Laboratorium - Konfiguracja zabezpieczeń przełącznika

Topologia sieci

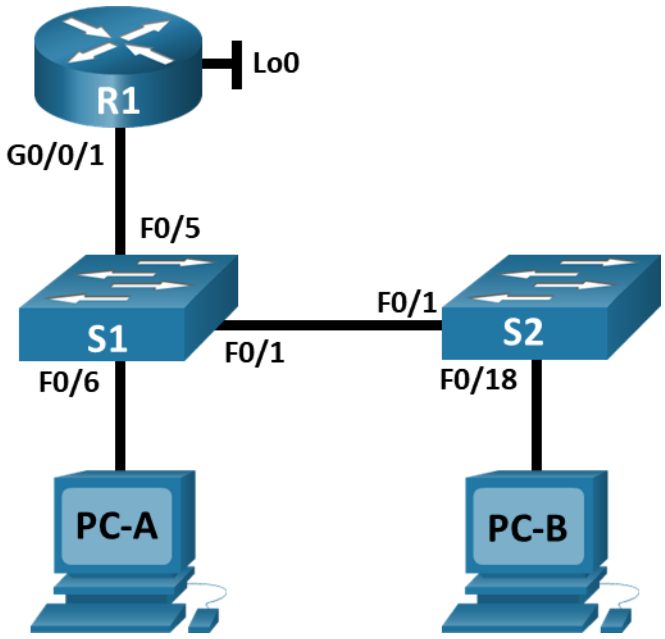

Tabela adresowania

Urządzenie	Interfejs / VLAN	Adres IP	Maska podsieci
R1	G0/0/1	192.168.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
Komputer A	karta sieciowa	DHCP	255.255.255.0
Komputer B	karta sieciowa	DHCP	255.255.255.0

Cele

Część 1: Konfiguracja urządzeń sieciowych

- Wykonaj okablowanie sieci.
- Skonfiguruj R1.
- Skonfiguruj i sprawdź podstawowe ustawienia przełącznika.

Część 2: Konfigurowanie sieci VLAN na przełącznikach.

- Skonfiguruj VLAN 10.
- Skonfiguruj SVI dla VLAN 10.
- Skonfiguruj VLAN 333 z nazwą Native na S1 i S2.
- Skonfiguruj VLAN 999 z nazwą ParkingLot na S1 i S2.

Część 3: Konfiguracja zabezpieczeń przełącznika.

- Zaimplementuj trunki 802.1Q.
- Skonfiguruj porty dostępu.
- Zabezpiecz i wyłącz nieużywane porty przełączników.
- Dokumentuj i zaimplementuj funkcje zabezpieczeń portów.
- Zaimplementuj zabezpieczenia DHCP snooping.
- Zaimplementuj PortFast i BPDU guard.
- Sprawdź łączność typu end-to-end.

Wprowadzenie

To obszerne laboratorium, w którym przerobiono wcześniej omówione funkcje zabezpieczeń warstwy 2.

Uwaga: Routery używane w laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.3 (obraz universalk9). Przełączniki używane w laboratoriach to Cisco Catalyst 2960 z Cisco IOS wydanie 15.0 (2) (obraz lanbasek9). Można używać Innych routerów lub przełączników oraz wersji Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, że konfiguracje przełączników zostały zresetowane oraz nie mają konfiguracji startowych. Jeśli nie jesteś pewien, to poproś o pomoc instruktora.

Wymagane zasoby

- 1 router (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.3 lub porównywalnym)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.0(2) image lanbasek9 lub porównywalny)
- 2 komputery PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez porty konsolowe
- Kable Ethernet zgodnie z przedstawioną topologią

Instrukcje

Część 1: Konfiguracja urządzeń sieciowych

Krok 1: Wykonaj okablowanie sieci.

a. Zbuduj sieć zgodnie z topologią.

b. Zainicjuj urządzenia.

Krok 2: Skonfiguruj R1.

a. Załaduj następujący skrypt konfiguracyjny na 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
```

b. Sprawdź bieżącą konfigurację na R1 za pomocą następującego polecenia:

```
R1# show ip interface brief
```

c. Sprawdź adresowanie IP i czy interfejsy są w stanie up / up (rozwiąż problemy w razie potrzeby).

Krok 3: Skonfiguruj i sprawdź podstawowe ustawienia przełącznika.

a. Skonfiguruj nazwę hosta dla przełączników S1 i S2.

b. Zapobieganie niepożądanym zapytaniom DNS na obu przełącznikach.

c. Skonfiguruj opisy interfejsów dla portów używanych w S1 i S2.

d. Ustaw bramę domyślną sieci VLAN zarządzania na 192.168.10.1 na obu przełącznikach.

Część 2: Skonfiguruj sieci VLAN na przełącznikach.

Krok 1: Skonfiguruj VLAN 10.

Dodaj VLAN 10 do S1 i S2 i nazwij go **Management**.

Krok 2: Skonfiguruj SVI dla VLAN 10.

Skonfiguruj adres IP zgodnie z tabelą adresowania dla SVI dla VLAN 10 na S1 i S2. Włącz interfejsy SVI i podaj opis interfejsu.

Krok 3: Skonfiguruj VLAN 333 z nazwą Native na S1 i S2.

Krok 4: Skonfiguruj VLAN 999 z nazwą ParkingLot na S1 i S2.

Część 3: Konfiguracja zabezpieczeń przełącznika.

Krok 1: Zaimplementuj trunki 802.1Q.

a. Na obu przełącznikach skonfiguruj trunk na F0/1, aby używał sieci VLAN 333 jako natywnej sieci VLAN.

b. Sprawdź, czy trunk jest skonfigurowany na obu przełącznikach.

```
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
```

c. Wyłącz negocjacje DTP na F0/1 na S1 i S2.

d. Sprawdź za pomocą polecenia **show interfaces**.

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

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

Krok 2: Skonfiguruj porty dostępu.

a. Na S1 skonfiguruj F0/5 i F0/6 jako porty dostępu skojarzone z siecią VLAN 10.

b. Na S2 skonfiguruj F0/18 jako port dostępu skojarzony z siecią VLAN 10.

Krok 3: Zabezpiecz i wyłącz nieużywane porty przełączników.

a. Na S1 i S2 przenieś nieużywane porty z sieci VLAN 1 do sieci VLAN 999 i wyłącz nieużywane porty.

b. Sprawdź, czy nieużywane porty są wyłączone i skojarzone z siecią VLAN 999, wydając polecenie **show** .

```
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
<output omitted>
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
<output omitted>
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
```

Krok 4: Dokumentuj i zaimplementuj funkcje zabezpieczeń portów.

Interfejsy F0/6 na S1 i F0/18 na S2 są skonfigurowane jako porty dostępu. W tym kroku można również skonfigurować zabezpieczenia portów na tych dwóch portach dostępu.

a. Na S1 wydaj polecenie **show port-security interface f0/6**, aby wyświetlić domyślne ustawienia zabezpieczeń portu dla interfejsu F0/6. Zanotuj swoje odpowiedzi w poniższych rubrykach.

Domyślna konfiguracja zabezpieczeń portu	
Funkcja	**Ustawienie domyślne**
Zabezpieczenie portu	
Maksymalna liczba bezpiecznych adresów MAC	
Tryb naruszenia	
Czas przedawnienia	
Rodzaj przedawnienia	
Przedawnienie bezpiecznego adresu statycznego	
Opcja Sticky adresów MAC	

b. 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**

c. Sprawdź zabezpieczenia portu F0/6 na S1.

```
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
```

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

e. Skonfiguruj następujące ustawienia zabezpieczeń portu f0/18 na S2:

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

f. Sprawdź zabezpieczenia portu F0/18 na S2.

```
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
```

Krok 5: Zaimplementuj zabezpieczenia DHCP snooping.

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

b. Skonfiguruj port trunk na S2 jako port zaufany.

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

d. 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:
```

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

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

f. 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
```

Krok 6: Zaimplementuj PortFast i BPDU guard.

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

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

c. 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
```

Krok 7: Zweryfikuj komunikację end-to-end.

Sprawdź łączność PING między wszystkimi urządzeniami w tabeli adresowania IP. Jeśli testy ping się nie powiedzą, może być konieczne wyłączenie zapory na hostach komputera.

Pytania refleksyjne

1. W odniesieniu do zabezpieczeń portów na S2, dlaczego nie ma wartości zegara przedawnienia w minutach, gdy skonfigurowano opcję uczenia Sticky?

2. W odniesieniu do zabezpieczeń portów na S2, jeśli załadujesz skrypt running-config na S2, dlaczego PC-B na porcie 18 nigdy nie otrzyma adresu IP przez DHCP?

3. W odniesieniu do zabezpieczeń portu, jaka jest różnica między bezwzględnym typem przedawnienia i typem przedawnienia w wyniku braku aktywności?