LABORATORIUM PROJEKTOWANIE I OBSŁUGA SIECI KOMPUTEROWYCH I

Data wykonania ćwiczenia:	13.12.2023
Rok studiów:	3
Semestr:	5
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	10

Temat: Packet Tracer - Konfiguracja zabezpieczeń przełącznika

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Packet Tracer - Konfiguracja zabezpieczeń przełącznika

Część 1: Konfiguracja urządzeń sieciowych

Po okablowaniu sieci w odpowiedni sposób, uruchomimy skrypt konfiguracyjny routera R1

```
enable
configure terminal
hostname R1
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 description Link to S1 Port 5
 ip dhcp relay information trusted
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 exec-timeout 0 0
```

Następnie możemy sprawdzić czy adresy się zgadzają

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  down                  down
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Loopback0              10.10.1.1       YES manual up                    up
```

Następnie musimy skonfigurować switche

S1

```
S1# config t
S1(config)# hostname S1

S1(config)# no ip domain-lookup
```

```
S1(config)# interface f0/1
S1(config-if)# description Link to S2
S1(config-if)# interface f0/5
S1(config-if)# description Link to R1
S1(config-if)# interface f0/6
S1(config-if)# description Link to PC-A

S1(config)# ip default-gateway 192.168.10.1
```

S2

```
S1# config t
S1(config)# hostname S2

S2(config)# no ip domain-lookup

S2(config)# interface f0/1
S2(config-if)# description Link to S1
S2(config-if)# interface f0/18
S2(config-if)# description Link to PC-B

S2(config)# ip default-gateway 192.168.10.1
```

Część 2: Skonfiguruj sieci VLAN na przełącznikach.

Zacznijmy od skonfigurowania VLAN 10 na obu switchach

```
S1(config)# vlan 10
S1(config-vlan)# name Management

S2(config)# vlan 10
S2(config-vlan)# name Management
```

Następnie ustawimy SVI dla vlan 10

```
S1(config)# interface vlan 10
S1(config-if)# ip address 192.168.10.201 255.255.255.0
S1(config-if)# description Management SVI
S1(config-if)# no shutdown

S2(config)# interface vlan 10
S2(config-if)# ip address 192.168.10.202 255.255.255.0
S2(config-if)# description Management SVI
S2(config-if)# no shutdown
```

Kolejnym krokiem jest vlan 333

```
S1(config)# vlan 333
S1(config-vlan)# name Native

S2(config)# vlan 333
S2(config-vlan)# name Native
```

Ostatecznie ustawimy vlan 999

```
S1(config-vlan)# vlan 999
S1(config-vlan)# name ParkingLot

S2(config-vlan)# vlan 999
S2(config-vlan)# name ParkingLot
```

Część 3: Konfiguracja zabezpieczeń przełącznika.

Zaczniemy od implementacji trunki 802.1Q

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 333

S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 333
```

Teraz możemy sprawdzić konfiguracje obu switchy

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,333,999

S2# show interface trunk
```

```
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,333,999
```

Teraz wyłączymy negocjację DTP dla F0/1

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate

S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

Ponownie zweryfikujemy czy wszystko idzie dobrze

```
S1# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off

S2# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

Teraz ustawimy access porty

```
S1(config)# interface range f0/5 - 6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
```

Teraz zabezpieczymy i wyłączymy nieużywane porty przełączników

```
S1(config)# interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
```

```
S2(config)# interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown
```

Następnie zweryfikujemy konfiguracje

```
S1# show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S2         connected    trunk      a-full  a-100 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
Fa0/4                        disabled     999          auto   auto 10/100BaseTX
Fa0/5     Link to R1         connected    10         a-full  a-100 10/100BaseTX
Fa0/6     Link to PC-A       connected    10         a-full  a-100 10/100BaseTX
Fa0/7                        disabled     999          auto   auto 10/100BaseTX
Fa0/8                        disabled     999          auto   auto 10/100BaseTX
Fa0/9                        disabled     999          auto   auto 10/100BaseTX
Fa0/10                       disabled     999          auto   auto 10/100BaseTX
...
S2# show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         connected    trunk      a-full  a-100 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
...
Fa0/14                       disabled     999          auto   auto 10/100BaseTX
Fa0/15                       disabled     999          auto   auto 10/100BaseTX
Fa0/16                       disabled     999          auto   auto 10/100BaseTX
Fa0/17                       disabled     999          auto   auto 10/100BaseTX
Fa0/18    Link to PC-B       connected    10         a-full  a-100 10/100BaseTX
Fa0/19                       disabled     999          auto   auto 10/100BaseTX
Fa0/20                       disabled     999          auto   auto 10/100BaseTX
Fa0/21                       disabled     999          auto   auto 10/100BaseTX
Fa0/22                       disabled     999          auto   auto 10/100BaseTX
Fa0/23                       disabled     999          auto   auto 10/100BaseTX
Fa0/24                       disabled     999          auto   auto 10/100BaseTX
Gi0/1                        disabled     999          auto   auto
10/100/1000BaseTX
Gi0/2                        disabled     999          auto   auto
10/100/1000BaseTX
```

Zapiszemy teraz dokumentację

Funkcja	**Ustawienie domyślne**
Zabezpieczenie portu	Disabled

Funkcja	Ustawienie domyślne
Maksymalna liczba bezpiecznych adresów MAC	1
Tryb naruszenia	Shutdown
Czas przedawnienia	0 mins
Rodzaj przedawnienia	Absolute
Przedawnienie bezpiecznego adresustatycznego	Disabled
Opcja Sticky adresów MAC	0

Na S1, włącz zabezpieczenia portu na F0/6 z następującymi ustawieniami

- Maksymalna liczba bezpiecznych adresów MAC: 3
- Rodzaj naruszenia: restrict
- Czas przedawnienia: 60 min
- Rodzaj przedawnienia: brak aktywności

```
S1(config)# interface f0/6
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation restrict
S1(config-if)# switchport port-security aging time 60
S1(config-if)# switchport port-security aging type inactivity
```

```
S1# show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3411:10
Security Violation Count   : 0

S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  10    0022.5646.3411    SecureDynamic                 Fa0/6       60 (I)
------------------------------------------------------------------------
```

```
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Enable port security for F0/18 on S2. Skonfiguruj port, aby automatycznie dodawać adresy MAC wyuczone na porcie do bieżącej konfiguracji.

```
S2(config)# interface f0/18
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security mac-address sticky
```

Skonfiguruj następujące ustawienia zabezpieczeń portu f0/18 na S2:

- Maksymalna liczba bezpiecznych adresów MAC: 2
- Rodzaj naruszenia: Protect
- Czas przedawnienia: 60 min

```
S2(config)# interface f0/18
S2(config-if)# switchport port-security aging time 60
S2(config-if)# switchport port-security maximum 2
S2(config-if)# switchport port-security violation protect
```

```
S2# show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3413:10
Security Violation Count   : 0

S2# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  10    0022.5646.3413    SecureSticky                  Fa0/18       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Zaimplementuj zabezpieczenia DHCP snooping

W przypadku S2 włącz DHCP snooping i skonfiguruj DHCP snooping w sieci VLAN 10.

```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10
```

Skonfiguruj port trunk na S2 jako port zaufany.

```
S2(config)# interface f0/1
S2(config-if)# ip dhcp snooping trust
```

Ogranicz niezaufane port F0/18 na S2 do pięciu pakietów DHCP na sekundę.

```
S2(config)# interface f0/18
S2(config-if)# ip dhcp snooping limit rate 5
```

Sprawdź DHCP snooping na S2.

```
S2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/18           no         no              5
  Custom circuit-ids:
```

Z wiersza polecenia na PC-B zwolnij, a następnie odnownów adres IP.

```

```

```
C:\Users\Student> ipconfig /release
C:\Users\Student> ipconfig /renew
```

Zweryfikuj powiązanie DHCP snooping za pomocą polecenia show ip dhcp snooping binding.

```
S2# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------
--------
00:50:56:90:D0:8E   192.168.10.11    86213       dhcp-snooping   10
FastEthernet0/18
Total number of bindings: 1
```

Zaimplementuj PortFast i BPDU guard

Skonfiguruj PortFast na wszystkich portach dostępu, które są używane na obu przełącznikach.

```
S1(config)# interface range f0/5 - 6
S1(config-if)# spanning-tree portfast

S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast
```

Włącz ochronę BPDU na portach dostępowych S1 i S2 VLAN 10 podłączonych do PC-A i PC-B.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable
```

Sprawdź, czy BPDU Guard i PortFast są włączone na odpowiednich portach

```
S1# show spanning-tree interface f0/6 detail
 Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   <output omitted for brevity>
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 128, received 0
```

Wnioski

1. **Konfiguracja portów:**
    - Skonfigurowaliśmy interfejsy przełączników jako trunks, access ports oraz ustawiliśmy porty PortFast, co pozwala na szybsze nawiązywanie połączeń.
2. **Zabezpieczenia portów:**
    - Skonfigurowaliśmy port-security, aby ograniczyć dostęp do określonych adresów MAC na wybranych portach.
    - Wykorzystaliśmy różne poziomy zabezpieczeń, takie jak `restrict` i `protect`, aby reagować w różny sposób na ewentualne naruszenia.
3. **Zabezpieczenia DHCP Snooping:**
    - Włączyliśmy DHCP Snooping na przełączniku, co umożliwia filtrowanie i kontrolę ruchu DHCP w sieci.
    - Skonfigurowaliśmy limity ruchu DHCP na portach, aby zapobiec nadmiernemu ruchowi lub atakom.
4. **BPDU Guard:**
    - Wykorzystaliśmy BPDU Guard na wybranych portach, co pomaga w wykrywaniu błędów sieciowych i niedozwolonych urządzeń, które próbują wysyłać protokoły drzewa rozpinającego.
5. **Dokumentacja:**
    - Stworzyliśmy tabelę z domyślnymi ustawieniami zabezpieczeń portów, co stanowi dobry punkt odniesienia w przypadku ewentualnych zmian.
6. **Weryfikacja konfiguracji:**
    - Przeprowadziliśmy serię poleceń weryfikacyjnych, aby upewnić się, że konfiguracja została poprawnie zastosowana na przełącznikach.