceń (polecenie **cmd**) systemu Windows. Wydaj polecenie **ipconfig** i dla interfejsu odpowiadającego interfejsowi maszyny wirtualnej zmostkowanemu z kartą fizyczną komputera odczytaj następujące parametry:

- adres IPv4
- maskę podsieci (*subnet mask*)

- adres bramy domyślnej (*default gateway*)

```
C:\Users\Michal>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cd3c:84bc:9b55:523c%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Połączenie lokalne* 1:

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

Wireless LAN adapter Połączenie lokalne* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9465:a3b3:10be:bd%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

Odpowiedz na następujące pytania:

- Co to jest adres IP i jaka jest jego rola w sieci IP? Co by było, gdyby w danej sieci były dwa interfejsy sieciowe o tym samym numerze IP?

  Adres IP to liczba 32 bitowa określająca adres logiczny interfejsu sieciowego. Jego zadaniem jest określenie adresu umożliwiającego połączenie z siecią i komunikację z nią. Sytuacja w której dwa interfejsy sieciowe mają ten sam adres IP doprowadzi do niedopuszczalnego konfliktu, który uniemożliwia poprawne przesyłanie pakietów sieciowych.

- Co to jest maska podsieci (zwana również maską sieciową)? Na podstawie adresu IP oraz maski sieciowej komputer lub router wyznacza adres sieci, do której należy dany adres – w jaki sposób wykonywane jest to obliczenie?

  Maska podsieci wyodrębnia w adresie IP część adresu podsieci oraz adresu hosta tej podsieci. Żeby znaleźć adres sieci zamienia się na postać binarną oraz wykonuje się koniunkcję logiczną (AND) adresu IP i maski podsieci.

  IP : 192.168.0.2 == 11000000.10101000.00000000.00000010

  Maska podsieci : 255.255.255.0 == 11111111.11111111.11111111.00000000

Adres sieci = 11000000.10101000.0000000000.00000000 ==192.168.0.0

- Co to jest brama domyślna (*default gateway*) i do czego służy? Czy w przypadku braku skonfigurowanej bramy domyślnej możliwa jest komunikacja w sieci? Rozpatrz dwa przypadki: komunikację pomiędzy hostami w tej samej sieci (np. pomiędzy dwoma komputerami w tej samej sieci lokalnej) i komunikację pomiędzy hostami w różnych sieciach (np. pomiędzy komputerem w sieci lokalnej a jakimś serwerem w Internecie).

  Brama domyślna to router, do którego wysyłane są pakiety przez urządzenia w sieci LAN, dzięki której mogą być wysyłane poza sieć lokalną.

  Komunikacja między dwoma hostami w tej samej sieci jest możliwa bez skonfigurowanej bramy, natomiast komunikacja między hostami w różnych sieciach nie.

Etap 2: Wyświetlenie szczegółowych informacji dotyczących interfejsu sieciowego

Wyświetl szczegółowe informacje dotyczące konfiguracji sieciowej za pomocą polecenia **ipconfig /all**. Zwróć uwagę na parametr **DHCP Enabled**: wartość **Yes** oznacza, że na interfejsie uruchamiany jest klient protokołu **DHCP** (*Dynamic Host Configuration Protocol*), który wysyła do sieci żądanie przydziału parametrów konfiguracyjnych. Jeśli w sieci działa **serwer DHCP**, przydziela klientowi odpowiednie parametry „dynamicznie”. To dlatego połączenie sieciowe (przeważnie) działa bez konieczności ingerencji ze strony użytkownika, umożliwiając łatwe korzystanie z sieci także użytkownikom nie posiadającym wiedzy technicznej.

Zwróć uwagę, że polecenie **ipconfig /all** wyświetla również adres serwera DHCP. Ponadto wyświetlane są inne ważne parametry, np. adresy IP serwerów DNS, z których aktualnie korzysta stacja robocza. To dzięki nim w komunikacji sieciowej można posługiwać się tzw. nazwami domenowymi (np. www.p.lodz.pl), które dla ludzi są znacznie wygodniejsze i łatwiejsze do zapamiętania niż adresy IP.

```
C:\Users\Michal>ipconfig/all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : DESKTOP-EKJ3QR1
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Ethernet:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 98-FA-9B-6B-6B-4D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
Ethernet adapter VirtualBox Host-Only Network:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-04
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cd3c:84bc:9b55:523c%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 688521255
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-44-FD-6B-98-FA-9B-6B-
6B-4D
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
```

```
   NetBIOS over Tcpip. . . . . . . . : Enabled
Wireless LAN adapter Połączenie lokalne* 1:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 2A-39-26-74-3A-1D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Połączenie lokalne* 2:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
#2
   Physical Address. . . . . . . . . : AA-39-26-55-2A-15
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8821CE Wireless LAN 802.11ac
PCI-E NIC
   Physical Address. . . . . . . . . : 28-39-26-66-18-7D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9465:a3b3:10be:bd%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : piątek, 23 października 2020 08:49:33
   Lease Expires . . . . . . . . . . : niedziela, 25 października 2020
14:14:06
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 120076582
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-44-FD-6B-98-FA-9B-6B-
6B-4D
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Odpowiedz na następujące pytania:

- Jakie parametry konfiguracyjne przydziela protokół DHCP?

  Kod operacji, długość adresu sprzętowego, identyfikator transakcji, czas dzierżawy, flagi, adres IP klienta, przydzielony adres IP klienta, maskę sieciową, adres IP serwera DHCP, adres IP bramy domyślnej, serwer DNS, adres MAC klienta, nazwę serwera i znacznie więcej.

- Które z parametrów przydzielanych przez DHCP są niezbędne, by komunikacja sieciowa działała, a które są opcjonalne?

  Niezbędne: kod operacji, długość adresu sprzętowego, identyfikator transakcji, czas dzierżawy, flagi, przydzielony adres IP klienta, adres IP serwera DHCP, adres IP bramy domyślnej, adres MAC klienta

  Zbędne: nazwa serwera, adres IP klienta

- Dlaczego w przypadku stacji roboczych najczęściej protokół DHCP jest uruchamiany domyślnie?

  Protokół DHCP ustawia parametry automatycznie, dlatego unika się błędów przy protokołach konfigurowanych manualnie.

Etap 3: Zwalnianie i odnawianie przydziału parametrów konfiguracyjnych przydzielanych przez protokół DHCP

Zwolnij przydział parametrów konfiguracyjnych na interfejsie za pomocą polecenia **ipconfig /release** i sprawdź efekt wydając polecenie **ipconfig** oraz próbując zestawić jakieś połączenie sieciowe, np. otwierając okno przeglądarki WWW. Odnów przydział parametrów konfiguracyjnych za pomocą polecenia **ipconfig /renew** i ponownie sprawdź, czy konfiguracja została przydzielona i czy działa poprawnie.

```
C:\Users\Michal>ipconfig/release
Windows IP Configuration

No operation can be performed on Ethernet while it has its media
disconnected.
No operation can be performed on Połączenie lokalne* 1 while it has its media
disconnected.
No operation can be performed on Połączenie lokalne* 2 while it has its media
disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cd3c:84bc:9b55:523c%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Połączenie lokalne* 1:

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

Wireless LAN adapter Połączenie lokalne* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9465:a3b3:10be:bd%11
   Default Gateway . . . . . . . . . :

C:\Users\Michal>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cd3c:84bc:9b55:523c%4
```

```
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Połączenie lokalne* 1:

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

Wireless LAN adapter Połączenie lokalne* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9465:a3b3:10be:bd%11
   Autoconfiguration IPv4 Address. . : 169.254.0.189
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

C:\Users\Michal>ipconfig/renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media
disconnected.
No operation can be performed on Połączenie lokalne* 1 while it has its media
disconnected.
No operation can be performed on Połączenie lokalne* 2 while it has its media
disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cd3c:84bc:9b55:523c%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Połączenie lokalne* 1:

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

Wireless LAN adapter Połączenie lokalne* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9465:a3b3:10be:bd%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

```
   Default Gateway . . . . . . . . . : 192.168.0.1
```

Etap 4: Konfiguracja sieciowa maszyny fizycznej

W analogiczny sposób zweryfikuj konfigurację sieciową oraz działanie protokołu DHCP w odniesieniu do maszyny fizycznej (komputera), na której zainstalowana jest maszyna wirtualna z systemem Windows 10.

Kierownik przedmiotu dr. inż. Roman Krasiukianis pozwolił wykonać konfigurację tylko na maszynie fizycznej z systemem operacyjnym Windows 10.

Część 2: Konfiguracja sieciowa stacji roboczej z systemem operacyjnym Linux

Część 2 zadania polega na weryfikacji konfiguracji sieciowej stacji roboczej zainstalowanej jako maszyna wirtualna z systemem operacyjnym Linux.

Etap 1: Weryfikacja podstawowej konfiguracji sieciowej stacji roboczej z systemem Linux

Otwórz okno terminala tekstowego **LXTerminal**. Wydaj polecenie **ip address show** i dla interfejsu odpowiadającego interfejsowi maszyny wirtualnej zmostkowanemu z kartą fizyczną komputera odczytaj następujące parametry:

- adres IPv4
- prefiks (ilość bitów odpowiadającą części sieciowej w masce podsieci)
- adres rozgłoszeniowy (*broadcast*)

```
[root@229879 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:2d:d3:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.4/24 brd 192.168.0.255 scope global dynamic enp0s3
       valid_lft 86331sec preferred_lft 86331sec
    inet6 fe80::4c:1c2b:a87d:4928/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:96:66:3a brd ff:ff:ff:ff:ff:ff
    inet6 fe80::e963:b896:6157:3b50/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:5e:2f:3e brd ff:ff:ff:ff:ff:ff
    inet6 fe80::4d40:40c8:6e3:8b9a/64 scope link
       valid_lft forever preferred_lft forever
```

Etap 2: Wyświetlenie tablicy routingu stacji roboczej z systemem Linux

Za pomocą polecenia **ip route show** wyświetl tablicę routingu i odczytaj następujące parametry:

- adres bramy domyślnej
- adres IPv4 oraz prefiks sieci, do której podłączony jest interfejs (w tym przypadku – interfejs maszyny wirtualnej)

```
[root@229879 ~]# ip r
default via 192.168.0.1 dev enp0s3 proto static metric 100
192.168.0.0/24 dev enp0s3 proto kernel scope link src 192.168.0.4 metric
100
```

Odpowiedz na następujące pytania:

- Co to jest tablica routingu i do czego służy?

  Tablica routingu zawiera informacje na temat sąsiadujących routerów oraz sieci lokalnych. Dzięki niej wyznaczana jest najszybsza trasa przy przesyłaniu pakietów sieciowych. Wyróżniamy tablice statyczne, czyli aktualizowane przez administratorów sieci, oraz dynamiczne, aktualizowane przez specjalne oprogramowanie.

- Co to jest adres rozgłoszeniowy (*broadcast*)?

  Adres rozgłoszeniowy pozwala na wysłanie informacji do wszystkich urządzeń znajdujących się w danej sieci.

- W jaki sposób dla danego adresu IP i maski sieciowej można obliczyć adres rozgłoszeniowy?

  Wpierw należy zanegować maskę podsieci, a następnie wykonać alternatywę logiczną (OR) dla adresu IP oraz zanegowanej maski.

Część 3: Testowanie łączności pomiędzy hostami w sieci IP

Celem części 3 zadania jest przetestowanie łączności w sieci za pomocą programu **ping**, który generuje komunikaty „żądania echa” *Echo Request* protokołu ICMP (*Internet Control Message Protocol*) i rejestruje wysyłane w odpowiedzi przez host docelowy komunikaty *Echo Reply*. Na tej podstawie program wykonuje podstawową analizę jakości połączenia, wyznaczając procent zagubionych pakietów oraz minimalny, maksymalny i średni czas opóźnienia przejścia pakietów od nadawcy do odbiorcy i z powrotem (RTT, *Round-Trip Time*).

W przypadku braku zarejestrowanych przez ping odpowiedzi jedną z możliwych przyczyn jest działanie w systemie docelowym zapory sieciowej (*firewall*), która może blokować komunikaty ICMP *Echo Request*. W takim przypadku należy dokonać sprawdzenia ustawień zapory w danym systemie i wykonać czynności opisane w części 4.

Etap 1: Testowanie łączności pomiędzy hostami w sieci lokalnej

W przypadku hostów podłączonych do tej samej sieci lokalnej transmisja jest bezpośrednia (bez udziału pośredniczących routerów). Zbadaj za pomocą polecenia **ping** komunikację pomiędzy:

- dwoma hostami zlokalizowanymi w tej samej maszynie fizycznej, np. pomiędzy dwiema maszynami wirtualnymi zainstalowanymi w tym samym komputerze fizycznym lub pomiędzy maszyną wirtualną a maszyną fizyczną, w której jest ona zainstalowana

```
C:\Users\Michal>ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:
Reply from 192.168.0.4: bytes=32 time<1ms TTL=64
Reply from 192.168.0.4: bytes=32 time<1ms TTL=64
Reply from 192.168.0.4: bytes=32 time<1ms TTL=64
Reply from 192.168.0.4: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- dwoma hostami zlokalizowanymi w tej samej sieci lokalnej, ale w różnych maszynach fizycznych

```
 Samsung Galaxy S9
C:\Users\Michal>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time=50ms TTL=64
Reply from 192.168.0.3: bytes=32 time=58ms TTL=64
Reply from 192.168.0.3: bytes=32 time=181ms TTL=64
Reply from 192.168.0.3: bytes=32 time=96ms TTL=64

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 50ms, Maximum = 181ms, Average = 96ms
```

- hostem (wirtualnym lub fizycznym) a bramą domyślną (czyli routerem) łączącą daną sieć lokalną z siecią zewnętrzną (Internetem)

```
C:\Users\Michal>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=4ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms
```

Na podstawie uzyskanych wyników dokonaj krótkiej oceny parametrów transmisji – poziomu niezawodności transmisji oraz czasów opóźnienia RTT.

Ewidentnie pingowania, które odbyły się w sieci lokalnej miały bardzo krótki czas przesyłania pakietów. W przypadku pingowania telefonu dłuższy czas jest prawdopodobnie spowodowany użyciem sieci Wi-Fi, a nie kabla ethernetowego.

Etap 2: Testowanie łączności z hostami zlokalizowanymi poza siecią lokalną

W przypadku komunikowania się z hostami spoza sieci lokalnej transmisja przebiega poprzez systemy pośredniczące (routery), przy czym pierwszym z nich jest router pełniący w danej sieci rolę bramy domyślnej. Za pomocą polecenia **ping** zbadaj komunikację pomiędzy hostem w sieci lokalnej (wirtualnym lub fizycznym) a trzema dowolnie wybranymi serwerami w Internecie.

```
C:\Users\Michal>ping www.gov.pl

Pinging www.gov.pl [194.181.92.100] with 32 bytes of data:
Request timed out.
Request timed out.
```

```
Request timed out.
Request timed out.

Ping statistics for 194.181.92.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Michal>ping www.google.pl

Pinging www.google.pl [172.217.22.3] with 32 bytes of data:
Reply from 172.217.22.3: bytes=32 time=52ms TTL=116
Reply from 172.217.22.3: bytes=32 time=61ms TTL=116
Reply from 172.217.22.3: bytes=32 time=52ms TTL=116
Reply from 172.217.22.3: bytes=32 time=63ms TTL=116

Ping statistics for 172.217.22.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 52ms, Maximum = 63ms, Average = 57ms

C:\Users\Michal>ping www.interia.pl

Pinging www.interia.pl [185.69.194.129] with 32 bytes of data:
Reply from 185.69.194.129: bytes=32 time=34ms TTL=57
Reply from 185.69.194.129: bytes=32 time=40ms TTL=57
Reply from 185.69.194.129: bytes=32 time=35ms TTL=57
Reply from 185.69.194.129: bytes=32 time=35ms TTL=57

Ping statistics for 185.69.194.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 40ms, Average = 36ms
```

Porównaj uzyskane wyniki z wynikami zebranymi w etapie 1 – czy widoczna jest różnica i których parametrów ona dotyczy?

Część 4: Kontrola ustawień zapory sieciowej (*firewall*) na stacji roboczej z systemem Windows

Jednym z typowych elementów instalowanych i domyślnie uruchamianych we współczesnych systemach operacyjnych jest oprogramowanie określane jako zapora sieciowa (*firewall*), chroniące system przed atakami zarówno ze strony hakerów, jak i tzw. złośliwego oprogramowania (*malware*). Działanie zapory sieciowej może w niektórych przypadkach utrudnić testowanie poprawności działania sieci oraz diagnostykę, której celem jest wyszukanie i zlokalizowanie ewentualnych błędów w konfiguracji. Przykładem takiego działania może być domyślne odfiltrowywanie przez zaporę sieciową komunikatów *Echo Request* protokołu ICMP. Najprostszym „usunięciem problemu" jest w tym przypadku wyłącznie zapory sieciowej, jednak takie działanie stwarza zagrożenie dla systemu i powinno być wykonywane jedynie w szczególnych przypadkach (np. w czasie zajęć laboratoryjnych) i tylko tymczasowo, np. na czas niezbędny do zdiagnozowania przyczyny występującego w sieci problemu.

Etap 1: Tymczasowe wyłącznie i ponowne włączenie zapory sieciowej w systemie Windows

Otwórz **Panel sterowania** systemu Windows, a następnie uruchom narzędzie **Zapora systemu Windows** i sprawdź, czy zapora sieciowa jest włączona. Jeśli tak, wyłącz zaporę i sprawdź, czy ma to wpływ na możliwość „pingowania" danego systemu. Jeśli nadal program ping nie rejestruje odpowiedzi *Echo Reply*, przyczyna obserwowanego problemu leży gdzie indziej (najczęściej w niepoprawnej konfiguracji sieciowej) i należy ją zlokalizować, a następnie usunąć. Po zakończeniu eksperymentu natychmiast włącz ponownie zaporę.

Zadanie: Konfiguracja podstawowa i testowanie sieci

```
Po wyłączeniu zapory

[root@229879 ~]# ping -c 5 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=0.255 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=0.218 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=0.288 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=128 time=0.253 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=128 time=0.251 ms

--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4133ms
rtt min/avg/max/mdev = 0.218/0.253/0.288/0.022 ms

Po włączeniu zapory

[root@229879 ~]# ping -c 5 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.

--- 192.168.0.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4136ms
```

Etap 2: Selektywne otwarcie „okna” w zaporze sieciowej

W celu zwiększenia bezpieczeństwa zapora sieciowa domyślnie blokuje ruch przychodzący. Jeśli świadomie chcemy zezwolić na dany rodzaj ruchu sieciowego (np. na przejście komunikatów *Echo Request* w celu umożliwienia diagnostyki za pomocą programu ping), zamiast wyłączania zapory sieciowej należy w jej konfiguracji zdefiniować **selektywną** regułę zezwalającą na ten rodzaj ruchu.

Ponownie uruchom narzędzie **Zapora systemu Windows** i wybierz **Ustawienia zaawansowane**, a następnie **Reguły przychodzące**. W sekcji **Akcje** wybierz **Nowa reguła…**, co spowoduje uruchomienie kreatora. W kolejnych okienkach kreatora należy wybrać:

- **Typ reguły** – niestandardowa.
- **Protokół i porty** – ICMPv4; następnie po wybraniu przycisku **Dostosuj…** należy ograniczyć typy komunikatów ICMP (domyślnie wybierane są wszystkie) do „Żądania echa”.
- **Nazwa** – dowolna, byle sensowna i kojarząca się z danym działaniem (np.: „Zezwól na żądanie echa”).

Po zdefiniowaniu reguły zaznacz ją i wypróbuj jej działanie włączając ją i wyłączając w sekcji **Akcje** oraz obserwując, jaki ma to wpływ na możliwość testowania danego systemu za pomocą programu ping.

W analogiczny sposób można definiować reguły dotyczące innych rodzajów pakietów, także w odniesieniu do ruchu wychodzącego (**Reguły wychodzące**).

Zdefiniowaną regułę można wyłączyć lub usunąć. W tym drugim przypadku, jeśli reguła będzie potrzebna w przyszłości, konieczne będzie ponowne jej stworzenie.

```
Z regułą

[root@229879 ~]# ping -c 5 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=0.391 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=0.321 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=0.235 ms
```

```
64 bytes from 192.168.0.2: icmp_seq=4 ttl=128 time=0.403 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=128 time=0.382 ms

--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4103ms
rtt min/avg/max/mdev = 0.235/0.346/0.403/0.064 ms

Bez reguły

[root@229879 ~]# ping -c 5 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.

--- 192.168.0.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4124ms
```

Część 5: Wyznaczanie tras pakietów w sieci IP

Celem części 5 zadania jest wyznaczenie tras pakietów wysyłanych ze stacji roboczych do różnych hostów zlokalizowanych zarówno w sieci lokalnej, jak i Internecie, za pomocą programu **traceroute** (w systemie Linux) oraz jego implementacji w systemie Windows, zwanej **tracert**.

Program **traceroute** pozwala na wyznaczenie trasy pakietu w sieci IP oraz opóźnień RTT dla każdego węzła pośredniczącego (routera) na trasie. W tym celu traceroute wykorzystuje pole „czasu życia" TTL (*Time To Live*) w nagłówku pakietu IP, odpowiednio modyfikując jego wartość tak, aby kolejne routery na trasie wysyłały do nadawcy komunikaty ICMP *Time Exceeded*. Pozwala to na ustalenie zarówno adresów IP kolejnych routerów, jak i opóźnień RTT. Domyślnie **traceroute** wysyła pakiety trójkami, wyświetlając w kolejnych wierszach adresy IP (lub nazwy domenowe) odpowiadające interfejsom kolejnych routerów i odpowiednie wartości opóźnień RTT. Jeśli odpowiedź na dany pakiet nie nadejdzie w zadanym czasie (który jest wartością konfigurowalną w programie), program wyświetla znak gwiazdki (*). Może to być spowodowane przeciążeniem sieci lub też celowym ustawieniem na danym routerze odpowiedniej reguły filtrującej (takie blokowanie jest typowe dla urządzeń pełniących w sieci rolę specjalizowanych zapór sieciowych).

Etap 1: Wyznaczanie tras do hostów zlokalizowanych w Internecie (poza siecią lokalną)

Za pomocą programu **traceroute** (w systemie Linux) oraz **tracert** (w systemie Windows) wyznacz trasy oraz opóźnienia odpowiadające poszczególnym etapom dla trzech dowolnych serwerów zlokalizowanych poza siecią lokalną. Spróbuj znaleźć taki adres IP, dla którego trasa przebiega przez węzeł nie ujawniający swojej obecności (nie wysyłający komunikatów ICMP).

```
Windows:

C:\Users\Michal>tracert www.google.pl

Tracing route to www.google.pl [172.217.22.3]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  router.totolink.com [192.168.0.1]
  2     7 ms     6 ms    13 ms  funbox.home [192.168.1.1]
  3    31 ms    28 ms    31 ms  lodz-bng4.neo.tpnet.pl [83.1.4.155]
  4    33 ms    30 ms    28 ms  lodz-r3.tpnet.pl [80.50.157.181]
  5    45 ms    42 ms    32 ms  195.116.35.42
  6    59 ms    55 ms    60 ms  ae106-10.ffttr6.frankfurt.opentransit.net
[193.251.249.7]
  7    53 ms    51 ms    64 ms  google-14.gw.opentransit.net
[193.251.252.246]
  8    54 ms    58 ms    67 ms  216.239.54.161
  9    49 ms    61 ms    51 ms  108.170.235.255
 10    66 ms    59 ms    65 ms  fra16s14-in-f3.1e100.net [172.217.22.3]

Trace complete.
```

```
C:\Users\Michal>tracert www.facebook.pl

Tracing route to star-mini.c10r.facebook.com [185.60.216.35]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  router.totolink.com [192.168.0.1]
  2     7 ms     6 ms     7 ms  funbox.home [192.168.1.1]
  3    33 ms    57 ms    34 ms  lodz-bng4.neo.tpnet.pl [83.1.4.155]
  4    79 ms    42 ms    36 ms  lodz-r3.tpnet.pl [80.50.157.181]
  5    31 ms    31 ms    33 ms  195.116.35.42
  6    52 ms    66 ms    60 ms  ae106-10.ffttr6.frankfurt.opentransit.net
[193.251.249.7]
  7    82 ms    93 ms    53 ms  facebook-13.gw.opentransit.net
[193.251.254.76]
  8    50 ms    51 ms    54 ms  po151.asw01.fra2.tfbnw.net [204.15.22.6]
  9    51 ms    52 ms    62 ms  po212.psw01.fra5.tfbnw.net [157.240.43.103]
 10    51 ms    52 ms    61 ms  173.252.67.25
 11    51 ms    54 ms    64 ms  edge-star-mini-shv-01-frx5.facebook.com
[185.60.216.35]

Trace complete.

C:\Users\Michal>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.250.74.206]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  router.totolink.com [192.168.0.1]
  2    16 ms     7 ms    14 ms  funbox.home [192.168.1.1]
  3    30 ms    30 ms    48 ms  lodz-bng4.neo.tpnet.pl [83.1.4.155]
  4    30 ms    29 ms    28 ms  lodz-r3.tpnet.pl [80.50.157.181]
  5    31 ms    32 ms    31 ms  195.116.35.42
  6    59 ms    53 ms    52 ms  ae106-10.ffttr6.frankfurt.opentransit.net
[193.251.249.7]
  7    52 ms    60 ms    65 ms  google-14.gw.opentransit.net
[193.251.252.246]
  8    59 ms    70 ms    64 ms  216.239.56.31
  9    53 ms    60 ms    62 ms  142.250.234.19
 10    66 ms    50 ms    57 ms  fra24s02-in-f14.1e100.net [142.250.74.206]

Trace complete.

Linux:

[root@229879 ~]# traceroute www.google.pl
traceroute to www.google.pl (172.217.16.163), 30 hops max, 60 byte packets
 1  router.totolink.com (192.168.0.1)  2.821 ms  2.802 ms  2.792 ms
 2  funbox.home (192.168.1.1)  14.277 ms  14.299 ms  14.290 ms
 3  lodz-bng4.neo.tpnet.pl (83.1.4.155)  40.983 ms  40.976 ms  40.711 ms
 4  lodz-r5.tpnet.pl (80.50.156.181)  40.660 ms lodz-r3.tpnet.pl
(80.50.157.181)  40.547 ms  40.495 ms
 5  195.116.35.42 (195.116.35.42)  40.501 ms  40.489 ms  40.475 ms
 6  ae106-10.ffttr6.frankfurt.opentransit.net (193.251.249.7)  63.589 ms *
59.044 ms
 7  google-14.gw.opentransit.net (193.251.252.246)  59.028 ms 72.14.214.52
(72.14.214.52)  49.877 ms google-14.gw.opentransit.net (193.251.252.246)
53.103 ms
 8  * * *
 9  108.170.252.65 (108.170.252.65)  54.575 ms 66.249.95.168 (66.249.95.168)
53.121 ms 216.239.47.246 (216.239.47.246)  54.471 ms
```

```
10  216.239.63.255 (216.239.63.255)  53.024 ms 64.233.175.171
(64.233.175.171)  54.428 ms 108.170.252.82 (108.170.252.82)  54.442 ms
11  108.170.226.3 (108.170.226.3)  52.967 ms fra15s11-in-f163.1e100.net
(172.217.16.163)  58.295 ms  58.265 ms
[root@229879 ~]# traceroute www.facebook.com
traceroute to www.facebook.com (185.60.216.35), 30 hops max, 60 byte packets
 1  router.totolink.com (192.168.0.1)  1.961 ms  1.942 ms  1.979 ms
 2  funbox.home (192.168.1.1)  15.143 ms  15.159 ms  15.149 ms
 3  lodz-bng4.neo.tpnet.pl (83.1.4.155)  46.265 ms  46.280 ms  46.276 ms
 4  lodz-r3.tpnet.pl (80.50.157.181)  46.273 ms lodz-r5.tpnet.pl
(80.50.156.181)  46.104 ms  46.092 ms
 5  195.116.35.42 (195.116.35.42)  49.754 ms  49.742 ms  49.717 ms
 6  ae106-10.ffttr6.frankfurt.opentransit.net (193.251.249.7)  70.756 ms
66.300 ms  66.294 ms
 7  facebook-13.gw.opentransit.net (193.251.254.76)  118.698 ms  110.232 ms
101.364 ms
 8  po131.asw01.fra5.tfbnw.net (157.240.47.212)  50.012 ms
po151.asw01.fra2.tfbnw.net (204.15.22.6)  55.517 ms  55.431 ms
 9  po223.psw01.fra5.tfbnw.net (157.240.41.5)  56.325 ms
po222.psw04.fra5.tfbnw.net (157.240.43.97)  55.474 ms
po241.psw01.fra5.tfbnw.net (157.240.43.53)  56.290 ms
10  173.252.67.191 (173.252.67.191)  56.295 ms 173.252.67.33 (173.252.67.33)
52.937 ms 173.252.67.35 (173.252.67.35)  52.896 ms
11  edge-star-mini-shv-01-frx5.facebook.com (185.60.216.35)  52.880 ms
50.101 ms  50.089 ms

[root@229879 ~]# traceroute www.youtube.com
traceroute to www.youtube.com (172.217.18.174), 30 hops max, 60 byte packets
 1  router.totolink.com (192.168.0.1)  1.881 ms  1.854 ms  1.842 ms
 2  funbox.home (192.168.1.1)  15.757 ms  15.772 ms  15.758 ms
 3  lodz-bng4.neo.tpnet.pl (83.1.4.155)  57.119 ms  57.109 ms  57.103 ms
 4  lodz-r3.tpnet.pl (80.50.157.181)  57.058 ms  56.946 ms lodz-r5.tpnet.pl
(80.50.156.181)  56.926 ms
 5  195.116.35.42 (195.116.35.42)  56.928 ms  56.863 ms  56.776 ms
 6  ae106-10.ffttr6.frankfurt.opentransit.net (193.251.249.7)  66.888 ms
62.068 ms  62.052 ms
 7  72.14.214.52 (72.14.214.52)  61.695 ms  50.202 ms  52.901 ms
 8  * * *
 9  108.170.252.65 (108.170.252.65)  52.933 ms 108.170.235.252
(108.170.235.252)  52.921 ms 108.170.252.65 (108.170.252.65)  52.917 ms
10  108.170.251.209 (108.170.251.209)  52.894 ms 108.170.252.83
(108.170.252.83)  52.843 ms 74.125.37.167 (74.125.37.167)  57.314 ms
11  fra15s29-in-f14.1e100.net (172.217.18.174)  52.865 ms  61.365 ms  61.343
ms
```

Etap 2: Wyznaczanie tras do hostów w tej samej sieci lokalnej

Zbadaj za pomocą programu **traceroute** / **tracert** komunikację pomiędzy dwoma hostami (fizycznymi lub wirtualnymi) zlokalizowanymi w tej samej sieci lokalnej w celu uzyskania potwierdzenia, że w takim przypadku komunikacja przebiega bezpośrednio, a więc bez udziału pośredniczących routerów.

```
C:\Users\Michal>tracert 192.168.0.4

Tracing route to 192.168.0.4 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.0.4

Trace complete.


[root@229879 ~]# traceroute 192.168.0.2
traceroute to 192.168.0.2 (192.168.0.2), 30 hops max, 60 byte packets
```

```
1  192.168.0.2 (192.168.0.2)  0.378 ms * *
```