Linux am Dienstag

„Wat to Höllen is UDP“

(Ein KI unterstützter Einstieg ins Netzwerk)

„Wat to Höllen is UDP“

„Zuerst war da der Draht“

„Wat to Höllen is UDP“

Quelle: you.com / SD 2.1

„Wat to Höllen is UDP“

Über den Draht müssen strukturiert

Signale gesendet und empfangen werden.

„Wat to Höllen is UDP“

physikalische Schicht

auch bekannt als OSI Layer 1

„Wat to Höllen is UDP“

Dazu braucht man den Ethernetframe

„Wat to Höllen is UDP“

Data Link Layer

auch bekannt als OSI Layer 2

„Wat to Höllen is UDP“

Aufbau eines Ethernetframe

Feld	Länge (Bytes)	Beschreibung
Start of Frame	8	Synchronisierungsbitfolge
Destination MAC	6	MAC-Adresse des Zielrechners
Source MAC	6	MAC-Adresse des Senderrechners
Length/Type	2	Länge des Datenpakets oder Protokolltyp
Data	46-1500	Nutzdaten
FCS (CRC)	4	Frame-Check-Sequenz zur Prüfung der Datenintegrität

„Wat to Höllen is UDP“

Network Layer

auch bekannt als OSI Layer 3

„Wat to Höllen is UDP“

Der IP-Header

Komponente	Feldlänge(Bytes)	Funktion
Version	½	die Version des IP-Protokolls
TOS (Type of Service)	1	die Priorität des Datenpaketes
TTL (Time to Live)	1	die maximale Lebensdauer des Datenpakets
Protokoll	1	Protokoll ID
Headerchecksumme	2	Integrität des Headers
Quelle-IP-Adresse	4	IP-Adresse des Paket-Senders
Ziel-IP-Adresse	4	IP-Adresse des Paket-Empfängers
Optionen	X	Zusatzinfos
Daten	XXXX	Inhalt des Datenpaketes

„Wat to Höllen is UDP“

Daten … was sind Daten?...

„Wat to Höllen is UDP“

„Daten, die in einem Ethernet-Frame transportiert werden, sind Nutzdaten, die ein Netzwerkgerät an ein anderes Netzwerkgerät sendet. Diese Daten können Informationen, Anweisungen oder andere Daten enthalten, die zur Übermittlung von Informationen und Daten zwischen Netzwerkgeräten erforderlich sind. Im Ethernet-Frame selbst befinden sich die Header-Informationen, die die Adressen des Senders und des Empfängers enthalten, sowie die Nutzdaten, die das eigentliche zu übertragende Datenpaket enthalten.“

Quelle: you.com - ChatGPT

„Wat to Höllen is UDP“

Transport Layer

auch bekannt als OSI Layer 4

„Wat to Höllen is UDP“

Im Transport Layer kommen endlich

UDP und TCP

zum Einsatz

„Wat to Höllen is UDP“

User Datagram Protocol (UDP)

„Wat to Höllen is UDP“

UDP Header

Feld	Länge(Bytes)	Funktion
Quell-Port	2	0-65535
Ziel-Port	2	0-65535
Länge	2	maximal 64k Bytes
Prüfsumme	2	Prüfung, ob das Paket intakt ist.
Daten	XXXXX	

„Wat to Höllen is UDP“

Die Besonderheit an UDP ist,

dass es zustandlos ist.

„Wat to Höllen is UDP“

Das bedeutet, die Anwendung die das Paket sendet muß selbst feststellen, ob das Paket an kam und ggf. den Absender informieren.

„Wat to Höllen is UDP“

Bei TCP kümmert sich dagegen der Netzwerkstack im Betriebssytem selbst darum.

„Wat to Höllen is UDP“

Da sich die Anwendung selbst kümmern muß, also für den Fall des Fehlens eines UDP Paketes vorbereitet sein muß, werden UDP Pakete bei Netzwerkengpäßen im Router als erstes gedroppt.

„Wat to Höllen is UDP“

UDP Pakete werden meistens bei schlanken Daten verwendet, da der „Overhead“ nicht so groß ist.

Das bezeichnet alles, was man für Ports & Ips und Checksummen braucht.

„Wat to Höllen is UDP“

TCP Pakete werden dagegen für große Datenmengen benutzt. Hier wird der Overhead bewußt in Kauf genommen, weil das die Komplexität in der Anwendung reduziert.

„Wat to Höllen is UDP“

Bekanntestes Beispiel

DNS

„Wat to Höllen is UDP“

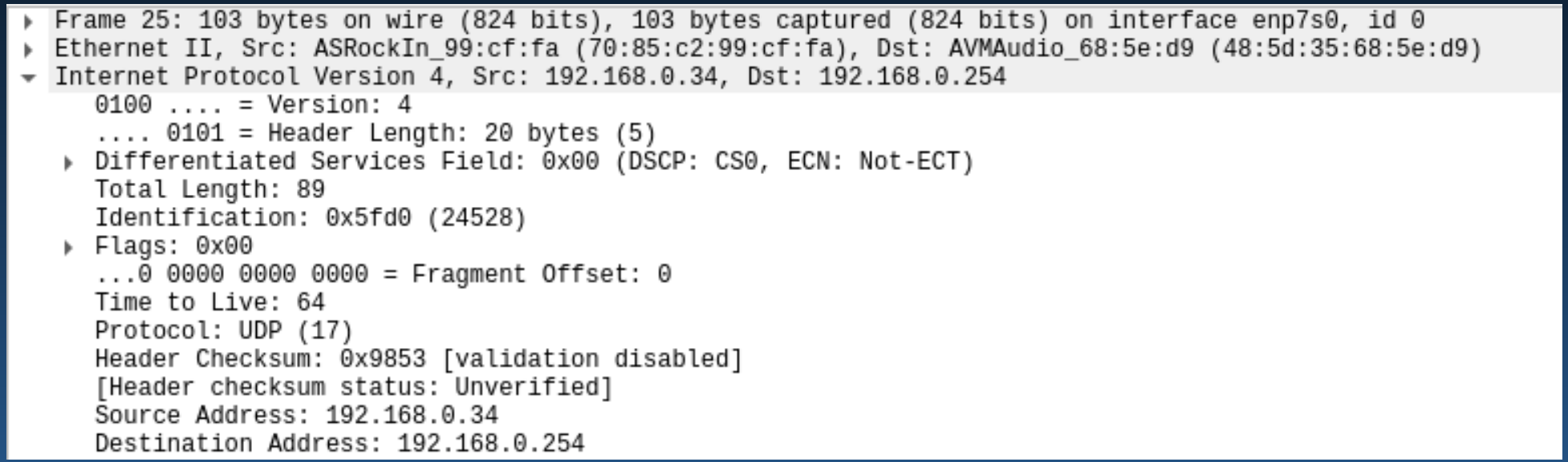
Frage: Wie lautet die IP für linux-am-dienstag?

```
0000  48 5d 35 68 5e d9 70 85  c2 99 cf fa 08 00 45 00   H]5h^·p· ·····E·
0010  00 59 5f d0 00 00 40 11  98 53 c0 a8 00 22 c0 a8   ·Y_···@· ·S···"··
0020  00 fe 8d a7 00 35 00 45  82 c7 fd 47 01 20 00 01   ·····5·E ···G· ··
0030  00 00 00 00 00 01 11 6c  69 6e 75 78 2d 61 6d 2d   ·······l inux-am-
0040  64 69 65 6e 73 74 61 67  02 64 65 00 00 01 00 01   dienstag ·de·····
0050  00 00 29 10 00 00 00 00  00 00 0c 00 0a 00 08 72   ··)····· ·······r
0060  df 6a 0f b0 66 66 44                              ·j··ffD
```

The response to this DNS query is in this frame (dns.response_in)

„Wat to Höllen is UDP“

Der IP-Header



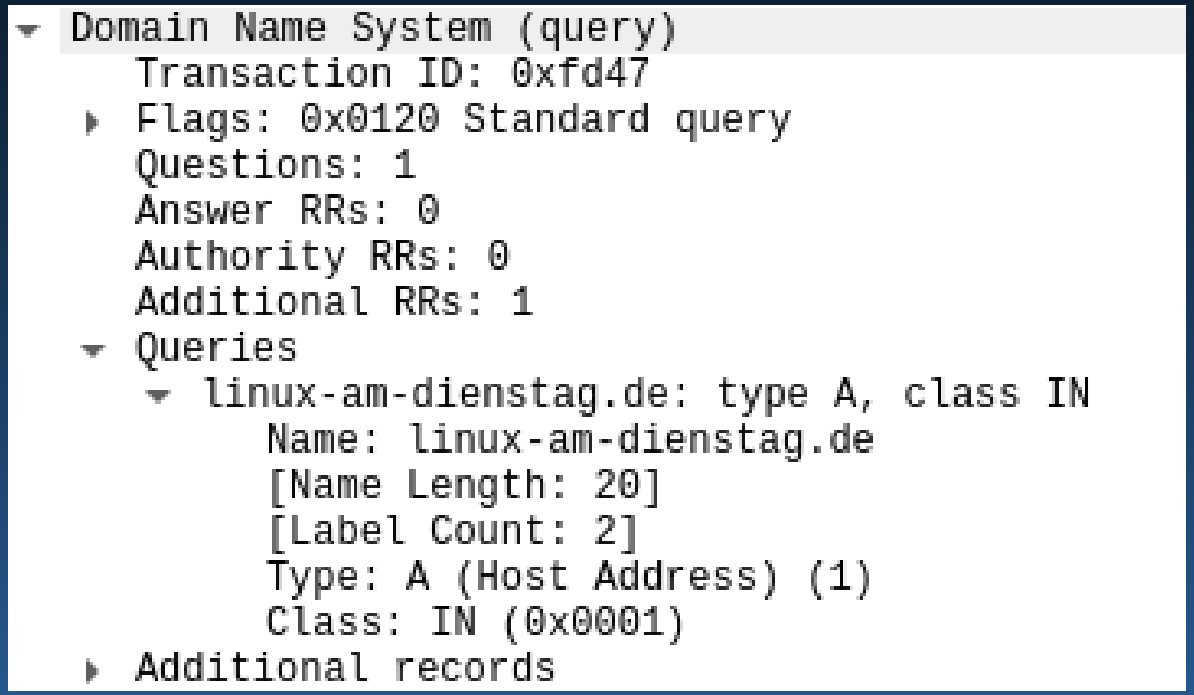
„Wat to Höllen is UDP“

Der UDP-Header

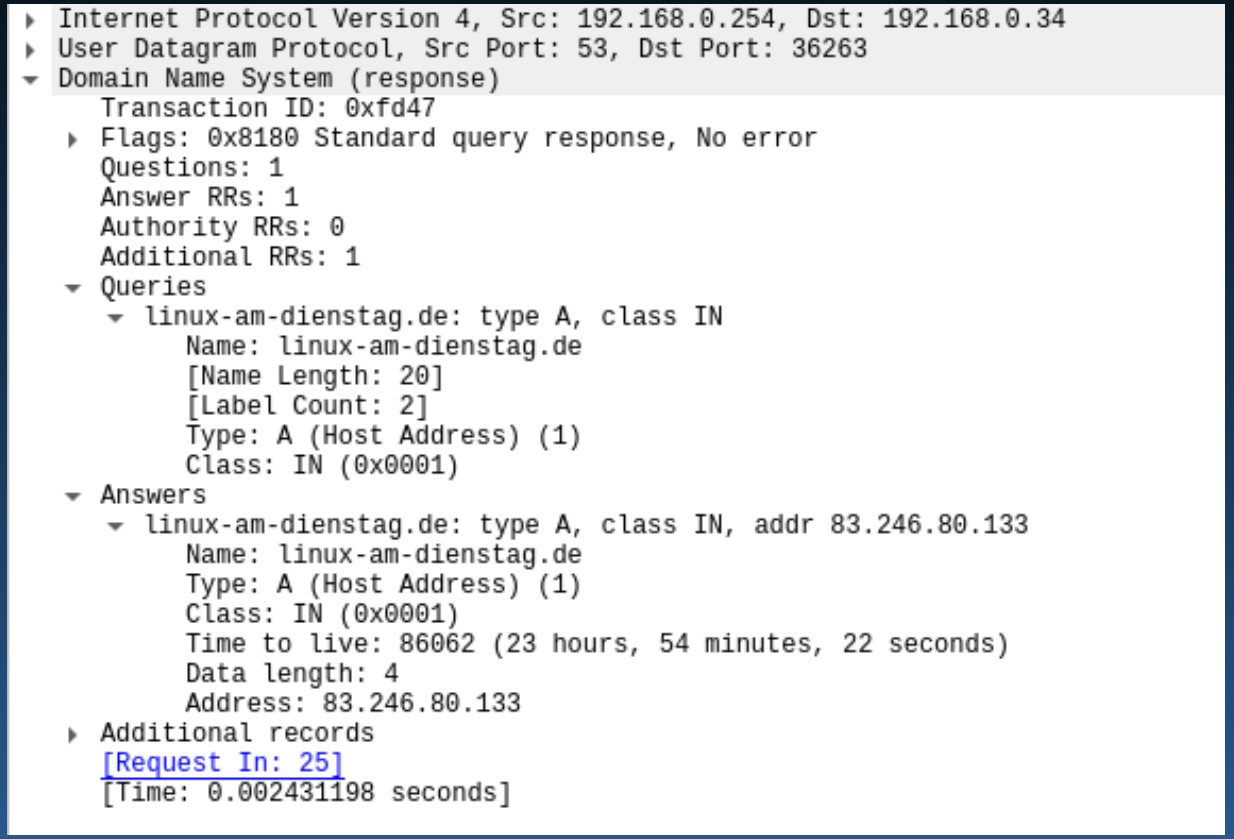
```
▾ User Datagram Protocol, Src Port: 36263, Dst Port: 53
    Source Port: 36263
    Destination Port: 53
    Length: 69
    Checksum: 0x82c7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  ▾ [Timestamps]
       [Time since first frame: 0.000000000 seconds]
       [Time since previous frame: 0.000000000 seconds]
    UDP payload (61 bytes)
```

„Wat to Höllen is UDP“

Das DNS-Datagram



„Wat to Höllen is UDP“



Die DNS-Antwort

IP+UDP Ziel und Quelle sind vertauscht.

Frage und Antwort werden geschickt, maximal 512 Bytes darf die Antwort insgesamt lang sein.

„Wat to Höllen is UDP“

Ist eine Antwort größer als 512 Byte, so signalisiert der DNS Server das dem Clienten, so dass dieser ggf. per TCP Daten nachfragt.

„Wat to Höllen is UDP“

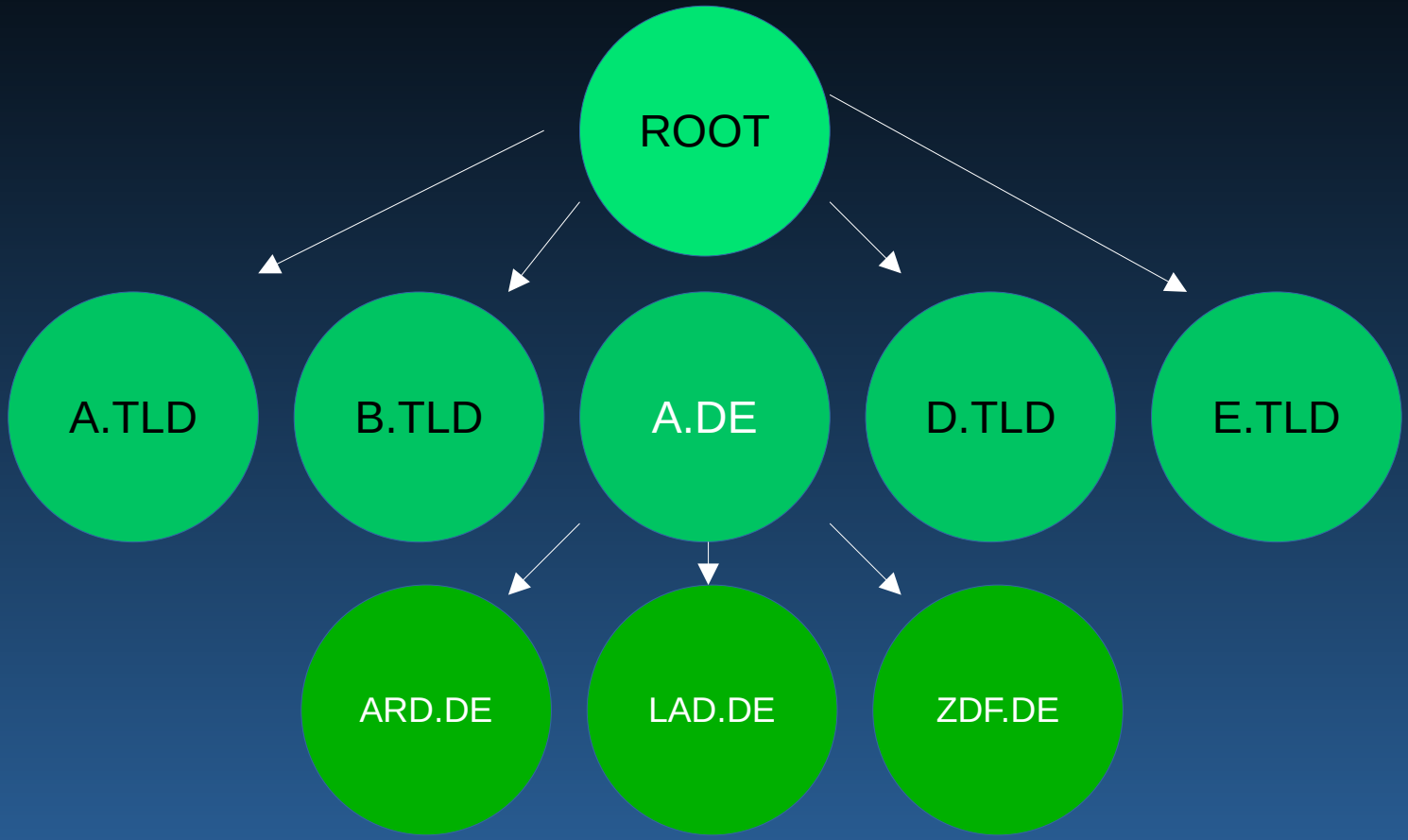
Ok, das war’s, hier gibt’s nic….

Woher weiß mein Router eigentlich die Antwort??

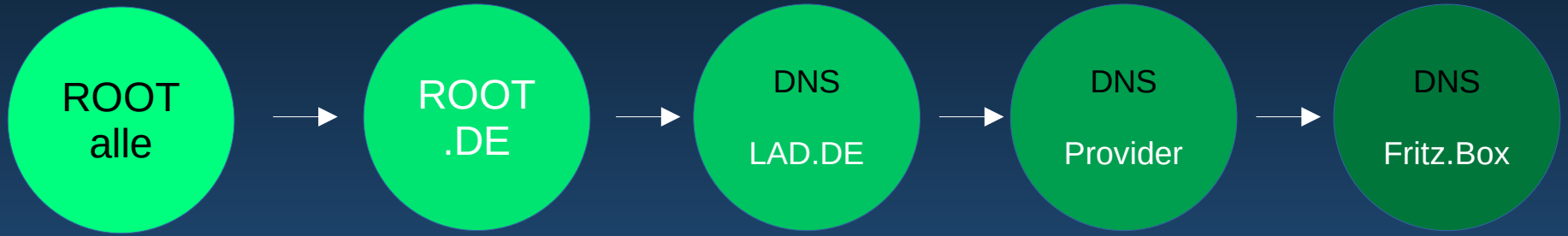
„Wat to Höllen is UDP“

DNS – Ein Baum voller Server

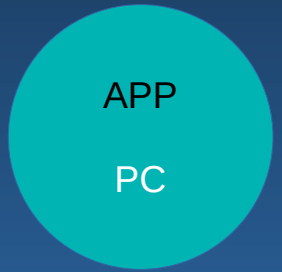
„Wat to Höllen is UDP“



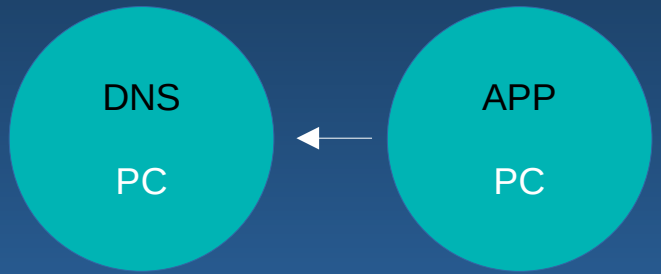
„Wat to Höllen is UDP“



„Wat to Höllen is UDP“

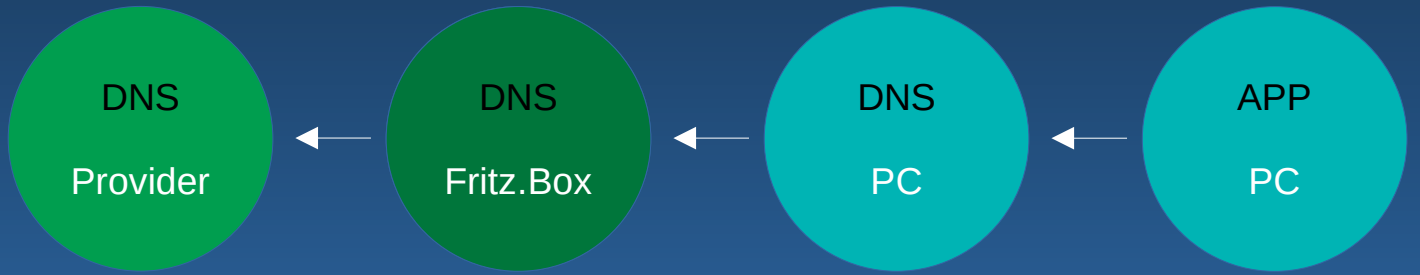


„Wat to Höllen is UDP“

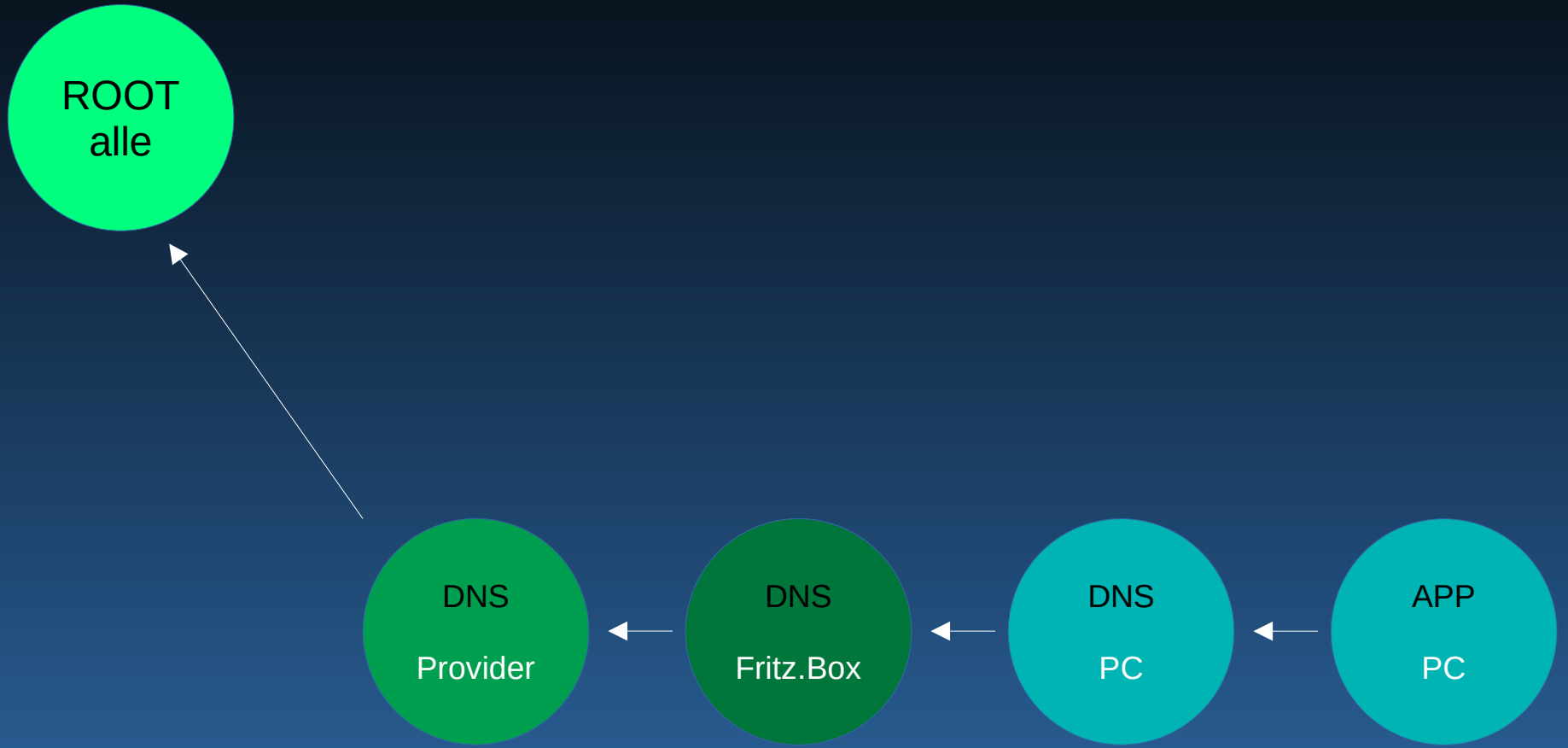


„Wat to Höllen is UDP“

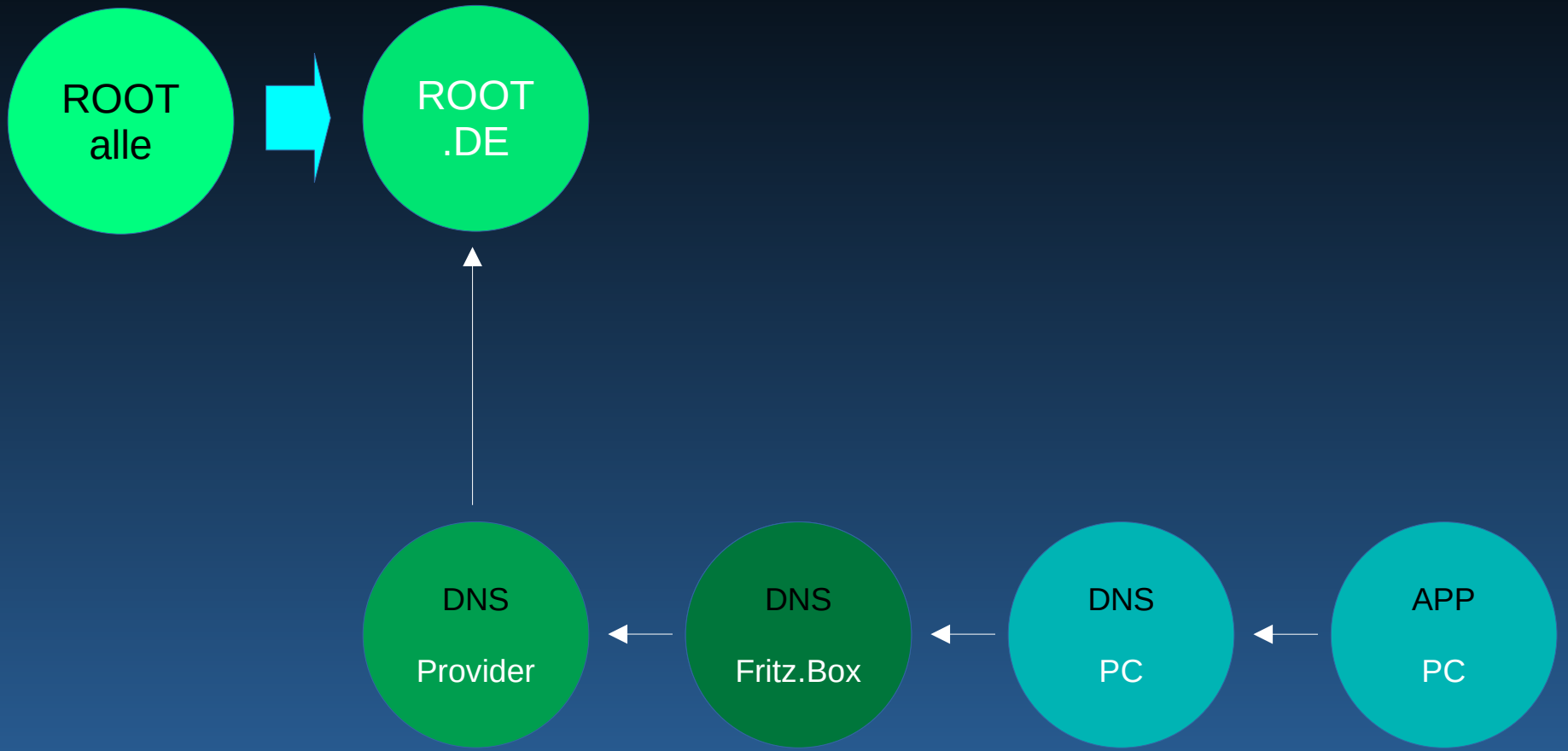
„Wat to Höllen is UDP“



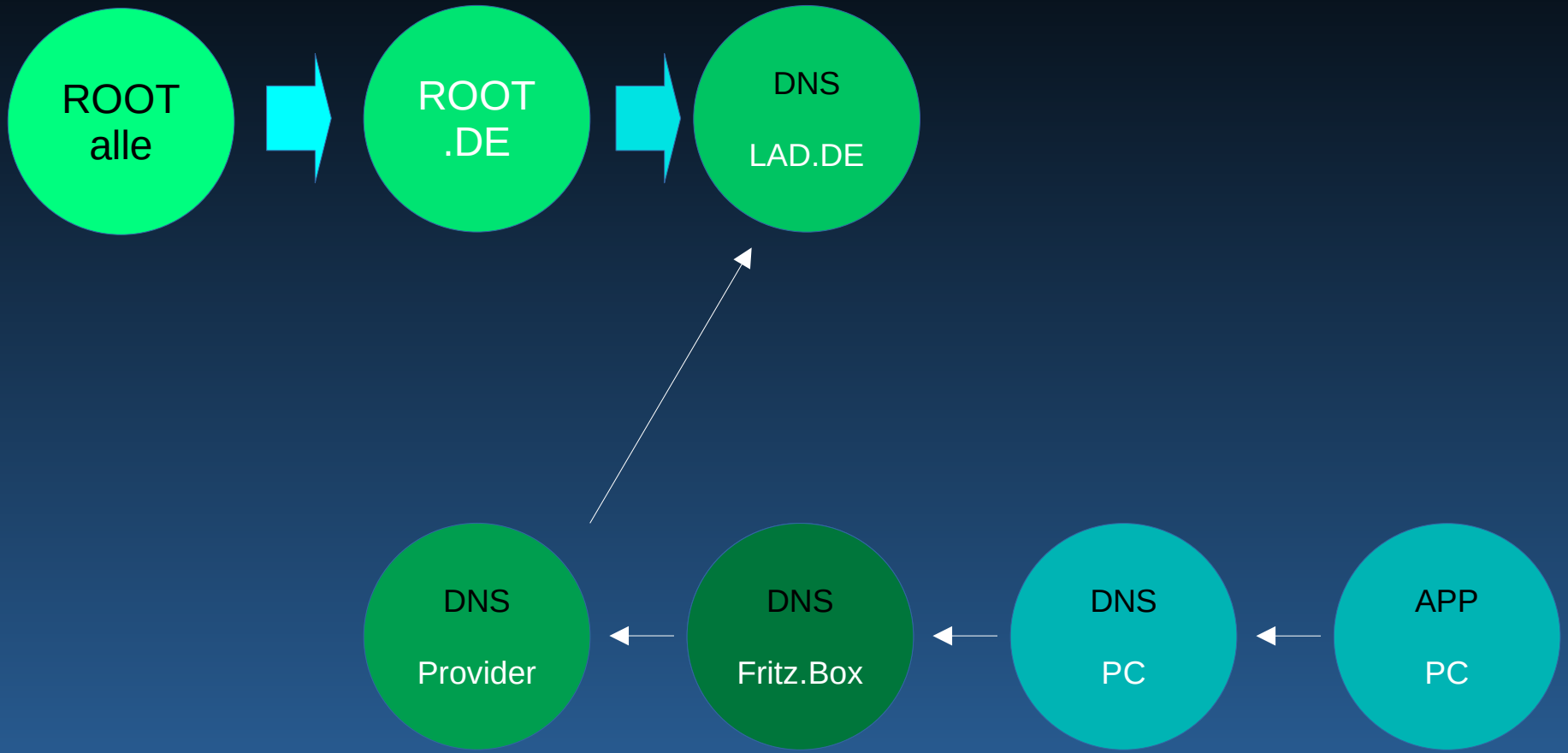
„Wat to Höllen is UDP“



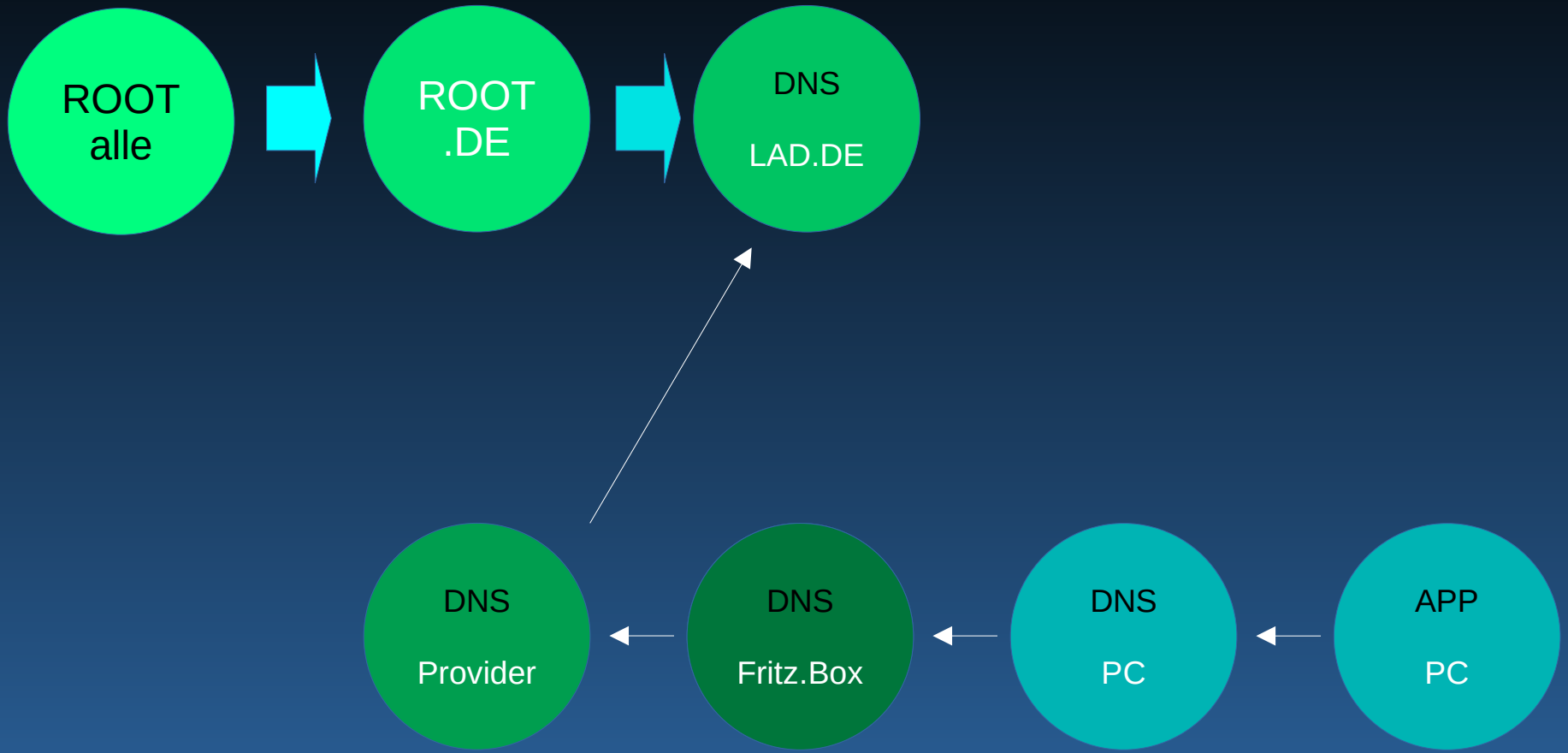
„Wat to Höllen is UDP“



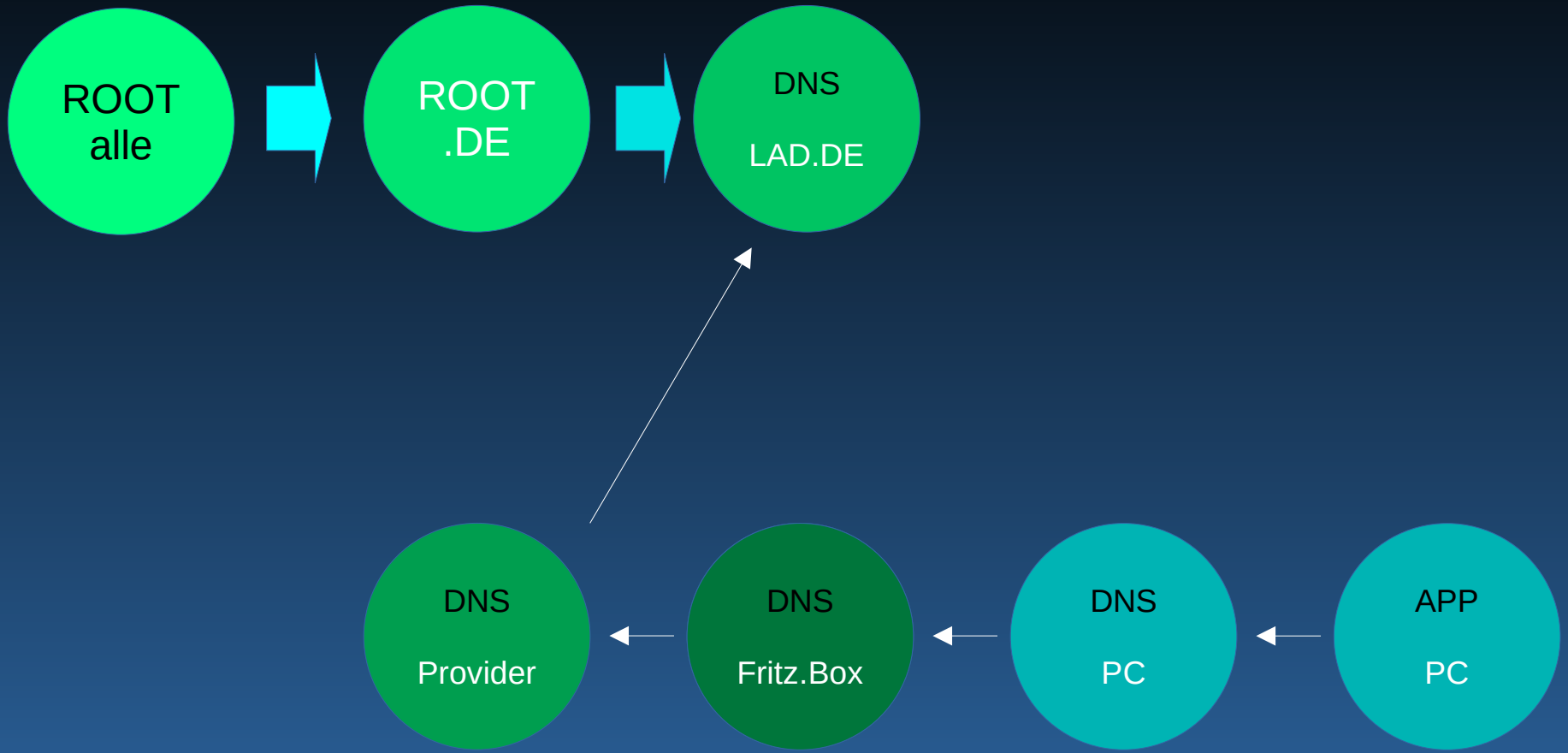
„Wat to Höllen is UDP“



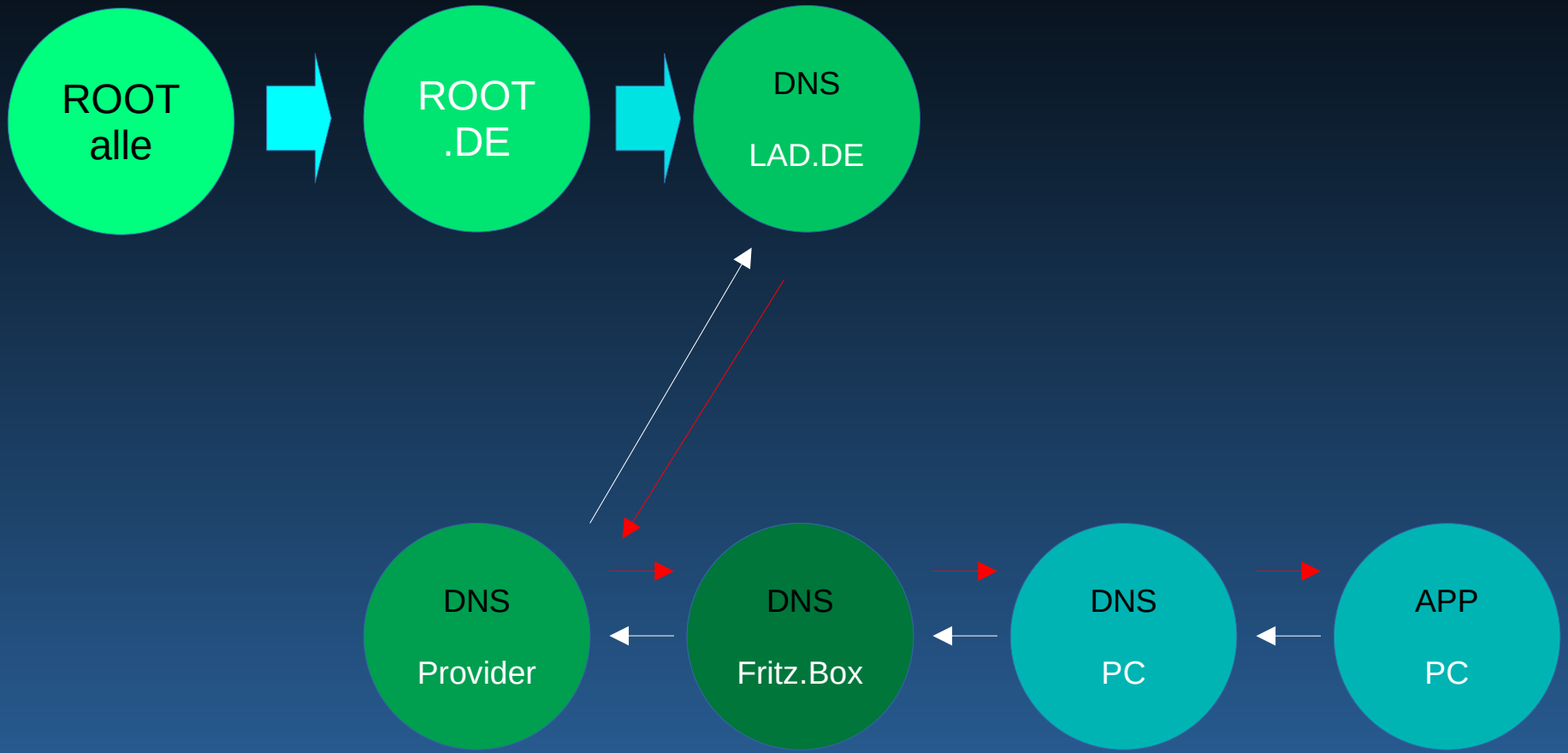
„Wat to Höllen is UDP“



„Wat to Höllen is UDP“



„Wat to Höllen is UDP“



„Wat to Höllen is UDP“

Was kann man alles im DNS finden?

„Wat to Höllen is UDP“

- Mailserver
- IP der (Sub)domain
- TEXT Infos
- SPF
- DKIM Signaturen
- Nameserver (Delegationen)
- CNAMEs
- SIP Server

und tausend andere Sachen...

„Wat to Höllen is UDP“

Fragen wir doch mal selbst … mit DIG :D

„Wat to Höllen is UDP“

```
$ dig any linux-am-dienstag.de

; <<>> DiG 9.16.37-RH <<>> any linux-am-dienstag.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18517
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;linux-am-dienstag.de.          IN    ANY

;; ANSWER SECTION:
linux-am-dienstag.de.    86400     IN    NS    ns2.resellerdesktop.de.
linux-am-dienstag.de.    86400     IN    NS    ns1.resellerdesktop.de.
linux-am-dienstag.de.    86400     IN    A     83.246.80.133
linux-am-dienstag.de.    86400     IN    MX    10 linux-am-dienstag.de.
linux-am-dienstag.de.    86400     IN    SOA   ns1.resellerdesktop.de. hostmaster\@linux-am-
dienstag.de. 0 86400 3600 604800 3600

;; Query time: 90 msec
;; SERVER: 192.168.0.254#53(192.168.0.254)
;; WHEN: Mon Mar 06 23:10:05 CET 2023
;; MSG SIZE  rcvd: 198
```

„Wat to Höllen is UDP“

Fragen?

„Wat to Höllen is UDP“

Danke.