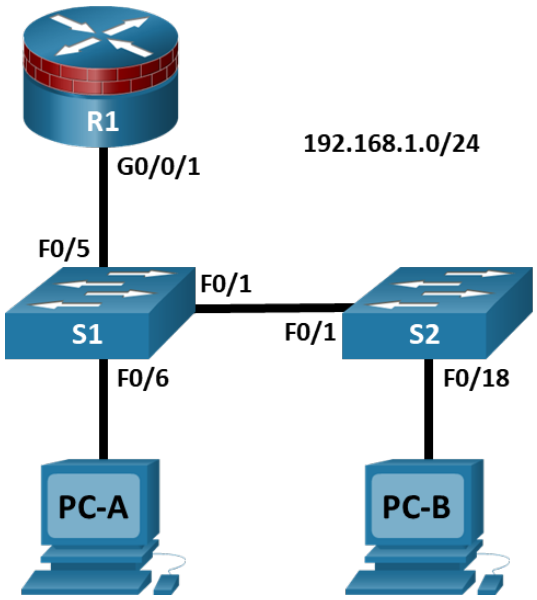
Cvičenie č. 8



Zariadenie	Rozhranie	IP adresa	Maska siete	Brána
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1

Úlohy

Časť 1: Konfigurácia základných nastavení prepínača

- Káblovanie topológie.
- Konfigurácia hostname, IP adries a prístupových hesiel.

Časť 2: Konfigurácia zabezpečených trunk rozhraní

- Konfigurácia rozhrania do trunk módu.
- Zmena natívnej VLAN pre trunk rozhrania.
- Overenie konfigurácie trunk.
- Zakázanie trunkovania.

Časť 3: Ochrana pred STP útokmi

- Konfigurácia PortFast a BPDU guard.
- Overenie BPDU guard.
- Konfigurácia root guard.
- Konfigurácia loop guard.

Časť 4: Konfigurácia port security a vypnutie nepoužívaných rozhraní

- Konfigurácia a overenie port security.
- Vypnutie nepoužívaných rozhraní.
- Prekonfigurovanie rozhraní z predvolenej VLAN 1 do alternatívnej VLAN.
- Konfigurácia PVLAN Edge na rozhraní.

O čo ide

L2 Infraštruktúra pozostáva hlavne z prepojených prepínačov (cez Ethernet). Väčšina zariadení koncových používateľov, ako sú počítače, tlačiarne, IP telefóny sa pripájajú do siete cez prístupové L2 prepínače. V dôsledku toho môžu prepínače predstavovať bezpečnostné riziko siete. Podobne ako pri smerovačoch, aj prepínače sú vystavené útokom zo strany interných používateľov.

V tomto cvičení si nakonfigurujete rôzne bezpečnostné funkcie na prepínačoch, vrátane zabezpečenia access rozhraní a STP bezpečnostných funcionalít (ako sú napríklad BPDU guard a root guard).

Zadanie

1. časť: Konfigurácia základných nastavení prepínača

V tejto časti urobíte topológiu a nakonfigurujete základné nastavenia, ako sú hostname, IP adresy a prístupové heslá.

1. krok: Káblovanie topológie.

Overte, že prepínač je v predvolenom nastavení `show running-config`, ak nie je zadajte `flash:empty`.

2. krok: Konfigurácia základných nastavení na smerovači a prepínači.

Vykonajte úlohy aj na R1, S1 a S2. Uvedený je len postup pre S1 (ako príklad).

Nakonfigurujte hostname podľa topológie.

Nakonfigurujte IP adresy rozhraní, podľa tabuľky na prvej strane. Nasledujúca konfigurácia zobrazuje rozhranie správy VLAN 1 na S1:

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
```

Zakážte preklad DNS na smerovači/prepínači pri preklade nesprávne zadaných príkazov. S1 ako príklad:

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

Nakonfigurujte šifrované heslo do privilegovaného módu:

```
S1(config)# enable secret cisco12345
```

Nakonfigurujte heslo do konzoly:

```
S1(config)# line console 0
S1(config-line)# password ciscoconpass
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
S1(config-line)# logging synchronous
```

3. krok: Nakonfigurujte sieťové nastavenia na PC

Nakonfigurujte statickú IP adresu, masku podsiete a predvolenú bránu na PC-A a PC-B tak, ako je uvedené v tabuľke vyššie.

4. krok: Overte základnú konektivitu

a. Ping z PC-A a PC-B na rozhranie G0/0/1 na R1 (IP adresa **192.168.1.1**).

Ak je ping neúspešný, pred pokračovaním odstráňte problém so základnou konfiguráciou.

b. Ping z PC-A na PC-B.

Ak je ping neúspešný, pred pokračovaním odstráňte problém so základnou konfiguráciou.

2. časť: Konfigurácia zabezpečených trunk rozhraní

V tejto časti nakonfigurujete trunk rozhrania, zmeníte natívnu VLAN pre trunk rozhrania a overíte konfiguráciu trunk.

Zabezpečenie trunk rozhraní môže pomôcť zastaviť VLAN hopping útoky. Najlepším spôsobom, ako zabrániť základnému VLAN hopping útoku je explicitne zakázať trunking na všetkých rozhraniach okrem portov, ktoré špecificky trunking vyžadujú. Na požadovaných rozhraniach v trunk móde deaktivujte DTP (auto trunking) a manuálne povoľte trunk. Ak sa na rozhraní nevyžaduje trunk, nakonfigurujte rozhranie ako access rozhranie. Tým zakážete trunking na rozhraní.

Poznámka: Úlohy by sa mali vykonať na S1 / S2.

1. krok: Nakonfigurujte S1 ako root switch.

S1 nakonfigurujete ako root bridge zmenou bridge ID priority.

a. Predvolená priorita na S1 a S2 je 32769 (32768 + 1 so system ID extension). Nastavte S1 prioritu na **0**, takže sa stane root prepínačom:

```
S1(config)# spanning-tree vlan 1 priority 0
S1(config)# exit
```

b. Zadajte príkaz **show spanning-tree** na overenie: že S1 je root bridge, na zobrazenie používaných portov a ich stavu:

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001d.4635.0c80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001d.4635.0c80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

Aká je priorita na S1?

Ktoré porty sa používajú a aký je ich stav?

2. krok: Konfigurácia rozhraní ako trunk na S1 a S2.

a. Nakonfigurujte rozhranie F0/1 na S1 ako trunk port:

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

Poznámka: Ak vykonávate toto cvičenie na prepínači rady 3560, používateľ musí najprv zadať príkaz **switchport trunk encapsulation dot1q**.

b. Nakonfigurujte rozhranie F0/1 na S2 ako trunk port:

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

c. Overte, že rozhranie F0/1 na S1 je v trunking móde, použitím príkazu **show interfaces trunk**:

```
S1# show interfaces trunk

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

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

3. krok: Zmeňte natívnu VLAN pre trunk rozhrania na S1 a S2.

a. Zmena natívnej VLAN pre trunk rozhrania do nepoužívanej VLAN pomáha predchádzať VLAN hopping útokom.

Z výstupu príkazu **show interfaces trunk** z minulého kroku, aká je aktuálna natívna VLAN na trunk rozhraní F0/1 na S1?

b. Nastavte natívnu VLAN na trunk rozhraní F0/1 prepínača S1 do nepoužívanej VLAN 99:

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

```
S1(config-if)# end
```

c. Po krátkom čase by sa mala zobraziť nasledujúca správa:

```
02:16:28: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (99), with S2 FastEthernet0/1 (1).
```

Čo správa znamená?

d. Nastavte natívnu VLAN na rozhraní S2 F0/1 do VLAN 99:

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# end
```

4. krok: Zabráňte použitiu DTP na S1 a S2

Nastavenie trunk portu na **nonegotiate** taktiež pomáha zmierniť VLAN hopping útoky, keďže vypne generovanie DTP rámcov:

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

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

5. krok: Overte konfiguráciu trunku na rozhraní F0/1.

```
S1# show interfaces f0/1 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

S1# show interfaces f0/1 switchport

Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 99 (Inactive)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

6. krok: Overte konfiguráciu pomocou show run príkazu.

Na zobrazenie bežiacej konfigurácie použite príkaz **show run**, začínajúc prvým riadkom, ktorý obsahuje textový reťazec „0/1“:

```
S1# show run | begin 0/1
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate

<output omitted>
```

7. krok: Zakážte trunking na access portoch na S1.

a. Na prepínači S1, nakonfigurujte rozhranie F0/5 (kde je napojený smerovač R1) do access módu:

```
S1(config)# interface f0/5
S1(config-if)# switchport mode access
```

b. Na prepínači S1, nakonfigurujte rozhranie F0/6 (kde je napojené PC-A) do access módu:

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
```

8. krok: Zakážte trunking na access portoch na S2.

Na prepínači S2, nakonfigurujte rozhranie F0/18 (kde je napojené PC-B) do access módu:

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

3. časť: Ochrana pred STP útokmi

Útočníci sa snažia zamaskovať (spoof) svoj systém alebo pridať podvodný (rogue) prepínač do siete tak, aby sa stal root bridge. Dosiahnúť to vedia manipuláciou STP root bridge parametrov. Ak rozhranie, ktoré je nakonfigurované ako PortFast, prijme BPDU, potom STP protokol dá rozhranie do blocking stavu. Zabezpečuje to funkcionalita nazývaná BPDU guard.

Topológia má iba dva prepínače a žiadne redundantné cesty, STP je však stále aktívny. V tejto časti povolíte funkcie zabezpečenia prepínačov, ktoré môžu pomôcť znížiť možnosti útočníka manipulovať s prepínačmi prostredníctvom metód súvisiacich s STP.

1. krok: Konfigurácia portfast.

PortFast sa konfiguruje na access portoch, ktoré sa pripájajú k jednej pracovnej stanici alebo serveru, čo im umožňuje rýchlejšie sa aktivovať.

a. Zapnite PortFast na access rozhraní F0/5 prepínača S1:

```
S1(config)# interface f0/5
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc... to this interface when
portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
 have effect when the interface is in a non-trunking mode.
```

b. Zapnite PortFast na access rozhraní F0/6 prepínača S1:

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

c. Zapnite PortFast na access rozhraní F0/18 prepínača S2:

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

2. krok: Konfigurácia BPDU guard.

BPDU guard je funkcionalita, ktorá môže pomôcť zabrániť podvodným (rogue) prepínačom a spoofingu na access rozhraniach.

a. Zapnite BPDU guard na rozhraní prepínača:

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

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

Poznámka: PortFast a BPDU guard je možné aktivovať aj globálne pomocou príkazov **spanning-tree portfast default** a **spanning-tree portfast bpduguard**.

Poznámka: BPDU guard je možné aktivovať na všetkých access rozhraniach, ktoré majú povolený PortFast. Na týchto rozhrania by nemalo byť BPDU nikdy prijaté. BPDU guard je najlepšie nasadiť na rozhraniach, kde sa pripája používateľ, čím sa útočníkom zabráni rozšíriť sieť o podovodné prepínače. Ak je na rozhraní konfigurovaný BPDU guard a rozhranie prijíme BPDU, potom bude rozhranie blokované a

musí sa povoliť manuálne. Na rozhraní je možné nakonfigurovať aj časový limit, po určitom časovom období sa rozhranie automaticky obnoví.

b. Overte, či je BPDU guard nakonfigurovaný za použitia príkazu **show spanning-tree interface f0/6 detail** na S1:

```
S1# show spanning-tree interface f0/6 detail

Port 6 (FastEthernet0/6) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   Designated root has priority 1, address 001d.4635.0c80
   Designated bridge has priority 1, address 001d.4635.0c80
   Designated port id is 128.6, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   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 3349, received 0
```

3. krok: Konfigurácia root guard.

Root guard je ďalšou možnosťou, ako zabrániť podvodným prepínačom a spoofingu. Root guard je možné povoliť na všetkých rozhraniach na prepínači, ktoré nie sú root portami. Bežne sa povoľuje iba na rozhraniach, ktoré sa pripájajú k okrajovým prepínačom, kde by nemalo byť nikdy prijaté nadradené BPDU. Každý prepínač by mal mať iba jeden root port, čo predstavuje najlepšiu cestu ku root prepínaču.

a. Nasledujúci príkaz nakonfiguruje root guard na rozhraní G0/1 prepínača S2. Zvyčajne sa to robí, ak je k tomuto portu pripojený ďalší prepínač. Root guard je najlepšie nasadiť na rozhrania, ktoré sa pripájajú k prepínačom, ktoré by nemali byť root bridge. V topológii by bol S1 F0/1 najlogickejším kandidátom pre root guard. Ako príklad je tu zobrazený S2 G0/1, keďže gigabitové porty sa používajú častejšie na prepojenie medzi prepínačmi:

```
S2(config)# interface g0/1
S2(config-if)# spanning-tree guard root
```

b. Zadajte príkaz **show run | begin Gig** a overte konfiguráciu root guard:

```
S2# show run | begin Gig
interface GigabitEthernet0/1
 spanning-tree guard root
```

Poznámka: Rozhranie S2 Gi0/1 momentálne nie je aktívne, takže sa nezúčastňuje v STP. V opačnom prípade by bolo možné použiť príkaz **show spanning-tree interface Gi0/1 detail**.

c. Ak rozhranie, kde je povolené BPDU guard, prijme nadradené BPDU, dostane sa do root-inconsistent stavu. Použite príkaz **show spanning-tree inconsistentports** na určenie, či existujú nejaké rozhrania, ktoré momentálne prijímajú nadradené BPDU:

```
S2# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
Number of inconsistent ports (segments) in the system : 0
```

Poznámka: Root guard umožňuje pripojenému prepínaču zúčastniť sa v STP, pokiaľ sa zariadenie nepokúša stať sa rootom. Ak root guard blokuje port, následné obnovenie sa je automatické. Rozhranie sa vráti do operačného stavu, ak sa príjem nadradených BPDU zastaví.

4. krok: Konfigurácia loop guard (potrebné overiť či konfigurácia bude na reálnom zariadení fungovať).

Funkcia STP loop guard poskytuje dodatočnú ochranu pred L2 slučkami (STP slučky). STP slučka sa vytvorí, ak STP blocking port v redundantnej topológii chybne prejde do forwarding stavu. To sa zvyčajne stáva, ak jeden z portov fyzicky redundantnej topológie (nie nevyhnutne STP blocking port) už neprijíma STP BPDU. Ak budú všetky porty vo forwarding stave, dôjde k slučkám. Ak rozhranie s aktivovaným loopguard prestane príjmať BPDU, prejde do loop nekonzistentného stavu namiesto prechodu do forwarding stavu. Nekonzistentný (loop inconsistent) stav je v podstate blokovanie a nepreposiela žiadnu prevádzku. Keď port opäť deteguje BPDU, potom sa automaticky obnoví (prejde späť do stavu blokovania).

a. Loop guard by sa malo použiť na non-designated rozhraniach. Preto je možné použiť globálny príkaz na non-root prepínačoch:

```
S2(config)# spanning-tree loopguard default
```

b. Overenie loopguard konfigurácie:

```
S2# show spanning-tree summary
Switch is in pvst mode

Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          3          3
---------------------- -------- --------- -------- ---------- ---------
```

4. časť: Konfigurácia port security a vypnutie nepoužívaných rozhraní

Prepínače môžu podliehať CAM table útokom (známe aj ako tabuľka MAC adries), pretečeniu, MAC spoofing útokom a neoprávneným pripojeniam k rozhraniam prepínača. V tejto úlohe nakonfigurujete zabezpečenie rozhraní (port security), čím obmedzíte počet MAC adries (ktoré je možné naučiť sa na rozhraní prepínača, pričom sa po jeho prekročení rozhranie deaktivuje).

1. krok: Zaznamenajte MAC adresu na R1 G0/0/1.

Na R1, použite príkaz **show interface** a poznačte si MAC adresu rozhrania:

```
R1# show interfaces g0/0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia fc99.4775.c3e1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

```
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
<Output Omitted>
```

Aká je MAC adresa rozhrania R1 G0/0/1?

2. krok: Konfigurácia základnej port security.

Tento postup by sa mal vykonať na všetkých access portoch, ktoré sa používajú (are in use). Ako príklad je tu zobrazené rozhranie F0/5 na S1.

a. Na S1 vstúpte do konfigurácie rozhrania, ktoré sa pripája na smerovač (Fast Ethernet 0/5):

```
S1(config)# interface f0/5
```

b. Vypnite rozhranie na prepínači:

```
S1(config-if)# shutdown
```

c. Aktivujte port security na rozhraní:

```
S1(config-if)# switchport port-security
```

Poznámka: Rozhranie prepínača musí byť nakonfigurované ako access port, čím sa umožní port security.

Poznámka: Zadanie príkazu **switchport port-security** predvolene nastaví maximálny počet MAC adries na **1** a mód naručenia na **shutdown**. Príkazy **switchport port-security maximum** a **switchport port-security violation** je možné použiť na zmenu predvoleného správania.

d. Nakonfigurujte statický záznam MAC adresy (poznačenej v 1. kroku z rozhrania G0/0/1 smerovača R1):

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

Poznámka: *xxxx.xxxx.xxxx* je skutočná MAC adresa rozhrania smerovača G0/0/1.

Poznámka: Môžete taktiež použiť príkaz **switchport port-security mac-address sticky** na pridanie všetkých zabezpečených MAC adries, ktoré sa dynamicky naučia na rozhraní (až do maximálne povolenej hodnoty) a uložia do bežiacej konfigurácie prepínača.

e. Aktivujte rozhranie na prepínači:

```
S1(config-if)# no shutdown
```

3. krok: Overte port security na F0/5 prepínača S1

a. Na prepínači S1, zadajte príkaz **show port-security** a overte port security konfigurovaný na S1 F0/5:

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Aká je hodnota Security Violation Count?

Aký je stav F0/5 rozhrania?

Aká je Last Source Address a VLAN?

b. Na smerovači R1, zadajte ping na PC-A (overenie konektivity). Tým sa zabezpečí, že sa prepínač naučí MAC adresu rozhrania G0/0/1 na smerovači R1:

```
R1# ping 192.168.1.10
```

c. Teraz narušte bezpečnosť zmenou MAC adresy na rozhraní smerovača. Vôjdite do konfigurácie rozhrania na Fast Ethernet 0/1. Nakonfigurujte MAC adresu na rozhraní na rozhraní pomocou **aaaa.bbbb.cccc** ako adresy (potrebné overiť či konfigurácia bude na reálnom zariadení fungovať):

```
R1(config)# interface g0/0/1
R1(config-if)# mac-address aaaa.bbbb.cccc
R1(config-if)# end
```

Poznámka: Môžete tiež zmeniť adresu MAC počítača pripojenú k S1 F0/6 a dosiahnuť podobné výsledky.

Zo smerovača R1, realizujte ping na PC-A. Bol ping úspešný?

d. Sledujte správy v konzole prepínača S1, keď port F0/5 deteguje MAC adresu (ktorá vyvolá narušenie):

```
*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5,
putting Fa0/5 in err-disable state
*Jan 14 01:34:39.750: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address aaaa.bbbb.cccc on port FastEthernet0/5.
*Jan 14 01:34:40.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5,
changed state to down
*Jan 14 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
```

e. Na prepínači použite príkaz **show port-security**, čím overíte narušenie port security:

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
```

```
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:1
Security Violation Count   : 1

S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    fc99.4775.c3e1    SecureConfigured              Fa0/5        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

f. Odstráňte nakonfigurovanú MAC adresu zo smerovača na rozhraní G0/0/1:

```
R1(config)# interface g0/0/1
R1(config-if)# no mac-address aaaa.bbbb.cccc
```

Poznámka: Týmto sa obnoví pôvodná MAC adresa rozhrania GigabitEthernet.

Zo smerovača R1 sa opäť pokúste pingnúť PC-A (192.168.1.10). Bol ping úspešný?

4. krok: Odstránenie stavu rozhrania F0/5 „error disabled“ na prepínači S1.

a. Cez konzolu na S1 odstráňte error a opäť povoľte rozhranie pomocou príkazov uvedených v príklade nižšie. Tým sa zmení stav portu zo Secure-shutdown na Secure-up.

```
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Poznámka: To predpokladá, že zariadenie/rozhranie s porušujúcou MAC adresou bolo odstránené a nahradené pôvodnou konfiguráciou zariadenia/rozhrania.

b. Zo smerovača R1 opäť realizujte ping na PC-A. Tentoraz by mal byť úspešný.

```
R1# ping 192.168.1.10
```

5. krok: Odstráňte základnú port security na S1 F0/5.

Cez konzolu na S1 odstráňte zabezpečenie rozhrania na F0/5. Tento postup je možné použiť aj na opätovné zapnutie rozhrania, ale **port security** príkazy sa musia prekonfigurovať.

```
S1(config)# interface f0/5
S1(config-if)# no switchport port-security
S1(config-if)# no switchport port-security mac-address fc99.4775.c3e1
```

Na obnovenie predvolených nastavení rozhrania môžete použiť aj nasledujúce príkazy:

```
S1(config)# default interface f0/5
S1(config)# interface f0/5
```

Poznámka: Tento **default interface** príkaz tiež vyžaduje, aby ste prekonfigurovali rozhranie ako access port, čo umožní znovu zadanie príkazov zabezpečenia.

6. krok: Nakonfigurujte zabezpečenie rozhrania pre VoIP

Tento príklad ukazuje typickú konfiguráciu zabezpečenia portu pre hlasové rozhrania. Povolené sú tri MAC adresy a mali by sa učiť dynamicky. Jedna MAC adresa je pre IP telefón, jedna pre prepínač a jedna pre PC pripojený k IP telefónu. Porušenie tejto politiky má za následok vypnutie rozhrania. Časový limit starnutia naučených MAC adries (port aging) je nastavený na dve hodiny.

Nasledujúci príkaz zobrazuje rozhranie F0/18 na prepínači S2:

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 3
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security aging time 120
```

7. krok: Vypnutie nepoužívaných rozhraní na S1 a S2.

Ako ďalšie bezpečnostné opatrenie zakážte rozhrania, ktoré sa na prepínači nepoužívajú.

a. Na prepínači S1 sa používajú rozhrania F0/1, F0/5 a F0/6. Zostávajúce rozhrania Fast Ethernet a dve rozhrania Gigabit Ethernet budú vypnuté.

```
S1(config)# interface range f0/2 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
```

b. Na prepínači S2 sa používajú rozhrania F0/1 a F0/18. Zostávajúce rozhrania Fast Ethernet a Gigabit Ethernet budú vypnuté.

```
S2(config)# interface range f0/2 – 17, f0/19 – 24, g0/1 - 2
S2(config-if-range)# shutdown
```

8. krok: Presuňte aktívne rozhrania do inej ako predvolenej VLAN 1.

Ako ďalšie bezpečnostné opatrenie môžete presunúť všetky aktívne rozhrania koncových používateľov a rozhrania pripajajúce sa na smerovač do inej VLAN, ako je predvolená VLAN 1 (na oboch prepínačoch).

a. Nakonfigurujte novú VLAN pre používateľov na každom prepínači pomocou nasledujúcich príkazov:

```
S1(config)# vlan 20
S1(config-vlan)# name Users

S2(config)# vlan 20
S2(config-vlan)# name Users
```

b. Pridajte aktuálne aktívne access (non-trunk) rozhrania do novej VLAN.

```
S1(config)# interface f0/6
```

```
S1(config-if-range)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20
```

Poznámka: Týmto sa zabráni komunikácii medzi zariadeniam koncových používateľov a IP adresou VLAN pre správu prepínača, ktorá je momentálne VLAN 1. K prepínaču je stále možné pristupovať a konfigurovať ho cez konzolu.

Poznámka: Na poskytnutie SSH prístupu k prepínaču je možné určiť špecifické rozhranie pre správu a pridať ho do VLAN 1 (s pripojenou špecifickou pracovnou stanicou pre správu). Prepracovanejším riešením je vytvorenie novej VLAN pre správu prepínača (alebo použitie existujúcej natívnej trunkovej VLAN 99) a konfigurácia samostatnej podsiete pre manažmentovú a používateľskú VLAN.

9. Konfigurácia rozhrania s funkcionalitou PVLAN Edge

Niektoré nasadenia vyžadujú, aby sa na 2. vrstve medzi rozhraniami na rovnakom prepínači nepresmerovala žiadna prevádzka, aby jeden sused nevidel prevádzku generovanú iným susedom. V takomto prostredí sa použije funkcia Private VLAN (PVLAN) Edge, známa aj ako protected ports, ktorá zaisťuje, že medzi týmito rozhraniami na prepínači nedochádza k výmene unicast, broadcast alebo multicast prevádzky. Funkciu PVLAN Edge je možné implementovať iba pre rozhrania na rovnakom prepínači a je lokálne signifikantná.

Ak chcete napríklad zabrániť prenosu medzi PC-A na S1 (port F0/6) a zariadením na inom S1 rozhraní (napr. port F0/7, ktorý bol predtým vypnutý), môžete použiť príkaz **switchport protected** na aktiváciu PVLAN Edge na týchto dvoch portoch. Na deaktiváciu chráneného portu použite konfiguračný príkaz **no switchport protected**.

a. Nakonfigurujte PVLAN Edge v režime konfigurácie rozhrania pomocou nasledujúcich príkazov:

```
S1(config)# interface f0/6
S1(config-if)# switchport protected
S1(config-if)# interface f0/7
S1(config-if)# switchport protected
S1(config-if)# no shut
S1(config-if)# end
```

b. Overte, že PVLAN Edge (protected port) je na rozhraní F0/6 povolené:

```
S1# show interfaces f0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 20 (Users)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
```

```
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

c. Deaktivujte protected port na rozhraniach F0/6 a F0/7 pomocou nasledujúcich príkazov:

```
S1(config)# interface range f0/6 - 7
S1(config-if-range)# no switchport protected
```