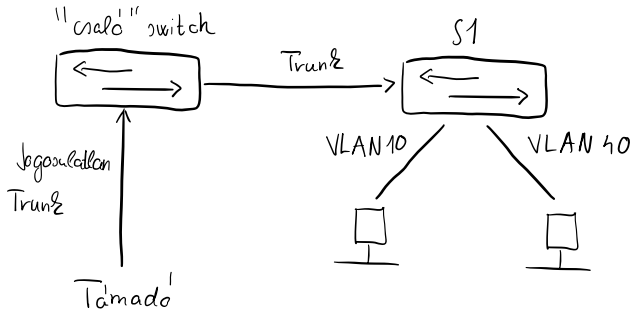
Adatkapcsolati rétegbeli támadások
kivédésének módjai

• CAM Table Attack

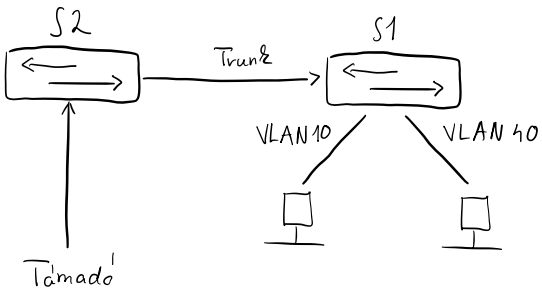
- CAM -> Content-addressable memory
- Hamis MAC címek áradatát küldi a switch-nek?
- Ez az adatáradat arra készteti a switch-et, hogy a CAM-adatbázis tábláiban lévő érvényes címeket kidobja, hogy helyet csináljon a hamis információknak.
  - Támadás -> macof Linux parancs
    ```
    # macof -i <Interfész>
    ```
  - Kivédése
    - Port security, vagyis a port nem továbbít olyan csomagokat, amik a forráscímei nem tartoznak a meghatározott címek csoportjába.
      ```
      # shutdown (MAC címek kiürítése)
      # no sh
      # switchport mode access
      # switchport port-security maximum <MAX> (Max MAC címek)
      # switchport port-security
      ```
    - Hibaüzenet -> SecurityViolation

•VLAN Attack -> VLAN Hopping

- A VLAN hálózati erőforrásainak támadására szolgáló módszer, ami csomagok küldésével történik egy olyan portra, ami általában nem érhető el egy végpontrendszerből.
- Fő célja, hogy hozzáférést szerezzen más VLAN-okhoz ugyanabban a hálózatban.
  - Támadás
    1. Switch spoofing -> A támadó trunk vonalat hoz létre egy "csaló" switch hálózatba kapcsolásával.



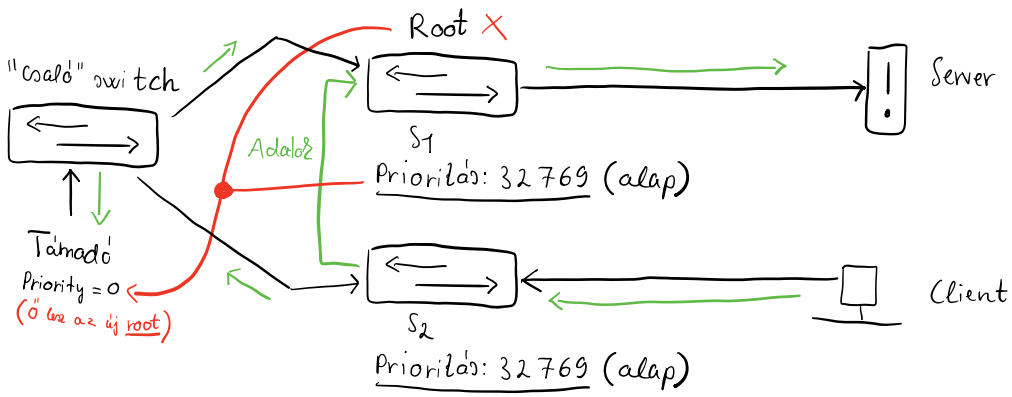
2. Double tagging -> A támadó hozzáad/módosítja a tag-eket az Ethernet-frame-ben. (802.1Q tagging)



- Kivédése
  - DTP (automatikus trunk) negotiation letiltása a nem trunk (switchport mode access) és trunk portokon (switchport non-negotiate)
  - Nem használt portok letiltása és külön VLAN-ba helyezése.
  - Trunk port engedélyezése manuálisan (switchport mode trunk).
  - VLAN 1 ne legyen natív, használaton kívüli VLAN-ra állítsa be.

• STP Attack

- STP → Spanning Tree Protocol
  - Loop-ok (hurkok) ellen →
- Az STP támadáskor a támadó meghamisítja a root bridge-t a topológiában.
  - A támadó egy STP konfiguráció / topológiaváltás BPDU (Bridge Protocol Data Unit) sugároz ki, hogy megpróbálja kikényszeríteni az STP újraszámítását.
  - A kiküldött BPDU azt jelenti, hogy a támadó rendszere lower bridge prioritással rendelkezik.
  - Minden BPDU-nak van id-je → Bridge ID (BID) = Bridge Priority + MAC
  - Támadás



  - Kivédése
    - BPDU Guard
    - Root Guard
    - Loop Guard

- **Address Spoofing Attack** → MAC address spoofing
  - Hálózati eszközök hálózati interfészének gyárilag kiosztott MAC címét változtatja meg.
    - A hálózat interfészvezérlő (NIC) "hard" kódolt MAC cím nem módosítható.
    - Ezt illesztőprogram (driver) ezt megakadályozza.
    - Támadás
      - Victim MAC cím megszerzése, majd a támadó a saját eszközének MAC címét átírja.
      - 11:CC:55:AA:77:BB
      - 33:AA:99:DD:44:FF

Támadó új MAC címe → 11:CC:55:AA:77:BB

- Kivédése
  - Port Security
  - Max MAC címek számának korlátozása

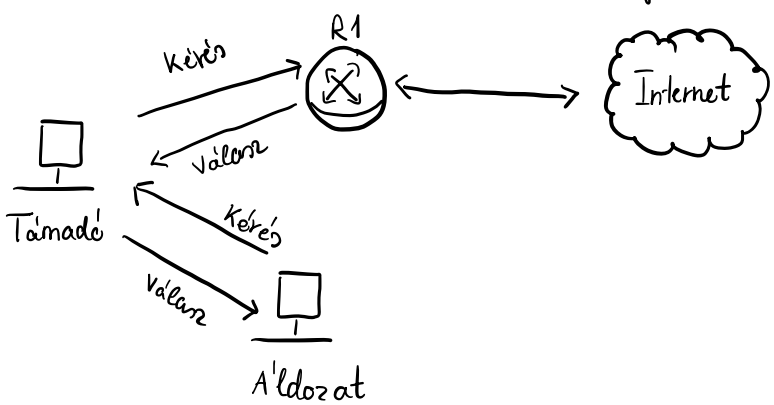
```
# shutdown (MAC címek kiürítése)
# no sh
# switchport mode access
# switchport port-security maximum <MAX> (Max MAC címek)
# switchport port-security
```

• DHCP Attack

- DHCP starvation
  - DHCP szolgáltatást célozza és aminer során a támadó hamisított DHCP szerelmet szúrt azzal a céllal, hogy kimerítse a DHCP szolgáló által kiosztható összes rendelkezésre álló IP címét.
  - Támadás -> Yersinia linuxon
    - DISCOVER csomagok küldésével
      - # show ip dhcp pool -> Hiba! (Nem hajtódik végre a parancs)
        ↳ Leterhelődik a DHCP adatbázis
      - # show ip dhcp binding -> Rengeteg IP cím, hamis MAC címmel.

- DHCP snooping
  - Támadás
    - Érvényesíti a nem megbízható forrásokból érkező DHCP üzeneteket és kiszűri az érvénytelen üzeneteket.
  - Kivédése
    - DHCP snooping megbízható port beállítása
    - DOT1x autentikáció
    - Port Security
    - Nem használt portok lekapcsolása

- **ARP Attack** -> Address Resolution Protocol
  - **ARP spoofing**
    - A támadó hamis ARP csomagokat küld, amik összekapcsolják a támadó MAC címét a LAN-on lévő számítógép IP címével.
    - Támadás -> Arpspoof
      - Szkennelés
      - Hamis ARP-válaszok küldése, ami tartalmazza a támadó MAC címét.
      - Az adatok most már a támadóhoz érkeznek meg.
  - **ARP poisoning**
    - Támadás
      - A sikeres ARP spoofing után a támadó megváltoztatja az ARP táblát, így a hamisított MAC térképeket tartalmaz és a fertőzés elkezdődik.



- Kivédése
  - Dynamic ARP Inspection használata
  - ARP forgalom monitorozása