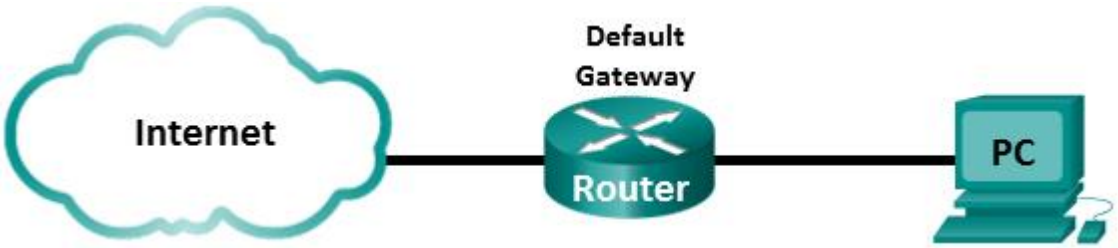
Laboratorium – Badanie protokołu ARP w wierszu poleceń systemu Windows oraz w programie Wireshark

Topologia



Cele

Część 1: Używanie polecenia ARP w systemie Windows

Część 2: Wykorzystywanie programu Wireshark do badania protokołu ARP

Scenariusz

Protokół ARP jest używany przez TCP/IP do odwzorowania adresu IP warstwy 3 na adres MAC warstwy 2. Gdy ramka jest przygotowywana do wysłania do sieci, to potrzebny jest docelowy adres MAC. W celu dynamicznego pozyskania adresu MAC docelowego urządzenia, protokół ARP wysyła zapytanie rozgłoszeniowe w sieci LAN. Urządzenie, które zawiera docelowy adres IP, zwraca odpowiedź, a adres MAC jest zapisywany w buforze ARP. Każde urządzenie w sieci posiada własną pamięć podręczną ARP (nazywaną w tym dokumencie buforem) albo mały obszar w pamięci RAM do przechowywania rezultatów operacji ARP. Licznik czasu bufora usuwa pozycje ARP, które nie były używane przez określony okres czasu.

ARP jest doskonałym przykładem skutecznego kompromisu wydajności. Gdyby protokół ARP nie miał bufora, to musiałby żądać translacji adresów za każdym razem, gdy ramka jest umieszczana w sieci. Wpływałoby to na zwiększenie opóźnienia w komunikacji i powodowałoby przeciążenie sieci. Nieograniczony czas przetrzymywania mógłby powodować błędy w przypadku urządzeń, których już nie ma w sieci lub w przypadku zmian adresu w warstwie 3.

Technik sieciowy musi mieć świadomość działania ARP, ale nie musi się nim regularnie zajmować. ARP jest protokołem, który umożliwia urządzeniom sieciowym komunikację z protokołami TCP/IP. Poza protokołem ARP nie istnieje inna efektywna metoda tworzenia adresu docelowego w datagramie warstwy 2. Z ARP związane jest jednak pewne ryzyko. Podszywanie się pod protokół ARP (ang. spoofing) albo zatruwanie (ang. poisoning) ARP to techniki wykorzystywane przez napastnika do wstawienia błędnego przyporządkowania adresu MAC w sieci. Jeżeli napastnik fałszuje adresy MAC urządzeń, to ramki są wysyłane do niepoprawnego adresu odbiorczego. Jednym ze sposobów obrony przed atakiem podszywania jest ręczne konfigurowanie statycznych odwzorowań ARP. Aby ograniczyć dostęp do sieci tylko dla upoważnionych urządzeń, można utworzyć listę autoryzowanych adresów MAC skonfigurowanych na urządzeniach Cisco.

W tym laboratorium będziesz korzystać z polecenia ARP w Windows, aby wyświetlić tablicę ARP. Możesz również wykasować zawartość bufora ARP i dodać statyczne wpisy ARP.

Wymagane wyposażenie

- 1 PC (Windows 7, Vista lub XP z dostępem do Internetu z zainstalowanym programem Wireshark)

Część 1. Używanie polecenia ARP w systemie Windows

Polecenie **arp** umożliwia użytkownikowi wyświetlenie i modyfikację bufora ARP w Windows. Dostęp do tego polecenia masz w wierszu poleceń systemu Windows.

Krok 1. Wyświetl zawartość bufora ARP.

a. Otwórz okno wiersza poleceń w PC-A i wpisz **arp**.

```
C:\Users\User1> arp


Wyświetla i modyfikuje tablicę translacji IP na adresy
fizyczne, używane przez protokół rozróżniania adresów (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a Wyświetla bieżące wpisy protokołu ARP przez odpytywanie bieżących danych
protokołu. Jeżeli parametr inet_addr jest podany, to wyświetlony jest adres IP i
fizyczny dla określonego komputera.  Jeżeli więcej niż jeden interfejs sieciowy
korzysta z protokołu ARP, to wyświetlane są wpisy dla każdej tabeli protokołu ARP.
  -g To samo co -a.
  -v Wyświetla bieżące wpisy protokołu ARP w trybie pełnym. Zostaną pokazane wszystkie
nieprawidłowe wpisy oraz wpisy interfejsu pętli zwrotnej.
  inet_addr Określa adres internetowy.
-N if_addr Wyświetla wpisy protokołu ARP dla interfejsu sieciowego określonego przez
if_addr.
-d Usuwa hosta określonego przez inet_addr. W inet_addr można użyć symbolu
wieloznacznego * do usunięcia wszystkich hostów.
-s Dodaje hosta i kojarzy adres internetowy inet_add z fizycznym adresem internetowym
eth_addr.
Adres fizyczny jest reprezentowany przez 6 szesnastkowych bajtów oddzielonych znakami
łącznika. Wpis dokonywany jest na stałe.
  eth_addr Określa adres fizyczny.
  if_addr Jeżeli jest określony, to wskazuje adres interfejsu, którego tabela
translacji powinna zostać zmieniona.
Jeżeli nie jest określony, zostanie użyty pierwszy odpowiadający interfejs.
Przykłady:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Dodaje zapis statyczny.
  > arp -a                                    .... Wyświetla tabelę arp.
```

b. Przeanalizuj wynik działania tego polecenia.

Które polecenie powinno być użyte do wyświetlenia wszystkich wpisów znajdujących się w buforze ARP?

_____

Które polecenie powinno być użyte do skasowania wszystkich wpisów znajdujących się w buforze ARP (opróżnienie pamięci podręcznej ARP)?

_____

Jakiego polecenia należy użyć, aby usunąć wpis z bufora ARP dla adresu 192.168.1.1?

_____

c. Wpisz **arp –a** aby wyświetlić tabelę ARP.

```
C:\Users\User1> arp –a

Interfejs: 192.168.1.3 --- 0xb
  Adres internetowy      Adres fizyczny      Typ
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamiczne
  192.168.1.255         ff-ff-ff-ff-ff-ff     statyczne
  224.0.0.22            01-00-5e-00-00-16 statyczne
  224.0.0.252           01-00-5e-00-00-fc statyczne
  239.255.255.250       01-00-5e-7f-ff-fa statyczne
```

Uwaga: Tablica ARP jest pusta, jeżeli używasz Windows XP (jak poniżej).

```
C:\Documents and Settings\User1> arp -a
Nie znaleziono wpisów ARP.
```

d. Wykonaj ping z komputera PC do innego komputera znajdującego się w tej samej sieci lokalnej, w celu dodania dynamicznych wpisów do bufora ARP.

```
C:\Documents and Settings\User1> ping 192.168.1.2

Interfejs: 192.168.1.3 --- 0xb
  Adres internetowy      Adres fizyczny      Typ
  192.168.1.2           00-50-56-be-f6-db     dynamiczne
```

Jaki jest adres fizyczny dla hosta który ma adres IP 192.168.1.2?

_____

Krok 2. Skoryguj ręcznie wpisy znajdujące się w buforze ARP.

W celu usunięcia wpisów w buforze ARP wykonaj polecenie **arp –d {inet-addr | *}**. Adresy mogą być kasowane pojedynczo poprzez podanie adresu IP albo wszystkie zapisy mogą być skasowane za jednym razem po wykorzystaniu znaku *.

Upewnij się, czy bufor ARP zawiera następujące wpisy: bramę domyślną (192.168.1.1) oraz komputery znajdujące się w tej samej sieci lokalnej.

a. Wykonaj ping z komputera do wszystkich znanych adresów komputerów w sieci lokalnej.

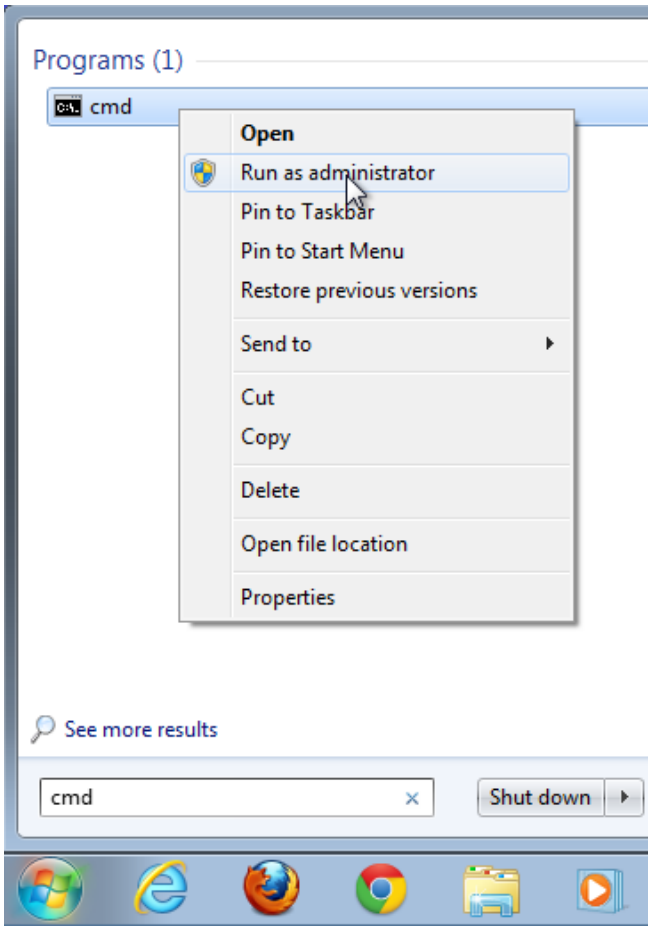
b. Sprawdź, czy wszystkie adresy zostały dodane do bufora ARP. Jeżeli adres nie znajduje się w buforze ARP, to wykonaj ping do adresu docelowego i upewnij się, że adres został dodany do bufora ARP.

```
C:\Users\User1> arp –a

Interfejs: 192.168.1.3 --- 0xb
  Adres internetowy      Adres fizyczny      Typ
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamiczne
  192.168.1.2           00-50-56-be-f6-db     dynamiczne
  192.168.1.11          0c-d9-96-e8-8a-40     dynamiczne
  192.168.1.12          0c-d9-96-d2-40-40     dynamiczne
  192.168.1.255         ff-ff-ff-ff-ff-ff     statyczne
  224.0.0.22            01-00-5e-00-00-16 statyczne
  224.0.0.252           01-00-5e-00-00-fc statyczne
  239.255.255.250       01-00-5e-7f-ff-fa statyczne
```

c. Przejdź do wiersza poleceń jako administrator. Kliknij ikonę **Start** a potem *Wyszukaj programy i* wpisz w polu **cmd**. Gdy pokaże się ikona **cmd.exe**, za pomocą prawego przycisku myszy wybierz **Uruchom jako administrator**. Kliknij **Tak** by pozwolić programowi na wykonanie zmian.

Uwaga: Dla użytkowników Windows XP nie jest wymagane posiadanie praw administratora by modyfikować wpisy w buforze ARP.



d. W oknie wiersza polecenia administratora wpisz **arp-d ***. To polecenie usuwa wszystkie wpisy z bufora ARP. Upewnij się, czy wszystkie wpisy w buforze ARP zostały usunięte za pomocą polecenia **arp –a**.

```
C:\windows\system32> arp -d *
C:\windows\system32> arp -a
Nie znaleziono wpisów ARP.
```

e. Poczekaj kilka minut. Protokół Neighbor Discovery rozpoczął działanie by ponownie wypełnić bufor ARP.

```
C:\Users\User1> arp -a

Interfejs: 192.168.1.3 --- 0xb
  Adres internetowy      Adres fizyczny      Typ
  192.168.1.255         ff-ff-ff-ff-ff-ff     statyczne
```

Uwaga: Protokół Neighbor Discovery nie jest zaimplementowany w systemie Windows XP.

f. Z komputera wykonaj ping do innego komputera w sieci lokalnej (np. 192.168.1.2). Sprawdź, czy wpis ARP został dodany do bufora.

```
C:\Users\User1> arp -a

Interfejs: 192.168.1.3 --- 0xb
```

```
  Adres internetowy      Adres fizyczny      Typ
  192.168.1.2           00-50-56-be-f6-db     dynamiczne
  192.168.1.11          0c-d9-96-e8-8a-40     dynamiczne
  192.168.1.12          0c-d9-96-d2-40-40     dynamiczne
  192.168.1.255         ff-ff-ff-ff-ff-ff     statyczne
```

g. Zanotuj adres fizyczny dla jednego z wybranych komputerów.

_____

Usuń konkretną pozycję z bufora ARP za pomocą polecenia **arp –d *inet-addr***. W wierszu poleceń wpisz **arp -d 192.168.1.12** aby usunąć pozycję wybranego komputera w ARP.

```
C:\windows\system32> arp –d 192.168.1.12
```

h. Wpisz polecenie **arp –a** aby sprawdzić, czy pozycja ARP została usunięta z bufora ARP.

```
C:\Users\User1> arp –a

Interfejs: 192.168.1.3 --- 0xb
  Adres internetowy      Adres fizyczny      Typ
  192.168.1.2           00-50-56-be-f6-db     dynamiczne
  192.168.1.11          0c-d9-96-e8-8a-40     dynamiczne
  192.168.1.255         ff-ff-ff-ff-ff-ff     statyczne
```

i. Możesz dodać konkretny wpis do bufora ARP za pomocą polecenia **arp –s *inet_addr mac_addr***. W tym przykładzie będą używane adresy IP i MAC wybranego komputera. Użyj adresu MAC zanotowanego w kroku g.

```
C:\windows\system32> arp –s 192.168.1.12 0c-d9-96-d2-40-40
```

j. Sprawdź czy do bufora ARP dodano pozycję wybranego komputera.

Część 2. Wykorzystywanie programu Wireshark do badania protokołu ARP

W części 2 będziesz badać wymianę informacji w protokole ARP za pomocą programu Wireshark. Będziesz także badać opóźnienia w sieci spowodowane przez wymianę informacji ARP pomiędzy urządzeniami.

Krok 1. Skonfiguruj program Wireshark do przechwytywania pakietów.

a. Uruchom program Wireshark.

b. Wybierz interfejs sieciowy używany do przechwytywania wymiany informacji ARP.

Krok 2. Przechwyć i oceń komunikację ARP.

a. Rozpocznij przechwytywanie pakietów w Wireshark. Użyj odpowiedniego filtra, aby wyświetlić tylko pakiety ARP.

b. Opróżnij bufor ARP za pomocą polecenia **arp –d ***.

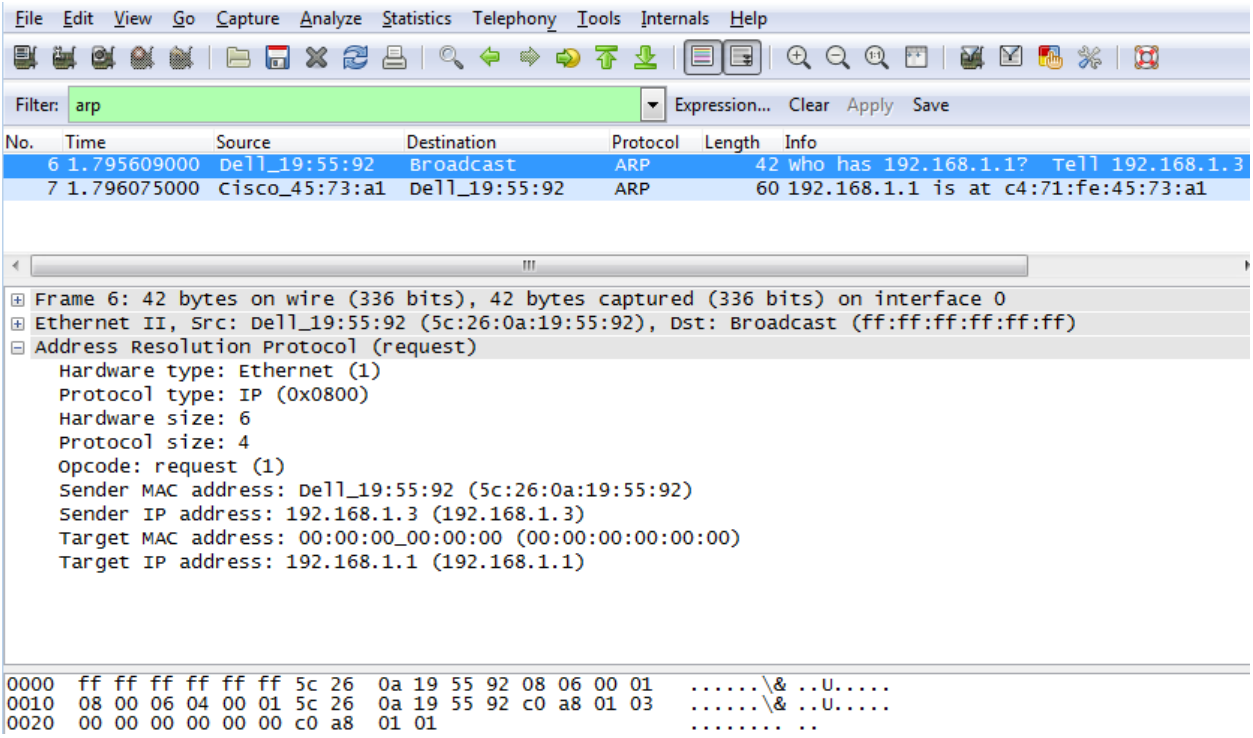
c. Sprawdź, czy bufor ARP został opróżniony.

d. Wykonaj ping do bramy domyślnej za pomocą polecenia **ping 192.168.1.1**.

e. Gdy proces ping do bramy domyślnej zakończy się, zatrzymaj przechwytywanie w programie Wireshark.

f. Zbadaj dane przechwycone w Wireshark - czy w panelu szczegółów pakietów znajdują się informacje pochodzące z ARP.

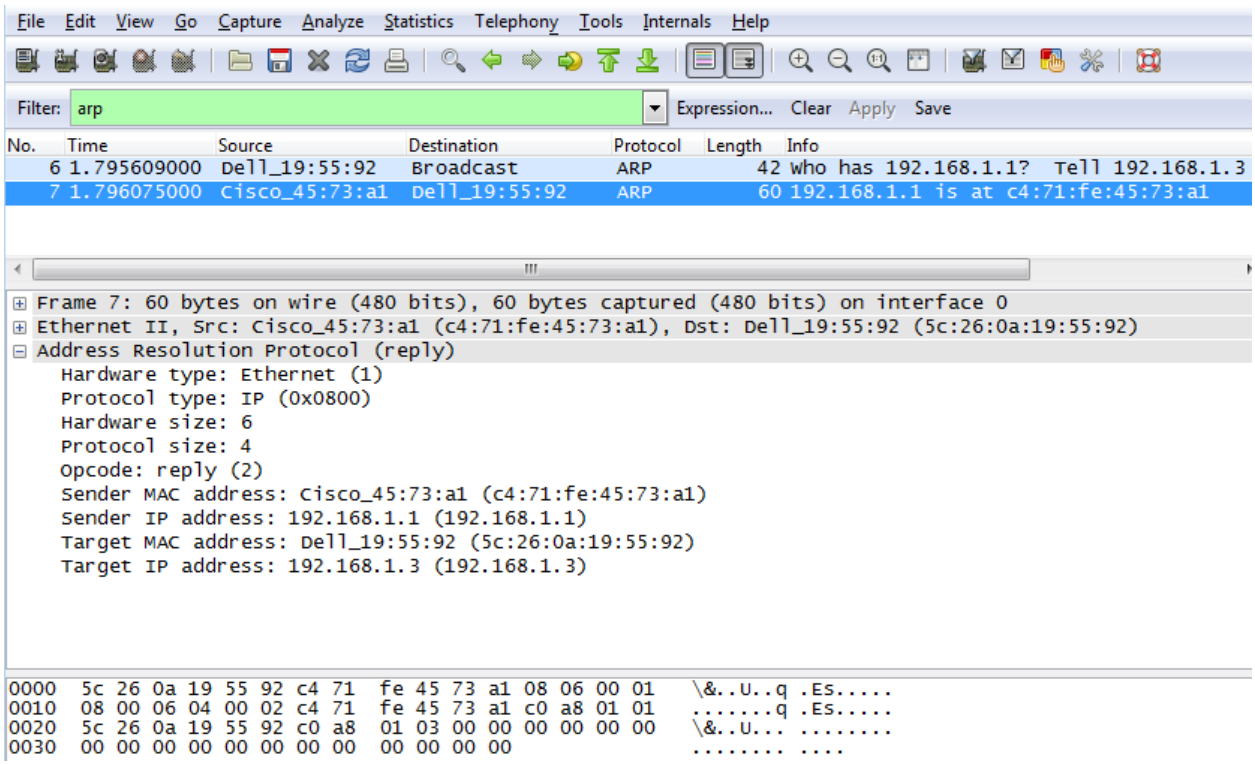
Jak nazywa się pierwszy pakiet ARP? _____



Wypełnij następującą tabelę korzystając z informacji zawartych w pierwszym przechwyconym pakiecie ARP.

Pole	Wartość
Adres MAC nadawcy	
Adres IP nadawcy	
Docelowy adres MAC	
Docelowy adres IP	

Jak nazywa się drugi pakiet ARP? _____



Wypełnij następującą tabelę korzystając z informacji zawartych w drugim przechwyconym pakiecie ARP.

Pole	Wartość
Adres MAC nadawcy	
Adres IP nadawcy	
Docelowy adres MAC	
Docelowy adres IP	

Krok 3. Zbadaj opóźnienia w sieci spowodowane przez protokół ARP.

a. Usuń wpisy ARP w komputerze.

b. W programie Wireshark uruchom przechwytywanie.

c. Wykonaj ping do innego komputera w tej samej sieci lokalnej (np. 192.168.1.12). Ping powinien zakończyć się pozytywnie po pierwszym żądaniu echa (ang. echo request).

Uwaga: Jeżeli wszystkie pingi zakończyły się pozytywnie, to wybrany komputer powinien zostać zrestartowany aby zaobserwować opóźnienie w sieci wprowadzane przez ARP.

```
C:\Users\User1> ping 192.168.1.12
Upłynął limit czasu żądania.
Odpowiedź z 192.168.1.1: bajtów=32 czas=2ms TTL=255
Odpowiedź z 192.168.1.12: bajtów=32 czas=2ms TTL=255
Odpowiedź z 192.168.1.12: bajtów=32 czas=2ms TTL=255

Statystyka badania ping dla 192.168.1.12:
    Pakiety: Wysłane = 4, Odebrane = 3, Utracone = 1 (25% straty),
```

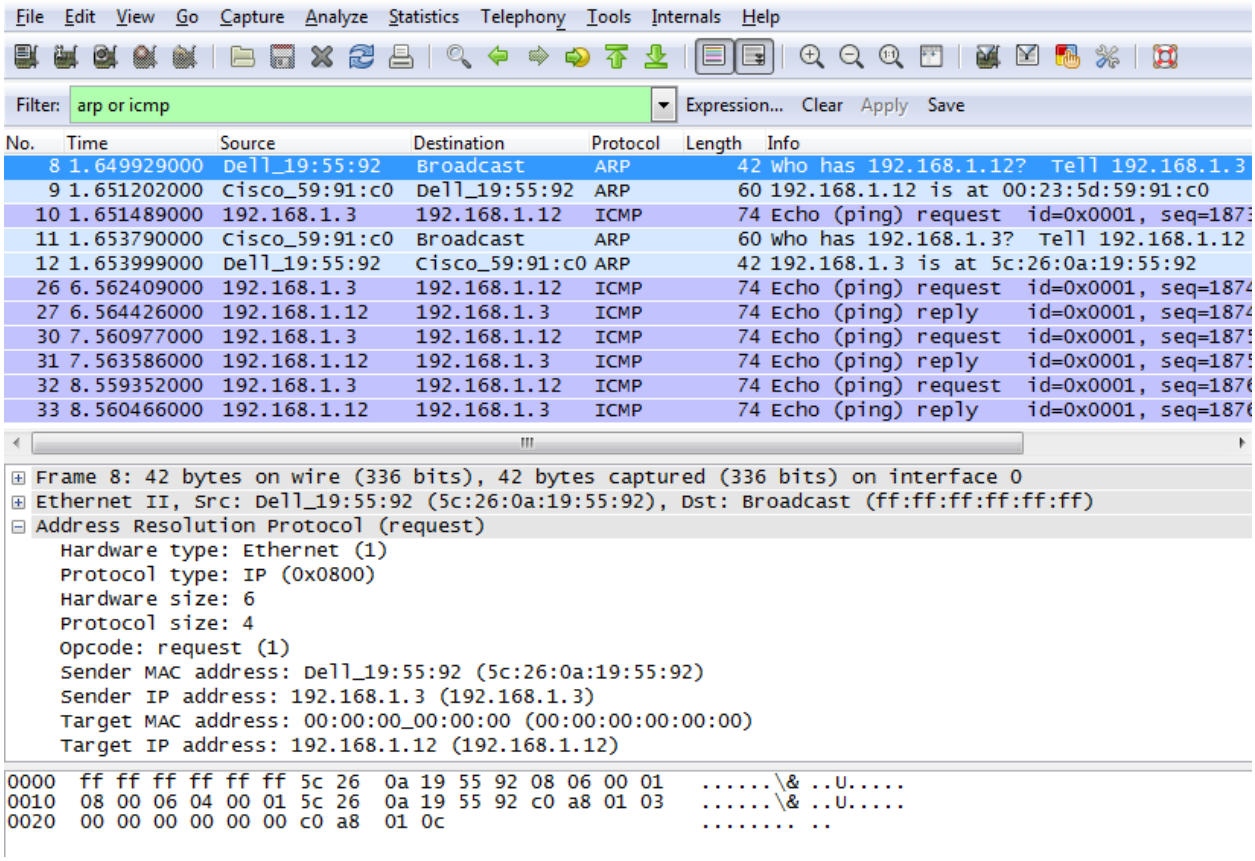
```
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 1 ms, Maksimum = 3 ms,Czas średni = 2 ms
```

d. Gdy proces ping zakończy się, zatrzymaj przechwytywanie w programie Wireshark. Aby wyświetlić tylko wyjścia ARP i ICMP, użyj odpowiedniego filtra Wireshark. W programie Wireshark wpisz **arp lub icmp** w obszarze **Filter:**.

e. Zbadaj przechwycone przez program Wireshark informacje. W tym przykładzie ramka 10 zawiera pierwsze żądanie ICMP wysłane przez komputer do innego komputera w sieci lokalnej. Ponieważ nie ma żadnych wpisów ARP, to żądanie ARP zostało wysłane na adres IP karty sieciowej komputera z prośbą o adres MAC. Podczas wymiany informacji w protokole ARP żądanie "echo request" nie otrzyma odpowiedzi przed upływem określonego limitu czasowego dla tego żądania. (ramki 8 – 12)

   Po dodaniu wpisu ARP dla wybranego komputera do bufora ARP, ostatnie trzy wymiany ICMP zakończyły się pozytywnie, co zostało pokazane w ramkach 26, 27 i 30 – 33.

   ARP jest doskonałym przykładem skutecznego kompromisu wydajności, co zostało zilustrowane w przechwyconych informacjach w programie Wireshark. Gdyby protokół ARP nie miał bufora, to musiałby żądać translacji adresów za każdym razem, gdy ramka jest umieszczana w sieci. Wpływałoby to na zwiększenie opóźnienia w komunikacji i mogło powodować przeciążenie sieci LAN.



Do przemyślenia

1. Jak i kiedy są usuwane statyczne wpisy ARP?

   _____

2. W jakim celu dodaje się statyczne wpisy ARP do bufora?

   _____

3. Jeżeli żądania ARP mogą spowodować opóźnienia w sieci, dlaczego złym pomysłem jest to, aby czas dla utrzymywania wpisów ARP był nieograniczony?

   _____