

Universität Ulm
Institut für Organisation und Management von
Informationssystemen

Praktikum
„Informations- und Medientechnik “
Sommersemester 2007

Gruppe 4: Adelheid Grob & Christian Renz

Vorversuch 1
durchgeführt am: 2. Mai 2007

1 Fragen zur Vorbereitung

1.1 Aufbau von *Manpages* unter Linux

Manpages unter Linux sind folgendermassen aufgebaut:

- **NAME** Zunächst wird der Name des Befehls kurz erläutert.
- **SYNOPSIS** Danach erfolgt die Angabe der Synopsis, d.h. wie der Befehl zu gebrauchen ist.
- **DESCRIPTION** Als nächstes wird der Befehl ausführlich beschrieben und alle möglichen Optionen, die dem Befehl mit gegeben werden können, erläutert.
- **FUNCTION LETTERS** und **OTHER OPTIONS** Bei einigen manpages gibt es für die Optionen und Funktionen extra Unterkapitel: **FUNCTION LETTERS** und **OTHER OPTIONS**
- **BUGS** Falls Bugs bekannt sind, werden diese hier aufgeführt.
- **OUTPUT FORMAT** Bei Kommandos, die eine Ausgabe erzeugen, wird diese in den Manpages unter **OUTPUT FORMAT** näher erläutert.
- **AUTHOR** Hier wird der Author des Kommandos erwähnt.
- **REPORTING BUGS** Diese Feld enthält Verfahrenshinweise sowie Kontaktmöglichkeiten für das Auftreten eines (nicht menschlichen) Bugs.
- **COPYRIGHT** Unter dieser Überschrift werden Copyright-Informationen zusammengefasst.
- **SEE ALSO** Hier werden Hinweise zu weiteren Kommandos oder Infoseiten, die artverwandt zum eigentlichen Befehl sind, gesammelt.
- **EXAMPLES** Bei manchen umfangreicheren Manpages gibt es zudem noch ein paar Beispiele, wie das Kommando zu benutzen ist.

1.2 IP-Adresse, Subnetzmaske und Default-Gateway

Die **IP-Adresse** dient dazu, einen Rechner in einem Netz eindeutig "identifizieren" zu können. Gebräuchlich sind hierbei entweder `ipv4`- oder `ipv6`-Adressen. Als Beispiel für eine `ipv4`-Adresse sei die 217.10.0.11 (32 Bit) genannt, für eine `ipv6`-Adresse `cd80:2000:0201:8033:fe3d:1957:a24a:52ea` (128 Bit).

Die **Subnetzmaske** wird verwendet, um Netzwerke richtig routen zu können. Je nachdem, wie groß ein Netz ist (z.B. ein `/27` Netz) läßt sich die Netzmaske errechnen. Die Netzmaske eines `/27` Netzes hat in binärer Schreibweise 27 führende Einsen. Bilden man eine

logische **AND**-Verknüpfung einer IP-Adresse des Netzes mit der Netzmaske erhält man den sogenannten "Netzwerkteil" - dieser Teil der IP-Adressen im entsprechenden Netz ist immer derselbe! Bei einem /27-Netz bleiben noch 5 Bits "übrig" ($32-27=5$). Aus diesen kann man nun ganz leicht die Anzahl der im entsprechenden Netz zur Verfügung stehenden IP-Adressen errechnen als $2^5 = 32$. Für die Adressierung von Rechnern können davon 30 genutzt werden.

Das **Default-Gateway** leitet alle nicht zu einem Subnetz gehörenden Netzwerkanfragen in ein anderes Subnetz weiter.

1.3 Broadcastadresse

Die Broadcastadresse dient dazu, jedem Rechner in einem bestimmten Netzwerk gleichzeitig eine Nachricht schicken zu können. Sie wird ermittelt, in dem alle Hostbits auf 1 gesetzt werden; die Broadcastadresse ist also die höchstmögliche IP-Adresse in einem Netz.

1.4 IP- und MAC-Adressen

IP- und MAC(media-access-control)-Adressen beziehen sich auf verschiedenen Layer im OSI-ISO-Schichtenmodell. MAC wird so dem Layer 2 zugeordnet, IP dem Layer 3. Die MAC-Adresse ist eine Hardware-Adresse, damit wird jedes Interface eines Rechners (z.B. Ethernetkarte oder WLANKarte) eindeutig benannt. Eine MAC-Adresse besteht aus 48 Bit und wird hexadezimal geschrieben: ein Beispiel hierfür ist 00:50:04:46:7A:F2. Hätte ein Netz nur IP-Adressen, gäbe es zum einen keine Adressierung auf Layer 2 mehr und zum anderen viel Chaos, denn IP-Adressen sind leicht fälschbar. Gäbe es hingegen nur MAC-Adressen, wäre das Netz an sich sehr chaotisch - mithilfe von nicht-geräte-gebunden Adressen (IP-Adressen) kann ein Netzwerk strukturiert aufgebaut werden. Das erleichtert das Routing eines Pakets immens. Außerdem ist es auf IP-Ebene egal, welches Protokoll auf der Ebene darunter liegt.

1.5 Loopback Device

Ein Loopback Device ist quasi ein Ringschluß eines Systems/Rechners mit sich selbst. Die hierfür verwendete IP-Adresse lautet 127.x.x.x, häufig wird die 127.0.0.1 benutzt. Mit ihr ist es möglich, seinen Rechner intern direkt anzusprechen (z.B. genutzt, damit Serverdienste mit Clientdienste auf derselben Maschine kommunizieren können). Auch zum Testen kann diese Adresse verwendet werden.

1.6 Rechnerei Teil I

Laut RFC 1219 ist die Subnetzmaske 255.255.255.1 nicht zulässig, von daher kann keine Aussage getroffen werden.

1.7 Rechnerei Teil II

Es können die folgenden Netze gebildet werden:

- 192.168.1.0
- 192.168.1.64
- 192.168.1.128
- 192.168.1.192

1.8 Klassen / CIDR

Die Einteilung in Klassen wurde früher bei der Vergabe von IP-Adressbereichen angewandt. Es wurde eine Einteilung in die vier Klassen A, B und C getroffen. Klasse A hat die Netzmaske 255.0.0.0, Klasse B 255.255.0.0 und Klasse C 255.255.255.0. D.h. in einem Netz der Klasse A können 2^{23} Adressen vergeben werden, in einem Klasse-B-Netz 2^{15} und in einem Klasse C Netz 2^7 . Da diese Einteilung von Netzen sehr grob ist und viele IP-Adressen so auch verschwendet wurden, wird diese Einteilung nicht mehr getroffen bei der Vergabe. Es wird inzwischen feiner abgestuft (/27-Netze z.B., CIDR [Classless Inter-Domain Routing])

Die Universität Ulm hatte früher ein Klasse B-Netz, inzwischen aber ein /16-Netz, d.h. es stehen 65536 Adressen zur Verfügung, was sehr gut ausreichend ist.

1.9 Routingtabellen

Eine Routingtabelle enthält Informationen zu

- den erreichbaren Adressen im Netz
- den Wegen dorthin
- den Kosten der einzelnen Wege
- den Verbindungsarten zu anderen Stationen im Netz

Sie sieht z.B. so aus:

```
corona:~>netstat -r
```

```
Routing Table: IPv4
```

Destination	Gateway	Flags	Ref	Use	Interface	
134.60.1.0	corona.rz.uni-ulm.de	U	1	79487	bge0	
134.60.1.0	gcg.rz.uni-ulm.de	U	1	0	bge0:66	
134.60.1.0	login.rz.uni-ulm.de	U	1	0	bge0:41	
BASE-ADDRESS.MCAST.NET	corona.rz.uni-ulm.de	U		1	0	bge0
default	1-gw-vrrp.rz.uni-ulm.de	UG		1	87113	
localhost	localhost	UH	49	489351	lo0	

```
corona:~>
```

Die erste Spalte "Destination" bezeichnet die möglichen Ziele. "Gateway" bezeichnet die IP-Adresse an die sich ein Paket wenden muß um zum Ziel zu gelangen (next hop). Die dritte Spalte "Flags" enthält Informationen über die Schnittstelle, wie z.B. U für UP oder G für GATEWAY. Die vierte Spalte "Ref" sagt aus, wie oft diese MAC-Adresse in der Routingtabelle referenziert wird. Die fünfte Spalte ist "Use" und sagt wie viele Pakete über diese Schnittstelle gegangen sind. Die letzte Spalte "Interface" zeigt das Device an, das ein Paket nehmen muß.

1.10 ICMP

ICMP (Internet Control Message Protocol) dient dazu, Fehler- und Informationsmeldungen des Internetprotokolls zu protokollieren. Es wird u.a. beim ping verwendet.

1.11 ARP/RARP

ARP und RARP sind Protokolle, die der Adressauflösung dienen. Will man ein Paket an einen Rechner schicken, von dem man nur die IP-Adresse kennt, wird ein ARP-Request per MAC-Broadcast an alle Stationen im Netz gesendet - die Station, welche die gewünschte IP-Adresse besitzt, sendet daraufhin Ihre MAC-Adresse zurück (ARP-Reply).

RARP liefert analog die IP-Adresse zu einer bekannten MAC-Adresse (des eigenen Rechners).

1.12 Vorgehensweise ICMP

Ein ICMP-Echo-Request wird beim Ausführen von ping versendet. Wenn der angepingte Rechner online ist, erhält man als Antwort einen ICMP-Echo-Reply. ping ausgeführt auf die entsprechende Maschine sieht wie folgt aus:

```
root@heidi:~# ping www.uni-ulm.de
PING www.uni-ulm.de (134.60.1.25) 56(84) bytes of data.
```

```
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=1 ttl=250 time=1.67 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=2 ttl=250 time=1.58 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=3 ttl=250 time=1.58 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=4 ttl=250 time=1.61 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=5 ttl=250 time=1.66 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=6 ttl=250 time=1.54 ms
```

```
--- www.uni-ulm.de ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5053ms
rtt min/avg/max/mdev = 1.543/1.610/1.679/0.052 ms
root@heidi:~#
```

Im Detail passiert dabei folgendes:

1. Ermitteln der MAC-Adresse des Default-Gateways mittels ARP-Request
2. Echo-ICMP-Paket an Router 1 senden
3. Router 1 ermittelt anhand seiner Routing-Tabellen mögliche weitere (Zwischen-)Station: Router 2 (evtl. muss er dazu noch mit arp request die MAC-Adresse des Routers 2 ermitteln)
4. Senden des Pakets an Router 2
5. Router 2 ermittelt wiederum die nächste Station aus den Routingtabellen: Router 3
6. Senden des Pakets an Router 3
7. Router 3 "kennt" das Ziel und sendet das Paket an 134.60.1.25 (www.uni-ulm.de)

2 Versuchsdurchführung

2.1 Versuchsteil 1: Konfiguration der Netzwerkkarte

Im ersten Versuchsteil konfigurieren wir unsere Netzwerkkarte. Hierzu führen wir folgende Befehle aus:

```
videoshow:~# ifconfig eth0 10.4.1.2
videoshow:~# route add default gw 10.4.1.100
```

Ifconfig trägt die Subnetzmaske (255.255.255.0) und die daraus resultierende Broadcastadresse (10.4.1.255) selbst ein.

Diese Konfiguration haben wir erfolgreich mit einem ping getestet.

2.2 Versuchsteil 2: Address Resolution Protocol

Um alle Einträge der ARP-Tabelle anzeigen zu lassen, muss

```
videoshow:~# arp -a
```

aufgerufen werden, um Einträge zu löschen,

```
root@heidi:~# arp -d hostname
```

aufgerufen werden.

Zunächst erscheinen beim Aufruf von `arp -a` keine Einträge:

```
videoshow:~# arp -a
```

```
videoshow:~#
```

Nun schicken wir einen Broadcastping an die Rechner im gleichen Subnetz und schauen uns danach die Einträge in der ARP-Tabelle an.

```
videoshow:~# ping -b 10.4.1.1
```

```
videoshow:~# arp -a
```

```
videotalk.itm.e-technik.uni-ulm.de (10.4.1.1) auf 00:10:DC:FE:7A:C1 [ether] auf eth0
```

```
videomax.itm.e-technik.uni-ulm.de (10.4.1.100) auf 00:E0:81:22:51:F3 [ether] auf eth0
```

```
videoshow:~#
```

videomax ist das Gateway und videotalk der Rechner von Christian. Beide sind in der ARP-Tabelle aufgeführt, da an beide ein ARP-Request geschickt wurde. Es wurden von diesen beiden Rechnern die MAC-Adressen gespeichert. Das Speichern hat den Vorteil, dass nicht ständig ARP-Requests gesendet werden müssen. Da bei einer Änderung der Interfaces bzw. der Zuordnung Interface - IP-Adresse Probleme auftreten, werden die MAC-Adressen nur ein paar Minuten gespeichert.

Danach haben wir einen ping an `www.uni-ulm.de` geschickt. Die ARP-Tabelle sieht nach diesem Ping unverändert aus:

```
videoshow:~# ping www.uni-ulm.de
```

```
PING www.uni-ulm.de (134.60.1.25) 56(84) bytes of data.
```

```
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=1 ttl=252 time=1.84 ms
```

```
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=2 ttl=252 time=2.27 ms
```

```
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=3 ttl=252 time=1.90 ms
```

```
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=4 ttl=252 time=1.98 ms
```

```
--- www.uni-ulm.de ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3012ms
```

```
rtt min/avg/max/mdev = 1.843/2.001/2.272/0.164 ms
```

```
videoshow:~# arp -a
```

```
videotalk.itm.e-technik.uni-ulm.de (10.4.1.1) auf 00:10:DC:FE:7A:C1 [ether] auf eth0
```

```
videomax.itm.e-technik.uni-ulm.de (10.4.1.100) auf 00:E0:81:22:51:F3 [ether] auf eth0
```

```
videoshow:~#
```

Die ARP-Tabelle ändert sich nicht, da die Anfrage an `www.uni-ulm.de` von dem Router direkt weitergeleitet wird.

2.3 Versuchsteil 3: ICMP

Im letzten Versuchsteil senden wir an verschiedene Adressen pings und schauen uns die Antwortzeiten an.

- `www.uni-ulm.de`

```
videoshow:~# ping www.uni-ulm.de
PING www.uni-ulm.de (134.60.1.25) 56(84) bytes of data.
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=1 ttl=252 time=21.8 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=2 ttl=252 time=1.95 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=3 ttl=252 time=2.04 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=4 ttl=252 time=20.9 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=5 ttl=252 time=1.92 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=6 ttl=252 time=1.99 ms

--- www.uni-ulm.de ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 1.929/8.459/21.864/9.165 ms
videoshow:~#
```

- `www.heise.de`

```
videoshow:~# ping www.heise.de
PING www.heise.de (193.99.144.85) 56(84) bytes of data.
64 bytes from www.heise.de (193.99.144.85): icmp_seq=1 ttl=246 time=13.6 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=2 ttl=246 time=12.7 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=3 ttl=246 time=12.4 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=4 ttl=246 time=12.8 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=5 ttl=246 time=12.6 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=6 ttl=246 time=14.6 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=7 ttl=246 time=12.2 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=8 ttl=246 time=12.8 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=9 ttl=246 time=12.5 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=10 ttl=246 time=12.6 ms
64 bytes from www.heise.de (193.99.144.85): icmp_seq=11 ttl=246 time=12.5 ms

--- www.heise.de ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10036ms
rtt min/avg/max/mdev = 12.262/12.903/14.675/0.652 ms
videoshow:~#
```


Der Rechner `www.ecu.edu.au` hat dagegen schon eine sehr lange Antwortzeit. Wenn man mithilfe des Programms `mtr` den `traceroute` zu diesem Server anschaut, zeigt sich, daß es zwischen den Stationen 6 und 7 einen extremen Anstieg gibt:

```
My traceroute [v0.67]
heidi (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00) Wed May 2 16:04:52 2007
Resolver error: Nameserver packet truncated.ics Order of fields quit
Host Loss% Snt Last Avg Best Wrst StDev
1. fe---2.Rx2.N25.ObE.IN-Ulm.DE 0.0% 140 0.1 0.1 0.1 0.7 0.1
2. 129.143.87.42 0.0% 140 1.6 45.2 0.8 469.8 104.8
3. POS1-0-0.ulmxs05.rz-mu13.ulm.spxs.net 0.0% 140 0.9 11.8 0.8 214.0 38.9
4. GiE6-2.ulmxs06.Mu13.ulm.spxs.net 0.0% 140 1.1 1.9 0.8 74.5 6.2
5. GiE5-1.ffmxs11.ix ffm.spxs.net 0.0% 139 5.9 10.2 5.7 200.2 24.1
6. ge-3-2-0.bb1.a.fra.aarnet.net.au 0.7% 139 6.8 7.1 6.4 13.8 0.8
7. so-0-1-0.bb1.a.sin.aarnet.net.au 0.0% 139 218.6 212.8 210.6 254.4 6.6
8. so-3-3-0.bb1.a.per.aarnet.net.au 0.0% 139 261.9 263.9 260.5 298.6 3.9
9. gigabitethernet0.er1.ecu.cpe.aarnet.net.au 0.0% 139 280.4 279.7 272.2 404.4 14.3
10. gw1.er1.ecu.cpe.aarnet.net.au 0.0% 139 271.9 268.0 260.7 309.7 5.7
11. 139.230.253.6 0.0% 139 271.4 269.7 265.9 310.1 4.3
12. ???
13. ???
14. ???
15. communitygeneticsinasia.com 0.0% 139 261.8 268.5 261.5 320.1 6.9
```

Dieser Anstieg rührt wahrscheinlich daher, daß die Verbindung über Satellit weitergeführt wird.

Zuletzt haben wir versucht, `www.hawaii.edu` zu pingen. Dieser Versuch scheint zu scheitern (100% loss), das kann daran liegen, daß entweder der Rechner offline ist oder daß die ICMP-Pakete nicht beantwortet werden. Da die Webseite aufrufbar war, nehmen wir zweiteres an.