Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 4: Warstwa sieciowa. Routing, rola bramy domyślnej i protokołu ICMP

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

03.2022

I. Wprowadzenie

Warstwa 3. modelu OSI — sieciowa — ma za zadanie przekazać ruch sieciowy pomiędzy różnymi sieciami. Decyduje o tym, którym łączem należy wypuścić pakiet, aby dotarł do odbiorcy, jednocześnie dbając o obciążenie łączy (*load balancing*).

Proces wyznaczania trasy dla pakietu nazywany jest **routingiem**, a urządzenie go wykonujące to **router**. Routery podejmują decyzje co do routowania na podstawie budowanej przez siebie **tablicy routingu**. Znajdują się w niej informacje o tym, jakie sieci zna dany router i którym interfejsem należy wypuścić pakiet kierowany do danej sieci. Podczas wysyłania pakietu, router sprawdza (na podstawie docelowego adresu IP w nagłówku pakietu), do której sieci kierowany jest pakiet, a następnie szuka w swojej tablicy routingu interfejsu wyjściowego do danego pakietu. Jeśli router nie znajduje odpowiedniego wpisu w tablicy routingu, wysyła dany pakiet za pomocą tzw. **trasy ostatniej szansy** — najczęściej do innego routera, który być może będzie posiadał właściwy wpis u siebie i właściwie pokieruje pakiet.

Każdy komputer też tworzy własną tablicę routingu. Jeśli wysyłany przez niego pakiet kierowany jest do komputera z tej samej podsieci, trafia poprzez switch bezpośrednio do urządzenia docelowego. Dopiero kiedy wysyłany pakiet kierowany jest do urządzenia spoza sieci, trafia on do routera, który decyduje potem o trasowaniu. Router, który odbiera pakiety z sieci lokalnej i przekazuje je do innych sieci, jest dla komputerów z sieci lokalnej **bramą domyślną** — jest to najczęściej pierwszy router na trasie z sieci

lokalnej. Jeśli komputer nie będzie w stanie skomunikować się z bramą domyślną (albo poprzez błędną konfigurację IP, brak skonfigurowania adresu bramy domyślnej lub trasy do niej), będzie mógł się komunikować jedynie z urządzeniami w ramach swojej sieci lokalnej, a nie poza nią.

Najbardziej popularnym protokołem, który działa na warstwie sieciowej, jest **protokół IP** (ang. *Internet Protocol*). Identyfikuje on urządzenia z różnych sieci za pomocą **adresów IP**. Nagłówek protokołu IP zawiera m.in. takie informacje jak:

- adres IP źródłowy i docelowy,
- wersja protokołu IP — IPv4 lub IPv6,
- flagi — informują o tym, czy dany pakiet może być/jest podzielony i wysłany w ramach kilku ramek ethernetowych (ramka ethernetowa może zawierać ładunek o wielkości maksymalnie 1500 bajtów, jeśli pakiet wyższej warstwy jest większy, musi zostać podzielony, o ile nie jest ustawiona flaga *Don't fragment*),
- TTL (ang. *Time to Live*) — czas życia, jaki pozostał pakietowi przed usunięciem go z sieci, innymi słowy maksymalna ilość przeskoków (routerów na trasie), które może jeszcze dokonać dany pakiet,
- informacja o zawartości pakietu (PDU jakiego protokołu enkapsulowany jest w ramach pakietu).

Protokołem, który wspomaga protokół IP w działaniu, jest **protokół ICMP** (ang. *Internet Control Message Protocol*). Służy on do przesyłania informacji kontrolnych o komunikacji w sieci — czy dane urządzenie zdalne jest dostępne, a jeśli nie, to dlaczego. Komendy systemu Windows (znany Ci już ping czy też tracert służący do śledzenia pakietów) wykorzystują pod spodem właśnie protokół ICMP. Informacje o rodzaju komunikatu ICMP przesyłane są w nagłówku ICMP w polu Type, przykładowo:

- 0 — pakiet jest odpowiedzią na żądanie echo,
- 3 — pakiet nie dotarł do odbiorcy, tzw. *Destination Unreachable*,
- 8 — pakiet jest żądaniem echo.

Dla komunikatów typu 3 można poznać przyczynę niepowodzenia komunikacji poprzez wartość z pola Code, przykładowo:

- 0 — sieć nieosiągalna,
- 1 — host nieosiągalny,
- 4 — zbyt duży pakiet, aby przesłać go bez fragmentacji.

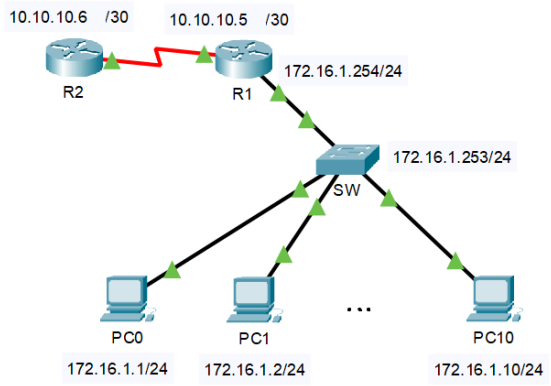
II. Cel ćwiczenia

Celem niniejszego ćwiczenia jest zapoznanie się z funkcjonowaniem warstwy sieciowej modelu OSI w sieciach komputerowych poprzez:

- obserwację procesu routingu na routerze na podstawie znanych tras,
- zaznajomienie się z rolą bramy domyślnej i konsekwencjami jej braku/nieprawidłowego działania,
- przechwycenie i analizę ruchu sieciowego ICMP wygenerowanego podczas wykonywania poleceń systemowych ping/tracert.

III. Stanowisko laboratoryjne

Do wykonania ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputerów klasy PC z zainstalowanym systemem Windows oraz oprogramowaniem Wireshark, połączonych w sieć za pomocą przełącznika sieciowego Cisco, który następnie dołączony jest do dwóch routerów.



Przed przystąpieniem do ćwiczenia:

- Włącz komputer do lokalnej sieci laboratoryjnej, uruchamiając na nim kartę sieciową o nazwie *LAB*. Kliknij *Start* ⇒ *Ustawienia* ⇒ *Połączenia sieciowe*. Prawym klawiszem wybierz kartę sieciową *LAB* i kliknij *Włącz*, podobnie wybierz kartę sieciową *Internet* i wybierz *Wyłącz* (od tego momentu komputer straci połączenie z internetem na rzecz sieci laboratoryjnej).
- Ustaw statycznie adres IP według schematu:
  IP: 172.16.1.*numer_Twojego_stanowiska*
  Maska podsieci: 255.255.255.0
  Brama domyślna: 172.16.1.254

IV. Przebieg ćwiczenia

1 Obserwacja procesu routingu i roli bramy domyślnej

1.1 Przyjrzyj się tablicy routingu na Twoim komputerze.

a) Otwórz Wiersz polecenia systemu Windows (*Start* $\Rightarrow$ *Uruchom* $\Rightarrow$ *cmd*) i zobacz, jakie możliwości daje komenda *route*:

```
route /?
```

Możesz:

- wyświetlić tablicę routingu na swoim komputerze (*route print*),
- dodać nowy wpis do tablicy routingu (*route add*),
- modyfikować istniejący wpis (*route change*),
- usuwać wpisy z tablicy (*route delete*).

b) Wyświetl tablicę routingu poleceniem *route print*.

```
route print
```

```
c:\>route print
===========================================================================
Lista interfejsów
0x1 ........................... MS TCP Loopback interface
0x10004 ...00 1a 92 32 3f a9 ...... Realtek RTL8168/8111 PCI-E Gigabit Ethernet
NIC - Sterownik miniport Harmonogramu pakiet˜w
===========================================================================
===========================================================================
Aktywne trasy:
Miejsce docelowe w sieci      Maska sieci      Brama       Interfejs       Metryka
          0.0.0.0          0.0.0.0     172.16.1.254      172.16.1.1       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
      172.16.1.0    255.255.255.0      172.16.1.1      172.16.1.1       20
      172.16.1.1  255.255.255.255        127.0.0.1       127.0.0.1       20
  172.16.255.255  255.255.255.255      172.16.1.1      172.16.1.1       20
        224.0.0.0        240.0.0.0      172.16.1.1      172.16.1.1       20
  255.255.255.255  255.255.255.255      172.16.1.1      172.16.1.1       1
Domyślna brama:     172.16.1.254.
===========================================================================
Trasy trwałe:
  Brak
```

Zwróć uwagę, jakie informacje są w niej zawarte. Widać adresy sieci, które komputer zna (*Network Destination*) wraz z odpowiadają im maską podsieci (*Netmask*), bramą (*Gateway*) i interfejsem prowadzącym do tej sieci (*Interface*).

Ważne: Sieć 0.0.0.0 oznacza **każdą** sieć, tzn. wszystkie te, które nie są umieszczone w tablicy. Komputer wyśle pakiet przez skojarzony z nią interfejs wtedy, kiedy nie znajdzie w tablicy routingu bardziej pasującego wpisu. Jest to zatem **trasa ostatniej szansy**.

c) Wyobraź sobie, że chcesz skomunikować się z urządzeniem o adresie IP 10.10.10.6 (jest to adres IP interfejsu szeregowego na routerze, który nie jest w ramach tej samej podsieci, co Twój komputer). Czy znajdujesz w

tablicy routingu wpis prowadzący do tej sieci? Wykonaj polecenie ping na ten adres IP — ping przechodzi pomyślnie, a zatem komunikacja jest możliwa. Jak myślisz, którędy powędrował Twój pakiet? Oczywiście z pomocą trasy ostatniej szansy został przekazany na adres IP 172.16.1.254, czyli do Twojej **bramy domyślnej**.

1.2 Zaobserwuj zachowanie sieci przy niedostępności bramy domyślnej.

a) Sprawdź zachowanie sieci, kiedy wszystko działa poprawnie: wyślij ping do sąsiada (w ramach sieci lokalnej) oraz pod adres IP interfejsu szeregowego na drugim (zdalnym) routerze:

```
ping 10.10.10.6
```

Oba pingi powinny zakończyć się sukcesem.

b) Poleceniem *route delete* usuń trasę ostatniej szansy (prowadzącą do bramy domyślnej) na swoim komputerze:

```
route delete 0.0.0.0
```

Możesz ponownie wyświetlić tablicę routingu (poleceniem *route print*), aby przekonać się, że wpis został rzeczywiście usunięty.

c) Powtórz wysłanie ping requesta do sąsiada i na interfejs routera z innej podsieci. Który z pingów zakończył się niepowodzeniem? Jak myślisz, dlaczego?

d) Poleceniem *route add* przywróć trasę ostatniej szansy do bramy domyślnej:

```
route add 0.0.0.0 mask 0.0.0.0 172.16.1.254
```

Powtórz wysłanie pingów pod oba adresy — wszystko powinno znów działać.

1.3 Prześledź drogę pakietu do zdalnej sieci.

Jak już wiesz, aby komunikacja z hostem 10.10.10.6 spoza Twojej sieci lokalnej była możliwa, konieczne jest wykorzystanie bramy domyślnej. Bez niej komunikacja odbywa się tylko na poziomie lokalnym. Twoją bramą domyślną jest router R1, posiadający adres IP 172.16.1.254 skonfigurowany na jednym z interfejsów Fast Ethernet.

Przyjrzyj się schematowi topologii zamieszczonej na stronie 3. Aby dotrzeć do hosta 10.10.10.6, pakiet musi pokonać drogę od Twojego komputera, przez bramę domyślną (router R1) do routera R2. Na każdym kroku jest on odpowiednio kierowany. Prześledźmy zatem, w jaki sposób przebiega tu proces routingu, zaglądając do tablicy routingu każdego z routerów.

a) Zaloguj się na router R1, wydając w Wierszu polecenia komendę *telnet*:

```
telnet 172.16.1.254
```

Podczas logowania zostaniesz poproszony o podanie hasła — wpis *cisco*.

Poleceniem enable przejdź do trybu uprzywilejowanego na routerze, aby zobaczyć jego tablicę routingu (znów podaj hasło *cisco*):

```
R1>enable
```

b) Wyświetl tablicę routingu routera R1, wydając mu polecenie *show ip route*:

```
R1#show ip route
```

```
6.1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.6   to network 0.0.0.0

     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4   is directly connected, Serial0/1/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 10.10.10.6
```

Zwróć uwagę, że R1 zna trasę i do naszej sieci lokalnej (172.16.1.0) i do sieci łączącej go z routerem R2 (10.10.10.4). Obie te sieci router zna, gdyż są do niego bezpośrednio dołączone (symbol C oznacza *directly connected*).

Oprócz tego router R1 ma skonfigurowaną trasę ostatniej szansy — zwróć uwagę, że prowadzi ona do routera R2.

c) Pakiet do 10.10.10.6 został zgodnie z tablicą routingu wypuszczony przez router R1 przez port szeregowy. Co się dzieje z nim dalej? Zaloguj się na router R2 i przejdź do trybu uprzywilejowanego, aby zobaczyć jego tablicę routingu.

```
telnet 10.10.10.6
```

```
Password: [cisco]
```

```
R2>enable
```

Ponownie wszędzie tam, gdzie jesteś pytany o hasło, wpisz *cisco*.

d) Wpisz polecenie *show ip route*, aby wyświetlić tablicę routingu routera R2.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.5   to network 0.0.0.0

     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4   is directly connected, Serial0/1/1
S*   0.0.0.0/0 [1/0] via 10.10.10.5
```

`R2#show ip route`

Zobacz, że poszukiwana przez nas trasa do sieci zawierającej hosta 10.10.10.6 jest dołączona bezpośrednio do portu szeregowego routera R2 — istnieje odpowiedni wpis w tablicy routingu. Pakiet moze więc być skierowany przez router bezpośrednio do odbiorcy.

2 Obserwacja działania protokołów warstwy sieciowej w programie Wireshark

W tej części ćwiczenia zobaczysz, jakie informacje dodawane są przez warstwę sieciową w nagłówku protokołu IP, a także jak działa protokół ICMP wspomagający działanie sieci.

2.1 Przyjrzyj się nagłówkowi pakietu IP.

a) Uruchom program Wireshark (*Start* $\Rightarrow$ *Programy* $\Rightarrow$ *Wireshark*) i włącz przechwytywanie danych na karcie sieciowej Realtek (*Capture* $\Rightarrow$ *Start*).

b) Wygeneruj ruch sieciowy, wysyłając ping na adres IP komputera sąsiada (*Start* $\Rightarrow$ *Uruchom* $\Rightarrow$ *cmd* $\Rightarrow$ *ping* [IP]). Pamiętaj, że adres IP możesz sprawdzić w Wierszu polecenia, korzystając z polecenia *ipconfig*.

c) Przejdź do programu Wireshark, zatrzymaj przechwytywanie ruchu sieciowego i włącz filtrowanie tak, by widoczne były tylko pakiety protokołu ICMP.

d) Zaznacz pierwszą przechwyconą ramkę (zawierającą wysłany od Ciebie *Echo (ping) request*) i rozwiń w środkowej części okna trzecią sekcję — odpowiadającą nagłówkowi protokołu IP.

- Wersja protokołu IP powinna wskazywać na IPv4.
- Żadna z Flag nie powinna być ustawiona (każda powinna przyjąć wartość 0), co oznacza, że przechwycona ramka nie zawiera fragmentu większego pakietu ani że fragmentacja nie została zabroniona.

- Czas życia pakietu (TTL) powinien przyjmować startową wartość 128 przypisywaną domyślnie pakietom tworzonym przez system Windows (jako że ten pakiet nie przeszedł przez żaden router, wartość ta nie została odpowiednio pomniejszona).
- Pole Protocol powinno wskazywać, że w pakiecie umieszczone są dane z protokołu ICMP (wartość 1).
- Porównaj źródłowy adres IP z adresem IP swojego komputera.
- Porównaj docelowy adres IP z adresem IP komputera sąsiada.

e) Zaznacz drugą przechwyconą ramkę (*Echo (ping) reply*, będącą odpowiedzią na Twojego requesta) i zaobserwuj, jak zmienił się źródłowy i docelowy adres IP.

2.2 Przyjrzyj się budowie pakietu ICMP.

a) Kliknij ponownie w pierwszą przechwyconą ramkę (echo request) i rozwiń czwartą sekcję, dotyczącą danych protokołu ICMP.

- Przyjrzyj się zawartości pola Type. Powinna ona wskazywać na to, że odebrany pakiet jest prośbą o potwierdzenie poprawności komunikacji (wartość 8, oznaczająca *echo request*).
- Rozwiń pole Data. Zobacz w dolnej części ekranu, że 32 bajty zawartości pakietu ICMP to tak naprawdę kolejne litery alfabetu.

b) Wybierz drugą przechwyconą ramkę. Zobacz, że tym razem pole Type zawiera wartość 0, sugerującą, że jest to odpowiedź na wcześniej otrzymanego *echo requesta*.

2.3 Poznaj inne opcje komendy ping.

a) W wierszu polecenia wyświetl wszystkie opcje, jakimi można zmodyfikować polecenie *ping*.

```
ping /?
```

- Dodając modyfikator -n, można zmienić ilość jednorazowo wysyłanych echo requestów.
- Dodając modyfikator -l, można zmienić wielkość pakietu ICMP (ilość bajtów wypełnianych literami alfabetu).
- Dodając modyfikator -t, można zmusić komputer do ciągłego wysyłania żądań echo, aż do zatrzymania przez użytkownika poprzez Ctrl+C.
- Dodając modyfikator -f, można zabronić komputerowi dzielić pakiet na części wysyłane osobnymi ramkami.

b) Wyślij do sąsiada ping składający się z 8, a nie domyślnych 4 requestów:

`ping IP_sąsiada -n 8`

Zobacz, jak w Wierszu polecenia pojawia się w wyniku 8 odpowiedzi.

c) Wyślij do sąsiada ping o zawartości 64, a nie domyślnych 32 bajtów:

`ping IP_sąsiada -l 64`

d) Wysyłaj do sąsiada ping nieprzerwanie:

`ping IP_sąsiada -t`

Zatrzymaj wysyłanie, wciskając Ctrl+C.

e) Zobacz, jak część modyfikacji można łączyć: wyślij do sąsiada ping o zawartości 64 bajtów i 8 jednoczesnych żądaniach:

`ping IP_sąsiada -l 64 -n 8`

```
C:\Users\marta>ping 192.168.1.1 -n 8 -l 64

Pinging 192.168.1.1 with 64 bytes of data:
Reply from 192.168.1.1: bytes=64 time=3ms TTL=64
Reply from 192.168.1.1: bytes=64 time=3ms TTL=64
Reply from 192.168.1.1: bytes=64 time=5ms TTL=64
Reply from 192.168.1.1: bytes=64 time=3ms TTL=64
Reply from 192.168.1.1: bytes=64 time=3ms TTL=64
Reply from 192.168.1.1: bytes=64 time=5ms TTL=64
Reply from 192.168.1.1: bytes=64 time=5ms TTL=64
Reply from 192.168.1.1: bytes=64 time=7ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms
```

f) Część modyfikacji nie można łączyć: spróbuj wysłać ping jednocześnie ciągły i zawierający 8 żądań:

`ping IP_sąsiada -t -n 8`

Jako że oba modyfikatory zmieniały ilość wysyłanych żądań, nowsza wartość (a zatem 8 żądań) nadpisała starszą (nieograniczona ilość), dlatego możesz zaobserwować, że wysłano ostatecznie 8 żądań i odebrano 8 odpowiedzi.

g) Podobnie, spróbuj wysłać pakiet ICMP o relatywnie dużej wielkości (ustaw ilość bajtów w echo requeście na 1500 — jest to maksymalna wielkość pakietu warstwy sieciowej, jaka może być zawarta w ramce ethernetowej) i jednocześnie zabroń komputerowi dzielić ten pakiet na kilka ramek.

`ping IP_sąsiada -f -l 1500`

Jako że wielkość pakietu łącznie z jego nagłówkiem przekracza wielkość, która pozwala na wysłanie go w jednej ramce, komputer jest zmuszony go podzielić, lecz ustawienie flagi Don't fragment nie pozwala na to, w związku z tym zapytanie w ogóle nie zostanie wysłane.

```
C:\Users\marta>ping 192.168.1.1 -f -l 1500

Pinging 192.168.1.1 with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2.4 Poznaj działanie komendy tracert.

Polecenie *tracert* umożliwia śledzenie drogi, jaką pokonuje pakiet IP od nadawcy do odbiorcy. Pokazuje listę routerów (przeskoków), przez które przeszedł pakiet. Jest szczególnie przydatne w sytuacji, gdy np. w którymś miejscu w sieci są problemy z łączem i chcemy zlokalizować, między którymi urządzeniami występują największe opóźnienia.

a) Włącz przechwytywanie ruchu w programie Wireshark, filtruj ruch ICMP.

b) Wyśledź trasę pomiędzy Twoim komputerem a interfejsem szeregowym na odległym routerze, wykonując w Wierszu polecenia komendę *tracert*:

`tracert 10.10.10.6`

```
C:\>tracert 10.10.10.6

Tracing route to 10.10.10.6   over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.16.1.254
  2    0 ms      0 ms      3 ms      10.10.10.6

Trace complete.
```

Zaobserwuj, jak pakiet najpierw przechodzi przez router R1 (172.16.1.254), a następnie przez router R2 (10.10.10.6).

c) Przejdź do Wiresharka i zaobserwuj ruch przechwycony podczas realizacji komendy tracert.

Jak działa tracert? W trakcie wykonywania komendy *tracert*, wysyłane są tak naprawdę pakiety ICMP. Komputer początkowy wysyła pierwszy

pakiet ICMP — *echo request* — ustawiając w nagłówku IP w polu TTL wartość 1. Co to oznacza? Pierwszy router, który odbierze pakiet, musi zmiejszyć TTL o 1, jest on wówczas zerowany, przez co router musi odrzucić ten pakiet i odesłać nadawcy informację zwrotną o odrzuceniu (pakiet ICMP typu 11 — *Time to Live Exceeded*). Komputer początkowy czeka więc na pierwszy pakiet ICMP typu 11 i sprawdza, kto jest jego nadawcą — ten router jest więc pierwszy na trasie do urządzenia docelowego. Proces ten powtarzany jest 3-krotnie. Następnie z komputera początkującego wysyłany jest pakiet o wyższym TTL (2) i oczekiwana jest odpowiedź od następnego routera na trasie (pierwszy router zmniejszy TTL z 2 na 1 i pakiet przepuści, drugi będzie musiał go odrzucić). Całość kontynuowana jest do momentu, w którym osiągnięte jest urządzenie docelowe — czyli w momencie, w którym odebrany jest zwykły *echo reply*.

V. Pytania kontrolne

1. Co to jest routing i na jakiej podstawie podejmowane są decyzje w ramach routingu?
2. Czym jest brama domyślna i do czego służy?
3. Jak interpretować wartość w polu TTL w nagłówku IP?
4. Do czego służy protokół ICMP?
5. Jak wygląda realizacja komendy *tracert*?