Tomasz MALINOWSKI[1]

REJESTROWANIE DANYCH O RUCHU SIECIOWYM W ŚRODOWISKU AKTYWNYCH URZĄDZEŃ SIECIOWYCH

Streszczenie

W artykule omówiony został mechanizm NetFlow, będący podstawą zbierania pełnych (kompletnych) statystyk dotyczących ruchu sieciowego na interfejsach urządzeń warstwy sieciowej (routery, przełączniki warstwy 3). Podany został również sposób rejestrowania danych o wybranych przepływach z wykorzystaniem list kontroli dostępu, aplikowanych na interfejsach warstwy sieciowej. Sposoby pozyskiwania danych o wielkości ruchu sieciowego dotyczą środowiska sieciowego z urządzeniami aktywnymi (przełącznikami i routerami) firmy Cisco Systems.

Abstract

In the article, the author discusses the NetFlow technology as an efficient method of gathering complete information about the network traffic on active network device interfaces. Cisco is still working on solutions for NetFlow-based billing, planning and monitoring. Another registering method of a number of chosen protocols packets, with a very simple implementation process based on access control lists, was also described and illustrated. In all presented examples, Cisco switches and routers were used.

1. WPROWADZENIE

Techniki rejestrowania danych niosących informację o obciążeniu segmentów sieci komputerowej (aktywności użytkowników sieci, aktywności aplikacji, aktywności urządzeń sieciowych wynikającej z uruchamiania na nich różnego rodzaju protokołów) i sposoby gromadzenia danych statystycznych wciąż są przedmiotem zainteresowania administratorów wielu sieci. Wyniki pomiaru ruchu sieciowego stanowią podstawę określenia newralgicznych, zbyt mocno obciążanych portów urządzeń, identyfikowania źródeł nadmiernego, a niezbyt pożądanego ruchu sieciowego, wyznaczania nowej konfiguracji urządzeń służącej np. równoważeniu obciążenia interfejsów urządzeń, czy zapewnianiu użytkownikom sieci odpowiedniego poziomu usług (*QoS*).

[1] Dr inż. Tomasz Malinowski pracuje w Warszawskiej Wyższej Szkole Informatyki, w Instytucie Teleinformatyki Wojskowej Akademii Technicznej i w Katedrze Sieci Komputerowych w Polsko-Japońskiej Wyższej Szkole Technik Komputerowych.

W niniejszym artykule przedstawione zostały alternatywne do metod wykorzystujących protokół SNMP sposoby rejestrowania danych o ruchu sieciowym w sieci zbudowanej z wykorzystaniem urządzeń firmy Cisco. Choć niniejszy artykuł nie jest poświęcony protokołowi SNMP, należy podkreślić, że protokół ten jest podstawą działania wielu komercyjnych analizatorów i aplikacji do zarządzania siecią i pozostaje nadal uznanym protokołem monitorowania sieci komputerowych. Najważniejszym dodatkiem do zbioru standardów objętych wspólną nazwą SNMP jest specyfikacja zdalnego monitorowania sieci RMON (*Remote Network Monitoring*). RMON zawiera definicję bazy MIB zdalnego nadzoru, która stanowi uzupełnienie bazy MIB-II i zawiera „liczniki" dla różnego typu ruchu z i do hostów dołączonych do danego segmentu sieci. Mechanizmy zdalnego monitorowania RMON implementowane są również w systemie IOS urządzeń Cisco. Jak w każdym przypadku, inżynierowie Cisco ostrzegają przed nieuzasadnionym uruchamianiem protokołu, szczególnie na niezbyt wydajnych urządzeniach, co zwykle przekłada się na spadek szybkości przełączania pakietów. Szczegółowe informacje nt. zasad wykorzystania protokołu SNMP dostępne są np. w [1, 2].

W artykule uwaga autora skupiona została na protokole NetFlow, zwykle odblokowywanym na interfejsach routerów brzegowych, eksportującym dane sumaryczne strumieni związanych z sesjami host-host i wskazanych interfejsów do tzw. NetFlow Collectora. Przedstawiona została także technika rejestrowania liczby pakietów związanych ze wszystkimi lub wskazanymi sesjami, bazująca na przesyłaniu do serwera *syslog* informacji o przypadkach naruszenia listy ACL (*Access Control List*).

2. WYKORZYSTANIE LIST KONTROLI DOSTĘPU DO REJESTROWANIA WYBRANYCH STATYSTYK RUCHU SIECIOWEGO

Poniżej zaprezentowane zostanie nietypowe zastosowanie list kontroli dostępu (aplikowanych na routerach Cisco) do selektywnego rejestrowania liczby pakietów przepływających przez wskazany interfejs. Wylistowany został fragment pliku konfiguracyjnego routera, z warunkami zawartymi w przykładowej liście o numerze 103.

```
access-list 103 permit icmp 10.3.50.0 0.0.0.255 any log-input
access-list 103 permit tcp 10.3.50.0 0.0.0.255 any eq ftp log-input
access-list 103 permit tcp 10.3.50.0 0.0.0.255 any eq telnet log-input
access-list 103 permit tcp 10.3.50.0 0.0.0.255 any eq domain log-input
access-list 103 permit tcp 10.3.50.0 0.0.0.255 any eq pop3 log-input
access-list 103 permit tcp 10.3.50.0 0.0.0.255 any eq www log-input
```

```
access-list 103 permit udp 10.3.50.0 0.0.0.255 any eq tftp log-input
access-list 103 permit udp 10.3.50.0 0.0.0.255 any eq rip log-input
access-list 103 permit udp 10.3.50.0 0.0.0.255 any eq domain log-input
access-list 103 permit udp 10.3.50.0 0.0.0.255 any eq netbios-ss log-input
access-list 103 permit ip any any
```

Warto zauważyć, że lista jest tzw. listą rozszerzoną, z określonymi adresami IP źródła i miejsca przeznaczenia oraz nazwami wykorzystywanych aplikacji. Jak widać lista zawiera jedynie warunki z akcją typu *permit,* co oznacza, że wszystkie pakiety sprawdzane pod kątem spełnienia warunków, niezależnie od wyniku sprawdzenia, będą przez router przepuszczane.

Cechą charakterystyczną list dostępu w implementacji Cisco jest dowiązanie do każdego warunku licznika zliczającego pakiety spełniające ten warunek. Dzięki temu można na bieżąco obserwować (rejestrować), jak wiele pakietów danego typu zostało przez interfejs z nałożoną listą ACL obsłużonych.

Na rysunku poniżej podana została odpowiedź routera po wydaniu polecenia „show access-list".

```
Output

Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/sh/access-list/103/CR
Command was:  sh access-list 103

------------------------------------------------------------------

Extended IP access list 103
    10 permit icmp 10.3.50.0 0.0.0.255 any log-input (186712 matches)
    20 permit tcp 10.3.50.0 0.0.0.255 any eq ftp log-input (2 matches)
    30 permit tcp 10.3.50.0 0.0.0.255 any eq telnet log-input (23923 matches)
    40 permit tcp 10.3.50.0 0.0.0.255 any eq domain log-input
    50 permit tcp 10.3.50.0 0.0.0.255 any eq pop3 log-input
    60 permit tcp 10.3.50.0 0.0.0.255 any eq www log-input (148 matches)
    70 permit udp 10.3.50.0 0.0.0.255 any eq tftp log-input
    80 permit udp 10.3.50.0 0.0.0.255 any eq rip log-input
    90 permit udp 10.3.50.0 0.0.0.255 any eq domain log-input (100 matches)
    100 permit udp 10.3.50.0 0.0.0.255 any eq netbios-ss log-input
    110 permit ip any any (4249 matches)
```

Rys. 1. Wynik polecenia show access-list

Jak widać, przez interfejs „przeszło" 186712 pakietów icmp (warunek pierwszy listy dostępu), 2 pakiety ftp, 23923 pakiety sesji telnet itd.

Okresowe (cykliczne) odpytywanie w sesji telnet (ssh) lub przez interfejs www routera o „przypadki naruszenia" specyficznej listy dostępu, odczytywanie i zapamiętywanie wartości odpowiednich liczników jest najprostszym sposobem przygo-

towania statystyk ruchu sieciowego dotyczących interesujących aplikacji. Pozostaje jedynie problem zautomatyzowania procesu logowania się do urządzenia i listowania z poziomu konsoli list dostępu. Zadania tego typu z powodzeniem realizowane są np. z użyciem języka *expect* [7].

Znacznie prostszym rozwiązaniem jest wykorzystanie w roli urządzenia rejestrującego przypadki naruszenia listy ACL serwera *syslog*. W tym przypadku rejestrowanie jest automatyczne, a napływające do serwera *syslog* dane są opatrzone dodatkowo znacznikami czasowymi.

Warto odnotować, patrząc na rysunek 2, że informacja o naruszeniu listy dostępu, pomimo zapisu adresu źródłowego w postaci 10.3.50.0, przekazywana do serwera *syslog* zawiera adres IP hosta źródłowego i docelowego, łącznie z numerami portów warstwy transportowej.

```
list 103 permitted tcp 10.3.50.250(1053) (FastEthernet0/0 000c.291f.4580) -> 1.0.0.1(21), 1 packet
list 103 permitted udp 10.3.50.250(1025) (FastEthernet0/0 000c.291f.4580) -> 172.16.1.1(53), 2 packets
list 103 permitted tcp 10.3.50.250(1054) (FastEthernet0/0 000c.291f.4580) -> 1.0.0.1(23), 1 packet
list 103 permitted udp 10.3.50.250(1025) (FastEthernet0/0 000c.291f.4580) -> 172.16.1.1(53), 2 packets
list 103 permitted tcp 10.3.50.119(1134) (FastEthernet0/0 000c.29d7.b72d) -> 2.0.0.2(23), 1 packet
list 103 permitted tcp 10.3.50.250(1054) (FastEthernet0/0 000c.291f.4580) -> 1.0.0.1(23), 9 packets
list 103 permitted tcp 10.3.50.119(1135) (FastEthernet0/0 000c.29d7.b72d) -> 2.0.0.2(23), 1 packet
list 103 permitted tcp 10.3.50.119(1134) (FastEthernet0/0 000c.29d7.b72d) -> 2.0.0.2(23), 5 packets
list 103 permitted tcp 10.3.50.119(1136) (FastEthernet0/0 000c.29d7.b72d) -> 2.0.0.2(80), 1 packet
list 103 permitted tcp 10.3.50.119(1137) (FastEthernet0/0 000c.29d7.b72d) -> 2.0.0.1(23), 1 packet
figured from console by vty0 (10.3.50.119)
list 103 permitted tcp 10.3.50.119(1138) (FastEthernet0/0 000c.29d7.b72d) -> 2.0.0.1(80), 1 packet
list 103 permitted tcp 10.3.50.225(3899) (FastEthernet0/0 0000.e280.b1fb) -> 10.3.50.222(80), 1 packet
list 103 permitted tcp 10.3.50.225(3901) (FastEthernet0/0 0000.e280.b1fb) -> 10.3.50.222(80), 1 packet
list 103 permitted tcp 10.3.50.225(3902) (FastEthernet0/0 0000.e280.b1fb) -> 10.3.50.222(80), 1 packet
```

Rys. 2. Informacje o przypadkach naruszenia ACL rejestrowane przez Kiwi Syslog Daemon

A zatem przykładowy warunek typu:

„... permit tcp any any eq ftp log”

powodowałby rejestrowanie wszystkich pakietów związanych z protokołem *ftp* na interfejsie, nie tylko z sieci źródłowej 10.3.50.0, natomiast warunek

„... permit tcp any any log”

powodowałby rejestrowanie wszystkich pakietów (a ściślej segmentów) *tcp* płynących z dowolnego źródła do dowolnego miejsca przeznaczenia.

Są to jednak przypadki „logowania” informacji nt. całego ruchu sieciowego, powodujące zwykle poważne obciążenie łącza na drodze router-serwer *syslog* i raczej nie należy stosować takich prostych list. Przed zaaplikowaniem listy administrator powinien w niej sprecyzować, jaki ruch chciałby badać, tzn. skąd pochodzący i dokąd płynący (zakres adresów źródłowych i docelowych), i z jakimi aplikacjami związany.

Odpowiednie listy dostępu pozwalają rejestrować również przypadki pojawiania się na interfejsach pakietów zawierających charakterystyczne, znane z teorii ataków sieciowych, konfiguracje flag TCP.

Przykładowa lista dostępu zawierająca warunki z nielegalnymi kombinacjami flag w nagłówkach TCP przedstawiona jest poniżej [8].

```
access-list 150 deny   tcp any any established fin psh syn urg
access-list 150 deny   tcp any any rst syn
access-list 150 deny   tcp any any established fin syn
access-list 150 deny   tcp any any fin syn
access-list 150 deny   tcp any any ack fin syn
```

Listy dostępu, stosowane zwykle do zabezpieczania sieci przed nieautoryzowanym dostępem, różnego rodzaju atakami czy modyfikowaniem konfiguracji urządzeń, mogą być z powodzeniem stosowane do rejestrowania ruchu dotyczącego wskazanych przed administratora sesji. Stosowane właściwie nie obciążają nadmiernie urządzeń, a przy tym umożliwiają precyzyjne wskazanie istotnych sesji i zapamiętanie tylko interesujących administratora informacji.

3. KONFIGUROWANIE SESJI SPAN, RSPAN I VSPAN

Niestety, tzw. logowanie przypadków naruszenia listy kontroli dostępu nie może być stosowane na przełącznikach warstwy drugiej, choć istnieje tutaj możliwość stosowania list dostępu filtrujących w oparciu o adresy fizyczne urządzeń (hostów) sieciowych, tzw. MAC ACL-i.

W pojedynczej domenie rozgłoszeniowej (podsieci IP), w przypadku konieczności analizowania aktywności wybranych hostów, pozostaje (obok stosowania RMON) przechwytywanie całego ruchu i analizowanie zawartości pakietów. Nieco bardziej skomplikowane staje się analizowanie ruchu w przypadku podzielenia sieci na mniejsze domeny rozgłoszeniowe za pomocą VLAN-ów.

SPAN (*Switch Port Analyzer*) jest funkcją przełącznika pozwalającą na przekazywanie wszystkich ramek pojawiających się na portach przełącznika (odbieranych bądź wysyłanych przez port) do wskazanego portu (SPAN destination), gdzie przyłączana jest stacja monitorująca (przechwytująca i analizująca pakiety).

Konfiguracja sesji SPAN jest bardzo prosta i sprowadza się do wskazania portów źródłowych (monitorowanych) i portu docelowego.

Przykładowo, zapis:

Switch(config)# **monitor session 1 source interface Fastethernet 0/1 – 10**
Switch(config)# **monitor session 1 destination interface Fastethernet 0/11**

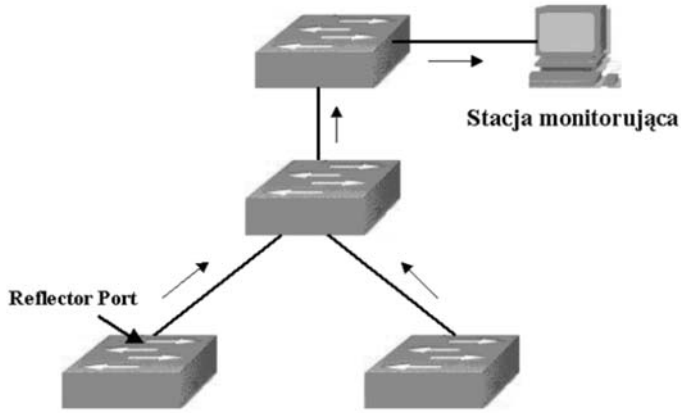
oznacza, że porty przełącznika Cisco Catalyst 2900 o numerach od 1 do 10 stają się portami źródłowymi, z których cały ruch będzie „kopiowany" i przesyłany do portu Fastethernet 0/11.

Sesje SPAN mogą być również stosowane w przypadku skonfigurowanych na przełączniku sieci wirtualnych (tzw. VSPAN – Virtual SPAN). Dla przykładu, zapis typu:

Switch(config)# **monitor session 2 source vlan 1 – 3 rx**
Switch(config)# **monitor session 2 destination interface gigabiteth 0/7**

oznacza, że na porcie gigabitethernet 0/7 pojawią się kopie ramek kierowanych do portów przełącznika przypisanych do VLAN-ów o numerach od 1 do 3.

RSPAN (Remote SPAN) jest z kolei implementacją sesji SPAN dla wielu przełączników połączonych kaskadowo, jak na rysunku 3.

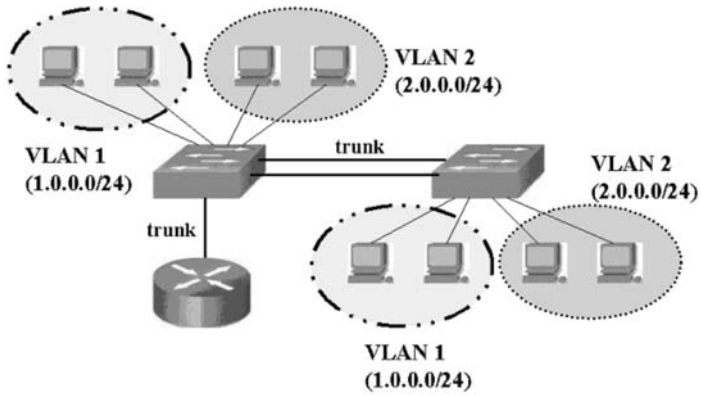


Rys. 3. Sesja RSPAN w środowisku kaskadowo połączonych przełączników

Pierwszym etapem konfigurowania sesji RSPAN jest utworzenie dedykowanego tej sesji VLAN-u. Ramki ze wskazanych portów (portów źródłowych) będą podlegały enkapsulacji (w tym oznaczaniu numerem tego VLAN-u), a następnie przekazywane będą tzw. łączami trunkingowymi pomiędzy przełącznikami do stacji monitorującej. Konieczne jest tutaj również wskazanie portów (*Reflector Ports*) odpowiedzialnych za przekazywanie ramek do sąsiedniego przełącznika na drodze do stacji monitorującej.

Szczegółowe informacje nt. konfigurowania sesji RSPN, również dla przypadku skonfigurowanych na przełącznikach sieci wirtualnych, dostępne są w dokumentacji technicznej przełączników.

Wykorzystywanie sieci wirtualnych, stosowane we współczesnych rozwiązaniach w środowiskach sieciowych, coraz rzadziej są jedynie sposobem odseparowania grup użytkowników. Możliwość skonfigurowania sieci VLAN powinna być i jest postrzegana jako sposób na podzielenie dużej i „zatłoczonej" sieci IP na kilka mniejszych podsieci IP, a tym samym na uzyskanie mniejszych domen rozgłoszeniowych. Typowe rozwiązanie pokazane jest na rysunku 4. Sieci VLAN1 i VLAN2 są tutaj różnymi sieciami IP, a tzw. „jednoręki" router służy przywróceniu komunikacji pomiędzy stacjami roboczymi należącymi do różnych VLAN-ów.



Rys. 4. „Jednoręki" router łączący sieci VLAN

Dzięki takim konfiguracjom możliwe jest ustawienie na poszczególnych subinterfejsach łącza trunkingowego pomiędzy routerem a przełącznikiem odpowiednich list kontroli dostępu, kierowanie informacji o ich naruszeniu do serwera *syslog* i obserwowanie ruchu pomiędzy VLAN-ami.

4. TECHNOLOGIA NETFLOW SWITCHING

NetFlow jest specyficznym sposobem przełączania pakietów, implementowanym w routerach firmy Cisco. NetFlow klasyfikuje ruch i umożliwia eksportowanie danych do aplikacji współpracujących. Przykładem takich aplikacji może być NetFlow Collector (serwer zbierający wszelkie dane napływające z routera z uruchomionym NetFlow) czy NetFlow Data Analyzer (aplikacja przetwarzająca i zobrazowująca zebrane dane).

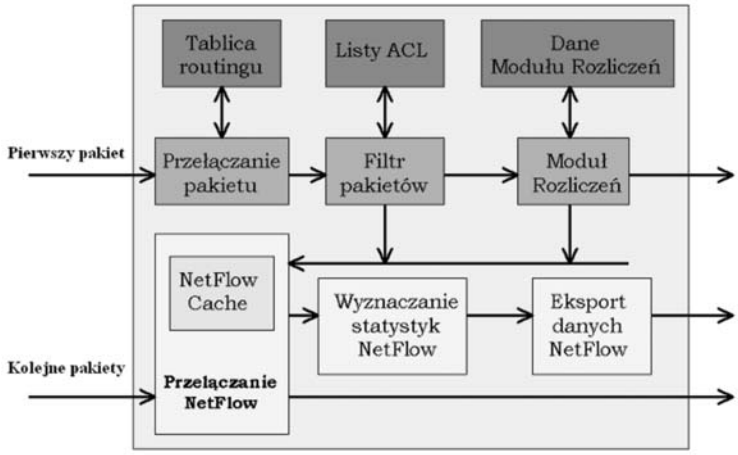
Podstawowym pojęciem związanym z technologią NetFlow jest ***przepływ*** *(flow)*. Jest on definiowany jako strumień pakietów płynący w jednym kierunku pomiędzy

zadanym źródłem a punktem przeznaczenia. Przepływy identyfikowane i rozróżniane są przez charakteryzujące je kombinacje następujących parametrów [3]:

- adresu IP nadawcy,
- adresu IP odbiorcy,
- numeru portu nadawcy,
- numeru portu odbiorcy,
- typu protokołu warstwy sieciowej,
- wartości pola ToS pakietu,
- interfejsu wejściowego routera identyfikującego przepływ.

Niekonwencjonalny sposób obsługi pakietów przy uruchomionym przełączaniu NetFlow polega na zastosowaniu tradycyjnego trybu przełączania tylko dla pierwszego pakietu z przepływu, utworzeniu charakterystycznego dla tego przepływu wpisu w pamięci NetFlow Cache i przełączaniu kolejnych pakietów należących do przepływu (przynależność potwierdza odpowiedni zapis w NetFlow Cache) bez podejmowania innych działań typu: wyznaczenie interfejsu wyjściowego dla pakietu, sprawdzenie pakietu pod kątem spełniania zdefiniowanych przez administratora warunków na listach dostępu itp.

Zasada przełączania NetFlow zilustrowana została na rysunku 5.



Rys. 5. Obsługa pakietów przez router z uruchomionym trybem przełączania NetFlow [3]

Oprócz specyficznego, szybkiego przełączania pakietów NetFlow zapewnia gromadzenie statystyk dotyczących przepływów przy minimalnym obciążeniu zasobów routera. Pomiary te stanowią integralną część procesu przełączania, a dane dotyczące ruchu sieciowego przechowywane są w NetFlow Cache.

Podstawowe funkcje oprogramowania zarządzającego przełączaniem NetFlow (tzw. NetFlow Cache Management) to:

a) szybkie określanie, czy pakiet należy do danego przepływu, czy też należy utworzyć dla niego nowy wpis w NetFlow Cache,
b) uaktualnianie na bieżąco statystyk dotyczących każdego przepływu rezydującego w NetFlow Cache,
c) wykrywanie wygaśnięcia przepływu.

Wygasanie wpisów w NetFlow Cache określają następujące reguły:

- przepływy, które pozostają nieaktywne przez zadany czas, są wykrywane i usuwane z pamięci,
- "stare" przepływy są wygaszane i usuwane z pamięci w myśl zasady, że przepływ nie może rezydować w pamięci dłużej niż 30 minut,
- z pamięci usuwane są natychmiast przepływy dotyczące połączeń TCP z stawioną flagą FIN lub RST,
- przepływy pewnych typów (np. związane z odwołaniami DNS) podlegają działaniu procedur agresywnego postarzania i tym samym szybszego rugowania z pamięci cache.

NetFlow Cache zapamiętuje skończoną liczbę przepływów. Administrator sieci powinien dostosować rozmiar pamięci cache do klasy posiadanego urządzenia, przeznaczenia danego interfejsu i ilości pakietów obsługiwanych przez ten interfejs. W dokumentacjach urządzeń zaleca się przemyślane uaktywnianie trybu przełączania NetFlow (NetFlow uaktywniany jest na wskazanym interfejsie urządzenia), tak aby nie obciążać niepotrzebnie routera zbieraniem statystyk dotyczących nieistotnych z punktu widzenia zadania monitorowania sieci przepływów.

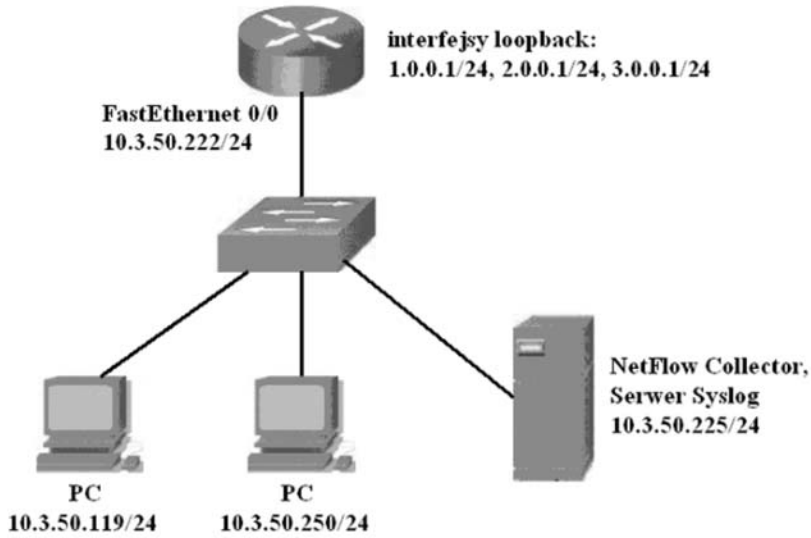
Wygasające przepływy mogą być przez router grupowane razem w datagramy i eksportowane (funkcja Eksport danych NetFlow na rysunku 5) do serwerów (aplikacji) rejestrujących przepływy w pamięci dyskowej. Przykładowo, w wersji 5 protokołu NetFlow datagramy przepływów mogą zawierać do 30 rekordów opisujących pojedyncze przepływy i są eksportowane przynajmniej raz na sekundę lub w momentach ukompletowania datagramu wygasłych przepływów.

Dane przekazywane do NetFlow Collectora, w zależności od wersji NetFlow, mogą zawierać [3]:

- źródłowy i docelowy adres IP,
- numery portów TCP i UDP,
- wartości pola ToS,
- liczbę pakietów i bajtów przesyłanych w strumieniu,
- moment startu i zakończenia transmisji danego strumienia,

- wartości flag TCP i informacje o ewentualnych enkapsulacjach,
- informacje dotyczące routingu, np. adres następnego skoku, numer systemu autonomicznego nadawcy i odbiorcy.

Podstawą eksperymentów z protokołem NetFlow było środowisko badawcze z routerem serii 2600 jak na rysunku 6. Wykorzystana została wersja demonstracyjna NetFlow Collectora o nazwie NetFlow Monitor firmy Crannog Software [4].



Rys. 6. Proste środowisko badawcze z routerem serii 2600 i NetFlow Collectorem

Poniżej zamieszczono fragment skryptu konfiguracyjnego routera, w którym wytłuszczonym drukiem zaznaczone zostały polecenia wprowadzające interfejs w tryb pracy NetFlow Switching i ustalające adres IP serwera rejestrującego przepływy (w tym przypadku 10.3.50.225).

```
.!
interface FastEthernet0/0
ip address 10.3.50.222 255.255.255.0
ip access-group 103 in
ip route-cache flow
speed auto
.
!
ip flow-export version 5
ip flow-export destination 10.3.50.225 2055
no ip http server
```

Statystyki NetFlow są dostępne po wydaniu polecenia **show ip cache flow** (rysunek 7), jednakże zbieranie ich w trybie przechwytywania wyników poleceń wydawanych w oknie konsoli urządzenia jest niewygodne i uciążliwe.

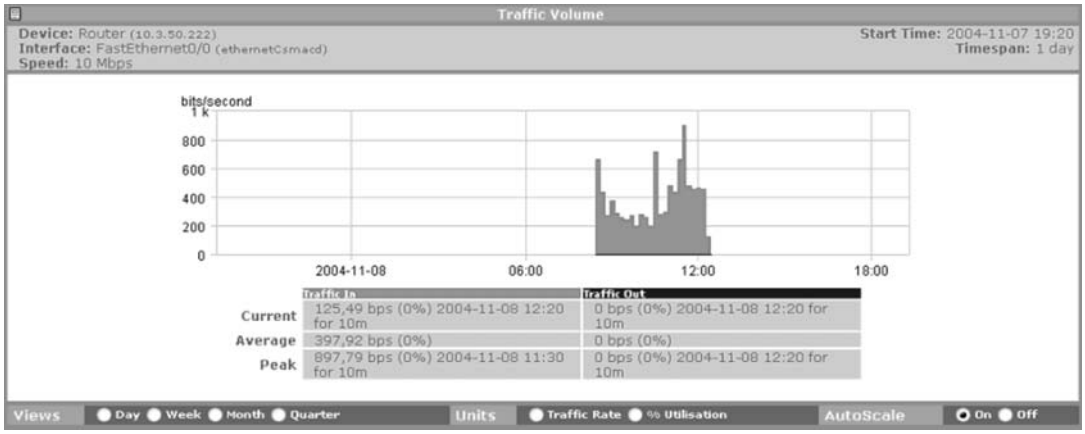
```
Output

Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/sh/ip/cache/flow/CR
Command was:  sh ip cache flow

------------------------------------------------------------------------

IP packet size distribution (212330 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .113 .005 .000 .000 .000 .000 .001 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .878 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 738 added
  15013 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17032 bytes
  1 active, 1023 inactive, 738 added, 738 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          40      0.0       598    40      3.2      38.6       5.6
TCP-FTP              2      0.0         1    60      0.0       0.0      15.2
TCP-WWW             26      0.0         5   110      0.0       2.3       4.2
UDP-DNS             17      0.0         5    65      0.0      24.7      11.2
UDP-other          608      0.0         2   117      0.1       1.6      15.5
ICMP                44      0.0      4242  1447     25.0      28.4       9.2
Total:             737      0.0       288  1278     28.4       5.8      14.1

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         10.3.50.225     Local         10.3.50.222     06 132B 0050     4
```

Rys. 7. Statystyki NetFlow wyświetlane po wydaniu polecenia show ip cache flow

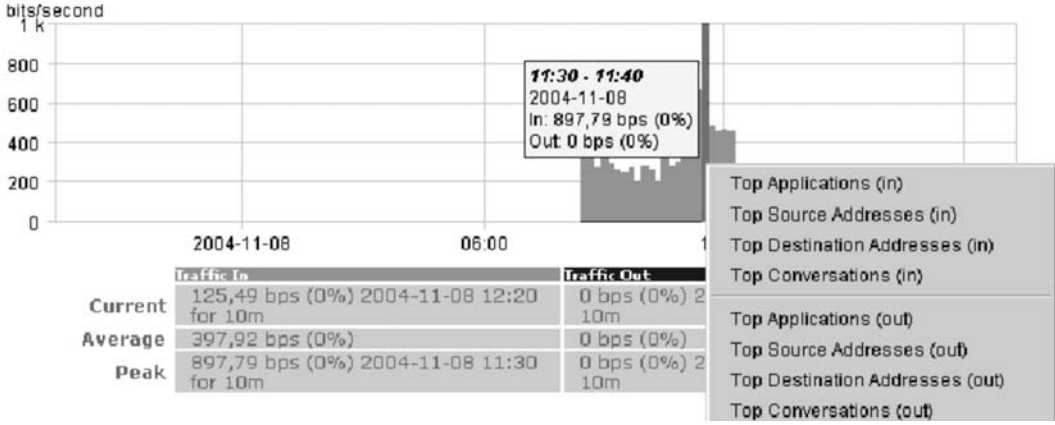
Znacznie praktyczniejsze jest eksportowanie, rejestrowanie i analiza danych przez dedykowaną aplikację, w tym przypadku NetFlow Monitor firmy Crannog Software.

Demonstracyjna wersja NetFlow Monitora posiada wbudowany analizator danych NetFlow, umożliwiający przygotowanie różnorodnych przekrojów dotyczących ruchu sieciowego.

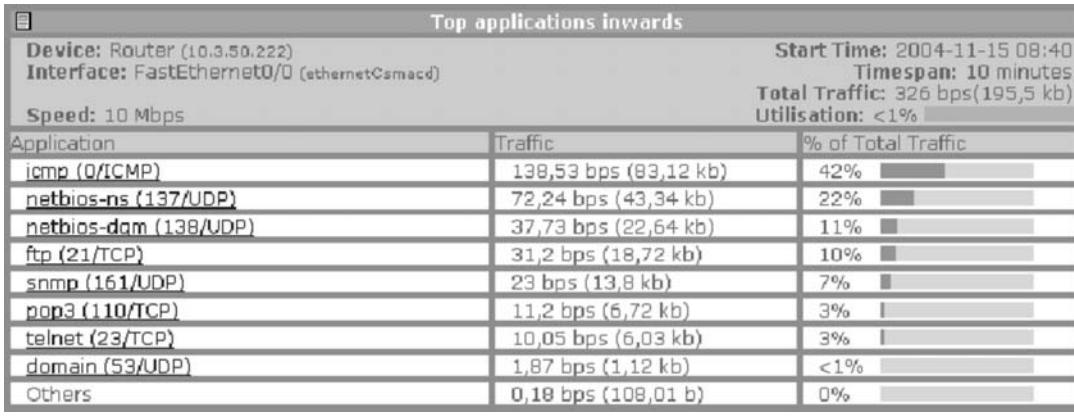
Na rysunkach poniżej (rys. 8 – rys. 13), na tle graficznego interfejsu NetFlow Monitora, przedstawione są jedynie wybrane zestawienia przygotowane na podstawie danych otrzymanych z routera.



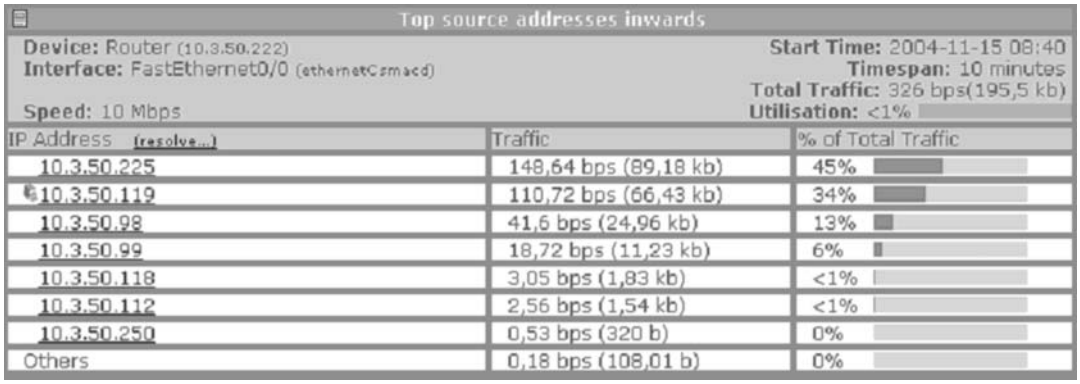
Rys. 8. Statystyki ogólne dotyczące ruchu sieciowego zebrane przez NetFlow Monitor



Rys. 9. Menu przekrojów dla wybranego czasu obserwacji sieci



Rys. 10. Zestawienie Top Application dla wybranego zakresu czasowego



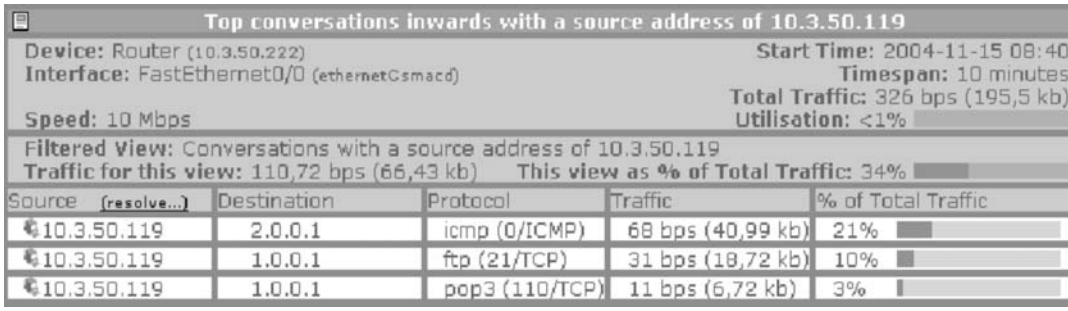
Top source addresses inwards

Device: Router (10.3.50.222)
Interface: FastEthernet0/0 (ethernetCsmacd)
Speed: 10 Mbps

Start Time: 2004-11-15 08:40
Timespan: 10 minutes
Total Traffic: 326 bps(195,5 kb)
Utilisation: <1%

IP Address (resolve...)	Traffic	% of Total Traffic
10.3.50.225	148,64 bps (89,18 kb)	45%
10.3.50.119	110,72 bps (66,43 kb)	34%
10.3.50.98	41,6 bps (24,96 kb)	13%
10.3.50.99	18,72 bps (11,23 kb)	6%
10.3.50.118	3,05 bps (1,83 kb)	<1%
10.3.50.112	2,56 bps (1,54 kb)	<1%
10.3.50.250	0,53 bps (320 b)	0%
Others	0,18 bps (108,01 b)	0%

Rys. 11. Najaktywniejsze hosty w wybranym oknie czasowym



Top conversations inwards with a source address of 10.3.50.119

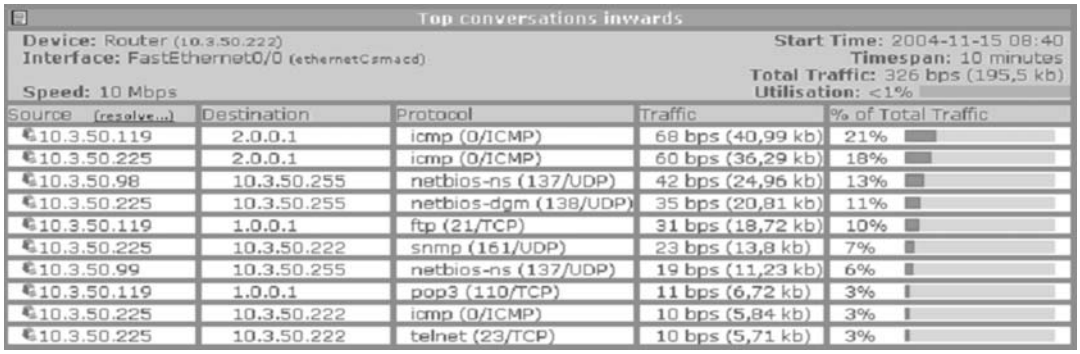
Device: Router (10.3.50.222)
Interface: FastEthernet0/0 (ethernetCsmacd)
Speed: 10 Mbps

Start Time: 2004-11-15 08:40
Timespan: 10 minutes
Total Traffic: 326 bps (195,5 kb)
Utilisation: <1%

Filtered View: Conversations with a source address of 10.3.50.119
Traffic for this view: 110,72 bps (66,43 kb) **This view as % of Total Traffic:** 34%

Source (resolve...)	Destination	Protocol	Traffic	% of Total Traffic
10.3.50.119	2.0.0.1	icmp (0/ICMP)	68 bps (40,99 kb)	21%
10.3.50.119	1.0.0.1	ftp (21/TCP)	31 bps (18,72 kb)	10%
10.3.50.119	1.0.0.1	pop3 (110/TCP)	11 bps (6,72 kb)	3%

Rys. 12. Sesje hosta 10.3.50.119



Top conversations inwards

Device: Router (10.3.50.222)
Interface: FastEthernet0/0 (ethernetCsmacd)
Speed: 10 Mbps

Start Time: 2004-11-15 08:40
Timespan: 10 minutes
Total Traffic: 326 bps (195,5 kb)
Utilisation: <1%

Source (resolve...)	Destination	Protocol	Traffic	% of Total Traffic
10.3.50.119	2.0.0.1	icmp (0/ICMP)	68 bps (40,99 kb)	21%
10.3.50.225	2.0.0.1	icmp (0/ICMP)	60 bps (36,29 kb)	18%
10.3.50.98	10.3.50.255	netbios-ns (137/UDP)	42 bps (24,96 kb)	13%
10.3.50.225	10.3.50.255	netbios-dgm (138/UDP)	35 bps (20,81 kb)	11%
10.3.50.119	1.0.0.1	ftp (21/TCP)	31 bps (18,72 kb)	10%
10.3.50.225	10.3.50.222	snmp (161/UDP)	23 bps (13,8 kb)	7%
10.3.50.99	10.3.50.255	netbios-ns (137/UDP)	19 bps (11,23 kb)	6%
10.3.50.119	1.0.0.1	pop3 (110/TCP)	11 bps (6,72 kb)	3%
10.3.50.225	10.3.50.222	icmp (0/ICMP)	10 bps (5,84 kb)	3%
10.3.50.225	10.3.50.222	telnet (23/TCP)	10 bps (5,71 kb)	3%

Rys. 13. Najaktywniejsze sesje w ujęciu host-host

Jak widać, zebrane w NetFlow Collectorze informacje pozwalają na przygotowanie bardzo szczegółowych przekrojów, które mogą usatysfakcjonować dociekliwego administratora sieci.

Dane zebrane przez jeden bądź wiele serwerów NetFlow Collector są zwykle przetwarzane z wykorzystaniem narzędzi do analizy danych (NetFlow Data Analy-

zer). Jeden NetFlow Collector może obsługiwać kilka urządzeń generujących dane (w praktyce 3 do 5 urządzeń). Sugeruje się, z oczywistych względów, umieszczanie NetFlow Collectora jak najbliżej źródła danych.

Niestety, cechą charakterystyczną przełączania NetFlow jest brak możliwości ograniczenia zbioru analizowanych (przeliczanych) przepływów do niezbędnego minimum. Administrator powinien mieć możliwość odfiltrowywania niepotrzebnych informacji już u źródła rejestrowanego strumienia, tym bardziej, że rejestrowanie pełne okupione musi być spadkiem użytecznej przepustowości sieci.

NetFlow jest wewnętrzną technologią pomiarową, która powinna być stosowana na odpowiednich interfejsach brzegowych i dostępowych routerów w celu uzyskania szerokiego przeglądu ruchu przychodzącego i wychodzącego. Cisco nie zaleca aktywowania NetFlow na routerach magistralnych (ze znacznie obciążonym procesorem). Poza tym istotna jest znajomość topologii sieci i struktury routingu i unikanie wtórnego (kilkakrotnego) grupowania tych samych przepływów.

Wykorzystanie mechanizmu NetFlow ogranicza w wielu wypadkach konieczność zakupu dedykowanych sond badających ruch w sieci [5].

Warto zaznaczyć, że protokół NetFlow jest postrzegany jako wydajny mechanizm przetwarzania (procesor) list dostępowych, niezwiększający jednak wydajności routera ponad maksymalną szybkość przełączania.

NetFlow jest ciągle udoskonalany. Ostatnia wersja protokołu ma numer 9. W wersjach 12.2(14)S i 12.2(15)T systemów operacyjnych dla routerów Cisco serii 7200, 7400 i 7500 możliwe jest uaktywnianie NetFlow na subinterfejsach z enkapsulacją IEEE 802.1Q [6].

5. PODSUMOWANIE

W artykule zostały przedstawione metody rejestrowania danych o ruchu sieciowym „pojawiającym się" na interfejsach routera lub portach przełącznika w pojedynczej domenie rozgłoszeniowej. Administrator sieci musi zdecydować:

- czy rejestrować wszystko i mieć pewność, że nie przeoczy się niczego istotnego, a następnie z całego potoku danych wyłuskiwać tylko użyteczne informacje, ale przy tym obciążać sieć i urządzenia ruchem związanym z procesem rejestrowania,
- czy prowadzić rejestrowanie wybiórcze, np. z wykorzystaniem list kontroli dostępu,
- czy może łączyć techniki typu NetFlow Switching (przyspieszające obsługę ACL) ze starannie przygotowanymi listami filtrowań, co umożliwi również rejestrowanie szczególnych przypadków, jak np. próby forsowania przez hakerów urządzeń sieciowych, czy nieautoryzowane próby zmiany konfiguracji urządzeń.

Nie da się tutaj udzielić jednoznacznej odpowiedzi, które rozwiązanie jest najlepsze, gdyż wybór metody jest uzależniony od oczekiwań i aspiracji administratora oraz wyników analizy funkcjonowania sieci przed i po jej zaaplikowaniu.

Literatura

[1] Filonik J., Malinowski T.: *System monitorowania obciążenia segmentów sieci LAN,* Biuletyn ITA 19/2003, Warszawa.
[2] Stallings W.: *Protokoły SNMP i RMON. Vademecum profesjonalisty*, Warszawa, Wyd. Helion, 2003.
[3] Cisco Systems NetFlow Services Export Version 9, RFC 3954, http://www.ietf.org/rfc/
[4] Strona domowa Crannog Software, Opisa pakietu NetFlow Monitor, http://www.crannog-software.com
[5] Kohler P., Claise B.: *IPFIX fine-tunes traffic analysis,* Network World, 08/11/03, http://www.nwfusion.com/news/tech/2003/0811techupdate.html
[6] Dokumentacja techniczna firmy Cisco, NetFlow Services Solutions Guide, http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html
[7] Expect for Windows – Online Docs**,** http://aspn.activestate.com/ASPN/docs/Expect
[8] Dooley K., Brown I.J., *Cisco. Receptury,* Warszawa, Wyd. Helion, 2004.