

[zurück](#)

DHCP Snooping - Grundlagen & Sicherheit

DHCP Snooping ist eine Sicherheitsfunktion auf Switches, die gefälschte DHCP-Server („Rogue DHCP“) blockiert.

Sie sorgt dafür, dass nur **vertrauenswürdige Ports** DHCP-Antworten senden dürfen.

Warum ist DHCP Snooping wichtig?

Ohne Schutz kann *jedes* Gerät im Netzwerk so tun, als wäre es ein DHCP-Server.

Angriffsszenario:

- Angreifer schließt Laptop an
- startet eigenen DHCP-Server
- verteilt falsche IPs, Gateways, DNS-Server
- Opfer gerät in ein Fake-Netz („Man-in-the-Middle“)

Auswirkungen:

- Ausfall kompletter Netzbereiche
- Umleitung des gesamten Traffics
- DNS-Manipulation
- Sicherheitsvorfälle

DHCP Snooping verhindert genau das.

Wie funktioniert DHCP Snooping?

DHCP Snooping unterscheidet:

- **Trusted Ports**
 - **Untrusted Ports**

Trusted Ports

- dürfen DHCP-Server-Antworten senden
 - * typischerweise Uplinks, Router, Firewall

Untrusted Ports

- alle normalen Access-Ports
 - * DHCP-Server-Antworten werden blockiert
 - * nur DHCP-Client-Anfragen erlaubt

ASCII-Illustration:

[Router/DHCP] --(trusted)-- [Switch] --(untrusted)-- PCs

DHCP Snooping Binding Table

Der Switch führt eine Tabelle, die alle gültigen DHCP-Leases speichert:

MAC-Adresse	IP-Adresse	VLAN	Port
-----	-----	---	---
A4:5E:60:3B:7D:12	192.168.10.20	10	5
3C:5A:B4:44:11:08	192.168.10.33	10	7

Diese Tabelle dient als Grundlage für weitere Security-Funktionen:

- **IP Source Guard**
 - **Dynamic ARP Inspection (DAI)**

Vorteile von DHCP Snooping

- Schutz vor Rogue DHCP-Servern
 - legt gültige MAC-IP-Port-Beziehungen fest
 - * schützt ARP und IP-Zuordnungen
 - * integriert sich mit NAC-Systemen
 - * unverzichtbar in Unternehmensnetzwerken

Ablauf im Detail

1. Client sendet DHCP Discover (untrusted → erlaubt)
2. Switch leitet Anfrage an trusted DHCP-Server weiter
3. DHCP-Server sendet OFFER / ACK auf trusted Port
4. Switch prüft Herkunft → nur trusted Ports akzeptiert
5. Switch trägt Lease in Binding Table ein
6. Client erhält gültige IP

Konfiguration - Cisco-Beispiel

```
ip dhcp snooping
ip dhcp snooping vlan 10,20,30

interface Gi0/1
  ip dhcp snooping trust      ← Uplink

interface Gi0/10
  ip dhcp snooping limit rate 20 ← Anti-Flood
```

Konfiguration - allgemeiner Ablauf (herstellernerneutral)

1. DHCP Snooping global aktivieren
2. VLANs definieren, in denen DHCP Snooping gilt
3. Uplink-Port(s) trusted setzen
4. Alle Access-Ports bleiben untrusted
5. Optional Rate-Limits setzen
6. Binding Table aktivieren

DHCP Snooping + ARP-Schutz

Mit aktivem Snooping kann DAI (Dynamic ARP Inspection) prüfen:

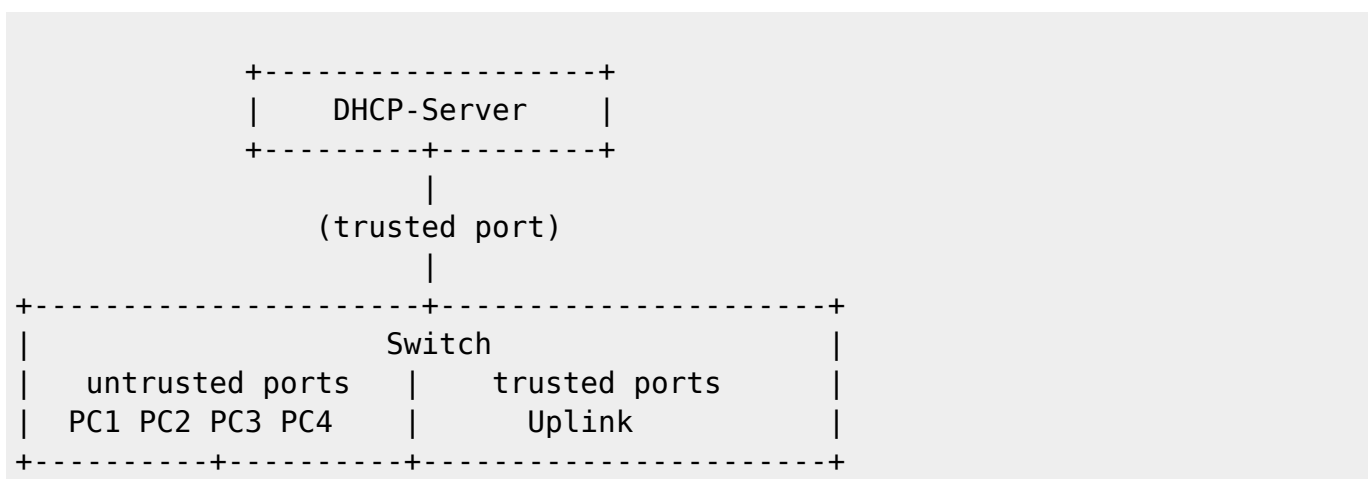
- passt IP zu MAC?
 - passt Port zur MAC?

Wenn nicht → blockiert.

Typische Fehlerquellen

- Uplink versehentlich untrusted → DHCP fällt komplett aus
 - nicht alle relevanten VLANs aktiviert
 - * Binding Table nicht persistent gespeichert
 - * Rate-Limits zu niedrig eingestellt

ASCII-Diagramm - DHCP Snooping Übersicht



Sicherheitsgewinn auf einen Blick

- verhindert DNS-Umlenkungen durch Rogue DHCP
 - verhindert Man-in-the-Middle

- * beschränkt DHCP-Verkehr auf vertrauenswürdige Ports
- * Grundlage für weitere Switch-Sicherheitsfunktionen

Zusammenfassung

- DHCP Snooping schützt vor falschen DHCP-Servern
 - unterscheidet trusted vs untrusted Ports
 - * speichert gültige MAC-IP-Port-Zuordnungen in Binding Tables
 - * essenziell in Unternehmen und VLAN-Umgebungen
 - * Grundlage für IP Source Guard & Dynamic ARP Inspection

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:dhcp-snooping&rev=1764588256>

Last update: **01.12.2025 12:24**

