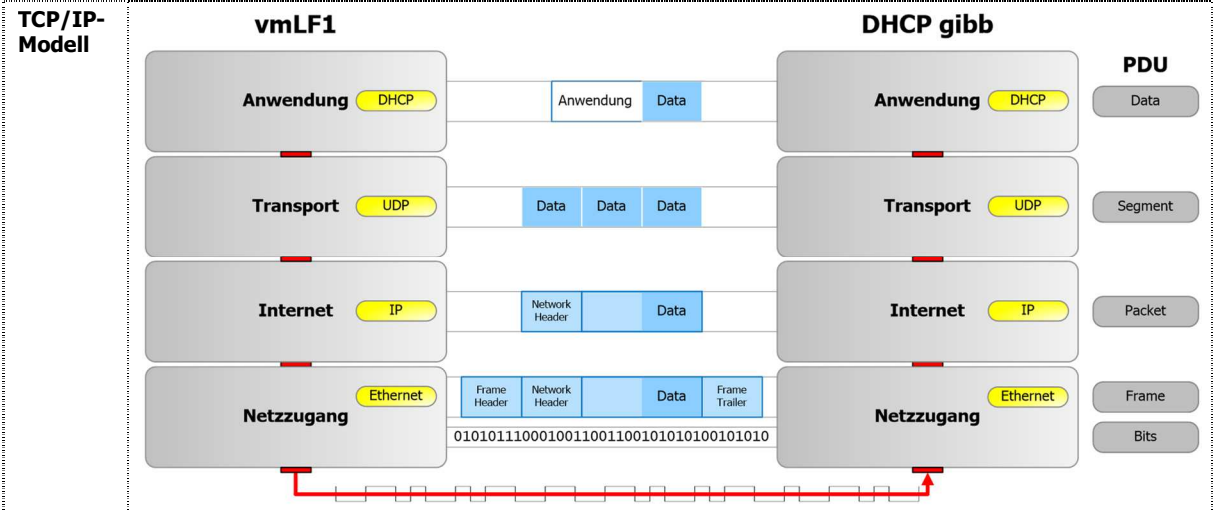


DHCP-Bezug

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 *vmWPI* kopiert und mit *WireShark* angezeigt.



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

Fragen

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

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

No.	Time	Delta Time	Source	Destination	Protocol	Length	Info
6	11.378498	8.924701	0.0.0.0	255.255.255.255	DHCP	367	DHCP D
8	12.384267	1.004630	192.168.100.1	192.168.100.158	DHCP	342	DHCP O
9	12.385042	0.000775	0.0.0.0	255.255.255.255	DHCP	379	DHCP R
10	12.561971	0.176929	192.168.100.1	192.168.100.158	DHCP	342	DHCP A

Frame 6: 367 bytes on wire (2936 bits), 367 bytes captured (2936 bits)
 Ethernet II, Src: Vmware_06:2a:81 (00:50:56:06:2a:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
 User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
 Bootstrap Protocol (Discover)