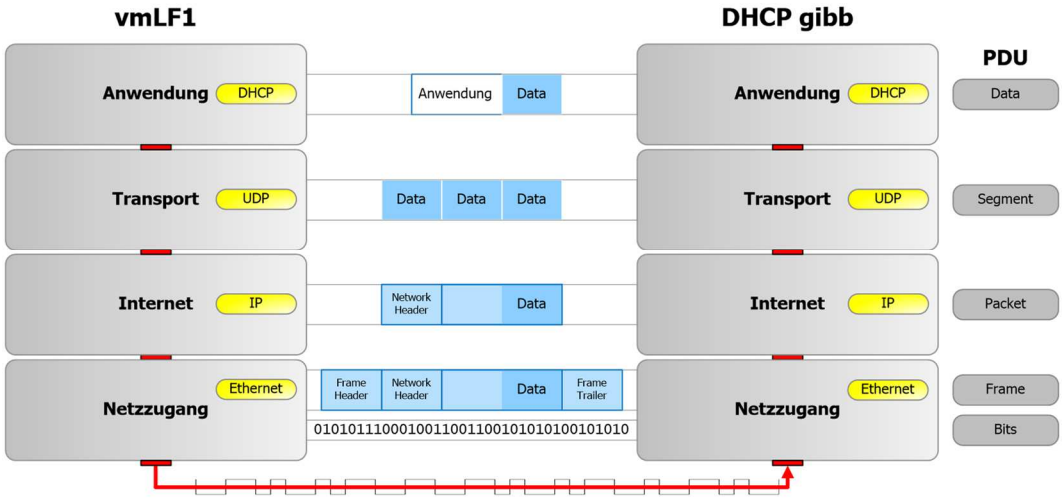
DHCP-Bezug

Ablauf

Szenario
Auf der Firewall *vmLF1* wird eine DHCP-Adresse für die Schnittstelle *red0* gelöscht und neu angefragt.

Erfassen und Auswerten
Auf der *vmLF1* wird der Datenverkehr auf *red0* mit `tcpdump` erfasst und gespeichert. Die Daten werden anschliessend auf den *vmWP1* kopiert und mit *WireShark* angezeigt .

TCP/IP-Modell



Schritt	Maschine	Aktion
1	*vmLF1* Konsole 2	`root@vmLF1:~# dhcpcd -k red0`
2	*vmLF1* Konsole 2	`root@vmLF1:~# ifconfig red0 up`
3	*vmLF1* Konsole 1	`root@vmLF1:~# tcpdump -i red0 -s 65535 -w /tmp/lf1-dhcp-iet-r.pcap`
4	*vmLF1* Konsole 2	`root@vmLF1:~# dhcpcd -n red0`
3	*vmLF1* Konsole 1	Aufzeichnung mit **`Ctrl+C`** abbrechen, mit folgendem Befehl die **Firewall zurücksetzen**: `root@vmLF1:~# /etc/init.d/network restart`
5	*vmWP1*	Aufzeichnung von *vmLF1* mit *pscp.exe* ins Verzeichnis **`C:\capdat`** kopieren.
6	*vmWP1*	`lf1-dhcp-iet-r.pcap` je mit *WireShark* öffnen.

Fragen

Welches Protokoll wird von DHCP auf der Transportschicht verwendet?	- UDP
Welchen Zielport benutzt *vmLF1* für die DHCP-Abfrage?	- 67
Welchen Quellport benutzt *vmLF1* für die DHCP-Abfrage?	- 68
Erstellen Sie einen Filter mit Ziel- und Quellport aus der DHCP-Anfrage?	- `udp.port == 68 and udp.port == 67`
Wie könnte die DHCP-Anfrage auch noch gefiltert werden? Schauen Sie die Framedetails eines DHCP-Paketes?	- `bootp`

Verbinden Sie die Schichten aus den Paketdetails mit den entsprechenden TCP/IP-Schichten.