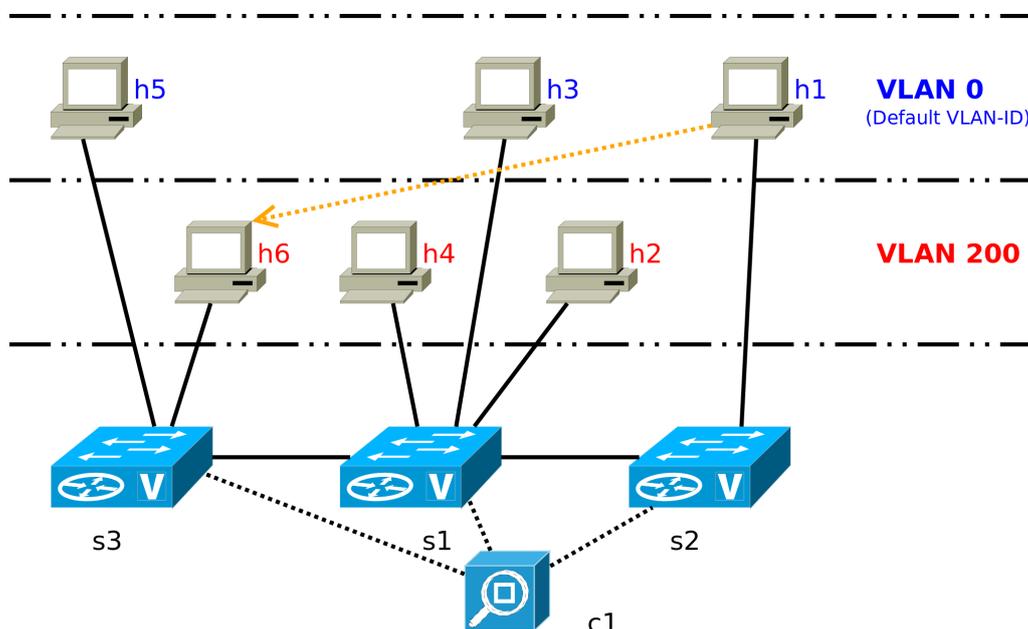


## Spezifikation und Messbeispiel aus dem Netzwerk-Labor

**VLAN** ist ein logisches Teilnetz innerhalb eines Switches bzw. eines gesamten physischen Netzwerks. Es kann sich über mehrere Switches hinweg ausdehnen. Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches Frames nicht in ein anderes VLAN weiterleitet, obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können.

Der **VLAN-Hopping**-Angriff ist eine Kombination aus **Switch-Spoofing** und **Double-Tagging**. Ziel ist es, Zugriff von einem VLANx in ein anderes VLANY aufzubauen. Folgendes Szenario ist gegeben:

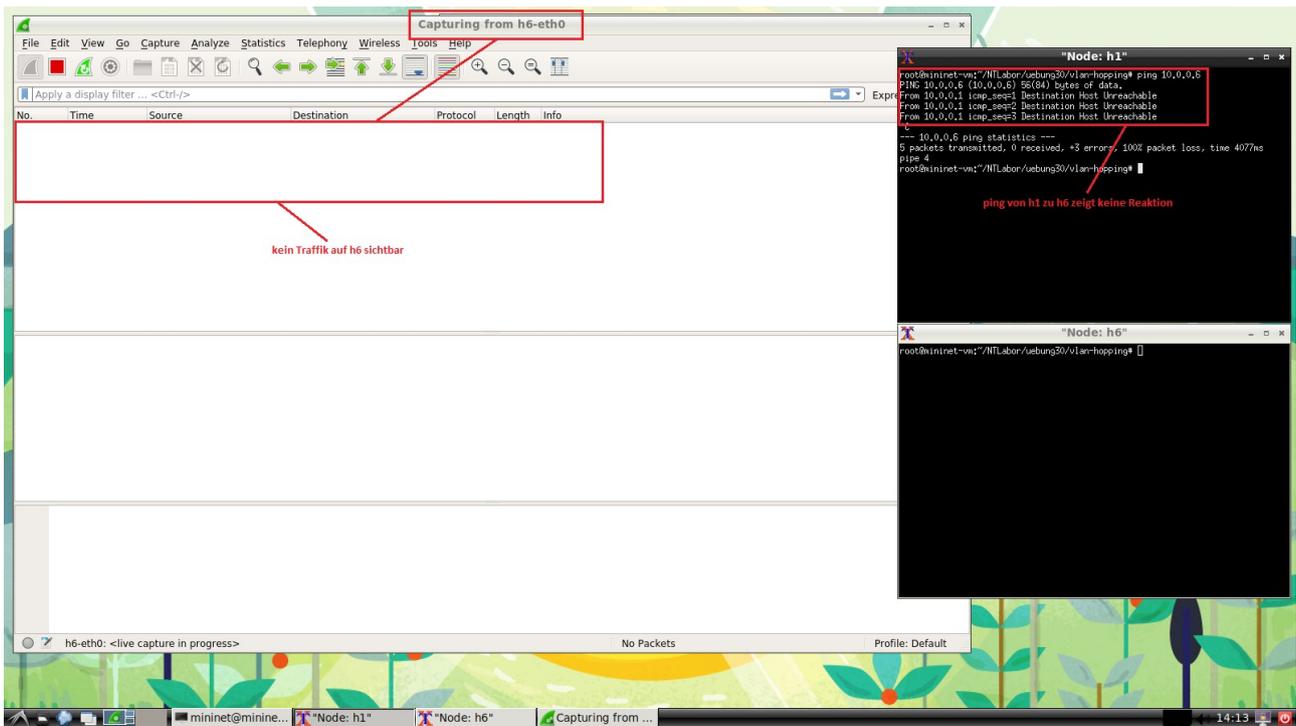


Host **h1** kann Aufgrund unterschiedlicher VLANs nicht mit Host **h6** in Verbindung treten. Mittels des **VLAN-Hopping-Angriffs** ist das aber möglich (gelber Pfeil).

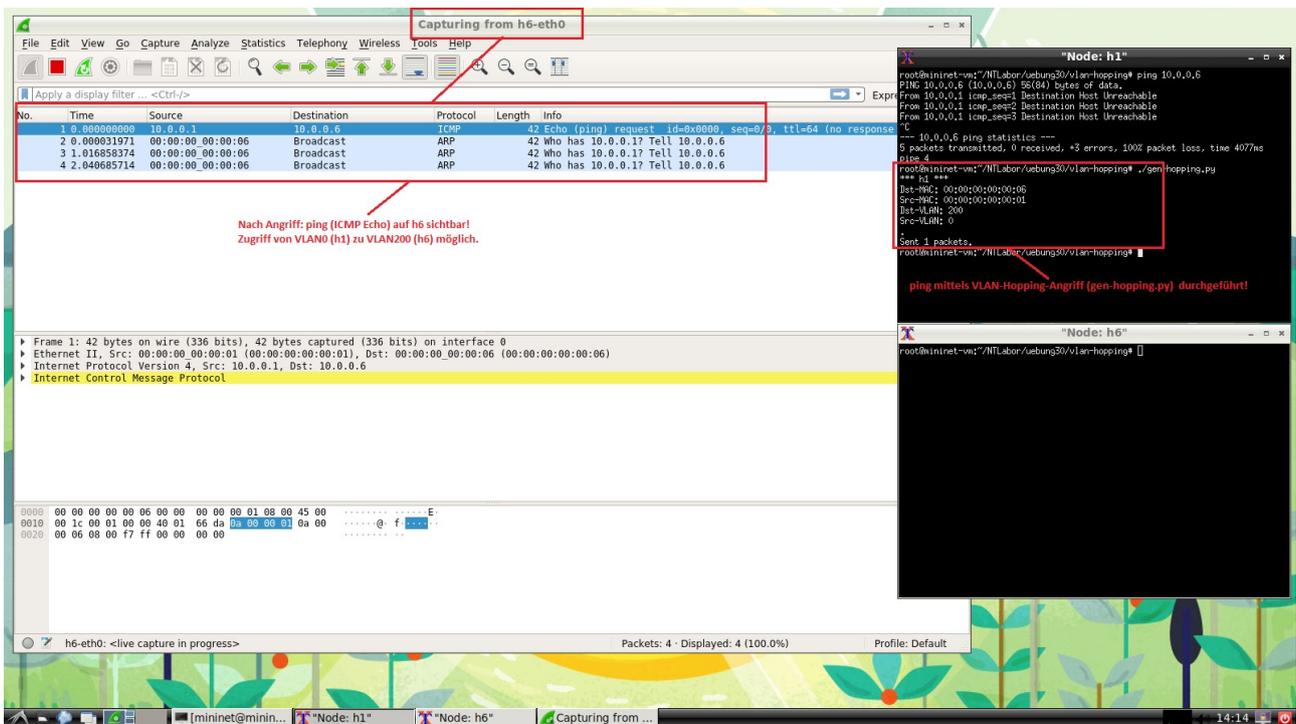
Zunächst der Zustand ohne Angriff:

- Wireshark wird auf Host **h6** gestartet.
- Ping wird von Host **h1** nach Host **h6** gestartet

# NWT-Labor



**Ergebnis:** Ping zeigt keinerlei Reaktion und in Wireshark ist auch keine Reaktion zu sehen. Nun folgt der VLAN-Hopping-Angriff:



**Ergebnis:** Host h1 in VLAN0 hat Zugriff auf Host h6 in VLAN 200.

→ Angriff erfolgreich!