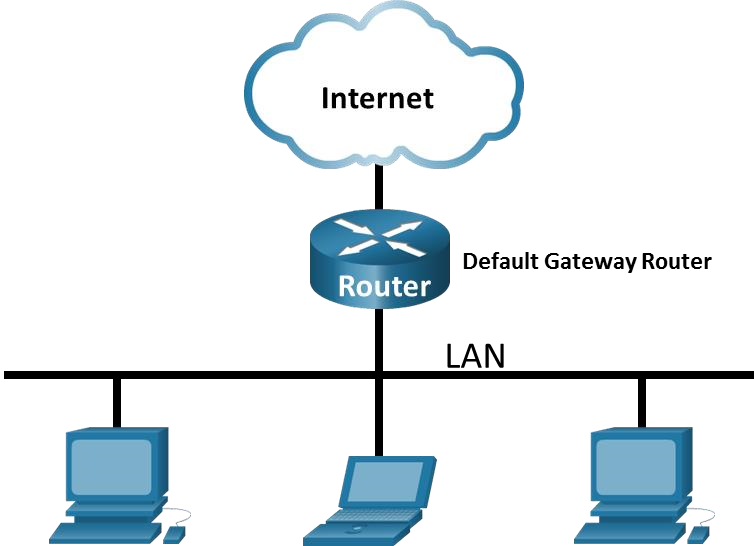


**Laboratorium - Wykorzystanie programu Wireshark do badania ruchu sieciowego**

# Topologia sieci



# Cele

**Część 1: Przechwytywanie i analiza lokalnych danych ICMP w Wireshark**

**Część 2: Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP.**

# Wprowadzenie

Wireshark jest programowym analizatorem protokołów sieciowych, czasem zwany bywa snifferem pakietów. Używany jest do analizy sieci, diagnozowania problemów, wspierania rozwoju różnego rodzaju oprogramowania i nowych protokołów. Jego głównym zastosowaniem jest również edukacja. W momencie gdy strumienie danych wędrują poprzez sieć, analizator przechwytuje i zapamiętuje każdą jednostkę PDU. Następnie dekoduje informacje w nich zawarte do postaci przejrzystej struktury odzwierciedlającej zalecenia RFC i umożliwiającej obserwatorowi bardzo wygodną ich analizę.

Wireshark jest bardzo użytecznym narzędziem dla każdego, kto w swej pracy ma do czynienia z sieciami komputerowymi. Może być z powodzeniem wykorzystywany w większości laboratoriów kursu CCNA w celu analizy przesyłanych danych oraz rozwiązywania napotkanych problemów. W tym laboratorium użyjesz programu Wireshark do przechwytywania danych ICMP w celu wyłuskiwania z nich adresów IP i adresów MAC.

# Wymagane zasoby

* 1 PC (Windows z dostępem do Internetu)
* Dodatkowy komputer PC w sieci lokalnej (LAN), którego zadaniem będzie odpowiadać na przychodzące żądania ping.

**Instrukcje**

# Część 1: Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP

W części 1 tego ćwiczenia będziesz wysyłać pakiety ping do innego komputera w sieci lokalnej i przechwycisz żądania i odpowiedzi ICMP w programie Wireshark. Zajrzysz również do przechwyconych ramek, aby uzyskać określone informacje. Analiza ta powinna przyczynić się do wyjaśnienia, w jaki sposób nagłówki pakietów są używane do transportu danych w miejsce przeznaczenia.

**Krok 1: Poznaj adresy interfejsu twojego PC.**

W tym laboratorium, musisz znać adres IP twojego komputera oraz fizyczny adres twojej karty sieciowej, nazywany adresem MAC.

*Otwórz wiersz polecenia systemu Windows.*

a. W oknie wiersza polecenia wpisz **ipconfig /all** aby zobaczyć adres IP interfejsu komputera, jego opis i adres MAC (fizyczny).

C:\Users\Student> **ipconfig /all**

Windows IP Configuration

Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC Primary Dns Suffix . . . . . . . :

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection

Physical Address. . . . . . . . . :00-26-B9-DD-00-91

DHCP Enabled. . . . . . . . . . . : No

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)

IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

<output omitted>

b. Poproś członka zespołu lub członków zespołu o adres IP ich komputera i podaj mu adres IP swojego komputera. Nie podawaj im swojego adresu MAC.

*Zamknij okno linii komend.*

**Krok 2: Uruchom Wireshark i zacznij przechwytywać dane.**

1. Przejdź do Wireshark. Kliknij dwukrotnie żądany interfejs, aby rozpocząć przechwytywanie pakietów. Upewnij się, że żądany interfejs ma ruch.
2. Informacje zaczną pojawiać się w górnej sekcji programu Wireshark. W zależności od typu protokołu, linie z danymi będą pojawiać się w różnych kolorach.

Ilość napływających danych może być bardzo duża i zależy od intensywności komunikacji między twoim PC a siecią LAN. Możemy nałożyć filtr, by ułatwić przeglądanie i pracę z danymi przechwytywanymi przez Wireshark. Dla celów tego laboratorium interesują nas tylko PDU typu ICMP (ping). By przeglądać tylko PDU typu ICMP (ping), w polu **Filter**, znajdującym się w górnej części programu Wireshark wpisz **icmp** i kliknij przycisk **Apply** lub naciśnij **Enter**.

1. Ten filtr spowoduje zniknięcie wszystkich danych w głównym oknie aplikacji, jednak nadal są one przechwytywane na interfejsie. Przejdź do okna wiersza polecenia i wykonaj ping adres IP otrzymany od członka zespołu.

C:\> **ping 192.168.1.114**

Pinging 192.168.1.114 with 32 bytes of data:

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

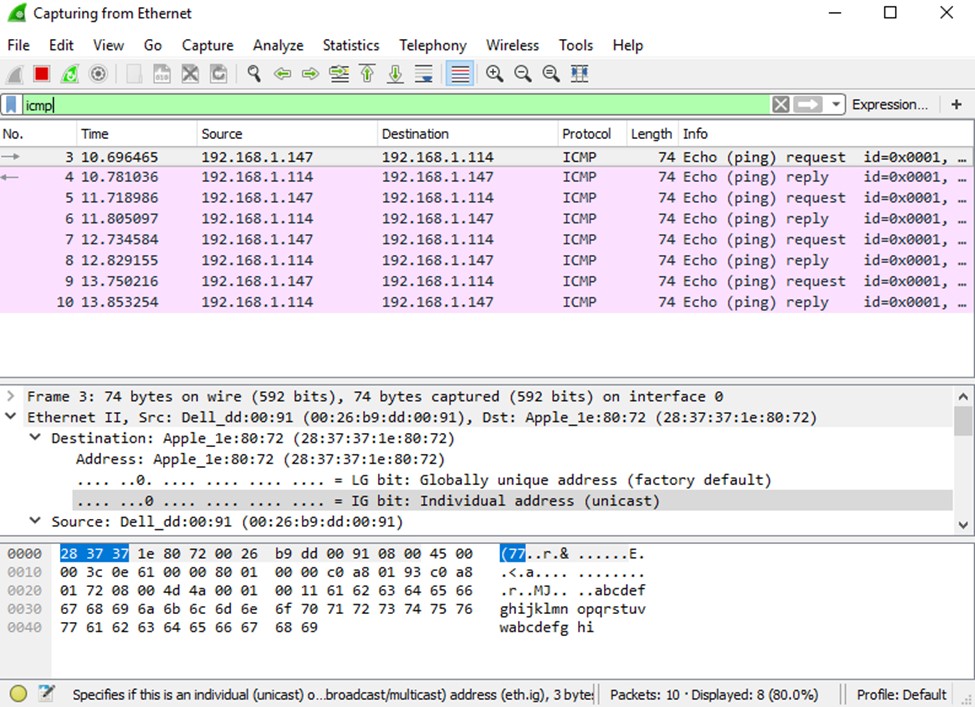
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Zauważ, że w głównym oknie programu Wireshark, ponownie pojawią się dane.



**Uwaga**: Jeśli komputer członka zespołu nie odpowiada na polecenia ping, może to wynikać z faktu, że zapora ogniowa komputera członka zespołu blokuje te żądania. Więcej informacji na temat przepuszczania ruchu ICMP przez zaporę w systemie Windows można znaleźć w Dodatek A: Umożliwienie ruchu ICMP przez zaporę ogniową.

d. Zatrzymaj proces przechwytywania danych klikając ikonę **Stop Capture**.

**Krok 3: Sprawdź przechwycone dane.**

W kroku 3 przeanalizuj dane, wygenerowane przez żądania ping, wysyłane do komputera twojego kolegi z zajęć. W programie Wireshark, dane te są wyświetlane w trzech sekcjach: 1) Górna sekcja wyświetla listę ramek PDU wraz z podsumowaniem informacji o danym pakiecie IP, 2) środkowa sekcja wyświetla informacje na temat ramki PDU zaznaczonej w górnej części ekranu oraz dzieli ją na bazie poszczególnych warstw protokołów, i 3) dolna sekcja wyświetla nieprzetworzone dane dla poszczególnej warstwy. Nieprzetworzone dane są wyświetlane w trybie szesnastkowym (heksadecymalnym) oraz dziesiętnym.

1. Kliknij na pierwsze żądanie ICMP z listy ramek PDU w górnej sekcji programu Wireshark. Zwróć uwagę, że w kolumnie **Source** zapisany jest adres IP twojego komputera, a w kolumnie **Destination** adres IP komputera kolegi z zajęć, na który wysyłałeś żądania ping.
2. Przejdź do środkowej sekcji programu, ramka PDU w sekcji górnej nadal musi być zaznaczona. Kliknij znak plusa znajdujący się po lewej stronie wiersza Ethernet II, by zobaczyć adresy MAC urządzenia źródłowego i docelowego.

Pytania:

Czy źródłowy adres MAC pasuje do interfejsu komputera?

***TAK***

Czy docelowy adres MAC w Wireshark odpowiada adresowi MAC członka zespołu?

***TAK***

W jaki sposób twój PC uzyskał MAC adres komputera PC, na który wysyłałeś żądania ping?

***Adres MAC uzyskuje soe poprzez żądanie ARP tutaj.***

**Uwaga**: W powyższym przykładzie ilustrującym przechwytywanie żądania ICMP, dane ICMP enkapsulowane są wewnątrz PDU pakietu IPv4 (nagłówek IPv4), który następnie enkapsulowany jest w PDU ramki Ethernet II (nagłówek Ethernet II) i przygotowany do transmisji w sieci LAN.

**Część 2: Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP.**

W części 2, wykonasz test ping do zdalnych komputerów (komputerów nie będących w sieci LAN) oraz zbadasz dane wygenerowane przez test ping. Następnie ustalisz, jaka jest różnica między tymi danymi, a danymi zbadanymi w Części 1.

**Krok 1: Rozpoczęcie przechwytywania danych z interfejsu.**

1. Rozpocznij przechwytywanie danych ponownie.
2. Przed rozpoczęciem nowego procesu przechwytywania, pojawi się okno informujące o możliwości zapisania wcześniej przechwyconych danych. Nie ma potrzeby ich zapisywać. Kliknij **Continue without Saving**.
3. Gdy przechwytywanie jest aktywne, pinguj następujące trzy adresy URL witryn z wiersza polecenia systemu Windows:

*Otwórz wiersz polecenia systemu Windows*

* 1. www.yahoo.com 74.6.143.25
  2. www.cisco.com 72.163.4.185
  3. www.google.com 142.250.203.206

**Uwaga**: Kiedy wykonujesz test ping kolejnych adresów URL, zwróć uwagę, że DNS tłumaczy URL na adres IP. Zanotuj adres IP dla każdego URL.

1. Zatrzymaj proces przechwytywania danych klikając ikonę **Stop Capture**.

**Krok 2: Badanie i analiza danych otrzymanych z hostów zdalnych.**

Przejrzyj przechwycone dane w programie Wireshark, sprawdź adresy IP i MAC trzech stron internetowych dla których wykonałeś polecenie ping. Poniżej wpisz, docelowy adres IP i MAC dla wszystkich trzech stron internetowych.

Pytania:

Adres IP **www.yahoo.com**: 74.6.143.25

Adres MAC dla **www.yahoo.com**: ec:bd:1d:c0:98:3f

Adres IP dla **www.cisco.com**: 72.163.4.185

Adres MAC dla **www.cisco.com**: ec:bd:1d:c0:98:3f

Adres IP **www.google.com**: 142.250.203.206

Adres MAC dla **www.google.com**: ec:bd:1d:c0:98:3f

***Wprowadź swoją odpowiedź tutaj.***

Co jest istotne w tej informacji?

Adresy MAC dla wszystkich trzech lokalizacji są takie same. ***tutaj.***

Czym różni się ta informacja od informacji uzyskanej w części 1, dotyczącej używania polecenia ping w sieci lokalnej?

Wykonując polecenie ping do komputera w sieci lokalnej, otrzymuję adres MAC jego karty sieciowej. Natomiast gdy pinguje urządzenie poza lokalną siecią, zwracany jest adres MAC interfejsu LAN domyślnej bramy.

*Zamknij okno linii komend.*

# Pytania do przemyślenia

Dlaczego Wireshark pokazuje aktualny adres MAC dla hostów lokalnych, ale już nie pokazuje aktualnego MAC dla hostów zdalnych?

W sieci lokalnej nie są dostępne adresy MAC urządzeń znajdujących się poza nią, dlatego pakiety są kierowane do domyślnej bramy, czyli routera. Gdy pakiet dotrze do tego routera, jego nagłówek warstwy 2 (adres MAC) zostaje usunięty, a na jego miejsce tworzony jest nowy nagłówek zawierający adres MAC kolejnego urządzenia w drodze do celu.

# Dodatek A: Umożliwienie ruchu ICMP przez zaporę ogniową

Jeżeli koledzy z zajęć nie otrzymują odpowiedzi z twojego PC na wysyłane żądania ping, prawdopodobnie zapora ogniowa blokuje te prośby. Niniejszy dodatek opisuje w jaki sposób stworzyć regułę w zaporze ogniowej, umożliwiającą przesyłanie żądań ping. Ponadto opisuje jak wyłączyć stworzoną regułę ICMP, gdy już ukończysz laboratorium.

**Część 1: Utworzenie nowej reguły przychodzącej, zezwalającej na ruch ICMP przez zaporę ogniową.**

1. Przejdź do **Panelu sterowania** i kliknij opcję **System i zabezpieczenia** w widoku kategorii.
2. W oknie **System i zabezpieczenia** kliknij **Zapora Windows Defender** lub **Zapora systemu Windows**.
3. W lewym okienku **Zapora Windows Defender** lub **Zapora systemu Windows** kliknij **Ustawienia zaawansowane**.
4. W lewym panelu okna **Ustawienia zaawansowane**, wybierz opcję **Reguły przychodzące**, a następnie w prawym panelu kliknij **Nowa reguła…**.
5. Spowoduje to uruchomienie Kreatora **nowej reguły ruchu przychodzącego**. Na ekranie **Typ reguły**, zaznacz opcję **Niestandardowa**, a następnie kliknij przycisk **Dalej**.
6. W lewym panelu, kliknij opcję **Protokół i porty** i przy użyciu **Typ protokołu** rozwijanego menu, wybierz **ICMPv4**, a następnie kliknij **Dalej**.
7. Sprawdź, czy wybrano **dowolny adres IP** zarówno dla lokalnych, jak i zdalnych adresów IP. Kliknij **Dalej** aby kontynuować.
8. Wybierz opcję **Zezwalaj na połączenie**. Kliknij **Dalej** aby kontynuować.
9. Domyślnie ta reguła ma zastosowanie do wszystkich profili. Kliknij **Dalej** aby kontynuować.
10. Nazwij regułę z **Zezwalaj na żądania ICMP**. Kliknij przycisk **Zakończ** , aby kontynuować. Ta nowa reguła powinna umożliwić twoim kolegom z zajęć otrzymanie odpowiedzi ping z twojego PC.

**Część 2: Wyłączenie lub usunięcie nowej reguły ICMP.**

Po zakończeniu laboratorium możesz chcieć wyłączyć lub nawet usunąć, regułę którą stworzyłeś w kroku 1. Użycie opcji **Wyłącz regułę** umożliwi ci jej ponowne włączenie w późniejszym czasie. Skasowanie reguły, permanentnie usuwa ją z listy Reguły przychodzące.

1. W lewym panelu okna **Ustawienia zaawansowane**, kliknij **Reguły przychodzące**, a następnie znajdź regułę, którą utworzyłeś wcześniej.
2. Kliknij prawym przyciskiem myszy regułę ICMP i wybierz **Wyłącz regułę** , jeśli chcesz. Możesz także wybrać opcję **Usuń** , jeśli chcesz ją trwale usunąć. Jeśli wybierzesz tę opcję, będziesz musiał ponownie utworzyć regułę by umożliwić wysyłanie odpowiedzi ICMP

*Koniec dokumentu*