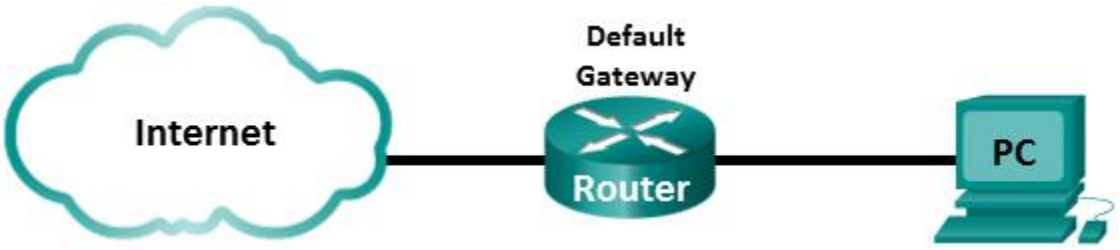
Laboratorium - Wykorzystanie programu Wireskark do badania ramek Ethernetowych

Topologia



Cele

Część 1: Badanie pól nagłówka w ramce Ethernet II.

Cześć 2: Użycie programu Wireshark do przechwycenia i analizy ramek Ethernetowych.

Tło / Scenariusz

Kiedy wyższe warstwy komunikują się między sobą, dane przechodzą w dół warstw modelu OSI (Open Systems Interconnection) i ostatecznie są enkapsulowane w ramkę warstwy 2. Budowa ramki jest zależna od technologii dostępu do medium. Na przykład jeśli protokołami warstw wyższych są TCP oraz IP, a technologia dostępu do mediów to Ethernet, wtedy metodą enkapsulacji w warstwie 2 będzie Ethernet II. Sytuacja ta jest typowa dla środowisk sieci lokalnych LAN.

W czasie poznawania sposobu działania warstwy 2, bardzo przydatne jest przeanalizowanie informacji zawartych w nagłówku ramki. W pierwszej części tego laboratorium będziesz przypominał sobie pola znajdujące się w ramce Ethernet II. W drugiej części użyjesz programu Wireshark do przechwycenia i analizy pól ramki typu Ethernet II dla ruchu lokalnego i zdalnego.

Wymagane wyposażenie

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

Część 1. Badanie pól nagłówka ramki Ethernet II

W części 1 będziesz badał pola i ich zawartość w nagłówku ramki Ethernet II. Do tego celu zostaną użyte dane przechwycone w Wireshark.

Krok 1. Przejrzyj opisy i długości pól nagłówka ramki typu Ethernet II.

Preambuła	Adres docelowy	Adres źródłowy	Typ ramki	Dane	FCS (suma kontrolna)
8 bajtów	6 bajtów	6 bajtów	2 bajty	46 – 1500 bajtów	4 bajty

Krok 2. Sprawdź konfigurację sieci w komputerze PC.

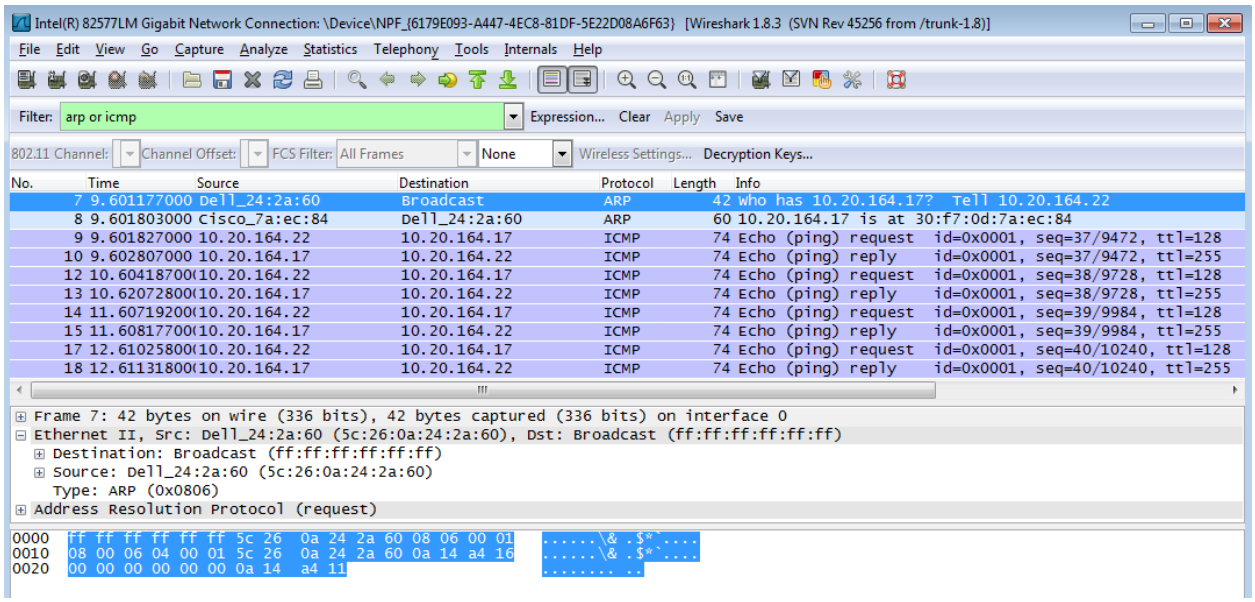
Adres IP tego komputera PC to 10.20.164.22, a brama domyślna ma adres 10.20.164.17.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cisco.com
   Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10
   IPv4 Address. . . . . . . . . . . : 10.20.164.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 10.20.164.17
```

Krok 3. Zbadaj ramki Ethernetowe w danych przechwyconych w Wireshark.

Widok okna programu Wireshark poniżej przedstawia pakiet wysłany w wyniku komendy ping wykonanej na komputerze PC do bramy głównej. W programie Wireshark zastosowano filtr, aby wyświetlić tylko protokoły ARP oraz ICMP. Sesja rozpoczyna się zapytaniem ARP o adres MAC bramy domyślnej, po którym następuje odpowiedź ARP. W następnym kroku wysyłane jest żądanie ping, na które brama domyślna udziela odpowiedzi. W systemach Windows typowo wykonanie komendy ping skutkuje wysłaniem 4 żądań echo request, na które host docelowy kolejno udziela odpowiedzi.



Krok 4. Badanie zawartości nagłówka ramki typu Ethernet II żądania ARP.

Poniższa tabela zawiera dane z pól nagłówka ramki typu Ethernet II dla pierwszej przechwyconej przez Wireshark ramki.

<table>
<tr><th>Pole</th><th>Wartość</th><th>Opis</th></tr>
<tr><td>Preambuła</td><td>Pominięte</td><td>To pole przedstawia bity synchronizujące używane przez kartę sieciową.</td></tr>
<tr><td>Adres docelowy</td><td>Rozgłoszenie (ff:ff:ff:ff:ff:ff)</td><td rowspan="2">Adres warstwy drugiej w ramce. Każdy adres ma długość 48 bitów lub 6 oktetów, zapisanych jako 12 cyfr szesnastkowych, 0-9, A-F.
Popularnym formatem zapisu jest 12:34:56:78:9A:BC.
Pierwsze sześć cyfr wskazuje producenta, ostatnie 6 cyfr to numer seryjny karty sieciowej (NIC).
Adresem docelowym może być adres rozgłoszeniowy, który zawiera same jedynki lub adres transmisji jednostkowej (ang. unicast). Adres źródłowy jest zawsze adresem transmisji jednostkowej (ang. unicast).</td></tr>
<tr><td>Adres źródłowy</td><td>Dell_24:2a:60 (5c:26:0a:24:2a:60)</td></tr>
<tr><td>Typ ramki</td><td>0x0806</td><td>W ramce typu Ethernet II to pole zawiera szesnastkową wartość, która wskazuje rodzaj protokołu wyższych warstw, którego datagram znajduje się w polu danych. Istnieje wiele protokołów wyższych warstw obsługiwanych przez ramki typu Ethernet II. Dwa z nich to:
<table>
<tr><th>Wartość</th><th>Opis</th></tr>
<tr><td>0x0800</td><td>Protokół IPv4</td></tr>
<tr><td>0x0806</td><td>Address resolution protocol (ARP)</td></tr>
</table>
</td></tr>
<tr><td>Dane</td><td>ARP</td><td>Zawiera enkaspulowane PDU wyższej warstwy. Pole danych ma rozmiar od 46 do 1500 bajtów.</td></tr>
<tr><td>FCS</td><td>Pominięte</td><td>Sekwencja kontrolna ramki (FCS) jest używana przez kartę sieciową do wykrywania błędów powstałych podczas transmisji. Jego wartość jest obliczana i umieszczana w ramce przez urządzenie wysyłające na podstawie zawartości pól: adres ramki, typ i dane. Pole to weryfikowane jest przez odbiorcę.</td></tr>
</table>

Dlaczego wartość pola adresu docelowego jest istotna przy przesyłaniu danych?

_____

_____

Dlaczego PC wysyła rozgłoszenie ARP przed wysłaniem pierwszego żądania ping?

_____

_____

_____

Jaki jest adres MAC źródła w pierwszej ramce? _____

Jaki jest producent (OUI) źródłowej karty sieciowej (NIC)? _____

Która część adresu MAC to OUI?

_____

Jaki jest numer seryjny źródłowej karty sieciowej (NIC)? _____

Część 2. Użycie programu Wireshark do przechwycenia i analizy ramek Ethernetowych.

W części 2 użyjesz programu Wireshark, aby przechwycić lokalne i zdalne ramki Ethernetowe. Następnie zbadasz informacje zawarte w polach nagłówków tych ramek.

Krok 1. Określ adres IP bramy domyślnej dla twojego PC.

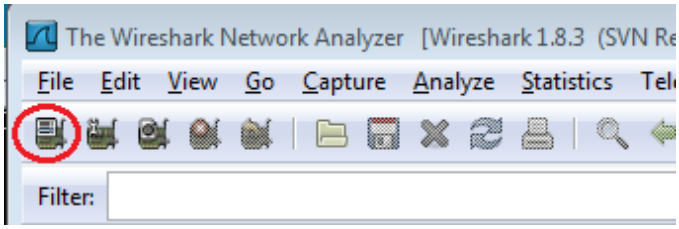
Otwórz okno linii komend i wykonaj polecenie **ipconfig**.

Jaki jest adres bramy domyślnej? _____.

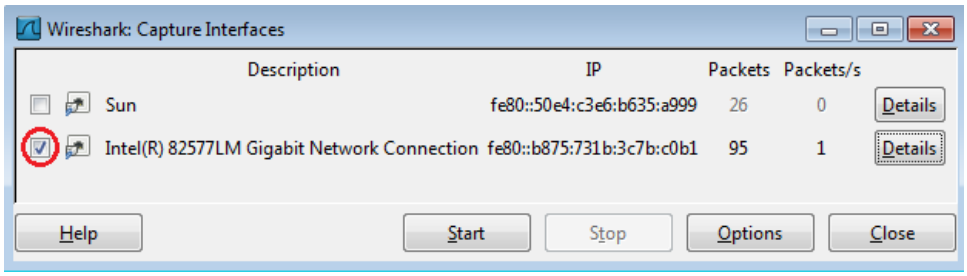
Krok 2. Rozpocznij przechwytywanie ruchu pojawiającego się na karcie twojego PCta.

a. Uruchom program Wireshark.

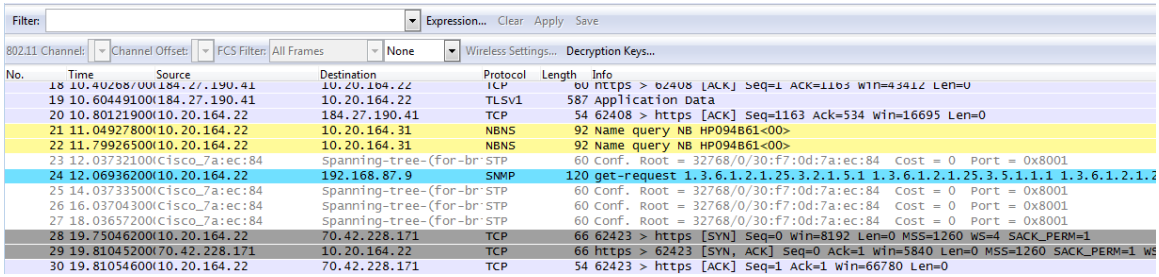
b. Na pasku narzędziowym Wireshark kliknij ikonę **Interface List** (Lista interfejsów).



c. W programie Wireshark w oknie Capture Interfaces wybierz odpowiedni interfejs w celu rozpoczęcia przechwytywania ruchu i następnie kliknij **Start**. Jeśli nie jesteś pewny, który interfejs wybrać, kliknij **Details** dla uzyskania dodatkowych informacji o interfejsach, które znajdują się na liście.



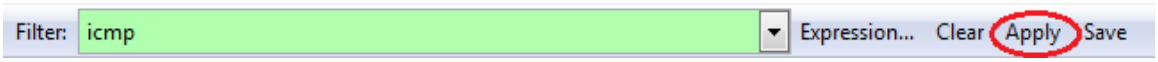
d. Obserwuj ruch, który pojawi się w oknie Packet List.



Krok 3. Przefiltruj zawartość okna Wireshark, tak aby pokazywał tylko ruch ICMP.

W celu zablokowania wyświetlania niechcianego ruchu w programie Wireshark można użyć filtrów. Filtr nie blokuje przechwytywania niechcianych danych, a tylko zapobiega ich wyświetlaniu. W tym przypadku ma być wyświetlony tylko ruch ICMP.

W polu **Filter** programu Wireshark wpisz **icmp**. Jeśli wpiszesz poprawną wartość w polu filtr, pole to będzie miało zielone tło. Jeśli pole jest zielone kliknij **Apply** w celu zastosowania filtrowania.

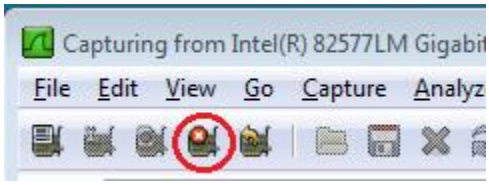


Krok 4. Używając okna linii komend komputera wydaj komendę ping do bramy domyślnej.

Używając okna linii komend wykonaj ping do bramy domyślnej używając adresu IP, który odczytałeś w kroku 1.

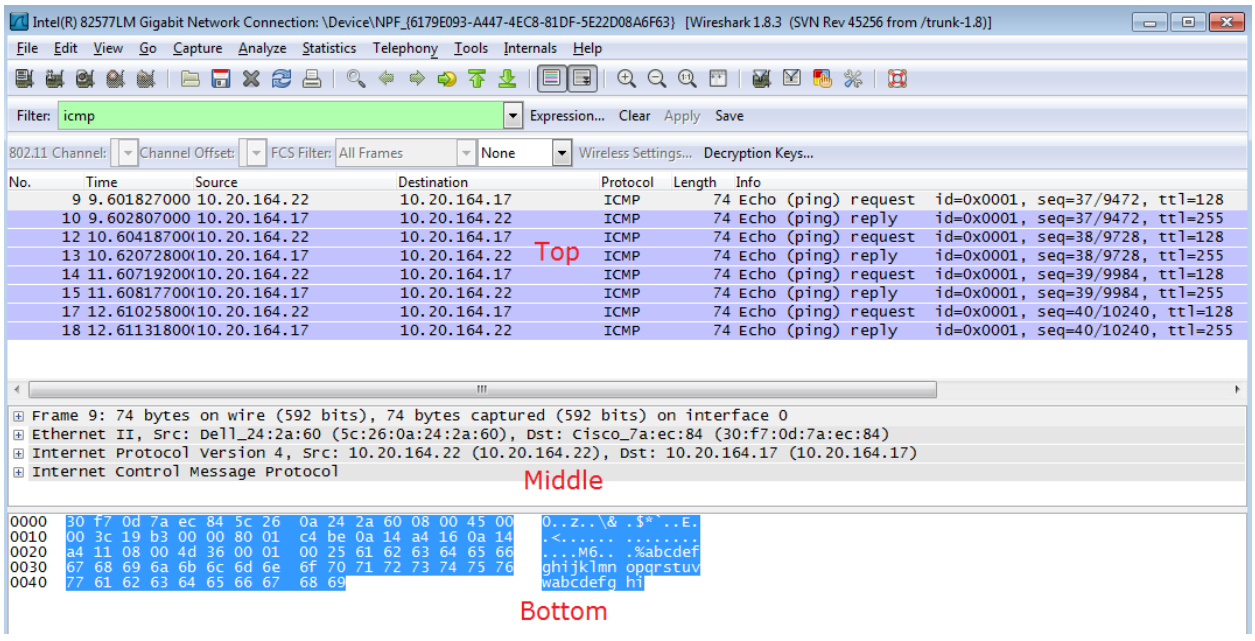
Krok 5. Zatrzymaj przechwytywanie ruchu na karcie sieciowej (NIC).

Kliknij ikonę **Stop Caputre** w celu zatrzymania przechwytywania ruchu.



Krok 6. Przeanalizuj w Wireshark pierwsze żądanie echa (ping).

Główne okno Wireshark podzielone jest na trzy sekcje: panel Packet List (na górze), panel Pacekt Details (po środku) i panel Packet Bytes (na dole). Jeśli wybrałeś właściwy interfejs dla przechwytywania ruchu w kroku 3, Wireshark powinien pokazywać informacje dotyczące ICMP w panelu Packet List, tak jak na poniższym przykładzie.



a. W panelu Packet List (górna część) kliknij pierwszą ramkę na liście. Powinieneś widzieć **żądanie echa (ping)** poniżej nagłówka **Info**. Kliknięcie powinno podświetlić linię na niebiesko.

b. Zbadaj pierwszą linijkę w panelu Packet Details (środkowa sekcja). Linia ta określa długość ramki, w tym przykładzie wynosi ona 74 bajty.

c. Druga linia w panelu Packet Details pokazuje, że jest to ramka typu Ethernet II. Widoczne są również adresy MAC źródłowy i docelowy.

   Jaki jest adres MAC karty sieciowej PCta? _____

   Jaki jest adres MAC bramy domyślnej? _____

d. Możesz kliknąć znak plus (+) na początku drugiej linii w celu wyświetlenia większej ilości informacji o ramce Ethernet II. Zauważ, że po kliknięciu znak plus zmienia się na minus (-).

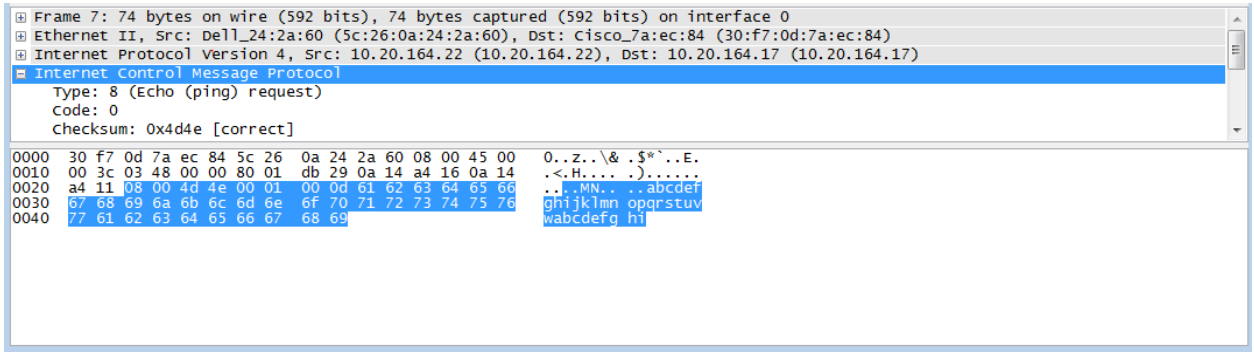
   Jaki typ danych wyższej warstwy zawarty jest w ramce? _____

e. Ostatnie dwie linie pokazane w części środkowej pokazują zawartość pola danych ramki. Zauważ, że dane zawierają źródłowy i docelowy adres IPv4.

   Jaki jest źródłowy adres IP? _____

   Jaki jest docelowy adres IP? _____

f. Możesz kliknąć dowolną linię w części środkowej okna w celu podświetlenia odpowiadającej jej części ramki przedstawionej szesnastkowo lub ASCII w panelu Packet Bytes (dolna sekcja). Kliknij linię **Internet Control Message Protocol** w środkowej części i zbadaj co zostanie podświetlone w panelu Packet Bytes.



   Jaką zawartość mają dwa ostanie oktety? _____ i

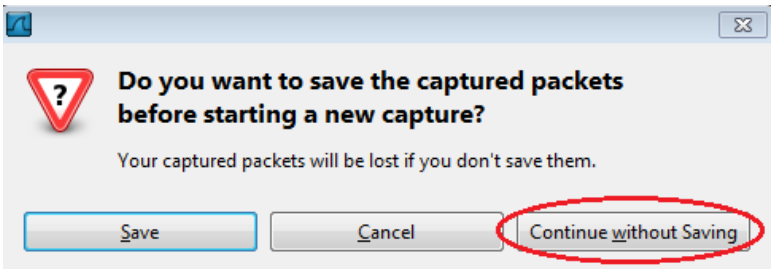
g. Kliknij następną ramkę w górnej części okna i zbadaj ramkę odpowiedzi na żądanie echa. Zauważ, że adresy MAC źródłowy i docelowy zostały zamienione miejscami, ponieważ ta ramka była wysłana z bramy domyślnej jako odpowiedź na pierwszy ping.

   Adres MAC jakiego urządzenia jest wyświetlony jako adres docelowy?

   _____

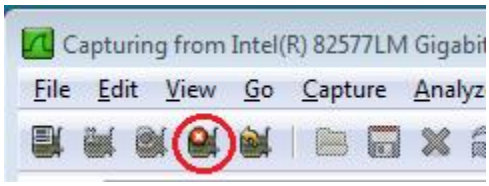
Krok 7. Uruchom ponownie przechwytywanie pakietów w Wireshark.

Kliknij ikonę **Start Capture**, aby uruchomić nowe przechwytywanie pakietów. Pojawi się wyskakujące okienko z pytaniem czy chcesz zapisać do pliku poprzednio przechwycone dane przed rozpoczęciem nowego przechwytywania. Kliknij **Continue without Saving** (Kontynuuj bez zapisania).



Krok 8. W oknie linii komend PC wydaj komendę: ping www.cisco.com.

Krok 9. Zatrzymaj przechwytywanie pakietów.



Krok 10. Zbadaj nowe dane w panelu Packet list.

Jaki jest adres MAC źródłowy i docelowy w pierwszej ramce żądania echa (ping)?

Źródło: _____.

Docelowy: _____

Jakie adresy IP źródłowy i docelowy znajdują się w polu danych ramki?

Źródło: _____

Docelowy: _____

Porównaj te adresy z adresami, które poznałeś w kroku 7. Jedynym adresem, który się zmienił jest docelowy adres IP. Dlaczego zmienił się docelowy adres IP, podczas gdy docelowy adres MAC pozostał ten sam?

_____

_____

_____

_____

Do przemyślenia

Wireshark nie pokazuje pola preambuła z nagłówka ramki. Co zawiera pole preambuła?

_____

_____