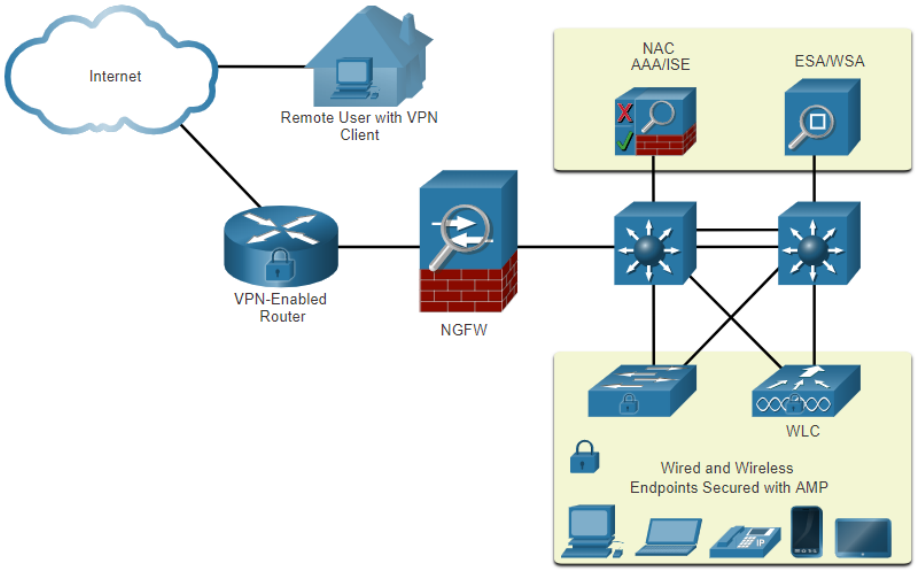
- Universitatea Politehnica Timisoara
- Concepte avansate de Securitate in Telecomunicatii, ianuarie 2026
- Instructor: **Liviu Bleotu**, CCIE #49250

CONCEPTE LAN SECURITY

SECURITATE ENDPOINT

Protecție Endpoint

- Endpoint-urile sunt gazde care includ, de obicei, laptopuri, desktopuri, servere și telefoane IP, precum și dispozitive deținute de angajați. Endpoint-urile sunt deosebit de vulnerabile la atacuri bazate pe malware care provin din e-mail sau din navigarea pe web.
- În mod tradițional, endpoint-urile au utilizat funcții de securitate locale, cum ar fi antivirus/antimalware, firewall-uri bazate pe host și sisteme de prevenire a intruziunilor bazate pe host (HIPS).
- În prezent, endpoint-urile sunt cel mai bine protejate printr-o combinație de NAC (Network Access Control), software AMP (Advanced Malware Protection), un dispozitiv de securitate pentru e-mail (ESA – Email Security Appliance) și un dispozitiv de securitate web (WSA – Web Security Appliance).



Cisco Email Security Appliance

- Dispozitivul Cisco ESA este proiectat pentru a monitoriza protocolul SMTP (Simple Mail Transfer Protocol). Cisco ESA este actualizat constant prin fluxuri în timp real furnizate de Cisco Talos, care detectează și corelează amenințările și soluțiile utilizând un sistem global de monitorizare bazat pe o bază de date mondială. Aceste date de inteligență privind amenințările sunt preluate de Cisco ESA la fiecare trei până la cinci minute.

- Iată câteva dintre funcțiile Cisco ESA:
  - Blochează amenințările cunoscute
  - Remediază malware-ul ascuns care a evitat detectarea inițială
  - Elimină e-mailurile care conțin linkuri malițioase
  - Blochează accesul la site-uri recent infectate
  - Criptează conținutul e-mailurilor trimise pentru a preveni pierderea de date.

Cisco Web Security Appliance

- Cisco Web Security Appliance (WSA) este o tehnologie de atenuare a amenințărilor bazate pe web. Aceasta ajută organizațiile să facă față provocărilor legate de securizarea și controlul traficului web.
- Cisco WSA combină protecția avansată împotriva malware-ului, vizibilitatea și controlul aplicațiilor, controalele politicilor de utilizare acceptabilă și funcțiile de raportare.
- Cisco WSA oferă control complet asupra modului în care utilizatorii accesează internetul. Anumite funcții și aplicații, precum chatul, mesageria, conținutul video și audio, pot fi permise, restricționate prin limite de timp și lățime de bandă sau blocate, în funcție de cerințele organizației.
- WSA poate realiza liste negre de URL-uri, filtrare URL, scanare malware, categorizare URL, filtrarea aplicațiilor web, precum și criptarea și decriptarea traficului web..

ACCESS CONTROL

Autentificarea cu o parolă locală

•Pe echipamentele de rețea pot fi realizate multe tipuri de autentificare, iar fiecare metodă oferă niveluri diferite de securitate.

Cea mai simplă metodă de autentificare pentru accesul de la distanță este configurarea unei combinații de nume de utilizator și parolă pe consola, liniile VTY și porturile AUX.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH este o formă mai sigură de acces de la distanță:

- Necesită un nume de utilizator și o parolă.
- Numele de utilizator și parola pot fi autentificate local.

```
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)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Metoda bazei de date locale are unele limitări:

- Conturile de utilizator trebuie configurate local pe fiecare dispozitiv, ceea ce nu este scalabil.
- Metoda nu oferă o soluție de autentificare de rezervă (fallback).

Componentele AAA

- AAA înseamnă Autentificare (Authentication), Autorizare (Authorization) și Contabilizare/Înregistrare (Accounting) și oferă cadrul principal pentru configurarea controlului accesului pe un dispozitiv de rețea.

- AAA reprezintă o metodă prin care se controlează cine are permisiunea de a accesa o rețea (autentificare), ce poate face în timp ce este conectat (autorizare) și ce acțiuni a efectuat în timpul accesării rețelei (contabilizare).

Autentificare

- Autentificarea AAA poate fi implementată folosind două metode comune: locală și bazată pe server.

- **Autentificare AAA locală:**
  - Metoda stochează numele de utilizator și parolele local pe un dispozitiv de rețea (de exemplu, un router Cisco).
  - Utilizatorii sunt autentificați folosind baza de date locală.
  - AAA local este ideal pentru rețele mici.

- **Autentificare AAA bazată pe server:**
  - În metoda bazată pe server, routerul accesează un server AAA central.
  - Serverul AAA conține numele de utilizator și parolele pentru toți utilizatorii.
  - Routerul utilizează protocoalele RADIUS (Remote Authentication Dial-In User Service) sau TACACS+ (Terminal Access Controller Access Control System Plus) pentru a comunica cu serverul AAA.
  - Atunci când există mai multe routere și switch-uri, autentificarea AAA bazată pe server este mai potrivită.

Autorizarea

- Autorizarea AAA este automată și nu necesită ca utilizatorii să efectueze pași suplimentari după autentificare.

- Autorizarea stabilește ce pot și ce nu pot face utilizatorii în rețea după ce au fost autentificați.

- Autorizarea utilizează un set de atribute care descriu accesul utilizatorului la rețea. Aceste atribute sunt folosite de serverul AAA pentru a determina privilegiile și restricțiile asociate acelui utilizator.

Accounting (Contabilizarea)

- Contabilizarea (Accounting) AAA colectează și raportează datele de utilizare. Aceste date pot fi folosite în scopuri precum auditarea sau facturarea. Datele colectate pot include momentele de început și de sfârșit ale conexiunii, comenzile executate, numărul de pachete și numărul de octeți.

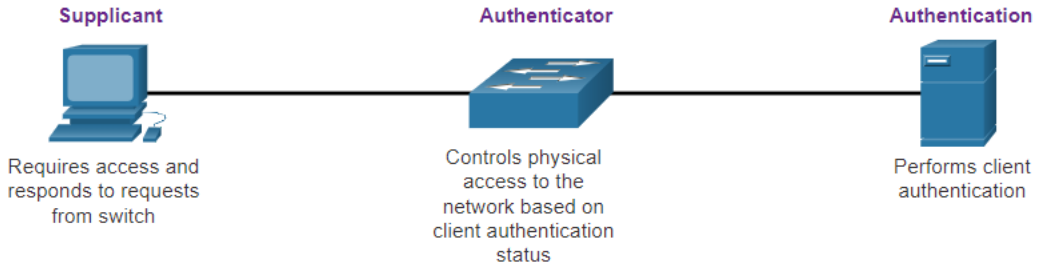
- O utilizare principală a contabilizării este combinarea acesteia cu autentificarea AAA.
  - Serverul AAA păstrează un jurnal detaliat al tuturor acțiunilor efectuate pe dispozitiv de către utilizatorul autentificat, așa cum este ilustrat în figură. Acest lucru include toate comenzile EXEC și de configurare emise de utilizato.
  - Jurnalul conține numeroase câmpuri de date, inclusiv numele de utilizator, data și ora, precum și comanda efectiv introdusă de utilizator. Aceste informații sunt utile la depanarea dispozitivelor și oferă, de asemenea, dovezi atunci când persoane efectuează acțiuni malițioase.

Access Control
802.1X

•Standardul IEEE 802.1X este un protocol de autentificare și control al accesului bazat pe port. Acest protocol restricționează stațiile de lucru neautorizate să se conecteze la o rețea LAN prin porturile de switch accesibile publicului. Serverul de autentificare autentifică fiecare stație de lucru conectată la un port de switch înainte ca orice servicii oferite de switch sau de rețeaua LAN să fie puse la dispoziție.

•În autentificarea bazată pe port 802.1X, dispozitivele din rețea au roluri specifice:

- **Client (Supplicant)** – Dispozitiv care rulează software client compatibil cu 802.1X, disponibil atât pentru dispozitive cablate, cât și wireless.
- **Switch (Authenticator) –** Switch-ul acționează ca intermediar între client și serverul de autentificare. Acesta solicită informații de identificare de la client, verifică aceste informații cu serverul de autentificare și transmite răspunsul către client. Un alt dispozitiv care poate îndeplini rolul de autentificator este un punct de acces wireless.
- **Server de autentificare** – Serverul validează identitatea clientului și notifică switch-ul sau punctul de acces wireless dacă respectivul client este sau nu autorizat să acceseze rețeaua LAN și serviciile switch-ului.



AMENINȚĂRÍ DE SECURITATE LAYER 2

Categorii de atacuri asupra switch-urilor

- Securitatea este la fel de puternică ca și cel mai slab punct din sistem, iar Layer 2 (stratul 2) este considerat acel punct slab. Acest lucru se datorează faptului că rețelele LAN erau, în mod tradițional, sub controlul administrativ al unei singure organizații. Aveam în mod inerent încredere în toate persoanele și dispozitivele conectate la LAN-ul nostru. Astăzi, odată cu conceptul BYOD (Bring Your Own Device) și atacurile tot mai sofisticate, rețelele LAN au devenit mai vulnerabile la penetrare.

Categoria	Exemple
Atacuri asupra tabelei MAC	Include atacuri de tip flood al adreselor MAC
Atacuri asupra VLAN	Include atacuri de tip VLAN hopping și VLAN double-tagging. De asemenea, include atacuri între dispozitive aflate în același VLAN.
Atacuri asupra DHCP	Include atacuri de tip DHCP starvation și DHCP spoofing.
Atacuri asupra ARP	Include atacuri de tip ARP spoofing și ARP poisoning
Atacuri de tip spoofing de adresă	Include atacuri de tip spoofing al adresei MAC și al adresei IP.
Atacuri asupra STP	Include atacuri de manipulare a protocolului Spanning Tree (STP).

Tehnici de atenuare a atacurilor asupra switch-urilor

Soluția	Descrierea
Securitatea porturilor	Previne multe tipuri de atacuri, inclusiv atacurile de tip MAC flooding și atacurile de tip DHCP starvation.
DHCP Snooping	Previne atacurile de tip DHCP starvation și DHCP spoofing.
Inspectarea dinamică ARP (DAI)	Previne atacurile de tip ARP spoofing și ARP poisoning.
Protecția sursei IP (IPSG)	Previne atacurile de tip spoofing al adreselor MAC și IP.

Aceste soluții la Layer 2 nu vor fi eficiente dacă protocoalele de management nu sunt securizate. Se recomandă următoarele strategii:

- Folosiți întotdeauna variante securizate ale protocoalelor de management, cum ar fi SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP) și Secure Socket Layer/Transport Layer Security (SSL/TLS).
- Luați în considerare utilizarea unei rețele de management out-of-band pentru administrarea dispozitivelor.
- Folosiți un VLAN dedicat pentru management, unde să circule doar traficul de management.
- Folosiți ACL-uri (Access Control Lists) pentru a filtra accesul nedorit.

ATACURI ASUPRA TABELEI MAC

Revizuirea funcționării unui switch

- Rețineți că, pentru a lua decizii de redirecționare, un switch LAN de Layer 2 construiește o tabelă bazată pe adresele MAC sursă din cadrele primite. Aceasta se numește tabelă de adrese MAC. Tabelele de adrese MAC sunt stocate în memorie și sunt utilizate pentru a comuta cadrele mai eficient.

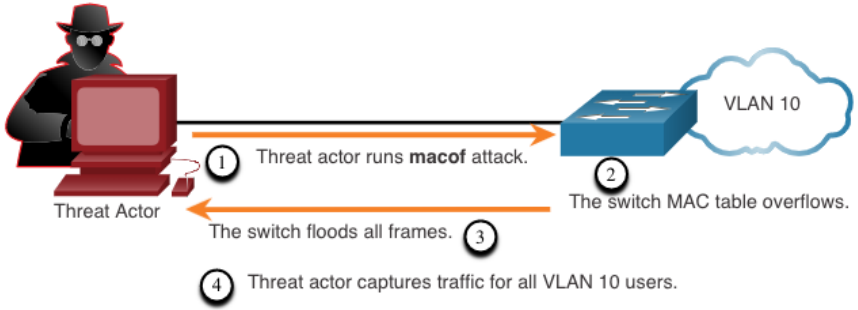
```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

Supraîncărcarea tabelei de adrese MAC

- Toate tabelele MAC au o dimensiune fixă și, în consecință, un switch poate rămâne fără resurse pentru stocarea adreselor MAC. Atacurile de tip MAC address flooding profită de această limitare prin bombardarea switch-ului cu adrese MAC sursă false, până când tabela de adrese MAC a switch-ului se umple.

- Când acest lucru se întâmplă, switch-ul tratează cadrele ca unicast necunoscut și începe să inunde tot traficul primit pe toate porturile din același VLAN, fără a consulta tabela MAC. Această situație permite unui actor malițios să captureze toate cadrele trimise de la o gazdă la alta în LAN-ul local sau în VLAN-ul local.

- **Notă:** Traficul este inundat doar în cadrul LAN-ului sau VLAN-ului local. Actorul malițios poate captura trafic numai în LAN-ul sau VLAN-ul local la care este conectat.



Atenuarea atacurilor asupra tabelei MAC

- Ceea ce face ca instrumente precum macof să fie atât de periculoase este faptul că un atacator poate crea foarte rapid un atac de tip MAC table overflow. De exemplu, un switch Catalyst 6500 poate stoca 132.000 de adrese MAC în tabela sa MAC. Un instrument precum macof poate inunda un switch cu până la 8.000 de cadre false pe secundă, creând un atac de tip overflow al tabelei MAC în doar câteva secunde.

- Un alt motiv pentru care aceste instrumente de atac sunt periculoase este că ele nu afectează doar switch-ul local, ci pot afecta și alte switch-uri Layer 2 conectate. Când tabela MAC a unui switch se umple, acesta începe să inunde toate porturile, inclusiv pe cele conectate la alte switch-uri Layer 2.

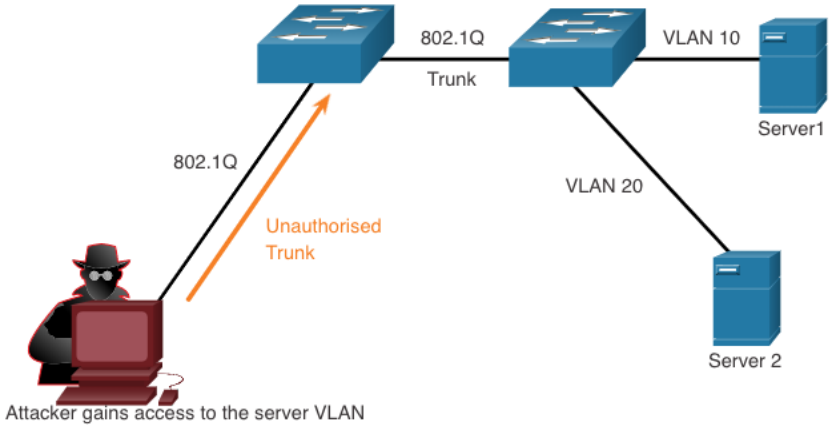
- Pentru a atenua atacurile de tip MAC address table overflow, administratorii de rețea trebuie să implementeze port security. Port security permite învățarea unui număr specificat de adrese MAC sursă pe port. Port security este discutat mai detaliat într-un alt modul.

ATACURI ASUPRA LAN

Atacuri de tip VLAN hopping

•Un atac de tip VLAN hopping permite ca traficul dintr-un VLAN să fie vizibil într-un alt VLAN fără utilizarea unui router. Într-un atac VLAN hopping de bază, actorul malițios configurează o gazdă să se comporte ca un switch, profitând de funcția de trunking automat activată implicit pe majoritatea porturilor de switch.

•Actorul malițios configurează gazda pentru a falsifica semnalizarea 802.1Q și semnalizarea Dynamic Trunking Protocol (DTP), specifică Cisco, pentru a stabili un trunk cu switch-ul la care este conectată. Dacă atacul reușește, switch-ul stabilește o legătură trunk cu gazda, așa cum este ilustrat în figură.În acest caz, actorul malițios poate accesa toate VLAN-urile de pe switch. Acesta poate trimite și primi trafic pe orice VLAN, „sărind” efectiv între VLAN-uri..



Atacuri de tip dublă etichetare VLAN

- În anumite situații, un actor malițios poate insera o etichetă 802.1Q ascunsă într-un cadru care are deja o etichetă 802.1Q. Această etichetă permite cadrului să ajungă într-un VLAN diferit față de cel specificat de eticheta 802.1Q originală.
  - **Pasul 1**: Actorul malițios trimite către switch un cadru 802.1Q cu dublă etichetare. Antetul exterior conține eticheta VLAN a actorului malițios, care este aceeași cu VLAN-ul nativ al portului trunk.
  - **Pasul 2**: Cadrul ajunge la primul switch, care analizează prima etichetă 802.1Q de 4 octeți. Switch-ul observă că cadrul este destinat VLAN-ului nativ și îl redirecționează pe toate porturile VLAN-ului nativ după eliminarea etichetei VLAN. Cadrul nu este reetichetat deoarece face parte din VLAN-ul nativ. În acest moment, eticheta VLAN internă rămâne intactă și nu a fost inspectată de primul switch.
  - **Pasul 3:** Cadrul ajunge la al doilea switch, care nu știe că acesta era destinat VLAN-ului nativ. Conform specificației 802.1Q, traficul VLAN-ului nativ nu este etichetat de switch-ul care trimite cadrul. Al doilea switch examinează doar eticheta 802.1Q internă inserată de actorul malițios și observă că cadrul este destinat VLAN-ului țintă. Al doilea switch trimite cadrul către destinație sau îl inundă, în funcție de existența unei intrări corespunzătoare în tabela de adrese MAC pentru VLAN-ul țintă.

Atacuri de tip dublă etichetare VLAN (Cont.)

- Un atac de tip VLAN double-tagging este unidirecțional și funcționează numai atunci când atacatorul este conectat la un port aflat în același VLAN ca VLAN-ul nativ al portului trunk. Ideea de bază este că dubla etichetare permite atacatorului să trimită date către gazde sau servere dintr-un VLAN care, în mod normal, ar fi blocat de un anumit tip de configurare a controlului accesului.
Se presupune că traficul de răspuns va fi, de asemenea, permis, oferindu-i astfel atacatorului posibilitatea de a comunica cu dispozitive din VLAN-ul care este în mod normal restricționat.

- **Atenuarea atacurilor VLAN –** Atacurile de tip VLAN hopping și VLAN double-tagging pot fi prevenite prin implementarea următoarelor ghiduri de securitate pentru trunk-uri, așa cum a fost discutat într-un modul anterior:

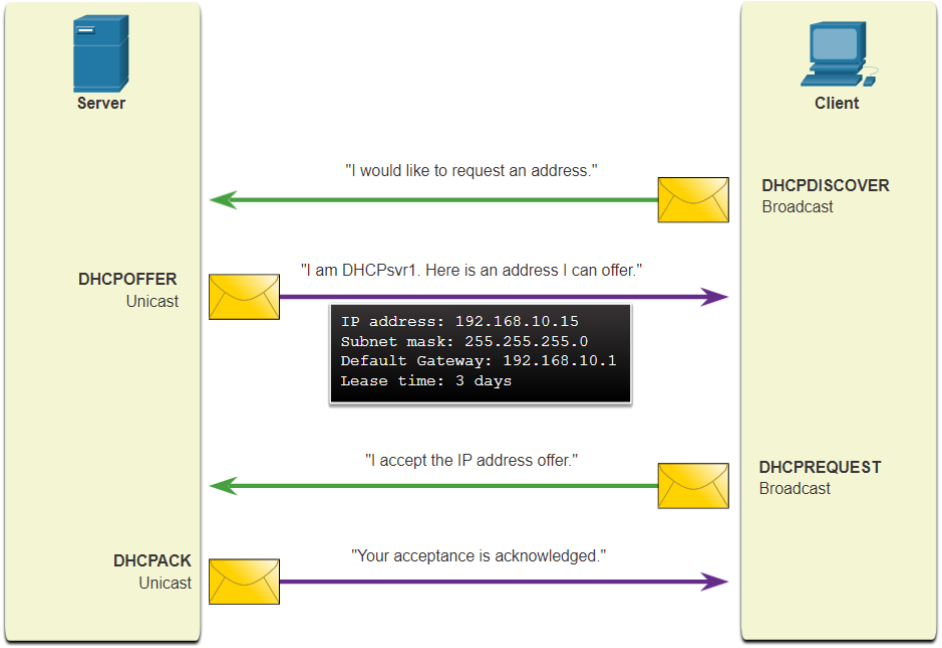
- Dezactivați trunking-ul pe toate porturile de tip access.

- Dezactivați auto-trunking pe legăturile trunk, astfel încât trunk-urile să fie activate manual.

- Asigurați-vă că VLAN-ul nativ este utilizat doar pentru legăturile trunk.

Mesaje DHCP

•Serverele DHCP furnizează în mod dinamic informații de configurare IP, inclusiv adresa IP, masca de subrețea, gateway-ul implicit, serverele DNS și altele către clienți. O revizuire a secvenței de schimb de mesaje DHCP între client și server este prezentată în figură.



DHCP Attacks

•Există două tipuri de atacuri DHCP: DHCP starvation și DHCP spoofing. Ambele atacuri pot fi prevenite prin implementarea DHCP snooping.

- **Atacul DHCP Starvation** – Scopul acestui atac este de a crea un atac de tip DoS (Denial of Service) pentru clienții care încearcă să se conecteze. Atacurile DHCP starvation necesită un instrument de atac precum Gobbler. Gobbler are capacitatea de a analiza întregul interval de adrese IP disponibile pentru alocare și încearcă să le închirieze pe toate. Mai exact, acesta generează mesaje DHCP Discover folosind adrese MAC false.
- **Atacul DHCP Spoofing** – Acesta apare atunci când un server DHCP neautorizat (rogue) este conectat la rețea și furnizează parametri de configurare IP falși clienților legitimi. Un server neautorizat poate oferi diverse informații înșelătoare, inclusiv următoarele:
  - **Gateway implicit greșit –** Serverul neautorizat furnizează un gateway invalid sau adresa IP a propriei gazde pentru a crea un atac de tip man-in-the-middle. Acest lucru poate trece complet neobservat, deoarece intrusul interceptează fluxul de date prin rețea.
  - **Server DNS greșit** – Serverul neautorizat furnizează o adresă incorectă de server DNS, redirecționând utilizatorul către un site web malițios.
  - **Adresă IP greșită** – Serverul neautorizat furnizează o adresă IP invalidă, creând efectiv un atac de tip DoS asupra clientului DHCP.

Atacuri ARP

- Gazdele transmit ARP Requests în broadcast pentru a determina adresa MAC a unei gazde cu o anumită adresă IP de destinație. Toate gazdele din subrețea primesc și procesează cererea ARP. Gazda care are adresa IP corespunzătoare din cererea ARP trimite un ARP Reply.
- Un client poate trimite un ARP Reply nesolicitat, numit „gratuitous ARP”. Celelalte gazde din subrețea stochează adresa MAC și adresa IP conținute în ARP-ul gratuit în tabelele lor ARP.
- Un atacator poate trimite un mesaj gratuitous ARP conținând o adresă MAC falsificată către switch, iar switch-ul va actualiza tabela MAC corespunzător. Într-un atac tipic, un actor malițios trimite ARP Replies nesolicitate către alte gazde din subrețea, folosind adresa MAC a atacatorului și adresa IP a gateway-ului implicit, configurând astfel un atac de tip man-in-the-middle.
- Există multe instrumente disponibile pe internet pentru a crea atacuri ARP de tip man-in-the-middle.
- IPv6 folosește ICMPv6 Neighbor Discovery Protocol pentru rezolvarea adreselor la Layer 2. IPv6 include strategii pentru a preveni spoofing-ul mesajelor Neighbor Advertisement, similar modului în care IPv6 previne un ARP Reply falsificat.
- Atacurile de tip ARP spoofing și ARP poisoning pot fi atenuate prin implementarea Dynamic ARP Inspection (DAI).

Atacuri de tip spoofing de adresă

- IP address spoofing apare atunci când un actor malițios preia o adresă IP validă a unui alt dispozitiv din subrețea sau folosește o adresă IP aleatorie. Spoofing-ul adreselor IP este dificil de prevenit, mai ales atunci când este folosit în interiorul unei subrețele unde adresa IP aparține deja unui dispozitiv legitim.
- MAC address spoofing apare atunci când actorii malițioși modifică adresa MAC a gazdei lor pentru a corespunde unei adrese MAC cunoscute a unei gazde țintă. Switch-ul suprascrie intrarea curentă din tabela MAC și atribuie adresa MAC noului port. Astfel, switch-ul redirecționează inadvertent cadrele destinate gazdei țintă către gazda atacatorului.
- Când gazda țintă trimite trafic, switch-ul corectează eroarea, realiniind adresa MAC la portul original. Pentru a împiedica switch-ul să readucă atribuirea portului la starea corectă, actorul malițios poate crea un program sau un script care trimite constant cadre către switch, astfel încât switch-ul să mențină informația incorectă sau falsificată.
- Nu există niciun mecanism de securitate la Layer 2 care să permită switch-ului să verifice sursa adreselor MAC, ceea ce face acest nivel vulnerabil la spoofing.
- Atacurile de tip IP și MAC address spoofing pot fi atenuate prin implementarea IP Source Guard (IPSG).

Atac STP

- Atacatorii de rețea pot manipula Spanning Tree Protocol (STP) pentru a realiza un atac prin falsificarea root bridge-ului și modificarea topologiei rețelei. Astfel, atacatorii pot captura întregul trafic din domeniul comutat imediat.
- Pentru a desfășura un atac de manipulare STP, gazda atacatoare transmite în broadcast BPDU-uri (Bridge Protocol Data Units) care conțin modificări de configurare și topologie, forțând recalculări ale spanning tree-ului. BPDU-urile trimise de gazda atacatoare anunță o prioritate de bridge mai mică, în încercarea de a fi aleasă ca root bridge.
- Acest tip de atac STP este atenuat prin implementarea BPDU Guard pe toate porturile de tip access. BPDU Guard este discutat mai detaliat mai târziu în curs.

Recunoaștere prin CDP

•Cisco Discovery Protocol (CDP) este un protocol proprietar de descoperire a legăturilor la Layer 2. Este activat implicit pe toate dispozitivele Cisco. Administratorii de rețea utilizează CDP și pentru a ajuta la configurarea și depanarea dispozitivelor de rețea.Informațiile CDP sunt trimise prin porturile activate CDP sub formă de broadcast periodic, necriptat și neautentificat. Informațiile CDP includ: adresa IP a dispozitivului, versiunea software IOS, platforma, capabilitățile și VLAN-ul nativ. Dispozitivul care primește mesajul CDP își actualizează baza de date CDP cu aceste informații.

•Pentru a atenua exploatarea CDP, limitați utilizarea CDP pe dispozitive sau porturi. De exemplu, dezactivați CDP pe porturile de margine care se conectează la dispozitive neîncredere.

- Pentru a dezactiva CDP la nivel global pe un dispozitiv, folosiți comanda în modul de configurare globală **no cdp run**. Pentru a activa CDP la nivel global, folosiți comanda **cdp run**.
- Pentru a dezactiva CDP pe un port, folosiți comanda în modul de configurare a interfeței **no cdp enable**. Pentru a activa CDP pe un port, folosiți comanda **cdp enable**.

•**Notă**: Link Layer Discovery Protocol (LLDP) este, de asemenea, vulnerabil la atacuri de recunoaștere. Pentru a dezactiva LLDP la nivel global, configurați comanda **no lldp run**. Pentru a dezactiva LLDP pe o interfață, configurați comenzile **no lldp transmit** și **no lldp receive**.

CONFIGURAREA SECURITĂȚII UNUI ȘWITCH

Securizarea porturilor neutilizate

•Atacurile de tip Layer 2 sunt printre cele mai ușor de executat de către hackeri, însă aceste amenințări pot fi și atenuate prin implementarea unor soluții comune la nivelul Layer 2.

- Toate porturile (interfețele) unui switch trebuie securizate înainte ca switch-ul să fie utilizat în producție. Modul în care este securizat un port depinde de funcția sa.
- O metodă simplă pe care mulți administratori o folosesc pentru a ajuta la securizarea rețelei împotriva accesului neautorizat este dezactivarea tuturor porturilor neutilizate de pe un switch. Navigați la fiecare port neutilizat și utilizați comanda Cisco IOS **shutdown**. Dacă un port trebuie reactivat ulterior, acesta poate fi activat cu comanda **no shutdown**.
- Pentru a configura un interval de porturi, folosiți comanda **interface range**.

```
Switch(config)# interface range type module/first-number - last-number
```

Activarea securității portului

- Port security este activată cu comanda de configurare a interfeței: **switchport port-security**.
- Observați în exemplu că comanda **switchport port-security** a fost respinsă. Acest lucru se întâmplă deoarece securitatea portului poate fi configurată doar pe porturi access configurate manual sau pe porturi trunk configurate manual. Implicit, porturile unui switch Layer 2 sunt setate pe dynamic auto (trunking activat). Prin urmare, în exemplu, portul este configurat cu comanda **switchport mode access**.
- **Notă:** Securitatea porturilor trunk depășește domeniul acestui curs.

```
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#
```

Activarea securității portului (Cont.)

- Folosiți comanda **show port-security interface** pentru a afișa setările curente de securitate a portului pentru FastEthernet 0/11.
  - Observați cum securitatea portului este activată, modul de încălcare (violation mode) este shutdown și numărul maxim de adrese MAC este 1.
  - Dacă un dispozitiv este conectat la port, switch-ul va adăuga automat adresa MAC a dispozitivului ca MAC securizat. În acest exemplu, niciun dispozitiv nu este conectat la port.

```
S1# show port-security interface f0/1
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

- **Notă**: Dacă un port activ este configurat cu comanda **switchport port-security** și mai mult de un dispozitiv este conectat la acel port, portul va trece în starea error-disabled.

Limitarea și învățarea adreselor (Cont.)

- Exemplul demonstrează o configurație completă de securitate a portului pentru FastEthernet 0/1.

- Administratorul specifică un număr maxim de 4 adrese MAC, configurează manual o adresă MAC securizată și apoi configurează portul pentru a învăța dinamic adrese MAC suplimentare, până la maximum 4 adrese MAC securizate.

- Folosiți comenzile **show port-security interface** și **show port-security address** pentru a verifica configurația.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
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      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1# show port-security address
              Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1#
```

Port Security Aging (Cont.)

- Exemplul arată un administrator care configurează tipul de îmbătrânire (aging type) la 10 minute de inactivitate.

- Comanda **show port-security** confirmă modificările. Folosiți comanda **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-shutdown
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
```

Moduri de încălcare a securității portului

- Dacă adresa MAC a unui dispozitiv conectat la un port diferă de lista de adrese MAC securizate, atunci are loc o încălcare a portului și portul trece în starea error-disabled.
- Pentru a seta modul de încălcare a securitătii portului, folositi următoarea comandă:

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

Următorul tabel arată cum reacționează un switch în funcție de **modul de încălcare a securității portului** configurat.

Modul	Descrierea
oprire (implicit)	Portul trece imediat în starea error-disabled, LED-ul portului se stinge și se trimite un mesaj syslog. Contorul de încălcări este incrementat. Când un port securizat se află în starea error-disabled, administratorul trebuie să-l reactiveze folosind comenzile **shutdown** și **no shutdown**
Limitare	Portul respinge pachetele cu adrese sursă necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a coborî sub valoarea maximă sau măriți valoarea maximă. Acest mod crește contorul de încălcări de securitate și generează un mesaj syslog
Protecție	Acesta este cel mai puțin sigur dintre modurile de încălcare a securității. Portul respinge pachetele cu adrese MAC sursă necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a coborî sub valoarea maximă sau măriți valoarea maximă. Nu este trimis niciun mesaj syslog

Verificarea securității portului

- După configurarea securității porturilor pe un switch, verificați fiecare interfață pentru a vă asigura că securitatea portului este setată corect și confirmați că adresele MAC statice au fost configurate corespunzător.
- Pentru a afișa setările de securitate ale portului, utilizați comanda **show port-security** .

- Exemplul arată că toate cele 24 de interfețe sunt configurate cu comanda **switchport port-security**, deoarece numărul maxim permis este 1, iar modul de încălcare a securității este shutdown.
- No devices are connected, therefore, the CurrentAddr (Count) is 0 for each interface.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa0/1             1           0                  0         Shutdown
      Fa0/2             1           0                  0         Shutdown
      Fa0/3             1           0                  0         Shutdown
(output omitted)
     Fa0/24             1           0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Verificarea securității portului (Cont.)

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

```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type            Ports     Remaining Age
                                                        (mins)
----    -----------       ----            -----     -------------
1       0025.83e6.4b01    SecureDynamic   Fa0/18          -
1       0025.83e6.4b02    SecureSticky    Fa0/19          -
-----------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

DHCP Snooping

•DHCP snooping filtrează mesajele DHCP și limitează rata traficului DHCP pe porturile neîncredere.

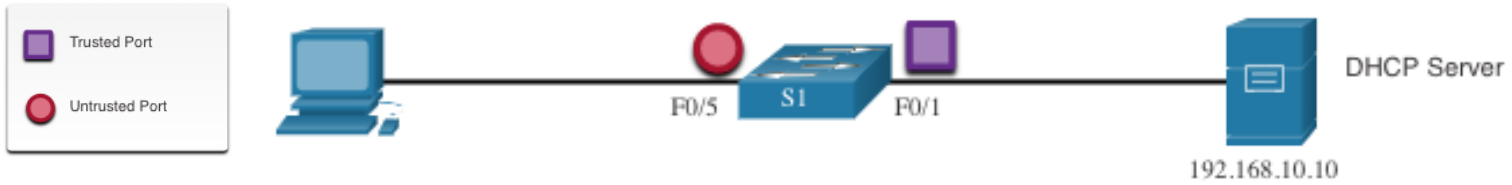
- Dispozitivele aflate sub control administrativ (de exemplu, switch-uri, routere și servere) sunt considerate surse de încredere.
- Interfețele de încredere (de exemplu, legăturile trunk, porturile serverelor) trebuie configurate explicit ca fiind de încredere.
- Dispozitivele din afara rețelei și toate porturile de tip access sunt în general tratate ca surse neîncredere.

•Se construiește o tabelă DHCP care include adresa MAC sursă a unui dispozitiv de pe un port neîncredere și adresa IP atribuită acelui dispozitiv de serverul DHCP.

- Adresa MAC și adresa IP sunt legate între ele.
- Astfel această tabelă se numește DHCP snooping binding table.

DHCP Snooping Configuration Example

- Consultați topologia de exemplu DHCP snooping cu porturi de tip trusted și untrusted.



- DHCP snooping este activat mai întâi pe S1.
- Interfața către serverul DHCP este configurată explicit ca fiind de încredere.
- Porturile F0/5 până la F0/24 sunt neîncredere și, prin urmare, traficul este limitabil la șase pachete pe secundă.
- În final, DHCP snooping este activat pe VLAN-urile 5, 10, 50, 51 și 52.

```
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)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Exemplu de configurare DHCP Snooping(Cont.)

- Folosiți comanda **show ip dhcp snooping** în modul privileged EXEC pentru a verifica setările DHCP snooping.

- Folosiți comanda **show ip dhcp snooping binding** pentru a vedea clienții care au primit informații DHCP.

- **Notă**: DHCP snooping este necesar și pentru Dynamic ARP Inspection (DAI).

```
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  192.168.10.10   193185     dhcp-snooping 5    FastEthernet0/5
```

Inspectarea dinamică ARP

- Într-un atac tipic ARP, un actor malițios poate trimite ARP Replies nesolicitate către alte gazde din subrețea, folosind adresa MAC a atacatorului și adresa IP a gateway-ului implicit. Pentru a preveni ARP spoofing și ARP poisoning, switch-ul trebuie să se asigure că doar ARP Requests și Replies valide sunt transmise mai departe.

- Dynamic ARP Inspection (DAI) necesită DHCP snooping și ajută la prevenirea atacurilor ARP prin:
  - Ne-transmiterea ARP Replies invalide sau gratuite către alte porturi din același VLAN.
  - Interceptarea tuturor ARP Requests și Replies pe porturile neîncredere.
  - Verificarea fiecărui pachet interceptat pentru a confirma legătura validă IP-MAC.
  - Respingerea și înregistrarea ARP Replies provenite de la surse invalide pentru a preveni ARP poisoning.
  - Dezactivarea portului (error-disable) dacă numărul de pachete ARP interceptate depășește limita configurată în DAI..

Exemplu de configurare DAI

- În topologia anterioară, S1 conectează doi utilizatori pe VLAN 10.

- DAI va fi configurat pentru a preveni atacurile de tip ARP spoofing și ARP poisoning.
- DHCP snooping este activat deoarece DAI necesită tabela DHCP snooping binding pentru a funcționa.
- Următorul pas este activarea DHCP snooping și a inspectării ARP pentru PC-urile din VLAN 10.
- Portul uplink către router este considerat trusted și, prin urmare, este configurat ca port trusted pentru DHCP snooping și ARP inspection.

```
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
```

PortFast și BPDU Guard

- Rețineți că atacatorii de rețea pot manipula Spanning Tree Protocol (STP) pentru a realiza un atac prin falsificarea root bridge-ului și modificarea topologiei rețelei.
- Pentru a preveni atacurile STP, utilizați PortFast și BPDU Guard (Bridge Protocol Data Unit Guard):

PortFast

- PortFast aduce imediat un port în starea de forwarding din starea de blocking, ocolind stările de listening și learning.
- Se aplică pe toate porturile de acces pentru utilizatori finali.

BPDU Guard

- BPDU Guard dezactivează imediat un port care primește un BPDU.
- La fel ca PortFast, BPDU Guard trebuie configurat doar pe interfețele conectate la dispozitive finale.

Configurarea PortFast

•PortFast ocolește stările listening și learning ale STP pentru a minimiza timpul de așteptare al porturilor de acces până la convergența STP.

- Activați PortFast doar pe porturile de acces.
- Activarea PortFast pe legăturile inter-switch poate crea un loop în spanning-tree.

PortFast poate fi activat:

- **Pe o interfață** – folosiți comanda în modul de configurare a interfeței **spanning-tree portfast** .
- **La nivel global**– folosiți comanda în modul de configurare globală pentru a activa PortFast pe toate porturile de acces **spanning-tree portfast default**.

```
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
```

Configurarea BPDU Guard

•Un port de acces ar putea primi un BPDU neașteptat, fie accidental, fie pentru că un utilizator a conectat un switch neautorizat la portul de acces.

- Dacă un BPDU este recepționat pe un port de acces cu BPDU Guard activat, portul este pus în starea error-disabled.
- Aceasta înseamnă că portul este dezactivat și trebuie să fie reactivat manual sau recuperat automat prin comanda globală **errdisable recovery cause psecure_violation**.

BPDU Guard poate fi activat:

- **Pe o interfață** – folosiți comanda în modul de configurare a interfeței **spanning-tree bpduguard enable.**
- **La nivel global**– folosiți comanda în modul de configurare globală pentru a activa BPDU Guard pe toate porturile de acces.

```
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#
```