Laboratorium 4 – Przechwytywanie i analiza danych z wykorzystaniem NetFlow

Cele ćwiczenia

Celem ćwiczenia jest zapoznanie z możliwościami funkcjonalności NetFlow dostępnej w urządzeniach Cisco w zakresie zbierania i analizy danych.

Celami szczegółowymi ćwiczenia są:

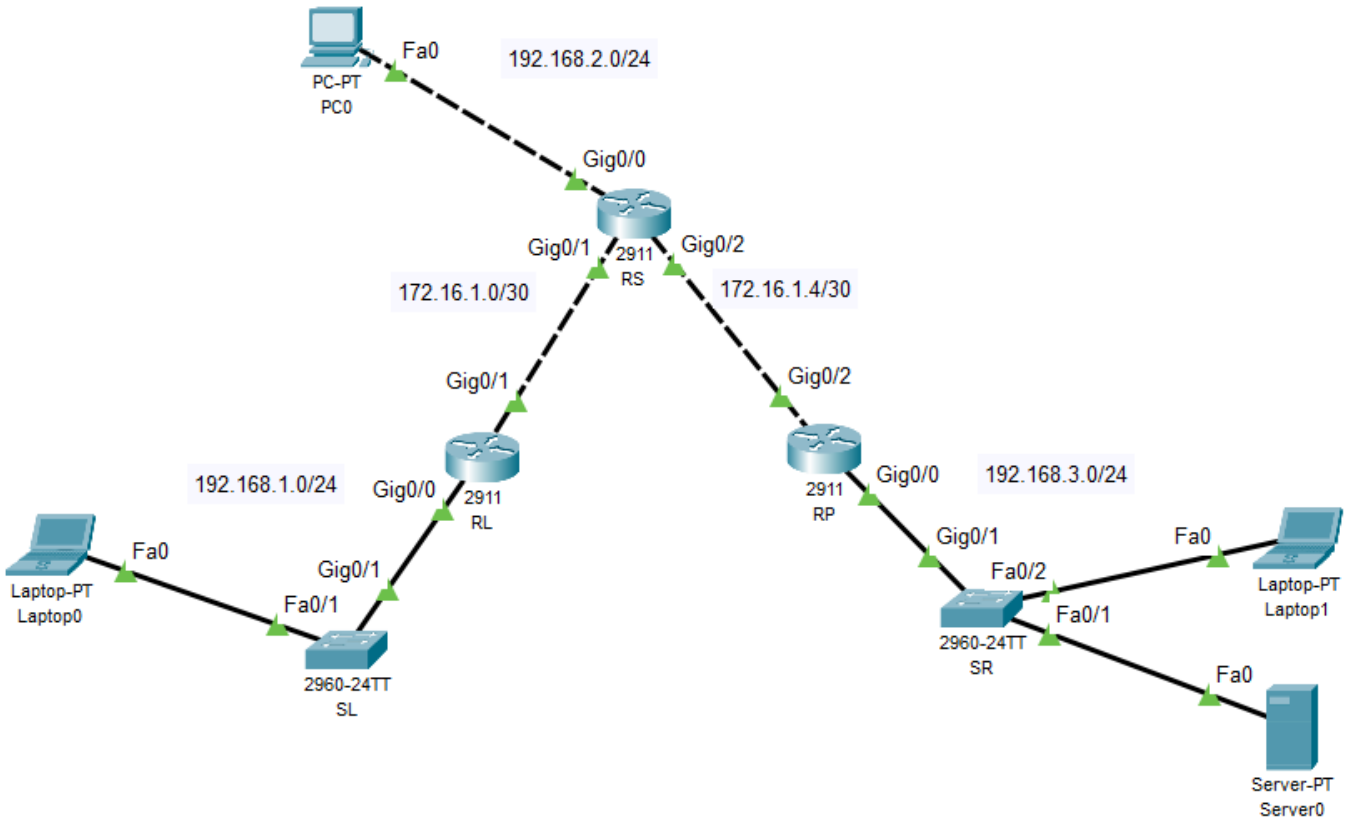
1. Konfiguracja sieci IP;
2. Konfiguracja funkcjonalności NetFlow w urządzeniach sieciowych;
3. Konfiguracja węzła zbierającego dane NetFlow (ang. NetFlow Collector);
4. Analiza danych NetFlow z wykorzystaniem linii poleceń.

Opis topologii logicznej i fizycznej sieci

1. Komputer Laptop0 o adresie IP 192.168.1.**3**/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SL
2. Port GigabitEthernet 0/1 przełącznika SL połączony z portem GigabitEthernet 0/0 rutera RL o adresie 192.168.1.**1**/24
3. Port GigabitEthernet 0/1 rutera RL o adresie 172.16.1.**1**/30 połączony z portem GigabitEthernet 0/1 rutera RS o adresie 122.16.1.**2**/30
4. Port GigabitEthernet 0/0 rutera RS, o adresie 192.168.2.**1**/24, połączony z komputerem PC0 (o adresie 192.168.2.**2**) pełniącym funkcję kolektora danych Netflow
5. Port GigabitEthernet 0/2 rutera RS o adresie 172.16.1.**5**/30 połączony z portem GigabitEthernet0/2 rutera RP o adresie 172.16.1.**6**/30
6. Port GigabitEthernet 0/0 rutera RP o adresie 192.168.3.**1**/24 połączony z portem GigabitEthernet 0/**1** przełącznika SR

7. Komputer Serwer0 o adresie IP 192.168.3.2/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SR
8. Serwer Laptop1 o adresie IP 192.168.3.**3**/24 połączony łączem FastEthernet z portem FastEthernet 0/2 przełącznika SR

Graficzną reprezentację opisanej topologii przedstawiono na poniższym rysunku



Przebieg ćwiczenia

Połączenie urządzeń zgodnie z topologią przedstawioną w poprzednim rozdziale

Nadanie adresów IP urządzeniom końcowym

1. Komputer Laptop0
    a. Adres 192.168.1.3 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.1.1 z maską 24 bitową
2. Komputer PC0
    a. Adres 192.168.2.2 z maską 24 bitową

b. Adres bramy domyślnej: 192.168.2.1 z maską 24 bitową

3. Komputer Laptop1
    a. Adres 192.168.3.3 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.3.1 z maską 24 bitową
4. Komputer Serwer0
    a. Adres 192.168.3.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.3.1 z maską 24 bitową

Konfiguracja interfejsów sieciowych ruterów

1. Ruter RL

```
RL>ena

RL#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

RL(config)#interface gigabitEthernet 0/0

RL(config-if)#ip address 192.168.1.1 255.255.255.0

RL(config-if)#no sh

RL(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

RL(config-if)#exit

RL(config)#int gig 0/1

RL(config-if)#ip add 172.16.1.1 255.255.255.252

RL(config-if)#no sh

RL(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

```
Router(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
```

2. Ruter RS

```
RS(config)#int gigabitEthernet 0/1
RS(config-if)#ip address 172.16.1.2 255.255.255.252
RS(config-if)#no sh
RS(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

RS(config)#int gigabitEthernet 0/2
RS(config-if)#ip address 172.16.1.5 255.255.255.252
RS(config-if)#no sh
RS(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

RS(config)#int gigabitEthernet 0/0
RS(config-if)#ip address 192.168.2.1 255.255.255.0
RS(config-if)#no sh
RS(config-if)#
```

3. Ruter RP

```
Router>ena

RP#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

RP(config)#interface gig 0/2

RP(config-if)#ip add 172.16.1.6 255.255.255.252
```

```
RP(config-if)#no sh


%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2,
changed state to up


RP(config)#int gig 0/0

RP(config-if)#ip add 192.168.3.1 255.255.255.0

RP(config-if)#no sh

RP(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

Sprawdzenie poprawności konfiguracji interfejsów ruterów:

```
Router#show ip interface brief
```

Uruchomienie rutingu RIP na wszystkich ruterach:

```
RL>ena

RL#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RL(config)#router rip

RL(config-router)#version 2

RL(config-router)#network 192.168.1.0

RL(config-router)#network 172.16.1.0
```

```
RL(config-router)#


RS>ena
RS#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RS(config)#router rip
RS(config-router)#version 2
RS(config-router)#network 172.16.1.0
RS(config-router)#network 172.16.1.4
RS(config-router)#network 192.168.2.1
RS(config-router)#


RP>ena
RP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RP(config)#router rip
RP(config-router)#version 2
RP(config-router)#network 172.16.1.4
RP(config-router)#network 192.168.3.0
RP(config-router)#
```

Sprawdzenie poprawności rutingu

```
RP#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R 172.16.1.0/30 [120/1] via 172.16.1.5, 00:00:25,
GigabitEthernet0/2
C 172.16.1.4/30 is directly connected, GigabitEthernet0/2
L 172.16.1.6/32 is directly connected, GigabitEthernet0/2
R 192.168.1.0/24 [120/2] via 172.16.1.5, 00:00:25,
GigabitEthernet0/2
R 192.168.2.0/24 [120/1] via 172.16.1.5, 00:00:25,
GigabitEthernet0/2
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.3.0/24 is directly connected, GigabitEthernet0/0
L 192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

Konfiguracja usługi telnet na ruterze RP

```
RP(config)#line vty 0 4

RP(config-line)#password AiTech

RP(config-line)#login

RP(config-line)#
```

Konfiguracja funkcjonalności NetFlow na ruterzez RS

1. Wskazanie interfejsów do przechwytywania ruchu:

```
RS#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RS(config)#int gigabitEthernet 0/1

RS(config-if)#ip flow ingress

RS(config-if)#ip flow egress
```

```
RS(config)#int gigabitEthernet 0/2

RS(config-if)#ip flow ingress

RS(config-if)#ip flow egress

RS#

%SYS-5-CONFIG_I: Configured from console by console
```

2. Wskazanie urządzenia, do którego będą przesyłane przechwycone dane poprzez określenie adresu IP i numeru portu UDP. W rozważanej topologii jest to komputer PC0 o adresie 192.168.2.2.

```
RS(config)#ip flow-export destination 192.168.2.2 9996
```

3. Określenie wersji protokołu NetFlow. Wersja protokołu zależy od systemu operacyjnego urządzenia sieciowego. W celu sprawdzenia można posłużyć się znakiem zapytania po poleceniu „ip flow-export version **?**”

```
RS(config)#ip flow-export version ?

9

RS(config)#ip flow-export version 9

RS(config)#
```

4. Sprawdzenie poprawności konfiguracji NetFlow na ruterze RS.

```
RS# show ip flow interface

RS# show ip flow export
```

Analiza danych NetFlow z wykorzystaniem CLI

1. Generowanie ruchu między RL i RP
    a. Nawiąż sesję www z komputera Laptop0 do Serwera0
    b. Uzyskaj dostęp z RL do usługi telnet na RP. Sprawdź wersję systemu operacyjnego RP
    c. Wyślij 2000 wiadomości ICMP Echo Request z R3 do interfejsu Gig0/0 rutera RL
2. Wyświetlenie statystyk odnośnie ruchu NetFlow na RP

```
   RP#show ip cache flow

   IP packet size distribution (9027 total packets):

      1-32   64   96  128  160  192  224  256  288  320  352  384  416  448
480

      .000 .114 .000 .886 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
.000


       512  544  576 1024 1536 2048 2560 3072 3584 4096 4608

      .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000


   IP Flow Switching Cache, 278544 bytes

     12 active, 4084 inactive, 186 added

     7 ager polls, 0 flow alloc failures

     Active flows timeout in 30 minutes

     Inactive flows timeout in 15 seconds

   IP Sub Flow Cache, 34056 bytes

     0 active, 1024 inactive, 0 added, 0 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
```

ICMP	4	0.0	2000	128	0.4	211.0	54.0
TCP-HTTP	20	0.0	5	40	0.0	0.0	54.0
TCP-TELNET	7	0.0	44	40	0.0	8.4	54.0
TCP-other	26	0.0	15	41	0.0	1.9	54.0
UDP-RIP	117	0.0	1	52	0.0	0.0	54.0
Total:	174	0.0	51	119	0.4	5.5	54.0

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gig0/1	192.168.1.3	Gig0/2	192.168.3.2	06	040b	0050	5
Gig0/2	192.168.3.2	Gig0/1*	192.168.1.3	06	0050	040b	3
Gig0/1	192.168.1.3	Gig0/2	192.168.3.2	06	040c	0050	11
Gig0/2	192.168.3.2	Gig0/1*	192.168.1.3	06	0050	040c	21
Gig0/1	192.168.1.3	Gig0/2	192.168.3.2	06	040d	0050	5
Gig0/2	192.168.3.2	Gig0/1*	192.168.1.3	06	0050	040d	3

```
   Gig0/1        192.168.1.3     Gig0/2*       192.168.3.2     06 040b 0050
5

   Gig0/2        192.168.3.2     Gig0/1        192.168.1.3     06 0050 040b
3

   Gig0/1        192.168.1.3     Gig0/2*       192.168.3.2     06 040c 0050
11

   Gig0/2        192.168.3.2     Gig0/1        192.168.1.3     06 0050 040c
21

   Gig0/1        192.168.1.3     Gig0/2*       192.168.3.2     06 040d 0050
5

   Gig0/2        192.168.3.2     Gig0/1        192.168.1.3     06 0050 040d
3

   RS#
```

3. Zaprzestanie generowania ruchu telnet i www
4. Usunięcie przechwyconych danych

```
RP#clear ip flow stats
```

5. Ponowne wyświetlenie statystyk odnośnie ruchu NetFlow na RP

```
RP#show ip cache flow
```

Zapoznanie się z oprogramowaniem służącym do analizy danych NetFlow

1. Znajdź i zapoznaj się z następującym oprogramowaniem:
    a. NFdump
    b. SiLK
    c. ELK
    d. ElastiFlow