Configurări pentru Securitate în LAN

Capitolul 12

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Întrebarea zilei

Cum putem preveni atacurile în LAN?

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Atacuri tabela CAM

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Atacuri tabela CAM

- 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**

© 2020 ccna.ro Toate drepturile rezervate

Prevenire atacuri

- Închiderea porturilor nefolosite
- Configurare port security
  - Detalii în prezentarea 2 - Basic Switched Concepts

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Atacuri VLAN

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Atacuri VLAN

- VLAN Hopping Attacks
- 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

© 2020 ccna.ro Toate drepturile rezervate

Prevenire atacuri VLAN

1. Dezactivare DTP pe porturile ce nu necesită trunking
2. Dezactivare porturi nefolosite și asignarea lor în VLAN-uri nefolosite
3. Activarea manuală a porturilor trunk
4. Dezactivare DTP pe porturile ce necesită trunking
5. Setarea VLAN-ului native într-un VLAN diferit de 1 (cel default)

© 2020 ccna.ro Toate drepturile rezervate

Configurare (1)

- Presupunem următorul Switch scenariu:
  - Porturile fa0/1-fa0/16 sunt active access
  - Porturile fa0/17-fa0/24 nu sunt folosite
  - Porturile fa0/21-fa0/24 sunt trunk

© 2020 ccna.ro Toate drepturile rezervate

Configurare (2)

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
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)# exit
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
```

© 2020 ccna.ro Toate drepturile rezervate

Atacuri DHCP

© 2020 ccna.ro Toate drepturile rezervate

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
- Soluție: Port Security

© 2020 ccna.ro Toate drepturile rezervate

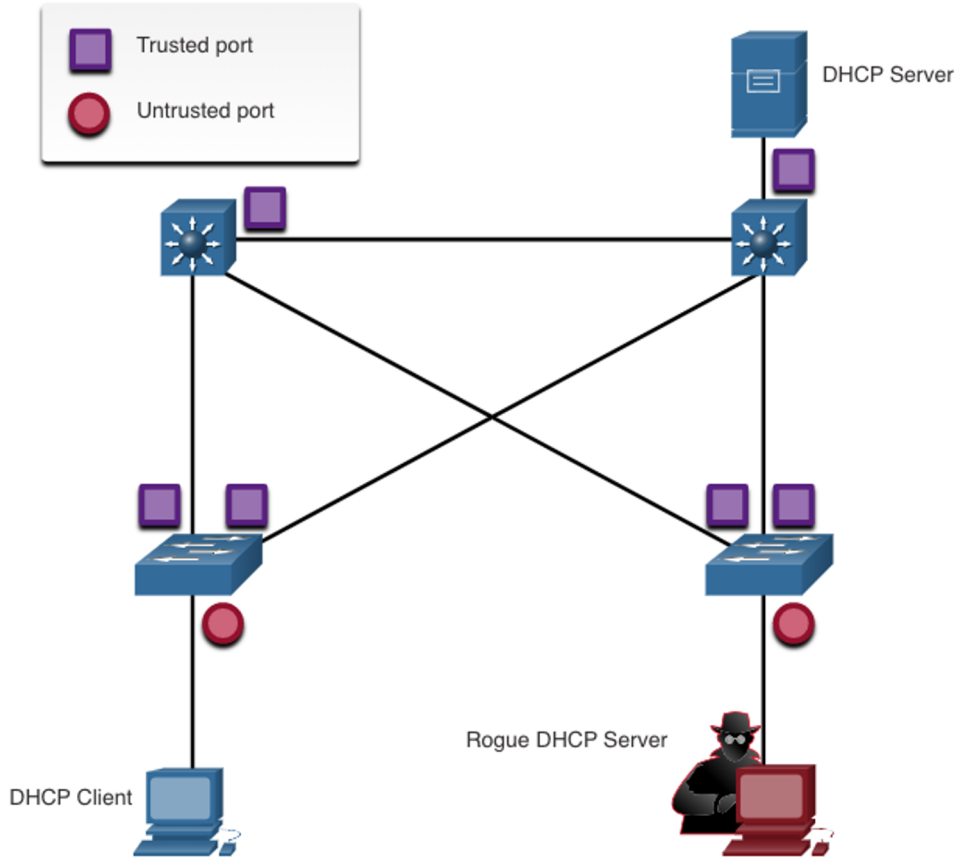
DHCP Spoofing Attack

- 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
- Soluție: DHCP Snooping

© 2020 ccna.ro Toate drepturile rezervate

Prevenire: DHCP Snooping

- DHCP Snooping nu se folosește de adrese MAC sursă
- Determină dacă mesajele DHCP provin dintr-o sursă administrativă de încredere
- Filtrează mesajele DHCP și limitează traficul DHCP provenit din surse nesigure



© 2020 ccna.ro Toate drepturile rezervate

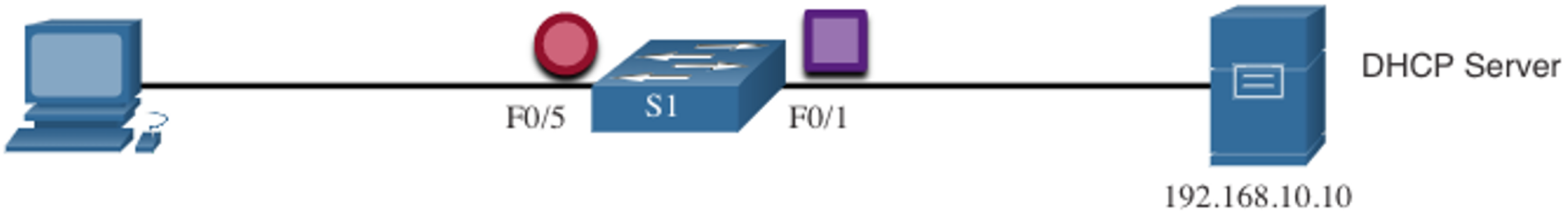
ccna.ro
You Need To Know

DHCP Snooping

1. Activare DHCP Snooping
2. Pe porturile sigure, activare DHCP Snooping Trust
3. Limitarea numărului de mesaje DHCP Discovery pe secundă provenite din surse nesigure
4. Activare DHCP Snooping per VLAN

© 2020 ccna.ro Toate drepturile rezervate

Configurare




```
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
```

© 2020 ccna.ro Toate drepturile rezervate

Atacuri ARP

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Atacuri ARP

- 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)

© 2020 ccna.ro Toate drepturile rezervate

Prevenire atacuri ARP

- DAI (Dynamic ARP Inspection)
- Folosește DHCP Snooping
- Interceptează toate mesajele ARP pe porturi nesigure
- Verifică fiecare pachet interceptat pentru o asociere validă între IP-MAC
- Face drop la pachete invalide

© 2020 ccna.ro Toate drepturile rezervate

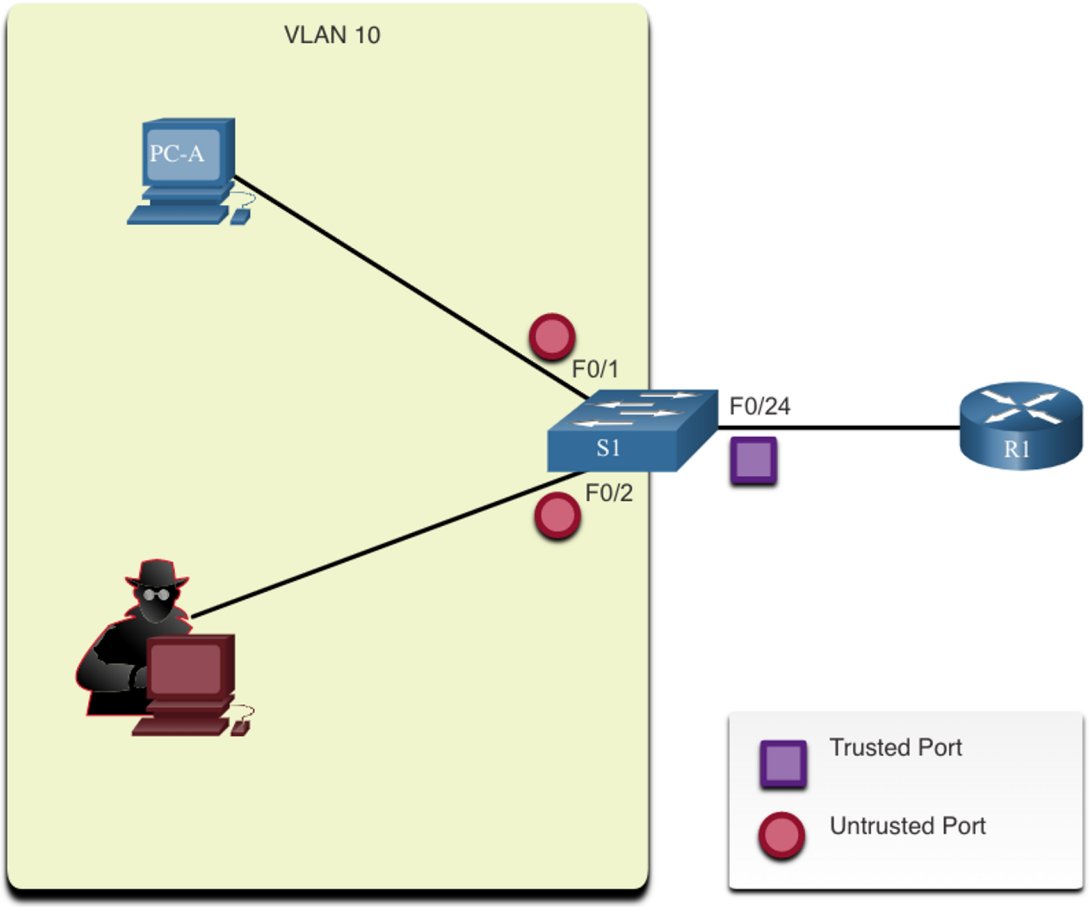
Dynamic ARP Inspection

1. Activare DHCP Snooping global
2. Activare DHCP Snooping per VLAN-uri selectate
3. Activare DAI pe VLAN-uri selectate
4. Configurarea interfețelor sigure pentru DHCP Snooping și DAI

© 2020 ccna.ro Toate drepturile rezervate

Configurare

```
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
```



© 2020 ccna.ro Toate drepturile rezervate

Atacuri STP

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Atacuri STP

- 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

© 2020 ccna.ro Toate drepturile rezervate

Prevenire atacuri STP

- PortFast
  - Forțează portul access sau trunk să treacă în starea de forwarding din starea de blocking
  - Se ignoră stările intermediare listening și learning
  - Se aplică tuturor porturilor către end device-uri
- BPDU Guard

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Prevenire atacuri STP

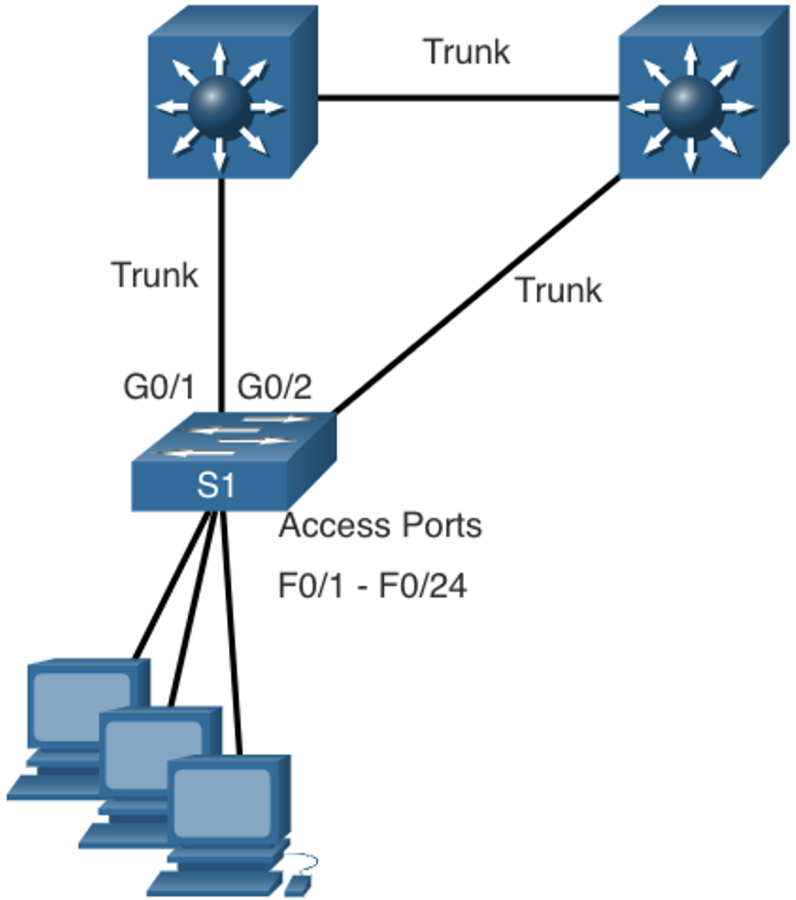
- PortFast
- BPDU Guard
  - Dezactivează portul ce are configurat PortFast
  - Se aplică tuturor porturilor către end device-uri

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Configurare (1)

- Porturile access vor trebui configurate cu PortFast și BPDU Guard



© 2020 ccna.ro Toate drepturile rezervate

Configurare (2)

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
S1(config-if)# exit
S1(config)# spanning-tree portfast default
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
```

© 2020 ccna.ro Toate drepturile rezervate

ccna.ro
You Need To Know

Răspunsul zilei

© 2020 ccna.ro Toate drepturile rezervate

Răspunsul zilei

Cum putem preveni atacurile în LAN?

© 2020 ccna.ro Toate drepturile rezervate