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

Topologia

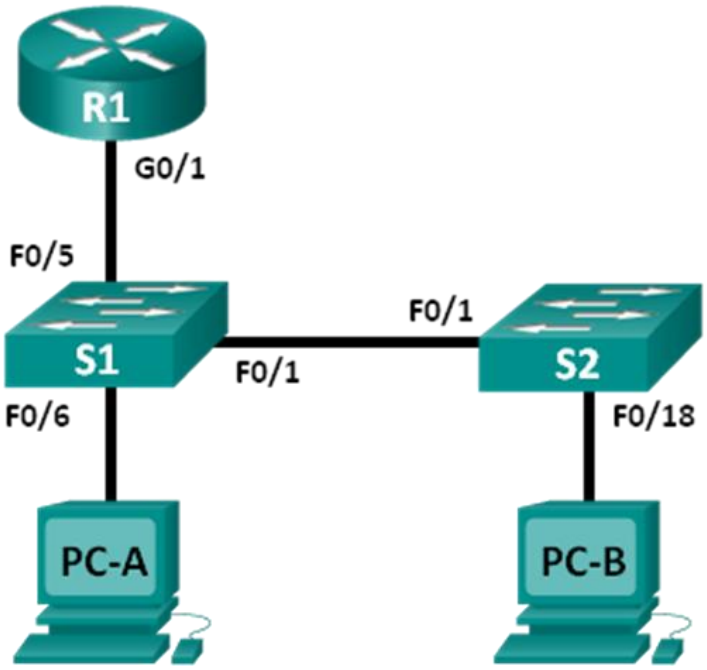


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.1.1	255.255.255.0	nie dotyczy
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	Karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	Karta sieciowa	192.168.1.2	255.255.255.0	192.168.1.1

Cele

Część 1: Tworzenie i konfiguracja sieci

Część 2: Używanie polecenia ARP w systemie Windows

Część 3: Używanie polecenia show arp w systemie IOS

Część 4: 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 i routerach Cisco, aby wyświetlić tablicę ARP. Możesz również wykasować zawartość bufora ARP i dodać statyczne wpisy ARP.

Uwaga: Routery używane w laboratorium to Cisco 1941 ISR (Integrated Services Routers) z oprogramowaniem Cisco IOS 15.2(4)M3 (obraz universalk9). Zastosowane w laboratorium przełączniki to Cisco Catalyst 2960 z oprogramowaniem Cisco IOS wersja 15.0(2) (obraz lanbasek9). Można używać innych routerów lub przełączników oraz wersji Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Prawidłowe identyfikatory interfejsów znajdują się w tabeli Interfejsów routerów na końcu tej instrukcji.

Uwaga: Upewnij się, że konfiguracje routerów i przełączników zostały usunięte i nie mają konfiguracji startowej. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane wyposażenie

- 1 router (Cisco 1941 z oprogramowaniem Cisco IOS, wersja 15.2 (4) M3 obraz uniwersalny lub porównywalny)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.0(2) obraz lanbasek9 lub porównywalny)
- 2 komputery PC (Windows 7, Vista lub XP z emulatorem terminala, takim jak Tera Term oraz zainstalowanym programem Wireshark)
- Kable konsolowe do konfiguracji urządzeń Cisco przez port konsolowy
- Kable Ethernet zgodnie z pokazaną topologią

Uwaga: interfejsy Fast Ethernet w przełączniku Cisco 2960 mają włączony mechanizm automatycznego wykrywania typu kabla, więc oba przełączniki można połączyć za pomocą kabla prostego. Do łączenia innych modeli przełączników Cisco konieczne może być użycie kabla Ethernet z przeplotem (crossover).

Część 1. Budowa i konfiguracja sieci

Krok 1. Połącz urządzenia zgodnie z topologią.

Krok 2. Zgodnie z tabelą adresacji skonfiguruj adresy IP dla urządzeń.

Krok 3. Z komputera PC-B sprawdź połączenie sieciowe za pomocą polecenia ping do wszystkich urządzeń.

Część 2. 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 192.168.1.11?

_____

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 komputera PC-A-B, 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: R1 G0/1 bramę domyślną (192.168.1.1), PC-B (192.168.1.2) oraz oba przełączniki (192.168.1.11 i 192.168.1.12).

a. Wykonaj ping z komputera PC-A do wszystkich adresów znajdujących się w tabeli adresowania.

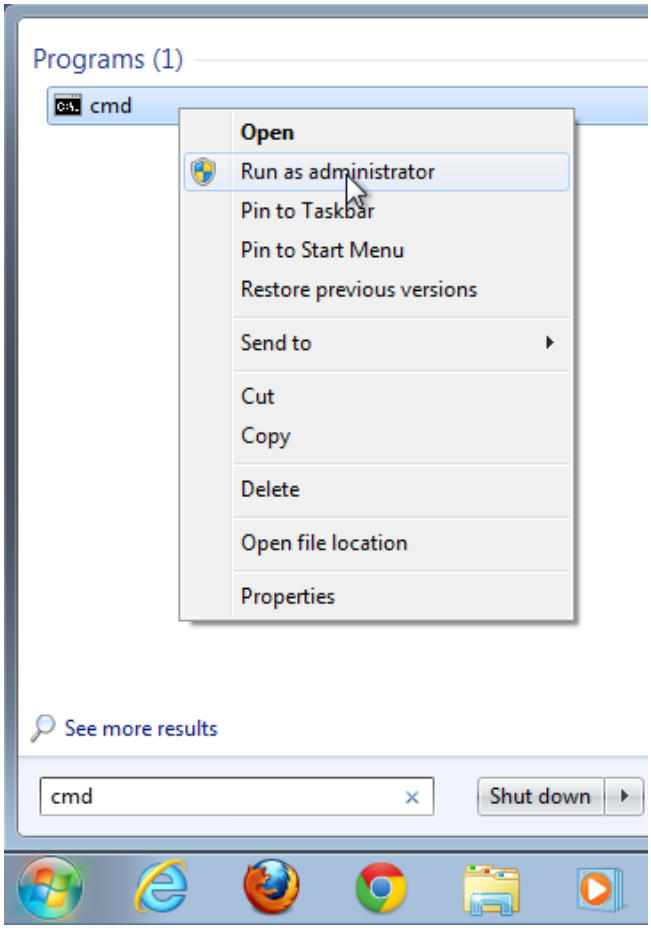
b. Sprawdź, czy wszystkie adresy zostały dodane do bufora ARP. Jeżeli adres nie znajduje się w buforze ARP, to wykonaj ping do adresu docelowego i upewnij się, że adres został dodany do bufora ARP.

```
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 PC-A wykonaj ping do komputera PC-B (192.168.1.2) i do przełączników (192.168.1.11 i 192.168.1.12), aby dodać wpisy ARP. Sprawdź, czy wpisy ARP zostały dodane 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 przełącznika S2.

_____

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 dla przełącznika S2 w ARP.

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

h. Wpisz polecenie **arp –a** aby sprawdzić, czy pozycja ARP dla S2 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 dla przełącznika S2. 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 dla przełącznika S2.

Część 3. Wykorzystanie polecenia IOS show arp

System Cisco IOS umożliwia wyświetlenie zawartości bufora ARP w routerach i przełącznikach za pomocą polecenia **show arp** lub **show ip arp**.

Krok 1. Wyświetli wpisy ARP na routerze R1.

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            0   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            0   0050.56be.768c  ARPA   GigabitEthernet0/1
R1#
```

Zauważ, że dla pierwszego wpisu nie ma wartości Age (-), dot. interfejsu routera G0/1 (brama domyślna sieci LAN). Age to czas (mierzony w minutach) jaki upłynął od ostatniego umieszczenia pozycji w buforze ARP i jest on zwiększany dla pozostałych wpisów. Protokół Neighbor Discovery służy do przekazywania adresów IP oraz adresów MAC komputerów PC-A i PC-B do ARP.

Krok 2. Dodaj wpisy ARP na routerze R1.

Można dodawać wpisy ARP do tabeli ARP w routerze poprzez wykonywanie polecenia ping do urządzeń.

a. Wykonaj ping do przełącznika S1.

```
R1# ping 192.168.1.11
Naciśnij odpowiednią kombinację klawiszy, aby przerwać.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

b. Upewnij się, że wpis ARP dla przełącznika S1 został dodany do tablicy ARP w routerze R1.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2              6   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3              6   0050.56be.768c  ARPA   GigabitEthernet0/1
Internet  192.168.1.11             0   0cd9.96e8.8a40  ARPA   GigabitEthernet0/1
R1#
```

Krok 3. Wyświetli wpisy ARP w przełączniku S1.

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             46   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2              8   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3              8   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
S1#
```

Krok 4. Dodaj wpisy ARP w przełączniku S1.

Za pomocą polecenia ping do innych urządzeń można wpisy ARP dodawać do tabeli ARP przełącznika.

a. Z przełącznika S1 wykonaj ping do przełącznika S2.

```
S1# ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
```

b. Sprawdź, czy wpis ARP dla przełącznika S2 został dodany do tablicy ARP w S1.

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              5   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2             11   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3             11   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
```

```
Internet  192.168.1.12           2   0cd9.96d2.4040  ARPA   Vlan1
S1#
```

Część 4. Wykorzystywanie programu Wireshark do badania protokołu ARP

W części 4 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 ***.

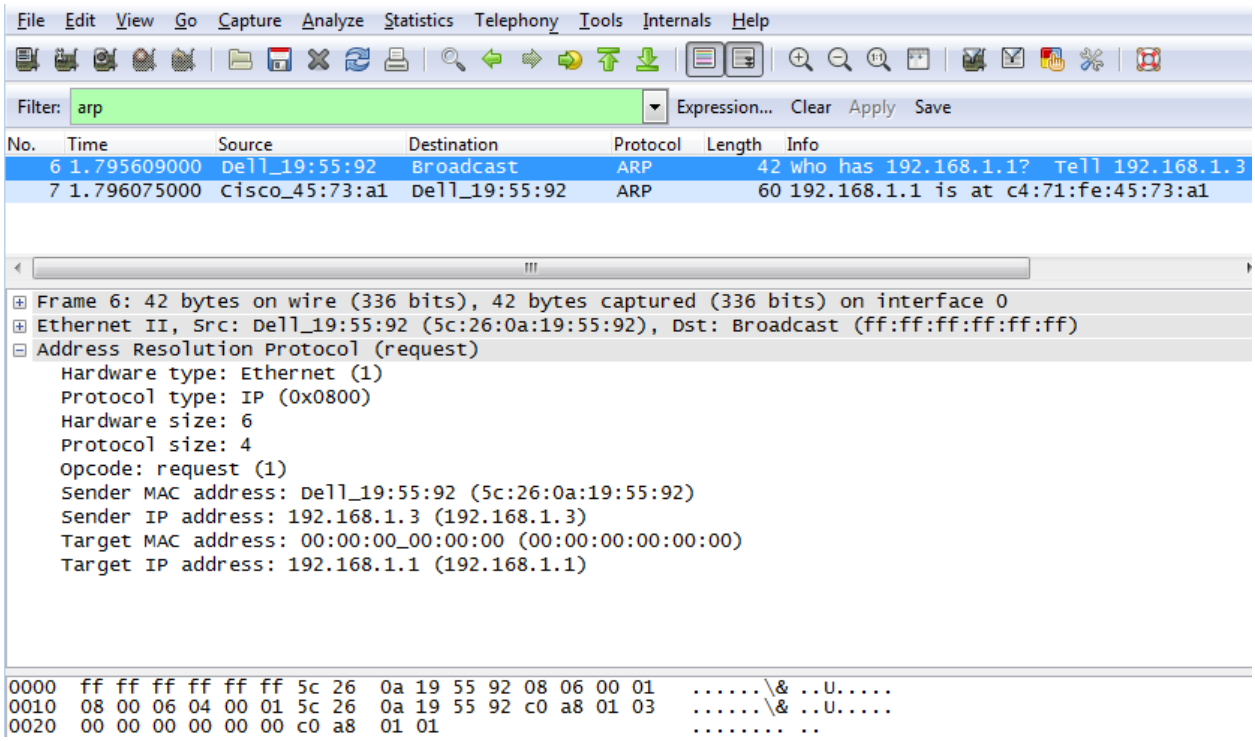
c. Sprawdź, czy bufor ARP został opróżniony.

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.

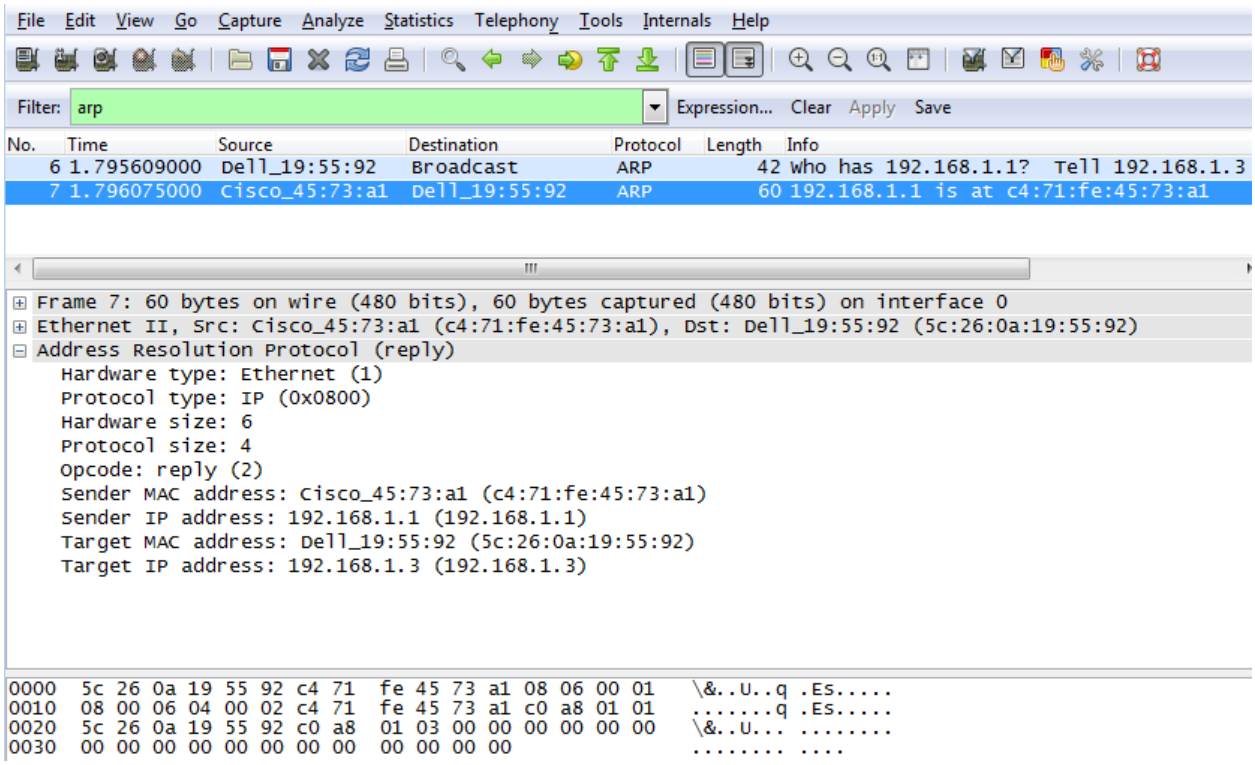
Jak nazywa się pierwszy pakiet ARP? _____



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 PC-A.

b. W programie Wireshark uruchom przechwytywanie.

c. Wykonaj ping do przełącznika S2 (192.168.1.12). Ping powinien zakończyć się pozytywnie po pierwszym żądaniu echa (ang. echo request).

Uwaga: Jeżeli wszystkie pingi zakończyły się pozytywnie, to S1 powinien zostać zrestartowany aby zaobserwować opóźnienie w sieci wprowadzane przez ARP.

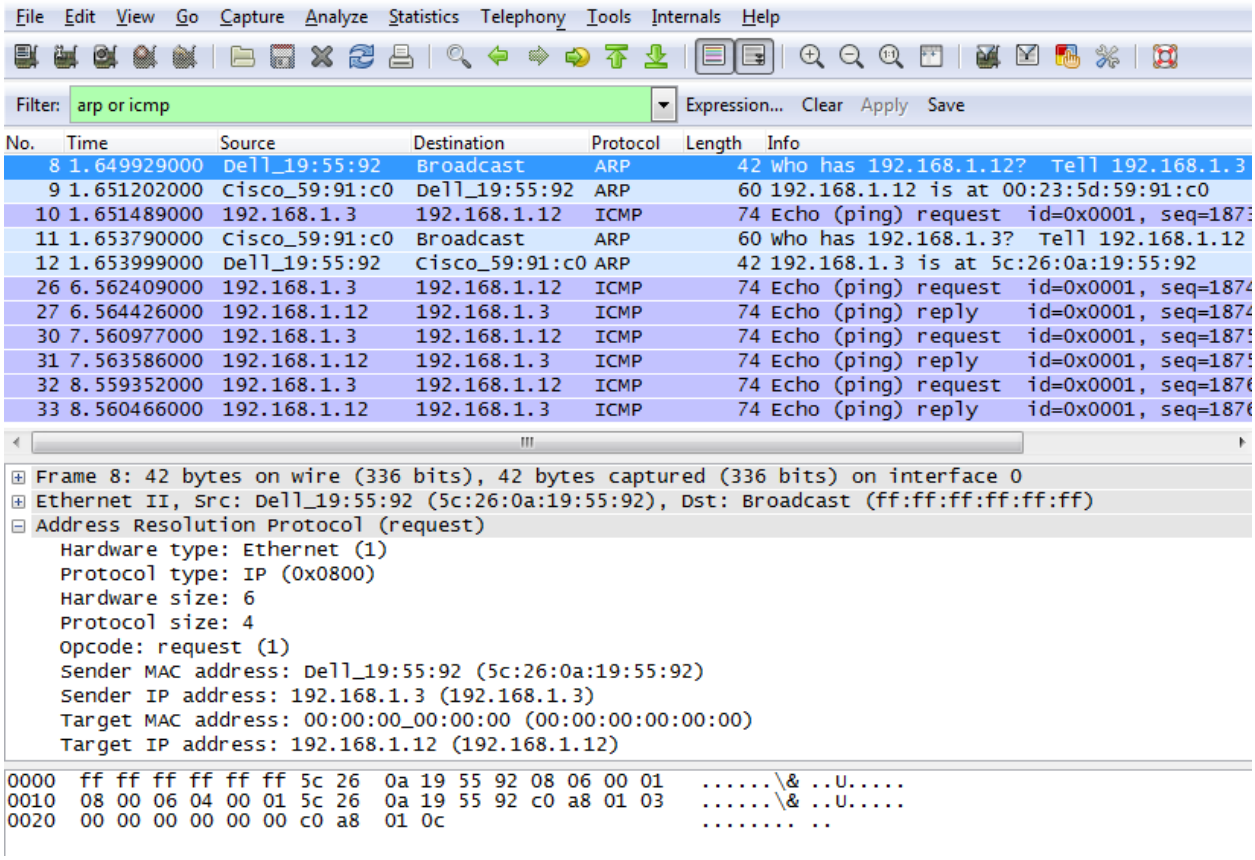
```
C:\Users\User1> ping 192.168.1.12
Upłynął limit czasu żądania.
Odpowiedź z 192.168.1.1: bajtów=32 czas=2ms TTL=255
Odpowiedź z 192.168.1.12: bajtów=32 czas=2ms TTL=255
Odpowiedź z 192.168.1.12: bajtów=32 czas=2ms TTL=255

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 PC-A do przełącznika S1. Ponieważ nie ma żadnych wpisów ARP dla S1, to żądanie ARP zostało wysłane na adres IP zarządzający przełącznikiem S1 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 S1 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?

   _____

Tabela zbiorcza interfejsów routera

Zestawienie interfejsów routera				
Model routera	**Interfejs Ethernet #1**	**Interfejs Ethernet #2**	**Interfejs Serial #1**	**Interfejs Serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Ta tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet i Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, mimo iż dany router może być w nie wyposażony. Przykładem może być interfejs ISDN BRI. Informacja w nawiasach jest dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.