Concepte de Securitate în LAN

Capitolul 10

ccna.ro
You Need To Know

Întrebarea zilei

Care sunt cele mai frecvente atacuri la nivelul legătură de date?

ccna.ro
You Need To Know

Frecvența atacurilor

ccna.ro
You Need To Know

Atacuri frecvente

- Distributed Denial of Service (DDoS)
  - Atac coordonat de mai multe dispozitive (zombies)
  - Scopul este degradarea/oprirea accesului public la o anumită resursă/website
- Data Breach
- Malware

ccna.ro
You Need To Know

Atacuri frecvente

- Distributed Denial of Service (DDoS)
- Data Breach
  - Atac în care serverele sau host-urile unei orgonizații sunt compromise
  - Informații confidențiale sunt “furate”
- Malware

Atacuri frecvente

- Distributed Denial of Service (DDoS)
- Data Breach
- Malware
  - Atac în care host-urile unei organizații sunt ținta unui software malițios
  - Ex. Ransomware

ccna.ro
You Need To Know

Network Security Devices

- VPN-Enabled Router
  - Oferă o conexiune sigură utilizatorilor la distanță peste o rețea publică în rețeaua organizației
  - Serviciile VPN pot fi integrate în firewall
- NGFW (Next-Generation FireWall)
- NAC (Network Access Control)

Network Security Devices

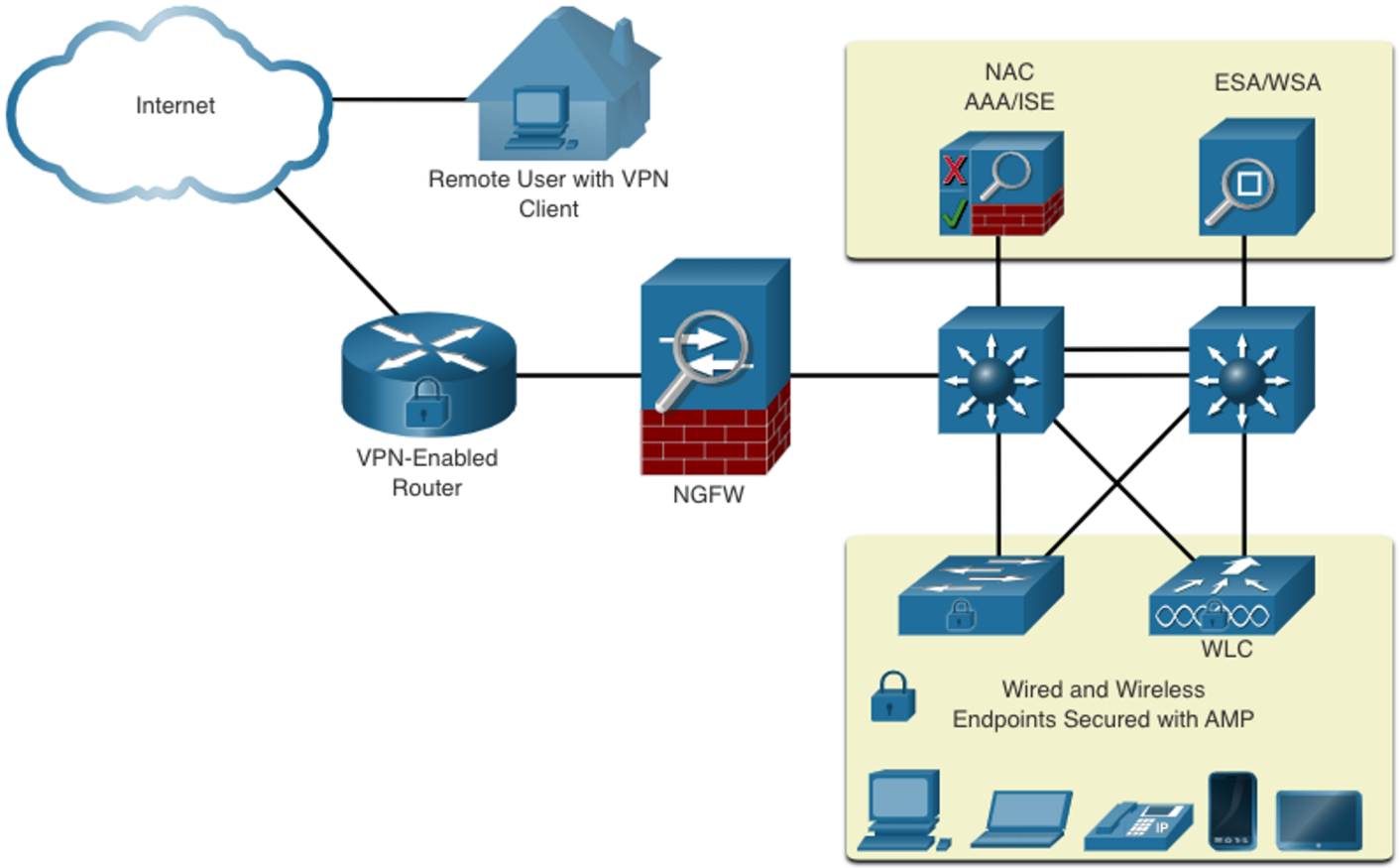
- VPN-Enabled Router
- NGFW (Next-Generation FireWall)
  - Oferă inspecția complete a unui pachet
  - Controlul aplicațiilor, filtrare de URL
- NAC (Network Access Control)

ccna.ro
You Need To Know

Network Security Devices

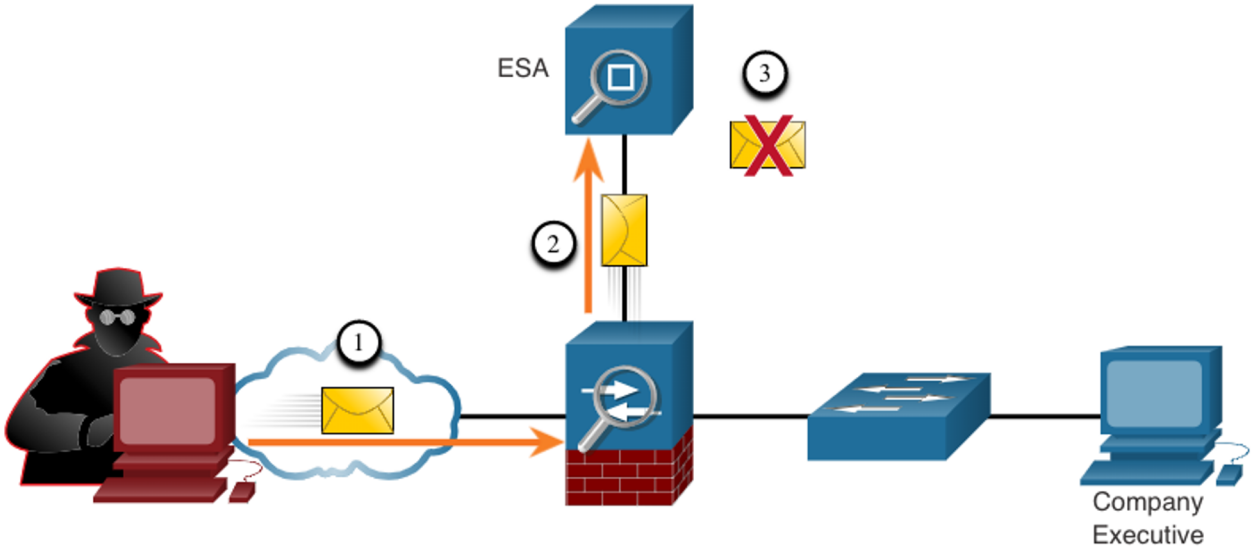
- VPN-Enabled Router
- NGFW (Next-Generation FireWall)
- NAC (Network Access Control)
  - Oferă servicii de tip AAA (authentication-authorization-accounting)

Secure topology



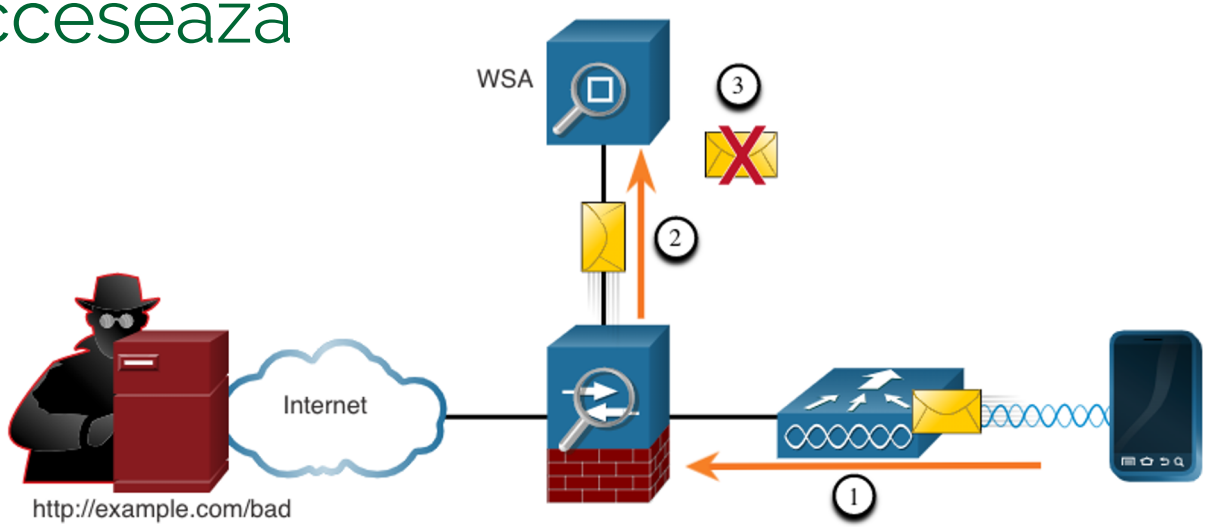
CESA

- Cisco Email Security Appliance
- Dispozitiv ce monitorizează SMTP



CWSA

- Cisco Web Security Appliance
- Dispozitiv ce controlează domeniile și aplicațiile pe care utilizatorii unei organizații le accesează



ccna.ro
You Need To Know

Access Control

ccna.ro
You Need To Know

Autentificarea clasică

- Autentificare locală cu parolă în clar

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

- Autentificare criptată prin SSH

```
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
```

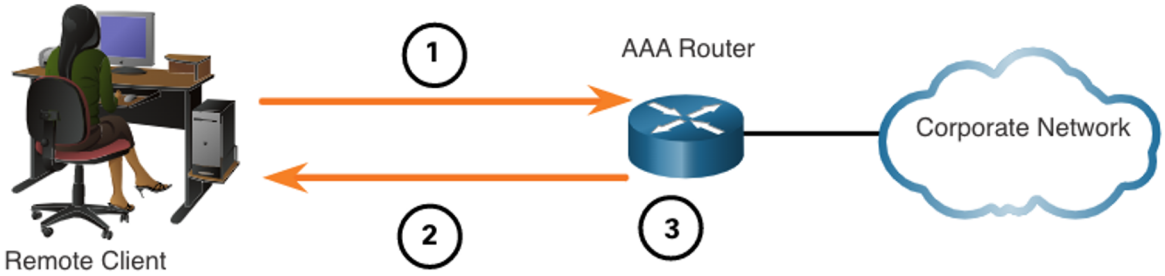

ccna.ro
You Need To Know

AAA

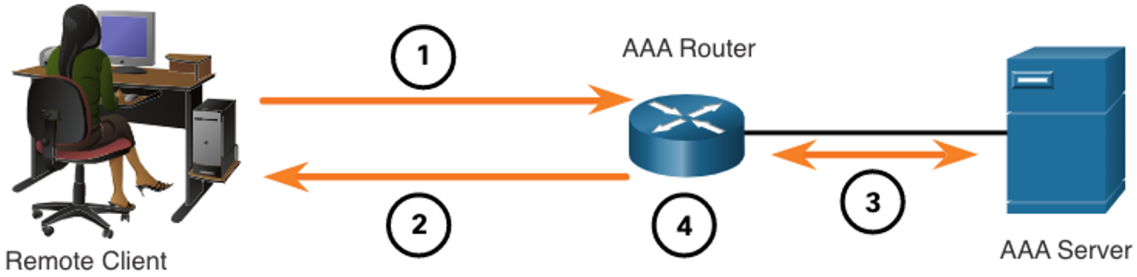
- Authentication
  - Autentificare – cine este utilizatorul
- Authorization
  - Autorizare – ce acțiuni are voie să facă utilizatorul
- Accounting
  - Contabilitate - Toate acțiunile sunt documentate/stocate

Autentificare AAA

- Locală

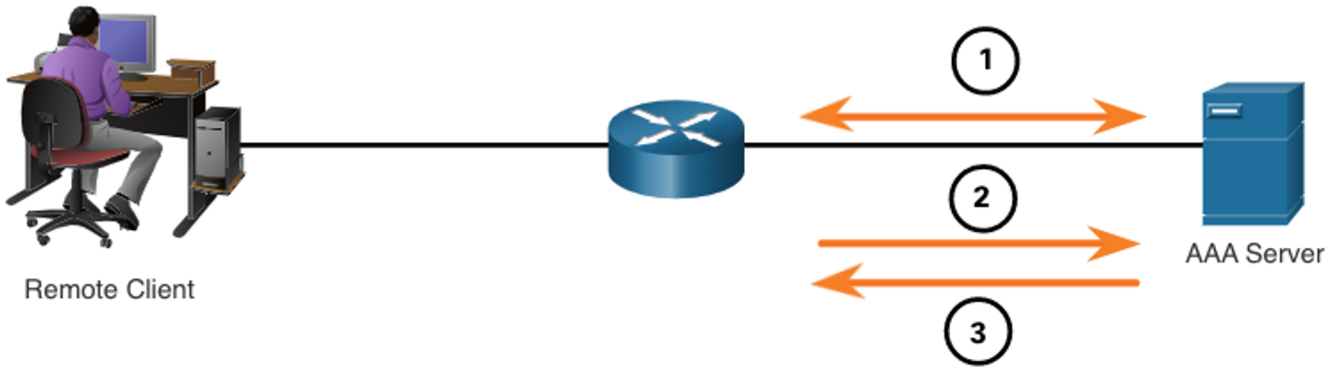


- Server-based



Autorizare AAA

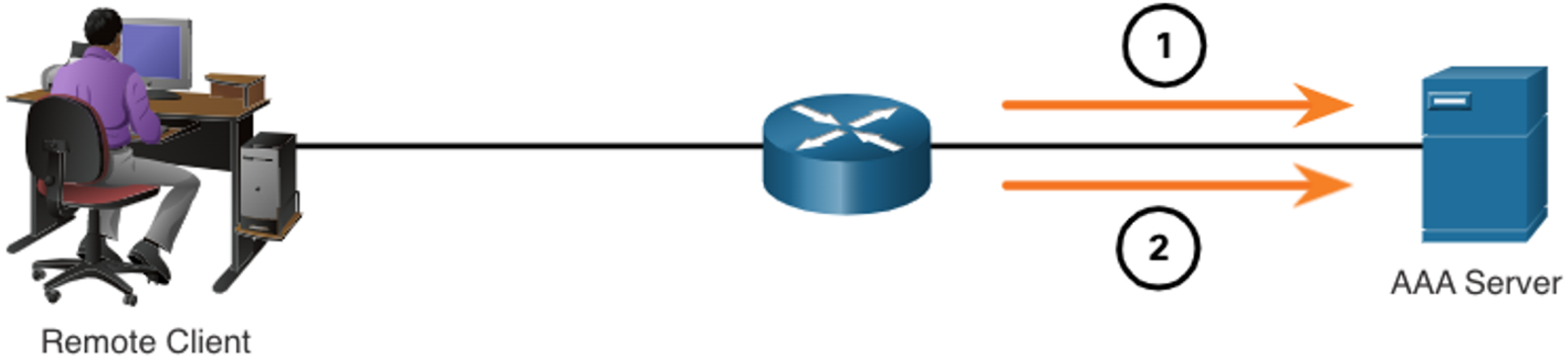
- Autorizarea este automată
- Utilizatorul nu trebuie să parcurgă pași suplimentari



ccna.ro
You Need To Know

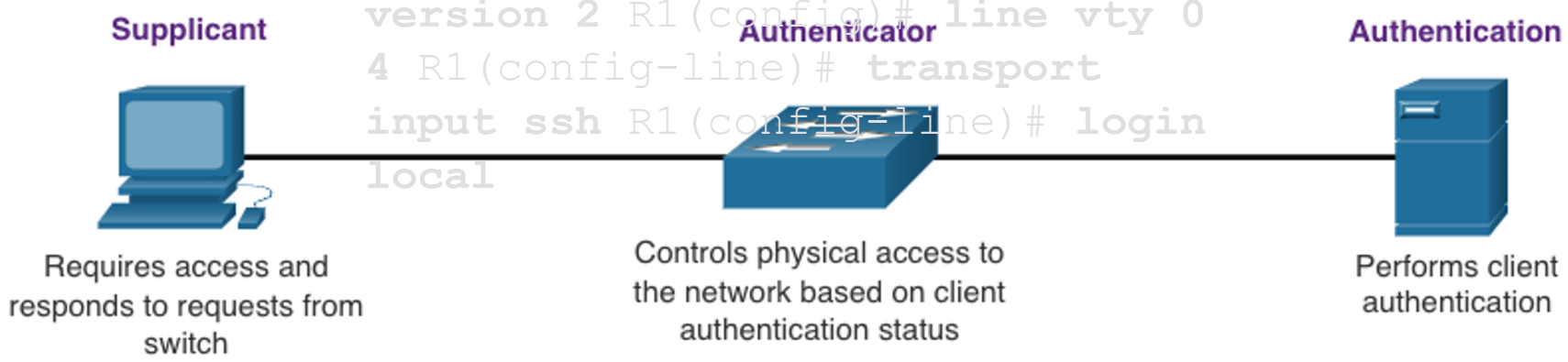
Contabilitate AAA

- Log-uri cu acțiunile utilizatorului
- Ex. comenzi de configurare, username, data și timpul conectării



802.1X

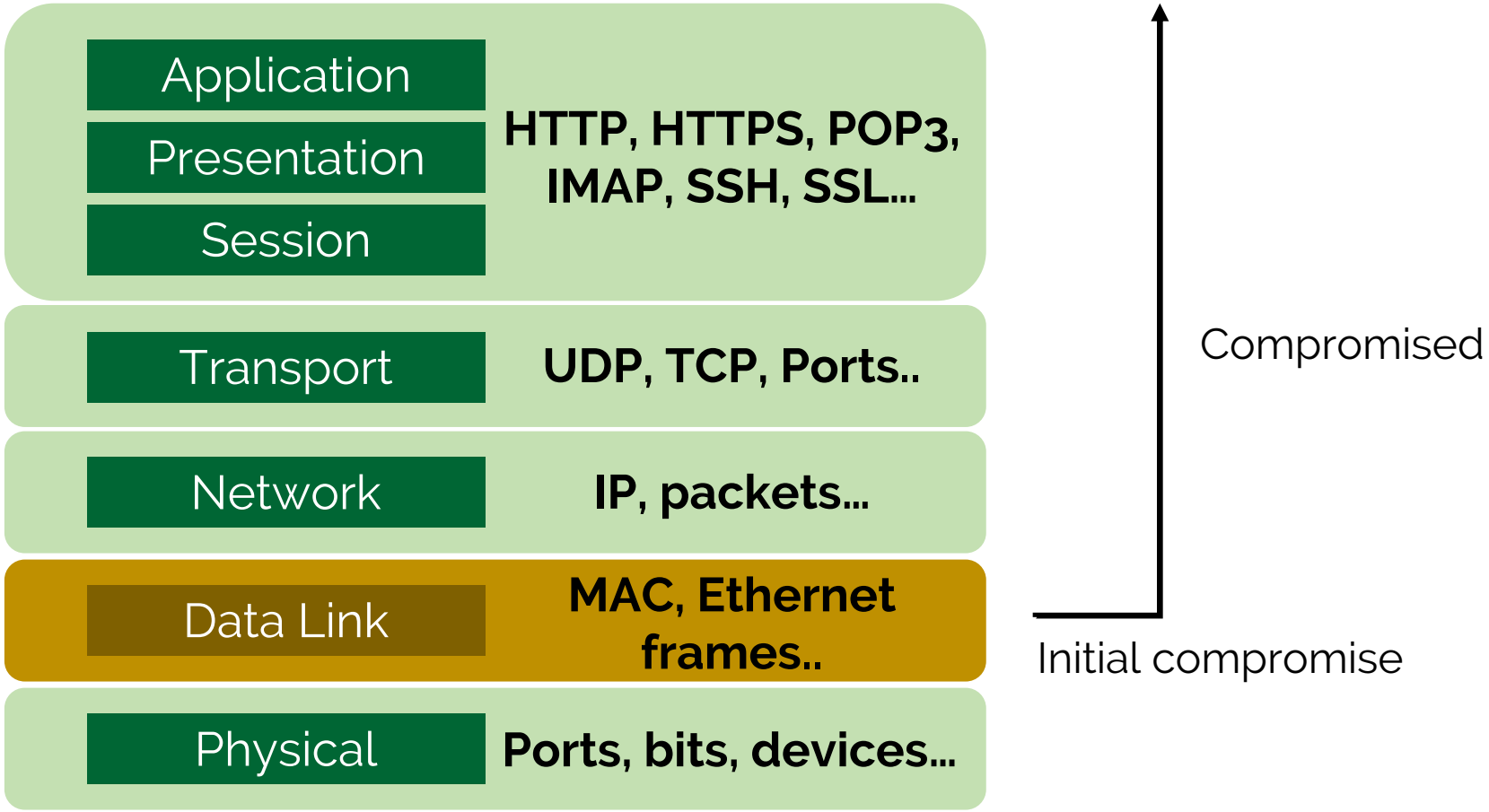
- Standardul IEEE 802.1X
- Control al accesului bazat pe porturi și pe un protocol de autentificare



Vulnerabilitățile nivelului legătură de date

ccna.ro
You Need To Know

Stiva OSI - Reminder



Switch Attack Categories

Categorie	Exemple
Atacuri tabela CAM	MAC Address Flooding attacks
Atacuri VLAN	VLAN hopping; VLAN double-tagging
Atacuri DHCP	DHCP starvation; DHCP spoofing
Atacuri ARP	ARP spoofing; ARP poisoning
Address Spoofing	MAC address and IP address spoofing
Atacuri STP	STP manipulation

Prevenție atacuri

Soluție	Descriere
Port Security	Prevents MAC address flooding; DHCP starvation
DHCP Snooping	Prevents DHCP starvation; DHCP spoofing
Dynamic ARP Inspection	Prevents ARP spoofing; ARP poisoning
IP Source Guard	Prevents MAC and IP spoofing

Reminder tabela CAM

- Switch primește cadru (frame)
  - Verifică sursa:
    - O are în tabela CAM -> reînnoiește timer-ul
    - Nu o are în tabela CAM -> adaugă MAC sursă <-> port sursă
  - Verifică destinația:
    - O are în tabela CAM -> trimite pe portul asociat
    - Nu o are în tabela CAM -> trimite pe toate porturile mai puțin cel de pe care a venit (flooding)

ccna.ro
You Need To Know

MAC Address Table Flooding

- Atacatorul “bombardează” switch-ul cu surse MAC false până când tabela CAM este plină
- Switch-ul tratează frame-urile ca pe unicast necunoscute, așa că face flood în toată rețeaua locală
- Un astfel de atac se poate realiza folosind tool-ul **macof**

Prevenire MAC flooding

- Port security
- Doar un anumit număr de adrese MAC sursă ce vor fi învățate pe un port

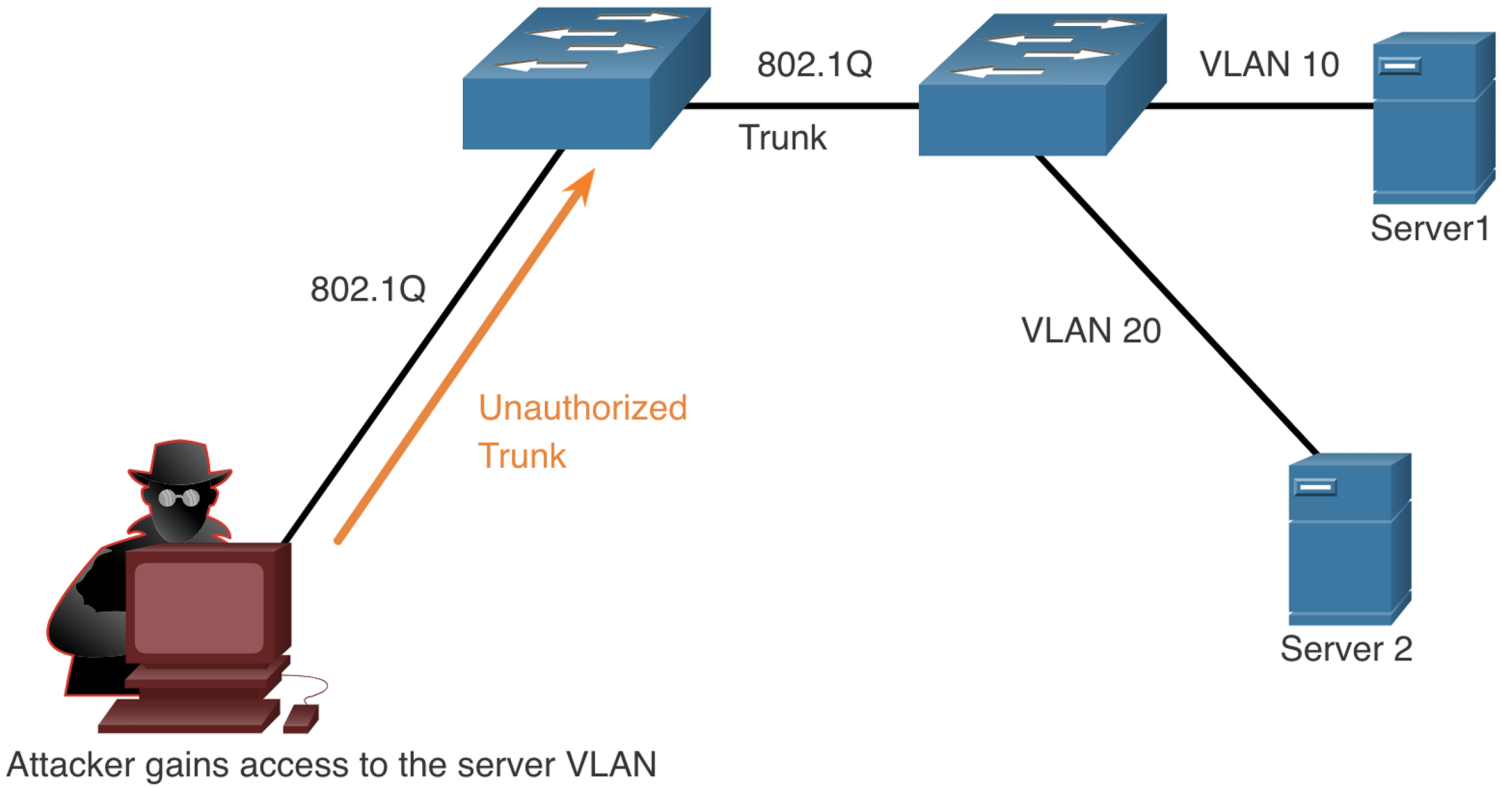
Atacuri în rețeaua locală

ccna.ro
You Need To Know

VLAN Hopping Attack

- Atacatorul se comportă ca un switch în LAN
- Configurează 802.1q și DTP pentru a forma o legătură trunk cu un alt switch din LAN
- O dată formată legătura, atacatorul poate trimite/primi trafic din orice VLAN

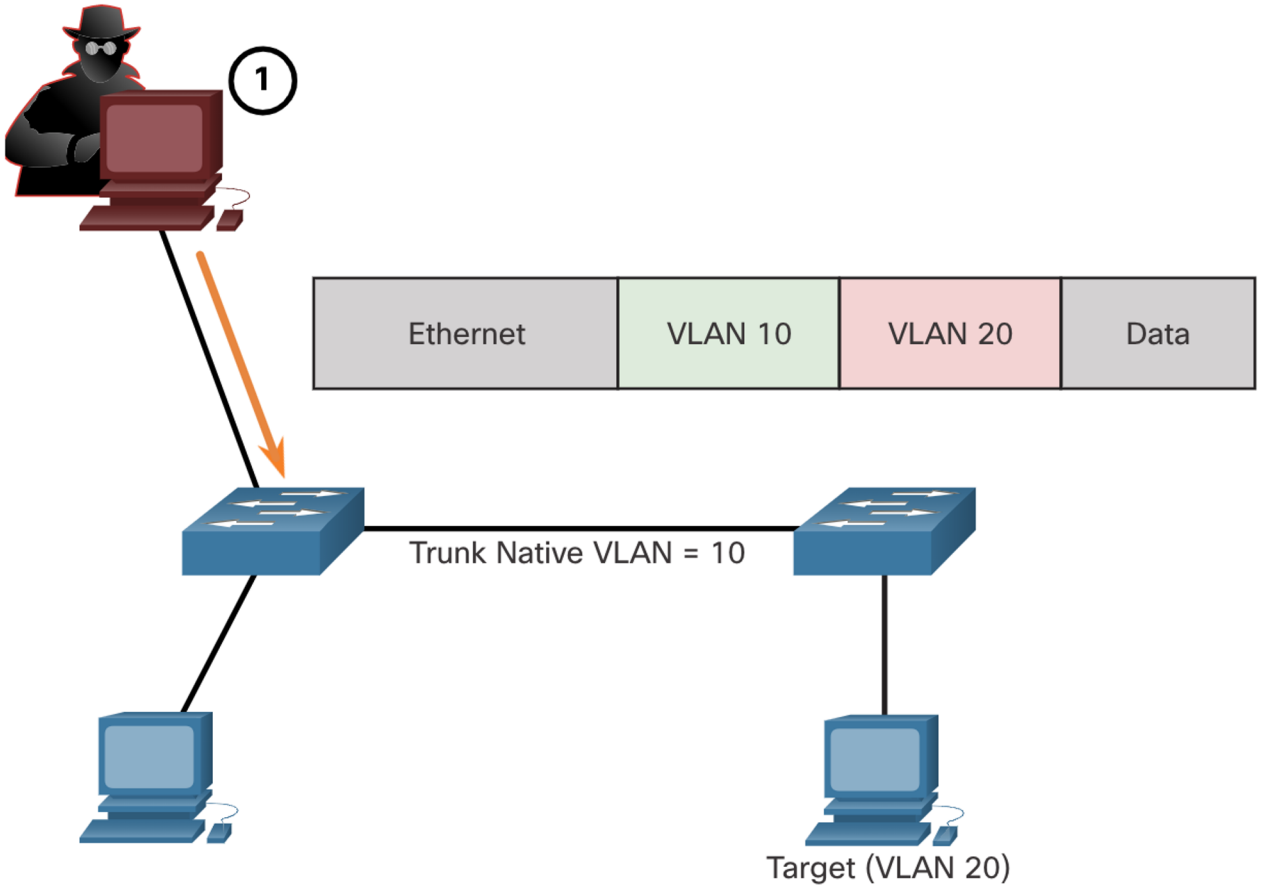
VLAN Hopping Attack



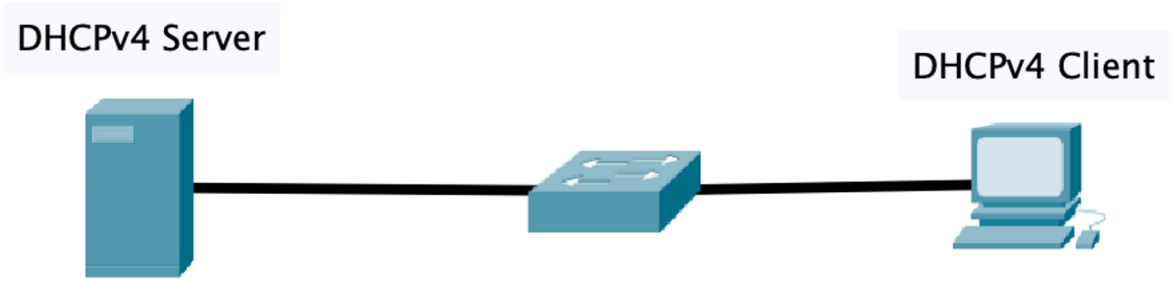
VLAN Double-Tagging Attack

- Atacatorul introduce un tag 802.1q suplimentar
- Astfel, cadrul poate ajunge la VLAN-uri atât din primul tag, cât și din al doilea

VLAN Double-Tagging Attack



DHCP messages - reminder



"Doresc o adresă IPv4"

DHCP Discover
Broadcast

DHCP Offer
Unicast

"Îți ofer o adresă IPv4 din pool-ul meu"

"Accept adresa oferită"

DHCP Request
Broadcast

DHCP ACK
Unicast

"Confirm acceptarea adresei"

ccna.ro
You Need To Know

DHCP Starvation Attack

- Atacatorul creează DoS (Denial of Service) al serviciului de DHCP
- Ex. tool-ul **Globber**
  - Generează mesaje DHCP Discovery cu adrese MAC sursă false
  - Toate adresele IP din pool-ul DHCP vor fi asignate unor stații inexistemte

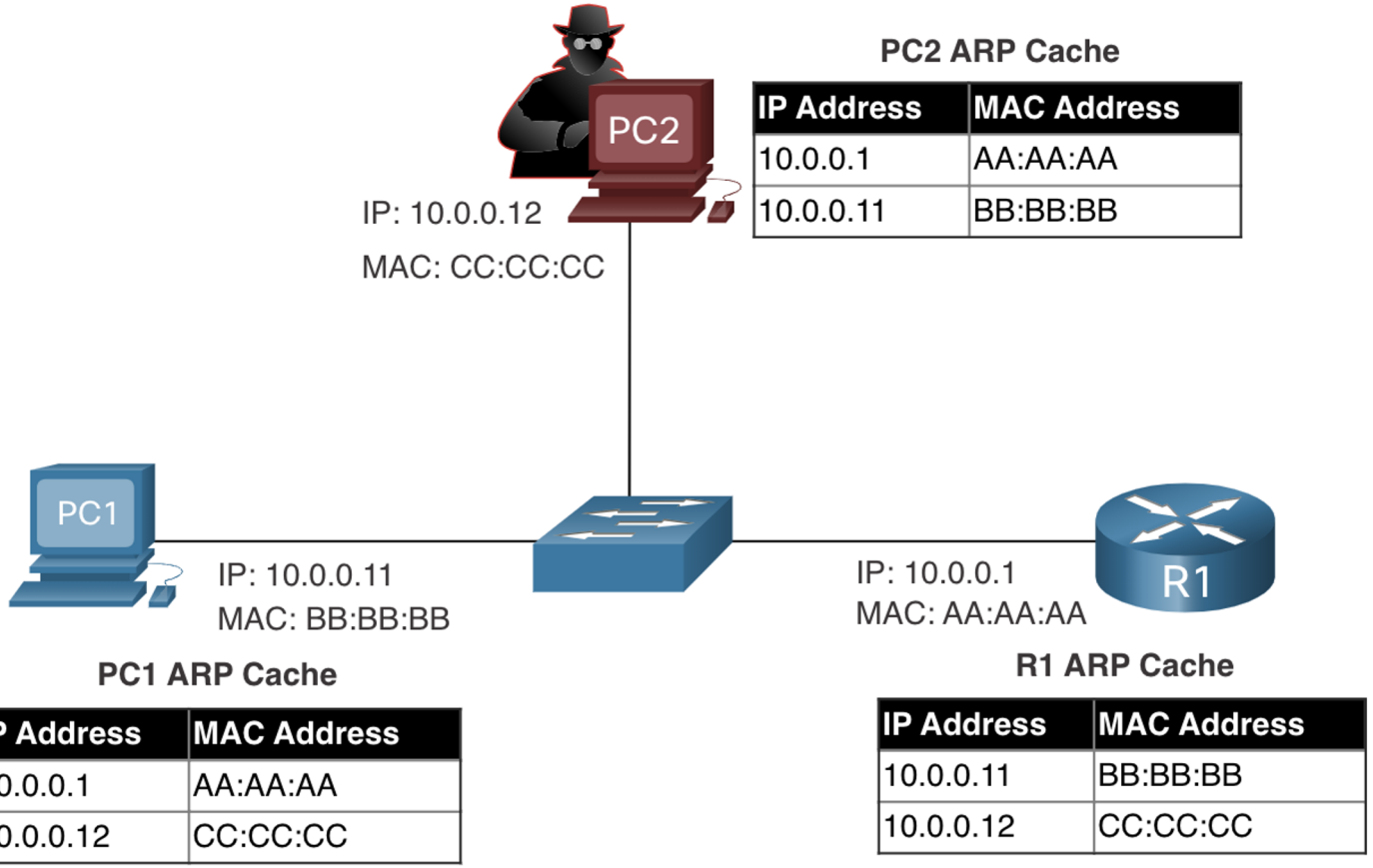
DHCP Spoofing Attack

- Atacatorul se conectează ca un server DHCP
- Va oferi servicii false clienților
  - Default gateway greșit (toate pachetele către internet vor trece prin atacator)
  - DNS Server greșit (clientul se va conecta la adrese web nefavorabile/malițioase)
  - Adresă IP greșită

ARP Attacks

- Pentru a afla MAC-ul unui host, o stație trimite un ARP Request
- Host-ul cu IP-ul cerut răspunde cu un ARP Reply
- Un atacator poate trimite un ARP Reply fals
- Toate stațiile din rețea vor asocia IP-ul respectiv cu stația atacatorului (ex. Default Gateway)

ARP Attacks (1)



PC2 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.11	BB:BB:BB

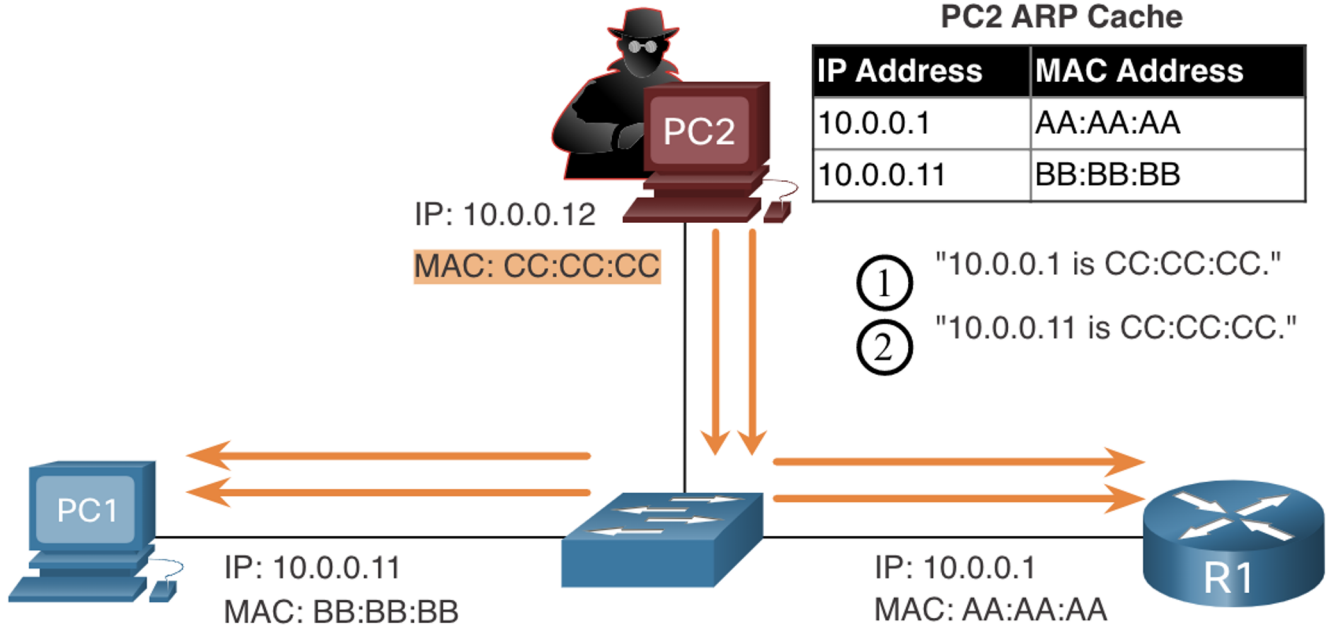
PC1 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.12	CC:CC:CC

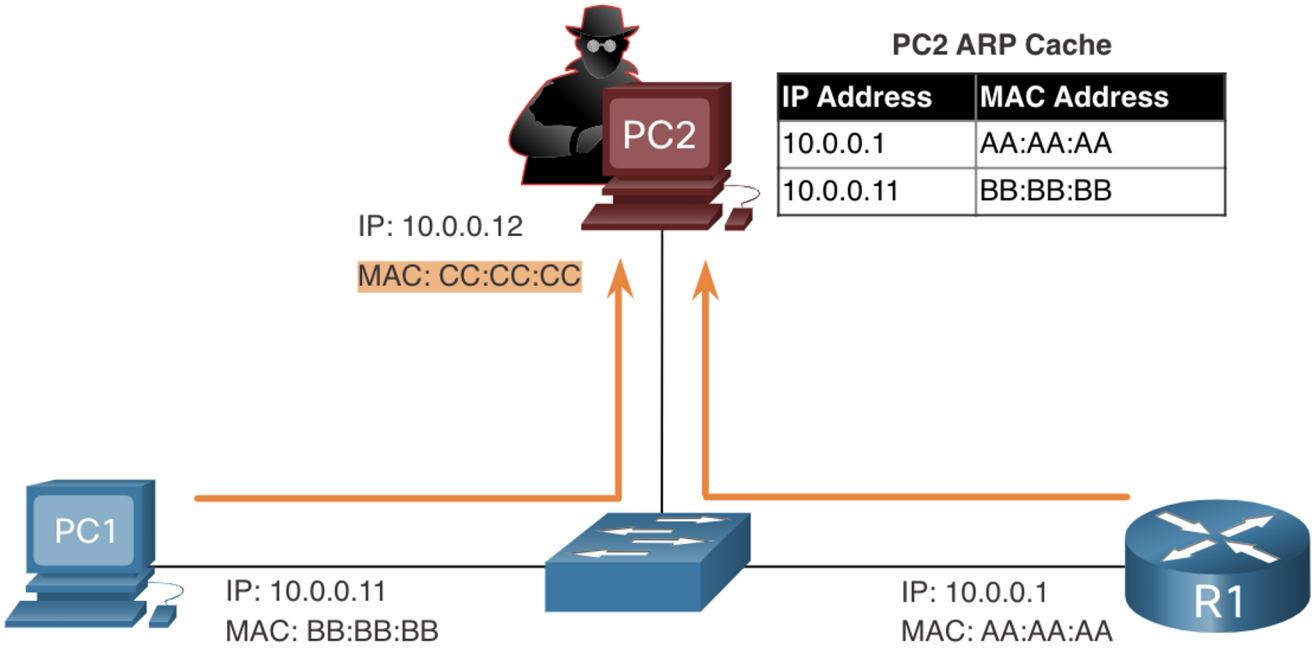
R1 ARP Cache

IP Address	MAC Address
10.0.0.11	BB:BB:BB
10.0.0.12	CC:CC:CC

ARP Attacks (2)



ARP Attacks (3)



PC2 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.11	BB:BB:BB

PC1 ARP Cache

IP Address	MAC Address
10.0.0.1	CC:CC:CC
10.0.0.12	CC:CC:CC

R1 ARP Cache

IP Address	MAC Address
10.0.0.11	CC:CC:CC
10.0.0.12	CC:CC:CC

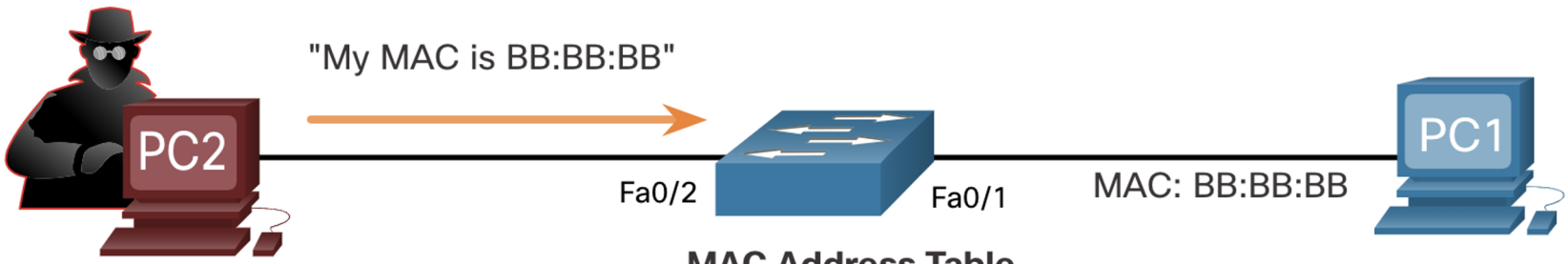
ccna.ro
You Need To Know

Address spoofing attack

- Atacatorul preia o adresă IP/MAC validă a unei stații din rețeaua locală
- Este greu de prevenit, dacă atacatorul se află deja în LAN
- Poate fi prevenit totuși cu IPSG

ccna.ro
You Need To Know

Address spoofing attack



MAC Address Table

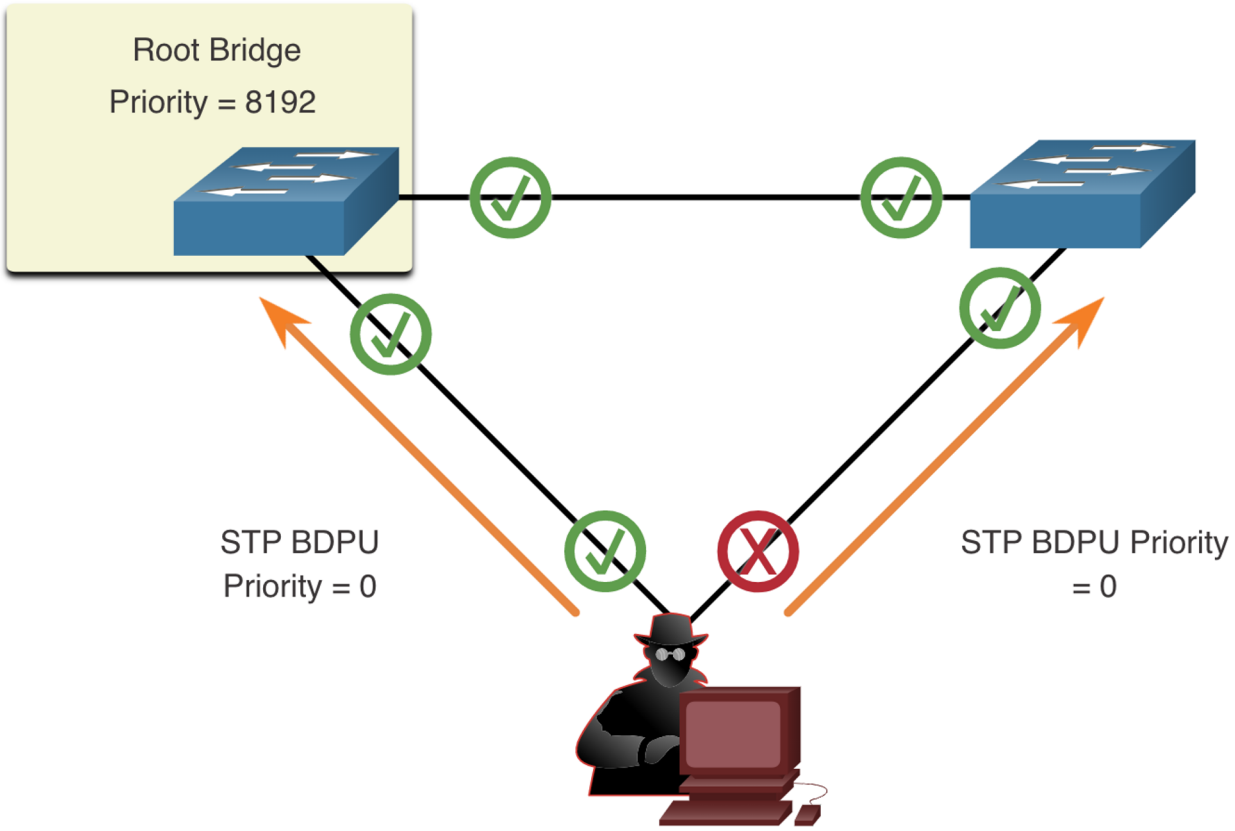
Port	MAC Address
Fa0/1	
Fa0/2	BB:BB:BB

ccna.ro
You Need To Know

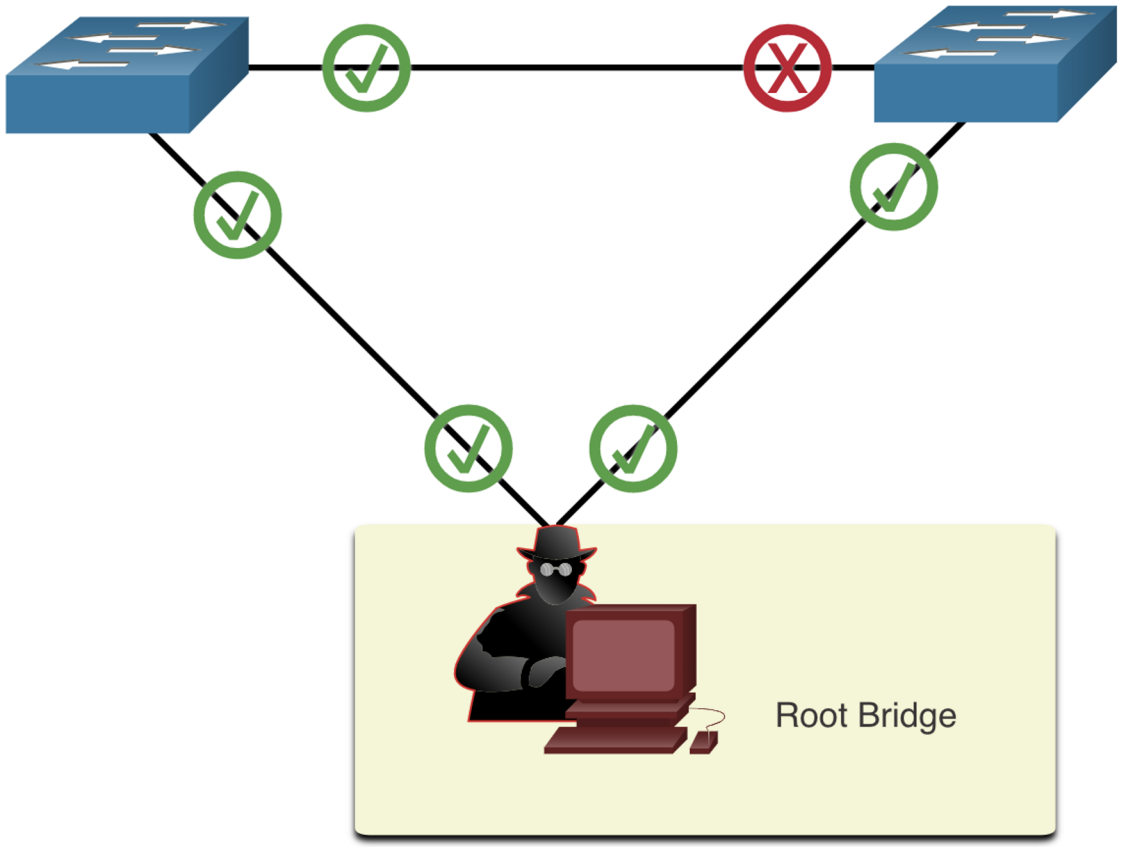
STP Attack

- Atacatorul se conectează ca un switch
- Va trimite BPDU-uri cu diferiți parametrii
- Forțează recalcularea rolurilor în topologie
  - Root ports, Designated ports, Blocked ports
  - Root Bridge, Non-Root Bridge

STP Attack (1)



STP Attack (2)



CDP Reconnaissance

- Cisco Discovery Protocol
- Descoperă alte dispozitive CDP enabled din LAN
- Folosit pentru a configura automat conexiunile între dispozitivele CDP
- Un atacator poate intercepta cadrele CDP (necriptate)

Răspunsul zilei

Răspunsul zilei

Care sunt cele mai frecvente atacuri la nivelul legătură de date?

ccna.ro
You Need To Know