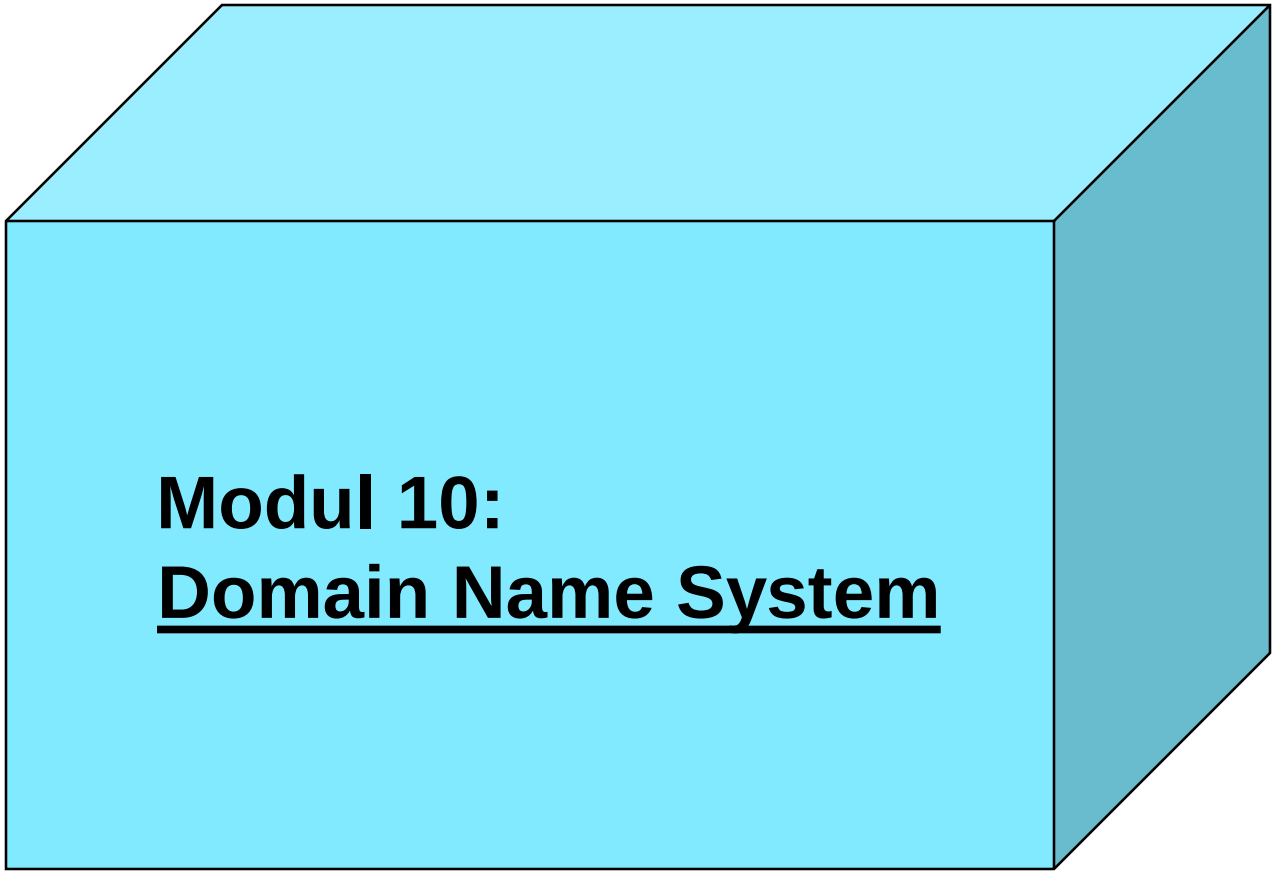
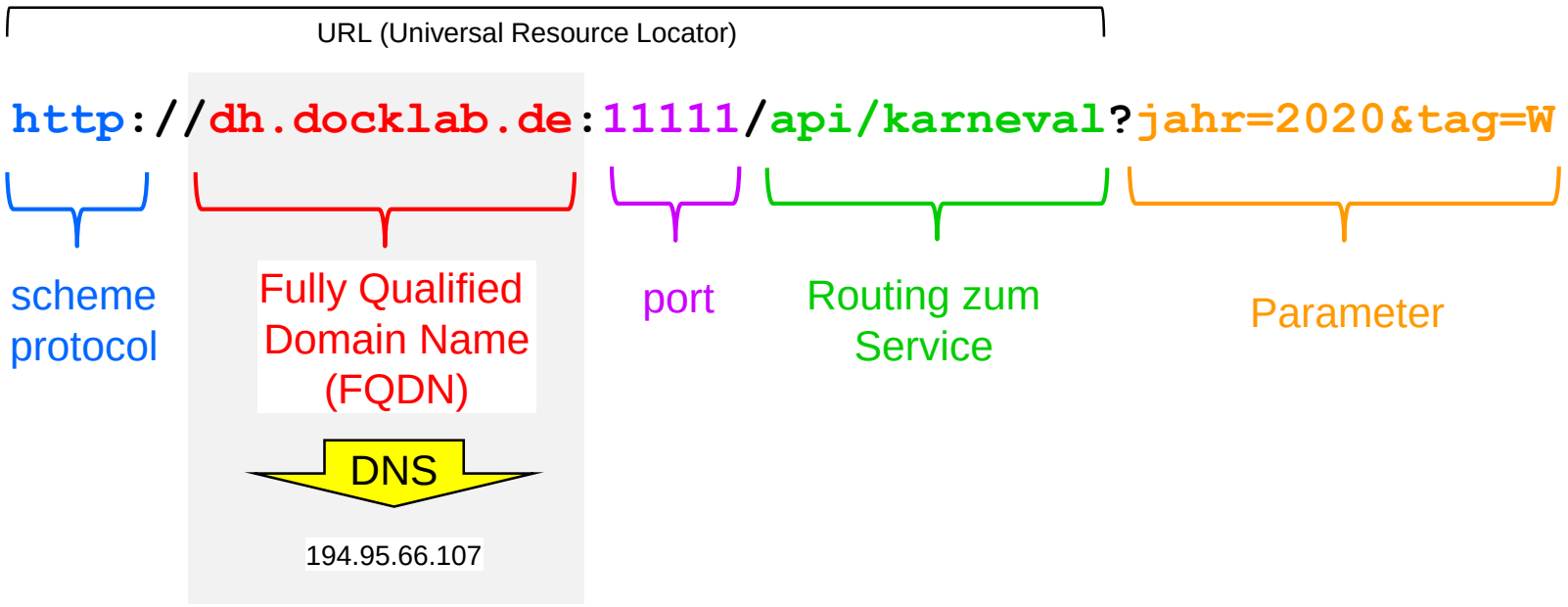


Namensraum: URL - URI - Domain

- **Jede Ressource im Internet wird kann durch einen vom Menschen lesbaren Identifikator (Uniform Resource Identifier, URI) identifiziert werden. Grundprinzip, eingeführt 1994 durch Timothy John Berners-Lee (Erfinder des WWW).**
- **Karnevalservice des Netzlabors liefert den Tag für Weiberfastnacht als JSON-Datensatz.
Aufruf des Services über einen speziellen URI.**

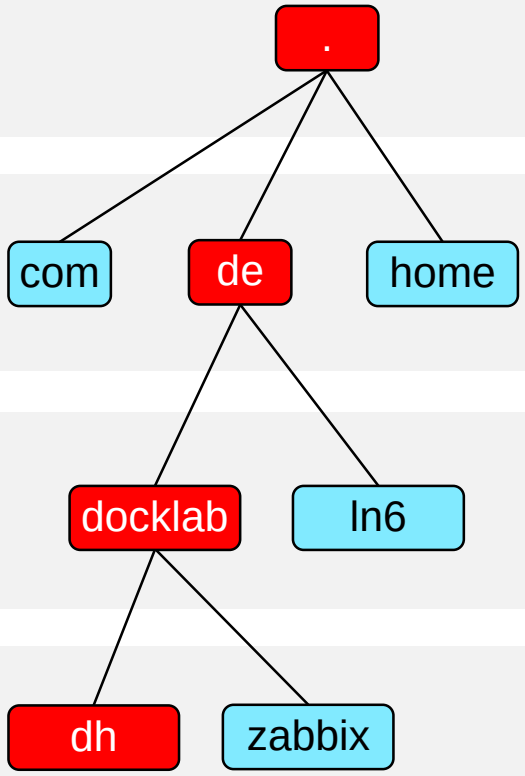


Überblick: Domain Name System

- **Aufgabe:**
  Namensauflösung Domain → IP
- **Bedeutung:**
  Extrem wichtiger Netzdienst, ohne diesen läuft praktisch nichts mehr.
- **Technische Realisierung:**
  Weltweit, verteilte Anwendung.
- **Organisation:**
  - hierarchisch strukturierter Namensraum.
  - dezentrale Verwaltung.
- **Sicherheit:**
  - Vielfältige Angriffe („Falsche Auskunft“, Denial of Service, …)
  - Abwehrmaßnahmen (z.B. DNSSEC (DNS Security))
- **Beschrieben in**
  - RFC IS 1034: Domain names - concepts and facilities, IS, November 1987.
  - schon 1987 IS (= Internet Standard), seither nur "Updates".

Struktur der Domain Names

DNS Root



Die Rootdomain ist leer.

TLD, top level domain

- Generische Domänennamen (gTLD)
- CountryCode-Domänennamen (ccTLD)
- Private TLDs, z.B. home/corp/mail (seit 2018)

Internet Corporation for Assigned Names and Numbers (ICANN) koordiniert TLDs und DNS.

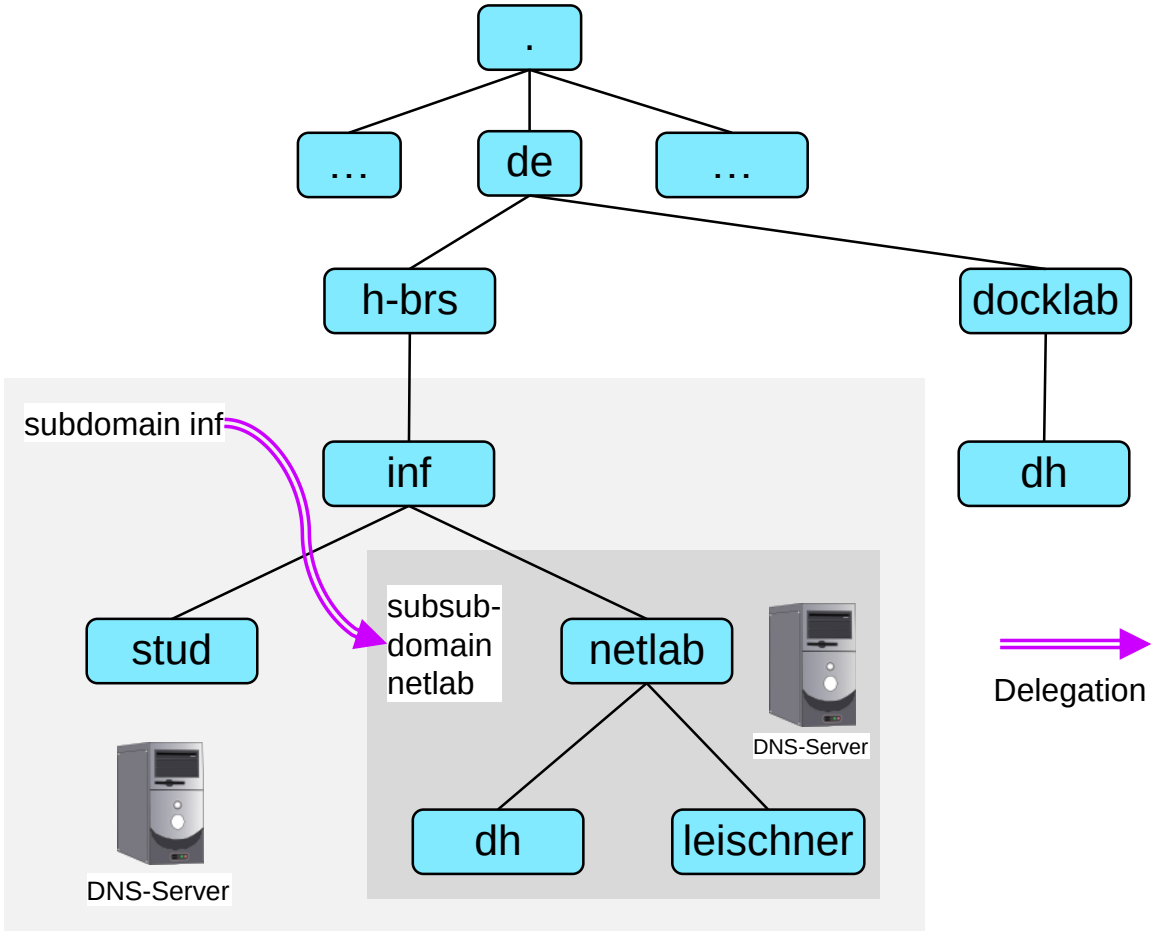
SLD, second level domain

- Werden in der Regel von einem beim zuständigen NIC (denic.de) akkreditierten privatwirtschaftlichen Registrar (Internet Service Provider) verkauft und betreut

TLD, subdomain

- Werden durch den Kunden verwaltet.

Domäne, Delegation, Zone und Zone-File



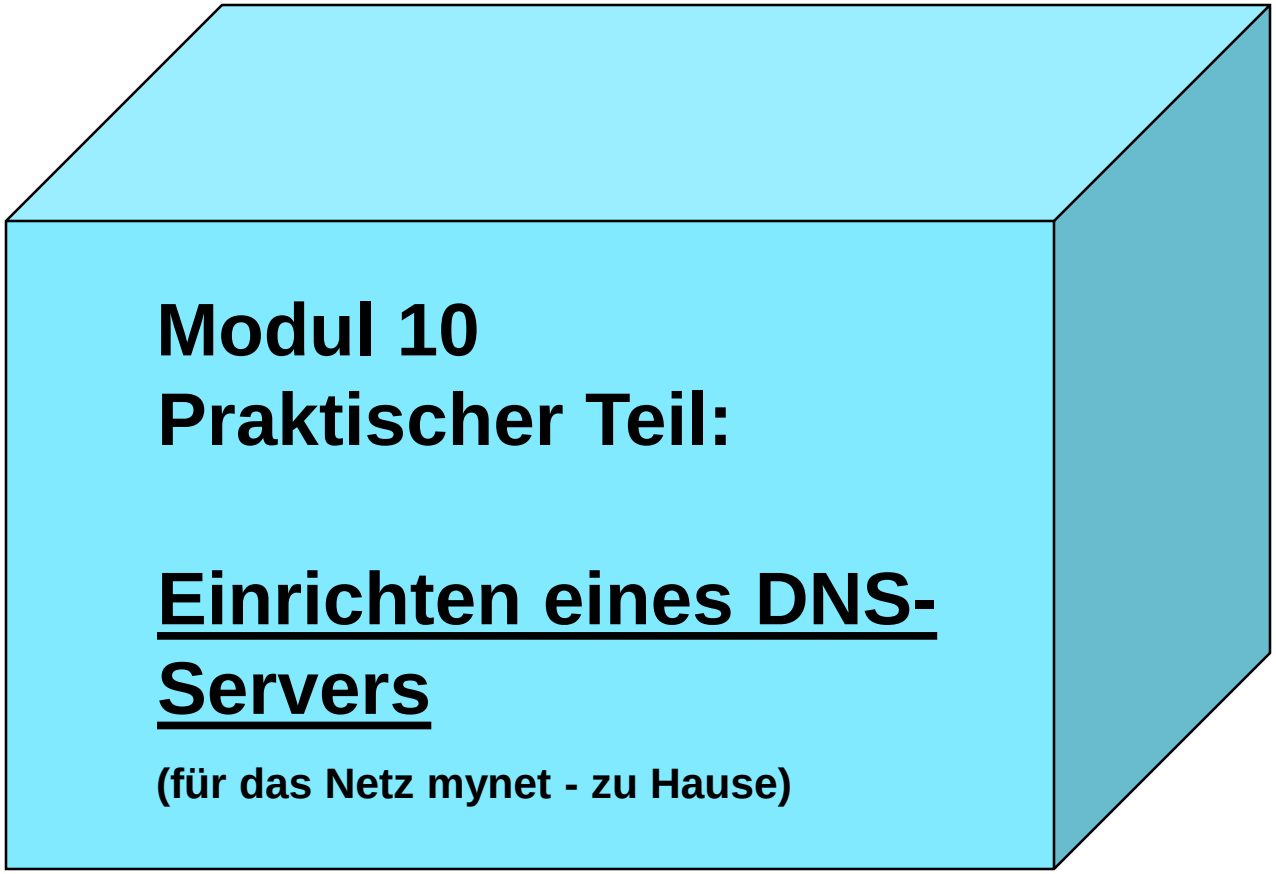
- Die technische und organisatorische Verantwortlichkeit („Authority“) für eine Domäne (Subdomäne, …) kann an einen anderen Administrator übergeben werden („Delegation“).
- Ein Administrator nutzt einen DNS-Server, um den Bereich, für den er verantwortlich ist zu verwalten („Zone“).
- Ein DNS-Server wird durch einen Zone-File konfiguriert, der alle notwendigen Konfigurationsinformationen enthält.
  Findet eine Delegation statt, so muss auch diese im Zone-File beschrieben werden.

Basics zu DNS-Abfrage

- **Einfaches Request/Response-Protokoll.**
- **DNS-Anfrage über UDP Port 53. Maximal 512 Byte. Beispiele von Flags:**
  - **QR: question response**
  - **AA: authoritative answer**
  - **RD: recursion support desired**
  - **RA: recursion support available**
- **Rekursive Antwort auf eine Anfrage (Beispiel: dh.docklab.de):**
  - **Falls Antwort im Cache, wird diese ausgeliefert**
  - **Andernfalls Anfrage an einen der 13 Root-Nameserver bezüglich dh.docklab.de.**
  - **Root-Server sendet Info (Name, IP-Adresse) zu de-Nameserver**
  - **Anfrage an de-Nameserver bezüglich dh.docklab.de.**
  - **de-Nameserver sendet Info (Name, IP-Adresse) bezüglich docklab.de-Nameserver**
  - **…**
- **Iterative Antwort auf eine Anfrage (Beispiel: dh.docklab.de):**
  - **Sendet Antwort, falls direkt möglich, sonst nur Info über weiteren Name-Server.**

DNS Servertypen

- **DNS-Resolver**:
  Software zur Namensauflösung. Können einen Cache enthalten. Betriebssysteme (W10, Ubuntu besitzen eine DNS-Resolver).
- **Forwarding DNS-Server**:
  Ein DNS-Server, der als Resolver betrieben wird. Beispiele: Fritzbox, Pi-Hole
- **Caching DNS-Server:**
  Holt Informationen von anderen DNS-Servern und speichert diese in eine Cache zwischen.
- **Autoritativer DNS-Server**:
  Verantwortlich für eine Zone. (Stichworte: Rekursive Namensauflösung, Reverse-DNS, Backup.)
- **Rekursiver DNS-Server**:
  Löst DNS-Anfrage bei Bedarf rekursiv auf. Betreibt meist zusätzlich einen Cache.
- **Primary / Slave DNS-Server**:
  In einer Domäne werden zwei DNS-Server betrieben. Falls der primäre DNS-Server ausfällt, übernimmt der Slave
- **Public / Private DNS-Server**



Modul 10
Praktischer Teil:

Einrichten eines DNS-Servers

(für das Netz mynet - zu Hause)

DNS Software

- **BIND**
  Standard DNS-Server. Offizielle aktuelle ist Version `bind10`, eingesetzt wird aber `bind9`.
  `Bind9` ist auch die offizielle Version im Ubuntu 18.04-Repo.
- **PowerDNS**
  Open source, Konkurrent zu BIND, BIND-kompatible Datenspeicherung
- **Unbound**
  High-Performance DNS-Server. Modularer Aufbau.
- **Dnsmasq**
  Leichter, einfach zu konfigurierender DNS-Server. Wird im Pi_hole verwendet
- **Pi-Hole**
  Spezial-DNS-Server, der Werbung im ganzen Netz blockt.

Installation und Konfiguration von BIND

```
$ apt install bind9
```

Erzeugt im Verzeichnis `/etc/bind` u.a. die folgenden Konfigurationsfile:

- `named.conf` — Lädt nur die folgenden drei Config-Files.
- `named.conf.options` — Setzt Optionen für den DNS-Server
- `named.conf.default-zones` — Enthält standardmäßig gesetzte Zonen, z.B. localhost
- `named.conf.local` — Hier werden vom Administrator, die von ihm verwalteten Zonen definiert. (insbesondere Zonennamen + Zonenfiles)

Für jede Domäne gibt es zwei Zonen: Forward-Lookup, Reverse-Lookup .
Eine Zonendefinition verweist auf einen Zone-File, z.B.

`fwd.netlab.inf.h-brs.de.db` oder `rev.netlab.inf.h-brs.de.db`

der die Ressourcen-Records der entsprechenden Zone enthält. Hier werden neue DNS-Einträge hinzugefügt.

mynet-Konfiguration von `named.conf.options`

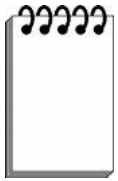
```
options {
        directory "/var/cache/bind";

        recursion yes;                  # enables resursive queries
        allow-recursion { trusted; };   # allows recursive queries from
                                        # "trusted" clients
        listen-on { 192.168.178.11; }; # ns1 private IP address
                                        # - listen on private network only
        allow-transfer { none; };       # disable zone transfers by default

        forwarders {
                192.168.178.1;
                1.1.1.1;
                8.8.4.4;
        };

        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
}
```



Allgemeines Beispiel einer Master-Zonenbeschreibung

```
zone "netlab.inf.h-brs.de" IN {
    type master;
    file "fwd.netlab.inf.h-brs.de.db";
      # Forward zone lookup file with resource records
};
```

Zonentypen:

- **master:** Enthält alle Daten der Zone und liefert eine „authoritative answers“.
- **slave:** Replikation der Master-Zone.
- **forward:** Nur Weiterleitung an andere Server

mynet-Konfiguration von `named.conf.local` (Zonennamen + Zonenfiles)

```
zone "mynet.home" IN {          # Domain name
    type master;                # Primary DNS
    file "/etc/bind/fwd.mynet.home.db";
                                # Forward lookup file
    allow-update { none; };     # Since this is a primary DNS,
                                # it should be none.
};

zone "178.168.192.in-addr.arpa" IN { # Reverse lookup name,
                                # should match your network
                                # in reverse order
    type master;                # Primary DNS
    file "/etc/bind/rev. mynet.home.db";
                                # Reverse lookup file
    allow-update { none; };     # Since this is a primary DNS,
                                # it should be none.
};
```

Allgemein: Aufbau des Zone-Files

Mailadresse:
admin@mynet.home

Zone-File: Liste von Resource Records für eine Zone:

- **Ein SOA Resource Record (*Start of Authority*) ist der erste Record im Zone-File. Enthält globale Parameter für die Zone.**

```
@   IN   SOA    ns1.mynet.home. admin.mynet.home. (
                   2019041001 ; serial YYYYMMDDnn
                   14400      ; refresh (4 hours)
                   1800       ; retry   (30 minutes)
                   1209600    ; expire  (2 weeks)
                   3600   )   ; minimum (negative Caching)
```

- `serial`: Seriennummer (wichtig, damit Änderungen autom. übernommen werden).
- `refresh` / `retry` / `expire`: steuern Zusammenspiel zwischen Master / Slave
- `minimum`: (Gültigkeitsdauer eines Negative-Eintrags im Cache)
- `@` steht für die aktuelle Domäne (hier: `mynet.home.`)
- Das `@` kann auch an manchen Stelle durch ein Blank ersetzt werden. Beispiel folgt.

Allgemein: Aufbau des Zone-Files

- Ein NS Resource Record definiert einen Name Server für die Zone.
  - Ein Zone File kann mehrere NS Records enthalten.
  - Ein NS Record kann auch auf einen Nameserver eine Subdomäne verweisen.

```
;Name Server Information for domain mynet.home
        IN      NS      ns1.mynet.home.
        IN      NS      ns2.mynet.home.

;IP address of Name Server
ns1     IN      A       192.168.178.11
ns2     IN      A       192.168.178.12
```

- $ORIGIN setzt den Zonenamen für alle darauffolgenden Einträge

```
$ORIGIN subdomain.mynet.home.
```

Allgemein: Aufbau des Zone-Files

- Ein A Resource Record weist einem DNS-Namen eine IPv4-Adresse zu:

```
pihole.mynet.home   3600   IN   A     192.168.178.13
```

(Gültigkeitsdauer im Cache: 3600 Sek.)

Kürzere Schreibeweise für diesen Record:

```
pihole   3600   IN   A     192.168.178.13
```

Noch kürzer:

```
pihole   A     192.168.178.13
```

- Ein AAAA Resource Record weist einem DNS-Namen eine IPv6-Adresse zu:

```
dh.docklab.de          3600   N   AAAA    2001:638::1
```

- CNAME Resource Record: Verweist auf einen anderen Domänennamen.
- MX Resource Record: Gibt den Mailserver (FQDN) für die Domäne an.
- PTR Resource Record: Ordnet einer IP-Adresse einen Domänennamen zu (FQDN). Anwendung für Reverse Lookup.

```
13    IN    PTR  pihole.mynet.home. 178.168.192.in-addr.arpa.
```

Eintrag im Zone-File der Reverse-Lookup-Zone

mynet-Konfiguration für den Forward-Zone-File

```
$TTL 1d
@       IN      SOA     ns1.mynet.home. admin.mynet.home. (
                        18122001        ; Serial
                             3h         ; Refresh
                            15m         ; Retry
                             3w         ; Expire
                             3h )       ; Negative Cache TTL

;Name Server Information
@       IN      NS      ns1.mynet.home.
@       IN      NS      ns2.mynet.home.
;IP address of Name Server
ns1     IN      A       192.168.178.11
ns2     IN      A       192.168.178.12

;A - Record HostName To Ip Address
fritzbox        IN      A       192.168.178.1
ns1             IN      A       192.168.178.11
ns2             IN      A       192.168.178.12
pihole          IN      A       192.168.178.13
```

mynet-Konfiguration für den Reverse-Zone-File

```
$TTL 1d
@       IN      SOA     ns2.mynet.home. admin.mynet.home. (
                        19041001        ; Serial
                             3h         ; Refresh
                            15m         ; Retry
                             3w         ; Expire
                             3h )       ; Negative Cache TTL

;Name Server Information
@       IN      NS      ns1.mynet.home.
@       IN      NS      ns2.mynet.home.
;Reverse lookup for Name Server
11      IN      PTR     ns1.mynet.home.
12      IN      PTR     ns2.mynet.home.

;PTR Record IP address to HostName
1       IN      PTR      fritzbox.mynet.home.
11      IN      PTR      ns1.mynet.home.
12      IN      PTR      ns2.mynet.home.
13      IN      PTR      pihole.mynet.home.
```

Literatur

1. DNS for Rocket Scientists: http://www.zytrax.com/books/dns/, Zugriff am 09.04.2019.
2. Ron Aitchison: Pro DNS and BIND 10, Springer Science+Business Media, 2011
3. Wiki: Domain Name System, https://de.wikipedia.org/wiki/Domain_Name_System , Zugriff am 09.04.2019.
4. Wiki: Zonendatei, https://de.wikipedia.org/wiki/Zonendatei , Zugriff am 10.04.2019.

Hausaufgabe bis zum nächsten Mal

Inhalt der nächsten Vorlesung ist das Protokoll SSH (Secure Shell).

Zur Vorbereitung benötigen Sie elementare Grundlagen aus dem Bereich der asymmetrische Verschlüsselung (die Sie sich in 5 Minuten über Videos „reinziehen“ können)**.**

- **Informieren Sie sich über die Begriffe:**
  - **Public-Key-Verfahren**
  - **Öffentlicher Schlüssel**
  - **Zertifikat**
  - **Privater Schlüssel**

Quellen:

- **Public-Key-Verfahren: https://www.youtube.com/watch?v=pULfS1_-EQk (1:10min)**
- **What is Public Key Infrastructure (PKI) by SecureMetric: https://www.youtube.com/watch?v=i-rtxrEz_E8 (3:40)**