

Grundlagen zu Computernetzwerken

am Beispiel von Linux

von Dirk Burkert

Inhaltsverzeichnis

- Wozu ein Computernetzwerk?
- Wer bin ich?
- Ein mögliches Beispielszenario
- Wenn mal was nicht so klappt

Wozu ein Computernetzwerk?

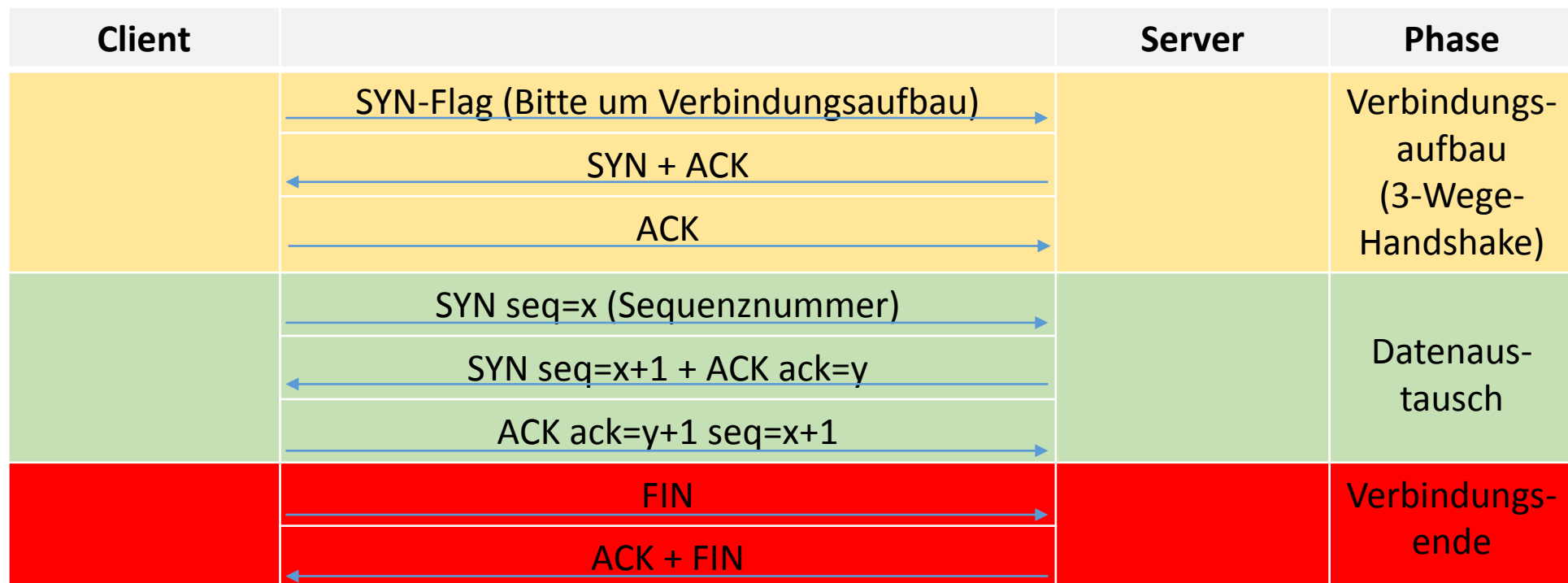
- Wenn Informationen nicht nur lokal (d.h. auf dem Computer) verfügbar sein sollen kann zum Austausch ein Computernetzwerk verwendet werden. Eine andere Möglichkeit Daten auszutauschen ist mit Wechseldatenträgern (z.B. CD, USB-Stick, ...).
- Wenn sich ein Computer in einem Computernetzwerk befindet werden IMMER Informationen ausgetauscht, es sei denn, der Computer ist ausgeschaltet.
- Unter Computer werden alle Geräte verstanden, die mit einem Netzwerk verbunden werden können (Laptop, Smartphone, Tablet, Kühlschrank ...).
- Ein Computernetzwerk ist somit ein Zusammenschluss von mindestens 2 Computern die miteinander kommunizieren.

Wer bin ich?

- Damit die auszutauschenden Informationen korrekt zugestellt werden können wird ein Empfänger und ein Absender benötigt, vergleichbar einem Brief (TCP) oder einer Postkarte (UDP).
- Bei UDP (User Datagram Protocol) handelt es sich um ein verbindungsloses Protokoll, d.h. es wird keine Antwort erwartet und wird auch nur bei geringem Datenverkehr verwendet. Ein Beispiel hierzu ist das verbreiten der Zeit in einem Netzwerk über NTP (Network Time Protocol).

Wer bin ich?

- Anders sieht das aus bei TCP (Transmission Control Protocol), hier wird eine sichere, verlustfreie Verbindung hergestellt.



Wer bin ich?

- Für einen Computer besteht seine Adresse aus einer Zahlenkolonne. Diese Zahlenkolonne ist für IPv4-Adressen 32 Bit lang und wird zur besseren Lesbarkeit in 4 Oktetten die durch Punkte voneinander getrennt sind dargestellt (ADDRESS).

11000000 10101000 00000010 00110101
192 . 168 . 2 . 53

- Die neueren IPv6-Adressen sind 128 Bit lang.

Wer bin ich?

- Damit wir auch „Namen“ verwenden können wird ein DNS (Domain Name Service) eingesetzt, der die Übersetzung des Namens in eine IP-Adresse vornimmt.

```
1 $ORIGIN .
2 $TTL 86400      ; 1 day
3 int.burkert.net IN SOA  DNSDHCP.int.burkert.net. root.burkert.net. (
4     170102      ; serial
5     604800      ; refresh (1 week)
6     86400       ; retry (1 day)
7     2419200     ; expire (4 weeks)
8     86400       ; minimum (1 day)
9 )
10      NS       DNSDHCP.int.burkert.net.
11      NS       BackupDNS.int.burkert.net.
12      MX       10 MailServer.int.burkert.net.
13 $ORIGIN int.burkert.net.
14 AdminPC      A       192.168.22.2
15 BackFirewall-admin  A       192.168.22.254
16 BackFirewall-client  A       192.168.21.254
17 BackFirewall-dienste  A       192.168.20.254
18 BackFirewall-dmz2    A       192.168.11.1
19 BackupDNS      A       192.168.20.2
20 bf             CNAME   BackFirewall-dmz2
21 $TTL 300       ; 5 minutes
22 desinfect      A       192.168.21.105
23               TXT     "004821ef1357512daa8ada6aa3669c3cf7"
24 $TTL 86400     ; 1 day
```

```
1 $ORIGIN .
2 $TTL 86400      ; 1 day
3 168.192.in-addr.arpa IN SOA  DNSDHCP.int.burkert.net. root.burkert.net. (
4     170102      ; serial
5     604800      ; refresh (1 week)
6     86400       ; retry (1 day)
7     2419200     ; expire (4 weeks)
8     86400       ; minimum (1 day)
9 )
10      NS       DNSDHCP.int.burkert.net.
11      NS       BackupDNS.int.burkert.net.
12      MX       10 MailServer.int.burkert.net.
13 $ORIGIN 10.168.192.in-addr.arpa.
14 10           PTR     WWWProxy.int.burkert.net.
15 2            PTR     DNSDHCP.int.burkert.net.
16 254         PTR     FrontFirewall-dmz1.int.burkert.net.
17 4           PTR     SmtGateway.int.burkert.net.
18 6           PTR     WWW1FTP.int.burkert.net.
19 7           PTR     WWW2.int.burkert.net.
20 8           PTR     Mysql.int.burkert.net.
21 $ORIGIN 11.168.192.in-addr.arpa.
22 1           PTR     BackFirewall-dmz2.int.burkert.net.
23 2           PTR     LOGServer.int.burkert.net.
24 254        PTR     FrontFirewall-dmz2.int.burkert.net.
```

Wer bin ich?

- Weiterhin muss klar sein, wo nachgefragt werden muss, wenn Informationen benötigt oder abgelegt werden sollen.
- Dabei geht es NICHT um irgendwelche Suchmaschinen.
- Computer können nur in dem Netz in dem sie sich befinden miteinander kommunizieren.
- Wenn die Informationen nicht in dem aktuellen Netz liegen muss eine ROUTE nach draußen beschrieben sein, über ein sogenanntes GATEWAY.

Wer bin ich?

- Woher weiß nun der Computer in welchem Netzwerk er sich befindet?
- Das eigene Netzwerk wird über die NETMASK beschrieben.
- Eine NETMASK kann z.B. 255.255.255.0 sein, d.h. in diesem Fall, dass die ersten 3 Oktetts das Netzwerk beschreiben und das letzte Oktett die Anzahl der möglichen Hosts (Computer). Bei CIDR-schreibweise /24 (Classless Inter-Domain Routing).
- Ob ein GATEWAY benötigt wird erkennt der Computer durch eine UND-Verknüpfung von Ziel-IP-Adresse und NETZMASKE.

Wer bin ich?

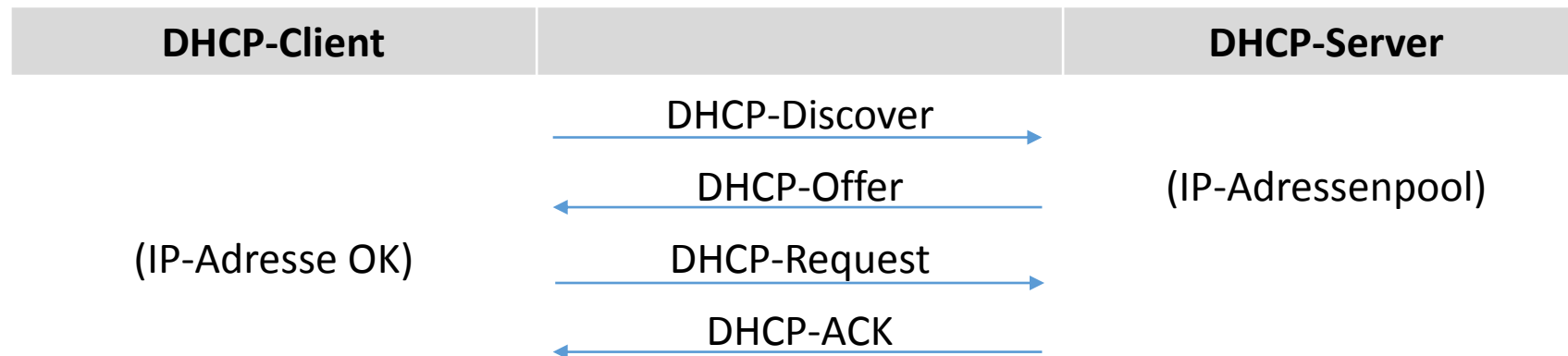
- Die bisherigen Informationen können wie folgt angezeigt werden.

```
root@DNSDHCP:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 08:00:27:2d:0f:16 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/24 brd 192.168.10.255 scope global eth0
    inet6 fe80::a00:27ff:fe2d:f16/64 scope link
        valid_lft forever preferred_lft forever
root@DNSDHCP:~# _
```

```
root@DNSDHCP:~# route -n
Kernel-IP-Routentabelle
Ziel          Router        Genmask         Flags Metric Ref    Use Iface
0.0.0.0      192.168.10.254 0.0.0.0         UG    0      0      0 eth0
192.168.10.0  0.0.0.0      255.255.255.0  U     0      0      0 eth0
root@DNSDHCP:~# _
```

Wer bin ich?

- Die „Erkenntnis“ zur Frage „Wer bin ich?“ wird, anders als im richtigen Leben, am einfachsten beim DHCP-Server (Dynamic Host Configuration Protocol) nachgefragt.



Wer bin ich?

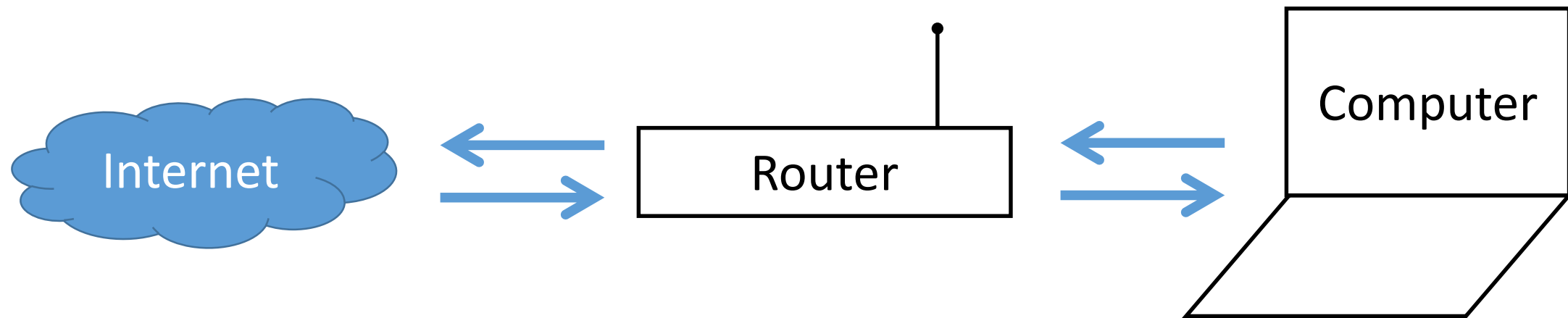
- Über den DHCP-Server werden die wichtigsten Informationen übertragen.

```
subnet 192.168.21.0 netmask 255.255.255.0 {  
  
    authoritative;  
    range 192.168.21.100 192.168.21.200;  
    filename "boot/pxelinux.0";  
    next-server 192.168.10.2;  
    option subnet-mask 255.255.255.0;  
    option broadcast-address 192.168.21.255;  
    option routers 192.168.21.254;  
    option domain-name "int.burkert.net";  
    option domain-name-servers 192.168.10.2, 192.168.20.2;  
    option ntp-servers 192.168.11.2;  
    option netbios-name-servers 192.168.20.8;  
}
```

```
Nov 5 20:48:29 DNSDHCP dhcpd: DHCPDISCOVER from 08:00:27:53:93:ff via 192.168.21.254  
Nov 5 20:48:30 DNSDHCP dhcpd: DHCPOFFER on 192.168.21.100 to 08:00:27:53:93:ff (LinuxClient) via 192.168.21.254  
Nov 5 20:48:30 DNSDHCP named[1902]: client 192.168.10.2#54161: updating zone 'int.burkert.net/IN': update unsuccessful: LinuxClient.int.burkert.net: 'name not in use' prerequisite not satisfied (YXDOMAIN)  
Nov 5 20:48:31 DNSDHCP dhcpd: DHCPREQUEST for 192.168.21.100 (192.168.10.2) from 08:00:27:53:93:ff (LinuxClient) via 192.168.21.254  
Nov 5 20:48:31 DNSDHCP dhcpd: DHCPACK on 192.168.21.100 to 08:00:27:53:93:ff (LinuxClient) via 192.168.21.254  
Nov 5 20:48:31 DNSDHCP named[1902]: client 192.168.10.2#54161: signer "updatekey" approved
```

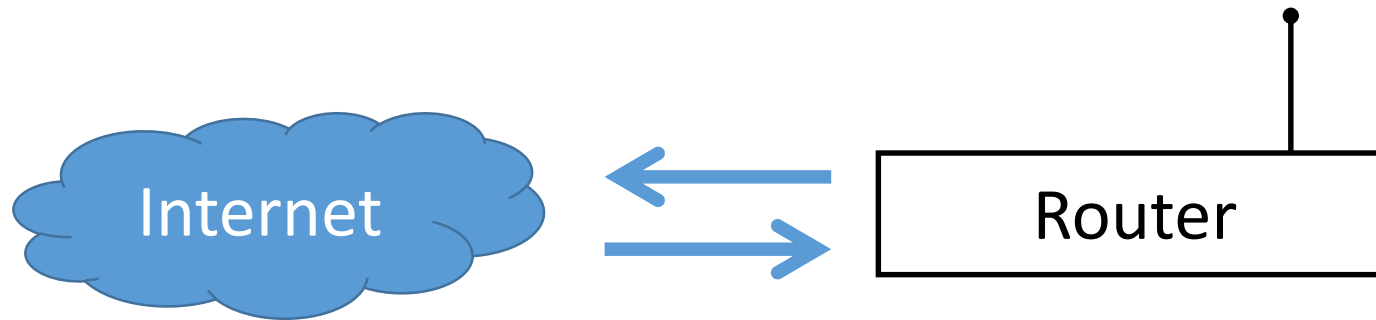
Ein mögliches Beispielszenario

- Was bedeutet es, wenn ich mit einem Computer ins Internet will?



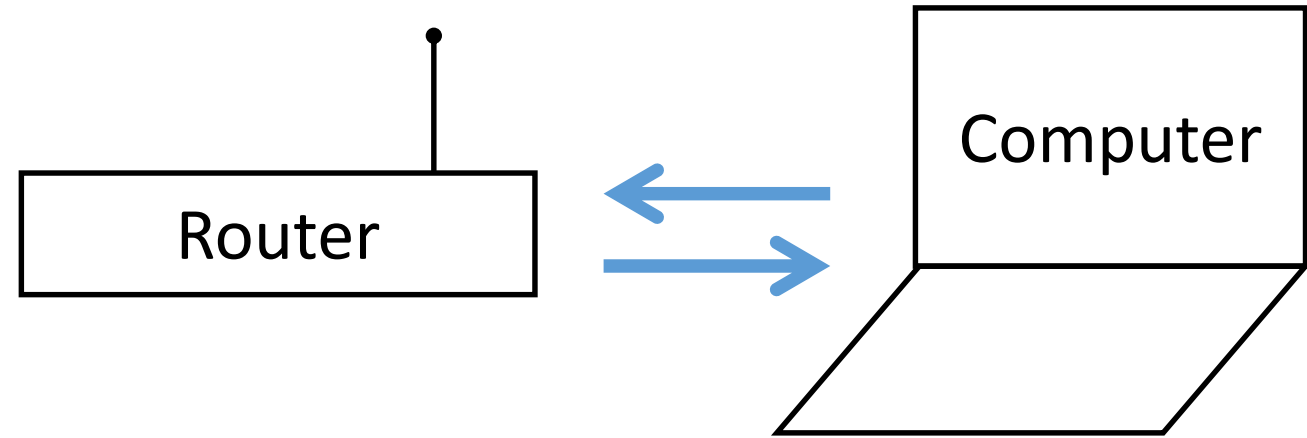
- Zum Datenaustausch muss eine Verbindung zwischen zwei Punkten aufgebaut werden.

Ein mögliches Beispielszenario



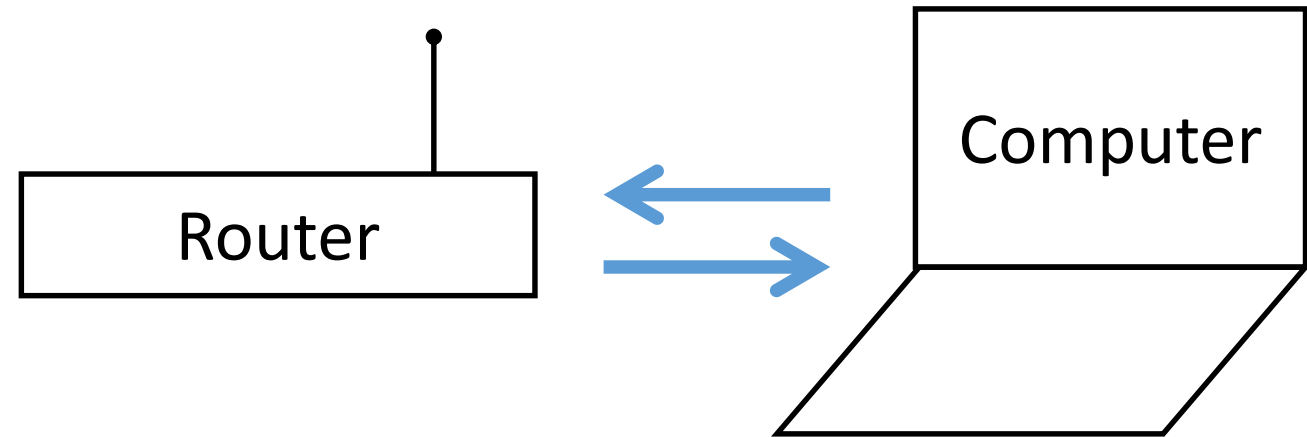
- Der Router wird an den Internetanschluss angeschlossen und mit den vom Internetprovider bekommenen Zugangsdaten eingerichtet.
- Der Router hat dadurch eine öffentliche WAN-IP Adresse, eine Gateway-Adresse und eine Adresse für den DNS-Server.
- NAT (Network Address Translation) bedeutet, dass der Router nach außen eine IP-Adresse hat und intern Anfragen verschiedener Adressen bearbeiten kann.

Ein mögliches Beispielszenario



- Live-Beispiel wie ein Client sich bei einem DHCP-Server anmeldet.

Ein mögliches Beispielszenario

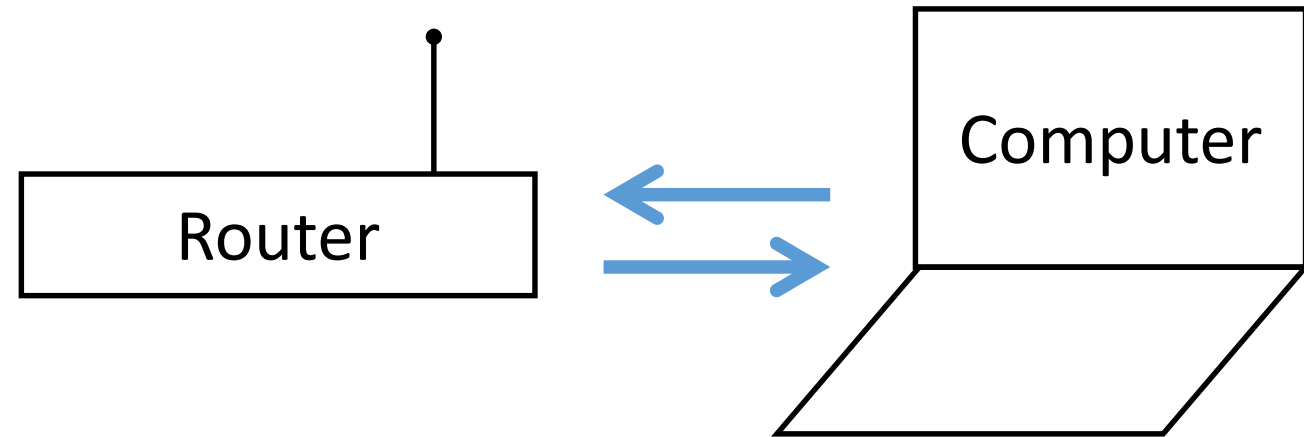


- Client-Konfigurationsdatei bei Verwendung von dhclient.

```
root@LinuxClient:/etc/dhcp# cat dhclient.conf | grep -v '^#' | less
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
       domain-name, domain-name-servers, domain-search, host-name,
       dhcp6.name-servers, dhcp6.domain-search,
       netbios-name-servers, netbios-scope, interface-mtu,
       rfc3442-classless-static-routes, ntp-servers;
```


Ein mögliches Beispielszenario



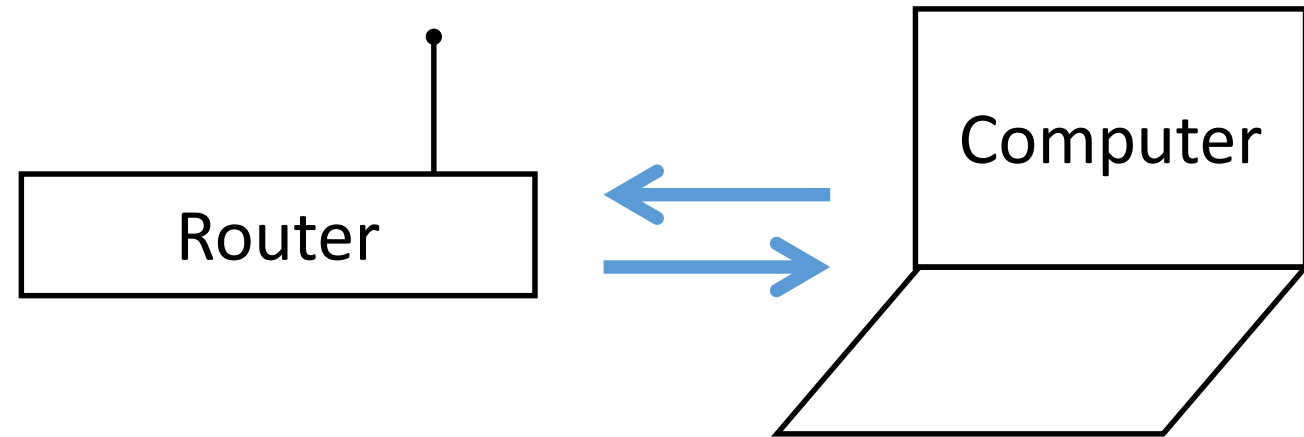
- Lease lösen dhclient -r

```
Nov  5 21:26:37 LinuxClient dhclient: DHCPRELEASE on eth0 to 192.168.10.2 port 67
Nov  5 21:26:36 DNSDHCP dhcpd: DHCPRELEASE of 192.168.21.110 from 08:00:27:53:93:ff (LinuxClient) via eth0 (found)
Nov  5 21:26:36 DNSDHCP dhcpd: DHCPRELEASE of 192.168.21.110 from 08:00:27:53:93:ff via 192.168.21.254 (found)
```

- Lease neu beziehen dhclient eth0

```
Nov  5 21:28:05 DNSDHCP dhcpd: DHCPDISCOVER from 08:00:27:53:93:ff via 192.168.21.254
Nov  5 21:28:06 DNSDHCP dhcpd: DHCPOFFER on 192.168.21.110 to 08:00:27:53:93:ff (LinuxClient) via 192.168.21.254
Nov  5 21:28:06 DNSDHCP named[1902]: client 192.168.10.2#54161: updating zone 'int.burkert.net/IN': update unsuccessful: LinuxClient.int.burkert.net: 'name not use' prerequisite not satisfied (YXDOMAIN)
Nov  5 21:28:06 DNSDHCP dhcpd: DHCPREQUEST for 192.168.21.110 (192.168.10.2) from 08:00:27:53:93:ff (LinuxClient) via 192.168.21.254
Nov  5 21:28:06 DNSDHCP dhcpd: DHCPACK on 192.168.21.110 to 08:00:27:53:93:ff (LinuxClient) via 192.168.21.254
Nov  5 21:28:06 DNSDHCP named[1902]: client 192.168.10.2#54161: signer "updatekey" approved
```

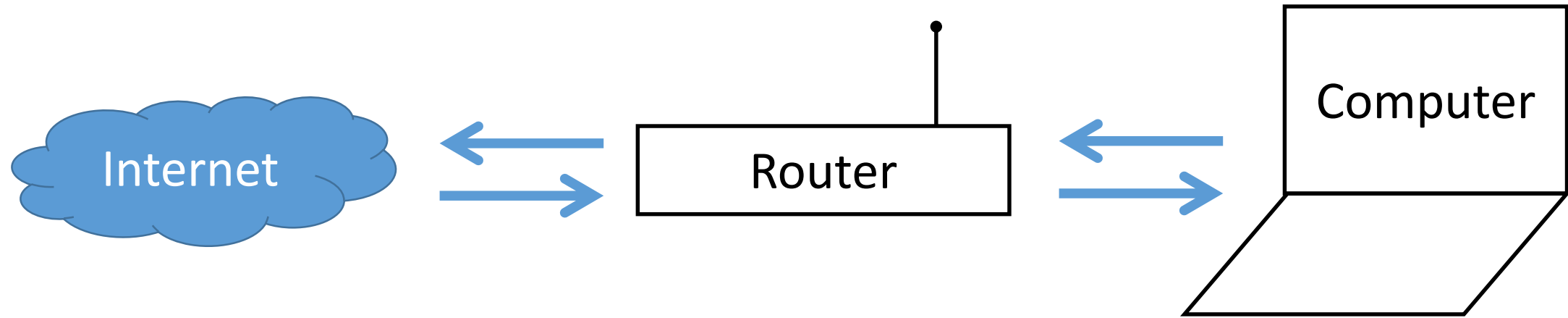
Ein mögliches Beispielszenario



- Einstellungen prüfen mit ifconfig

```
root@LinuxClient:/etc/dhcp# ifconfig
eth0      Link encap:Ethernet  Hardware Adresse 08:00:27:53:93:ff
          inet Adresse:192.168.21.110  Bcast:192.168.21.255  Maske:255.255.255.0
          inet6-Adresse: fe80::a00:27ff:fe53:93ff/64  Gültigkeitsbereich:Verbindu
ng
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
          RX packets:132 errors:0 dropped:0 overruns:0 frame:0
```

Ein mögliches Beispielszenario



- Beispielhaftes mitschneiden einer Email, erstellt über telnet mit Hilfe von wireshark.

Wenn mal was nicht so klappt

- Bei LAN-Verbindungen prüfen ob Lämpchen an der Netzwerkkarte des Endgerätes grün leuchtet bzw. blinkt.
- Bei WLAN-Verbindungen prüfen ob das WLAN eingeschaltet ist (mechanisch und softwaretechnisch) und ob der Access-Point betriebsbereit ist.

Wenn mal was nicht so klappt



Wenn mal was nicht so klappt

- Prüfen ob eine Anmeldung an einem Netzwerk besteht.

```
dirk@AdminPC:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN 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,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:41:95:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.22.2/24 brd 192.168.22.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe41:9562/64 scope link
        valid_lft forever preferred_lft forever
dirk@AdminPC:~$
```

- Da hier die Anmeldung über DHCP stattfindet ist die Anmeldung erfolgreich gewesen.

Wenn mal was nicht so klappt

- Prüfen ob eine ROUTE zu einem GATEWAY besteht.

```
root@AdminPC:~# route -n
Kernel-IP-Routentabelle
Ziel          Router        Genmask       Flags Metric Ref    Use Iface
0.0.0.0      192.168.22.254  0.0.0.0       UG    0      0      0 eth0
192.168.22.0  0.0.0.0       255.255.255.0 U     0      0      0 eth0
root@AdminPC:~# route
Kernel-IP-Routentabelle
Ziel          Router        Genmask       Flags Metric Ref    Use Iface
default      BackFirewall-ad 0.0.0.0       UG    0      0      0 eth0
192.168.22.0 *             255.255.255.0 U     0      0      0 eth0
root@AdminPC:~#
```

- In diesem Fall ist eine Default-ROUTE gesetzt.

Wenn mal was nicht so klappt

- Prüfen ob das GATEWAY verfügbar ist und die Namensauflösung klappt.

```
dirk@AdminPC:~$ ping 192.168.22.254
PING 192.168.22.254 (192.168.22.254) 56(84) bytes of data.
64 bytes from 192.168.22.254: icmp_req=1 ttl=255 time=0,759 ms
64 bytes from 192.168.22.254: icmp_req=2 ttl=255 time=0,658 ms
64 bytes from 192.168.22.254: icmp_req=3 ttl=255 time=0,943 ms
^C
--- 192.168.22.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0,658/0,786/0,943/0,122 ms
dirk@AdminPC:~$ ping BackFirewall-admin
PING BackFirewall-admin.int.burkert.net (192.168.22.254) 56(84) bytes of data.
64 bytes from BackFirewall-admin.int.burkert.net (192.168.22.254): icmp_req=1 ttl=255 time=0,627 ms
64 bytes from BackFirewall-admin.int.burkert.net (192.168.22.254): icmp_req=2 ttl=255 time=0,835 ms
64 bytes from BackFirewall-admin.int.burkert.net (192.168.22.254): icmp_req=3 ttl=255 time=0,933 ms
^C
--- BackFirewall-admin.int.burkert.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0,627/0,798/0,933/0,129 ms
dirk@AdminPC:~$
```


Wenn mal was nicht so klappt

- Prüfen ob andere Computer im Internet verfügbar sind.
- Dabei zeigen sich nun Schwierigkeiten

```
dirk@AdminPC:~$ ping www.t-online.de
ping: unknown host www.t-online.de
dirk@AdminPC:~$ nslookup www.t-online.de 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   www.t-online.de
Address: 62.138.238.100
Name:   www.t-online.de
Address: 62.138.239.100

dirk@AdminPC:~$ ping 63.138.239.100
PING 63.138.239.100 (63.138.239.100) 56(84) bytes of data.
^C
--- 63.138.239.100 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9211ms

dirk@AdminPC:~$ █
```

Wenn mal was nicht so klappt

- Prüfen ob andere Computer im Internet verfügbar sind.
- Dabei zeigen sich nun Schwierigkeiten

```
dirk@AdminPC:~$ ping www.t-online.de
ping: unknown host www.t-online.de
dirk@AdminPC:~$ nslookup www.t-online.de 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   www.t-online.de
Address: 62.138.238.100
Name:   www.t-online.de
Address: 62.138.239.100

dirk@AdminPC:~$ ping 63.138.239.100
PING 63.138.239.100 (63.138.239.100) 56(84) bytes of data.
^C
--- 63.138.239.100 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9211ms

dirk@AdminPC:~$ █
```

Wenn mal was nicht so klappt

- Eine Verfolgung der ROUTE klappt nicht obwohl ein Server zur Namensauflösung eingetragen ist (nameserver).

```
root@AdminPC:~# traceroute www.t-online.de
www.t-online.de: Der Name oder der Dienst ist nicht bekannt
Cannot handle "host" cmdline arg `www.t-online.de' on position 1 (argc 1)
root@AdminPC:~# cat /etc/resolv.conf | grep -v '^#'
domain int.burkert.net
search int.burkert.net
nameserver 192.168.10.2
root@AdminPC:~#
```

- Daher liegt das Problem nicht am Rechner sondern am DNS-Server.

Wenn mal was nicht so klappt

- Ein Blick in die Konfigurationsdatei des DNS-Servers zeigt die Misere.

```
27
28 ###dirk161104### nachfolgende Zeilen hinzufuegen!
29     forwarders { 172.16.43.1; };
30 #     forwarders { 192.168.43.1; };
31     forward only;
32
33 # erste Adresse ist localhost; zweite ist IP-Adresse des DNS-Servers
34     listen-on port 53 { 127.0.0.1; 192.168.10.2; };
"named.conf,options" 55L, 1618C
```

- Nach der Korrektur und Neustart des Dienstes (nicht des kompletten Servers funktioniert auch die Namensauflösung wieder.

```
dirk@AdminPC:~$ ping www.t-online.de
PING www.t-online.de (62.138.239.100) 56(84) bytes of data:
64 bytes from www.t-online.de (62.138.239.100): icmp_req=1 ttl=248 time=23,2 ms
64 bytes from www.t-online.de (62.138.239.100): icmp_req=2 ttl=248 time=22,3 ms
^C
--- www.t-online.de ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 22,345/22,821/23,298/0,499 ms
dirk@AdminPC:~$ █
```

Wenn mal was nicht so klappt

- Und auch die Internetseite ist verfügbar.

