Linux Netzwerk Grundlagen

TCP, UDP, IP, BGP
. . . und Spaß dabei

Sebastian „tokkee“ Harl
<tokkee@lusc.de>

Schwabacher Linux Tag 2011
01. Oktober 2011

Netzwerken unter Linux

facebook

XING openBC

VZ

Hintergrundwissen

- IP-Adressen, Netzwerkmasken, CIDR
- Routing
- Default Gatway
- Protokolle: TCP, UDP, IP, ICMP, BGP

IPv6

- „next-generation“ des Internet-Protokolls (seit 1996)
- seit Februar 2011 „kein IPv4 mehr“
- 340282366920938463463374607431768211456 Adressen
- Beispiel: `2001:67c:14c:12f::5:1`

Konfiguration mit `ip`

- `ip`
- Standardbefehl zur Konfiguration der Netzwerk-Schicht (Nachfolger von `ifconfig`, `route` und Konsorten)
- Wichtigste Kommando-Gruppen:
  - `addr`
  - `link`
  - `route`
- Dokumentation in der `ip(8)` Manpage

`ip`: Beispiele

- `ip addr show` – Anzeige der IP-Adresskonfiguration
- `ip route show` – Anzeige der Routing-Tabelle
- `ip add add 10.1.2.3/24 dev eth0` – Konfiguration der Adresse `10.1.2.3/24` auf der Schnittstelle `eth0`
- `ip link set eth0 promisc on` – „promiscuous“ Modus aktivieren (**gesamten** Netzwerkverkehr annehmen und zur Verarbeitung (z.B. Filter) an das Betriebssystem oder Userspace weitergeben)

Domain Name System

- Auflösung von „merkbaren“ Namen zu den Computer-verständlichen Adressen
- `/etc/resolv.conf`
- `host [-t TYP] NAME [NAMESERVER]`
- `whois [-h SERVER] OBJEKT`

Internet Control Message Protocol

- Rück- und Fehlermeldungen von Netzwerkgeräten
- am bekanntesten durch „pingen“
  (ECHO REQUEST / REPLY)
- `ping [-c ANZAHL] HOST`
- `traceroute` oder `mtr`

Netzwerk-Konfiguration

- `/etc/network/interfaces`, `/etc/sysconfig/network`
- `/etc/hostname`, `/etc/HOSTNAME`
- `/etc/hosts`

Netzwerk-Schnittstellen

- Persistente Namen
- /lib/udev/write_net_rules

```
SUBSYSTEM=='net', ACTION=='add', DRIVERS=='?*',
ATTR{address}=='5c:ff:35:08:e3:c8',
ATTR{dev_id}=='0x0', ATTR{type}=='1', KERNEL=='eth*',
NAME='eth0'
```

Netzwerk analysieren

- `ethtool IFACE`
- `netstat -tulpen`
- `nmap HOST`
- `tcpdump -i IFACE`
- `wireshark`

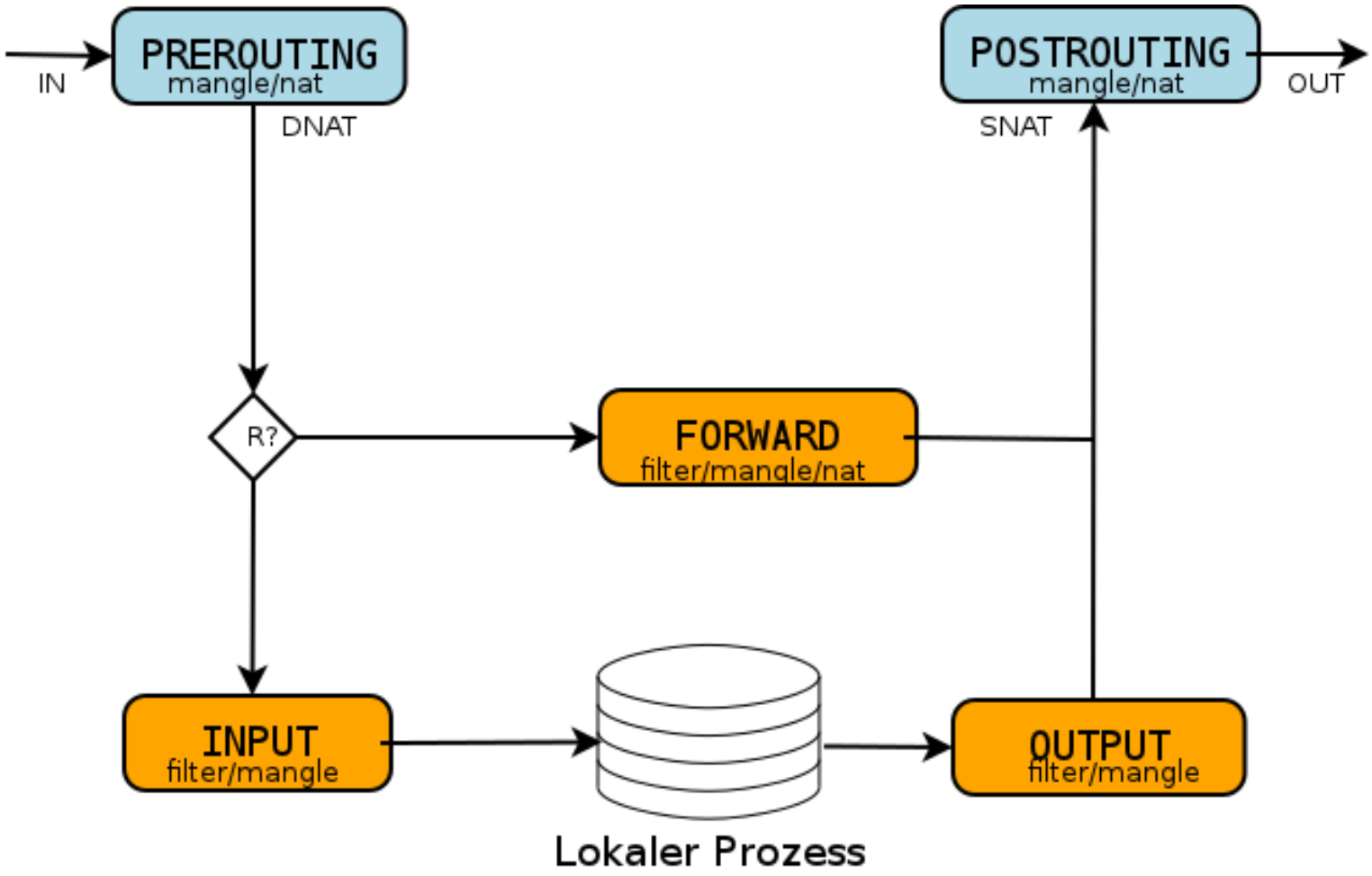
Beispiel: Gateway aufbauen

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -i IFACE -o IFACE \
    -j MASQUERADE
```

IPTables

- Paketfilter von Linux ab Version 2.4
- technisches Rückgrad einer Firewall
- durch Module sehr leicht erweiterbar
  - Connection Tracking
  - NAT
  - Paket Mangeling
  - Weiterleitung in den Userspace
  - u.v.m.

Netfilter Überblick



Firewall entwerfen

- Aufteilen des Traffics nach Quelle bzw. Ziel
  - Netzwerk-Interfaces
  - IP-Adressen/-Netze
- Matrix der möglichen Wege Von-Nach
- Matrix füllen mit Erlaubt, Verboten, Teilweise
- „Teilweise“-Bereiche genauer ansehen

Linux Netzwerk Grundlagen

Vielen Dank für die Aufmerksamkeit!

Gibt es Fragen?

Kontakt:
Sebastian „tokkee“ Harl
<tokkee@lusc.de>