Wie funktioniert DoH?

Ein Vortrag

über

„Was DNS-over-HTTPS ist!“

Wie funktioniert DoH?

HTTPS ist das

HyperText Transport Protokoll Secured

Wie funktioniert HTTPS?

Für weitere Details verweise ich auf den Vortrag

„Wie funktioniert HTTPS?“

Was ist DNS?

DNS steht für

„DomainName Service“

Was ist DNS?

DNS löst Domainnamen in IP-Adressen

und vice versa auf.

Was ist DNS?

Beispiel:

bs-lug.de hat die IP 81.169.174.151

„Am Anfang war die IP ...“

Warum braucht man DNS?

„Am Anfang war die IP ...“

aber es gab noch keine Domainnamen.

Wo kommt die IP her?

Damit das DNS-System funktioniert,

muß es eine zentrale Stelle geben,

die festlegt, wer das überhaupt festlegen darf.

Wo kommt die IP her?

Die oberste Instanz, die festlegt, welche „Domain“ von welchem anderen Nameserver beantwortet werden darf, nennt man Rootnameserver.

„13 Freunde sollt Ihr sein!“

Die ICANN ROOT-Nameserver

„13 Freunde sollte Ihr sein!“

Die Internet Corporation for Assigned Names and Numbers (ICANN) koordiniert den Betrieb der Root-Nameserver.

„13 Freunde sollte Ihr sein!“

Die Internet Corporation for Assigned Names and Numbers (ICANN) koordiniert den Betrieb der Root-Nameserver.

HEUTE!

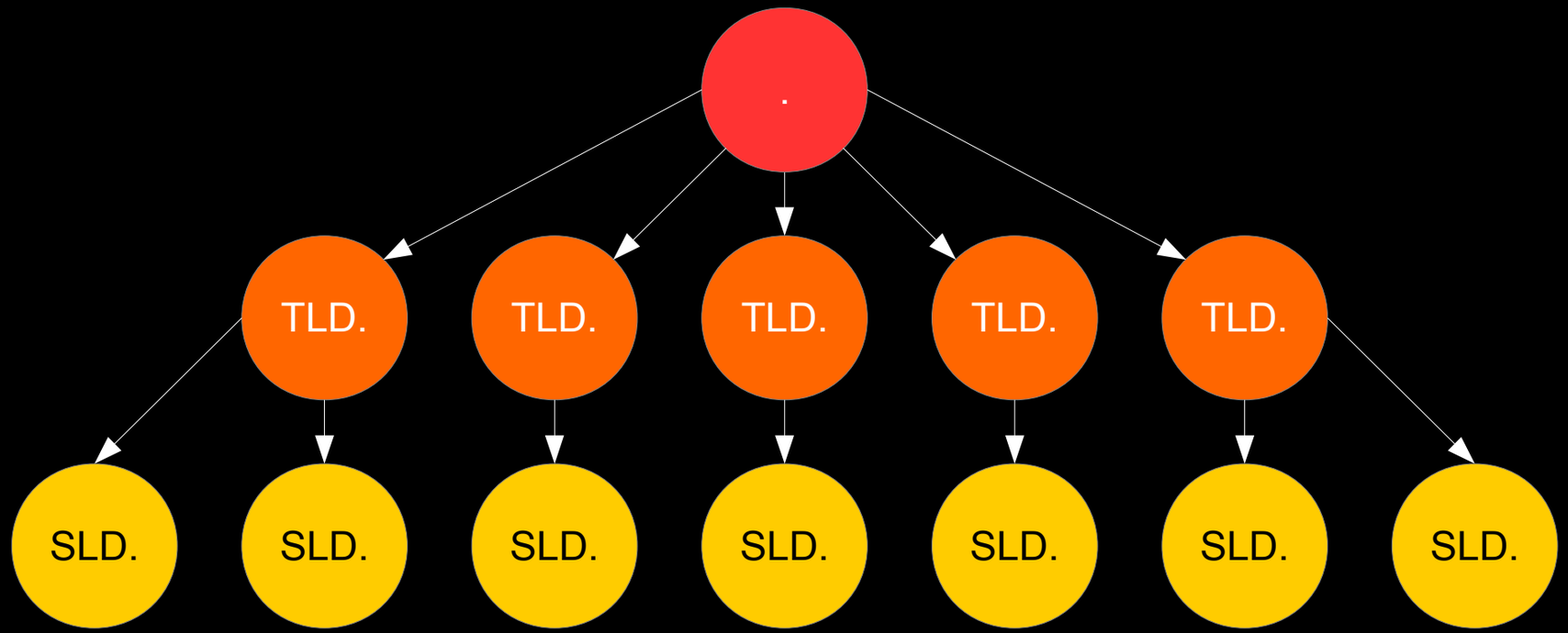
„Was ist überhaupt eine Domain?“

Um zu verstehen, wie das organisiert ist, muß man erst mal wissen, was eine Domain ist, und was ein Domainname.

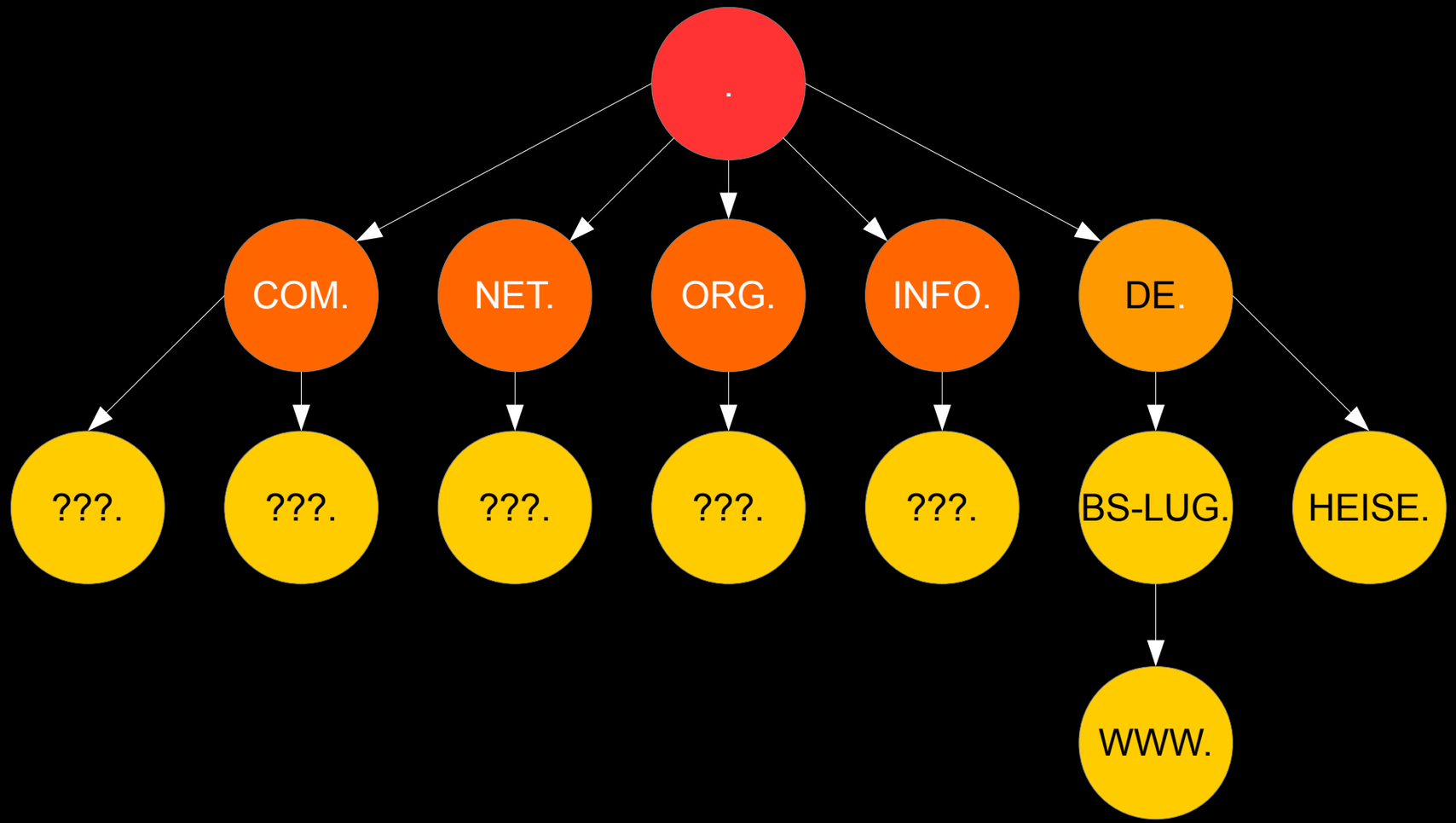
„Was ist überhaupt eine Domain?“

Eine Domain ist eine STUFE in der Hierarchie des DNS Baums.

„Die Hierachie“



„Die Hierachie“



„Was ist überhaupt eine Domain?“

Ein Domainname hat mindestens zwei Bestandteile:

second-level-domain.top-level-domain.

„Was ist überhaupt eine Domain?“

Es gehen beliebig lange Domainnamen:

….9ld.8ld.7ld.6ld.5ld.4ld.3ld.2ld.tld.

„Was ist überhaupt eine Domain?“

Jede Domain(Stufe) hat Ihre eigenen DomainNameServer.

„Was ist überhaupt eine Domain?“

Die DomainNameServer geben die Domain-Informationen aus.

„Was steht denn nun im DNS?“

```
$ dig a www.bs-lug.de

; <<>> DiG 9.11.10-RedHat-9.11.10-1.fc29 <<>> a www.bs-lug.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11094
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bs-lug.de.          IN   A

;; ANSWER SECTION:
www.bs-lug.de.       149  IN   CNAME    bs-lug.de.
bs-lug.de.           149  IN   A    81.169.174.151

;; Query time: 43 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mi Nov 06 16:46:08 CET 2020
;; MSG SIZE  rcvd: 72
```

„Was steht denn nun im DNS?“

```
$ dig ns www.bs-lug.de

; <<>> DiG 9.11.10-RedHat-9.11.10-1.fc29 <<>> ns www.bs-lug.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29993
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bs-lug.de.                 IN      NS

;; ANSWER SECTION:
www.bs-lug.de.          149     IN      CNAME   bs-lug.de.
bs-lug.de.              149     IN      NS      shades10.rzone.de.
bs-lug.de.              149     IN      NS      docks20.rzone.de.

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mi Nov 06 16:49:56 CET 2020
;; MSG SIZE  rcvd: 107
```

„Wer betreibt die ganzen DNS Server“

Die DN-Server werden von den Webhoster betrieben und stehen i.d.R. in Rechenzentren.

Die DN-Server der TLDs werden von den zuständigen NICs (NetworkInformationCenter) betrieben.

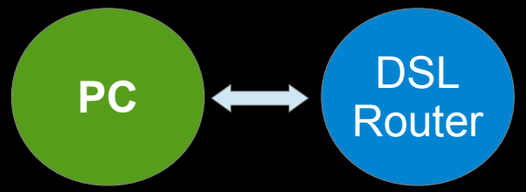
Hier leitet sich auch der Name DENIC für Deutschland her.

„Und wo stehen die nun?“

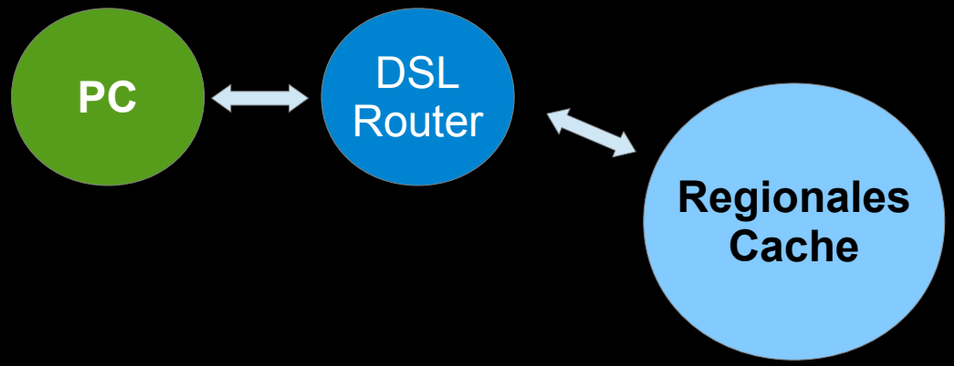
```
$ host  shades10.rzone.de.
shades10.rzone.de has address 85.214.0.240
shades10.rzone.de has IPv6 address 2a01:238:20b:43:6653::510

$ whois 85.214.0.240

inetnum:        85.214.0.0 - 85.214.3.255
netname:        STRATO-RZG-DED2
org:            ORG-SRA1-RIPE
descr:          Strato Rechenzentrum, Berlin
country:        DE
```

„Wer fragt wen?“

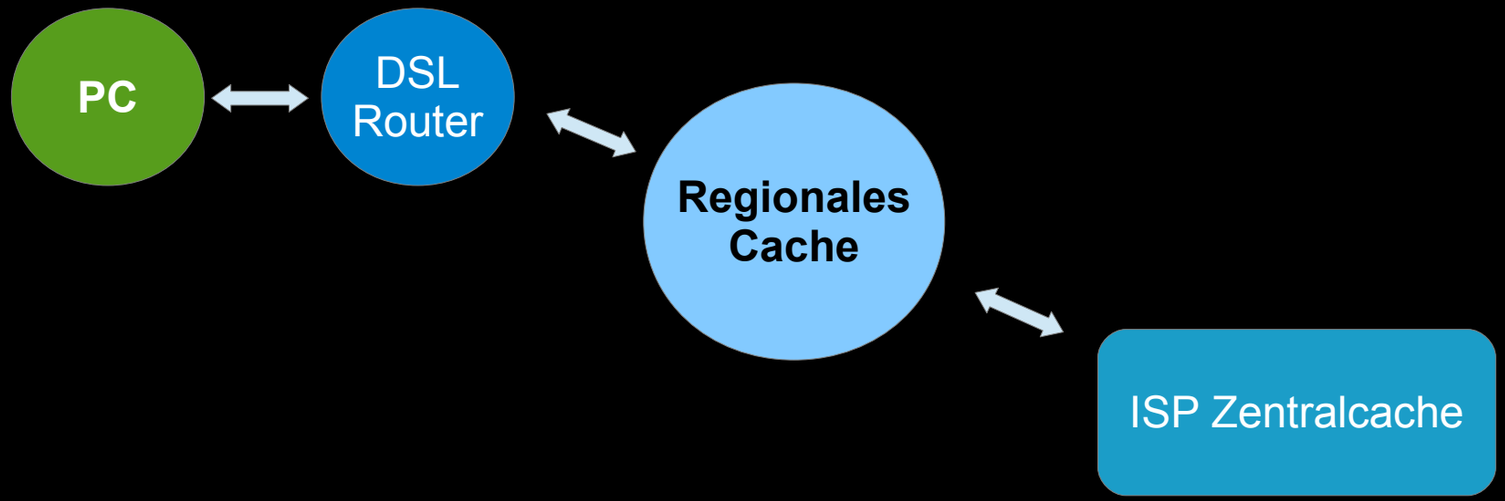
„Wer fragt wen?“



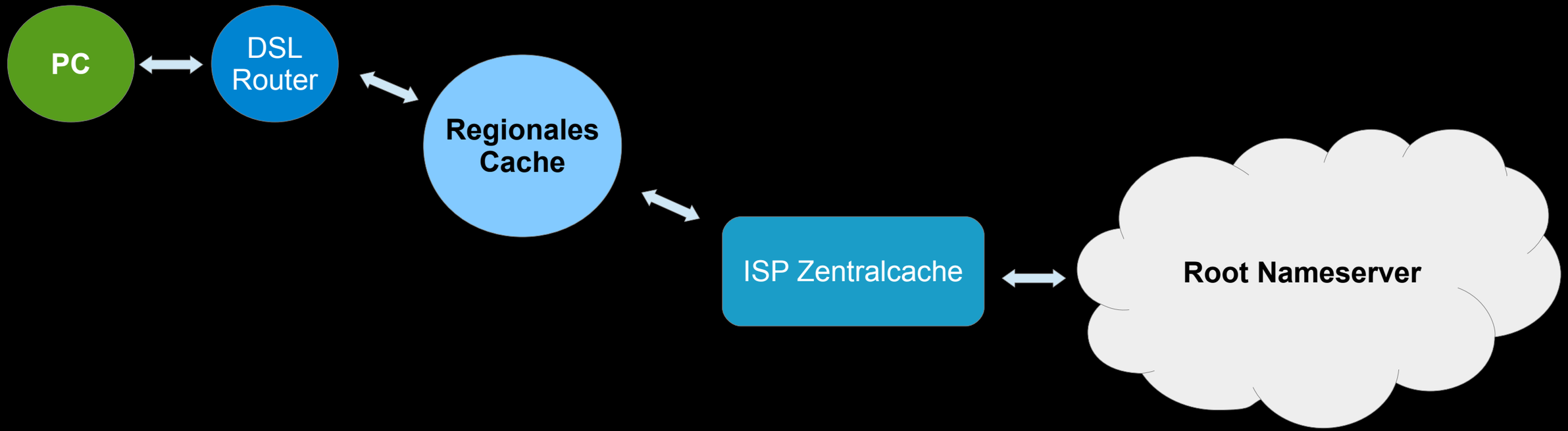
„Wer fragt wen?“



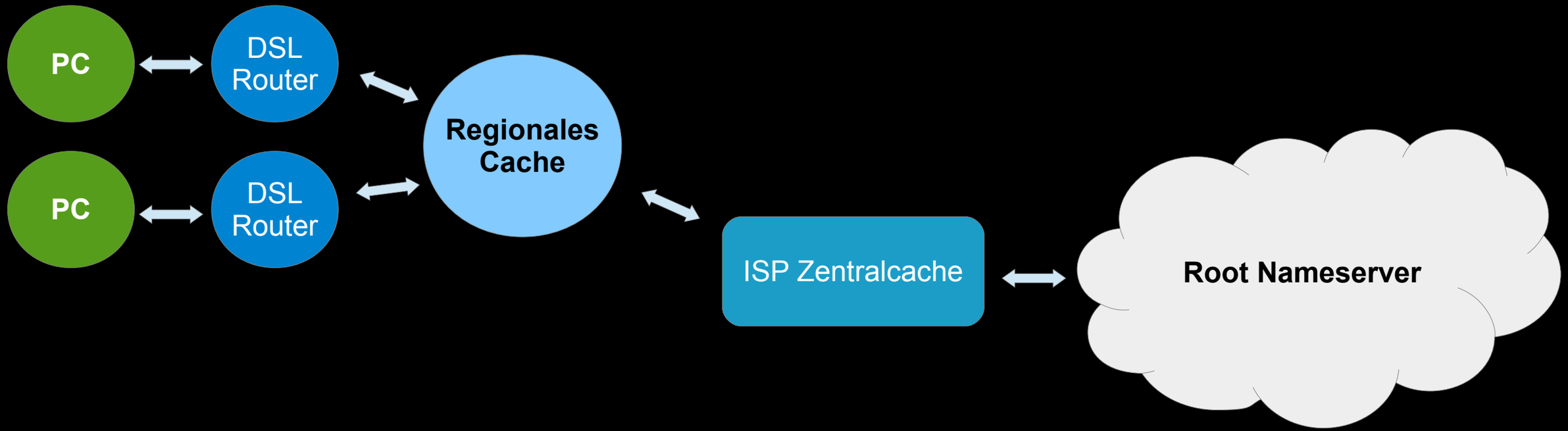
„Wer fragt wen?“



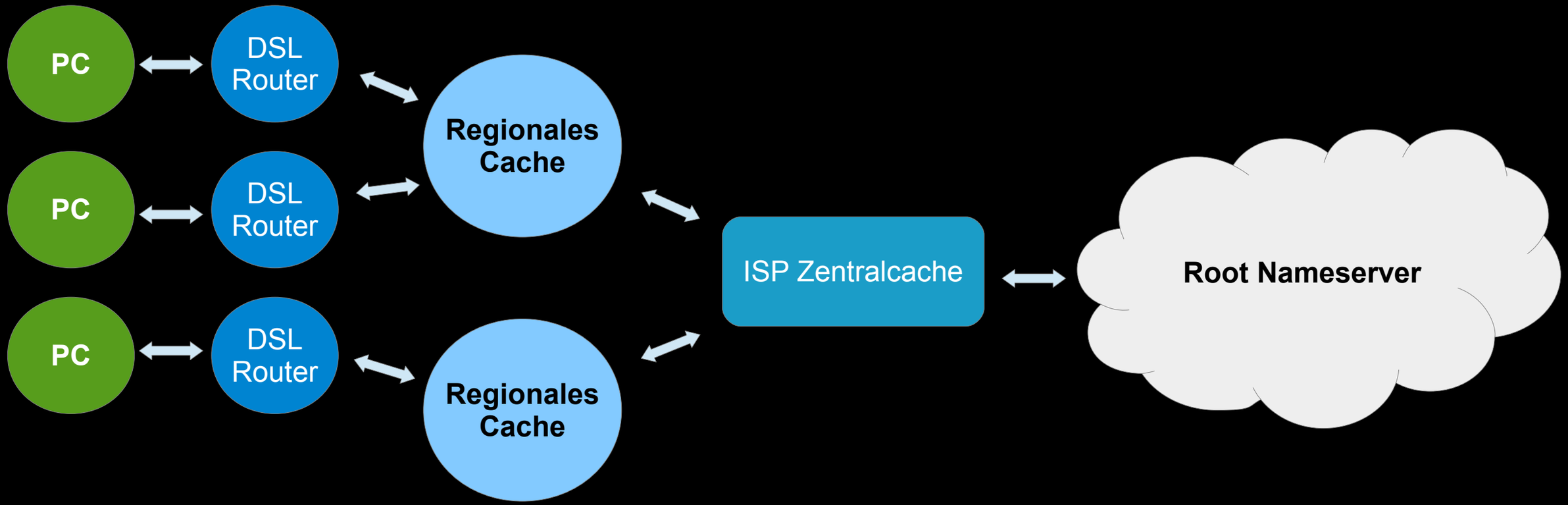
„Wer fragt wen?“



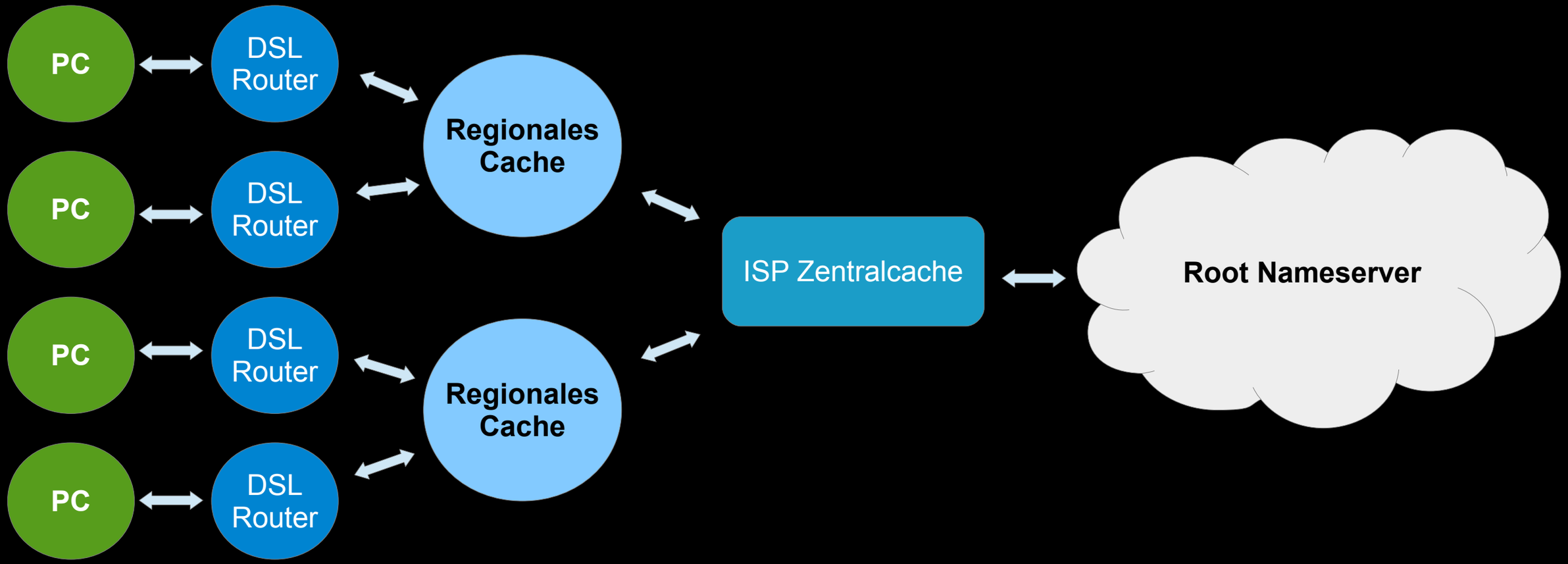
„Wer fragt wen?“



„Wer fragt wen?“

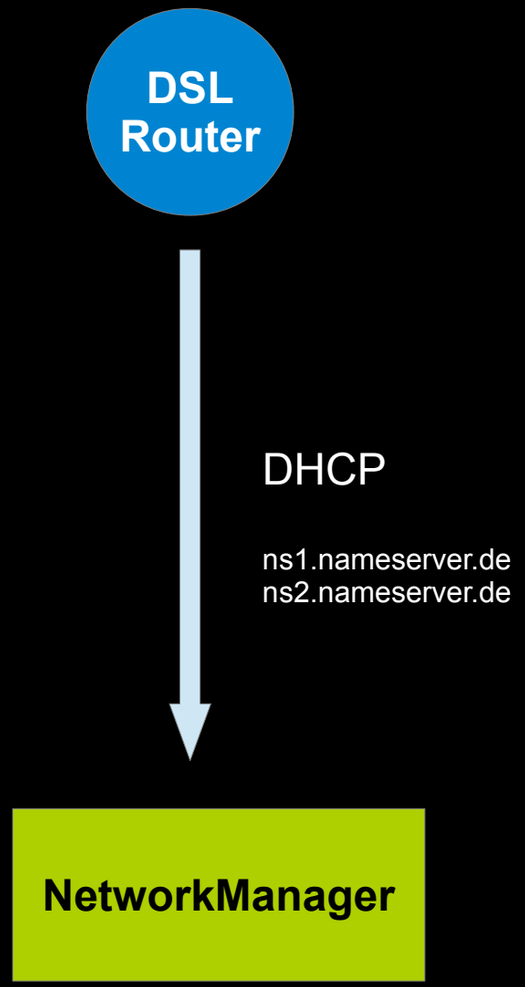


„Wer fragt wen?“

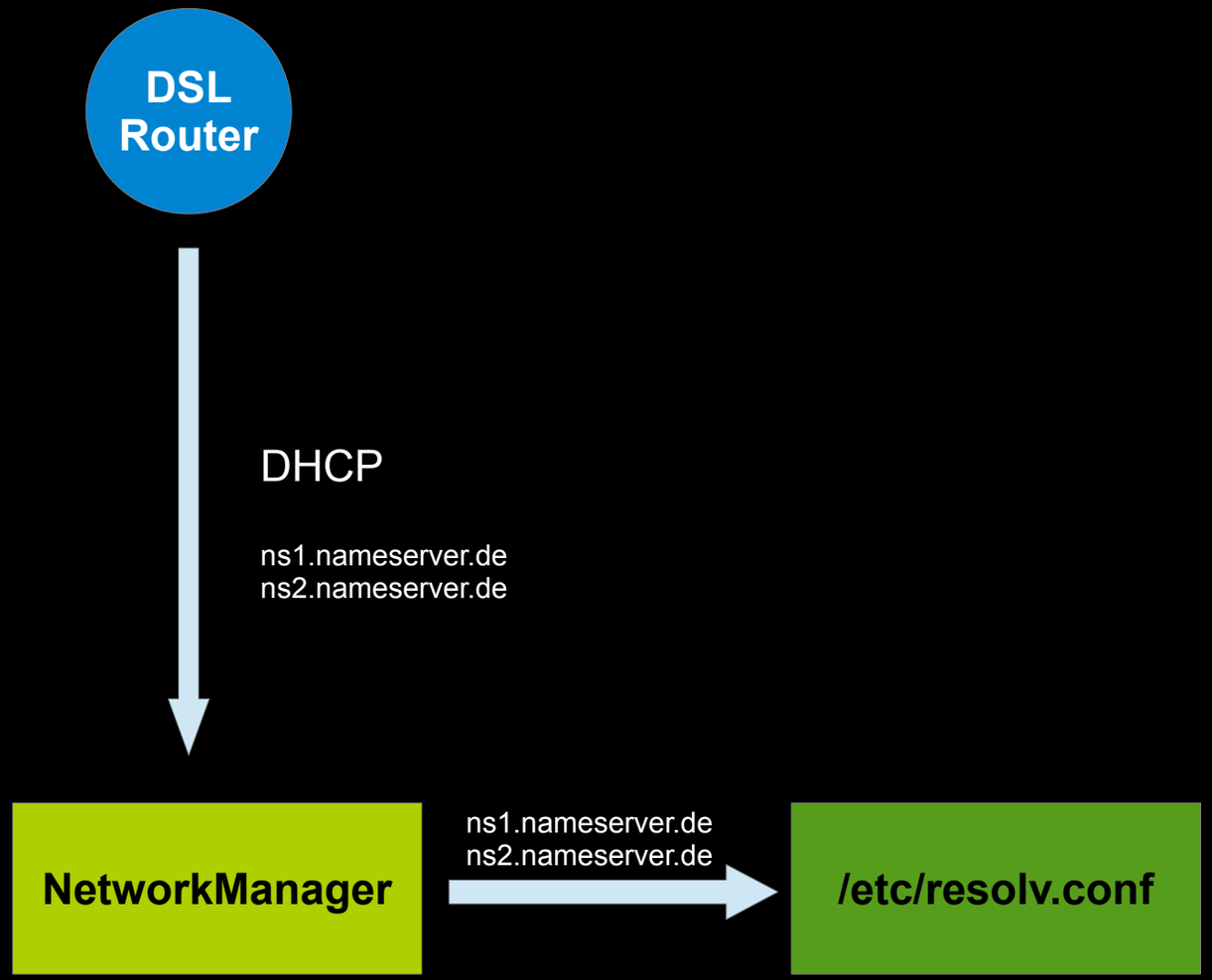


„Wie läuft das im PC ab?“

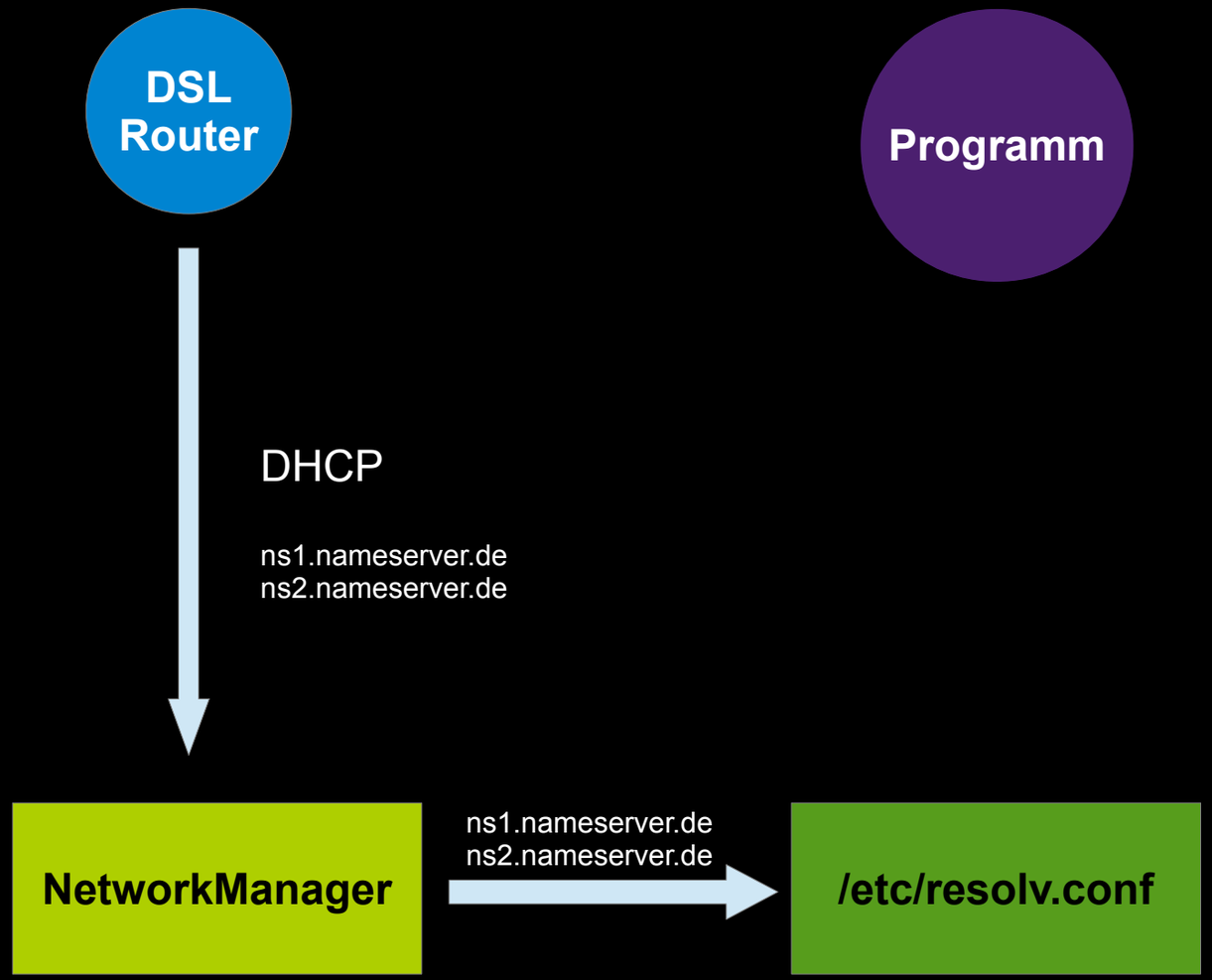
„Wie läuft das im PC ab?“



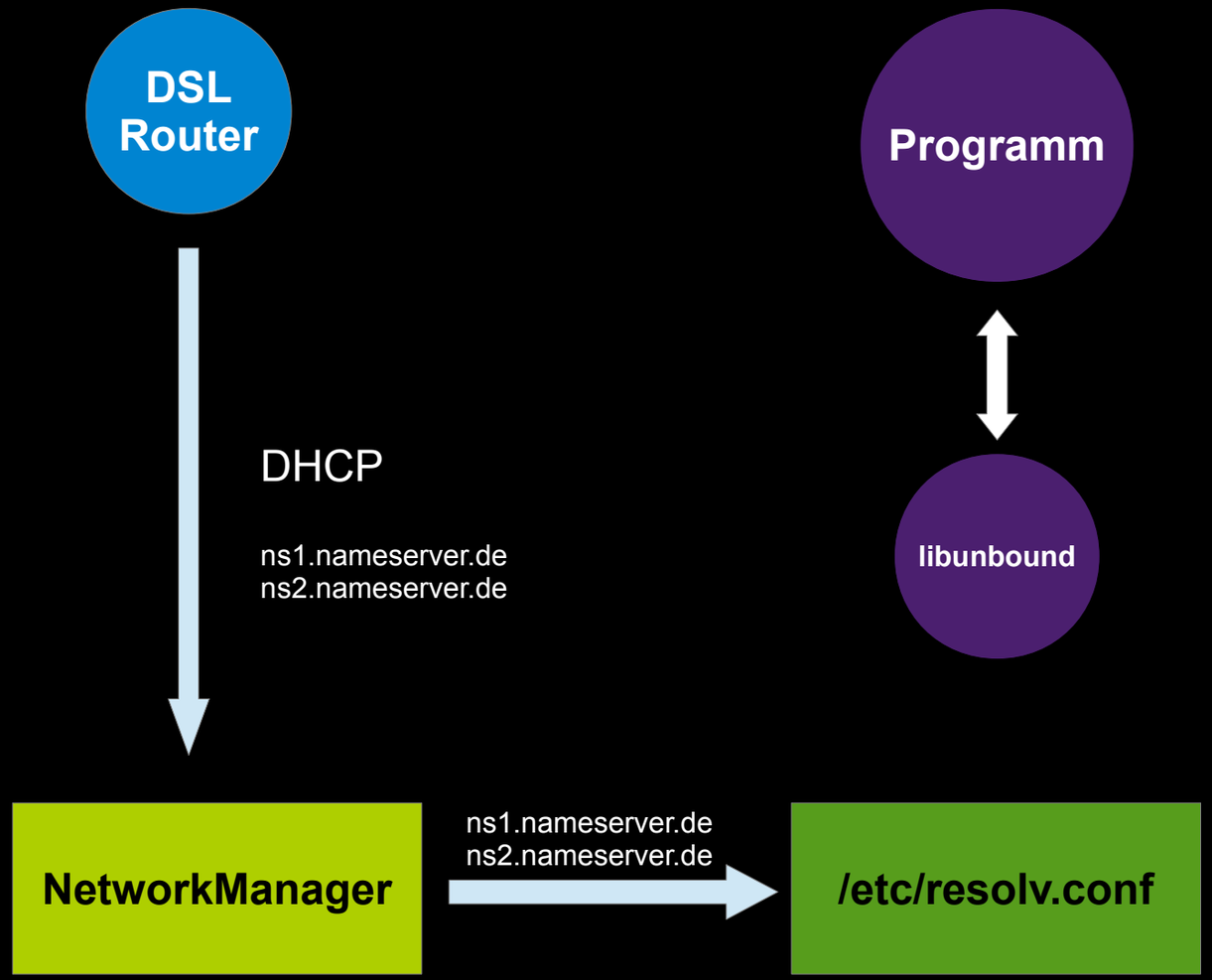
„Wie läuft das im PC ab?“



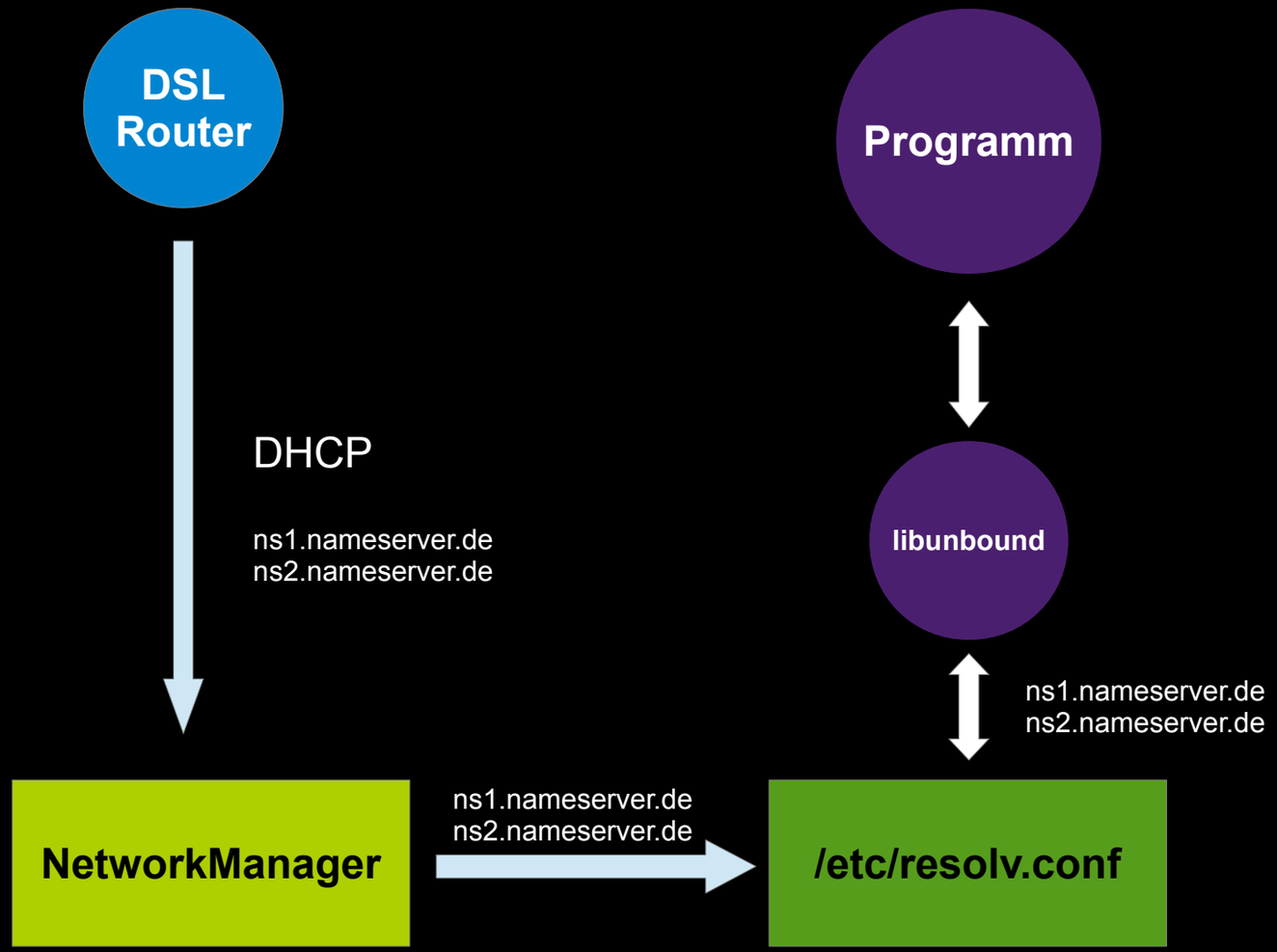
„Wie läuft das im PC ab?“



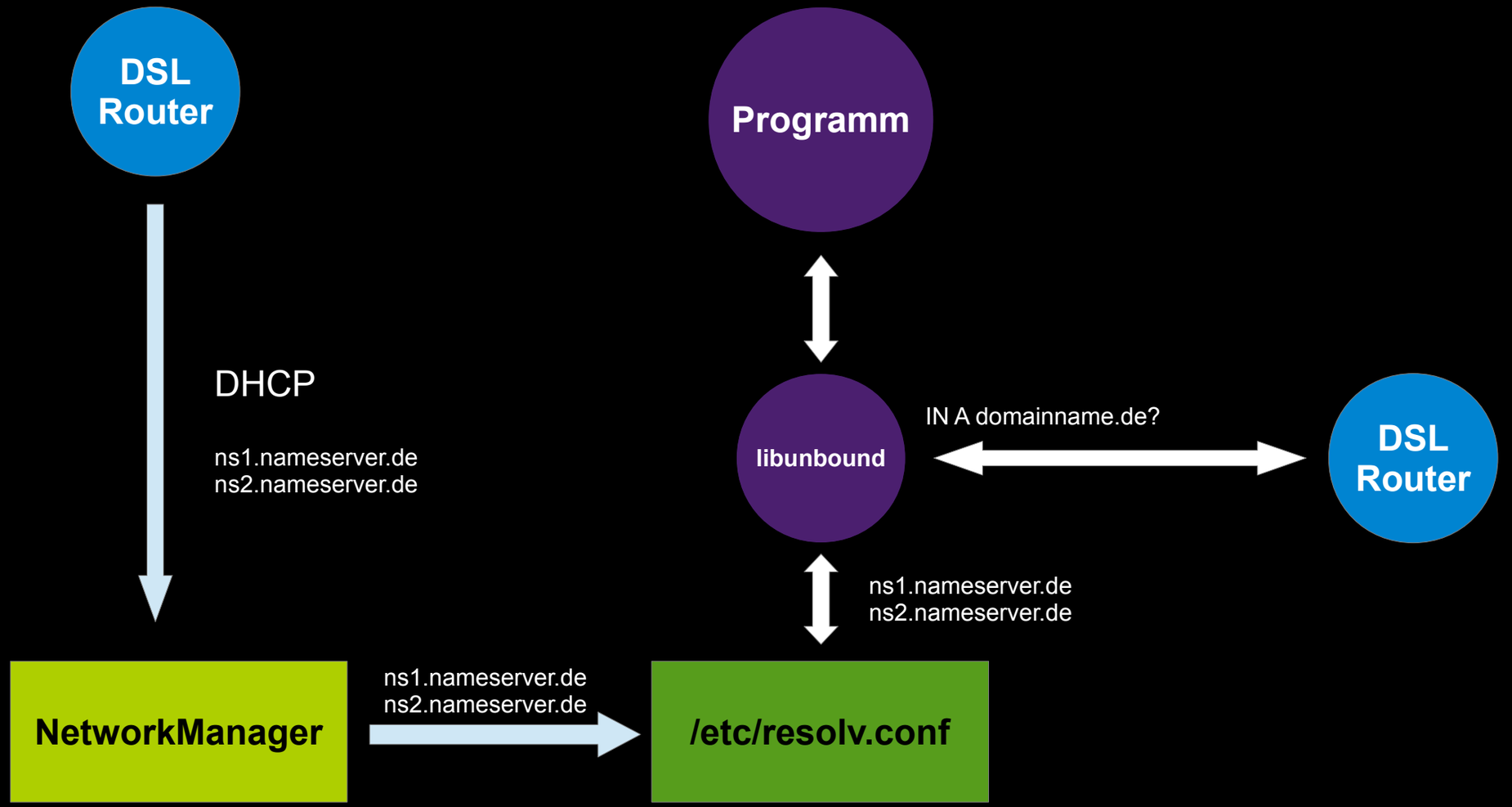
„Wie läuft das im PC ab?“



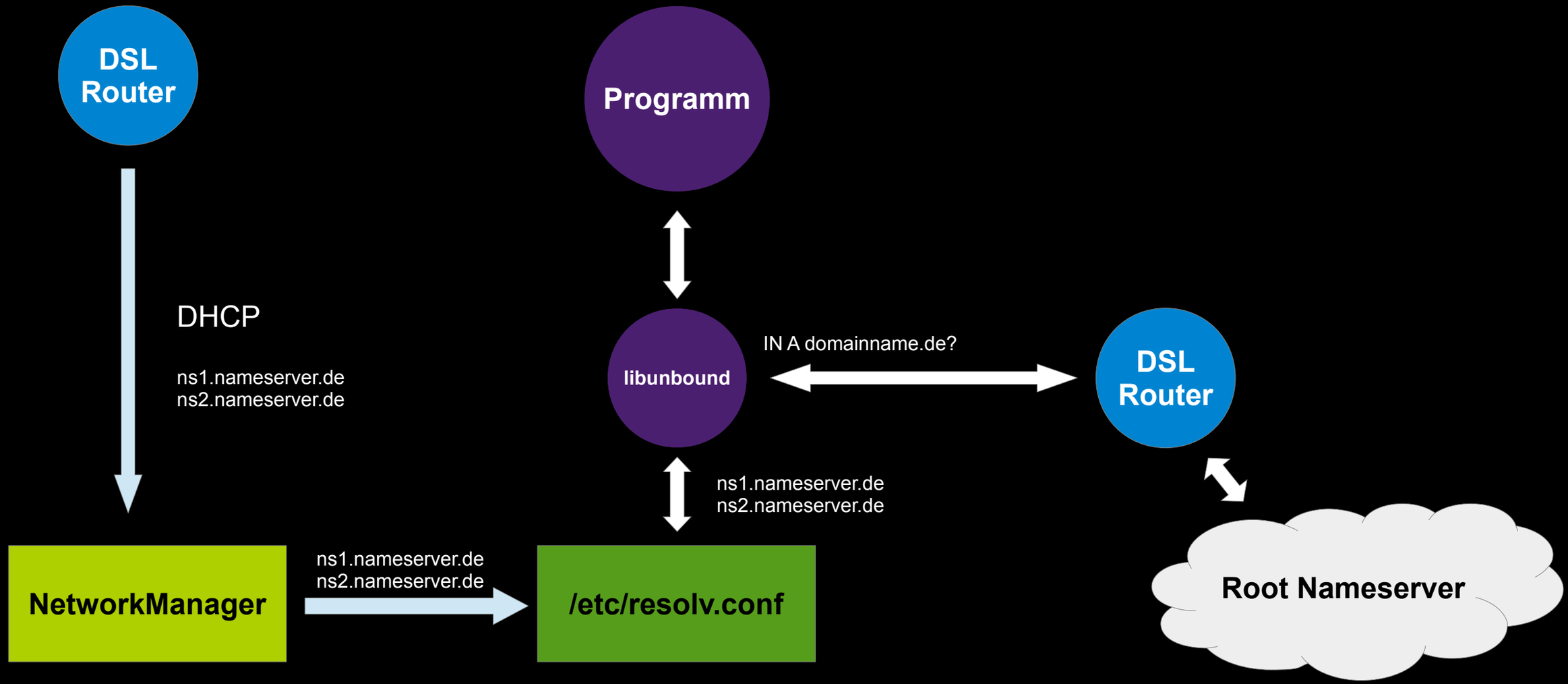
„Wie läuft das im PC ab?“



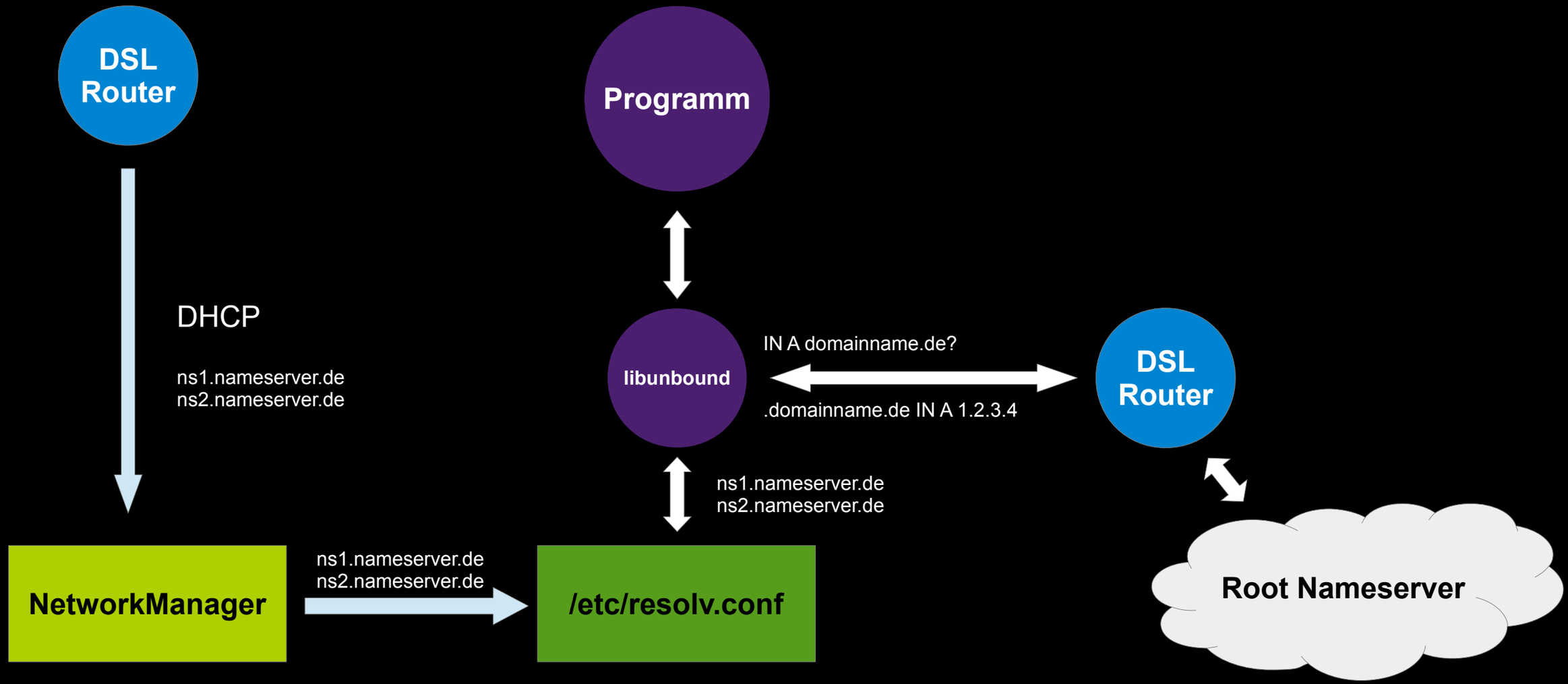
„Wie läuft das im PC ab?“



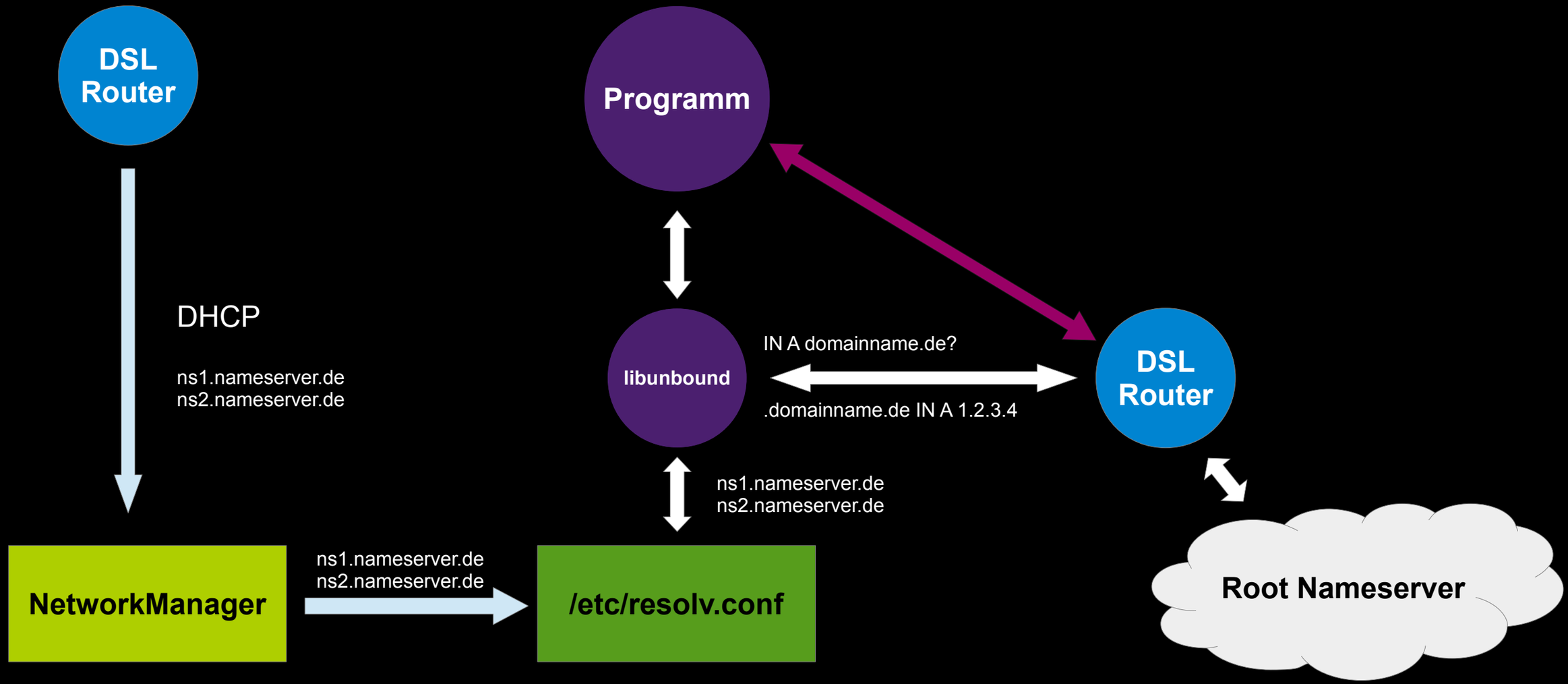
„Wie läuft das im PC ab?“



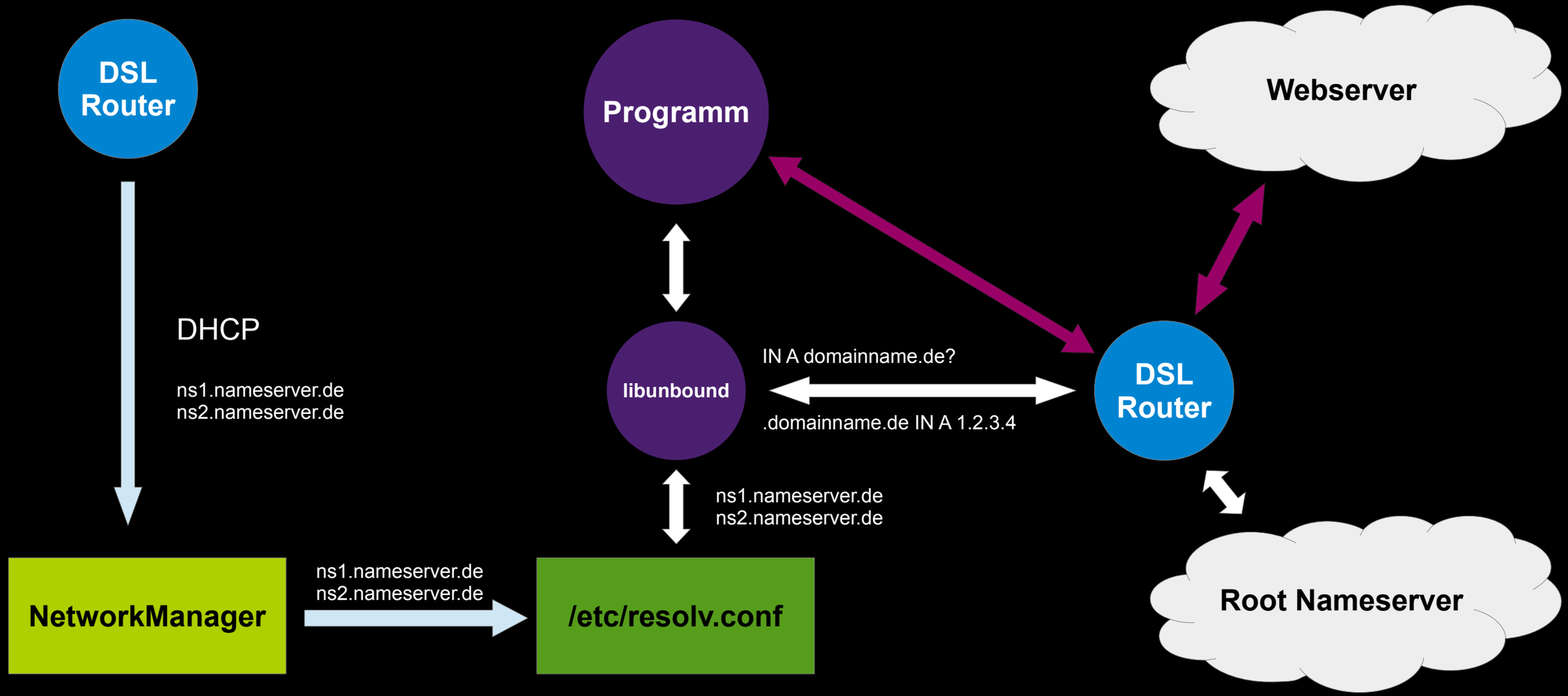
„Wie läuft das im PC ab?“



„Wie läuft das im PC ab?“



„Wie läuft das im PC ab?“



„Wie viele DNS Server gibt es?“

Millionen.

„Wer fragt wen?“

In der Regel, bekommen Internetteilnehmer die Namen und IP Adressen von zwei DNS-Caching Servern des jeweiligen Providers.

„Wer fragt wen?“

Die Caches merken sich Domaininformationen.

„Wer fragt wen?“

Das macht Sinn, weil jeder Webseiten Besuch eine DNS Abfrage erzeugt und so nicht alle INET Benutzer immer die ganze Kette von Root bis zum Domainnameserver durchfragen müssen.

„Wer fragt wen?“

Das DNS-System würde sonst unter der Last zusammenbrechen.

„Die Vertrauensfrage“

Kann ich meinem DNS-Cache vertrauen?

„Die Vertrauensfrage“

Kommt drauf an.

„Die Vertrauensfrage“

In Deutschland würde ich Ja sagen,
in den USA und anderen Ländern tendiere ich zu Nein.

„Die Vertrauensfrage“

Provider in den USA und anderswo müssen Domainsperren im DNS umsetzen. D.b., daß bei Anfrage nach

www.piratebay.com

bei DNS-Caches der Provider eine andere IP kommt, als die Domain wirklich hat.

„Die Vertrauensfrage“

Was bei PirateBay noch legitim sein mag, kann ein DNS Betreiber auch für alle anderen Domainanfragen machen.

„Die Vertrauensfrage“

Abhilfe schafft ein eigenes DNS-Cache zuhause.

„Die Vertrauensfrage“

Vertrauen sich denn die ganzen Nameserver gegenseitig?

„Die Vertrauensfrage“

Das tun sie nicht.

„Die Vertrauensfrage“

Im originalen DNS-System kann ein Angreifer Antworten so fälschen, daß der Anfragene den Unterschied nicht merkt.

„Die Vertrauensfrage“

Deswegen wurde DNS-SEC erfunden.

„Die Vertrauensfrage“

DNS-SEC sichert kryptografisch die Antworten ab,

so daß jederzeit verifiziert werden kann,

ob eine Antwort stimmt.

„Die Vertrauensfrage“

Wo ist dann das Problem?

„Die Vertrauensfrage“

DNS Sec erfordert einigen Aufwand auf Seiten der Betreiber,

aber schlimmer ist die Programmseite beim Benutzer.

„Die Vertrauensfrage“

Es gibt kaum DNS-SEC fähige Resolversoftware(Auflöser).

„Die Vertrauensfrage“

Für Linux sind dies gerade mal → 2 ← Apps im gesamten Fedora Repository.

„Die Vertrauensfrage“

Wo keine Anfrage ist, ist auch kein Angebot.

„Die Vertrauensfrage“

Der Einsatz von DNS SEC bedeutet nämlich auch,

daß die Anfragen langsamer und die Datenpakete größer sind.

„Die Vertrauensfrage“

Langsamer wollen die Internetnutzer aber nicht akzeptieren.

„Die Vertrauensfrage“

Da auch bei DNS SEC die Datenpakete unverschlüsselt transportiert werden, hat man DoT erfunden.

DNS-over-TLS

„Die Vertrauensfrage“

DoT ist aber noch langsamer

und daher praktisch nicht im Einsatz.

„Die Vertrauensfrage“

Fazit

DNS SEC ist nicht so umfänglich verbreitet, wie man es bräuchte.

DoT ist noch langsamer

„DNS over HTTPS?“

Und das führt uns zu

DNS over HTTPS

„DNS over HTTPS?“

Weil DoT nicht verbreitet ist, haben sich Mozilla, Google,

Cloudflare und die üblichen anderen Verdächtigen,

verabredet, DNS über eine HTTPS Verbindung zu machen.

„DNS over HTTPS?“

Dabei sendet der Browser, weil der ja ohnehin schon HTTPS sprechen kann, die DNS Anfragen an einen Cloudflare Server, der dann die echten DNS fragt.

„DNS over HTTPS?“

Jetzt gibt es aber nur EINEN Cloudflare Server,

der alle Anfragen von allen Firefox Browsern bekommen soll.

„DNS over HTTPS?“

Da liegt das Problem.

„DNS over HTTPS?“

Selbst wenn Cloudflare als US Firma, seine Benutzer nicht zu Marketingzwecken ausspionieren würde, es wäre immer noch eine US Firma, die dem US Recht und der US Gerichtsbarkeit unterliegt.

„DNS over HTTPS?“

D.b. wenn es z.B. der US Regierung nicht paßt,
das bs-lug.de noch weiter freie Inhalte ausliefert,
dann wird Cloudflare angewiesen, dies zu unterbinden.

„DNS over HTTPS?“

Dies alleine ist schon ein Grund DoH
in der geplanten Form zu unterbinden.

„DNS over HTTPS?“

Jetzt vermarkten praktisch alle US Provider die DNS Daten Ihrer Kunden um noch besser Werbung platzieren zu können.

Mozilla lies dies „angeblich“ vertraglich unterbinden,
aber wer sollte das schon kontrollieren?

„DNS over HTTPS?“

Von der technischen Seite betrachtet, ist ein zentralisierter Dienst ein Flaschenhals. Bricht der Dienst zusammen, merken das alle User, statt nur örtlich begrenzter Benutzergruppen.

„DNS over HTTPS?“

Von der technischen Seite betrachtet, ist ein zentralisierter Dienst ein Flaschenhals. Bricht der Dienst zusammen, merken das alle User, statt nur örtlich begrenzter Benutzergruppen.

Firefox „soll“ dann auf normales DNS ausweichen.

„DNS over HTTPS?“

Bitte diskutieren Sie jetzt!