Laboratorium 6 – Wykorzystanie SPAN i RSPAN na potrzeby telemetrii systemów wykrywania i zapobiegania intruzom

Cele ćwiczenia

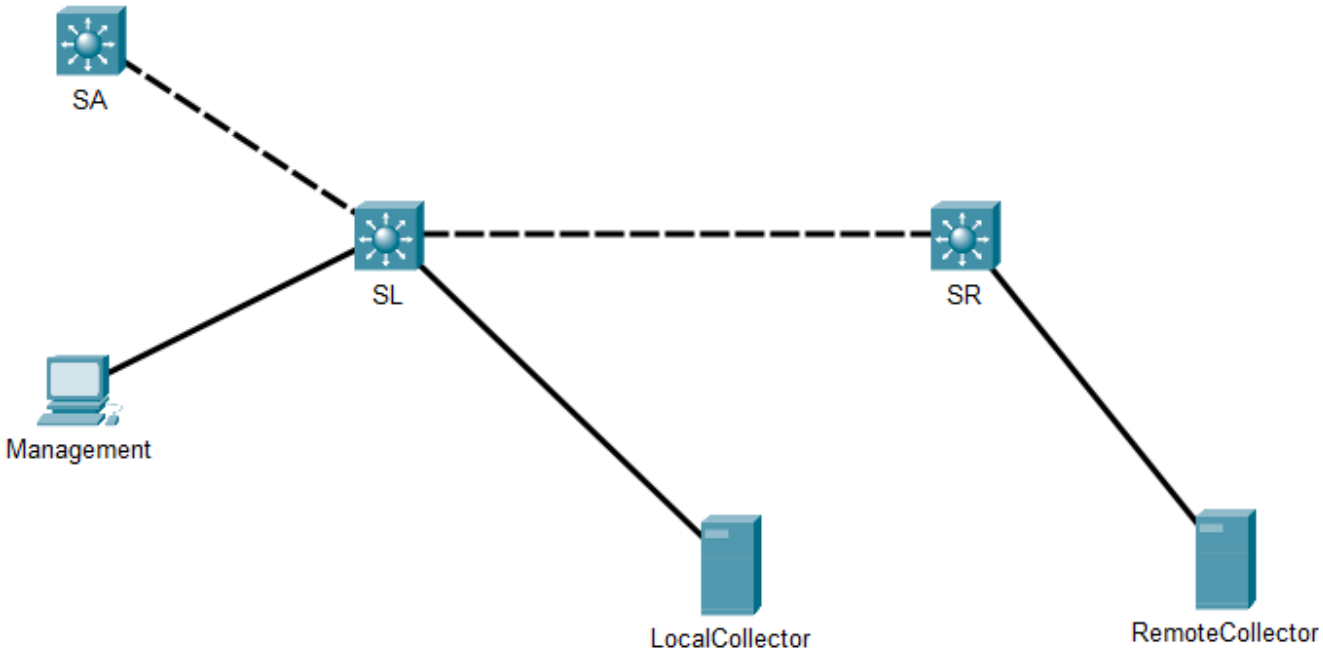
Celem ćwiczenia jest skonfigurowanie funkcjonalności SPAN i RSPAN na potrzeby analizy ruchu przy wykorzystaniu analizatora Wireshark. Cele szczegółowe są następujące:

1. Podstawowa konfiguracja sieci zbudowanej z wielu przełączników.
2. Konfiguracja usługi SPAN i analiza ruchu, za pomocą programu Wireshark, w obrębie pojedynczego przełącznika.
3. Konfiguracja usługi RSPAN (Remote SPAN) i analiza ruchu kopiowanego do określonej sieci VLAN za pomocą programu Wireshark.

Opis topologii logicznej i fizycznej sieci

1. Komputer Management o adresie IP 172.16.1.10/24 połączony łączem GigabitEthernet z portem GigabitEthernet 1/0/10 przełącznika SL.
2. Komputer LocalCollector o adresie IP 172.16.1.11/24 połączony łączem GigabitEhternet z portem GigabitEthernet 1/0/11 przełącznika SL.
3. Port GigabitEthernet 1/0/1 przełącznika SL połączony z portem GigabitEthernet 1/0/1 przełącznika SA.
4. Port GigabitEtherent 1/0/2 przełącznika SL połączony z portem GigabitEthenet 1/0/1 przełącznika SR.
5. Komputer RemoteCollector o adresie 172.16.1.12 połączony z portem GigabitEthernet 1/0/12 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 Management

   Adres 172.16.1.10 z maską 24 bitową

2. Komputer LocalCollector

   Adres 172.16.1.11 z maską 24 bitową

3. Komputer RemoteCollector

   Adres 172.16.1.12 z maską 24 bitową

Nadanie adresu IP interfejsowi VLAN1

Skonfiguruj adres IP interfejsu SA:

```
S1(config)# interface vlan 1

S1(config-if)# ip address 172.16.1.1 255.255.255.0
```

Konfiguracja portu GE1/0/2 przełącznika SL i portu GE1/0/1 przełącznika SR

```
SL(config)# interface g1/0/2

SL(config-if)# switchport mode trunk

SR(config)# interface g1/0/1

SR(config-if)# switchport mode trunk
```

Konfiguracja usługi telnet na przełączniku SA

W celu uzyskania zdalnego dostępu przy wykorzystaniu usługi telnet, skonfiguruj hasło „AiTech”

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

SA(config-line)# password AiTech

SA(config-line)# login
```

Konfiguracja SPAN w obrębie pojedynczego przełącznika, tj. przełącznika SL

Skonfiguruj porty źródłowy i docelowy w SL na potrzeby monitorowania ruchu. Cały ruch wchodzący lub wychodzący z GE1/0/1 przełacznika SL powinien być kopiowany i przekazywany przez GE1/0/11.

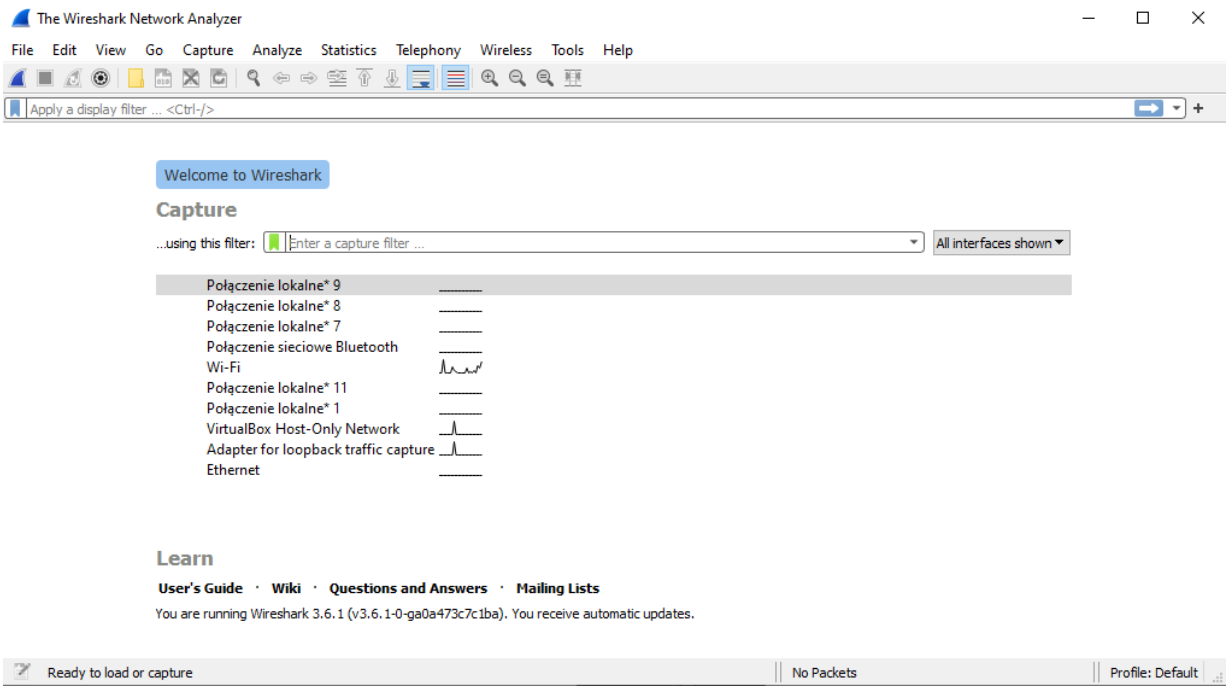
```
SL(config)# monitor session 1 source interface g1/0/1

SL(config)# monitor session 1 destination interface g1/0/11
```

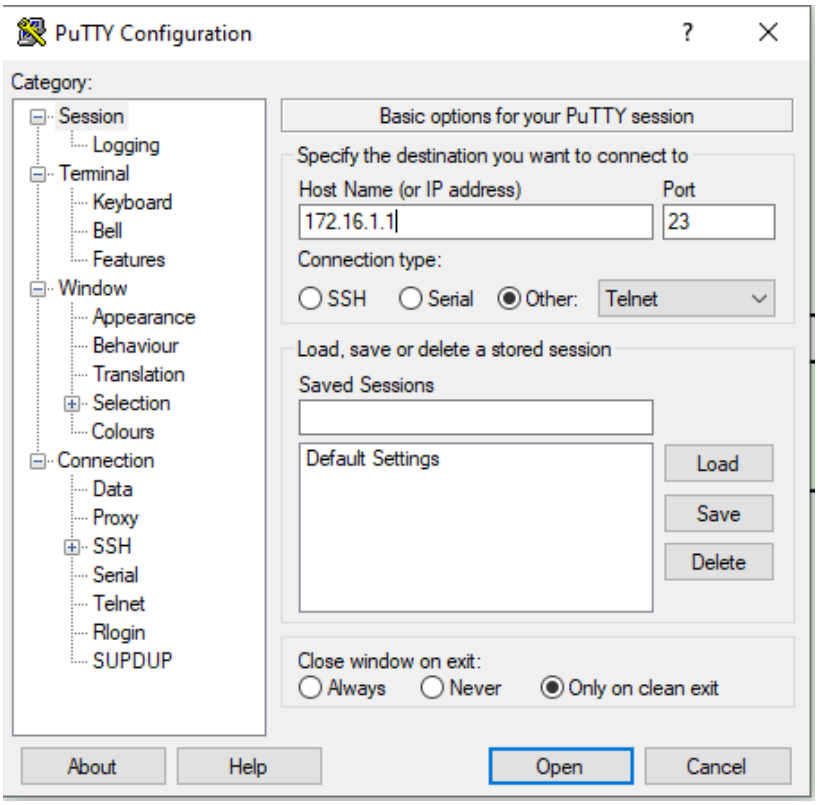
Uruchomienie program Wireshark na komputerze LocalCollector.

Wybierz odpowiedni interfejs sieciowy komputera do przechwytywania ruchu.

Na rysunku poniżej przedstawiono zrzut ekranu zawierający listę dostępnych interfejsów sieciowych komputera LocalCollector.



Wygeneruj ruch typu telnet z komputera „Management” do vlanu zarządzającego VLAN1 na przełączniku SA. Konfigurację programu PuTTY na komputerze „Management”, umożliwiającą realizację połączenia telnet, przedstawiono na poniższym rysunku.

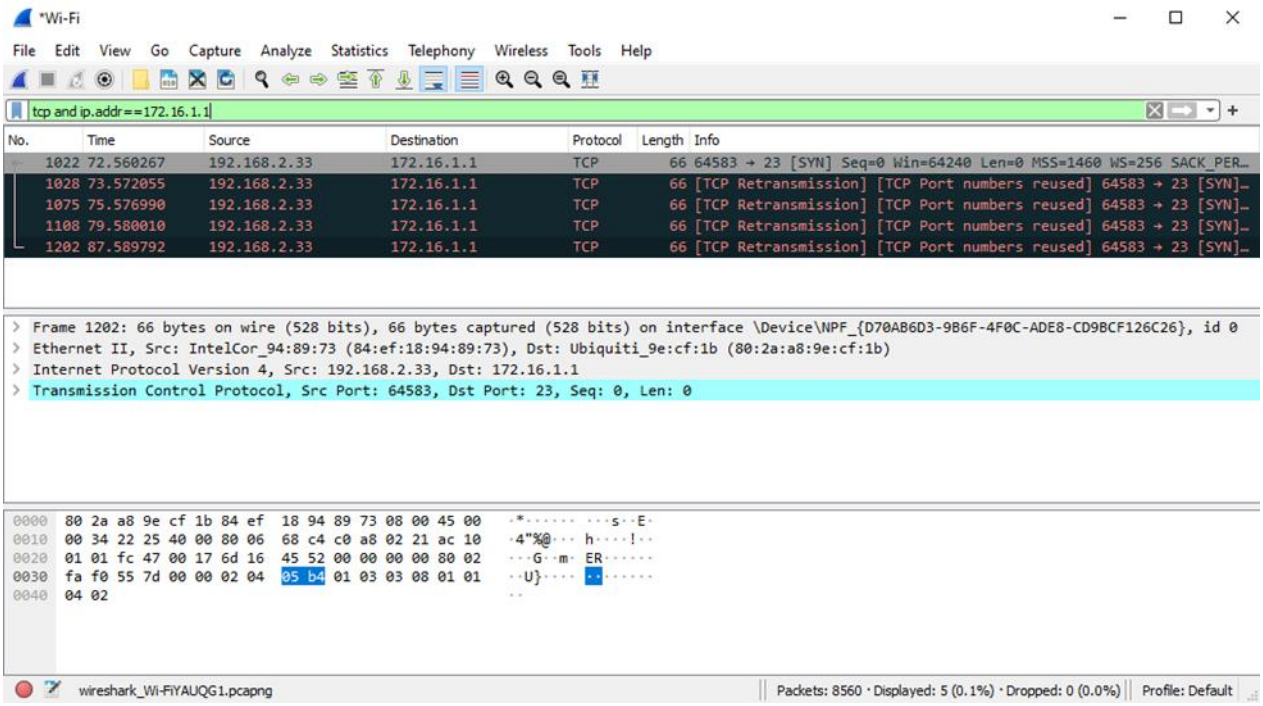


Po nawiązaniu połączenia, wyświetl bieżącą konfigurację przełącznika oraz stan wszystkich interfejsów.

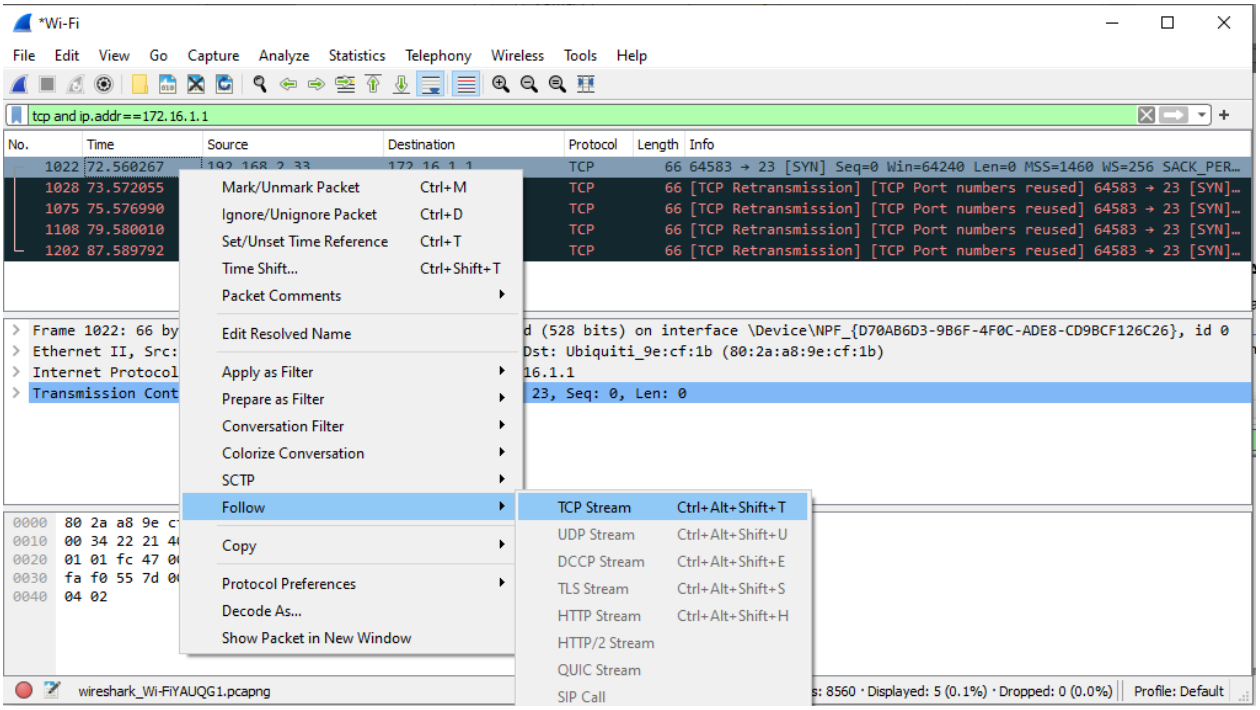
Zakończ przechwytywanie ruchu w programie Wireshark oraz zastosuj filtr ograniczający wyświetlane informacje do usługi telnet

Wprowadź polecenie: tcp and ip.addr==172.16.1.1

Przykładowy rezultat przechwytywania ruchu przedstawiono na rysunku poniżej:



Następnie scal informacje o przechwyconym ruchu telnet, wybierając z menu podręcznego odpowiednio „Follow -> TCP Stream”. Zrzut ekranu przedstawiający tę operację przedstawiono na poniższym rysunku:



Konfiguracja zdalnej sesji SPAN, tj. RSPAN, oraz analiza ruchu z wykorzystaniem programu Wireshark

1. Skonfiguruj na przełączniku SL dedykowany VLAN nr 90, który będzie wykorzystywany do przesyłania ruchu z monitorowanych interfejsów jednego przełącznika do przełącznika, do którego dołączony jest RemoteCollector. W rozważnym przypadku, interfejsy źródłowy i docelowy sesji RSPAN są skonfigurowane na różnych przełącznikach, odpowiednio SL i SR. Oznacza to, że VLAN 90 musi być skonfigurowany zarówno na przełączniku SL (źródłowym), jak i SR (docelowym), do którego dołączono kolektor danych.

```
SL(config)# vlan 90

SL(config-vlan)# remote-span

SL(config-vlan)# end
```

2. Skonfiguruj port źródłowy i vlan docelowy na przełączniku SL tak, aby cały ruch otrzymywany na interfejsie GE1/0/1 był kopiowany i przekazywany do VLANu nr 90 przez port GE1/0/2, w kierunku przełącznika SR.

```
SL(config)# monitor session 2 source interface g1/0/1 rx

SL(config)# monitor session 2 destination remote vlan 90
reflector-port g1/0/2
```

3. Skonfiguruj na przełączniku SR vlan 90, służący do przesyłania ruchu kopiowanego z monitorowanych interfejsów przełącznika SL

```
SR(config)# vlan 90

SR(config-vlan)# remote-span

SR(config-vlan)# end
```

4. Skonfiguruj vlan źródłowy i interfejs docelowy na przełączniku SR tak, aby cały ruch otrzymywany w VLAN 90 był kopiowany na GE1/0/21 przełącznika SR.

```
SR(config)# monitor session 2 source remote vlan 90

SR(config)# monitor session 2 destination interface g1/0/12
```

Analiza ruchu na komputerze RemoteController

1. Uruchom program Wireshark na komputerzez RemoteCollector.
2. Wygeneruj ruch telnet z komputera Management do przełącznika SA.
3. Zatrzymaj działające przechwytywanie Wireshark na komputerzez RemoteCollector.
4. Filtruj przechwytywanie Wireshark pod kątem ruchu telnet. Wpisz tcp i ip.addr==172.16.1.1 i naciśnij Enter. Następnie spróbuj odszyfrować przechwycony ruch telnet. Kliknij prawym przyciskiem myszy przechwycone wiadomości telnet i wybierz z menu kontekstowego Follow-> TCP Stream.