Rodzaje testów i pomiarów pasywnych

Adam Banasiak

12.06.2014

POWIATOWY ZESPÓŁ SZKÓŁ NR 2
IM. PIOTRA WŁOSTOWICA W TRZEBNICY

ZAGADNIENIA

- Na czym polegają pomiary pasywne sieci?
- Jak przy pomocy sniffera przechwycić dane przesyłane w sieci?
- W jaki sposób analizować dane przechwycone przez sniffer?

- Podczas wykonywania testów pasywnych administrator tylko obserwuje funkcjonowanie sieci.
- W wielu sytuacjach jest to wystarczające do zebrania informacji o sposobie działania sieci.
- Dużo informacji dotyczących funkcjonowania sieci, administrator może uzyskać, monitorując ruch pakietów pomiędzy urządzeniami.
- Zawartości nagłówków jednostek danych umożliwiają dokładną analizę ruchu i jego zawartości. Programy wykorzystywane do tego celu nazywane są snifferami.

Sniffer

Sniffer to program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci.

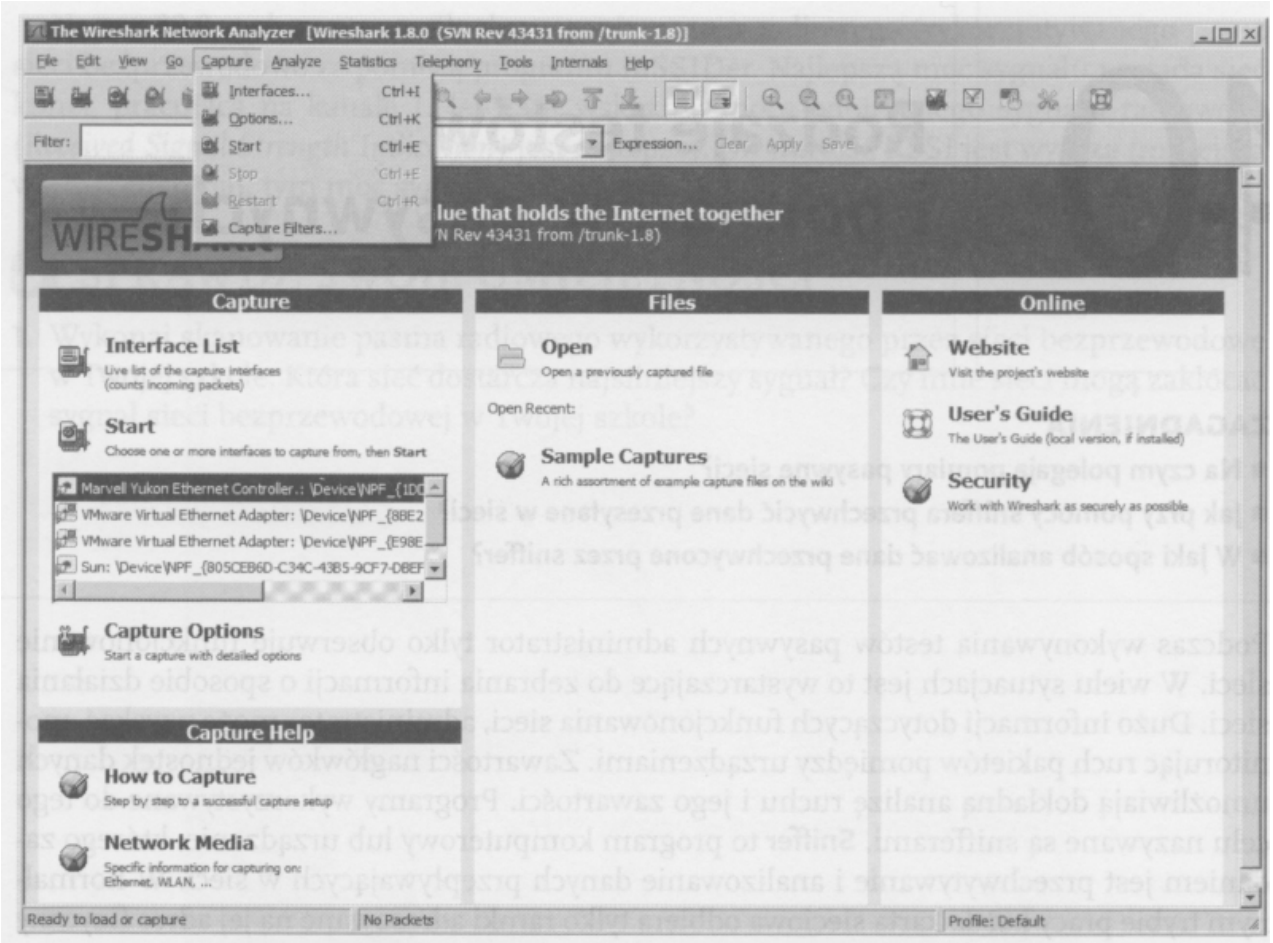
- W normalnym trybie pracy każda karta sieciowa odbiera tylko ramki adresowane na jej adres fizyczny MAC oraz ramki rozgłoszeniowe.
- Sniffer przełącza kartę sieciową w tryb mieszany (promiscuous), w którym urządzenie odbiera wszystkie ramki z segmentu sieci.
- Sniffery wykorzystywane są do analizowania ruchu w sieci przez administratorów, jak i hakerów. Z tego powodu podczas pracy w sieci nie wolno bez powodu uruchamiać tego typu programów.
- Administrator sieci po wykryciu uruchomionego sniffera na komputerze może potraktować użytkownika jako potencjalnego intruza i odłączyć jego komputer od sieci.

Wireshark

Bardzo popularnym snifferem jest program Wireshark. Dostępny jest w wersji na platformę Windows, Linux i MacOS X. Program można bezpłatnie pobrać ze strony http://www.wireshark.org/download.html. Program pracuje w środowisku graficznym, ale w środowisku Windows wymaga zainstalowanej biblioteki WinPcap (najnowsze wersje dostarczane są razem z biblioteką).

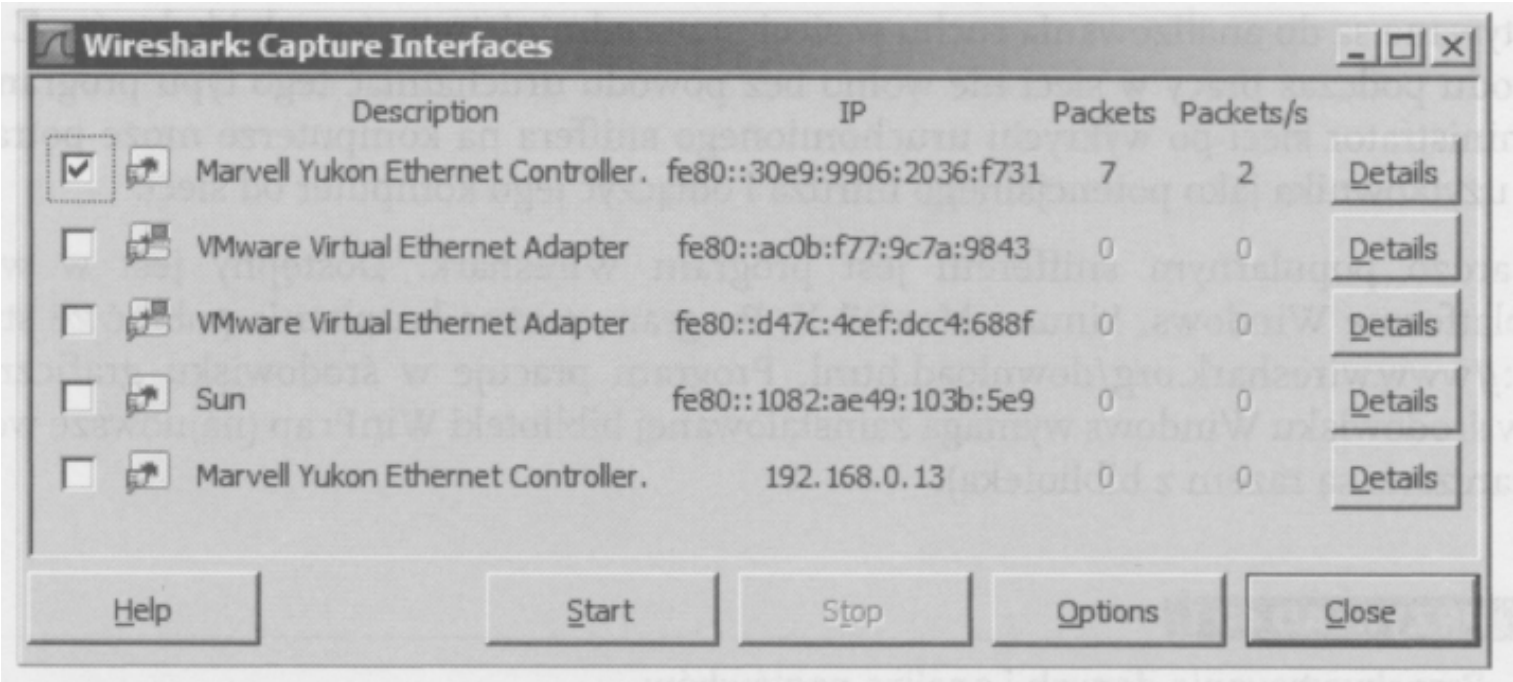
Przechwytywanie danych i analiza nagłówków. Aby przechwycić dane przesyłane w sieci i przeanalizować nagłówki, należy:

1. Uruchomić program Wireshark.
2. Wybrać z paska narzędzi polecenie Capture, a następnie Interfaces



Rysunek: Włączenie przechwytywania danych

3. W oknie wyboru interfejsu wskazać, który interfejs ma być ustawiony w trybie przechwytywania danych, i kliknąć przycisk Start.

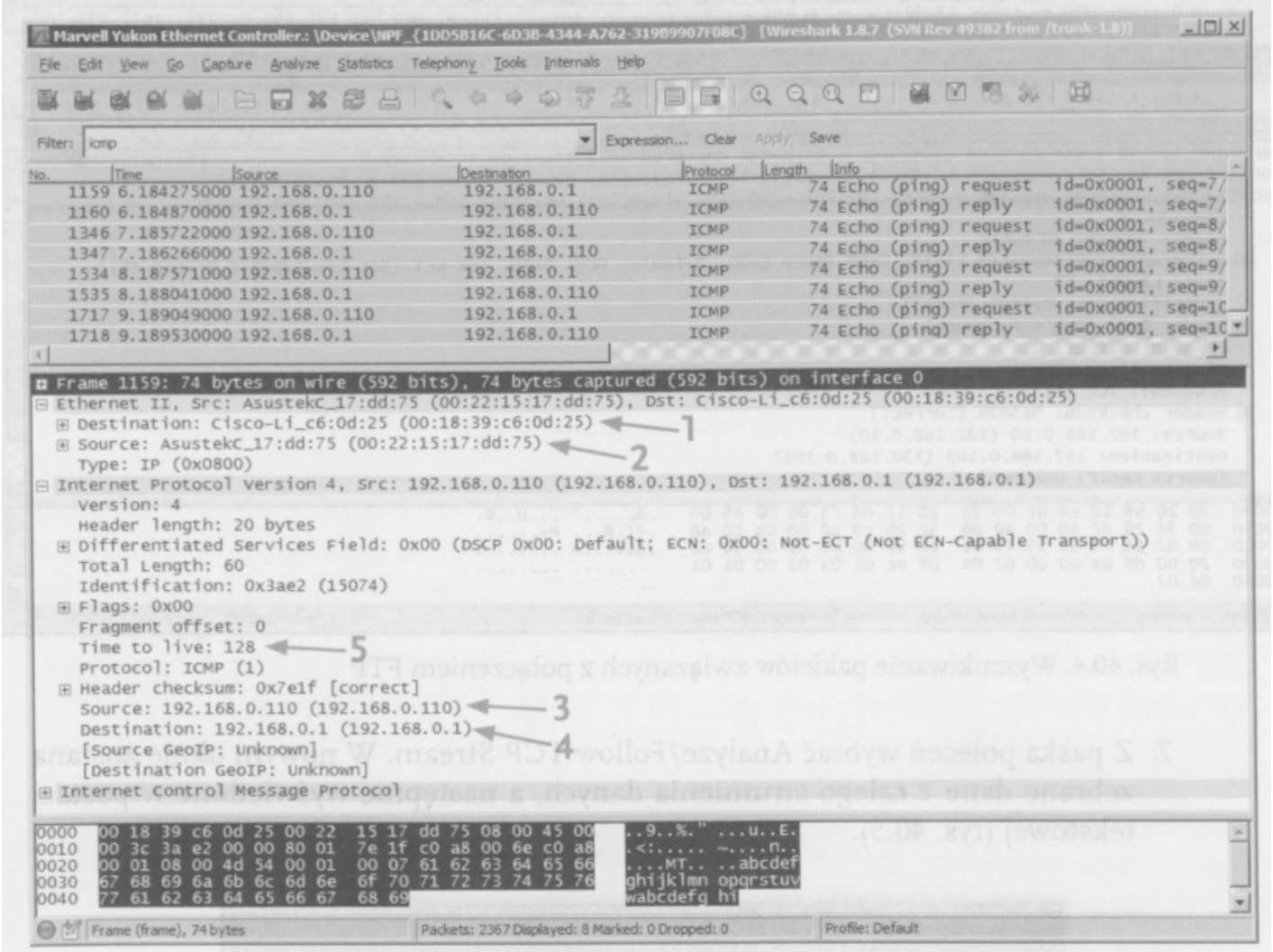


Rysunek: Okno wyboru interfejsu do przechwytywania danych

4. Uruchomić dowolny program generujący przepływ danych w sieci, np. polecenie ping, albo zaczekać na pojawienie się ruchu w sieci.

5. Obserwować w oknie głównym programu przychwytywane dane. Po zebraniu wymaganej ilości danych zatrzymać przechwytywanie poleceniem Capture/Stop. W oknie rozwinąć gałęzie Ethernet II i Internet Protocol Version 4. Na rysunku strzałkami zaznaczone są ważne informacje uzyskane z analizy nagłówków:
   - adres docelowy MAC - strzałka 1,
   - adres źródłowy MAC - strzałka 2,
   - adres źródłowy IP - strzałka 3,
   - adres docelowy IP - strzałka 4,
   - parametr TTL - strzałka 5.

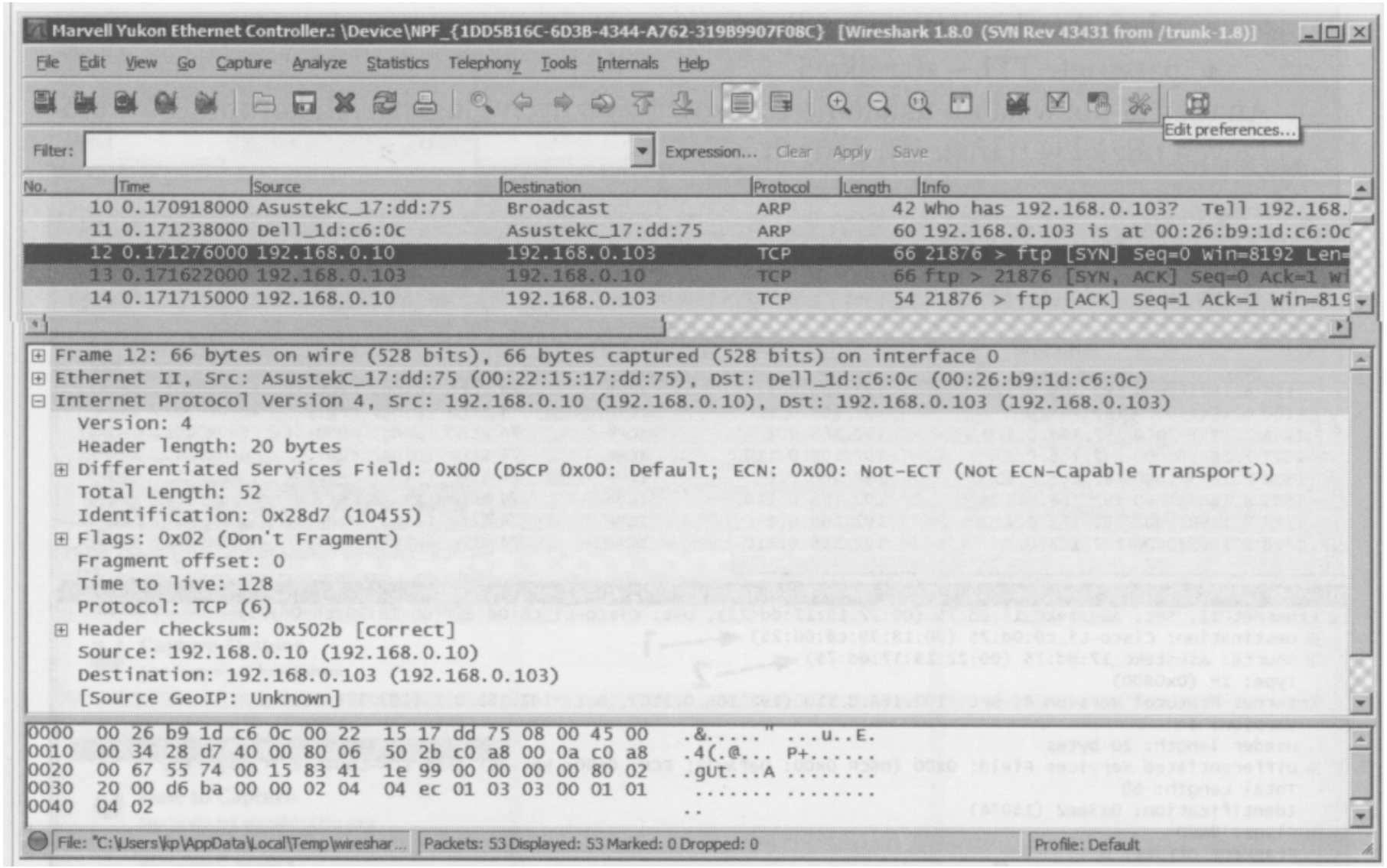
   Analiza ta pozwala na ustalenie adresów fizycznych i logicznych komputerów biorących udział w transmisji danych.



Rysunek: Analiza nagłówków przechwyconych danych

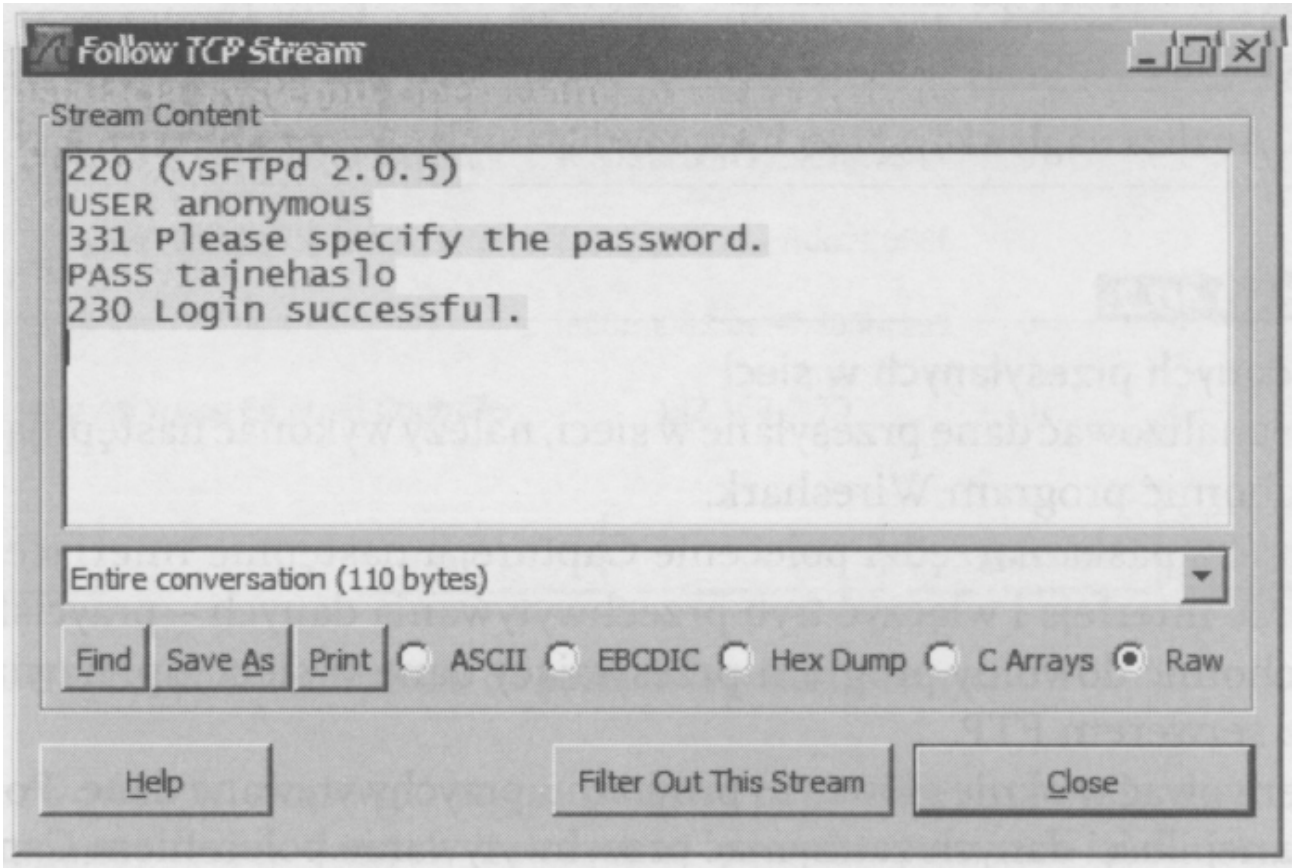
Analiza danych przesyłanych w sieci

1. Uruchomić program Wireshark
2. Wybrać z paska narzędzi polecenie Capture, a następnie Interfaces.
3. Wybrać interfejs i włączyć tryb przechwytywania danych - przycisk Start.
4. Uruchomić dowolny program przesyłający dane w sieci, np. nawiązać połączenie z serwerem FTP.
5. Obserwować w oknie głównym programu przychwytywane dane. Po zebraniu wymaganej ilości danych zatrzymać przechwytywanie poleceniem Capture/Stop.
6. Odszukać w oknie dowolny fragment transmisji związanej z nawiązywaniem połączenia FTP. Na następnym rysunku pakiety o numerach 10 i 11 związane są z zapytaniem odpowiedzią protokołu ARP. W pakiecie 12 rozpoczyna się proces nawiązywania sesji między klientem a serwerem FTP (jest to jeden z pakietów związanych z transmisją) - można kliknąć ten pakiet lub inny należący do tej samej sesji.



Rysunek: Wyszukiwanie pakietów związanych z połączeniem FTP

7. Z paska poleceń wybrać Analyze/Follow TCP Stream. W nowym oknie zostaną zebrane dane z całego strumienia danych, a następnie wyświetlone w postaci tekstowej.



Rysunek: Przesyłane dane wyświetlone w postaci tekstowej

Uwaga: Jeżeli dane były wysyłane bez stosowania szyfrowania, to zostaną wyświetlone łącznie z nazwami użytkowników i hasłami, jak na rysunku.

Przechwyć i przeanalizuj przebieg transmisji danych związanych z uzyskiwaniem adresu za pomocą protokołu DHCP. W transmisji zlokalizuj:

- adres MAC i IP klienta przed i po uzyskaniu adresu,
- komunikaty: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.

Uwaga:
Sniffer należy uruchomić na serwerze DHCP lub pobrać dane dla klienta w maszynie witrualnej.

Rodzaje testów i pomiarów aktywnych

Adam Banasiak

12.06.2014

POWIATOWY ZESPÓŁ SZKÓŁ NR 2
IM. PIOTRA WŁOSTOWICA W TRZEBNICY

- Jak przeprowadzać pomiary aktywne w sieci?
- Jak zmierzyć jakość usług sieciowych?
- Kto ustanawia standardy dotyczące jakości usług sieciowych?
- Jakie parametry służą do oceny jakości usług sieciowych?
- Jak wykorzystać programy ping i traceroute do pomiarów sieci?

Podczas wykonywania testów aktywnych administrator wprowadza do sieci dodatkowe dane, które ułatwiają wykonywanie pomiarów lub diagnozowanie sieci. Testy te mogą być wykonywane podczas normalnej eksploatacji sieci. Umożliwiają uzyskanie wiedzy o stanie sieci, jak również o zjawiskach w niej zachodzących. Metody aktywne uwzględniają podczas pomiarów obciążenie sieci ruchem generowanym przez aplikacje użytkowników, jak i samą sieć (np. protokoły routingu, DHCP, DNS).

Pomiary aktywne pozwalają na określenie jakości usług sieciowych (Quality of Service - QoS). QoS określa poziom gwarantowanych wartości parametrów sieciowych w celu osiągnięcia satysfakcji użytkownika. Użytkownicy w różny sposób oceniają jakość usług poprzez takie parametry, jak:

- przepustowość sieci,
- opóźnienie przesyłania danych,
- różnice opóźnienia poszczególnych pakietów,
- straty pakietów danych.

W celu zapewnienia porównywalności wyników, pomiary aktywne wykonywane są na podstawie metryki zdefiniowanej przez organizacje standaryzacyjne, np. ITU-T lub IETF. Przykładowo organizacja IETF zdefiniowała metryki:

Dostępność usługi

możliwość przekazu pakietów między danym źródłem a urządzeniem docelowym. Urządzenie docelowe uznawane jest za dostępne, jeśli pakiet dotrze w określonym czasie.

Opóźnienie w jednym kierunku OWD (One Way Delay)

czas przekazu pakietu między dwoma punktami w sieci. OWD jest mierzone jako czas od momentu, w którym źródło wysłało pierwszy bit pakietu, do momentu, w którym urządzenie docelowe odebrało ostatni bit pakietu. Wielkość pakietu pomiarowego ma wpływ na opóźnienie i musi być zdefiniowana przed pomiarem. Wartość metryki podawana jest w postaci parametrów statystycznych próbki:

- minimalne opóźnienie OWD (One Way Delay Minimum) - najmniejsza wartość opóźnienia w próbce
- średnie opóźnienie OWD (Mean One Way Delay) - średnia wartość opóźnienia w próbce
- percentyl opóźnienia OWD (One Way Delay Percentile) - x-ty percentyl opóźnienia danej próbki
- mediana opóźnienia OWD (One Way Delay Median) - wartość mediany danej próbki.

Zmienność opóźnienia przekazu pakietów IPDV (IP Packet Delay Variation)

różnica pomiędzy wartością OWD dla dwóch pakietów w mierzonej próbce pakietów (zwykle przyjmuje się różnicę opóźnienia sąsiednich pakietów).

Opóźnienie pakietów w pętli RTD (Round Trip Delay)

opóźnienie przekazu pakietu mierzone na drodze źródło -> przeznaczenie -> źródło. Wartość mierzona jako czas od wysłania pierwszego bitu pakietu do odebrania ostatniego bitu pakietu przez źródło.

Straty pakietów OWL (One Way Loss)

w przypadku poprawnego odebrania pakietu przyjmuje wartość 0, w przeciwnym wypadku -1.

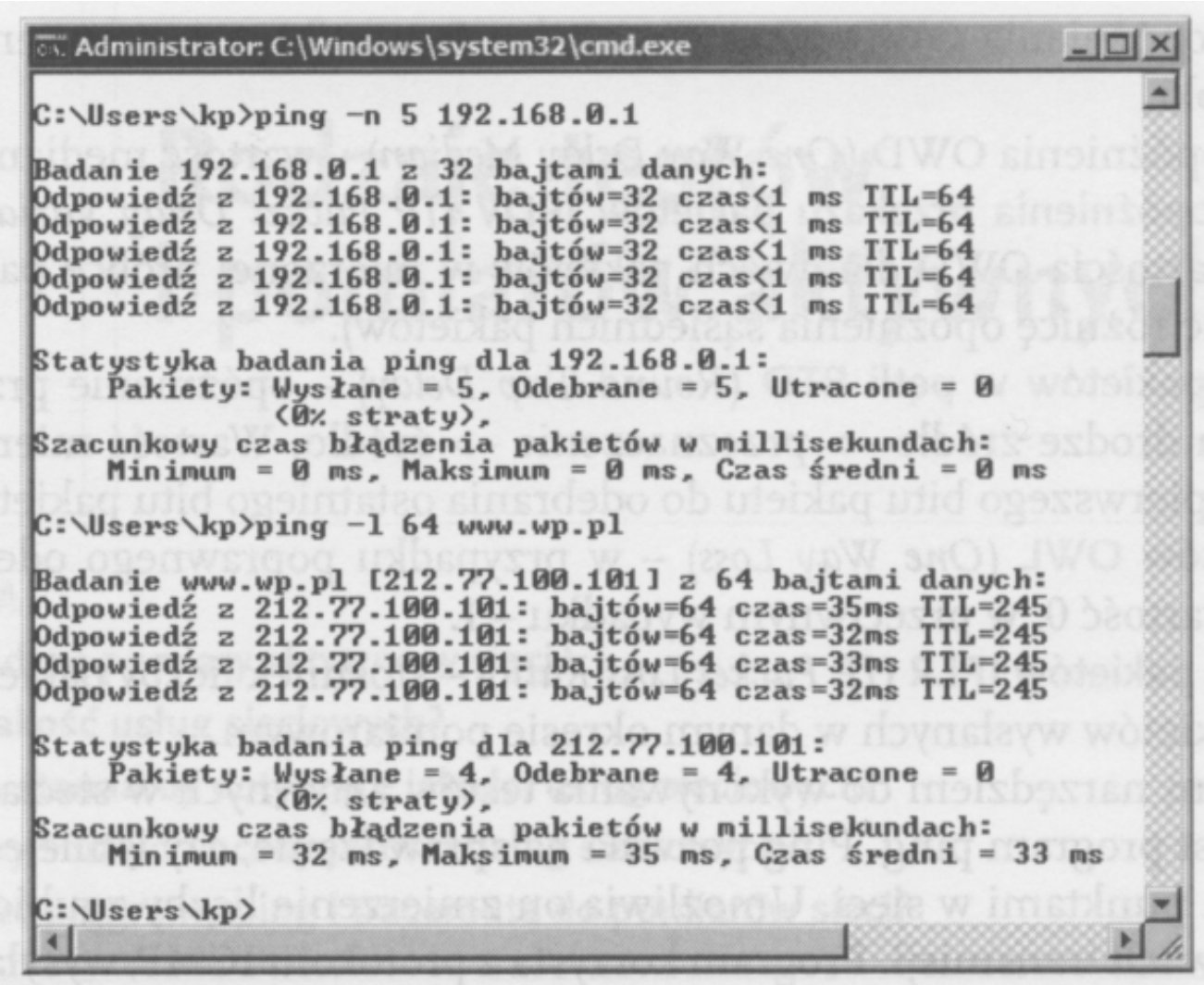
Poziom strat pakietów IPLR (IP Packet Loss Ratio)

stosunek liczby pakietów straconych do liczby pakietów wysłanych w danym okresie pomiarowym.

- Podstawowym narzędziem do wykonywania testów aktywnych w sieciach opartych na protokole IP jest program ping.
- Ping pozwala na sprawdzenie, czy istnieje połączenie pomiędzy dwoma punktami w sieci.
- Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji.
- Program korzysta z protokołu ICMP, wysyła pakiety ICMP Echo Request i odbiera ICMP Echo Reply.
- Aby wykonać test przy użyciu polecenia ping, należy w wierszu polecenia wpisać polecenie ping i adres IP lub nazwę domenową komputera, który ma zostać osiągnięty.
- Odpowiedź „Sieć docelowa jest nieosiągalna" oznacza, że nie istnieje trasa prowadząca do miejsca docelowego.
- Odpowiedź „Upłynął limit czasu żądania" oznacza, że w domyślnym czasie 1 sekundy nie nadeszła odpowiedź na polecenie ping.
- Informacje o dodatkowych opcjach programu można uzyskać poprzez wywołanie pomocy do programu (w systemie Windows ping /?). Przykładowe opcje programu ping:

- n liczba - określa liczbę pakietów testowych do wysłania. Wartością domyślną dla Windows jest 4, dla Linuksa pakiety są wysyłane do odwołania,
- l rozmiar - określa rozmiar pakietu testowego (domyślnie 32 bajty),
- t - wysyłanie ciągłe pakietów testowych (dotyczy systemu Windows).

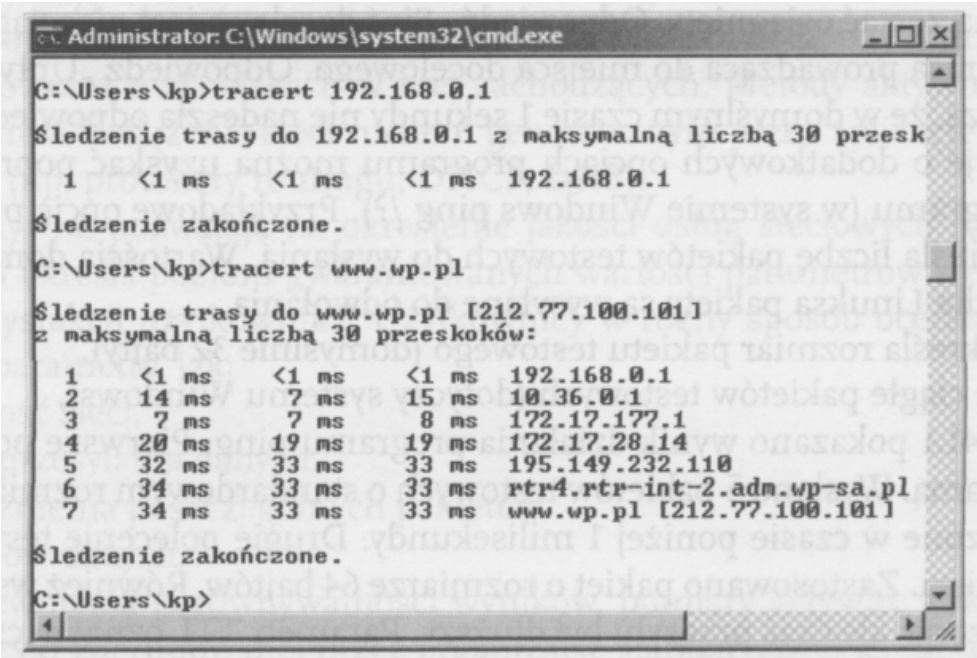
- Na następnym rysunku pokazano wynik działania programu ping. Pierwsze polecenie testuje połączenie z bramą. Wysłano 5 pakietów testowych o standardowym rozmiarze. Wszystkie zostały dostarczone w czasie poniżej 1 milisekundy.
- Drugie polecenie testuje połączenie z serwerem w sieci. Zastosowano pakiet o rozmiarze 64 bajtów. Również wszystkie pakiety zostały dostarczone, ale czas przesyłu był dłuższy.
- **Parametr TTL oznacza czas życia pakietu i pozwala na określenie liczby routerów na trasie.**



Rysunek: Wynik działania programu ping

- Do badania trasy, po której przesyłane są pakiety, i mierzenia czasu pomiędzy poszczególnymi routerami można wykorzystać program traceroute (w systemie Windows tracert).
- Działanie traceroute opiera się o protokole ICMP. Wysyłane są pakiety z polem TTL (Time To Live) ustawionym na kolejne wartości, zaczynając od 1. Wartość ta jest zmniejszana przez każdy router na trasie.
- Jeżeli pole TTL osiągnie wartość 0, to pakiet jest odrzucany, a router wysyła informację zwrotną do komputera źródłowego. W ten sposób komputer źródłowy uzyskuje kolejne adresy IP routerów na trasie.

- Na początku wysyłany jest pakiet z polem TTL ustawionym na 1, co pozwala na ustalenie adresu IP pierwszego routera na trasie. Następnie wysyłany jest pakiet z polem TTL 2. Pierwszy router zmniejszy tę wartość do 1 i przekaże do drugiego routera na trasie. Drugi router zmniejszy TTL do 0 i odrzuci pakiet, wysyłając komunikat do komputera źródłowego. Testowanie kończy się po osiągnięciu miejsca docelowego lub przekroczeniu dopuszczalnej liczby routerów (standardowo 30).
- Na rysunku pokazano wyniki działania programu tracert. W pierwszym poleceniu testowano trasę do bramy; trasa składała się tylko z 1 routera.



Rysunek: Wynik działania programu tracert

- Trasa do serwera w internecie była dłuższa i składała się z siedmiu routerów (ich adresy lub nazwy znajdują sie po prawej stronie rysunku).
- Na podstawie pomiaru administrator może określić łącza, w których występuje największe opóźnienie. Na działanie polecenia ping może mieć wpływ zapora sieciowa skonfigurowana na testowanym komputerze.
- Wiele zapór standardowo blokuje wysyłanie odpowiedzi na żądanie echa wysyłane przez program ping.