**10.1.1 Network Attacks Today**

**Distribuit Denial of Service (DDoS)** - Acesta este un atac coordonat de la multe dispozitive, numite zombi, cu intenția de a degrada sau opri accesul public la site-ul și resursele unei organizații.

**Încălcarea datelor** - Acesta este un atac în care serverele de date sau gazdele unei organizații sunt compromise pentru a fura informații confidențiale.

Malware - Acesta este un atac în care gazdele unei organizații sunt infectate cu software rău intenționat care cauzează o varietate de probleme.

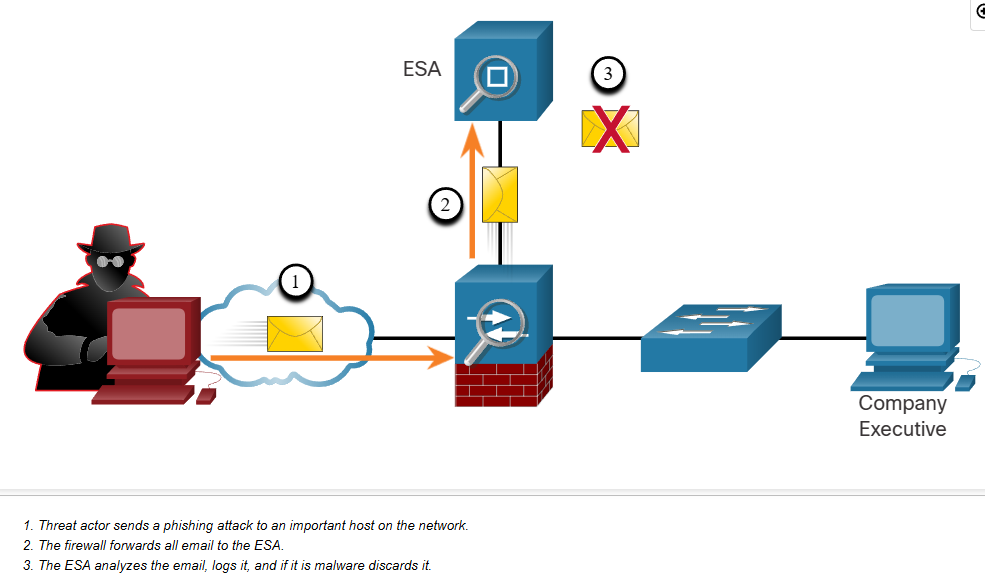
**10.1.2 Network Security Devices**

VPN router – acces de la disnta prin retea publica in retea private

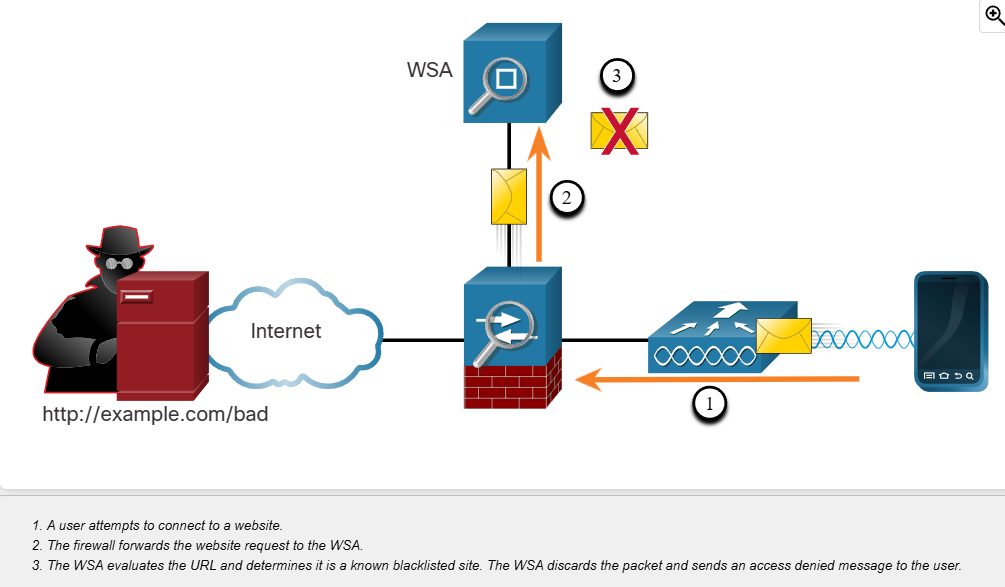
NGFW inspectia complete a pachetelr

Un dispozitiv NAC include servicii de autentificare, autorizare și contabilitate (AAA).

**Cisco ESA** este un dispozitiv conceput pentru a monitoriza protocolul SMTP (Simple Mail Transfer Protocol).



**Cisco WSA** oferă control complet asupra modului în care utilizatorii accesează internetul. Anumite funcții și aplicații, cum ar fi chat, mesagerie, video și audio, pot fi permise, restricționate cu limite de timp și lățime de bandă sau blocate, în funcție de cerințele organizației.



**10.2.1 Authentication with a Local Password**

**SSH** este o formă mai sigură de acces la distanță: Necesită un nume de utilizator și o parolă, ambele fiind criptate în timpul transmiterii.

R1(config)# **ip domain-name example.com**

R1(config)# **crypto key generate rsa general-keys modulus 2048**

R1(config)# **username Admin secret Str0ng3rPa55w0rd**

R1(config)# **ip ssh version 2**

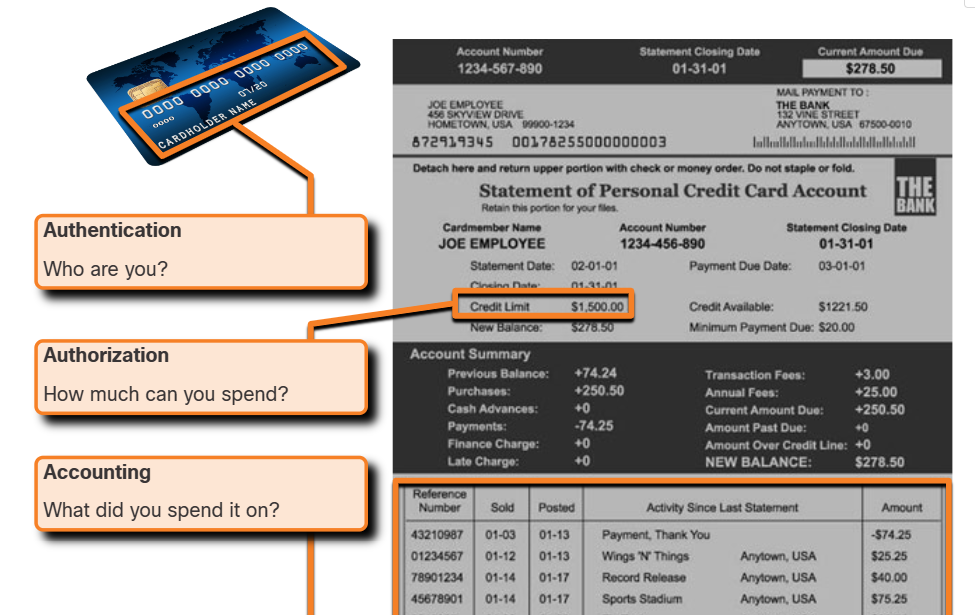
R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

R1(config-line)# **login local**

**10.2.2 AAA Components**

AAA înseamnă Autentificare(acces), Autorizare(restrictii) și Contabilitate(ce a facut). (Authentication, Authorization, Accounting)



**10.2.3 Authentication**

- Local AAA Authentication

- Server-Based AAA Authentication

**10.2.4 Authorization**

Autorizarea guvernează ce pot și nu pot face utilizatorii în rețea după ce sunt autentificați.

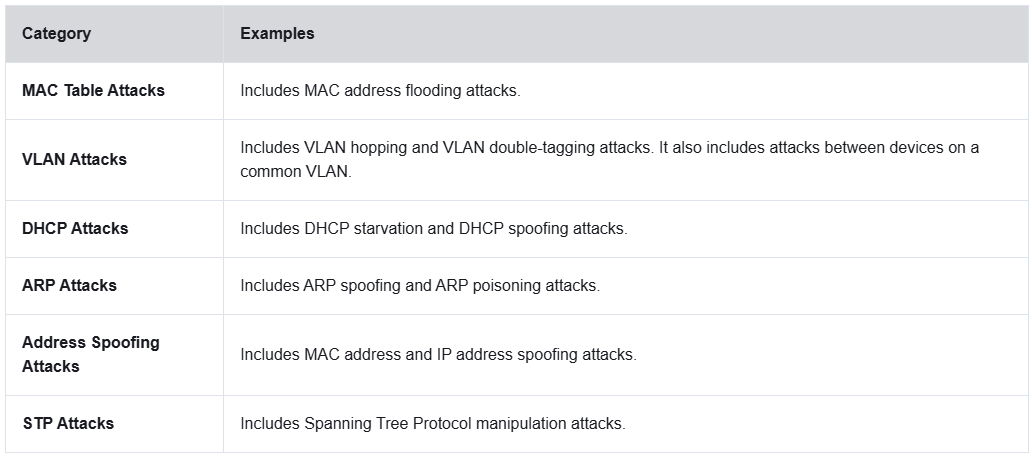
**10.2.5 Accounting**

Contabilitatea AAA colectează și raportează date de utilizare.

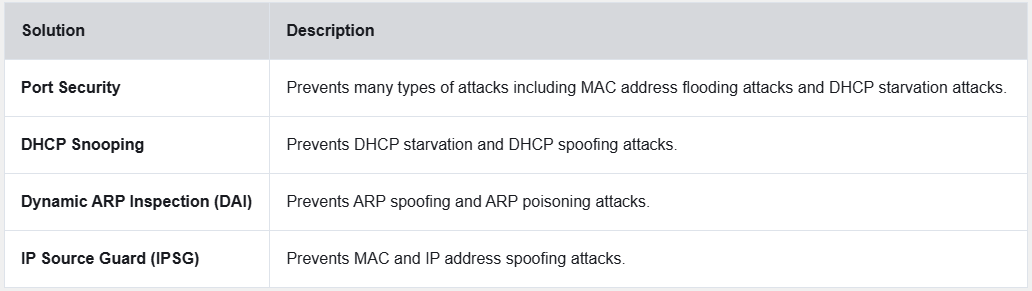
**10.2.6 802.1X**

Standardul IEEE 802.1X este un protocol de autentificare și control al accesului bazat pe porturi. Acest protocol restricționează stațiile de lucru neautorizate să se conecteze la o rețea LAN prin porturi de comutare accesibile public.

**Layer 2 Attacks**



**Layer 2 Attack Mitigation**



Tabelele de adrese MAC sunt stocate în memorie și sunt folosite pentru a transmite mai eficient cadrele.

S1# **show mac address-table dynamic**

          Mac Address Table

-------------------------------------------

Vlan    Mac Address       Type        Ports

----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4

   1    000a.f38e.74b3    DYNAMIC     Fa0/1

   1    0090.0c23.ceca    DYNAMIC     Fa0/3

   1    00d0.ba07.8499    DYNAMIC     Fa0/2

S1#

**10.4.2 MAC Address Table Flooding**

Atacurile de inundare a adreselor MAC profită de limitare tabelului de adrese MAC bombardând comutatorul cu adrese MAC sursă false până când tabelul de adrese MAC al comutatorului este plin. Când se întâmplă acest lucru, comutatorul tratează cadrul ca un unicast necunoscut și începe să inunde tot traficul de intrare în toate porturile de pe același VLAN fără a face referire la tabelul MAC

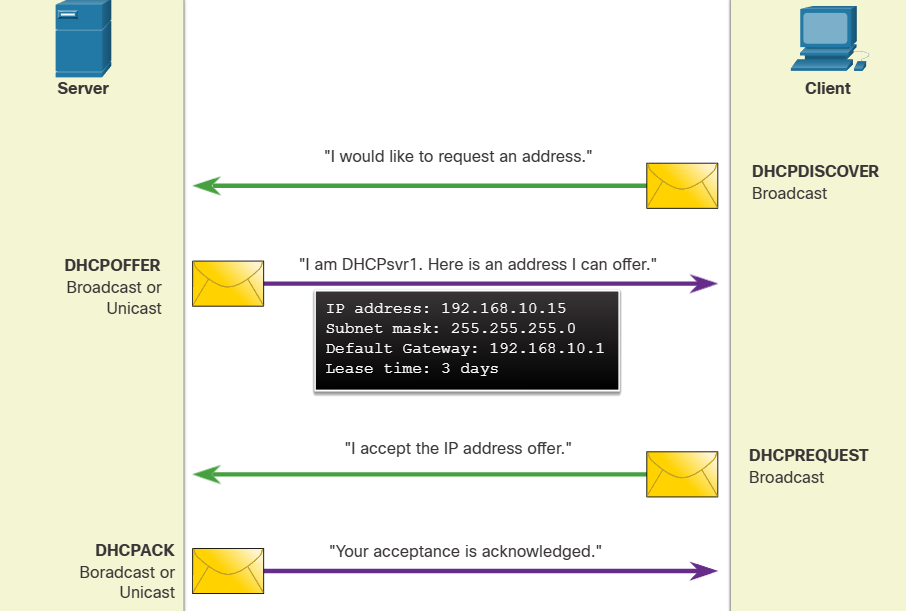
**10.5.2 VLAN Hopping Attacks**

Un atac de salt VLAN permite traficul de la un VLAN să fie văzut de un alt VLAN fără ajutorul unui router. Într-un atac de bază de salt VLAN, actorul amenințării configurează o gazdă să acționeze ca un comutator pentru a profita de funcția de port trunking automat activată în mod implicit pe majoritatea porturilor de comutare

**10.5.3 VLAN Double-Tagging Attack**

Un actor de amenințare în situații specifice ar putea încorpora o etichetă 802.1Q ascunsă în interiorul cadrului care are deja o etichetă 802.1Q.

**10.5.4 DHCP Messages**



**10.5.5 DHCP Attacks**

- **DHCP Starvation Attack** : Scopul atacului DHCP Starvation este de a crea un DoS pentru conectarea clienților. Atacurile de foame DHCP necesită un instrument de atac precum Gobbler. Gobbler are capacitatea de a analiza întregul domeniu al adreselor IP care pot fi închiriate și încearcă să le închirieze pe toate. Mai exact, creează mesaje de descoperire DHCP cu adrese MAC false.

**- DHCP Spoofing Attack** : Un atac de falsificare DHCP are loc atunci când un server DHCP nepoliticos este conectat la rețea și oferă parametri de configurare IP falși clienților legitimi.

**10.5.7 ARP Attacks**

Problema este că un atacator poate trimite un mesaj ARP gratuit care conține o adresă MAC falsificată către un comutator, iar comutatorul își va actualiza tabelul MAC în consecință. Prin urmare, orice gazdă poate pretinde că este proprietarul oricărei combinații de adrese IP și MAC pe care o alege. Într-un atac tipic, un actor de amenințare poate trimite răspunsuri ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IPv4 a gateway-ului implicit.

**10.5.8 Address Spoofing Attack**

Falsificarea adresei IP este atunci când un actor de amenințări deturnează o adresă IP validă a unui alt dispozitiv din subrețea sau folosește o adresă IP aleatorie.

**10.5.9 STP Attack**

Atacatorii de rețea pot manipula protocolul Spanning Tree (STP) pentru a efectua un atac prin falsificarea podului rădăcină și modificarea topologiei unei rețele. Atacatorii își pot face gazdele să apară ca punți rădăcină; și, prin urmare, capturați tot traficul pentru domeniul comutat imediat.

This STP attack is mitigated by implementing BPDU Guard on all access ports.

**10.5.10 CDP Reconnaissance**

CDP poate descoperi automat alte dispozitive compatibile cu CDP și poate ajuta la configurarea automată a conexiunii acestora. Emisiunile CDP sunt trimise necriptate și neautentificate.

Pentru a dezactiva global CDP pe un dispozitiv, utilizați comanda **no cdp run** global configuration mode. Pentru a activa CDP la nivel global, utilizați comanda **cdp run** global configuration.

Pentru a dezactiva CDP pe un port, utilizați comanda de configurare a interfeței **no cdp enable**. Pentru a activa CDP pe un port, utilizați comanda de configurare a interfeței **cdp enable**.

Protocolul Link Layer Discovery (LLDP) este, de asemenea, vulnerabil la atacurile de recunoaștere. Configurați **no lldp run** pentru a dezactiva LLDP la nivel global. Pentru a dezactiva LLDP pe interfață, configurați **no lldp transmit** si **no lldp receive**..

**11.1.2 Mitigate MAC Address Table Attacks**

Cea mai simplă și eficientă metodă de a preveni atacurile de depășire a tabelului de adrese MAC este activarea securității porturilor. Securitatea porturilor limitează numărul de adrese MAC valide permise pe un port.

**11.1.3 Enable Port Security**

S1(config)# **interface f0/1**

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

Command rejected: FastEthernet0/1 is a dynamic port.

S1(config-if)# **switchport mode access**

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

S1(config-if)# **end**

S1#

Utilizați comanda show port-security interface pentru a afișa setările curente de securitate a portului pentru FastEthernet 0/1.

S1# **show port-security interface f0/1**

Port Security              : Enabled

Port Status                : Secure-down

Violation Mode             : Shutdown

Aging Time                 : 0 mins

Aging Type                 : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses      : 1

Total MAC Addresses        : 0

Configured MAC Addresses   : 0

Sticky MAC Addresses       : 0

Last Source Address:Vlan   : 0000.0000.0000:0

Security Violation Count   : 0

S1#

S1(config-if)# **switchport port-security ?**

  aging        Port-security aging commands

  mac-address  Secure mac address

  maximum      Max secure addresses

  violation    Security violation mode

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

**11.1.4 Limit and Learn MAC Addresses**

Switch(config-if)# **switchport port-security maximum** value

The default port security value is 1. The maximum number of secure MAC addresses that can be configured depends the switch and the IOS. In this example, the maximum is 8192.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security maximum ?**

  <1-8192>  Maximum addresses

S1(config-if)# **switchport port-security maximum**

Comutatorul poate fi configurat pentru a afla despre adresele MAC pe un port securizat într-unul din trei moduri:

1. Manually Configured

Switch(config-if)# **switchport port-security mac-address** mac-address

1. Manually ConfiguredDynamically Learned

Când este introdusă comanda switchport port-security, sursa MAC curentă pentru dispozitivul conectat la port este securizată automat, dar nu este adăugată la configurația de pornire. Dacă comutatorul este repornit, portul va trebui să învețe din nou adresa MAC a dispozitivului.

1. ManuaDynamically Learned – Stickylly ConfiguredDynamically Learned

Switch(config-if)# **switchport port-security mac-address sticky**

Salvarea configurației de rulare va trimite adresa MAC învățată dinamic la NVRAM.

Ecemplu :  
\*Mar  1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar  1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1#**conf t**

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

S1(config)#

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

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

S1(config-if)# **switchport port-security maximum 2**

S1(config-if)# **switchport port-security mac-address aaaa.bbbb.1234**

S1(config-if)# **switchport port-security mac-address sticky**

S1(config-if)# **end**

S1# **show port-security interface fa0/1**

Port Security              : Enabled

Port Status                : Secure-up

Violation Mode             : Shutdown

Aging Time                 : 0 mins

Aging Type                 : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses      : 2

Total MAC Addresses        : 2

Configured MAC Addresses   : 1

Sticky MAC Addresses       : 1

Last Source Address:Vlan   : a41f.7272.676a:1

Security Violation Count   : 0

S1# **show port-security address**

               Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan    Mac Address       Type                          Ports   Remaining Age

                                                                   (mins)

----    -----------       ----                          -----   -------------

1    a41f.7272.676a    SecureSticky                  Fa0/1        -

1    aaaa.bbbb.1234    SecureConfigured              Fa0/1        -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port)     : 1

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

S1#

**11.1.5 Port Security Aging**

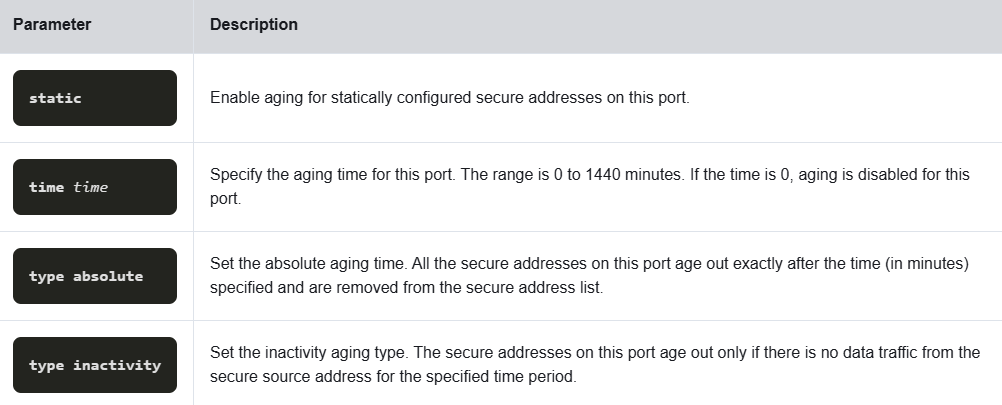
Îmbătrânirea securității porturilor poate fi utilizată pentru a seta timpul de îmbătrânire pentru adresele securizate statice și dinamice pe un port. Două tipuri de îmbătrânire sunt acceptate pentru fiecare port:

1. **Absolut** - Adresele securizate de pe port sunt șterse după perioada de vechime specificată.
2. **Inactivitate** - Adresele securizate de pe port sunt șterse numai dacă sunt inactive pentru perioada de vechime specificată.

Utilizați vechimea pentru a elimina adresele MAC securizate de pe un port securizat fără a șterge manual adresele MAC securizate existente.

Utilizați comanda **switchport port-security aging** pentru a activa sau dezactiva îmbătrânirea statică pentru portul securizat sau pentru a seta timpul sau tipul de îmbătrânire.

Switch(config-if)# **switchport port-security aging** { **static** | **time** time | **type** {**absolute** | **inactivity**}



**Adresele MAC sunt afișate ca 24 de biți pentru simplitate.**

Exemplul arată un administrator care configurează tipul de vechime la 10 minute de inactivitate și utilizând comanda show port-security interface pentru a verifica configurația.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport port-security aging time 10**

S1(config-if)# **switchport port-security aging type inactivity**

S1(config-if)# **end**

S1# **show port-security interface fa0/1**

Port Security              : Enabled

Port Status                : Secure-up

Violation Mode             : Shutdown

Aging Time                 : 10 mins

Aging Type                 : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses      : 2

Total MAC Addresses        : 2

Configured MAC Addresses   : 1

Sticky MAC Addresses       : 1

Last Source Address:Vlan   : a41f.7272.676a:1

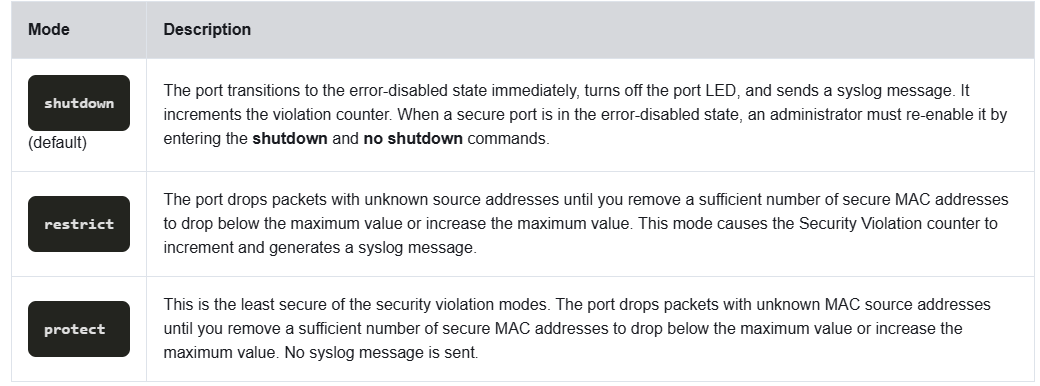
Security Violation Count   : 0

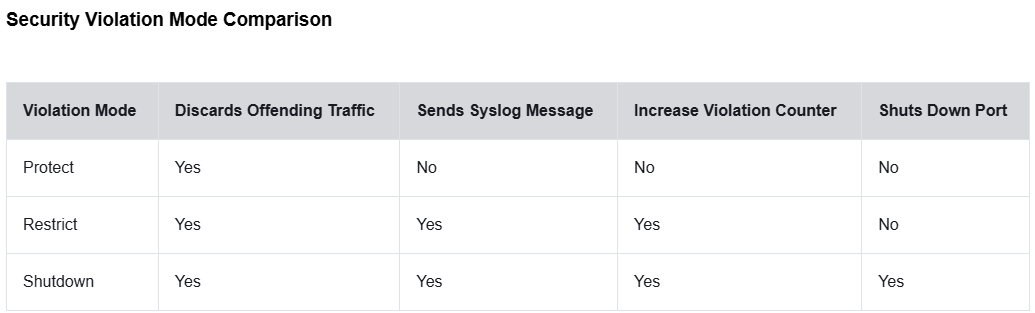
S1#

**11.1.6 Port Security Violation Modes**

Dacă adresa MAC a unui dispozitiv atașat la port diferă de lista de adrese securizate, atunci are loc o încălcare a portului. În mod implicit, portul intră în starea dezactivată de eroare. Pentru a seta modul de încălcare a securității porturilor, utilizați următoarea comandă:

Switch(config-if)# **switchport port-security violation** { **protect** | **restrict** | **shutdown**}





Următorul exemplu arată un administrator care modifică încălcarea securității în „restricționare”. Ieșirea comenzii show port-security interface confirmă că modificarea a fost făcută.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security violation restrict**

S1(config-if)# **end**

S1#

S1# **show port-security interface f0/1**

Port Security              : Enabled

Port Status                : Secure-up

Violation Mode             : Restrict

Aging Time                 : 10 mins

Aging Type                 : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses      : 2

Total MAC Addresses        : 2

Configured MAC Addresses   : 1

Sticky MAC Addresses       : 1

Last Source Address:Vlan   : a41f.7272.676a:1

Security Violation Count   : 0

**11.1.7 Ports in error-disabled State**

Ce se întâmplă când încălcarea securității portului este oprită și are loc o încălcare a portului?Portul este oprit fizic și plasat în starea dezactivată de eroare și nu este trimis sau primit niciun trafic pe acel port.

În figură, încălcarea securității portului este schimbată înapoi la setarea implicită de oprire. Apoi gazda cu adresa MAC a41f.7272.676a este deconectată și o nouă gazdă este conectată la Fa0/1.

S1(config)# **int fa0/1**

S1(config-if)# **switchport port-security violation shutdown**

S1(config-if)# **end**

S1#

\*Mar  1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar  1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

\*Mar  1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar  1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1#

\*Mar  1 00:24:32.829: %PM-4-ERR\_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state

\*Mar  1 00:24:32.838: %PORT\_SECURITY-2-PSECURE\_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.

\*Mar  1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar  1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

În exemplu, comanda show interface identifică starea portului ca fiind err-disabled. Ieșirea comenzii show port-security interface arată acum starea portului ca Secure-shutdown în loc de Secure-up. Contorul de încălcări de securitate crește cu 1.

S1# **show interface fa0/1 | include down**

FastEthernet0/18 is down, line protocol is down (err-disabled)

(output omitted)

S1# **show port-security interface fa0/1**

Port Security              : Enabled

Port Status                : Secure-shutdown

Violation Mode             : Shutdown

Aging Time                 : 10 mins

Aging Type                 : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses      : 2

Total MAC Addresses        : 2

Configured MAC Addresses   : 1

Sticky MAC Addresses       : 1

Last Source Address:Vlan   : a41f.7273.018c:1

Security Violation Count   : 1

S1#

În exemplul următor, prima gazdă este reconectată la Fa0/1. Pentru a reactiva portul, utilizați mai întâi comanda shutdown, apoi folosiți comanda no shutdown pentru a face portul operațional, așa cum se arată în exemplu.

S1(config)# **interface fa0/1**

S1(config-if)# **shutdown**

S1(config-if)#

\*Mar  1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

S1(config-if)# **no shutdown**

S1(config-if)#

\*Mar  1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar  1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#

**11.1.8 Verify Port Security**

Pentru a afișa setările de securitate a porturilor pentru comutator, utilizați comanda **show port-security.**

S1# **show port-security**

Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action

                (Count)       (Count)          (Count)

---------------------------------------------------------------------------

      Fa0/1              2            2                  0         Shutdown

---------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port)     : 1

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

S1#

Securitate port pentru o interfață specifică Utilizați comanda **show port-security interface** pentru a vizualiza detaliile pentru o anumită interfață, așa cum se arată anterior și în acest exemplu.

S1# **show port-security interface fastethernet 0/1**

Port Security               : Enabled

Port Status                 : Secure-up

Violation Mode              : Shutdown

Aging Time                  : 10 mins

Aging Type                  : Inactivity

SecureStatic Address Aging  : Disabled

Maximum MAC Addresses       : 2

Total MAC Addresses         : 2

Configured MAC Addresses    : 1

Sticky MAC Addresses        : 1

Last Source Address:Vlan    : a41f.7273.018c:1

Security Violation Count    : 0

S1#

Verify Learned MAC Addresses

S1# **show run interface fa0/1**

Building configuration...

Current configuration : 365 bytes

!

interface FastEthernet0/1

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky a41f.7272.676a

switchport port-security mac-address aaaa.bbbb.1234

switchport port-security aging time 10

switchport port-security aging type inactivity

switchport port-security

end

S1#

**Verify Secure MAC Addresses**

Pentru a afișa toate adresele MAC securizate care sunt configurate manual sau învățate dinamic pe toate interfețele switch-ului, utilizați comanda **show port-security address**, așa cum se arată în exemplu.

S1# **show port-security address**

               Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan    Mac Address       Type                          Ports   Remaining Age

                                                                   (mins)

----    -----------       ----                          -----   -------------

   1    a41f.7272.676a    SecureSticky                  Fa0/1        -

   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1        -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port)     : 1

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

S1#

**11.2.1 Revizuirea atacurilor VLAN**

Ca o revizuire rapidă, un atac de salt VLAN poate fi lansat în unul din trei moduri: Falsificarea mesajelor DTP de la gazda atacatoare pentru ca comutatorul să intre în modul trunking. De aici, atacatorul poate trimite trafic etichetat cu VLAN-ul țintă, iar comutatorul livrează apoi pachetele la destinație. Introducerea unui comutator necinstiți și activarea trunchiului. Atacatorul poate accesa apoi toate VLAN-urile de pe comutatorul victimă de la comutatorul necinstiți. Un alt tip de atac de salt VLAN este un atac cu etichetare dublă (sau dublu încapsulat). Acest atac profită de modul în care funcționează hardware-ul pe majoritatea switch-urilor.

**11.2.2 Steps to Mitigate VLAN Hopping Attacks**

Utilizați următorii pași pentru a atenua atacurile de salt VLAN:

* Pasul 1: Dezactivați negocierile DTP (trunking automat) pe porturile non-trunking utilizând comanda de configurare a interfeței de acces în modul switchport.
* Pasul 2: Dezactivați porturile neutilizate și puneți-le într-un VLAN neutilizat.
* Pasul 3: Activați manual legătura trunk pe un port trunk utilizând comanda switchport trunk mode.
* Pasul 4: Dezactivați negocierile DTP (trunking automat) pe porturile de trunking utilizând comanda switchport nonegotiate.
* Pasul 5: Setați VLAN-ul nativ la un alt VLAN decât VLAN 1 utilizând comanda switchport trunk native vlan vlan\_number.
* FastEthernet ports 0/1 through fa0/16 are active access ports
* FastEthernet ports 0/17 through 0/20 are not currently in use
* FastEthernet ports 0/21 through 0/24 are trunk ports.
* S1(config)# **interface range fa0/1 - 16**
* S1(config-if-range)# **switchport mode access**
* S1(config-if-range)# **exit**
* S1(config)#
* S1(config)# **interface range fa0/17 - 20**
* S1(config-if-range)# **switchport mode access**
* S1(config-if-range)# **switchport access vlan 1000**
* S1(config-if-range)# **shutdown**
* S1(config-if-range)# **exit**
* S1(config)#
* S1(config)# **interface range fa0/21 - 24**
* S1(config-if-range)# **switchport mode trunk**
* S1(config-if-range)# **switchport nonegotiate**
* S1(config-if-range)# **switchport trunk native vlan 999**
* S1(config-if-range)# **end**
* S1#

**11.3.1 DHCP Attack Review**

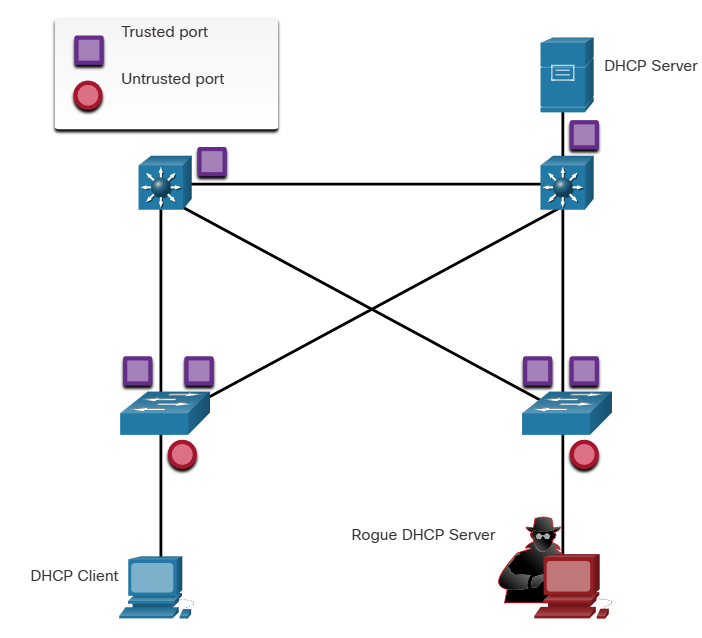
Scopul unui atac de foame DHCP este de a crea un Denial of Service (DoS) pentru conectarea clienților. Atacurile de foame DHCP necesită un instrument de atac precum Gobbler. Amintiți-vă că atacurile de foame DHCP pot fi atenuate eficient prin utilizarea securității porturilor, deoarece Gobbler utilizează o adresă MAC sursă unică pentru fiecare solicitare DHCP trimisă.

Gobbler ar putea fi configurat să folosească adresa MAC reală a interfeței ca adresă Ethernet sursă, dar să specifice o adresă Ethernet diferită în încărcarea DHCP. Acest lucru ar face ca securitatea porturilor să fie ineficientă, deoarece adresa MAC sursă ar fi legitimă.

Atacurile de falsificare DHCP pot fi atenuate prin utilizarea DHCP snooping pe porturile de încredere.

**11.3.2 Snooping DHCP**

Snoopingul DHCP nu se bazează pe adresele MAC sursă. În schimb, DHCP Snooping determină dacă mesajele DHCP provin dintr-o sursă de încredere configurată administrativ sau nede încredere.



**11.3.3 Steps to Implement DHCP Snooping**

S1(config)# **ip dhcp snooping**

S1(config)# **interface f0/1**

S1(config-if)# **ip dhcp snooping trust**

S1(config-if)# **exit**

S1(config)# **interface range f0/5 - 24**

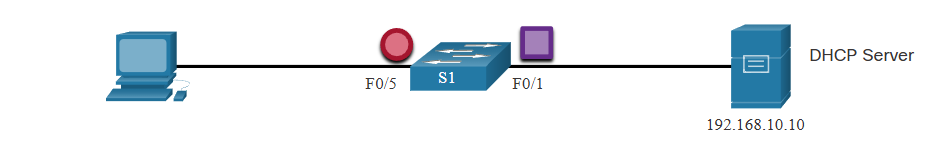
S1(config-if-range)# **ip dhcp snooping limit rate 6**

S1(config-if-range)# **exit**

S1(config)# **ip dhcp snooping vlan 5,10,50-52**

S1(config)# **end**

S1#



Utilizați comanda **show ip dhcp snooping** EXEC privilegiat pentru a verifica DHCP snooping și afișați **ip dhcp snooping binding** pentru a vedea clienții care au primit informații DHCP.

S1# **show ip dhcp snooping**

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

5,10,50-52

DHCP snooping is operational on following VLANs:

none

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:

FastEthernet0/5            no         no              6

  Custom circuit-ids:

FastEthernet0/6            no         no              6

  Custom circuit-ids:

S1# **show ip dhcp snooping binding**

MacAddress         IpAddress       Lease(sec) Type          VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:03:47:B5:9F:AD  192.168.10.11   193185     dhcp-snooping 5    FastEthernet0/5

**11.4.1 Dynamic ARP Inspection**

Într-un atac ARP tipic, un actor de amenințare poate trimite cereri ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IP a gateway-ului implicit.

Inspecția dinamică ARP (DAI) necesită DHCP snooping și ajută la prevenirea atacurilor.

**11.4.2 DAI Implementation Guidelines**

1. Activați DHCP Snooping la nivel global.

2. Activați DHCP Snooping pe VLAN-urile selectate.

3. Activați DAI pe VLAN-urile selectate.

4. Configurați interfețe de încredere pentru inspecția DHCP și inspecția ARP.

**11.4.3 DAI Configuration Example**

S1(config)# **ip dhcp snooping**

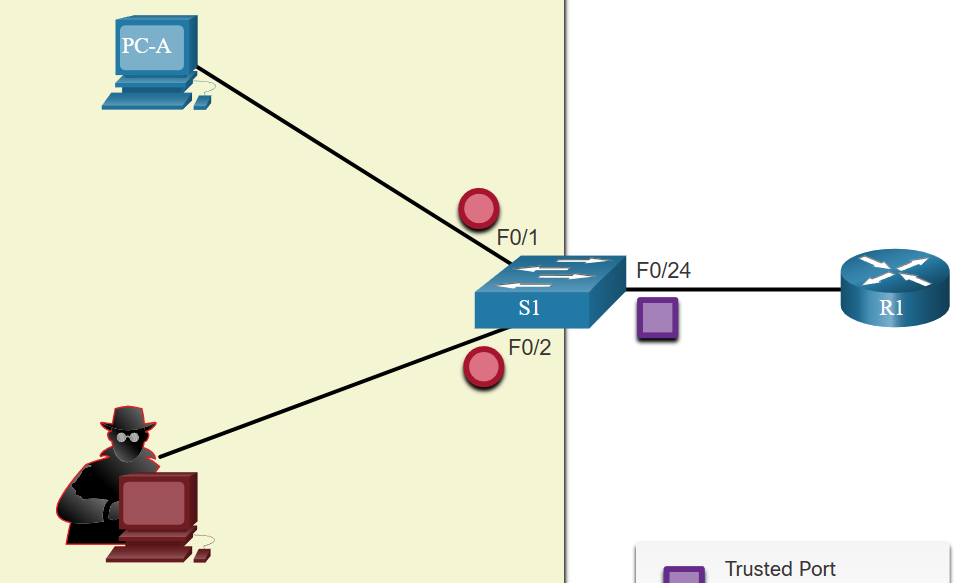
S1(config)# **ip dhcp snooping vlan 10**

S1(config)# **ip arp inspection vlan 10**

S1(config)# **interface fa0/24**

S1(config-if)# **ip dhcp snooping trust**

S1(config-if)# **ip arp inspection trust**



DAI poate fi, de asemenea, configurat pentru a verifica ambele adrese MAC și IP de destinație sau sursă:

* 1. Destination MAC
  2. Source MAC
  3. IP Address

Comanda de configurare globală **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** este utilizată pentru a configura DAI să renunțe la pachetele ARP atunci când adresele IP sunt invalide.

S1(config)# **ip arp inspection validate ?**

dst-mac  Validate destination MAC address

  ip       Validate IP addresses

  src-mac  Validate source MAC address

S1(config)# **ip arp inspection validate src-mac**

S1(config)# **ip arp inspection validate dst-mac**

S1(config)# **ip arp inspection validate ip**

S1(config)# **do show run | include validate**

ip arp inspection validate ip

S1(config)# **ip arp inspection validate src-mac dst-mac ip**

S1(config)# **do show run | include validate**

ip arp inspection validate src-mac dst-mac ip

S1(config)#

**11.4.4 Syntax Checker - Mitigate ARP Attacks**

You are currently logged into S1. Enable DHCP snooping globally for the switch.

S1(config)#ip dhcp snooping

Enter interface configuration mode for **g0/1 - 2**, trust the interfaces for both DHCP snooping and DAI, and then return to global configuration mode.

S1(config)#interface range g0/1 - 2

S1(config-if-range)#ip dhcp snooping trust

S1(config-if-range)#ip arp inspection trust

S1(config-if-range)#exit

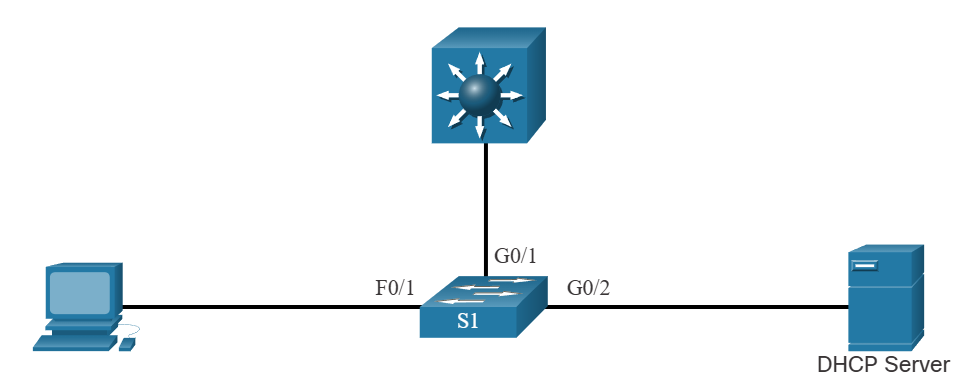
Enable DHCP snooping and DAI for VLANs **10,20,30-49**.

S1(config)#ip dhcp snooping vlan 10,20,30-49

S1(config)#ip arp inspection vlan 10,20,30-49

S1(config)#

You have successfully configured DAI for the switch.



**11.5.1 PortFast and BPDU Guard**

Pentru a atenua atacurile de manipulare Spanning Tree Protocol (STP), utilizați PortFast și Bridge Protocol Data Unit (BPDU) Guard:

1. PortFast - PortFast aduce imediat o interfață configurată ca port de acces la starea de redirecționare dintr-o stare de blocare, ocolind stările de ascultare și de învățare.
2. BPDU Guard - eroarea BPDU Guard dezactivează imediat un port care primește un BPDU.

**11.5.2 Configure PortFast**

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

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 FastEthernet0/1 but will only

have effect when the interface is in a non-trunking mode.

S1(config-if)# **exit**

S1(config)# **spanning-tree portfast default**

%Warning: this command enables portfast by default on all interfaces. You

should now disable portfast explicitly on switched ports leading to hubs,

switches and bridges as they may create temporary bridging loops.

S1(config)# **exit**

S1# **show running-config | begin span**

**11.5.3 Configure BPDU Guard**

S1(config)# **interface fa0/1**

S1(config-if)# **spanning-tree bpduguard enable**

S1(config-if)# **exit**

S1(config)# **spanning-tree portfast bpduguard default**

S1(config)# **end**

S1# **show spanning-tree summary**

Switch is in pvst mode

Root bridge for: none

Extended system ID           is enabled

Portfast Default             is enabled

PortFast BPDU Guard Default  is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default            is disabled

EtherChannel misconfig guard is enabled

UplinkFast                   is disabled

BackboneFast                 is disabled

Configured Pathcost method used is short

(output omitted)

S1#

**11.5.4 Syntax Checker - Mitigate STP Attacks**

You are currently logged into S1. Complete the following steps to implement PortFast and BPDU Guard on all access ports:

* Enter interface configuration mode for **fa0/1 - 24**.
* Configure the ports for access mode.
* Return to global configuration mode.
* Enable PortFast by default for all access ports.
* Enable BPDU Guard by default for all access ports.

S1(config)#interface range fa0/1 - 24

S1(config-if-range)#switchport mode access

S1(config-if-range)#exit

S1(config)#spanning-tree portfast default

S1(config)#spanning-tree portfast bpduguard default

S1(config)# exit

Verify that PortFast and BPDU Guard is enabled by default by viewing STP summary information.

S1#show spanning-tree summary

Switch is in pvst mode

Root bridge for: none

Extended system ID is enabled

Portfast Default is enabled

PortFast BPDU Guard Default is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default is disabled

EtherChannel misconfig guard is enabled

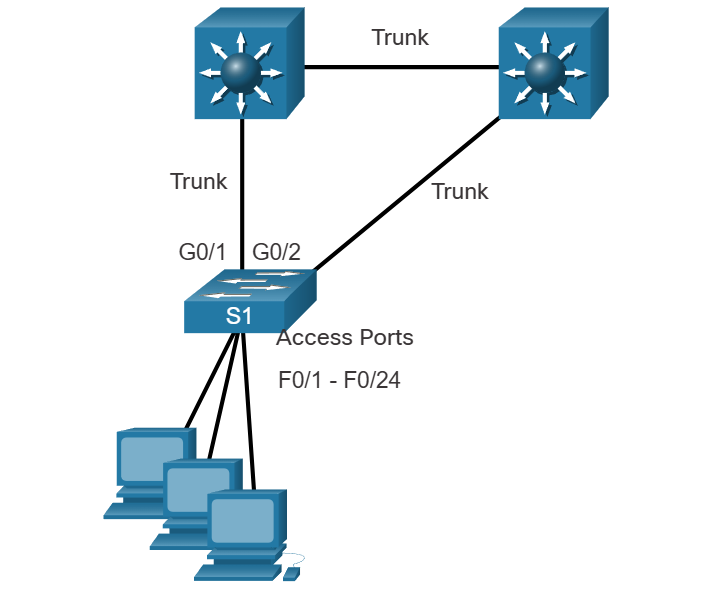
UplinkFast is disabled

BackboneFast is disabled

Configured Pathcost method used is short

(output omitted)

S1#



Pc1 : 192.168.1.1

Pc2: 192.168.1.2

Pc3: 192.168.1.3

L1: 192.168.1.5

L2: 192.168.1.4

4.

S1

interface FastEthernet0/3

switchport mode access

spanning-tree portfast

exit

2.

Pentru ca sa cada inactive cand conectam la latop :  
interface FastEthernet0/1

000D.BDA8.A434  
show port-security interface FastEthernet0/1

interface FastEthernet0/1  
shutdown

no shutdown

interface FastEthernet0/1

switchport mode access

switchport port-security

switchport port-security mac-address 000D.BDA8.A434

switchport port-security maximum 1

switchport port-security violation shutdown

3.

enable

configure terminal

interface FastEthernet0/2

no switchport port-security