LAN Security

Übersicht

LAN Attack	Attack Mitigation
MAC Table Attack	
- MAC Address Flooding	Port Security
VLAN Attack	
- VLAN Hopping	Mitigate VLAN Hopping
- VLAN Double Tagging	
DHCP Attack	
- DHCP Starvation	Port Security, DHCP Snooping
- DHCP Spoofing	Port Security, DHCP Snooping
ARP Attack	
- ARP Spoofing	DAI
- ARP Poisoning	DAI
Address Spoofing	
- MAC Address Spoofing	IPSG
- IP Address Spoofing	IPSG
STP Attack	
- STP Manipulation	BPDU Guard
Reconnaissance Attack	
- CDP Reconnaissance	Deactivate CDP

Port Security

kohnlehome.de/netz/port-security.pdf

Mitigate VLAN Hopping

- Manually enable access ports (switchport mode access)
- Manually enable trunk ports (switchport mode trunk)
- Disable DTP (switchport nonegotiate)
- Set native VLAN other than VLAN 1
- Disable unused ports, put them in an unused VLAN

DHCP Snooping

- DHCP-Server-Frames von Untrusted Ports werden nicht weitergeleitet ⇒ kein DHCP-Spoofing
- Die Anzahl von DHCP-Client-Frames auf Untrusted Ports kann limitiert werden ⇒ kein DHCP-Starvation

1. Global UND für VLANS aktivieren

```
SWITCH(config)# ip dhcp snooping                    # alle Ports auf Untrusted
SWITCH(config)# ip dhcp snooping vlan 5,10-12       # VLANs konfigurieren
```

2. Trusted Ports festlegen

```
SWITCH(config-if)# ip dhcp snooping trust           # Trusted Port
```

3. (Optional) Untrusted Ports konfigurieren

```
SWITCH(config-if)# ip dhcp snooping limit rate 6    # Untrusted Port: 6 packets per second
```

4. Diagnose

```
SWITCH# show ip dhcp snooping
SWITCH# show ip dhcp snooping binding
```

DAI (Dynamic ARP Inspection)

- Voraussetzung: DHCP Snooping
- ARP-Frames auf Untrusted Ports werden überprüft
  - QuellMAC: Vgl. Ethernet-Header - ARP-Daten
  - ZielMAC: Vgl. Ethernet-Header - ARP-Daten
  - IP: DHCP
  - Begrenzung der Anzahl von ARP-Requests

1. DHCP Snooping akitiveren

```
SWITCH(config)# ip dhcp snooping
SWITCH(config)# ip dhcp snooping vlan 5,10-1
SWITCH(config-if)# ip dhcp snooping trust           # Trusted Port
```

2. DAI für VLANs aktiveren

```
SWITCH(config)# ip arp inspection vlan 5,10-12
```

3. Trusted Ports festlegen

```
SWITCH(config-if)# ip arp inspection trust          # Trusted Port
```

4. (Optional) DAI Modus festlegen

```
SWITCH(config)# ip arp inspection validate src-mac dst-mac ip
```

5. Diagnose

```
SWITCH# show ip arp inspection
SWITCH# show ip arp inspection interfaces
SWITCH# show ip arp inspection statistics
```

IPSG (IP Source Guard)

- Voraussetzung: DHCP Snooping
- QuellMAC und QuellIP von eingehenden Frames in untrusted Ports werden mit der DHCP snooping database verglichen

BPDU Guard und Portfast

- BPDU Guard: Switchport wird deaktiviert, sobald er ein Spanning-Tree-BPDU-Frame empfängt
- Portfast: Switchport springt sofort in den Forwarding-Modus
- Sollte an Edge-Ports konfiguriert werden

1a. Konfiguration BPDU Guard

```
SWITCH(config-if)# spanning-tree bpduguard enable
 oder
SWITCH(config)# spanning-tree bpduguard default
```

1b. Konfiguration Portfast

```
SWITCH(config-if)# spanning-tree portfast
 oder
SWITCH(config)# spanning-tree portfast default
```

2. Diagnose

```
SWITCH# show spanning-tree summary
```

Deactivate CDP

```
SWITCH(config)# no cdp run
 oder
SWITCH(config-if)# no cdp enable
```