

[zurück](#)

# VLAN-Sicherheit & Switching-Security

VLANs sorgen für logische Netztrennung – aber nur korrekt konfiguriert sind sie auch sicher. Switching-Security umfasst alle Maßnahmen, die Layer-2-Angriffe verhindern und Manipulationen im LAN unterbinden.

Diese Seite behandelt:

- VLAN-Hopping
- Native VLAN Sicherheit
- Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- BPDU Guard / Root Guard
- Sturmschutz (Broadcast- & Multicast-Limits)

## 1. VLAN-Hopping

VLAN-Hopping bedeutet, dass ein Angreifer versucht, in ein anderes VLAN zu gelangen, obwohl sein Port dies eigentlich nicht erlaubt.

Zwei typische Angriffe:

### a) Double-Tagging

Angreifer sendet Frames mit **zwei VLAN-Tags**:

```
[Outer Tag: Native VLAN]
[Inner Tag: Ziel-VLAN]
```

Wenn der Switch die Native-VLAN-Tags entfernt → gelangt das Paket unter Umständen in ein anderes VLAN.

## Schutz

- Native VLAN **nicht in Nutzung** oder auf eigenes, leeres VLAN legen
- Native VLAN  $\neq$  VLAN 1
- VLAN 1 NICHT produktiv verwenden
- nur explizit erlaubte VLANs auf Trunks

## b) Switch-Spoofing

Angreifer versucht, den Switch dazu zu bringen, seinen Port als **Trunk-Port** zu behandeln.

Beispiel:

```
DTP (Dynamic Trunking Protocol) manipulieren → trunk negotiation
```

## Schutz

- alle Access-Ports fest auf access setzen:

```
switchport mode access  
switchport access vlan X
```

- DTP deaktivieren (Cisco):

```
switchport nonegotiate
```

---

## 2. Native VLAN Sicherheit

Das Native VLAN ist das VLAN **ohne Tag** auf einem Trunk.  
Standard = VLAN 1 → **immer unsicher**.

### Best Practices

- Native VLAN ändern auf ein ungenutztes VLAN (z. B. VLAN 99)
- kein produktives Gerät in Native VLAN
- nur definierte VLANs taggen

```
Trunk:
```

```
VLAN 10 (tagged)
VLAN 20 (tagged)
VLAN 99 (native, ungenutzt)
```

---

## 3. Port Security

Port Security schützt Access-Ports vor:

- MAC-Spoofing
- MAC-Flooding
- unerlaubten Geräten

### Beispiel Cisco-Konfiguration

```
interface Gi0/10
  switchport mode access
  switchport access vlan 10
  switchport port-security
  switchport port-security maximum 1
  switchport port-security violation shutdown
  switchport port-security mac-address sticky
```

Funktionen:

- maximale MAC-Adressen pro Port
- Sticky MAC (lernt automatisch)
- Shutdown bei Verstoß

---

## 4. DHCP Snooping

Hatten wir bereits ausführlich – Teil der VLAN-Security:

Schützt vor:

- Rogue DHCP-Servern
- falschen IP-Konfigurationen
- Manipulation von Gateway/DNS

Bindet Basis für:

- **IP Source Guard**
  - **Dynamic ARP Inspection**
- 

## 5. Dynamic ARP Inspection (DAI)

DAI verhindert ARP-Spoofing / ARP-Poisoning.

Angreifer versucht:

```
Ich bin das Gateway. Schickt mir euren Traffic.
```

DAI nutzt die DHCP Snooping Binding Table:

```
MAC ↔ IP ↔ Port
```

Wenn ARP nicht passt → blockiert.

### Beispiel Cisco

```
ip arp inspection vlan 10
```

---

## 6. IP Source Guard

Schützt Ports vor IP-Spoofing.

Nur IPs, die in der DHCP-Snooping-Tabelle stehen, dürfen vom Port ausgehen.

Schema:

```
MAC A darf nur IP 192.168.10.20 senden → sonst block
```

## 7. STP-Sicherheit: BPDU Guard & Root Guard

Spanning Tree Protocol (STP) schützt das LAN vor Schleifen.  
Aber Angreifer können BPDUs senden, um Root Bridge zu manipulieren.

### a) BPDU Guard

Blockiert Ports, wenn sie BPDUs empfangen.

Perfekt für Access-Ports.

```
spanning-tree portfast
spanning-tree bpduguard enable
```

### b) Root Guard

Verhindert, dass ein unerlaubter Switch Root wird.

```
spanning-tree guard root
```

## 8. Storm Control (Broadcast-, Multicast- & Unicast-Limits)

Schützt vor:

- Broadcast-Stürmen
- Loop-Katastrophen
- schlecht programmierten Geräten (z. B. Kameras)

Beispiel Cisco:

```
storm-control broadcast level 5
storm-control multicast level 5
```

## 9. Trunk-Sicherheit

- nur nötige VLANs auf Trunk erlauben:

```
switchport trunk allowed vlan 10,20
```

- Native VLAN sichern (siehe oben)
- DTP deaktivieren (keine automatischen Trunks)

## 10. Access-Port-Härtung

Standard-Template:

```
switchport mode access
switchport access vlan X
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping trust [ ] (nur Uplinks!)
ip arp inspection limit rate 15
```

## Zusammenfassung

- VLAN-Hopping → verhindern durch Native VLAN + feste Access-Ports
  - Port Security → verhindert MAC-Spoofing & unbekannte Geräte
    - \* DHCP Snooping → schützt IP-Konfiguration
    - \* DAI → schützt ARP
    - \* IP Source Guard → schützt IP/MAC-Zuordnung
    - \* BPDU Guard → schützt STP vor Angriffen
    - \* Storm Control → schützt vor Broadcast-Stürmen
    - \* Nur notwendige VLANs auf Trunks → Minimierungsprinzip
    - \* VLAN 1 NICHT nutzen → Sicherheitsrisiko

From:

<http://wiki.nctl.de/dokuwiki/> - `Veni. Vidi. sudo rm -rf / vici.`

Permanent link:

[http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:vlan\\_sicherheit&rev=1764839252](http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:vlan_sicherheit&rev=1764839252)

Last update: **04.12.2025 10:07**

