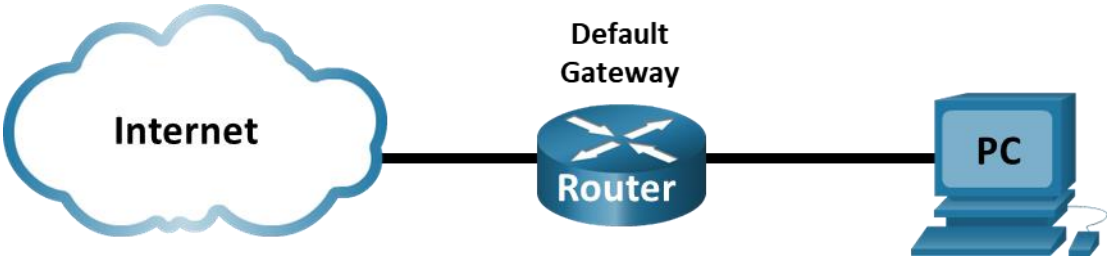
Laboratorium - Używanie programu Wireshark do badania ramek Ethernet

Topologia sieci



Cele

Część 1: Badanie pól nagłówka w ramce Ethernet II.

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

Wprowadzenie

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.Składnia ramki jest zależna od rodzaju 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 koncepcji warstwy 2, bardzo jest przydatne 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 zasoby

- 1 komputer PC (Windows z dostępem do Internetu i zainstalowanym Wireshark)

Instrukcje

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
8 bajtów	6 bajtów	6 bajtów	2 bajty	46 – 1500 bajtów	4 bajty

Krok 2: Sprawdź konfigurację sieci w komputerze PC.

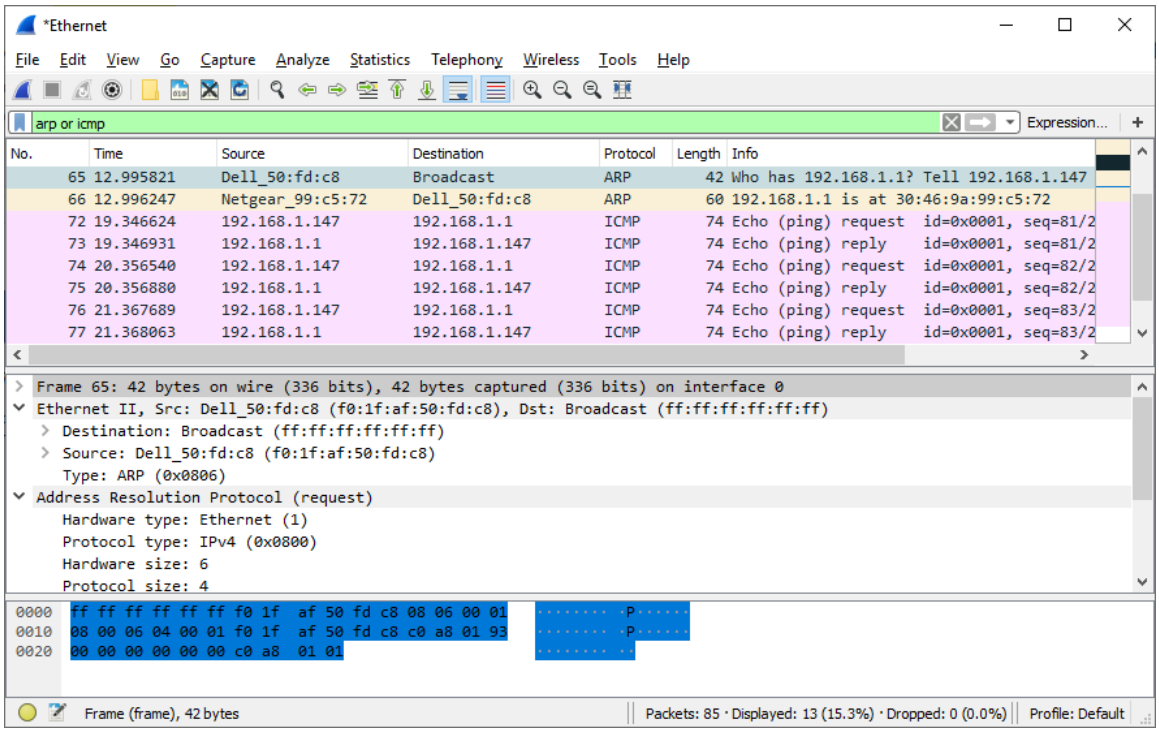
W tym przykładzie adres IP tego komputera PC to 192.168.1.147, a brama domyślna ma adres IP 192.168.1.1.

```
C:\>ipconfig /all

Ethernet adapter Ethernet:

Connection-specific DNS Suffix .:
Description ............: Intel(R) 82579LM Gigabit Network Connection
Physical Address.........: F0-1F-AF-50-FD-C8
DHCP Enabled............: Yes
Autoconfiguration Enabled ....: Yes
Link-local IPv6 Address ..... : fe80::58c5:45f2:7e5e:29c2%11(Preferred)
IPv4 Address............: 192.168.1.147(Preferred)
Subnet Mask ............: 255.255.255.0
Lease Obtained..........: Friday, September 6, 2019 11:08:36 AM
Lease Expires ..........: Saturday, September 7, 2019 11:08:36 AM
Default Gateway .........: 192.168.1.1
DHCP Server ............: 192.168.1.1
<output omitted>
```

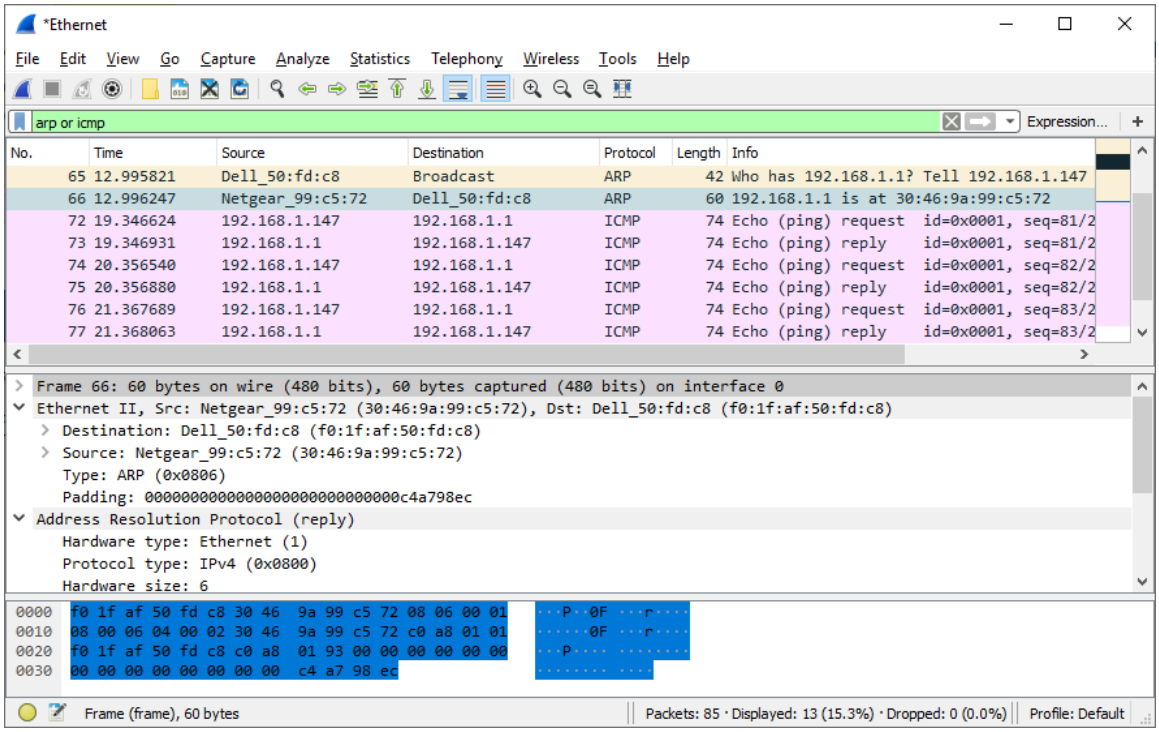
Krok 3: Zbadaj ramki Ethernetowe w danych przechwyconych w Wireshark.

Zrzuty ekranowe z przechwytywania Wireshark poniżej pokazują pakiety generowane przez ping wysyłany z hosta PC do jego domyślnej bramy. W programie Wireshark zastosowano filtr, aby wyświetlić tylko protokoły ARP oraz ICMP.ARP oznacza protokół odwzorowania adresów. ARP jest protokołem komunikacyjnym, który jest używany do określania adresu MAC skojarzonego z adresem IP. Sesja rozpoczyna się zapytaniem ARP i odpowiedzią na adres MAC routera bramy, a następnie czterema żądaniami ping i odpowiedziami.

Ten zrzut ekranu podświetla szczegóły ramki dla żądania ARP.



Ten zrzut ekranu podświetla szczegóły ramki dla odpowiedzi ARP.



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.

Pole	Wartość	Opis
Preambuła	Pominięte	To pole zawiera bity synchronizujące używane przez kartę sieciową.
Adres docelowy Adres źródłowy	Broadcast (ff:ff:ff:ff:ff:ff) Netgear_99:c5:72 (30:46:9a:99:c5:72)	Adres warstwy drugiej w ramce. Każdy adres ma długość 48 bitów (6 bajtów), przedstawiony jest w postaci 12 cyfr szesnastkowych, `0-9, A-F` Powszechnie używany sposób zapisu to `12:34:56:78:9A:BC` Pierwsze sześć cyfr wskazuje producenta, ostatnie 6 cyfr to numer seryjny karty sieciowej. 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).
Typ ramki	0x0806	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. Są dwa popularne typy ramek: Wartość Opis `0x0800` Protokół IPv4 `0x0806` Protokół ARP
Dane	ARP	Zawiera enkaspulowane jednostki PDU wyższej warstwy. Pole danych ma rozmiar od 46 do 1500 bajtów.
FCS	Pominięte	Sekwencja kontrolna ramki (FCS) jest używana przez kartę sieciową do wykrywania błędów powstałych podczas transmisji. Jej wartość jest obliczana przez nadawcę na podstawie pól zawierających adresy, typ oraz dane. Pole to weryfikowane jest przez odbiorcę.

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 identyfikator dostawcy (OUI) źródłowej karty sieciowej w odpowiedzi ARP?

Która część adresu MAC to OUI?

Jaki jest numer seryjny źródłowej karty sieciowej?

Część 2: Użycie programu Wireshark, aby przechwycić i przeanalizować ramkę Ethernetową.

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 IP domyślnej bramy?

Krok 2: Rozpocznij przechwytywanie ruchu pojawiającego się na karcie twojego PC.

a. Otwórz Wireshark, aby rozpocząć przechwytywanie danych.

b. 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.

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 wcześniej wybrano prawidłowy interfejs do przechwytywania pakietów, Wireshark powinien wyświetlić informacje ICMP w okienku listy pakietów Wireshark.

a. W panelu Packet List (górna część) kliknij pierwszą ramkę na liście. Powinieneś widzieć **żądanie echa (ping)** poniżej nagłówka **Info**. Linia powinna być teraz podświetlona.

b. Zbadaj pierwszą linijkę w panelu Packet Details (środkowa sekcja).Linia ta określa długość ramki.

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?

Jaki jest adres MAC bramy domyślnej?

d. Możesz kliknąć znak większości (>) na początku drugiej linii w celu wyświetlenia większej ilości informacji o ramce Ethernet II.

Jaki typ ramki jest wyświetlany?

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**.

Co oznaczają ostatnie dwa wyróżnione oktety?

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.

Jakie urządzenie i adres MAC są wyświetlane jako adres docelowy?

Krok 7: Pakiety przechwytywania dla zdalnego hosta.

a. 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**.

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

c. Zatrzymaj przechwytywanie pakietów.

d. Zbadaj nowe dane w panelu Packet list.

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

Źródło:

Odbiorca:

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

Źródło:

Odbiorca:

Porównaj te adresy z adresami, które poznałeś w kroku 6.Jedynym adresem, który się zmienił jest docelowy adres IP. Dlaczego zmienił się docelowy adres IP, podczas gdy docelowy adres MAC pozostał ten sam?

Pytania do przemyślenia

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