

15 Domain Name-Server einrichten

IP-Adressen identifizieren Rechner im Internet eindeutig. Diese Art der Adressierung ist für Maschinen ganz praktisch, aber nicht für Menschen. Diesen kommt das hierarchische System von Domain-Namen in der Form `www.linuxbu.ch` oder allgemeiner `Host.Server.Domain.TopLevelDomain` entgegen.

Mehr zum Aufbau von Domain-Namen finden Sie in Internet-Büchern wie *Linux Wegweiser für Netzwerker* von Olaf Kirch und im Internet bei jedem NIC (s.u.).

Ruft jemand eine Webseite des Servers `www.linuxbu.ch` auf, so muss der Browser die IP-Nummer von `www.linuxbu.ch` herausfinden. Diese Aufgabe überlässt er dem Domain Name Service (DNS).

Jedes Programm, das einen Host-Namen mitgeteilt bekommt, versucht sofort, ihn in eine IP-Adresse aufzulösen. Dazu benutzen Internet-Clients folgendes Verfahren:

Zuerst suchen sie eine Datei `hosts`, bei Windows 9x im Windows-Verzeichnis (meist `c:\windows`), bei Windows NT unter `winnt\system32\drivers\etc`, bei Linux im Verzeichnis `/etc`. Zunächst prüfen Sie, ob dort zu dem Domain-Namen eine IP-Adresse steht. Wenn nicht, nehmen sie mit dem DNS-Server Kontakt auf, den sie im lokalen Netz finden oder den ihnen der Provider zur Verfügung stellt.

Host-Dateien auf Clients lokal zu pflegen, ist sehr aufwändig. Daher nimmt man gern die Dienste von DNS-Servern in Anspruch.

15.1 Wann Sie einen eigenen Name-Server brauchen

Eigene Name-Server sollte man immer dann einrichten, wenn man ein lokales Netz an das Internet anbindet. Lokale Name-Server haben folgende Aufgaben:

- Verwalten der Namen für das lokale Netz (Hosting genannt),
- Weiterleiten der DNS-Anfragen an den DNS-Server des Providers (Caching).

15.2 So funktionieren das Domain Name System und Internet-Domains

Bis 1984 pflegte das Network Information Centre (NIC) diese Zuordnung in Form einer großen Tabelle. Als diese Liste zu groß wurde, hat die Netzgemeinde den hierarchischen Domain Name Service eingeführt. Zur Zeit gibt es zwei Arten von Top-Level-Domains, die nationalen, die mit zwei Buchstaben das Land identifizieren und die ursprünglichen, die jeweils aus drei Buchstaben bestehen.

Die beiden Arten von Top-Level-Domains werden verschieden verwaltet: nationale NICs – Network Information Centers (www.nic.de, www.nic.at, www.nic.ch, www.nic.li) – verwalten die Landesdomains wie **de** (Deutschland), **at** (Österreich), **ch** (Schweiz) und **li** (Liechtenstein).

Die Drei-Buchstaben-Domains aus der Anfangszeit des Internet (**com**, **edu**, **gov**, **mil**, **net**, **org**, **int**) werden inzwischen von zahlreichen konkurrierenden Firmen verwaltet. Hier kommt es immer häufiger zu Pannen wie Doppelvergabe.

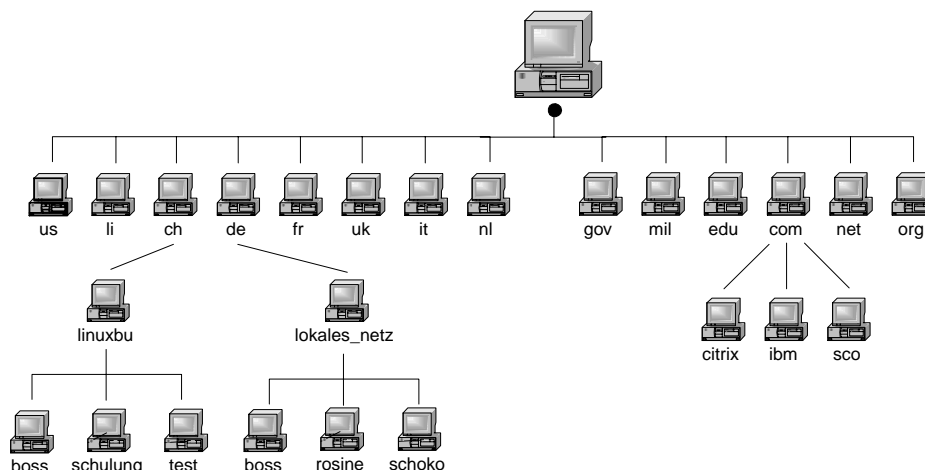


Abbildung 15.1: Baumstruktur

Der Ablauf einer Namens-Anfrage ist folgendermaßen:

- Ruft jemand in den USA die Web-Adresse `www.linuxbu.ch` auf, so landet dessen Name-Server-Anfrage über Zwischenschritte beim zentralen Name-Server des NIC.
- Der gibt die Anfrage an den Name-Server des Ch-NIC, der Sie dann an den für `linuxbu.ch` zuständigen Name-Server (`nameserv.deltaweb.de`) weitergibt,
- von wo er nun endgültig die IP-Adresse (`195.37.188.187`) bekommt.
- Diese IP-Adresse wird dann an den anfragenden Rechner übermittelt.

Da sich die meisten Name-Server Adressen in einem Cache merken, nehmen Anfragen nur selten diesen langen Weg. Dieser Cache hat aber auch den Nachteil, dass es ein paar Tage dauern kann, bis der letzte Name-Server einen neuen Eintrag oder eine Änderung mitbekommen hat.

Zusätzlich zu diesen Anfragen, bei denen zu einem Namen eine IP-Adresse ermittelt wird, muss ein Name-Server auch Anfragen beantworten können, bei denen zu einer IP-Adresse ein Name ermittelt wird (Reverse Lookup).

15.2.1 Die Hosts-Datei

In kleineren Netzen ist ein eigener Name-Server nicht notwendig. Hier kann man die vorhandenen Rechner einfach in die Hosts-Datei eines jeden Rechners eintragen. Das Format dieser Datei ist für Linux und Windows identisch.

```
/etc/hosts
#
# hosts          This file describes a number of hostname-to-
address
#               mappings for the TCP/IP subsystem.  It is
mostly
#               used at boot time, when no name servers are
running.
#               On small systems, this file can be used
instead of a
#               "named" name server.
# Syntax:
#
# IP-Address    Full-Qualified-Hostname  Short-Hostname
#
127.0.0.1      localhost

# special IPv6 addresses
::1           localhost ipv6-localhost ipv6-loopback

fe00::0       ipv6-localnet

ff00::0       ipv6-mcastprefix
ff02::1       ipv6-allnodes
```

```
ff02::2      ipv6-allrouters
ff02::3      ipv6-allhosts

192.168.1.2  boss.lokales-netz.de  boss
```

Zumindest die beiden hervorgehobenen Zeilen, die den lokalen Rechner beschreiben, müssen sich immer in der Hosts-Datei finden. Einen großer Teil der Datei können Sie ignorieren, er wird erst bei der Erweiterung des IP-Adressformates auf 6Byte bedeutsam.

15.2.2 Name-Server installieren und konfigurieren

Der Name-Server befindet sich bei SuSE im Paket `bind8` der Serie `n` bzw. der Datei `bind8.rpm` im Verzeichnis `n1`. Standardmäßig wird das Paket nicht mit installiert, man muss die Installation also gegebenenfalls nachholen, bevor man den DNS konfiguriert.

Folgende Dateien sind für die Konfiguration wichtig:

<i>Datei</i>	<i>Bedeutung</i>
<code>/usr/sbin/named</code>	Die Binärdatei, die den Name-Server bildet.
<code>/etc/hosts</code>	Liste mit IP-Adressen und zugehörigen Rechnernamen.
<code>/etc/host.conf</code>	Bestimmt die Art der Namensauflösung.
<code>/etc/resolv.conf</code>	Konfiguration für den Name Resolver (Namensauflöser).
<code>/etc/named.conf</code>	Hauptkonfigurationsdatei.
<code>/var/named/root.hint</code>	Datei mit den Root-Name-Servern.
<code>/var/named/privat.zone</code>	Datei für die Namenszuordnung im lokalen Netz.
<code>/var/named/localhost.zone</code>	Namenszuordnung für localhost im lokalen Netz.
<code>/var/named/tavirp.zone</code>	Umgekehrte Zuordnung IP \leftrightarrow Name.
<code>/var/named/tsohlaicol.zone</code>	Umgekehrte Zuordnung 127.0.0.1 localhost.

Tabelle 15.1: Konfigurationsdateien des Name-Servers

Hinweis: Sie können den Name-Server erst starten, wenn sie alle Konfigurationsdateien angelegt haben.

Damit der Rechner später auch auf den Name-Server zugreifen kann, sollte man zuerst YaST starten und dort unter

Administration des Systems • Netzwerk konfigurieren • Konfiguration Name-Server

die notwendigen Angaben machen. Im ersten Fenster muss man auswählen, dass man auf einen Name-Server zugreifen möchte (*Ja*), im zweiten Fenster gibt man die IP-Adresse (192.168.1.2) bzw. die IP-Adressen für den oder die Name-Server, sowie den Domainnamen (lokales-netz.de) an

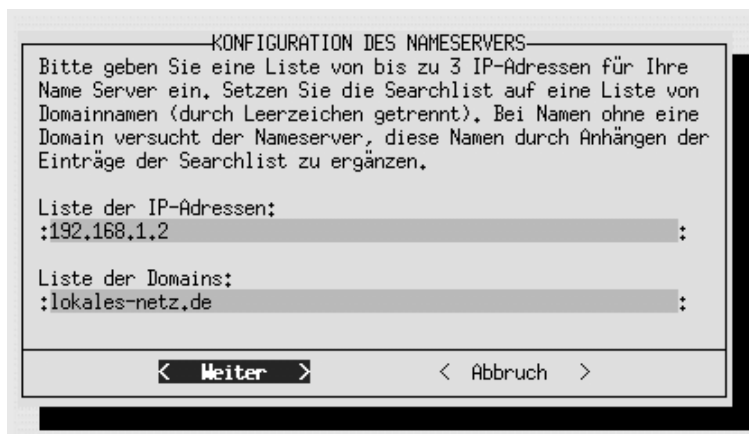


Abbildung 15.2: Konfiguration des Name-Servers

YaST erzeugt bzw. verändert dann die Dateien `/etc/host.conf` und `/etc/resolv.conf`.

`/etc/host.conf`

```
#
# /etc/host.conf - resolver configuration file
#
# Please read the manual page host.conf(5) for more
information.
#
#
# The following option is only used by binaries linked against
# libc4 or libc5. This line should be in sync with the "hosts"
# option in /etc/nsswitch.conf.
#
order hosts, bind
#
# The following options are used by the resolver library:
#
multi on
```

Dies legt fest, wie Namen aufgelöst werden. Zuerst wird in der Datei `/etc/hosts` nachgesehen. Falls sich die gesuchte Adresse dort nicht findet, wird der Name-Server `bind` befragt. Der Eintrag `multi on` bewirkt, dass zu einem Rechnernamen in der `/etc/hosts` mehrere IP-Adressen angegeben werden dürfen.

```
/etc/resolv.conf
```

```
#
# /etc/resolv.conf
#
# Automatically generated by SuSEconfig on
# Mon Mar  6 17:58:19 CET 2000.
#
# PLEASE DO NOT EDIT THIS FILE!
#
# Change variables (NAMESERVER + SEARCHLIST)
# in /etc/rc.config instead.
#
#
search lokales-netz.de
nameserver 192.168.1.2
```

Die beiden Zeilen in dieser Datei bewirken, dass für die Suche nach Rechnern der Domain `lokales-netz.de` der Name-Server `192.168.1.2` befragt wird.

Der DNS-Server wertet beim Start die Konfigurationsdatei `named.conf` aus. Sie enthält die Pfade und Namen aller weiteren Konfigurationsdateien und muss mit einem Texteditor angelegt werden.

Die hier vorgestellte Beispielkonfiguration ist möglichst einfach und übersichtlich gehalten. Die von SuSE installierten Musterdateien sind wesentlich umfangreicher, aber für unsere Zwecke nicht notwendig. Eine umfangreiche Dokumentation zum Name-Server *Bind* findet sich im Ordner `/usr/share/doc/packages/bind8`.

```
/etc/named.conf
```

```
// BIND8-Konfigurationsdatei
// Vereinfachte Version fuer Linuxbu.ch

options {
    directory "/var/named";
    allow-query { 127.0/16; 192.168.1/24; };
    forwarders { 194.25.2.129; };
```

```

};

zone "lokales-netz.de" in {
    type master;
    file "privat.zone";
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "1.168.192.in-addr.arpa" in {
    type master;
    file "tavirp.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "tsohlacol.zone";
};

zone "." in {
    type hint;
    file "root.hint";
};

```

Zu den einzelnen Abschnitten dieser Datei:

```
// BIND8-Konfigurationsdatei
```

Zeilen, die mit zwei Schrägstrichen beginnen sind Kommentare. Hier wird betont, dass es sich um eine Konfigurationsdatei für das aktuelle Bind8 und nicht das ältere Bind4 handelt.

```

options {
    directory "/var/named";
    allow-query { 127.0/16; 192.168.1/24; };
    forwarders { 212.185.253.70; };
};

```

Im Options-Statement wird zuerst der Pfad zu den weiteren Konfigurationsdateien angegeben. In der zweiten Zeile folgt dann eine Angabe, von wo aus auf den Name-Server zugegriffen werden darf. Hier wird ein Zugriff nur aus dem lokalen Netz heraus zugelassen. Anfragen, die der Name-Server nicht beantworten kann,

werden an den oder die Name-Server weitergegeben, die im `forwarders`-Statement aufgeführt sind. Als `forwarders` sollten Sie hier die Name-Server Ihres Providers eintragen.

```
zone "lokales-netz.de" in {
    type master;
    file "privat.zone";
};
```

Mit dem Zone-Statement bekommt der Name-Server die Zuständigkeit für `lokales-netz.de`. Er ist primärer Name-Server (`master`) für diese Domain und die eigentlichen Adressen finden sich in der Datei `/var/named/privat.zone` (`s.u.`).

```
zone "localhost" in {
    type master;
    file "localhost.zone";
};
```

Dieses Zone-Statement ist notwendig, damit wir auch den Namen `localhost` zu `127.0.0.1` auflösen können, der nichts mit `lokales-netz.de` zu tun hat.

```
zone "1.168.192.in-addr.arpa" in {
    type master;
    file "tavirp.zone";
};
```

Im vorliegenden Beispiel hat `boss.lokales-netz.de` die IP-Adresse `192.168.1.2`, diese Zuordnung ergibt sich aus der Zonendatei `privat.zone`. Für die Rückwärtsauflösung von `192.168.1.2` zu `boss.lokales-netz.de` ist diese Datei zuständig. Die Rückwärtsauflösung soll auch mit dem `tavirp` (*privat* rückwärts gelesen) angedeutet werden.

```
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "tsohlaacol.zone";
};
```

Für die Rückwärtsauflösung `127.0.0.1` zu `localhost` ist wieder eine eigene Zonendatei notwendig. Der Name `tsohlaacol` ergibt sich wenn man *localhost* rückwärts liest.

```
zone "." in {
    type hint;
    file "root.hint";
};
```


Diese Zonendatei enthält die IP-Adressen der Root-Name-Server. Eine Änderung ist normalerweise nicht notwendig.

15.2.3 DNS-Zonen konfigurieren

Wichtigster Inhalt der Zonendateien (Master Files) sind die Ressource Records, die die eigentliche Zuordnung zwischen Namen und IP-Adresse vornehmen. Die Dateien haben folgende Grundstruktur:

Sie beginnen mit Direktiven, die jeweils mit dem `$`-Zeichen anfangen:

Mit `$ORIGIN` wird festgelegt, welche Domain an unvollständige Adressangaben angehängt werden soll. Fehlt diese Angabe, so wird der Zonenname aus der `/etc/named.conf` benutzt. In den folgenden Beispielen findet sich diese Direktive daher nicht.

`$TTL` (Time To Live) gibt eine Standard-Gültigkeitsdauer für die Ressource Records vor, hier ein Tag (1D).

`$GENERATE` ist eine nicht standardisierte Direktive, die für Bind8 spezifisch ist. Hiermit lassen sich viele gleichartige Ressource Records erzeugen. Eine genauere Beschreibung findet sich im Beispiel `privat.zone`.

Alle weiteren Zeilen sind dann Ressource Records, sie haben folgenden Aufbau:

```
<Name> IN <Typ> <Beschreibung>
```

Der erste Record ist am aufwendigsten, er ist vom Typ `SOA` (Start Of Authority) und beinhaltet Grundeinstellungen für die Zone. Dazu gehören die Angabe des Name-Servers und der E-Mail-Adresse der Kontaktperson. Bei dieser Mail-Adresse ersetzt man das `@`-Zeichen durch einen Punkt.

Danach kommen in Klammern eine Seriennummer und Zeitangaben für das Caching. Die Zeitangaben können einfach übernommen werden, `3H` steht für 3 Stunden, `15M` für 15 Minuten, `1W` für eine Woche und `1D` für einen Tag.

Hat man auch sekundäre Name-Server im Netz, so muss man die Seriennummer bei jeder Änderung erhöhen, damit die anderen Server Änderungen übernehmen. Baut das Nummernsystem auf dem Kalenderdatum auf, sollte man stets eine mehrstellige Nummer anfügen, z.B. `2000031203`, für die dritte Version vom 12. März 2000.

Nun folgen einige Adressangaben. Vollständige DNS-Namen bekommen noch einen Punkt dahinter, alle Namen ohne Punkt am Ende bekommen den betreffenden Domainnamen angehängt.

Für die Datei `privat.zone` ist es also gleichbedeutend, ob man `boss.lokales-netz.de.` (beachten Sie den Punkt am Ende) oder `boss` (kein Punkt am Ende) schreibt.

Die meisten Records sind vom Typ A und dienen der Adresszuordnung. Vor dem IN steht der Name des Rechners und nach dem A seine IP-Adresse.

Ein Record vom Typ CNAME vergibt einen weiteren Namen (Alias) für einen Rechner. Meist werden so `www`, `ftp`, `mail` und `news` definiert. Links von IN steht wieder der zu definierende Name und rechts vom CNAME der offizielle Name.

Über einen Record vom Typ NS werden Name-Server definiert. Ein Netz mit ständiger Internetverbindung muss zwei Name-Server besitzen, für den Fall, dass einer davon einmal ausfällt.

Für den Mailaustausch wichtig sind die MX-Records (Mail-Exchange). Hier wird nach dem Schlüsselwort MX noch eine Priorität für den Rechner angegeben. Das dient dazu, eine Rangfolge festzulegen, wenn mehrere Mailserver eingetragen sind. Je kleiner die Zahl, desto höher die Priorität, Null entspricht also der höchsten Priorität. Man kann z.B. 10 weitere Rechner mit niedrigerer Priorität angeben, die notfalls eingehende Mails annehmen, falls der primäre Rechner ausfällt.

`/var/named/privat.zone`

```
$TTL      1D
$GENERATE 20-127 client-$ A 192.168.1.$
@ IN SOA  boss.lokales-netz.de. postmaster.lokales-netz.de. (
                                2000031203 ; serial (12.03.2000 Version
03)
                                3H      ; refresh
                                15M     ; retry
                                1W      ; expiry
                                1D )    ; minimum

                                IN NS   boss
                                IN MX  0      boss

boss      IN A      192.168.1.2
www       IN CNAME  boss
www2      IN CNAME  boss
mail      IN CNAME  boss
ns        IN CNAME  boss
ftp       IN CNAME  boss
```

```
news      IN CNAME    boss
;
rosine   IN A        192.168.1.10
nuss     IN A        192.168.1.11
flocke  IN A        192.168.1.12
schoko   IN A        192.168.1.13
```

Boss ist Name-Server und Mail-Server mit höchster Priorität für die Domain lokales-netz.de. Weiter werden für boss, rosine, nuss, flocke und schoko noch die IP-Adressen festgelegt.

Mit einem Record vom Typ A kann man für beliebig viele Rechner die IP-Adressen angeben.

Manche Betreiber geben sich bei den Rechnernamen sehr viel Mühe und überlegen sich ein System. Namen von Bäumen (Bonsai, Erle, ...), Planeten (Mars, Venus, ...) oder Müsli-Bestandteilen (Boss, Rosine, Nuss, ...).

Das ist zwar nett, praktischer ist es aber die Namen einfach systematisch aufzubauen, dann kann man die Datei von einem Konfigurations-Programm erzeugen lassen und gleich für alle 255 möglichen IP-Adressen einen Namen generieren lassen, z.B. nach dem System

```
client-20 IN A        192.168.1.20
client-21 IN A        192.168.1.21
client-22 IN A        192.168.1.22
...
client-127 IN A       192.168.1.127
```

Geht man so vor, dann braucht man bei späteren Erweiterungen des Netzes am Name-Server nichts mehr zu ändern. Genau diese Zeilen erzeugt die \$GENERATE Direktive.

```
$GENERATE 20-127 client-$ A 192.168.1.$
```

Für die Werte von 20 bis 127 (die Werte sind willkürlich gewählt) werden Ressourcen Records erzeugt, die nach dem Muster

```
client-$ IN A        192.168.1.$
```

aufgebaut sind, wobei das \$-Zeichen jeweils durch den aktuellen Wert ersetzt wird.

Als Alias für Boss sind www, mail, ns, ftp und news eingetragen. In einem lokalen Netz ist das praktisch. Für Rechner, die ständig mit dem Internet verbunden sind, gilt aber:

Warnung: Wenn Rechnernamen über Rechner-Funktionen informieren, freuen sich Eindringlinge. Es kann hilfreich sein, unverfängliche Namen zu vergeben.

Viele Programme adressieren den Rechner auf dem sie laufen über `localhost` und nicht über `boss.lokales-netz.de`, es gibt für `localhost` aber auch `127.0.0.1` als allgemeingültige IP-Adresse.

Die Zuordnung von `localhost` zu `127.0.0.1` erfolgt in einer eigenen Zonendatei.

Diese Datei hat den gleichen Aufbau wie die `privat.zone`, definiert aber nur den einzigen Namen `localhost` mit der zugehörigen IP `127.0.0.1`.

`/var/named/localhost.zone`

```
$TTL 1D
@ IN SOA boss.lokales-netz.de. postmaster.lokales-netz.de. (
    2000031203 ; serial (12.03.2000 Version 03)
    3H        ; refresh
    15M       ; retry
    1W        ; expiry
    1D )      ; minimum

    IN NS     boss.lokales-netz.de.
localhost.  IN A     127.0.0.1
```

15.2.4 Von der IP-Nummer zum Hostnamen: Reverse Name Server Lookup

Die bisher beschriebenen Dateien `privat.zone` und `localhost.zone` dienen dazu einem Rechnernamen eine IP-Adresse zuzuordnen. Manchmal ist es aber auch notwendig zu einer IP-Adresse den Rechnernamen zu ermitteln, dies bezeichnet man als Reverse Lookup.

Auch diese Namensauflösung erfolgt über Zonendateien, es kommt nur der neue Record-Typ PTR (Pointer) zur Anwendung.

Für das Reverse Lookup wurde eine spezielle Domain eingerichtet, `in-addr.arpa`, die IP-Adressen werden in verdrehter Reihenfolge davor gesetzt. Für die Suche nach dem Namen zu `192.168.1.2` geht man mit `2.1.168.192.in-addr.arpa` an eine geeignete Zonendatei und sucht dort den zugehörigen Namen.

```
/var/named/tavirp.zone
```

```
$TTL 1D
$GENERATE 20-127 $ PTR client-$.lokales-netz.de.
@ IN SOA boss.lokales-netz.de. postmaster.lokales-netz.de. (
    2000031203 ; serial (12.03.2000 Version 03)
    3H        ; refresh
    15M       ; retry
    1W        ; expiry
    1D )      ; minimum

    IN NS     boss.lokales-netz.de.

2       IN PTR boss.lokales-netz.de.
10      IN PTR rosine.lokales-netz.de.
11      IN PTR nuss.lokales-netz.de.
12      IN PTR flocke.lokales-netz.de.
13      IN PTR schoko.lokales-netz.de.
```

Als Name wird hier nur jeweils die letzte Zahl der IP-Adresse angegeben, da 1.168.192.in-addr.arpa ergänzt wird.

Auch in dieser Datei wird ein großer Teil der Ressource Records wieder mit der \$GENERATE Direktive erzeugt.

Für die Zuordnung 127.0.0.1 zu localhost wird eine eigene Pseudo-Adresse 1.0.0.127.in-addr.arpa benutzt und damit auch eine eigene Zonen-datei.

```
/var/named/tsohla101.zone
```

```
$TTL 1D
@ IN SOA boss.lokales-netz.de. postmaster.lokales-netz.de. (
    2000031203 ; serial (12.03.2000 Version 03)
    3H        ; refresh
    15M       ; retry
    1W        ; expiry
    1D )      ; minimum

    IN NS     boss.lokales-netz.de.
1       IN PTR localhost.
```

15.3 Erster Start des Name-Servers

Nach dem Start des Name-Servers mit

```
/sbin/init.d/named start
```

finden Sie in der Datei `/var/log/messages` Meldungen wie:

```
Nov 20 14:41:08 boss named[907]: starting.  named 8.2.3-T5B
↳ Wed Sep 20 18:10:28
Nov 20 14:41:09 boss named[907]: master zone "lokales-netz.de"
↳ (IN) loaded (serial 2000031203)
Nov 20 14:41:09 boss named[907]: master zone "localhost" (IN)
↳ loaded (serial 2000031203)
Nov 20 14:41:09 boss named[907]: master zone
↳ "1.168.192.in-addr.arpa" (IN) loaded (serial 2000031203)
Nov 20 14:41:09 boss named[907]: master zone
↳ "0.0.127.in-addr.arpa" (IN) loaded (serial 2000031203)
Nov 20 14:41:09 boss named[907]: hint zone "" (IN) loaded
↳ (serial 0)
Nov 20 14:41:09 boss named[907]: listening on [127.0.0.1].53
↳ (lo)
Nov 20 14:41:09 boss named[907]: listening on
↳ [192.168.0.99].53 (ipp0)
Nov 20 14:41:09 boss named[907]: listening on [192.168.1.2].53
↳ (eth0)
Nov 20 14:41:09 boss named[907]: Forwarding source address is
↳ [0.0.0.0].1026
Nov 20 14:41:09 boss named[908]: group = named
Nov 20 14:41:09 boss named[908]: user = named
Nov 20 14:41:09 boss named[908]: Ready to answer queries.
Nov 20 14:41:09 boss named[908]: sysquery:
↳ sendto([194.25.2.129].53): Das Netzwerk ist nicht
↳ erreichbar
```

- Die erste Zeile ist eine allgemeine Start-Meldung des Name-Servers, aus der sich vor allem die Versionsnummer, hier 8.2.3, ergibt.
- Die folgenden fünf Zeilen zeigen das Laden der Zonendateien an, unsere vier Dateien und die Hint-Datei mit den Root-Name-Servern.
- Danach werden dann die IP-Adressen angezeigt, auf die der Name-Server anspricht, 192.168.1.2 und 127.0.0.1 sowie jeweils Port 53.
- Änderungen müssen keinem anderen Name-Server mitgeteilt werden, daher ist 0.0.0.0 die Adresse für Forwarding.
- Besonders wichtig ist die vorletzte Zeile, hier wird angezeigt, dass der Name-Server sich in der Lage sieht, Anfragen zu beantworten.

- Die Fehlermeldung in der letzten Zeile zeigt, dass die Name-Server der höheren Ebene nicht erreichbar sind, weil die Wählverbindung nicht aufgebaut ist.

15.3.1 Test und Diagnose

Wenn der Name-Server erfolgreich gestartet wurde (Ready to answer queries) kann man mit `nslookup` Anfragen auf dem Linux-Server testen, ob er

- lokale Anfragen und
- weltweite Anfragen

richtig beantwortet.

Zum Testen geht man systematisch Beispiele durch, die alle Zonendateien benötigen.

Zuerst `privat.zone`:

```
nslookup www
```

sollte folgende Antworten ergeben:

```
Server:  boss.lokales-netz.de
Address: 192.168.1.2

Name:    boss.lokales-netz.de
Address: 192.168.1.2
Aliases: www.lokales-netz.de
```

NSLookup nennt in den ersten beiden Zeilen, welcher Name-Server benutzt wurde, hier der eigene. Die letzten drei Zeilen beziehen sich auf die Anfrage. NSLookup antwortet mit dem Namen des Rechners, seiner IP, sowie dem vollständigen Alias.

Als Zweites testen wir `localhost.zone`:

```
nslookup localhost
```

muss ergeben:

```
Server:  boss.lokales-netz.de
Address: 192.168.1.2

Name:    localhost
Address: 127.0.0.1
```

370 Kapitel 15: Domain Name-Server einrichten

Dann die Auflösung gemäß `tavirp.zone`:

```
nslookup 192.168.1.12
```

wird aufgelöst zu:

```
Server:  boss.lokales-netz.de
Address: 192.168.1.2

Name:    flocke.lokales-netz.de
Address: 192.168.1.12
```

Zum Abschluss dann noch `tsohlaicol.zone`:

```
nslookup 127.0.0.1
```

wird aufgelöst zu

```
Server:  boss.lokales-netz.de
Address: 192.168.1.2

Name:    localhost
Address: 127.0.0.1
```

Wenn die bisherigen Tests erfolgreich verlaufen sind und eine Verbindung ins Internet besteht, sollte man auch externe Adressen abfragen können:

```
nslookup ns.suse.de
```

Hier such `nslookup` den Name-Server von SuSE. Als Antwort erhält man

```
Server:  boss.lokales-netz.de
Address: 192.168.1.2

Non-authoritative answer:
Name:    ns.suse.de
Address: 194.112.123.193
```

Die Zeile *Non-authoritative Answer* weist darauf hin, dass der hier getestete Name-Server für diese Adresse nicht zuständig ist, sich aber eine Auskunft besorgt hat.

Mit

```
nslookup www.suse.de ns.suse.de
```

kann man direkt den SuSE-Name-Server abfragen:


```
Server: Cantor.suse.de
Address: 194.112.123.193

Name: Turing.suse.de
Address: 194.112.123.200
Aliases: www.suse.de
```

Die Antwort ist nun natürlich authoritative, da der befragte Name-Server für diesen Bereich zuständig ist.

Wenn alle Tests erfolgreich verlaufen sind, muss man nur noch veranlassen, dass der Name-Server zukünftig beim Hochfahren des Systems automatisch startet. Dazu geht man in YaST unter *Administration des Systems • Konfigurationsdatei verändern*, sucht in der Liste den Schalter

```
START_NAMED
```

und setzt den Wert von *no* auf *yes*.

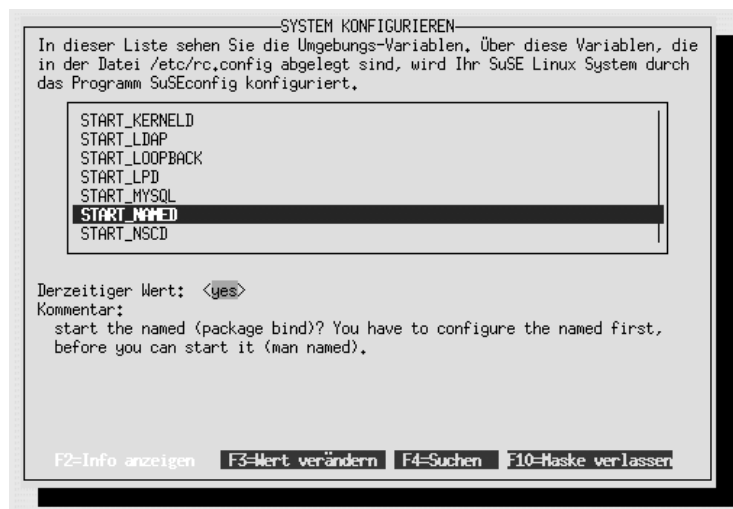


Abbildung 15.3: START_NAMED=yes

15.3.2 Troubleshooting

Die Konfiguration des Name-Servers ist eine der wenigen Konfigurationen, bei denen SuSE bzw. YaST wenig helfen können.

Sollte der Name-Server nicht richtig starten, so gibt er seine Fehlermeldungen in der Datei `/var/log/messages` aus.

Syntaxfehler in der Datei `/etc/named.conf` gibt Bind dort mit der zugehörigen Zeilennummer an. Diese Fehler führen meist dazu, dass der Name-Server überhaupt nicht gestartet wird.

Fehler in einer der Zonendateien werden ebenfalls vermerkt und führen zu einer Teilfunktion des Name-Servers. Es müssen alle Anfragen der Art:

```
nslookup boss
nslookup 192.168.1.2
nslookup localhost
nslookup 127.0.0.1
```

erfolgreich aufgelöst werden. Sollten einzelne dieser Anfragen fehlschlagen, so ist die zugehörige Zonendatei fehlerhaft.

Bei fehlerhaften Zonendateien spielt oft der abschließende Punkt eine Rolle. Immer dann, wenn nichts mehr ergänzt werden darf, weil eine vollständige Adresse vorliegt, muss am Ende ein Punkt stehen. Bei unvollständigen Angaben, die noch ergänzt werden sollen, darf am Ende kein Punkt stehen.