

Linux for Beginners 2005

Mit Linux ins Netz
Modem-, ISDN-, DSL-Konfiguration

Martin Heinrich
obrien@lusc.de

Agenda

- Technik
- Konfiguration
- Test
- Fehlersuche
- Sicherheit
- Router

Verschiedene Techniken

- POTS (Plain Old Telephone Service) – analog
- ISDN (Integrated Services Digital Network)
- xDSL (Digital Subscriber Line)
- GPRS (General Packet Radio Service)
- HSCSD (High Speed Circuit Switched Data)
- UMTS (Universal Mobile Telecommunications System)
- WLAN (Wireless Local Area Network)
- Kabelmodem
- WiMax (Worldwide Interoperability for Microwave Access)

POTS

Modem an TAE-Dose

(TAE=Telekommunikations-Anschluss-Einheit)

Maximale Übertragungsrate 56kbit, bei guter Leitungsqualität

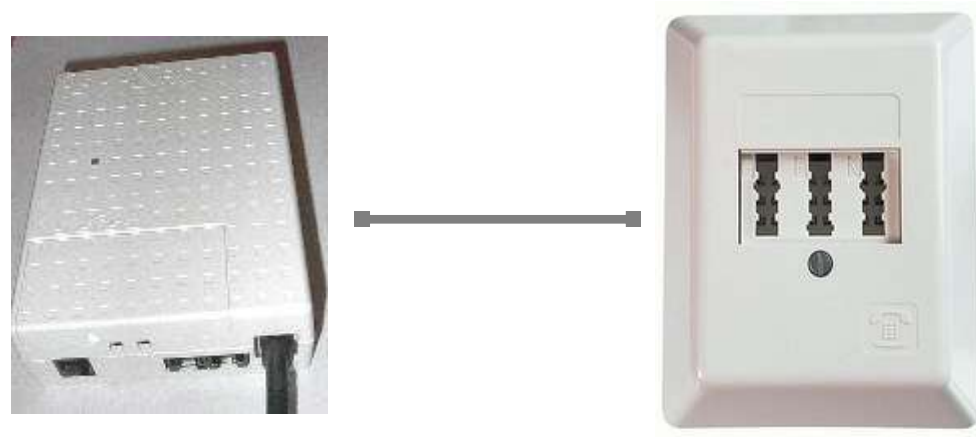


ISDN I

NTBA (Network Termination for Basic Access) an TAE-Dose

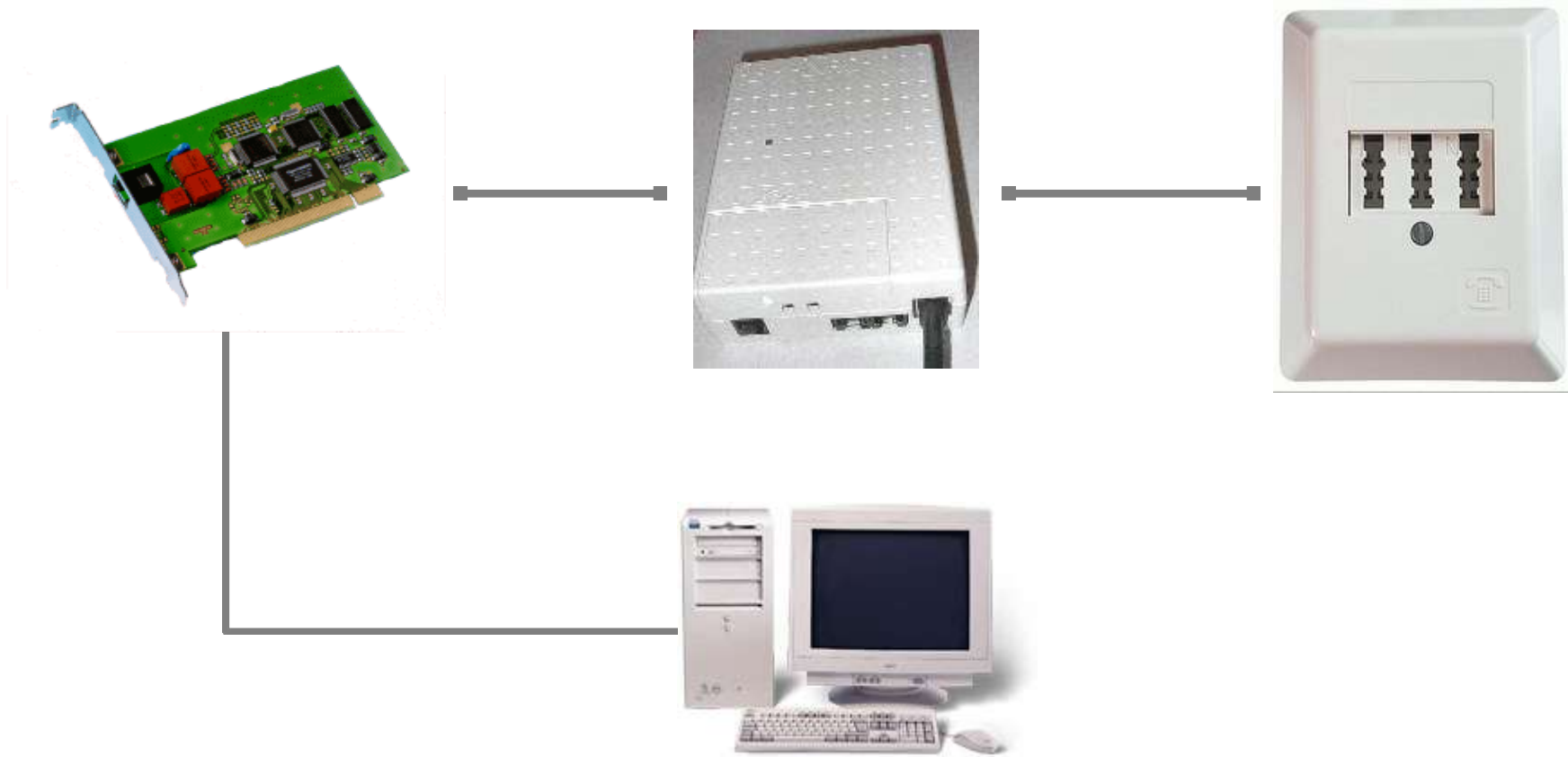
Übertragungsrate:

1. Kanal – 64 kbit
2. Kanäle – 128 kbit



ISDN II

ISDN-Karte/Modem an NTBA



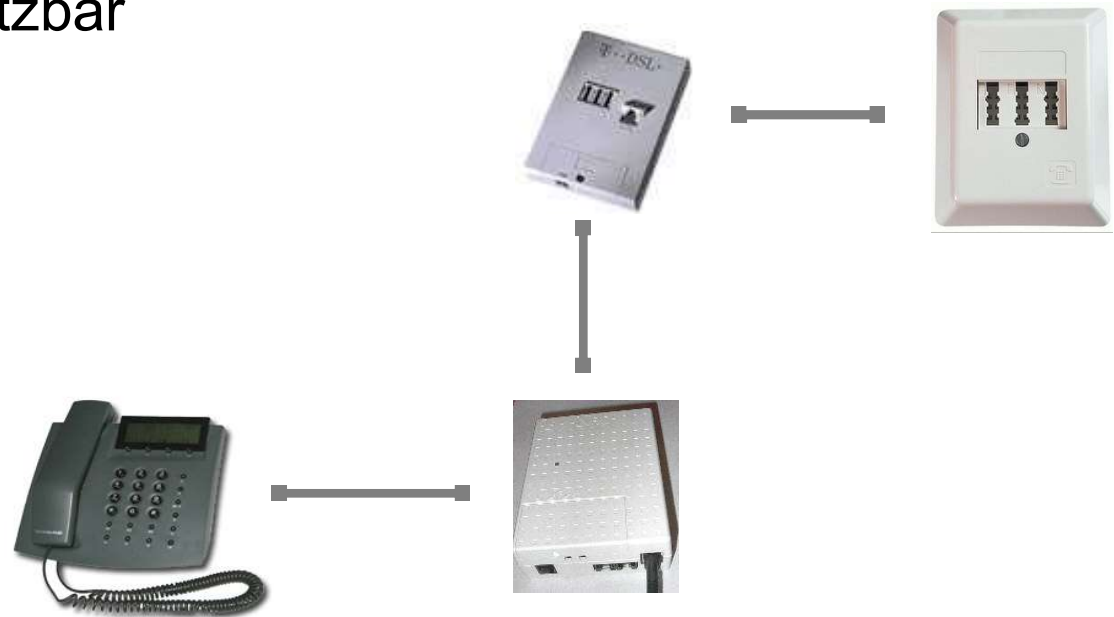
ADSL

Splitter/BBAE (Breitbandanschlusseinheit) zwischen NTBA und TAE

Trennung von ISDN und DSL

ISDN und DSL parallel nutzbar

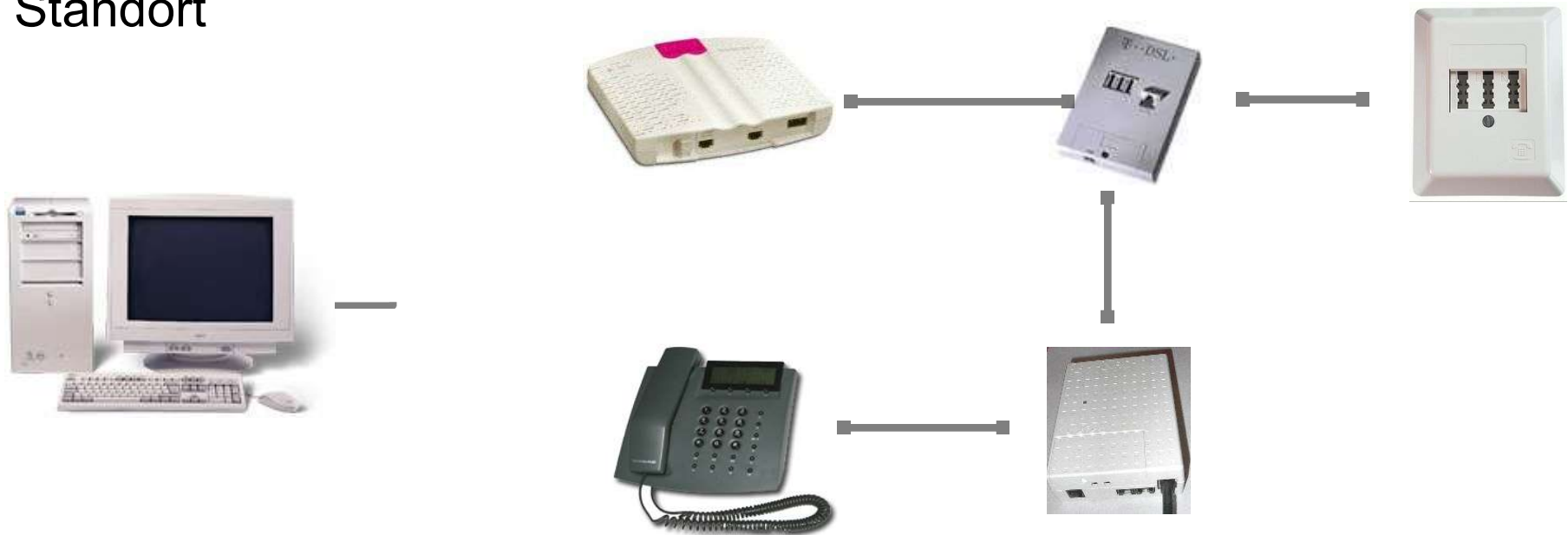
(selten Analog und DSL)



ADSL

DSL-Modem an Splitter

aktuell bis zu 6Mbit down-/2Mbit upstream, je nach Anbieter und Standort
Standort



Router I

Router an DSL-Modem



Router II

Router mit integriertem Modem



Was machen wir?

Computer direkt an das Netz

Mögliche Hürde :

Widerspenstige Hardware z.B. „Winmodems“

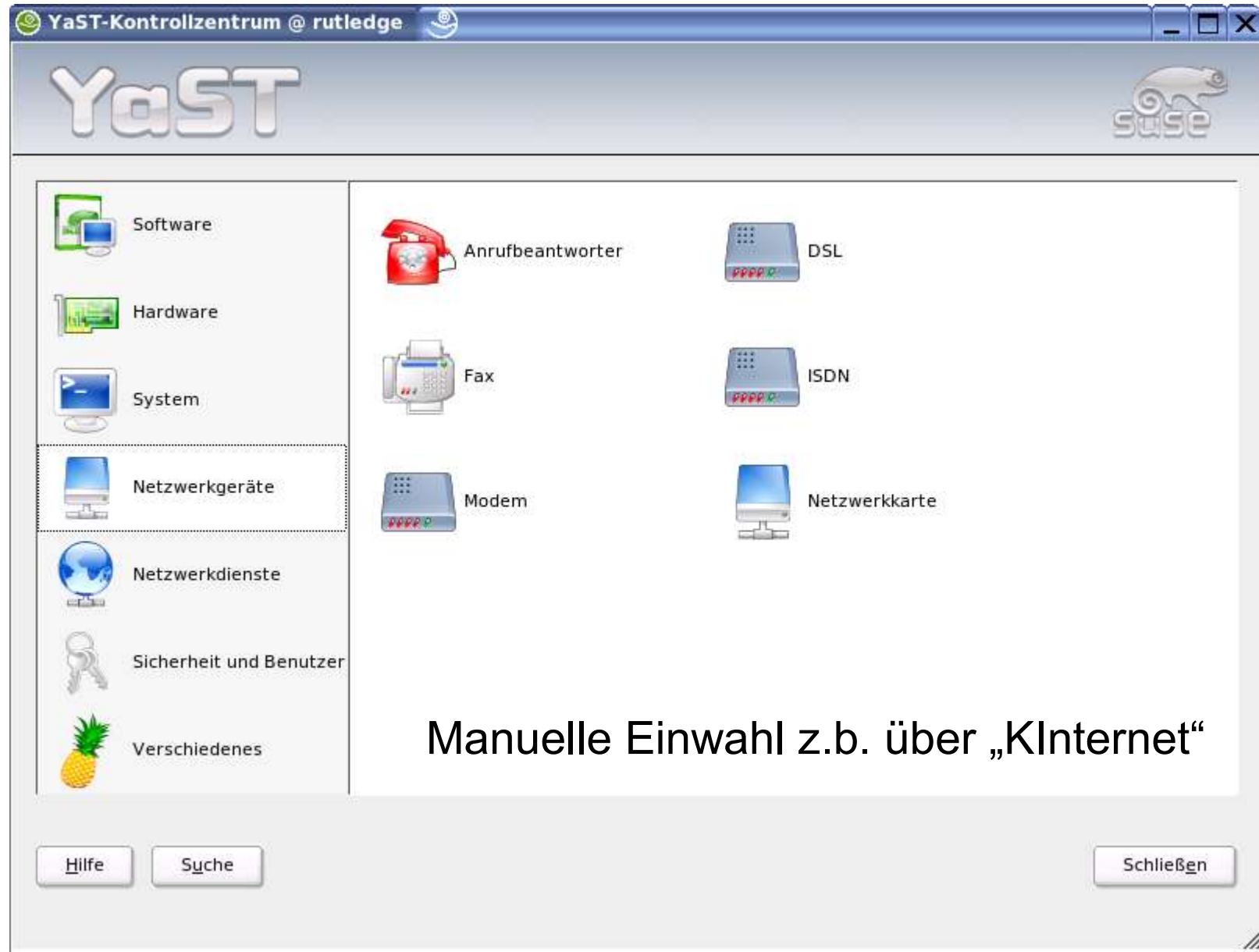
Abhilfe:

www.linuxant.com/drivers/ für Conexant Chips

www.smlink.com/content.aspx?id=105 für Smart Link Modems

Teilweise in Distributionen enthalten

Konfiguration - SuSE



Konfiguration - Fedora

Systemwerkzeuge --> Wizard zur Internetkonfiguration



Konfiguration - Debian – Modem I

pppconfig (als root)

Benötigte Daten:

- Login- oder Benutzername
- Passwort
- Telefonnummer zur Einwahl beim Provider

Anmeldeverfahren:

PAP Peer Authentication Protocol

Chat Use chat for login:/password: authentication

CHAP Crypto Handshake Auth Protocol

Konfiguration - Debian – Modem II

Verbindung testen

pon „Providername“

ifconfig zeigt jetzt ein Device ppp0 an

ping -c 1 www.lusc.de

poff „Providername“

Bei Fehlersuche Logfiles anschauen

/var/log/ppp.log

/var/log/messages

Konfiguration - Debian - ISDN

Verschiedene Treibermodelle

hisax <http://www.isdn4linux.de/>

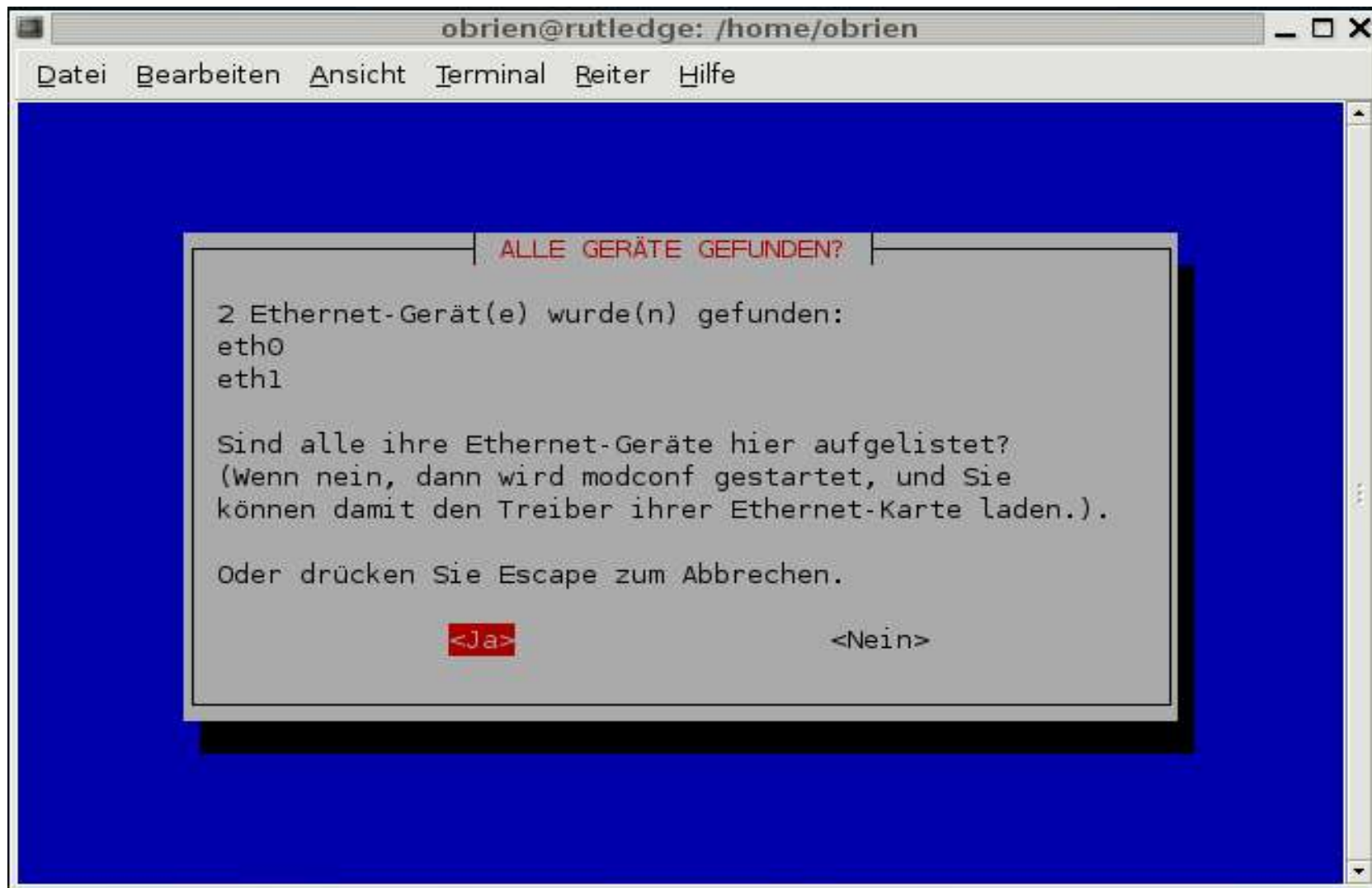
neu in Kernel 2.6

mISDN <http://rcum.uni-mb.si/~uvp00845b/>

Weitere Hilfe: <http://www.debiananwenderhandbuch.de>

Konfiguration - Debian - DSL


pppoeconf als 'root' starten.



Konfiguration - Debian - DSL

SUCHE NACH PPPoE-HARDWARE

Es wird jetzt nach einem PPPoE-Access-Concentrator an der Schnittstelle eth0 gesucht...



A horizontal progress bar with a red segment on the left and a blue segment on the right. The text "36%" is centered in the blue segment.

DSL-VERBINDUNG GEFUNDEN

Es wurde ein Access-Concentrator an der Schnittstelle eth1 gefunden. Soll eine PPPoE-Verbindung für diese Schnittstelle eingerichtet werden?

Konfiguration - Debian - DSL



Konfiguration - Debian - DSL

ÜBLICHE OPTIONEN

Die meisten Leute benutzen für die üblichen Dialup-Verbindungen die Optionen 'noauth' und 'defaultroute' in ihrer Konfiguration, und entfernen die Option 'nodetach'. Soll ich ihre Konfigurationsdatei überprüfen und die genannten Einstellungen ggf. anpassen?

<Ja>

<Nein>

Konfiguration - Debian - DSL

BENUTZERNAMEN EINGEBEN

Bitte geben Sie den Benutzernamen ein, den Sie normalerweise zum Einloggen bei ihrem Provider benötigen. Zum Anzeigen der Hilfe den Benutzernamen löschen und OK drücken.

00xxxxxx32xxx#0001@t-online.de

PASSWORT EINGEBEN

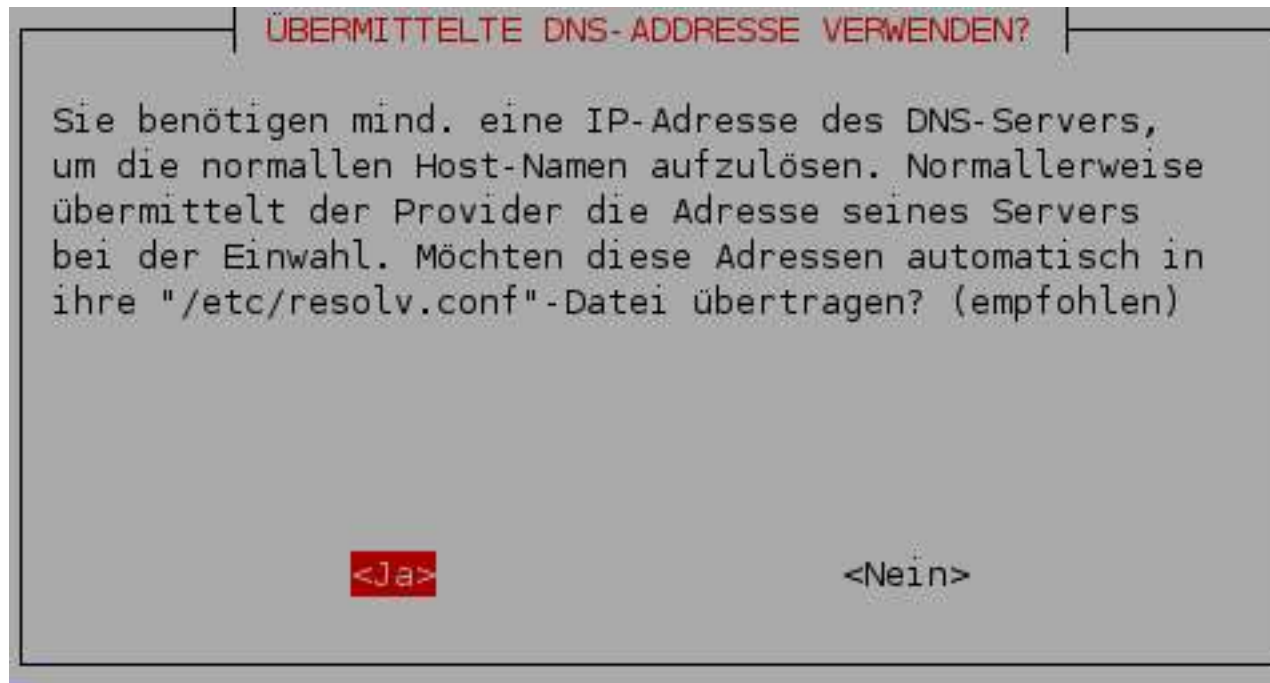
Bitte geben Sie das Passwort ein, das Sie normalerweise zum Einloggen bei ihrem Provider benötigen.

WICHTIG: das Passwort wird während der Eingabe angezeigt!

geheim

<ok>

Konfiguration - Debian - DSL



Konfiguration - Debian - DSL

PROBLEM MIT BESCHRÄNKTER MSS

Viele Provider haben Router, die nur TCP-Pakete mit MSS-Grösse von mehr also 1460 nicht unterstützen. Normalerweise ist das ausreichend für Standard-Verbindungen über genau eine Ethernet-Verbindung mit der Standard-MTU-Grösse (1500). Machen Sie aber Weiterleitung für andere Rechner (z.B. bei Masquerading), kann die MSS-Grösse je nach Paketgrösse und Route zum Client überschritten werden. Deswegen können die Clients bestimmte Adressen nicht mehr erreichen. Es gibt auch eine Lösung: pppoe kann die Grösse der ausgehenden Pakete beschränken. Mehr Details darüber finden Sie in der pppoe-Doku.

Soll pppoe die MSS-Grösse auf 1452 festlegen?

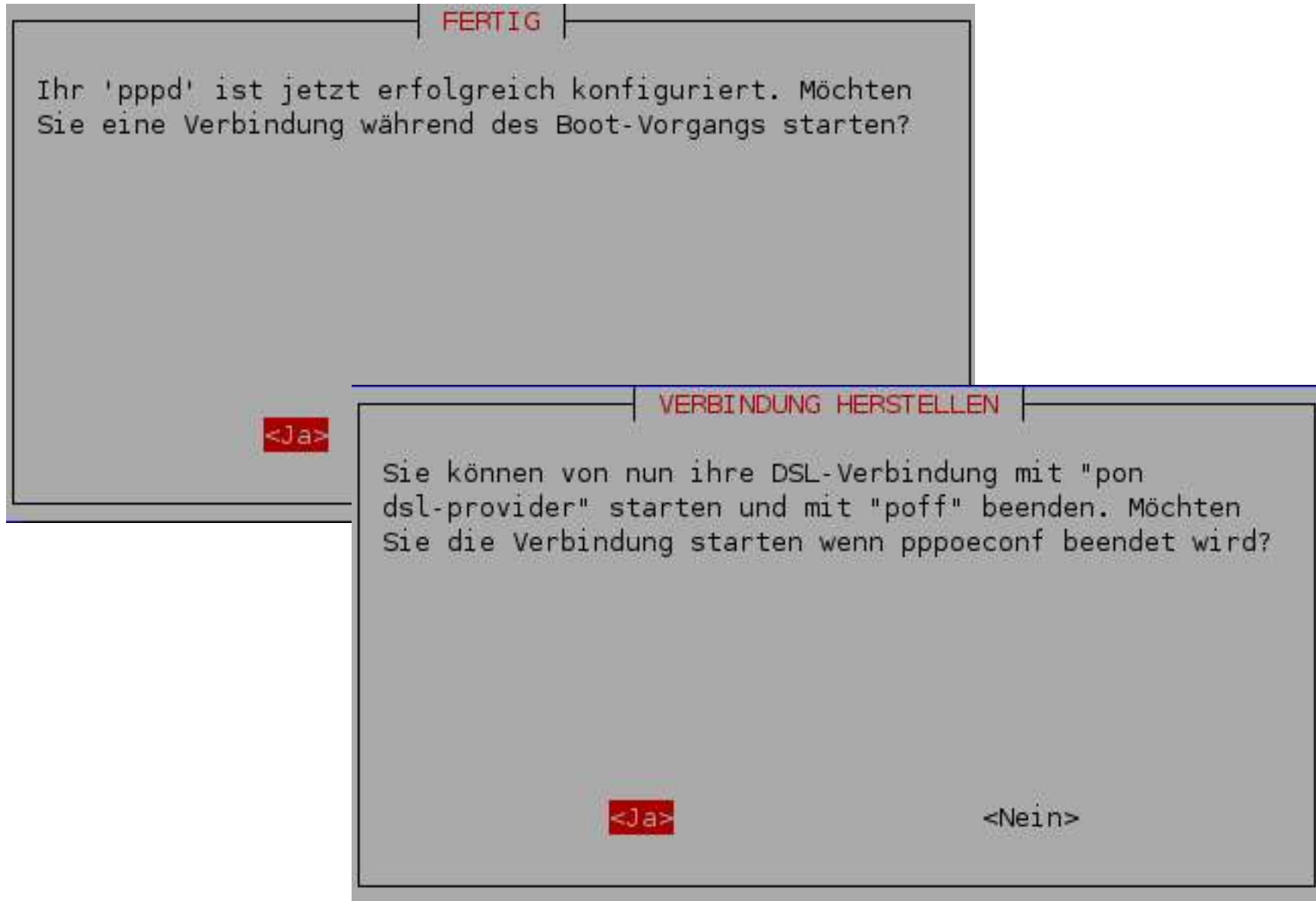
In Zweifelsfall eher Ja.

(Falls Sie weiterhin das oben beschriebenen Probleme bekommen,

<Ja>

<Nein>

Konfiguration - Debian - DSL



Konfiguration - Debian - DSL



Funktionstest I

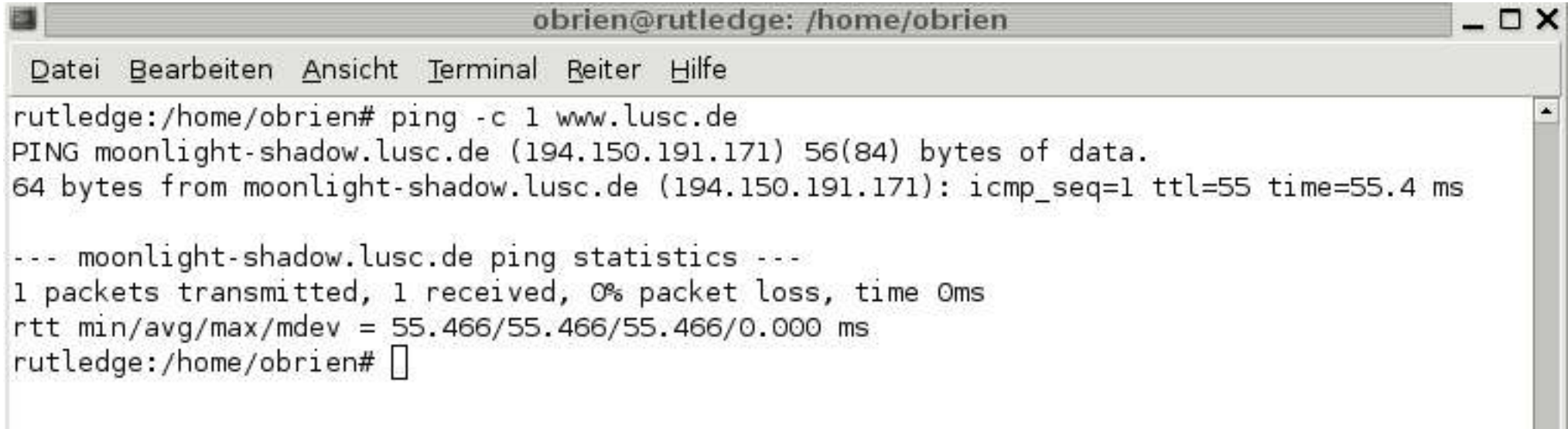


```
obrien@rutledge: /home/obrien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/home/obrien# pon dsl-provider
Plugin rp-pppoe.so loaded.
RP-PPPoE plugin version 3.3 compiled against pppd 2.4.2
rutledge:/home/obrien# ifconfig ppp0
ppp0      Protokoll:Punkt-zu-Punkt Verbindung
          inet Adresse:212.114.238.251  P-z-P:212.114.214.1  Maske:255.255.255.255
          UP PUNKTZUPUNKT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:3
          RX bytes:54 (54.0 b)  TX bytes:108 (108.0 b)

rutledge:/home/obrien#
```

bei SUSE dsl0 verwenden

Funktionstest II

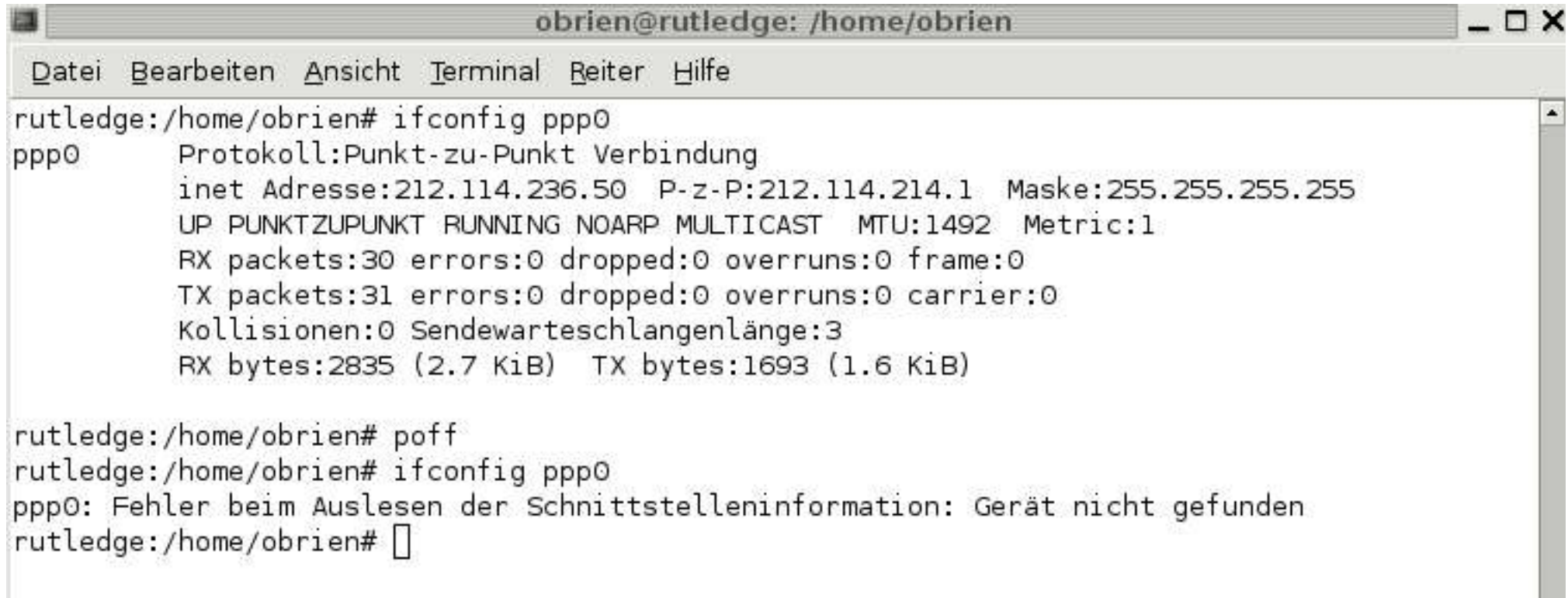


```
obrien@rutledge: /home/obrien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/home/obrien# ping -c 1 www.lusc.de
PING moonlight-shadow.lusc.de (194.150.191.171) 56(84) bytes of data.
64 bytes from moonlight-shadow.lusc.de (194.150.191.171): icmp_seq=1 ttl=55 time=55.4 ms

--- moonlight-shadow.lusc.de ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 55.466/55.466/55.466/0.000 ms
rutledge:/home/obrien#
```

Namensauflösung klappt

Verbindung trennen



```
obrien@rutledge: /home/obrien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/home/obrien# ifconfig ppp0
ppp0      Protokoll:Punkt-zu-Punkt Verbindung
          inet Adresse:212.114.236.50  P-z-P:212.114.214.1  Maske:255.255.255.255
          UP PUNKTZUPUNKT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 Sendewarteschlangenlänge:3
          RX bytes:2835 (2.7 KiB)  TX bytes:1693 (1.6 KiB)

rutledge:/home/obrien# poff
rutledge:/home/obrien# ifconfig ppp0
ppp0: Fehler beim Auslesen der Schnittstelleninformation: Gerät nicht gefunden
rutledge:/home/obrien#
```

Fehlersuche

```
obrien@rutledge: /home/obrien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/home/obrien# route -n
Kernel IP Routentabelle
Ziel          Router      Genmask      Flags Metric Ref    Use Iface
212.114.214.1 0.0.0.0    255.255.255.255 UH    0      0      0 ppp0
192.168.1.0   0.0.0.0    255.255.255.0  U     0      0      0 eth1
0.0.0.0       212.114.214.1 0.0.0.0      UG    0      0      0 ppp0
rutledge:/home/obrien#
```

Falls keine Defaultroute vorhanden ist

```
route add default gw 212.114.214.1 ppp0
```

```
obrien@rutledge: /home/obrien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/home/obrien# cat /etc/resolv.conf
nameserver 212.114.152.1
nameserver 212.114.153.1
search
rutledge:/home/obrien#
```

Wie steht es um die Sicherheit?

Welche Dienste sind erreichbar?

(telnet, ssh, smtp, rpc, ident, nfs, samba)

„nmap localhost“ zeigt was läuft

Also, alles abschalten, das nicht gebraucht wird.

<http://www.debian.org/doc/manuals/securing-debian-howto/>

Wer hat Angst vor dem Portscan?

Paketfilter mit iptables (ab Kernel 2.4)

„Minimalistische Firewall“

```
iptables -A INPUT -p tcp --syn -i ppp0 -j DROP
```

Grafische Konfigurationstools:

lokkit, Knetfilter, Kmyfirewall

Mit mehreren Rechnern ins Netz

Geht das überhaupt? Wir haben doch nur eine IP vom Provider bekommen.

Klar, dafür gibt es NAT. (Network Address Translation)

IP-Adressen von Datenpaketen aus dem internem Netz werden mit der externen des Routers ersetzt

Die Antwortpakete werden vom Router wieder an die entsprechenden Rechner im internen Netz zugestellt

Rechner als DSL-Router I

Man nehme:

- einen 'alten Rechner'
- zwei Netzwerkkarten
- aktuelle Linuxdistribution (alternativ IPCop, FLI4L)
- Zeit

Rechner als DSL-Router II

```
obrien@rutledge: /home/obrien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/home/obrien# cat /etc/network/options
ip_forward=yes
spoofofprotect=yes
syncookies=no
rutledge:/home/obrien# cat /proc/sys/net/ipv4/ip_forward
1
rutledge:/home/obrien#
```

```
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
rutledge:/etc/ppp/ip-up.d# cat filter
#!/bin/sh

iptables -F

iptables -t nat -A POSTROUTING -o ppp0 -s 192.168.1.0/24 -j MASQUERADE
iptables -A INPUT -p tcp --syn -i ppp0 -j DROP

rutledge:/etc/ppp/ip-up.d#
```

Rechner als DSL-Router III

- Client muss im selben Subnetz wie Router (192.168.1.1) sein
- IP-Adresse des Routers als Defaultgateway eintragen
- `route add default gw 192.168.1.1 eth0`
- DNS des Providers in `/etc/resolv.conf` eintragen

Wie geht es weiter?

- Paketfilter weiter konfigurieren (Dienste von aussen erreichbar machen)
- Bandbreitenmanagement (QoS, Trafficshaping) z.B. wondershaper

Zum Nachlesen

- www.debiananwenderhandbuch.de
- www.google.com/linux
- iptables - www.netfilter.org
- Bandbreitenmanagement - www.lartc.org