Wireshark

Analiza działania polecenia ping za pomocą aplikacji Wireshark.

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.

Po użyciu komendy ping helios.et.put.poznan.pl otrzymano powyższe wartości:

a. Komputer wysłał 4 wiadomości typu echo ping request
b. Komputer otrzymał 10 wiadomości typu 3 destination unreachable
c. Źródła IP: 192.168.13.114 MAC:e8:d8:d1:3a:a3:c5
    i. CeluIP: 150.254.11.6 MAC: e8:d8:d1:3a:a3:c5
d. Między IPv4 i MAC występują następujące różnice
    i. IPv4 jest zapisywane dziesiętnie i składa się z czterech oktetów od 0 do 255 i oddzielają je kropki natomiast MAC ma 6 bajtów zapisanych w formacie szesnastkowym i rozdzielone dwukropkiem
    ii. Adresy MAC są unikatowe na całym świecie natomiast IPv4 są przypisywane dynamicznie przez serwer DHCP i podlegają zmianie
    iii. IPv4 służą do identyfikacji w sieci internetowej, natomiast MAC w sieci lokalnej do identyfikowania urządzeń w tejrze sieci
e. TTL poszczególnych pakietów różni sie od siebie, poszczególne pakiety mają
    i. TTL :64 dla pakietów ze 192.168.13.1 do 192.168.13.114
    ii. TTL: 128 dla pakietów ze 192.168.13.114 dohelios.et.put.poznan.pl 150.254.11.6
    iii. TTL: 54 dla pakietów ze PUTNET-X450A-A3-2.put.poznan.pl (150.254.6.58) do 192.168.13.114
f. TTL (time to live) to wartość określająca maksymalną liczbę przeskoków (hopów) jakie może wykonać pakiet zanim zostanie odrzucony, każdy ruter przez który przechodzi pakiet zmniejsza wartość TTL o jeden. Gdy wartosc ta osiągnie zero, pakiet zostaje odrzucony a nadawca dostaje powiadomienie o błedzie. Wartości TTL mogą być ustawiane przez administratora (zwyczajowe wartości domyślne wynoszą 64 lub 128)
g. W ramce ethernet występuje ta sama wartość TTL
h. Wartość błędu zmienila się na TTL Expired in Transit oznacza to, pakiet osiągnął maksymalną liczbę przeskoków określoną w nagłówku TTL.

i. Graf przepływu: