# Analiza ruchu w sieci. Programy tcpdump i ethereal

Programy wymienione w tytule należą do tzw. analizatorów sieciowych. Ich zadaniem jest przechwytywanie ramek przesyłanych w sieci, zapisywanie ich do bufora, a następnie analiza nagłówków poszczególnych warstw protokołów, jak również prezentacja danych przenoszonych w ramkach.

## tcpdump

Jest to program działający w trybie tekstowym, umożliwia on oglądanie i analizę nagłówków poszczególnych warstw modelu OSI w ramkach i pakietach przesyłanych w lokalnym segmencie sieci. Uruchamia się go poleceniem

tcpdump opcje filtr

gdzie opcjonalny filtr jest wyrażeniem określającym jakie pakiety mają być przechwytywane, a następnie prezentowane. W przeciwnym przypadku przechwytywane są wszystkie pakiety przesyłane w segmencie sieci, do którego podłączony jest interfejs. Oto znaczenie niektórych opcji:

– c liczba : program kończy działanie po przechwyceniu określonej liczby ramek

– i interfejs : program nasłuchuje na wskazanym interfejsie, domyślnie nasłuchiwanie prowadzone jest na aktywnym interfejsie o najniższym numerze

– n : zapobiega zamianie adresów IP na nazwy

– r plik : pobiera ramki z pliku (utworzonego uprzednio przy pomocy opcji –w), a nie interfejsu sieciowego

– w plik : zapisuje przechwycone ramki do pliku o podanej nazwie (ścieżce) , zamiast wyświetlać je na ekranie

Pozostałe opcje opisane są w podręczniku man (man tcpdump).

Wyrażenie filtrujące składa się z wyrażeń podstawowych połączonych operatorami logicznymi (zasady używania operatorów są opisane w dalszej części). Z kolei wyrażenie podstawowe jest to identyfikator (nazwa lub adres) poprzedzony co najmniej jednym kwalifikatorem. Istnieją trzy grupy kwalifikatorów: typ, kierunek, protokół

Typ: Sa trzy kwalifikatory typu: „host”, „net” i „port”. Pierwszy z nich oznacza, że identyfikator dotyczy hosta, drugi - sieci, a trzeci – portu. Brak kwalifikatora typu oznacza, że domyślnie identyfikowany jest host.

Kierunek: określa kierunek przesyłania ramki. Możliwe kwalifikatory to: src, dst, src or dst, src and dst. Brak kwalifikatora kierunku oznacza domyślnie „src or dst”.

Protokół: określa protokół. Możliwe kwalifikatory to: ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp, udp. Brak kwalifikatora oznacza wszystkie protokoły zgodne z podanym kwalifikatorem typu, np src sz123 oznacza (ip or arp or rarp) src sz123, net 192.168.1 oznacza (ip or arp or rarp) net 192.168.1, port 53 oznacza (tcp or udp) port 53.

Przykłady wyrażeń podstawowych:

src host sz123 : wartością logiczną jest prawda, jeśli pole „źródłowy adres IP" zawiera adres IP maszyny sz123

dst host sz123 : prawda, jeśli pole „docelowy adres IP" zawiera adres IP maszyny sz123

host 192.168.10.1 : prawda, jeśli pole „źródłowy adres IP" lub „docelowy adres IP" zawiera adres 192.168.10.1

ether src u:v:w:x:y:z : prawda, jeśli pole „źródłowy adres MAC"
zawiera adres sprzętowy u:v:w:x:y:z

ether dst u:v:w:x:y:z : prawda, jeśli pole „docelowy adres MAC"
zawiera adres sprzętowy u:v:w:x:y:z

ether host u:v:w:x:y:z : prawda, jeśli pole „źródłowy adres MAC" lub „docelowy adres MAC" zawiera adres sprzętowy u:v:w:x:y:z

gateway sz123 : prawda, jeśli źródłowy lub docelowy MAC był adresem maszyny o nazwie sz123, ale ani źródłowy ani docelowy IP nie był adresem maszyny o nazwie sz123, innymi słowy maszyna sz123 przekazywała pakiet, ale nie była ani maszyną źródłową ani docelową..

net 192.168.10 : prawda, jeśli źródłowy lub docelowy adres IP ma część sieciowa 192.168.10. Może być poprzedzony kwalifikatorem „src" lub „dst".

net 10.0.1.0 mask 255.255.255.0 : prawda, jeśli po nałożeniu maski 255.255.255.0 na źródłowy lub docelowy adres IP otrzymamy 10.0.1.0. Może być poprzedzony kwalifikatorem „src" lub „dst".

net 128.1.0.0/16 : prawda, jeśli po nałożeniu maski 16-bitowej na źródłowy lub docelowy adres IP otrzymamy 128.1.0.0. Może być poprzedzony kwalifikatorem „src" lub „dst".

port 23 : prawda, jeśli pakiet jest typu ip/tcp, ip/udp, ipv6/tcp, ipv6/udp, a numer portu źródłowego lub docelowego tcp lub udp wynosi 23. Liczbę można zastąpić nazwą usługi z pliku /etc/services. Może być poprzedzony kwalifikatorem „src" lub „dst", jak również „tcp" lub „udp".

less 520 lub len <=520 : prawda, jeśli długość pakietu jest mniejsza lub równa 520

greater 520 lub len>=520 : prawda, jeśli długość pakietu jest większa lub równa 520

**Uwaga:** len jest bezargumentowym operatorem zwracającym długość pakietu w bajtach

ip proto <protokół> : prawda, jeśli ramka przenosi pakiet IP, a zawartość pola „Typ protokołu” (drugi bajt trzeciego 32-bitowego słowa nagłówka IP) odpowiada jednemu z następujących protokołów warstwy transportu: icmp, igmp, igrp, udp, tcp (pozostałe wymienione w opisie polecenia tcpdump). **Uwaga:** nazwy icmp, tcp i udp muszą być poprzedzone znakiem „\”, ponieważ są słowami kluczowymi w składni wyrażeń filtrujących.

ether proto <protokół> : prawda, jeśli ramka przenosi datagram Ethernet II, a zawartość pola ‘Typ protokołu” (trzynasty i czternasty bajt nagłówka Ethernet II) odpowiada jednemu z następujących protokołów warstwy sieci: ip, ip6, arp, rarp, atalk, ipx, netbeui (pozostałe wymienione w opisie polecenia tcpdump). **Uwaga 1:** nazwy protokołów muszą być poprzedzone znakiem „\”, ponieważ są słowami kluczowymi w składni wyrażeń filtrujących. **Uwaga 2:** kwalifikatory ip, ip6, arp, rarp, atalk, ipx, netbeui można stosować zamiast wyrażenia ether proto <protokół>, gdzie <protokół> jest jednym z wymienionych protokołów.

expr relop expr : prawda, jeśli zachodzi dana relacja, gdzie relop jest operatorem relacji, czyli jednym z symboli: < , > , <= , >= , = , != , natomiast expr jest wyrażeniem arytmetycznym zbudowanym ze stałych całkowitych, operatorów arytmetycznych + , - , * , / , operatorów bitowych & (iloczyn mod 2), | (suma mod 2), << (przesunięcie w lewo), >> (przesunięcie w prawo), operatora len, oraz wyrażenia udostępniającego poszczególne bajty pakietu. To ostatnie wyrażenie ma następującą postać:

protokół[numer początkowego bajta: liczba bajtów]

Liczba bajtów jest opcjonalna, może być równa 1, 2 lub 4, domyślna wartość to 1. Na przykład, ether[0] oznacza pierwszy bajt ramki Ethernet, ip[2:2] oznacza trzeci i czwarty bajt pakietu IP, czyli szesnastobitowe pole, w którym zapisana jest całkowita długość pakietu IP. (**Uwaga:** bajty są numerowane od zera). A oto przykłady wyrażeń relacyjnych:

„ether[0] & 1 != 0” oznacza ramki typu multicast (w warstwie łącza)

„ip[0] & 0xf != 5” – pakiety IP z niepustym polem opcji

„ip[6:2] & 0x1FFF = 0” – pakiety nie fragmentowane i pierwsze fragmenty (o numerze zero) pakietów fragmentowanych

Wyrażenia podstawowe mogą być łączone w formuły logiczne przy użyciu następujących operatorów: ! lub not – negacja, && lub and – koniunkcja, || lub or – alternatywa. Operator negacji ma wyższy priorytet od operatorów koniunkcji i alternatywy, których priorytet jest jednakowy. Wartość formuły obliczana jest od lewej do prawej strony. Wskazane jest używanie nawiasów dla uniknięcia błędów, oraz zwiększenia czytelności złozonych wyrażeń.

## Ethereal (WireShark)

Jest to program działający w trybie graficznym, umożliwiający przeglądanie i analizę nagłówków poszczególnych warstw modelu OSI, a także danych, w ramkach przesyłanych w lokalnym segmencie sieci. Aby go uruchomić, należy na pulpicie graficznym otworzyć okno konsoli, a następnie wydać polecenie ethereal.

Program ethereal umożliwia filtrowanie zarówno przechwytywanych jak i wyświetlanych ramek. Do tego celu służą opcje „Capture Filters" i „Display Filters" dostępne z menu rozwijanych po naciśnięciu przycisków „Capture" i „Analyze" znajdujących się w menu głównym. Aby zdefiniować nowy filtr przechwytywania, należy wybrać opcję „Capture Filters" i w oknie „Ethereal: Capture Filter" podać nazwę filtru, oraz wyrażenie filtrujące, konstruowane tak samo jak wyrażenie filtrujące polecenia tcpdump. Następnie należy nacisnąć przycisk „New", aby dodać filtr do listy wcześniej zdefiniowanych filtrów. Wciśnięcie przycisku „Save" powoduje zapisanie wyrażenia filtrującego w pliku, którego położenie należy określić (domyślnie plik zapisuje się w katalogu domowym). W starszych wersjach Fedory filtr zapisywał się do pliku ~/.ethereal/cfilters (~ oznacza katalog domowy użytkownika). Katalog ~/.ethereal tworzony był automatycznie z chwilą zapisania pierwszego filtru przyciskiem „Save".

Przykład 1: Analiza działania protokołu ARP

Przechwyć i przeanalizuj komunikaty protokołu ARP przesyłane w celu ustalenia adresu MAC maszyny z sieci lokalnej o podanym adresie IP. Powinny zostac przechwycone 2 komunikaty.

Wskazówka: zastosuj następujący filtr przechwytywania:

host <IP maszyny lokalnej> and host <IP maszyny docelowej> and arp

Następnie wydaj polecenie:

arping – c1 <IP maszyny docelowej>

**Uwaga:** wyrażenie „arp" jest skróconą formą wyrażenia „ether proto \arp". Należy zwrócić uwagę na znak „\" poprzedzający nazwę „arp".

Przykład 2: Analiza fragmentacji IP

Wyślij do maszyny w tej samej sieci lokalnej pakiet IP o całkowitej długości (nagłówek IP + pole danych) przekraczającej wartość MTU (1500 dla sieci Ethernet). Przeanalizuj zawartość kolejnych fragmentów, zwracając szczególną uwagę na zawartość pól „Identification", „Flags" i „Fragment Offset" występujących w drugim 32-bitowym słowie nagłówka IP.

Wskazówka: wydaj polecenie:

ping –s 5000 –c 1 <IP maszyny docelowej>

Do przechwytywania pakietów zastosuj następujący filtr:

icmp and src host <IP maszyny lokalnej>

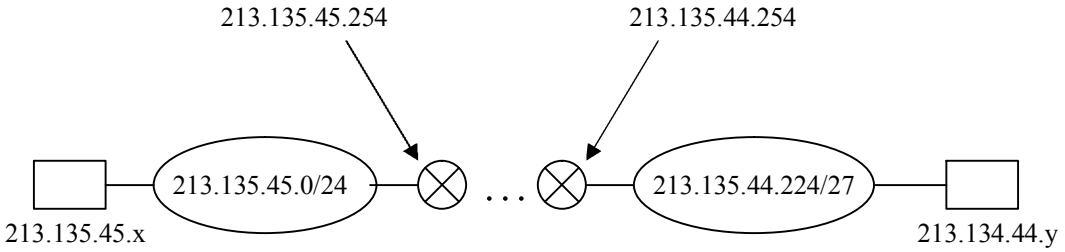
**Uwaga:** wyrażenie „icmp" jest skróconą formą wyrażenia „ip proto \icmp". Należy zwrócić uwagę na znak „\" poprzedzający nazwę „icmp".

Przykład 3: Analiza opcji zapisywania trasy

Na maszynie z sieci 213.135.45.0/24 wydaj nastepujące polecenie:

ping –R –c1 213.135.44.y

Przeanalizuj pakiety wysłane i odebrane w wyniku działania powyższego polecenia, w przypadku działania i nie działania komputera 213.135.44.y Konfiguracja środowiska sieciowego przedstawiona jest na poniższym rysunku.




Wskazówka: zastosuj następujący filtr przechwytywania:

icmp and host 213.135.45.x and host 213.135.44.y

gdzie x jest numerem komputera w sieci 213.135.45.0/24, a y – numerem komputera w sieci213.135.44.224/27.

Przykład 4: Analiza działania polecenia traceroute

Na maszynie z sieci 213.135.45.0/24 wydaj następujące polecenie:

traceroute –q1 213.135.44.y

Przeanalizuj pakiety wysłane i odebrane w wyniku działania powyższego polecenia, w przypadku działania i nie działania komputera 213.135.44.y

Wskazówka: zastosuj następujący filtr przechwytywania:

(udp and src host 213.135.45.x and dst host 213.135.44.y) or (icmp and dst host 213.135.45.x)