SV3: Linux Server

Netzwerkkonfiguration

WBS TRAINING

UNSER ♥ SCHLÄGT FÜR BILDUNG

Agenda

Netzwerkkonfiguration

- Konfigurationsdateien
- Befehle zur Konfiguration
- Befehle zur Netzwerkadministration

Der NetworkManager

funktioniert nur, wenn das Programm die Kontrolle über die Voraussetzungen Schnittstellen hat. Alle gängigen Distributionen sollten eine entsprechende Konfiguration standardmäßig durchführen.

- Bei Debian stellen Sie sicher, dass **`/etc/network/interfaces`** nur Einstellungen für die Loopback-Schnittstelle enthält. Schnittstellen, die vom **`NetworkManager`** gesteuert werden sollen (typischerweise **`eth0`** und **`wlan0`**), dürfen nicht durch diese Datei konfiguriert werden!

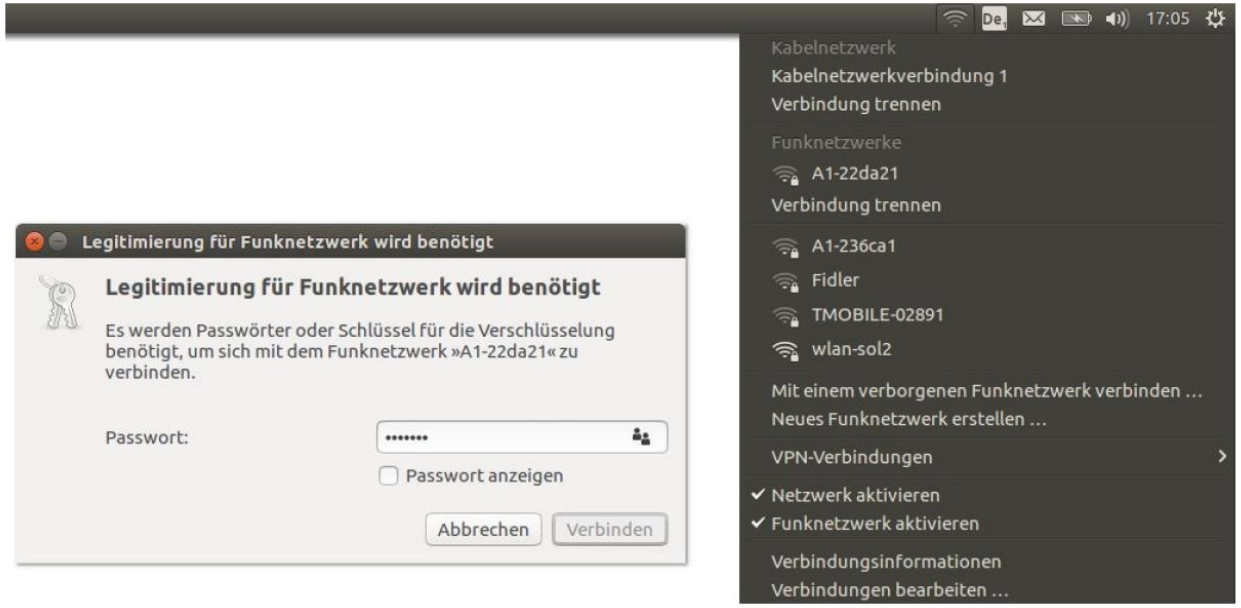
```
# The loopback network interface
auto lo
iface lo inet loopback
```

Netzwerkkonfiguration

Der NetworkManager

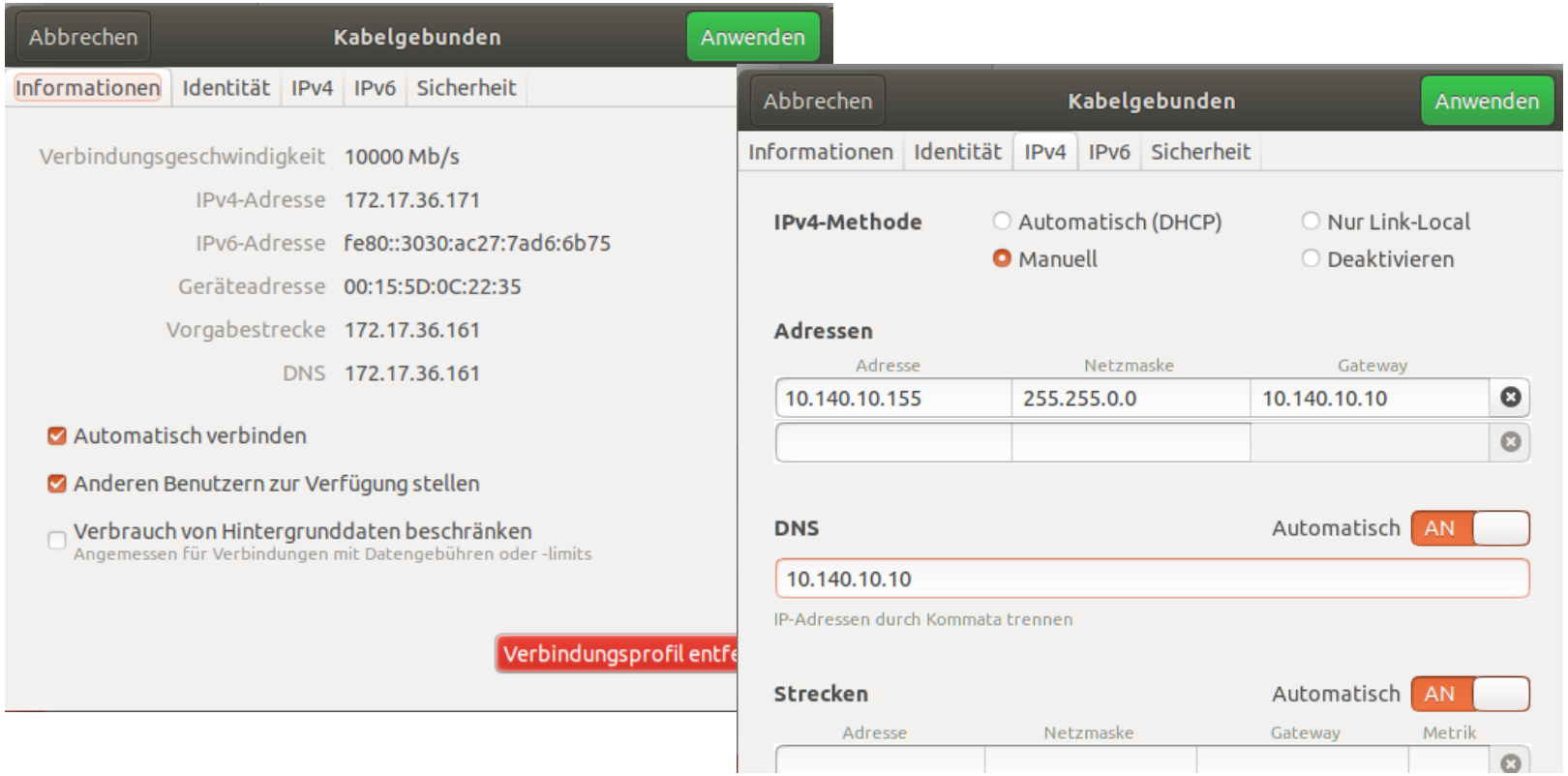
Bei den meisten gängigen Distributionen zeigt ein Icon in der Menüleiste oder im Panel den aktuellen Netzwerkzustand an.

- Dieses Icon führt in ein Menü, das die aktive Verbindung und alle erreichbaren bzw. vorkonfigurierten Netzwerke auflistet



Netzwerkkonfiguration

Der NetworkManager



Netzwerkkonfiguration

Netzwerkgrundlagen etwas Wiederholung..

Für den Großteil des Datenverkehrs in lokalen Netzen und im Internet ist das Protokoll TCP/IP verantwortlich. Dabei werden Netzwerkdaten in Form von relativ kleinen Paketen transportiert.

Abkürzung	Bedeutung	Funktion
IP	Internet Protocol	Verbindungsloses Protokoll, Basis für TCP und UDP
TCP	Transmission Controll Protocol	Ende zu Ende Verbindung zwischen 2 Geräten
UDP	User Datagram Protocol	Minimales, verbindungsloses Protokoll
ICMP	Internet Control Message Protocol	Austausch von IP-Status- und Fehlermeldungen
PPP	Point to Point Protocol	IP-Verbindungsaufbau über Wählleitungen. Z.b ADSL und UMTS.

Netzwerkkonfiguration

Netzwerkgrundlagen etwas Wiederholung..

IP-Adressen mögen für Computer praktisch sein, Menschen können sich IP-Adressen aber nur schwer merken. Aus diesem Grund werden Rechner im Netzwerk durch eine Kombination aus Host- und Domainnamen identifiziert.

- Benennung von Rechnern in lokalen Netzen
- Als Hostname sollte nicht der Name des Rechnerherstellers, des Besitzers oder des gerade anstehenden Projekts verwendet werden – all das kann Verwirrung stiften.
- Verwenden Sie kurze und einprägsame Namen.

Netzwerkkonfiguration

Manuelle LAN- und WLAN-Konfiguration

Netzwerkschnittstellen haben je nach Distribution unterschiedliche Namen. Bei einigen Distributionen sind noch die Schnittstellennamen eth0, eth1 etc. üblich, aber immer mehr Distributionen verwenden Device-Namen wie enp0s3 oder p5p1.

- Eine Liste aller auf Ihrem Rechner verfügbaren Netzwerkschnittstellen liefert das Kommando:

```
sb@ub:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 00:15:5d:0c:22:35 brd ff:ff:ff:ff:ff:ff
sb@ub:~$
```

Netzwerkkonfiguration

Manuelle LAN- und WLAN-Konfiguration

Falls die Schnittstelle deaktiviert ist können Sie diese wie folgt aktivieren:

```
sb@ub:~$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:15:5d:0c:22:35 brd ff:ff:ff:ff:ff:ff
sb@ub:~$
sb@ub:~$ sudo ip link set eth0 up
sb@ub:~$
sb@ub:~$ ip -c a | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    inet 172.17.36.171/28 brd 172.17.36.175 scope global dynamic noprefixroute eth0
sb@ub:~$
```

Manuelle LAN- und WLAN-Konfiguration

Nun können Sie mit ping überprüfen, ob Sie Kontakt zu anderen Rechnern im lokalen oder externen Netzwerk aufnehmen können.

```
sb@ub:~$ ping -c4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=13.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=13.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=13.4 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 13.044/13.510/13.923/0.352 ms
sb@ub:~$
```

Die Option **-c4** bewirkt, dass genau vier ping-Pakete versendet werden

Manuelle LAN- und WLAN-Konfiguration

Momentan können Pakete nur innerhalb des lokalen Netzwerks versandt werden. Damit auch ein Kontakt in das Internet möglich wird, muss der Rechner wissen, wohin er derartige Pakete leiten soll.

```
sb@ub:~$ ip route
default via 172.17.36.161 dev eth0 proto dhcp metric 100
169.254.0.0/16 dev eth0 scope link metric 1000
172.17.36.160/28 dev eth0 proto kernel scope link src 172.17.36.171 metric 100
sb@ub:~$ sudo ip route del default via 172.17.36.161
sb@ub:~$
sb@ub:~$ ip route
169.254.0.0/16 dev eth0 scope link metric 1000
172.17.36.160/28 dev eth0 proto kernel scope link src 172.17.36.171 metric 100
sb@ub:~$
sb@ub:~$ sudo ip route add default via 172.17.36.161
```

Sie müssen dazu die Adresse des Internet-Gateways Ihres Netzwerks mit ip route angeben.

Manuelle LAN- und WLAN-Konfiguration

IPv6-Konfiguration mit ip

```
sb@ub:~$ sudo ip -6 addr add 2a01:4d8:161:107::1/64 dev eth0
sb@ub:~$
sb@ub:~$ sudo ip -6 route add default via 2a01:4d8:161:107::100 dev eth0
sb@ub:~$
sb@ub:~$ ping6 -c4 google.de
PING google.de(fra16s45-in-x03.1e100.net (2a00:1450:4001:800::2003)) 56 data bytes
```

Netzwerkkonfiguration

DHCP-Informationen abrufen

Falls es im Netzwerk einen DHCP-Server gibt, können Sie diesen zur Konfiguration zu Hilfe nehmen. Nach der Aktivierung der Schnittstelle durch **ip link set enp4s0 up** führen Sie bei den meisten Distributionen das Kommando **dhclient** aus:

```
sb@ub:~$ sudo tail -f /var/log/syslog
Apr 17 13:37:07 ub systemd[1]: Started Network Manager Script Dispatcher Service.
Apr 17 13:37:07 ub nm-dispatcher: req:1 'dhcp4-change' [eth0]: new request (1 scripts)
Apr 17 13:37:07 ub nm-dispatcher: req:1 'dhcp4-change' [eth0]: start running ordered scripts...
Apr 17 13:37:07 ub dhclient[7830]: bound to 172.17.36.171 -- renewal in 279 seconds.
Apr 17 13:37:20 ub avahi-daemon[733]: Leaving mDNS multicast group on interface eth0.IPv6 with address fe80
::3030:ac27:7ad6:6b75.
Apr 17 13:37:20 ub avahi-daemon[733]: Joining mDNS multicast group on interface eth0.IPv6 with address 2a01
:4d8:161:107::2.
Apr 17 13:37:20 ub avahi-daemon[733]: Registering new address record for 2a01:4d8:161:107::2 on eth0.*.
Apr 17 13:37:20 ub avahi-daemon[733]: Withdrawing address record for fe80::3030:ac27:7ad6:6b75 on eth0.
Apr 17 13:38:15 ub avahi-daemon[733]: Registering new address record for 2a01:4d8:161:107::1 on eth0.*.
Apr 17 13:38:43 ub NetworkManager[732]: <info>  [1587123523.8167] policy: set 'Kabelgebundene Verbindung 1'
 (eth0) as default for IPv6 routing and DNS
```

Netzwerkkonfiguration

/etc/hosts

Sie enthält eine Liste bekannter IP-Adressen und der ihnen zugeordneten Namen. Die Datei muss auf jeden Fall die Daten der Loopback-Schnittstelle enthalten.

- Default Einstellungen unter Ubuntu:

```
127.0.0.1       localhost
127.0.1.1       ub

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Netzwerkkonfiguration

/etc/hosts

Wenn Sie die anderen Rechner im lokalen Netz namentlich ansprechen möchten und es keinen lokalen Nameserver gibt, müssen Sie auch deren Namen in /etc/hosts angeben.

```
192.168.0.10      server.local.lan      server
192.168.0.11      plex.local.lan        plex
192.168.0.12      rpi.local.lan         rpi
```

Analoge Einträge sind in den **/etc/hosts-Dateien** aller Rechner im lokalen Netz erforderlich. Je mehr Rechner es im lokalen Netzwerk gibt, desto mühsamer wird die Administration der **/etc/hosts-Dateien.**

Netzwerkkonfiguration

/etc/hosts.conf

Die folgende Beispieldatei bestimmt, dass zuerst die Datei **/etc/hosts** ausgewertet (Schlüsselwort **hosts**) und danach der in **/etc/resolv.conf** angegebene Nameserver befragt werden soll (bind).

```
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
```

Die zweite Zeile erlaubt, dass Hostnamen mehrere IP-Adressen zugeordnet werden dürfen.

Netzwerkkonfiguration

/etc/network/interfaces

Bei einer statischen Konfiguration sind je nach Distribution unterschiedliche Dateien verantwortlich.

- Bei Debian beschreibt **/etc/network/interfaces** alle Netzwerkschnittstellen.
- Bei statisch konfigurierten Schnittstellen wird das Gateway durch das Schlüsselwort gateway eingestellt.

```
# The looback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
   address 192.168.0.111
   netmask 255.255.255.0
   gateway 192.168.0.1
   dns-nameservers 192.168.0.1
```

Netzwerkkonfiguration

DNS-Konfiguration resolv.conf

Sie steuert, wie die IP-Adressen für unbekannte Hostnamen ermittelt werden.

»Unbekannt« bedeutet, dass die Namen nicht in **/etc/hosts** definiert sind.

```
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0
search mshome.net
```

Netzwerkkonfiguration

Bei vielen Distributionen wird resolv.conf dynamisch erzeugt:

Wenn Ihre lokale Netzwerkverbindung (LAN, WLAN) mit DHCP konfiguriert ist, trägt das Script für den Verbindungsaufbau bzw. der NetworkManager die vom DHCP-Server übertragenen Nameserver-Adressen ein.

- Wenn eine Internetverbindung per PPP (ADSL,UMTS, VPN) hergestellt wird, trägt das Script für den Verbindungsaufbau automatisch die nameserver-Adressen Ihres Internet-Providers in **`/etc/resolv.conf`** ein.

- Ubuntu richtet ab Version 12.04 standardmäßig einen lokalen Nameserver ein.

Netzwerkkonfiguration

Wenn Sie den Nameserver manuell einrichten möchten, müssen Sie seine Adresse **/etc/network/interfaces** mit dem Schlüsselwort **dns-nameservers** angeben:

```
# The looback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
   address 192.168.0.111
   netmask 255.255.255.0
   gateway 192.168.0.1
   dns-nameservers 192.168.0.1
```

Netzwerkkonfiguration

Hostname

Der aktuelle Hostname kann mit dem Kommando **hostname** ermittelt werden. Sofern der Hostname nicht durch DHCP eingestellt wird, erfolgt die Konfiguration durch unterschiedliche Dateien.

Distribution	Datei
Die meisten aktuellen Distributionen	/etc/hostname
CentOS 6 / RHEL 6	/etc/sysconfig/network
Alte SUSE Distributionen	/etc/HOSTNAME

Denken Sie daran, auch **/etc/hosts** anzupassen, falls diese Datei eine Zeile mit dem Hostnamen des Rechners enthält.

NetworkManager deaktivieren

Natürlich können Sie gemäß den folgenden Anleitungen auch Desktop-Systeme konfigurieren. Dort sollten Sie aber unbedingt vorher den **`NetworkManager`** deaktivieren bzw. gleich deinstallieren. Dazu führen Sie je nach Distribution eines der folgenden Kommandos aus:

```
sb@ub:~$    sudo apt remove network-manager (Debian, Ubuntu, ...)
sb@fedo:~$  sudo dnf remove NetworkManager (Fedora)
sb@suse:~$  sudo yum remove NetworkManager (SuSe, CentOS, ...)
```

- Unter Ubuntu sollten Sie gleich auch das Paket **`resolvconf`** deinstallieren.

```
sb@ub:~$  sudo apt remove resolv.conf
sb@ub:~$  sudo reboot now
```

Befehle zur Netzwerkadministration

Vergleichstabelle **`ip`** versus **`ifconfig`**

Zweck	iproute2 Kommando	iproute2 Kommando Kurzversion	net-tools Kommando
Linkstatus anzeigen	ip link show	ip l	ifconfig
Linkstatus	ip -statistics link show	ip -s l	ifconfig
IP-Adresse anzeigen	ip addr show	ip a	ifconfig -a
IP-Adresse setzen	ip addr add IP/NETMASK dev DEVICE	ip a a IP/NETMASK dev DEVICE	ifconfig DEVICE IP/NETMASK
IP-Adresse entfernen	ip addr del IP/NETMASK dev DEVICE	ip a d IP/NETMASK dev DEVICE	
IP-Adresse entfernen	ip addr flush dev DEVICE	ip a f dev DEVICE	
Routingtabelle anzeigen	ip route show	ip r	route -n
Standardgateway setzen	ip route add default via IP	ip r a default via IP	route add default gw IP DEVICE
ARP-Cache anzeigen	ip neigh show	ip n	arp -na
Verbindungen anzeigen	ss --tcp --all --processes --extended --numeric	ss -tapen	netstat -tapen

Befehle zur Netzwerkadministration

ping - ist ein Programm / Befehl zum Prüfen der Erreichbarkeit von anderen Rechnern oder Geräten über ein (beliebiges) Netzwerk.

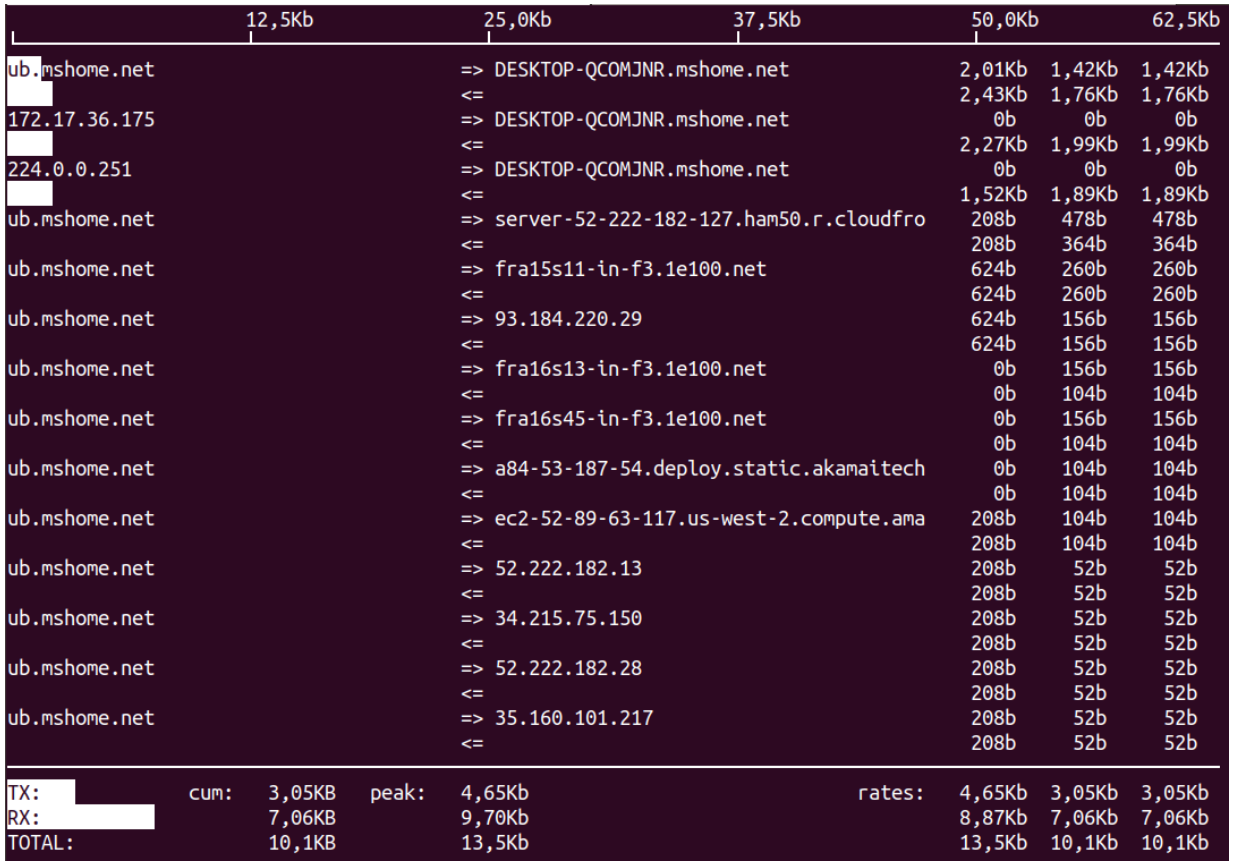
Optionen	Bedeutung	Beschreibung
-c	Anzahl	ANZAHL gibt an, wie viele ping-Anfragen gesendet werden sollen, danach stoppt ping automatisch
-w	Ende	ENDE wird in Sekunden angegeben. ping wird nach dieser Zeit beendet, egal wie viele Anfragen (un-) beantwortet wurden.
-W	Auszeit	AUSZEIT wird in Sekunden angegeben und gibt an, wie lange ping auf eine Antwort wartet, bevor es automatisch stoppt
-i	Intervall	INTERVALL wird in Sekunden angegeben und gibt vor, in welchen Abständen die ping-Anfragen gesendet werden. Voreinstellung ist eine Sekunde.
-I	Schnittstelle	legt fest, über welche Schnittstelle die ping-Anfragen gesendet werden

Befehle zur Netzwerkadministration

Iftop

ist eine dem top-Programm ähnliche Anzeige für IP-Tabellen Status Einträge.

- iftop wird im einfachsten Fall ohne weitere Parameter aufgerufen.
- Damit bekommt man eine top-ähnliche interaktive Anzeige.



Befehle zur Netzwerkadministration

Linux Netzwerk Analyse mit traceroute

Traceroute ist bei Ubuntu nicht standardmäßig installiert, und muss daher mit den Befehl `apt install traceroute` installiert werden.

Funktionsweise:

Traceroute verfolgt den Weg von Netzwerk-Paketen hin zu einem bestimmten Host. Dazu verändert traceroute das time-to-live (TTL) Feld des IP Protokolls. Durch kleine TTL Werte versucht traceroute ICMP TIME_EXCEEDED Antworten der einzelnen Router zu bekommen. Für das Erfassen der einzelnen Hops (Router) am Weg vom aktuellen Rechner hin zum gewünschten Host geht traceroute folgendermaßen vor:

Befehle zur Netzwerkadministration

- Zuerst verschickt es ein IP Paket mit TTL=1. Damit verwirft bereits der erste Router (das Default Gateway) das Paket und schickt eine ICMP TIME_EXCEEDED Antwort zurück.

- Nun verschickt traceroute weitere Pakete und erhöht dabei die TTL sukzessive jeweils um 1. Beim zweiten Paket (TTL=2) gelangt das Paket zuerst über das Default Gateway weiter zum nächsten Router am Weg zum Host. Da das Default Gateway beim Weiterleiten des Pakets die TTL um 1 verringert, kommt das Paket mit TTL=1 am zweiten Router an. Dieser verwirft das Paket und schickt eine ICMP TIME_EXCEEDED Antwort an den ursprünglichen Rechner zurück. Analog funktioniert es dann mit TTL=3 beim dritten Router, TTL=4 beim vierten Router, usw.

- Erreicht ein IP Paket mit ausreichend hoher TTL schließlich den Ziel-Host, antwortet er mit einer ICMP "port unreachable" Meldung.

Befehle zur Netzwerkadministration

Linux Netzwerk Analyse mit traceroute

Für die verschickten IP Testpakete können unterschiedliche Protokolle genutzt werden.

- **UDP (default)**

  In der Standard-Konfiguration weren UDP Datagramme als IP Testpakete verwendet.
- **ICMP (-I)**

  Diese Methode verwendet ICMP echo requests ('Ping') zum Testen.
- **TCP (-T)**

  Diese Methode verwendet einen fixen TCP Port (Port 80 ist default).

Befehle zur Netzwerkadministration

Linux Netzwerk Analyse mit traceroute

- Beispiel:

```
sb@ub:~$ traceroute google.de
traceroute to google.de (172.217.23.99), 30 hops max, 60 byte packets
 1  DESKTOP-QCOMJNR.mshome.net (172.17.36.161)  0.417 ms  0.282 ms  0.374 ms
 2  fritz.box (10.11.12.1)  0.706 ms  1.954 ms  1.951 ms
 3  62.155.242.224 (62.155.242.224)  6.965 ms  6.982 ms  6.977 ms
 4  217.5.116.86 (217.5.116.86)  15.708 ms 217.5.116.90 (217.5.116.90)  15.692 ms  16.846 ms
 5  62.157.250.46 (62.157.250.46)  16.206 ms  16.347 ms  14.502 ms
 6  * * *
 7  108.170.235.244 (108.170.235.244)  15.667 ms 108.170.252.1 (108.170.252.1)  14.998 ms 172.253.64.118 (1
72.253.64.118)  14.027 ms
 8  fra16s45-in-f3.1e100.net (172.217.23.99)  14.006 ms 108.170.252.18 (108.170.252.18)  14.550 ms fra16s45
-in-f3.1e100.net (172.217.23.99)  14.522 ms
sb@ub:~$
```

Befehle zur Netzwerkadministration

Linux Netzwerk Analyse mit mtr

Das Netzwerk-Diagnose-Tool **`mtr`** (My Traceroute) kombiniert in einem einzelnen Programm die Funktionalität der beiden Tools **`traceroute`** und **`ping`**.

- Es kann als textbasiertes **`ncurses`** Programm oder als grafisches GTK+ Programm benutzt werden.
- Das Programm wird auf der Kommandozeile zusammen mit einem Host als Parameter aufgerufen.
- Als Host gibt man jenen Hostnamen bzw. jene IP an, zu welcher man die Verbindung vom aktuellen Rechner aus überprüfen will: **`mtr www.google.com`**

Befehle zur Netzwerkadministration

Linux Netzwerk Analyse mit mtr

Die folgende Ausgabe zeigt den Aufruf von mtr google.de.

```
                                My traceroute  [v0.92]
ub (172.17.36.171)                                      2020-04-17T14:19:40+0200
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                 Packets               Pings
 Host                                         Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. DESKTOP-QCOMJNR.mshome.net                 0.0%     8    0.3   0.3   0.2   0.6   0.1
 2. fritz.box                                  0.0%     8    0.7   0.8   0.6   1.1   0.2
 3. 62.155.242.224                             0.0%     8    5.4   5.2   4.8   5.5   0.2
 4. 217.5.116.94                               0.0%     8   12.5  12.7  12.5  13.1   0.2
 5. 87.128.238.134                             0.0%     8   12.7  12.6  12.3  12.8   0.2
 6. 216.239.63.199                             0.0%     8   13.7  13.6  13.2  14.1   0.3
 7. 216.239.47.245                             0.0%     8   13.4  13.8  13.4  14.3   0.3
 8. fra15s22-in-f163.1e100.net                 0.0%     8   12.0  12.2  12.0  12.8   0.2
```

Befehle zur Netzwerkadministration

Linux Netzwerk Analyse mit mtr

Bei weiter entfernten Seiten kann man durch die jeweilige round trip time erkennen zwischen welchen Hops (Routern) Seekabel-Verbindungen (beispielsweise über den Atlantik) vorliegen. Beim Analysieren der Verbindung zu www.areca.com.tw ist dies erkennbar:

```
sb@ub:~$ mtr -4 -r -w -c 10 www.area.com.tw
Start: 2020-04-17T14:20:36+0200
HOST: ub                                      Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- DESKTOP-QCOMJNR.mshome.net             0.0%    10    0.3   0.3   0.2   0.4   0.1
  2.|-- fritz.box                              0.0%    10    0.7   0.8   0.6   1.1   0.2
  3.|-- 62.155.242.224                         0.0%    10    5.1   7.1   4.8  21.5   5.2
  4.|-- 217.5.116.114                          0.0%    10   13.0  12.9  12.5  13.3   0.3
  5.|-- ffm-b4-link.telia.net                 10.0%    10   13.6  13.1  12.8  13.6   0.3
  6.|-- ffm-bb2-link.telia.net                 0.0%    10  156.1 156.0 155.7 156.5   0.2
  7.|-- ???                                  100.0    10    0.0   0.0   0.0   0.0   0.0
  8.|-- rest-bb1-link.telia.net               0.0%    10   99.9 100.2  99.8 100.8   0.3
  9.|-- las-b24-link.telia.net                0.0%    10  154.5 153.6 152.5 155.9   1.1
 10.|-- chunghwa-ic-335211-las-b24.c.telia.net 0.0%    10  159.4 160.2 158.8 166.7   2.4
 11.|-- r4002-s2.tp.hinet.net                10.0%    10  306.3 314.5 304.8 352.2  14.5
 12.|-- r4102-s2.tp.hinet.net                 0.0%    10  315.0 316.5 312.3 323.8   3.2
 13.|-- 220-128-13-94.HINET-IP.hinet.net      0.0%    10  315.3 317.4 312.5 324.0   3.0
 14.|-- tyfo-3031.hinet.net                   0.0%    10  317.7 319.1 314.4 325.7   3.4
 15.|-- tyfo-3302.hinet.net                   0.0%    10  309.6 309.6 306.5 316.5   3.0
 16.|-- h101.s229.ts.hinet.net                0.0%    10  309.2 310.9 308.1 316.9   2.6
 17.|-- ???                                  100.0    10    0.0   0.0   0.0   0.0   0.0
 18.|-- 211-72-121-211.HINET-IP.hinet.net     0.0%    10  345.7 347.5 343.5 352.8   2.6
```

Bei dieser Abfrage geht es offensichtlich zwischen folgenden Routern über eine längere Seekabelverbindung durch ein Meer, erkennbar an den hohen Differenzen der durchschnittlichen Pingzeiten (Avg):

- zwischen Hop 1 (0.3 ms) und 9 (153.6 ms)
- zwischen Hop 11 (314.5 ms) und 18 (347.5 ms)

Befehle zur Netzwerkadministration

TCP und UDP Netzwerk Performance mit iperf messen

Das OpenSource Tool iperf erlaubt das Messen der maximalen TCP und UDP Netzwerk Bandbreite.

- **Installation**

  Iperf ist im Debian und Ubuntu Repository bereits enthalten, d.h. eine Installation ist ganz einfach via apt-get install iperf möglich.

- **Verwendung**

  Iperf funktioniert nach dem Client-Server Modell. D.h. man startet zuerst den iperf Daemon auf einem Server und verbindet sich danach mit dem iperf Client. Client und Server sind praktischerweise im selben Binary enthalten.

Befehle zur Netzwerkadministration

TCP Performance messen

In diesem Fall wird die TCP Performance einer virtuellen Netzwerkkarte gemessen.

```
root@ub:~# iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size:  128 KByte (default)
------------------------------------------------------------
[  4] local 127.0.1.1 port 5001 connected with 127.0.0.1 port 43426
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  37.4 GBytes  32.1 Gbits/sec
```

```
sb@ub:~$ iperf -c ub
------------------------------------------------------------
Client connecting to ub, TCP port 5001
TCP window size: 2.50 MByte (default)
------------------------------------------------------------
[  3] local 127.0.0.1 port 43426 connected with 127.0.1.1 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  37.4 GBytes  32.1 Gbits/sec
sb@ub:~$
```

WBS TRAINING

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!