

ITM-Praktikum - Vorversuch

Andreas Klingler, Hannes Stahl, Simon Lüke

13. Januar 2010

Inhaltsverzeichnis

1	vorbereitende Fragen	2
1.1	Teil 1	2
1.2	Teil 2	4
2	Versuchsdurchführung	6
2.1	Teil 1	6
2.1.1	Konfiguration der Netzwerkkarte	6
2.1.2	Adress Resolution Protocol (ARP)	7
2.1.3	Internet Control Message Protocol (ICMP)	8
2.2	Teil 2	9
2.2.1	Mitschreiben des Netzwerkverkehrs	9
2.2.2	Internet Protocol (IP)	9
2.2.3	TCP vs UDP	10
2.2.4	Domain Name Service (DNS)	10

1 vorbereitende Fragen

1.1 Teil 1

1. Aufbau einer **Manpage**:

Nach der Bedeutung des Befehls werden die möglichen Optionen aufgelistet. Eckige Klammern weisen auf Optionalität hin. Es folgt eine allgemeine Beschreibung und eine genaue Erklärung der Optionen. Nach Ausnahmen und Besonderheiten folgen noch weitere Angaben zum Exit Status und/oder Geschichte des Befehls. Hilfreich ist auch der Bereich 'Siehe auch' für weitere Befehle in diesem Kontext.

Der Aufbau einer Manpage anhand einiger möglicher Abschnitte ist im folgenden aufgelistet:

MAN (1)	Manual Hilfsprogramme	MAN (1)
NAME		
SYNTAX		
BESCHREIBUNG		
BEISPIELE		
UEBERSICHT		
NORMALEINSTELLUNGEN		
OPTIONEN		
UMGEBUNG		
DATEIEN		
EXIT STATUS		
SIEHE AUCH		
FEHLER		
GESCHICHTE		
2.5.2	2008-05-05	MAN (1)

2. **IP-Adresse**: IP steht für Internetprotokoll. Die Adresse wird verwendet, um einen Rechner im Netz anzusprechen. Gebräuchlich sind IPv4-Adressen aus vier durch Punkte getrennte Zahlen zwischen 0 und 255 und lässt sich somit durch 32 bit darstellen. **Subnetz**: Unterteilt IP-Adressbereiche mittels einer *bitmaske* in 'Unternezte'. Gesetzte Bits der Sunnetzmaske definieren den Netzteil, nicht gesetzte den Hostteil innerhalb des Netzes. **Default-Gateway**: Teilnehmer, über den die Rechner eines Subnetzes andere Subnetze erreichen

können / mit dem ganzen Netz kommunizieren. Alle Pakete, die nicht auf Grund der Informationen der Routingtabelle des Senders losgeschickt werden können, werden über das Default-Gateway geleitet.

3. Die **Broadcastadresse** ist die letzte / höchste IP-Adresse des Subnetzes (alle Bits im Hostteil sind gesetzt). Über sie können Pakete an alle Rechner des Subnetzes gesendet werden. Ein Broadcast ist ein Rundruf an alle Teilnehmer des Subnetzes und wird z.B. verwendet, wenn der genaue Empfänger noch nicht bekannt ist (z.B. bei DHCP).
4. **MAC-Adresse:** ist an die Hardware (Ethernetkarte) gebunden. Es können per MAC-Adresse nur Rechner des selben Subnetzes angesprochen werden (sofern sie bekannt sind). Mit MAC-Adressen sind Punkt-zu-Punkt Verbindungen möglich, bei denen die Teilnehmer direkt miteinander kommunizieren können. **IP-Adresse:** wird *dynamisch* per Software vergeben. Die IP Adresse dient dem Routing und ermöglicht so Transparenz im ISO/OSI-Modell, d.h. es kann unabhängig von verwendeter oder ausgetauschter Hardware adressiert werden.
Über MAC-Adressen kommunizieren Teilnehmer, die direkt miteinander Verbunden sind (Punkt-zu-Punkt-Verbindung). IP-Adressen sind hierarchisch aufgebaut und ermöglichen die Adressierung eines Rechners, der nicht direkt (per MAC-Adresse) angesprochen werden kann → *routing*.
5. Ein **Loopback-Device** schleift eine Nachricht zum Sender zurück. Es wird v.a. zum Testen der grundlegenden eigenen Netzwerkfunktion (Software/Betriebssystem-Stack) verwendet oder um Dienste nur lokal verfügbar zu machen. Meist wird 127.0.0.1 als IP-Adresse dafür verwendet.
6. Der Rechner kann nur jeden zweiten Teilnehmer des Subnetzes erreichen und zwar nur die mit einer ungeraden Dezimalzahl im 4. / niedrigsten Oktett. Die Subnetzmaske ist allerdings ungültig, es dürfen nur führende Bits verwendet werden.
7. Mit einem **/26-Subnetz** können die 4 Netze

```
192.168.1.0
192.168.1.64
192.168.1.128
192.168.1.192
```

gebildet werden.

8. IP-Adressen wurden in die folgenden **Netzklassen** eingeteilt:

```
Netzbereich der Klasse A: 0.0.0.0 - 127.255.255.255
Netzbereich der Klasse B: 128.0.0.0 - 191.255.255.255
Netzbereich der Klasse C: 192.0.0.0 - 223.255.255.255
Netzbereich der Klasse D: 224.0.0.0 - 239.255.255.255
Netzbereich der Klasse E: 240.0.0.0 - 255.255.255.255
```

Die Uni hat ein Klasse B Netz, was mit 65.534 möglichen Adressen auch bis jetzt ausreichend ist. Mti der einföhrung von *CIDR* (1993) wurde diese Einteilung aufgehoben.

9. Mit **CIDR** (Classless Inter-Domain Routing) wurde die feste Einteilung in Netzklassen abgeschafft, wodurch Netzgrößen in passender Größe zu den angeforderten Adressanzahlen der 'Kunden' vergeben werden können, anstatt der Netzklassen werden Subnetze einfach

flexibel mit Hilfe der Subnetzmasken gebildet. Routingtabellen können kleiner werden, da IP-Adressen geografisch sortiert vergeben werden und daher weniger Einträge in den Tabellen nötig sind. Die Netzmasken können auch in der Suffix-Notation angegeben werden. /24 steht für 24 Eins-Bits in der Netzmaske und entspricht damit also 255.255.255.0

10. Die **Routingtabelle** beinhaltet Einträge die mindestens aus folgenden Einträgen bestehen:
- einem zu erreichenden Zielnetz (Netzadresse und Subnetzmaske),
 - dem nächsten Router (Gateway),
 - sowie der Schnittstelle, über welche das Zielnetz erreichbar ist.

Dadurch ist es einem Rechner oder Router erst möglich Pakete über das eigene Subnetz hinaus zu versenden.

11. Das **Internet Control Message Protocol** enthält Methoden zur Netzwerk-Diagnose (Fehlermeldungen und Informationssammlung). ICMP ist eigentlich ein Teil des IP-Protocols, wird aber auch getrennt behandelt. Am bekanntesten ist wohl der Befehl *ping*, der den Echo-Request des ICMP nutzt, um die Erreichbarkeit anderer Teilnehmer zu überprüfen. Außer diesem Echo-Request lösen ICMP-Pakete keine weiteren ICMP-Nachrichten aus.

12. **ARP** (Address Resolution Protocol) ordnet einer IP Adresse die zugehörige MAC-Adresse zu. In der ARP-Tabelle sind alle bekannten Zuordnungen des eigenen Subnetzes aufgelistet. Ist zu einer IP-Adresse noch keine MAC-Adresse vorhanden, so wird ein Broadcast mit der eigenen IP-Adresse und der IP-Adresse, zu der die MAC-Adresse gesucht wird losgeschickt, worauf hoffentlich der Rechner mit der gesuchten MAC-Adresse eine Antwort (also die zur IP gehörige MAC-Adresse) liefert.

RARP (Reverse Address Resolution Protocol) kann bei bekannter MAC-Adresse die zugehörige IP-Adresse auflösen.

13. Ablauf beim schicken eines ICMP-Pakets (Echo Request) aus dem Praktikumsnetz an 134.60.1.25 (www.uni-ulm.de).
- Rechner 1 (IP A) findet in seiner eigenen Routing Tabelle keinen Eintrag für die gewünschte IP und wählt deshalb Router 1 (IP B.1) als Gateway.
 - Rechner 1 sucht in seiner ARP-Tabelle die zur IP B.1 gehörige MAC-Adresse und schickt das Paket los.
 - Router 1 nimmt das Paket an und kann die Ziel-IP, wiederum nicht in seiner Routing-Tabelle finden, also nutzt er ein weiteres Gateway (Router 2), Auflösung der MAC-Adresse wie oben.
 - Router 2 und 3 gehen genau so vor.
 - Router 3 jedoch ist mit einer Netzwerkschnittstelle im Selben Subnetz wie der Zielrechner und kann den Echo-Request direkt zustellen.

1.2 Teil 2

1. **Paketsniffing** dient zum 'mithören' von Paketen des Netzwerkverkehrs. Es kann zu folgenden Zwecken dienen:

- Diagnose von Problemen im Netzwerk
- Aufdecken von Einbruchsversuchen
- Analyse des Datenverkehrs
- Filterung verdächtiger Nachrichten
- Datenspionage.

2. Im **Promiscuous Mode** werden alle an der Netzwerkschnittstelle eingehenden Pakete empfangen und an das Betriebssystem weitergegeben, auch jene, die nicht für den Rechner bestimmt waren (per MAC-Adresse).
3. **Hub**: sendet alle eingehende Pakete an allen angeschlossenen Geräte weiter.
Switch: verteilt jedes eingehende Pakete an den korrekten Adressaten des Subnetzes (MAC-Adress-Ebene).
Router: kann mittels Informationen der Routing-Tabelle (IP-Adress-Ebene) auch Pakete über Subnetze hinaus weiterleiten.
4. Monitor-Port oder Mirroring-Port eines Managed Switch nutzen oder die MAC-Adresse des abzuhörenden Rechners fälschen.
5. Packet-Sniffer am Hub im Gegensatz zu einem Switch: Da im Switch die Nachrichten nicht an alle Ports kopiert werden, kann man mit einem Sniffer hier nicht ohne weiteres den gesamten Verkehr mitschneiden. Ausserdem kann man mit zahlreichen Anfragen für unterschiedliche MAC-Adressen den Speicher des Switches volllaufen lassen, dadurch wird er zum Hub und sendet alle Pakete an alle Ports
6. SSH bietet eine Authentifizierung der Kommunikationspartner und Verschlüsselung des Datenverkehrs, wogegen Telnet im 'Klartext' überträgt.
7. **Ethernet-Frame** enthält:
 - a) Ziel-MAC-Adresse
 - b) Quellen-MAC-Adresse
 - c) VLAN-Tag: ?
 - d) Typ: IPv4, IPv6, ARP, ...
 - e) Daten: 0-1500 Byte, hier ist z.B. das IP-Paket enthalten.
 - f) PAD-Füllfeld: ?
 - g) CRC-PrüfsummeAußer dem aktuellen Ethernet 802.3 Standard, gibt es den Vorgänger Ethernet 2 und Tagged-MAC-Frames.
8. **IP-Paket** enthält
 - a) Version
 - b) IHL (IP Header Length)
 - c) TOS (Type Of Service)
 - d) Total Length
 - e) Identification
 - f) Flags
 - g) Fragment Offset
 - h) TTL (Time To Live)
 - i) Protocol (IP)
 - j) Header Checksum
 - k) Source Address
 - l) Destination Address
 - m) Options and Padding (optional)
 - n) Datenteil

Das **TTL Feld** gibt die max. Anzahl der Hops an, bis das Paket verworfen wird. Damit kann verhindert werden, dass ein Paket 'ewig' geroutet wird, falls es nicht zum Zielhost gelangt, sollte eine Route im Kreis verlaufen.

9. Mittels des DNS-Eintrags wird einer IP-Adresse ein leicht zu merkender Name zugeordnet, ausserdem wird location transparency möglich: Name bleibt gleich, IP bzw. Server ändert sich. Ohne das **Domain Name System** müsste, um eine Website aufzurufen die IP-Adresse des Servers eingegeben werden.
10. Von einem Nameserver muss die IP bekannt sein, er kann nicht von einem Host aufgelöst werden, da er ja gerade zur Namensauflösung dienen soll (analog zum Henne-Ei-Problem).
11. **Primäre und Sekundäre Nameserver** ermöglichen Redundanz und Lastverteilung bei Anfragen von Clients. Ein Nachteil ist jedoch, dass der Sekundäre Nameserver die Änderungen des Primären Nameservers, auf dem die Änderungen des Einträge vorgenommen werden, nachziehen muss.
12. Speichert ein **Caching-Nameserver** die IP-Adress-Namens-Zuordnung zwischen und aktualisiert diese eben nicht korrekt mit dem zuständigen Nameserver, kann evtl. ein Name nicht korrekt aufgelöst werden: eine URL zeigt auf einen falschen oder nicht mehr vorhandenen Rechner. Dieser Nachteil wird wieder mit einer TTL versucht zu verringern, nachdem ein gecacheter Eintrag ungültig wird.
13. Bei der **dynamischen Vergabe von IP-Adressen** in einem Netzwerk, müssen die Nameservereinträge ständig aktualisiert werden. Mittels DynDNS-Diensten kann dieser Nachteil umgangen werden.

2 Versuchsdurchführung

2.1 Teil 1

2.1.1 Konfiguration der Netzwerkkarte

Nach der Löschung der laufenden Konfiguration sollten folgende Einstellungen (wieder-)hergestellt werden:

Der Host sollte die IP 10.5.40.1 mit Netzmaske 255.255.255.0 bekommen.

Als Default Gateway sollte der Router 10.5.40.99 eingetragen werden.

Ersteres erreichen wir über folgenden ifconfig-Befehl:

```
multirouter: # ifconfig eth0 10.5.40.1 netmask 255.255.255.0
```

Das Default Gateway taucht zwar in der Routingtabelle mit 0.0.0.0 auf, muss aber mit einem speziellen Befehl angelegt werden:

```
multirouter: # route add default gw 10.5.40.99
```

Abschließend lassen wir uns zur Kontrolle mit

```
multirouter: # route -n
```

die Kernel IP Routentabelle anzeigen:

Ziel-Adresse	Router-Adresse	zugeh. Genmask	Flags	Metric	Ref	Use	Iface
10.5.40.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	10.5.40.99	0.0.0.0	UG	0	0	0	eth0

2.1.2 Adress Resolution Protocol (ARP)

Die Anzeige der ARP-Tabelle erfolgt mit dem Programm arp durch die Option -n
multirouter: # arp -n

```
Address HWtype HWaddress Flags Mask Iface
10.5.40.99 ether 00:E0:7D:B4:A5:87 C eth0
```

Zur Löschung des Eintrags gaben wir

```
multirouter: # arp -d 10.5.40.99
```

ein und ließen uns die Tabelle erneut anzeigen:

```
multirouter: # arp -n
Address HWtype HWaddress Flags Mask Iface
10.5.40.99 (unvollständig) eth0
```

Nach einem Broadcast-Ping:

```
multirouter: # ping -b 10.5.40.255
WARNING: pinging broadcast address
PING 10.5.40.255 (10.5.40.255) 56(84) bytes of data.
```

worauf der Router offenbar nicht reagierte, versuchten wir, ihn direkt zu erreichen:

```
multirouter: # ping 10.5.40.99
PING 10.5.40.99 (10.5.40.99) 56(84) bytes of data.
64 bytes from 10.5.40.99: icmp_seq=1 ttl=64 time=0.295 ms
```

Dies gelang nun und dadurch aktualisierte sich auch die ARP-Tabelle:

```
multirouter: # arp -n
Address HWtype HWaddress Flags Mask Iface
10.5.40.99 ether 00:E0:7D:B4:A5:87 C eth0
```

Die MAC-Adresse des Routers wurde erneut abgespeichert. Vorteil dieser Speicherung ist, dass nicht bei jedem Aufruf die MAC-Adresse nicht erneut abgefragt werden muss. Nachteile können jedoch bei Änderung der Hardware entstehen, so dass solche Einträge sinnvollerweise nur Minuten erhalten bleiben.

Durch das pingen der Webadresse `www.uni-ulm.de`

```
multirouter: # 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=0.440 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=2 ttl=252 time=0.536 ms
```

kam es nicht zu einer Änderung in der ARP-Tabelle, da der Webserver nicht direkt angesprochen wird.

2.1.3 Internet Control Message Protocol (ICMP)

Ping wird oft zur Messung der Verzögerung, die ein Netzwerk aufweist, verwendet. So pingten wir abschließend in diesem ersten Vorversuchsteil unterschiedliche Webserver auf der ganzen Welt an:

Der Uniserver hatte Zeiten von ca. einer halben Millisekunde:

```
multirouter: # ping -c 3 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=0.459 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=2 ttl=252 time=0.523 ms
64 bytes from www.rz.uni-ulm.de (134.60.1.25): icmp_seq=3 ttl=252 time=0.534 ms
```

```
— www.uni-ulm.de ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.459/0.505/0.534/0.037 ms
```

Der heise.de-Server lag bei ca. 10 ms:

```
multirouter: # ping -c 3 heise.de
PING heise.de (193.99.144.80) 56(84) bytes of data.
64 bytes from redirector.heise.de (193.99.144.80): icmp_seq=1 ttl=245 time=10.2 ms
64 bytes from redirector.heise.de (193.99.144.80): icmp_seq=2 ttl=245 time=9.49 ms
64 bytes from redirector.heise.de (193.99.144.80): icmp_seq=3 ttl=245 time=12.6 ms
```

```
— heise.de ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 9.495/10.796/12.646/1.346 ms
```

Nicht werreicht werden konnten die Adressen in Australien und auf Hawaii.

```
multirouter: # ping -c 3 www.ecu.edu.au
PING prod.web.ecu.edu.au (139.230.244.59) 56(84) bytes of data.
```

```
— prod.web.ecu.edu.au ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2008ms
```

```
multirouter: # ping -c 3 www.hawaii.edu
PING web00.its.hawaii.edu (128.171.224.100) 56(84) bytes of data.
```

```
— web00.its.hawaii.edu ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

Da diese Server aber zumindest als Webserver agieren, ist es wahrscheinlich, dass sie so konfiguriert sind, keine Antwort auf einen Ping zu liefern.

Google z.B. reagierte wie heise.de im Bereich weniger ms:

```
multirouter: # ping -c 3 www.google.de
PING www.l.google.com (74.125.39.99) 56(84) bytes of data.
64 bytes from fx-in-f99.google.com (74.125.39.99): icmp_seq=1 ttl=243 time=10.0 ms
64 bytes from fx-in-f99.google.com (74.125.39.99): icmp_seq=2 ttl=243 time=9.96 ms
64 bytes from fx-in-f99.google.com (74.125.39.99): icmp_seq=3 ttl=243 time=13.2 ms
```

```
— www.l.google.com ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 9.967/11.090/13.230/1.516 ms
```

2.2 Teil 2

2.2.1 Mitschreiben des Netzwerkverkehrs

Mit dem Paket-Sniffer Wireshark ließen wir uns im Promiscuous Mode Pakete in Echtzeit anzeigen. Wireshark ist in der Lage, uns alle Ethernet-Pakete anzuzeigen. ARP wurden nicht ausgetauscht, da die Mac-Adresse noch gespeichert war. Wenn es aber zum Austausch von ARP-Paketen kommt, so folgt auf ein request ein reply. Bei uns fragte der Router nach der Mac-Adresse des Hosts, dieser antwortete an den Router zurück. Die übertragenen Informationen enthalten Sender- und Empfänger-IP-Adresse und ermöglicht so die Verknüpfung und das Abspeichern und ermöglichen Rückschlüsse auf die Erreichbarkeit.

Wireshark kann die Hersteller der Ethernet-Karten erkennen. Das liegt daran, dass die Hersteller bestimmte Adressbereiche für ihre Geräte erhalten, deren erste 6 Hex-Zahlen sich dann zuordnen lassen. Bei uns hatte der Host (10.5.40.1) eine Karte von 3Com, der Router (10.5.40.99) eine von Netronix.

Im TCP-Stream einer Telnet-Session sollte das Passwort unverschlüsselt übertragen werden. Wireshark scheint dies jedoch im Plain Text nicht mehr anzuzeigen. Wir wurden allerdings im Hex-Code fündig. Auffallend ist, dass jeder Tastendruck sofort verarbeitet wird, also ebenfalls Vertipper und Korrekturen. In der SSH Sitzung konnten wir das Passwort nicht mehr entdecken.

2.2.2 Internet Protocol (IP)

Im Header eines IP-Pakets erkannten wir die einzelnen Bereiche, wie in den Vorbereitungsfragen geschildert. Länge beträgt 213 Byte, 20 davon benötigt der Header. Es handelte sich im IPv4, es war eine TTL angegeben, anhand von checksum correct sahen wir, dass das Paket korrekt

übertragen wurde.

Das Programm traceroute ist in der Lage, die Strecke eines Pakets über Router anzuzeigen. Wir testeten das am Beispiel des Uni-Webservers. traceroute versendet dazu Pakete mit zunehmender TTL, so dass auch Fehlermeldungen von den zwischenliegenden Routern zurückgegeben werden. Auf diese Art kann der Weg eines Paketes verfolgt werden. Zu www-hawaii.com ist die Route länger und so werden die Rückmeldungen auch deutlich verzögert. Ein Sprung ist bei Satellitenverbindungen zu erkennen, wenn z.B. der erste US-Server erreicht wird. Auch wenn sich manche Rechner keine Rückmeldung liefern, so leiten sie Meldungen anderer Router doch weiter und somit kann die Route bis auf wenige Lücken dargestellt werden.

2.2.3 TCP vs UDP

in diesem Versuchsteil riefen wir eine Webseite auf und analysierten die TCP-Pakete. Auffällig bei einem TCP-Stream ist hier ein dreifach-Handshake um sicher zu gehen, dass die Verbindung steht. Eine derartige "virtuelle Verbindung" über ein weiterhin paketorientiertes Protokoll gibt es bei UDP nicht. Durch den Verzicht auf Synchronisation (SYN) und Acknowledgement (ACK) ist UDP für Dienste wie VoIP besser geeignet, büßt damit aber an Verlässlichkeit ein.

2.2.4 Domain Name Service (DNS)

Für einen ping an imap.uni-ulm.de muss die Adresse aufgelöst werden. imap.uni-ulm.de ist ein Alias-Name. Der Kanonische Name ist mail.uni-ulm.de der mittels DNS aufgeschlüsselt wird zu 134.60.1.11. DNS benutzt dazu UDP auf Port 53. Unterschiedliche Namen werden im DNS durch Records ermöglicht (Z.B. A Resource Record). Auch gibt es einen Eintrag "Time to live", der das Ansammeln veraltete Einträge verhindert. Üblich sind Zeiten von ca. 2 Tagen.

Unter Umständen können in der Netzwerkschnittstelle auch ICMP-Nachrichten auftauchen, die nicht vom aktuellen Befehl herrühren. Dies können Nachrichten sein, dass die TTL erreicht, eine Warteschlange voll oder das Ziel nicht erreichbar war.