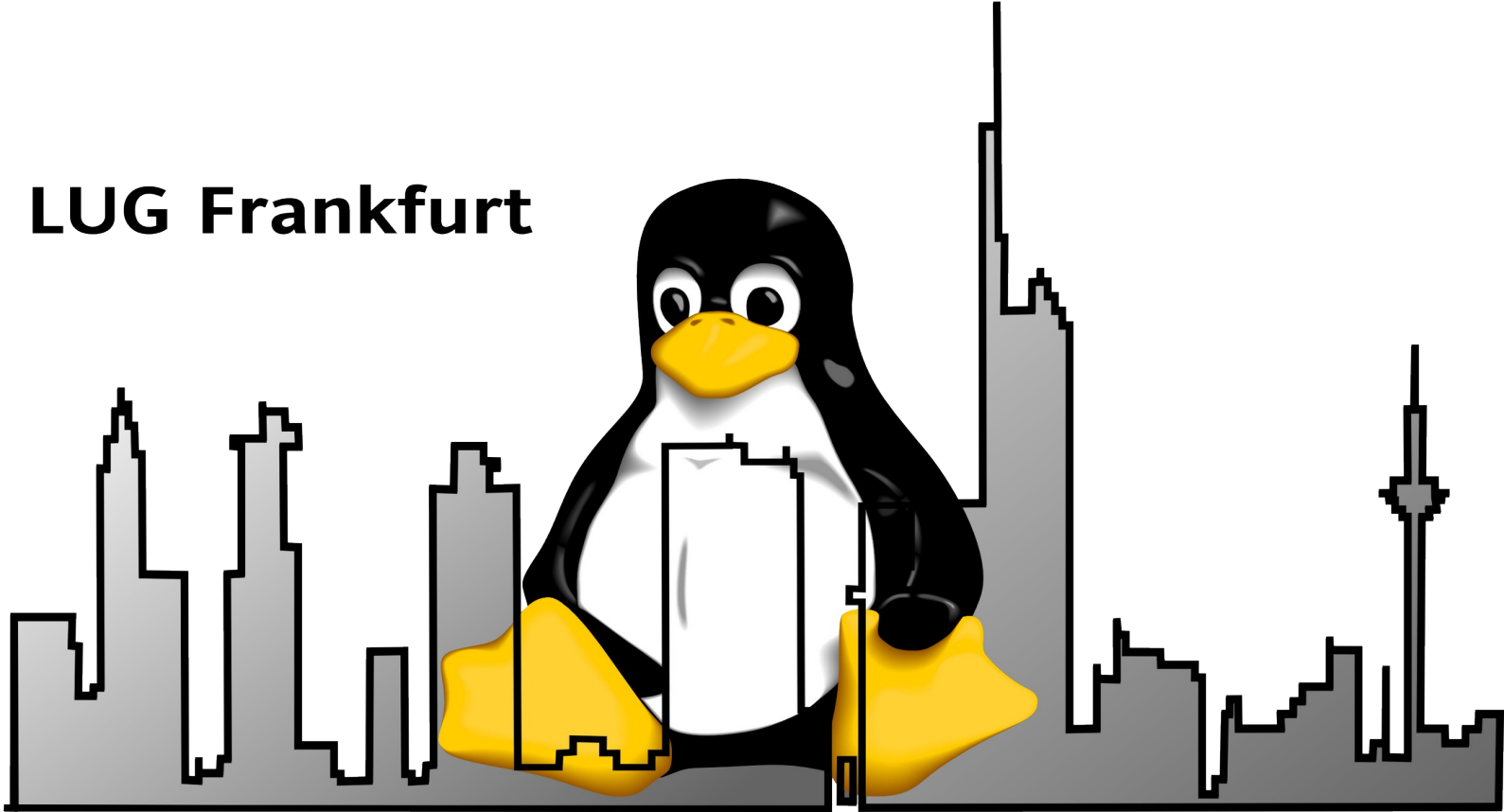
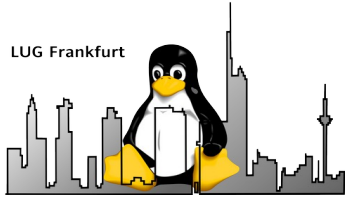


Debian-DNS

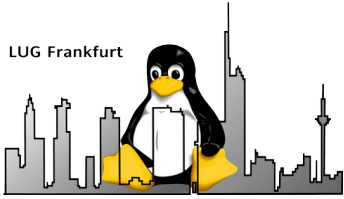
LUG Frankfurt





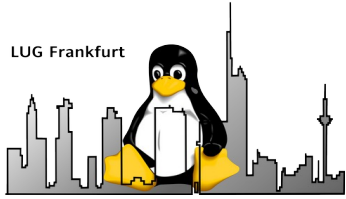
Inhalt

- Motivation und Konzept für router+DNS+DHCP
- Basis-Infos DNS
- Virtuelle Maschine clonen
- Installation / Konfiguration DNS
- Test DNS
- Ausblick auf DDNS und DHCP



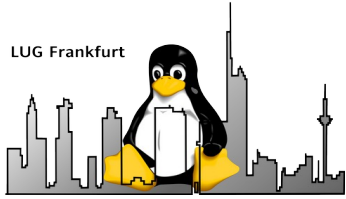
Konzept

- Vier virtuelle Maschinen
 - fralug-rtg (router-gateway-firewall)
 - fralug-local (Testmaschine)
 - fralug-dns (DDNS-Server)
 - fralug-dhcp (DHCP-Server)
- Getrennte virtuelle Maschinen für jede Funktion



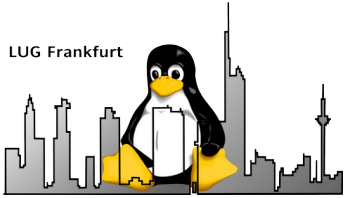
Bisherige virtuelle Maschinen

- Router: fralug-rtg
- Lokale virtuelle Testmaschine: fralug-local



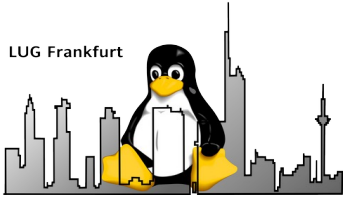
Inhalt

- Motivation und Konzept für router+DNS+DHCP
- **Basis-Infos DNS**
- Virtuelle Maschine clonen
- Installation / Konfiguration DNS
- Test DNS
- Ausblick auf DDNS und DHCP



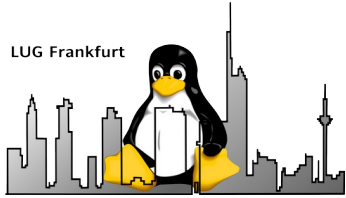
DNS-Basis-Info-1

- Aufgaben:
 - Namen statt Zahlenkolonnen (IP-Adressen)
 - Zielrechner und Zielnetze unabhängig von IP-Adressen über Namen erreichen
 - Lokale **/etc/hosts**-Datei für die Auflösung ersetzen
→ zentrale verteilte Verwaltung (Domain-Hierarchie)
 - Weitere Netzwerkparameter möglich



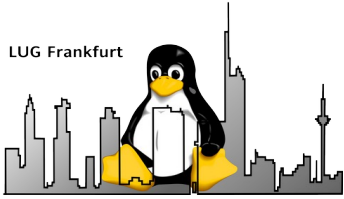
DNS-Basis-Info-2

- Ablaufreihenfolge (Name → IP-Adresse)
 - Beispiel: **www.heise.de**
 - /etc/hosts (/etc/host.conf)
 - Lokaler DNS-Cache
 - DNS ↔ /etc/resolv.conf
 - DNS der nächsten Ebene (bis root-Server)



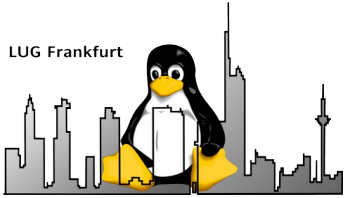
Inhalt

- Motivation und Konzept für router+DNS+DHCP
- Basis-Infos DNS
- **Virtuelle Maschine clonen**
- Installation / Konfiguration DNS
- Test DNS
- Ausblick auf DDNS und DHCP



Clone erstellen und anpassen

- fralug-local → fralug-dns
 - Lokale Anpassungen vornehmen
 - **Eineindeutige** UUIDs aller Partitionen!
 - Dateien anpassen: hosts, hostname, fstab, grub
 - *clone_vm.sh* : vollständiger Clone inkl. lokaler Anpassungen
- Im Testnetz als eigenständige Maschine sichtbar.



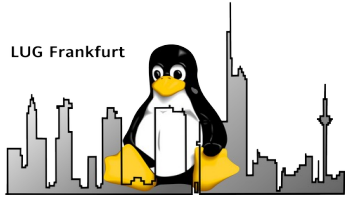
fralug-dns-1

- Statische IP-Adresse für das lokale Netz

/etc/network/interfaces

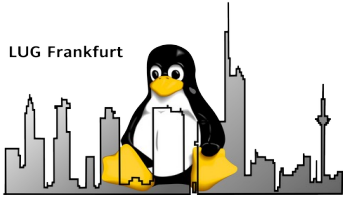
```
# The secondary network interface
allow-hotplug enp0s8
iface enp0s8 inet static
    address 10.66.80.250
    netmask 255.255.255.0
    network 10.66.80.0
    broadcast 10.66.80.255
    gateway 10.66.80.254
```

- Für DNS sind statische IP-Adressen erforderlich!



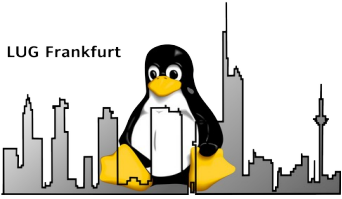
Inhalt

- Motivation und Konzept für router+DNS+DHCP
- Basis-Infos DNS
- Virtuelle Maschine clonen
- **Installation / Konfiguration DNS**
- Test DNS
- Ausblick auf DDNS und DHCP



DNS-Installation

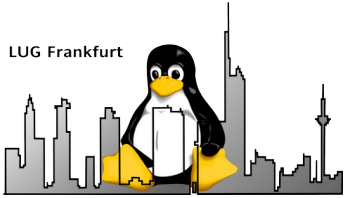
- Minimales DNS installieren
 - aptitude install bind9
 - aptitude install bind9-dnsutils
- Beschränkung auf IPv4
 - /etc/default/named
OPTIONS="-u bind -4"
- Konfigurationsfiles in /etc/bind
 - Basis: **named.conf**



File: named.conf (1)

- **/etc/bind/named.conf (options)**

```
options {
  directory "/var/cache/bind";
  version "DNS for fralug-net"; // Damit bei Anfragen keine valide
                                // Versions-Nummer von bind übermittelt wird.
  listen-on port 53 {10.66.80.250; };
  listen-on-v6 {none; }; // kein IPv6 !!
  allow-query {10.66.80.0/24; };
  allow-recursion {10.66.80.0/24; };
  forward only;
  forwarders {10.xx.yy.254; }; // Weiterleiten der DNS-Anfragen an
                                // den DNS-Server des "Heimnetz"
  dnssec-validation no; // ist erforderlich für den Kontakt
                          // zum "Heimnetz"
  auth-nxdomain no; // conform to RFC1035
  masterfile-format text; // Config-Files im Text-Format
}
```



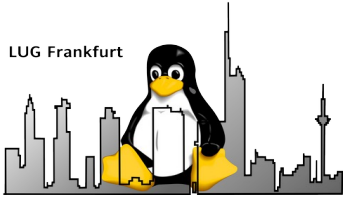
File: named.conf (2)

- **/etc/bind/named.conf (Zonendefinition)**

```
// prime the server with knowledge of the root servers
zone "." { type hint; file "/etc/bind/db.root"; };
```

```
// be authoritative for the localhost forward and reverse zones, and
// for broadcast zones as per RFC 1912
zone "localhost" { type primary; file "/etc/bind/localhost"; };
zone "127.in-addr.arpa" { type primary; file "/etc/bind/localhost.rev"; };
```

```
// fralug-net
zone "fralug-net" { type primary; file "/etc/bind/fralug-net"; };
zone "80.66.10.in-addr.arpa" { type primary; file "/etc/bind/fralug-net.rev"; };
```



File: named.conf (3)

- **/etc/bind/named.conf (nicht Zuständigkeiten)**

```
include "/etc/bind/named.conf.10";    //eigene IP-range ausblenden  
include "/etc/bind/named.conf.10.66"; //eigene IP-range ausblenden
```

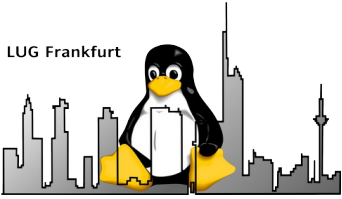
```
zone "64.100.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; }; ...  
zone "127.100.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; };
```

```
zone "254.169.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; };
```

```
zone "16.172.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; }; ...  
zone "31.172.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; };
```

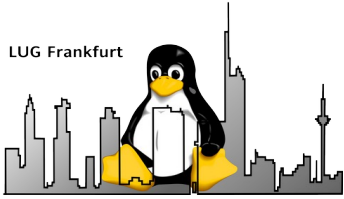
```
zone "168.192.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; };
```

```
zone "18.198.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; };  
zone "19.198.in-addr.arpa" { type primary; file "/etc/bind/db.empty"; };
```



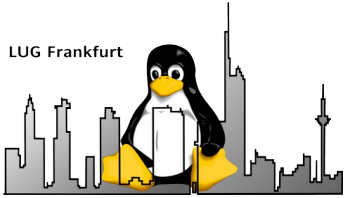
File: db.empty

- **/etc/bind/db.empty**
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
\$TTL 86400
@ IN SOA localhost. root.localhost. (
 1 ; Serial
 604800 ; Refresh
 86400 ; Retry
 2419200 ; Expire
 86400) ; Negative Cache TTL
;
@ IN NS localhost.



fralug-dns-2

- Standard-Files in /etc/bind
 - localhost
 - localhost.rev
 - In -s /usr/share/dns/root.hints db.root
- **fralug-net** und **fralug-net.rev** neu anlegen



File: fralug-net (1)

- **/etc/bind/fralug-net**

```
$ORIGIN fralug-net.
```

```
$TTL      86400      ; 1 day
```

```
fralug-net.  IN  SOA  rtg.fralug-net. root.rtg.fralug-net. (
```

```
2025020701 ; serial
```

```
3600      ; refresh (1 hour)
```

```
600       ; retry (10 minutes)
```

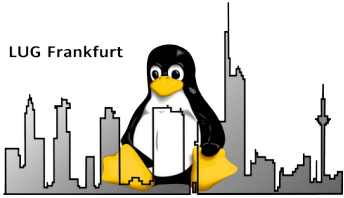
```
3600000   ; expire (5 weeks 6 days 16 hours)
```

```
3600      ; negative cache TTL (1 hour)
```

```
)
```

```
NS  dns.fralug-net.
```

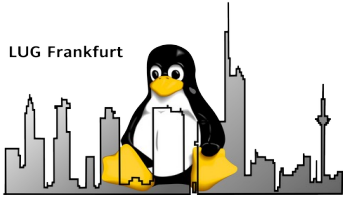
```
MX  10      mail.fralug-net.
```



File: fralug-net (2)

- **/etc/bind/fralug-net**

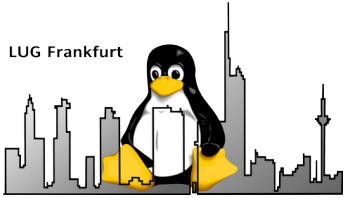
rtg	A	10.66.80.254
fralug-rtg	CNAME	rtg
mail	A	10.66.80.251
dns	A	10.66.80.250
fralug-dns	CNAME	dns
dhcp	A	10.66.80.249
fralug-dhcp	CNAME	dhcp



File: fralug-net.rev

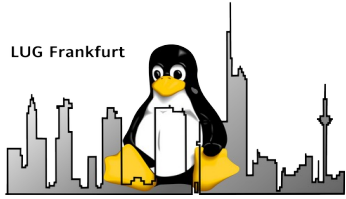
- **/etc/bind/fralug-net.rev**

```
$ORIGIN 80.66.10.in-addr.arpa.  
$TTL    86400  
@       IN      SOA    rtg.fralug-net. root.rtg.fralug-net. (  
        2025020701 ; Serial  
        3600       ; Refresh (60 Min = 3600s)  
        600        ; Retry   (10 Min = 600s)  
        3600000    ; Expire  (1000h = 3600000s)  
        3600       ; neg. cache TTL(60 Min = 3600s)  
        )  
        NS       dns.fralug-net.  
254     PTR      rtg.fralug-net.  
251     PTR      mail.fralug-net.  
250     PTR      dns.fralug-net.  
249     PTR      dhcp.fralug-net.
```



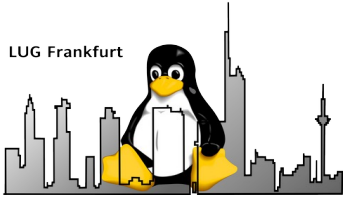
fralug-dns-3

- `/etc/resolv.conf`
`search fralug-net`
`nameserver 10.66.80.250`
- File-Rechte anpassen
`chown bind:bind /etc/bind/fralug-net*`
`chmod 775 /etc/bind`
- `aptitude purge isc-dhcp-client isc-dhcp-common`



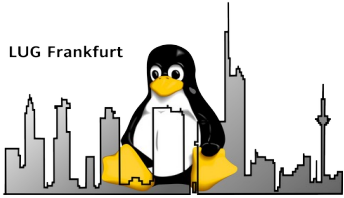
Inhalt

- Motivation und Konzept für router+DNS+DHCP
- Basis-Infos DNS
- Virtuelle Maschine clonen
- Installation / Konfiguration DNS
- **Test DNS**
- Ausblick auf DDNS und DHCP



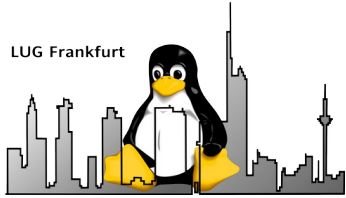
Test DNS (lokal)

- Tests direkt auf fralug-dns
`named-checkconf -l`
`named-checkconf -z`
- `cd /etc/bind`
`named-checkzone fralug-net fralug-net`
`zone 80.66.10.in-addr.arpa/IN: loaded serial 2025020701`
`OK`
`named-checkzone 80.66.10.in-addr-arpa fralug-net.rev`
`zone fralug-net/IN: loaded serial 2025020701`
`OK`
- `host -v <Station>; host -v <IP-Adresse>`
- `grep named /var/log/syslog`



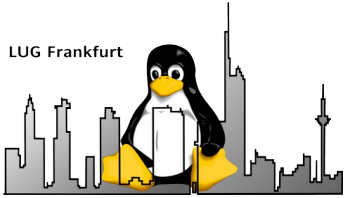
Test mit fralug-local

- Mit fester IP-Adresse (10.66.80.10)
- `/etc/resolv.conf`
search fralug-net
nameserver 10.66.80.250
- ping dns; ping rtg; ping www.heise.de
- ping <station>.<hausnetz>



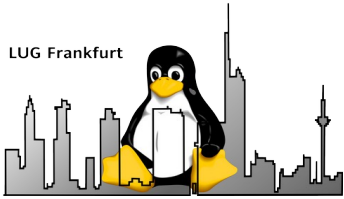
Inhalt

- Motivation und Konzept für router+DNS+DHCP
- Basis-Infos DNS
- Virtuelle Maschine clonen
- Installation / Konfiguration DNS
- Test DNS
- Ausblick auf DDNS und DHCP



Ausblick

- Eigene virtuelle Maschine mit DHCP-Server (fralug-dhcp)
- DDNS + DHCP (isc-dhcp-server)
- Literatur
 - <https://bind9.readthedocs.io> (Referenz für bind9)
 - <https://zytrax.com/books/dns/>



Ende

**Danke für's zuhören und
viel Spaß mit Debian**

Fragen und Anmerkungen gerne an m1ist@hk-vision.de