Sprawozdanie nr 7

Sieci Komputerowe

Temat: Analiza działania polecenia **ping** za pomocą aplikacji Wireshark.

Informatyka (niestacjonarnie) - Semestr IV

Kacper Stanowicki

Wireshark to aplikacja służąca do analizy pakietów sieciowych, która pozwala na przechwytywanie i analizowanie ruchu sieciowego. Może ona analizować wiele protokołów sieciowych, takich jak TCP, UDP, HTTP, DNS, DHCP, FTP, SMTP i wiele innych. Może być wykorzystywany do różnych celów, w tym do diagnostyki problemów sieciowych, analizy wydajności sieciowej, wykrywania ataków sieciowych oraz do testowania bezpieczeństwa sieci.

Wynik zapytania **ping Helios.et.pu.poznan.pl**:

- w wierszu poleceń:

```
C:\Users\Stan>ping helios.et.put.poznan.pl

Pinging helios.et.put.poznan.pl [150.254.11.6] with 32 bytes of data:
Reply from 150.254.6.58: Destination host unreachable.
Reply from 150.254.6.58: Destination host unreachable.
Reply from 150.254.6.58: Destination host unreachable.
Reply from 150.254.6.58: Destination host unreachable.

Ping statistics for 150.254.11.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- w aplikacji Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
198	53.932672	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (no response found!)
207	57.117336	150.254.6.58	10.202.14.156	ICMP	102	Destination unreachable (Host unreachable)
208	57.126550	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (no response found!)
212	60.227049	150.254.6.58	10.202.14.156	ICMP	102	Destination unreachable (Host unreachable)
213	60.236083	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (no response found!)
216	63.346032	150.254.6.58	10.202.14.156	ICMP	102	Destination unreachable (Host unreachable)
217	63.354914	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (no response found!)
224	66.466971	150.254.6.58	10.202.14.156	ICMP	102	Destination unreachable (Host unreachable)

a) Ile wiadomości i jakiego typu wysłał komputer?

Komputer wysłał wiadomość typu ICMP (Internet Control Message Protocol) Echo Request (żądanie Echa) do wskazanego hosta. Zostały wysłane 4 pakiety.

b) Ile wiadomości i jakiego typu komputer otrzymał?

Komputer otrzymał 4 wiadomości typu ICMP.

c) Określić adres IP oraz MAC źródła i odbiorcy przechwyconych wiadomości ICMP.

Źródło:

- IP: 10.202.14.156
- MAC: fc:f8:ae:77:3f:da

Odbiorca:

- IP: 150.254.11.6
- MAC: 88:e0:f3:c0:87:f0

d) Jakie są różnice między adresem MAC a IPv4?

- Długość adresu: Adres MAC składa się z 6 bajtów (48 bitów), natomiast adres IPv4 składa się z 4 bajtów (32 bitów).
- Zakres adresów: Adres MAC jest unikalny w obrębie jednej sieci LAN (Local Area Network), a adresy IPv4 są unikalne globalnie. Adresy IPv4 mogą być używane do identyfikowania urządzeń w różnych sieciach komputerowych na całym świecie.
- Struktura adresu: Adres MAC składa się z dwóch części: identyfikatora producenta karty sieciowej (OUI) oraz unikalnego identyfikatora karty sieciowej. Adres IPv4 składa się z dwóch części: identyfikatora sieci oraz identyfikatora hosta.
- Przypisanie adresu: Adres MAC jest przypisywany przez producenta karty sieciowej, a adresy IPv4 są przypisywane przez administratora sieci.
- Format zapisu: Adres MAC jest zapisywany w postaci szesnastkowej z dwukropkami lub bez nich (np. 00:11:22:33:44:55), a adres IPv4 jest zapisywany w postaci dziesiętnej z kropkami (np. 192.168.1.1).
- Funkcja adresu: Adres MAC służy do identyfikacji karty sieciowej w sieci lokalnej, natomiast adresy IPv4 służą do identyfikacji urządzenia w sieci komputerowej i umożliwiają jego komunikację z innymi urządzeniami w sieci.

e) Określić wartość parametru TTL?

Wartość parametru TTL wynosi 128.

f) Co to jest TTL i dlaczego jest ustawiany w pakietach IP?

TTL (Time To Live) to parametr określający maksymalny czas życia pakietów. TTL definiuje jak długo wysłany pakiet danych może krążyć w sieci przechodząc od jednego routera do drugiego. Po przejściu przez każdy sieciowy węzeł, wartość TTL zmniejszana jest o 1, i kiedy pakiet osiągnie w końcu wartość 0, jest po prostu kasowany przez ostatni router. Procedura taka stosowana jest po to, aby pakiety, których adres przeznaczenia jest nieprawdziwy lub nieosiągalny, nie błąkały się bez końca w Sieci i nie generowały niepotrzebnego ruchu.

g) Czy pole o podobnym znaczeniu znajduje się w ramce ethernetowej?

Tak w ramce ethernetowej podobną rolę pełni kod kontrolny ramki. Jest pole zawierające sumę kontrolną ramki, służącą do wykrywania ewentualnych błędów ramki. Urządzenie wysyłające dane oblicza sumę kontrolną i umieszcza ją w ramce, odbiorca danych, po jej otrzymaniu również taką sumę oblicza, jeśli obydwie sumy się zgadzają ramka jest akceptowana, jeśli się różnią, ramkę traktuje się jako uszkodzoną i odrzuca.

h) Co się stanie jeżeli polecenie ping zostanie użyte z przełącznikiem -i 2?

Wynik zapytania **ping Helios.et.pu.poznan.pl -i 2**:

- w wierszu poleceń:

```
C:\Users\Stan>ping helios.et.put.poznan.pl -i 2

Pinging helios.et.put.poznan.pl [150.254.11.6] with 32 bytes of data:
Reply from 10.1.5.1: TTL expired in transit.
Reply from 10.1.5.1: TTL expired in transit.
Reply from 10.1.5.1: TTL expired in transit.
Reply from 10.1.5.1: TTL expired in transit.

Ping statistics for 150.254.11.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- w aplikacji Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
452	74.659998	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=2 (no response found!)
453	74.667143	10.1.5.1	10.202.14.156	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
457	75.669679	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=2 (no response found!)
458	75.674967	10.1.5.1	10.202.14.156	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
467	76.686123	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=2 (no response found!)
468	76.691722	10.1.5.1	10.202.14.156	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
474	77.702931	10.202.14.156	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=2 (no response found!)
475	77.707886	10.1.5.1	10.202.14.156	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Dodatkowa opcja „-i” określa czas między wysłaniem kolejnych pakietów ping w sekundach. Jeśli wywołamy polecenie z dodatkową opcją „-i 2”, oznacza to, że pakiety ping będą wysyłane co 2 sekundy.

i) Narysuj graf przepływu.