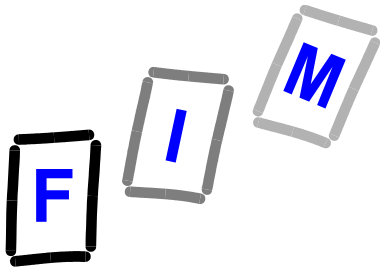


SS 2004

KV Betriebssysteme

(Rudolf Hörmanseder, Michael Sonntag)

IP (Minifassung)

ICMP

Internet Control Message Protocol

ICMP Basisaufgaben

- IP bietet ja „nur“ verbindungslose und unsichere Übertragung an.

Damit wichtig:

- Informationen über Fehler und deren Behandlung
- Steuerung des Datentransfers
- Diagnose

ICMP arbeitet selber über IP

Auswahl aus den ICMP Nachrichten

- **<u>Destination Unreachable:</u> Paket kann nicht zugestellt werden (Fragmentation needed but DF=1 / Network / Host / Protocol / Port / ...)**
- **<u>Time Exceeded:</u> TTL ist abgelaufen (=> TRACEROUTE), Fragment Reassembly Time**
- **<u>Echo Request / Reply:</u> Fragt per Request ein System, ob es noch am Leben ist. Dieses antwortet mit Reply. (=> PING)**
- **<u>Timestamp Request / Reply:</u> Wie Echo, aber mit Zeitstempel**

Wozu dient die TTL? [1] (TTL=Time To Live)

Wozu wird die TTL benötigt:

- **Pakete, welche z.B. durch Routingfehler "im Kreis" gesendet werden, werden verworfen (und kreisen damit nicht endlos im Netz).**

`E:\>ping www.fim.uni-linz.ac.at` `Reply from 140.78.100.130: TTL=128`	(NT, gleiches Netz)
`E:\>ping fimlinux02.fim.uni-linz.ac.at` `Reply from 140.78.100.170: TTL=255`	(Suse Linux, gleiches Netz)
`E:\>ping mail.fim.uni-linz.ac.at` `Reply from 140.78.100.3: TTL=127`	(NT, 1 Hop dazwischen)
`E:\>ping pserv.fim.uni-linz.ac.at` `Reply from 140.78.100.45: TTL=14`	(Axis Printserver, 1 Hop dazwischen)
`E:\>ping www.uni-linz.ac.at` `Reply from 140.78.3.23: TTL=126`	(2 Hops dazwischen)

Wozu dient die TTL? [2] (TTL=Time To Live)

- Routingfehler (Kreise, siehe vorige Folie)
- Sicherstellen, daß Paket-Lifetime limitiert
  - ein Beispiel dazu folgt: ID & Fragmentierung
- bei Multicasts ...
- Traceroute Utility

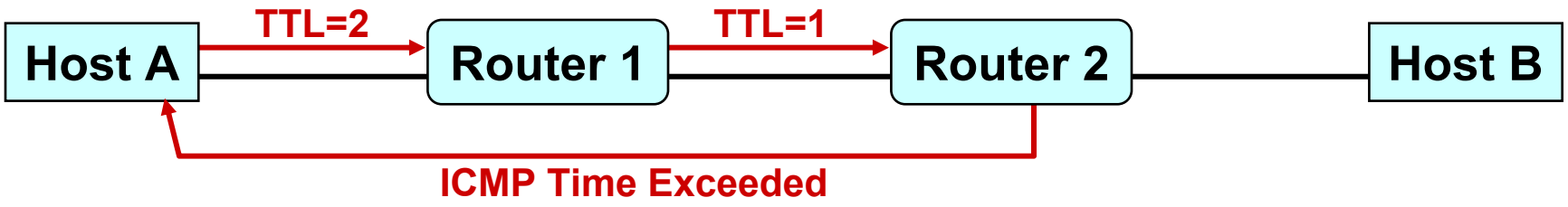
Anmerkungen:

- heute nicht mehr TTL sondern Hop-Count
- Größe + Zählmode:
  - IP V4: 8 Bits, count-down
  - IP V6: nur??!! 8 Bits, count-down
  - IPX: 8 Bits, count-up
  - Appletalk: nur!! 4 Bits, count-up

Beispiel: TTL & ICMP (TTL=Time To Live)

- Jeder Knoten (auf dem Weg eines IP-Paketes) zählt die TTL um (mindestens) 1 nach unten.
- Erreicht der Wert 0, so wird das Paket verworfen und (zumeist) eine ICMP-Nachricht als Fehlernachricht zurückgeschickt.

  (Natürlich löst ein Fehler bei einer ICMP-Nachricht selbst keine ICMP-Nachricht mehr aus.)



PING & TRACEROUTE

(als spätere Verbindung von ICMP zum Routing)

PING
Syntax und Optionen

```
PING [optionen] Zielliste
```

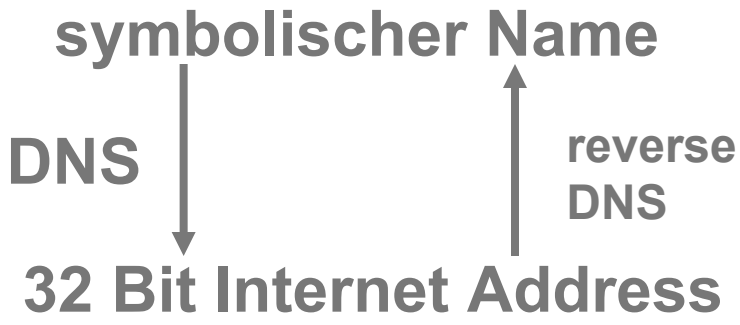
-t	Sendet fortlaufend Ping-Signale
-a	Adressen zu Host-Namen auswerten
-n Anzahl	Anzahl zu sendender Echo-Anforderungen
-l Länge	Pufferlänge senden
-f	Flag für "Don't Fragment" setzen
-i TTL	Time To Live.
-v TOS	Type Of Service.
-r Anzahl	Route für Anzahl Hops aufzeichnen
-s Anzahl	Zeiteintrag für Anzahl Abschnitte (Hops)
-j Host-Liste	"Loose Source Route" gemäß Host-Liste
-k Host-Liste	"Strict Source Route" gemäß Host-Liste
-w Timeout	Timeout in Millisekunden für eine Antwort

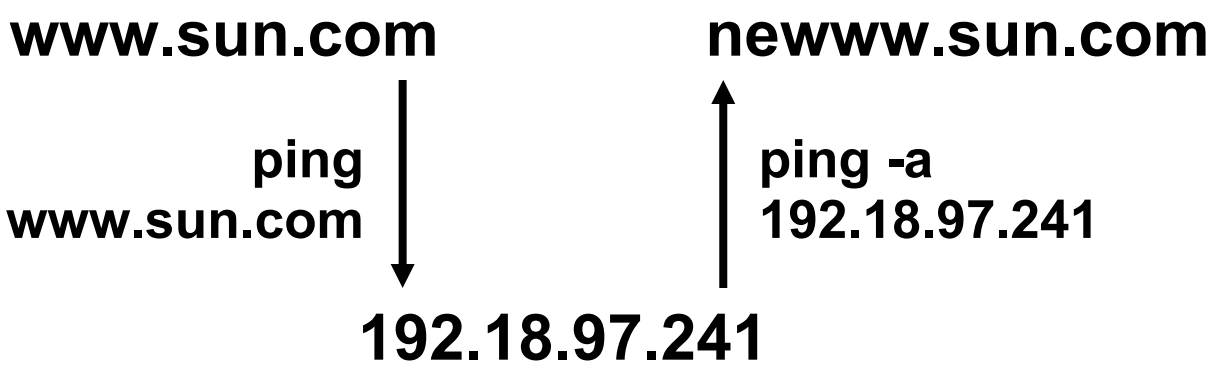
PING Beispiel
Round-Trip-Time (RTT)

```
L:\users\hoe>ping www.sun.com
Pinging www.sun.com [192.18.97.241] with 32 bytes of data:
Reply from 192.18.97.241: bytes=32 time=591ms TTL=228
Reply from 192.18.97.241: bytes=32 time=601ms TTL=228
Reply from 192.18.97.241: bytes=32 time=491ms TTL=228
Reply from 192.18.97.241: bytes=32 time=551ms TTL=228

L:\users\hoe>ping -a 192.18.97.241
Pinging newww.sun.com [192.18.97.241] with 32 bytes of data:
Reply from 192.18.97.241: bytes=32 time=451ms TTL=228
Reply from 192.18.97.241: bytes=32 time=511ms TTL=228
Reply from 192.18.97.241: bytes=32 time=511ms TTL=228
Reply from 192.18.97.241: bytes=32 time=871ms TTL=228

L:\users\hoe>_
```

PING Beispiel mit Switch -a

- **Switch -a: IP-Adresse (via reverse DNS) auf Host-namen auslösen**





PING Kompatibilität Grenzbereich Broadcasts [1]

- **SUSE Linux 6.3 mit IP 140.78.100.147/25**

```
hoe@linux04: > ping -c 2  140.78.100.255
PING 140.78.100.255 (140.78.100.255): 56 data bytes
64 bytes from 140.78.100.147: icmp_seq=0 ttl=255 time=0.447 ms
64 bytes from 140.78.100.138: icmp_seq=0 ttl=255 time=0.920 ms (DUP!)
64 bytes from 140.78.100.150: icmp_seq=0 ttl=63 time=6.292 ms (DUP!)
64 bytes from 140.78.100.147: icmp_seq=1 ttl=255 time=0.164 ms
--- 140.78.100.255 ping statistics ---
2 packets transmitted, 2 packets received, +2 duplicates,
0% packet loss, round-trip min/avg/max = 0.164/1.955/6.292 ms
```

Anmerkungen:

Nur Linux-Systeme (140.78.100.147 und 140.78.100.138) sowie ein System von Bay Networks (140.78.100.150) antworten. Die Windows-Systeme (98 / NT 4 / 2000) reagieren nicht.
Der Suse-Rechner antwortet auch sich selbst, sodaß das ping auch ohne Anschluß an das Netz Replies (ohne Duplicates) erhält.

PING Kompatibilität Grenzbereich Broadcasts [2]

- **Windows 2000 mit IP 140.78.100.145/25**

```
L:\users\hoe>ping  -n 2 140.78.100.255
Pinging 140.78.100.255 with 32 bytes of data:
Reply from 140.78.100.255: bytes=32 time<10ms TTL=255
Reply from 140.78.100.255: bytes=32 time<10ms TTL=255
Ping statistics for 140.78.100.255:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Anmerkungen:

Der Protocol-Analyzer zeigt, daß die Duplicates genau wie in der vorigen Folie über das Netz gehen. Das Ping von Windows 2000 zeigt aber nichts davon an. Der Rechner antwortet sich aber nicht selbst, sodaß ein PING ohne Anschluß an das Netzwerk mit „Request timed out“ beantwortet wird.

Verfolgen der (einer??) Route von A nach B [1]

- **Möglichkeit 1: PING mit Angabe der TTL (-i)**

```
C:\>PING -n 1 www.suse.com
Reply from 202.58.118.8: bytes=32 ... TTL=228

C:\>PING -n 1 -i 1 www.suse.com
Reply from 140.78.100.31: TTL expired in transmit.

C:\>PING -n 1 -a 140.78.100.31
Pinging routerzid.fim.uni-linz.ac.at [ ...

C:\>PING -n 1 -i 2 www.suse.com
Reply from 193.171.22.17; TTL expired in transmit.

C:\>PING -n 1 -a 193.171.22.17
Pinging Linz.ACO.net [ ...
```

Verfolgen der (einer??) Route von A nach B [2]

<u>Möglichkeit 1:</u> PING mit Angabe der TTL (-i)

```
...
...
C:\>PING -n 1 -i 23 www.suse.com
Reply from 198.32.128.81: TTL expired in transmit.
C:\>PING -n 1 -a 198.32.128.81
Pinging oak-rtr.dtelecom.com [ ...

C:\>PING -n 1 -i 24 www.suse.com
Request timed out.

C:\>PING -n 1 -i 25 www.suse.com
Reply from 202.58.118.8: bytes=32 ... TTL=228
```

Verfolgen der (einer??) Route von A nach B [3]

<u>Möglichkeit 2:</u> eigenes Tool TRACEROUTE

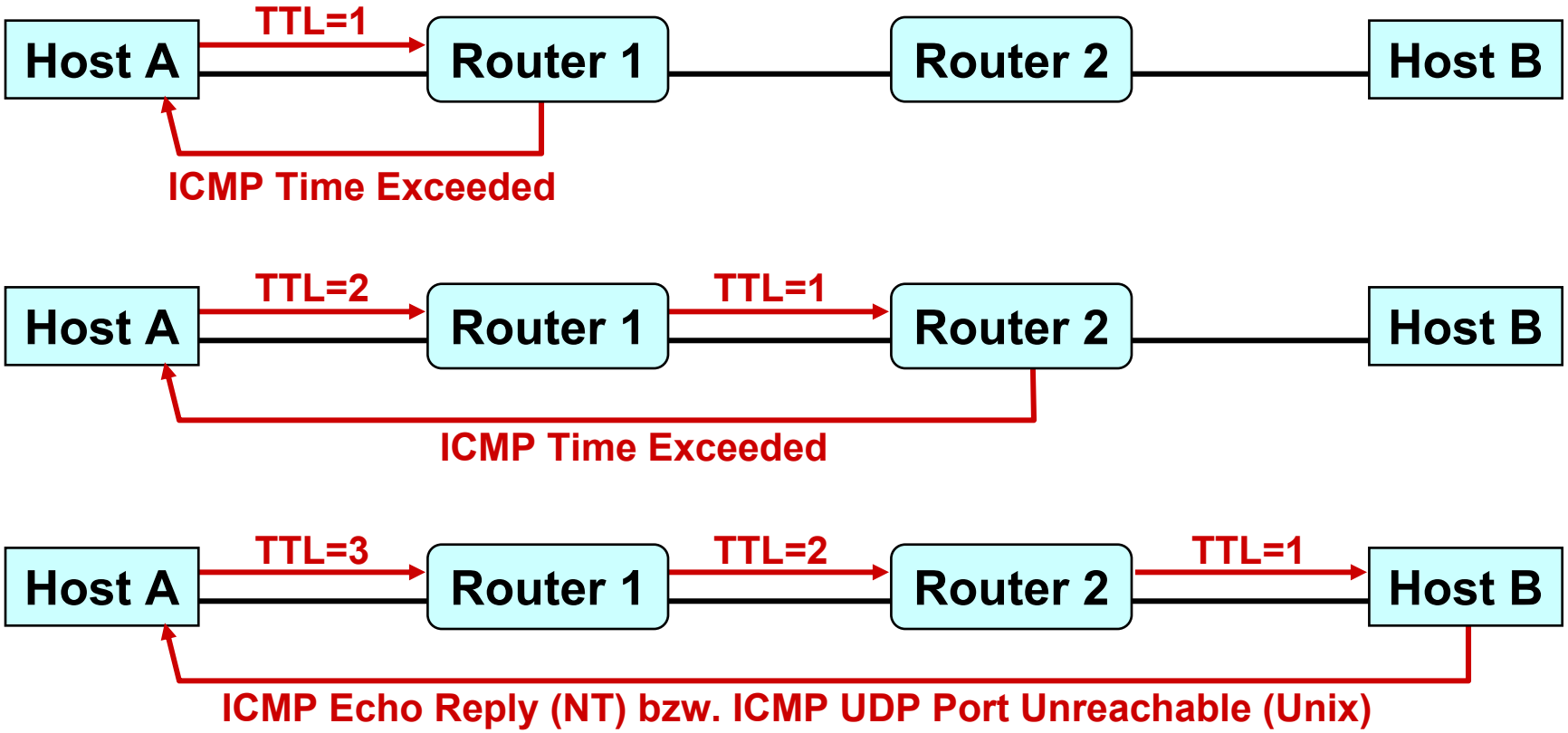
- **Funktion: Zeichnet auf Basis der ICMP-Messages „TTL Exceeded in Transmit“ bzw. „Port Unreachable“ die (besser gesagt eine) Route auf.**

- **Einige Optionen des Tools:**

`-d`	Adressen nicht zu Host-Namen auswerten
`-h hops`	max. Anzahl an Hops bei Zielsuche
`-j hostlist`	"Loose Source Route" gemäß hostlist
`-w Timeout`	Timeout in Millisekunden für eine Antwort

Verfolgen der (einer??) Route von A nach B [4]

Wie funktionieren PING und TRACEROUTE?



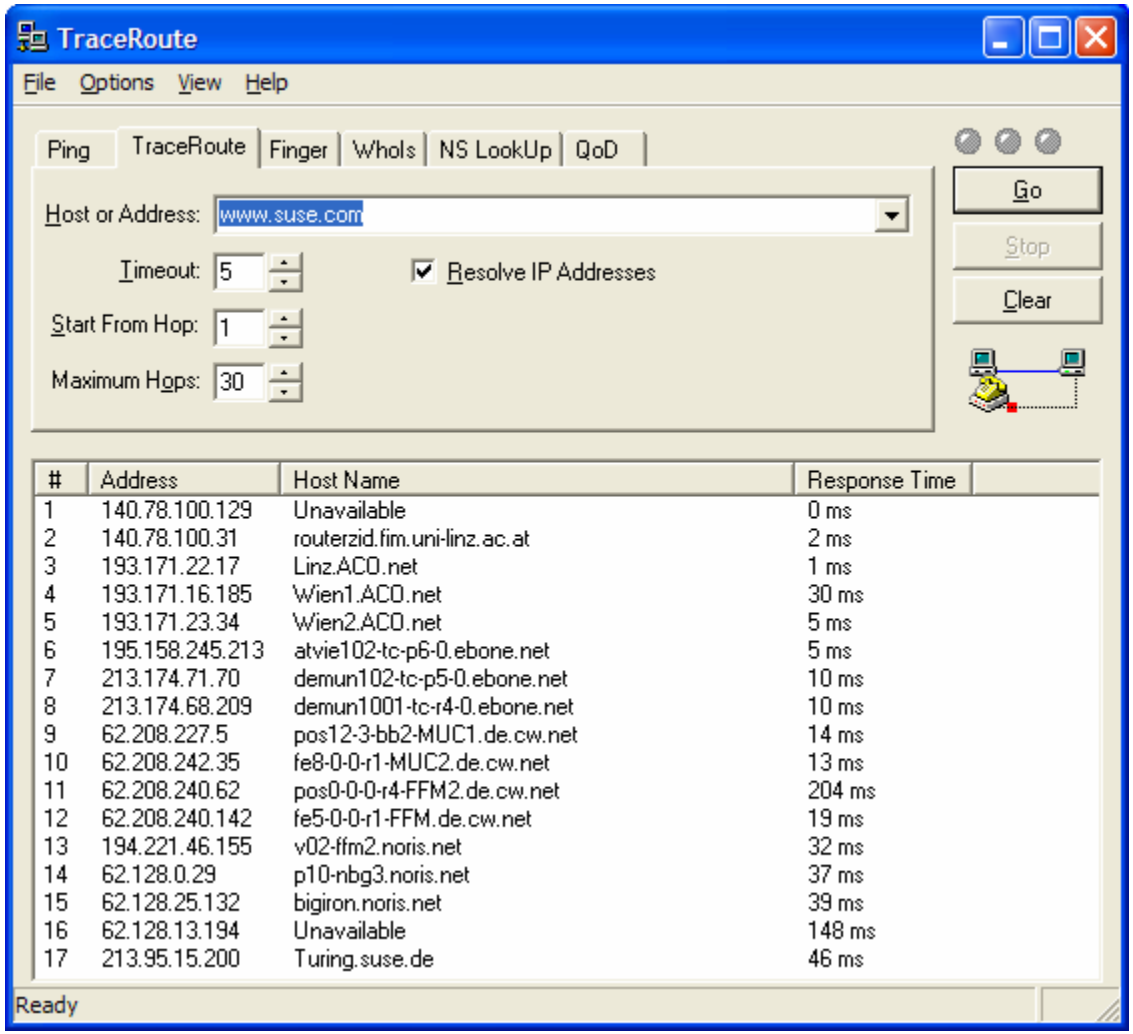
(übernommen von Windows 2000 Online Help)

Arbeiten mit TRACEROUTE [1]

```
L:\users\hoe>tracert www.suse.com

Tracing route to www.suse.com [202.58.118.8]
over a maximum of 30 hops:
  1  <10  <10  <10  routerzid.fim.uni-linz.ac.at [140.78.100.31]
  2  <10  <10  <10  linz.aco.net [193.171.22.17]
  3   20   10   10  Vienna-RBS.ACO.net [193.171.25.13]
  4  <10  <10  <10  atvie203-tc-f2-2.ebone.net [195.158.245.129]
  5   10   10   10  atvie101-tc-p0-2.ebone.net [213.174.70.2]
  6   10   10   10  czpra103-tc-p2-0.ebone.net [195.158.242.45]
  7   20   20   20  debln302-tc-p2-0.ebone.net [213.174.70.45]
 ..
 11   30   31   30  nlams303-tc-p2-0.ebone.net [213.174.70.134]
 12   30   30   30  bebru203-tc-p1-0.ebone.net [195.158.225.85]
 ..
 23  180  191  190  oak-rtr.dtelecom.com [198.32.128.81]
 24    *    *    *  Request timed out.
 25  921  958 1012  www1.SuSE.com [202.58.118.8]

Trace complete.
```

(Millisekunden-Bezeichner etc. für bessere Darstellung im Output entfernt)

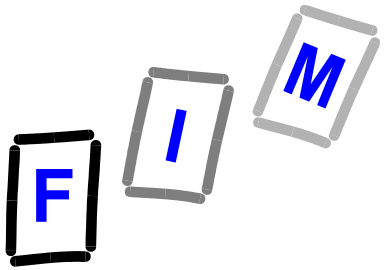
Arbeiten mit TRACEROUTE [2]



~ 1,5 Jahre später

mehrere Unterschiede:

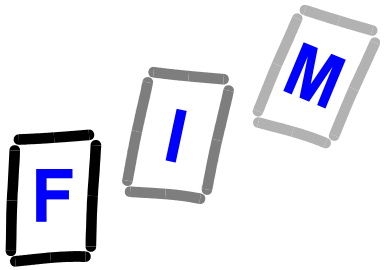
- **ein Router zwischen Rechner und UNI-Netz**
- **andere IP und damit andere (kürzere) Route**
- **Geschwindigkeits-unterschiede**
- **...?**



Basis-Test von IP

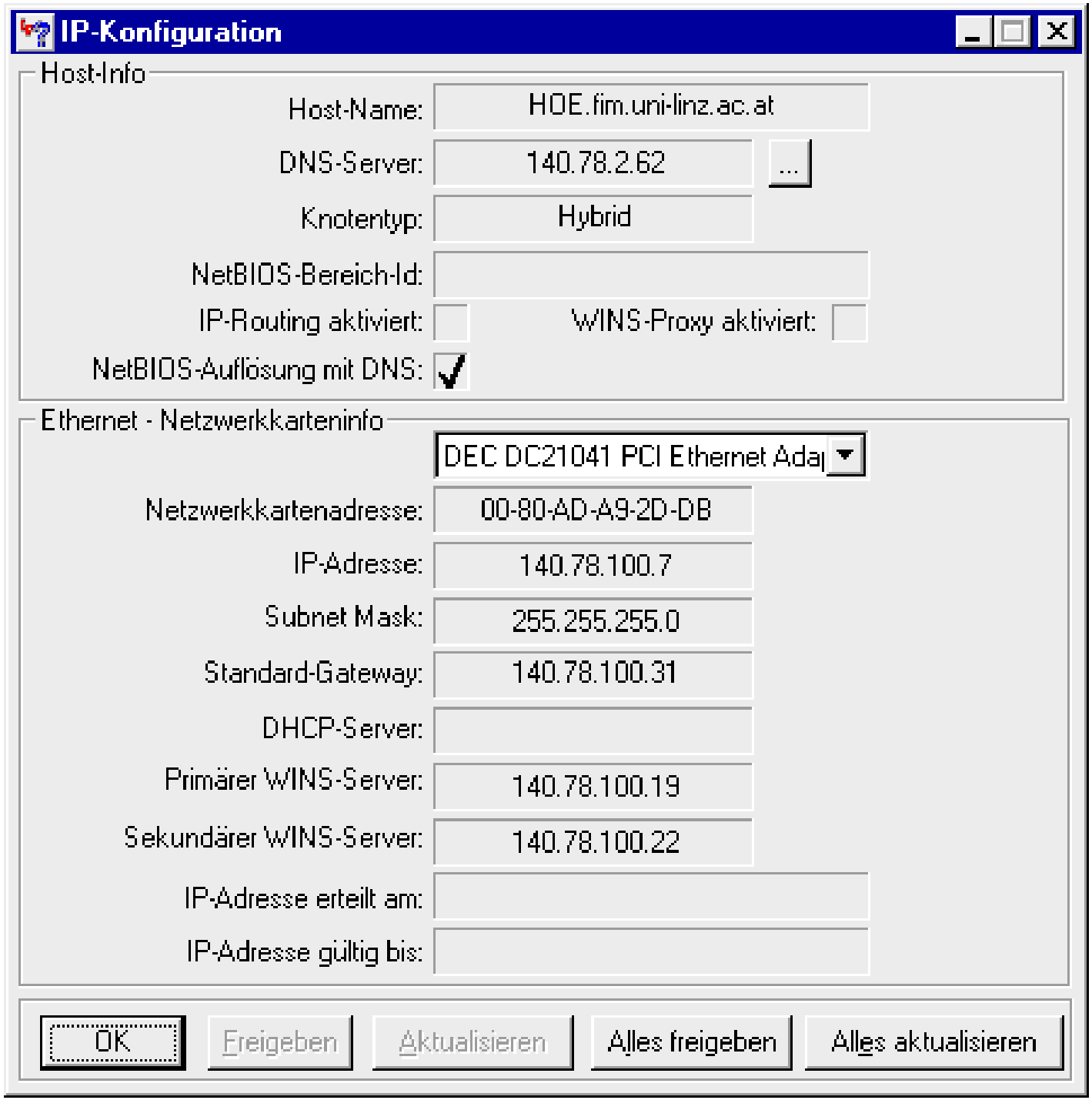
mit überall verfügbaren, einfachsten Mitteln

Testreihenfolge:
inside ==> subnet ==> internet



WNTIPCFG.EXE

= IPCONFIG graphisch



R. Hörmanseder

Test von IP [1] (mit einfachsten Mitteln)

1) **ipconfig / winipcfg / wntipcfg ifconfig**

   Allgemeine Informationen über unsere IP-Konfiguration

2) **ping loopback / ping 127.0.0.1 / ping localhost**

   Test, ob IP-Software am Rechner verfügbar und ok

3) **ping *ip-address of computer***

   noch internes Ping auf eigenen Rechner

Test von IP [2] (mit einfachsten Mitteln)

4) ping *ip-address of default gateway*

   nach außen auf einen anderen Rechner, insb. das default gateway für weiteren Zugriff außerhalb des eigenen Netzes

5) ping *ip-address of local stable server*

   falls 4 nicht funktioniert hat, ein weiterer Test ob eventuell nur das Default-Gateway nicht verfügbar ist.

(4 error und 5 ok ==> keine Verbindung nach außen)

Test von IP [3] (mit einfachsten Mitteln)

6) ping *ip-address of remote host*

   Test ob ein remote Rechner (also ein Rechner außerhalb des eigenen Netzes) erreichbar ist

7) ping *ip-address of nameserver1*
   ping *ip-address of nameserver2*

   Ist ein Nameserver verfügbar?

8) ping *near stable server*
   ping www.fim.uni-linz.ac.at

   Sprechen wir einen korrekten Nameserver an?
   Bessere Test etc. =>NSLOOKUP.

Test von IP [4] (mit einfachsten Mitteln)

9) **traceroute www.fim.uni-linz.ac.at**

   Ansehen der Route zum WEB-Server des FIM

10) **ping *name of remote host***

   Ist der Nameserver für den remote Host korrekt (gibt es den Namen, …..)?

11) **ping -a *ip-address of remote host***

   Ist die „reverse“ Namensauflösung für den remote host ok?

x) **nslookup, netstat, nbtstat, netsh, ...**

NETSTAT: was ist los auf meinem IP-Stack? [1v2]

```
L:\users\hoe>netstat -s -e
```

IP Statistics

Packets Received, Received Header Errors, Received Address Errors, Datagrams Forwarded, Unknown Protocols Received, Received Packets Discarded, Received Packets Delivered, Output Requests, Routing Discards, Discarded Output Packets, Output Packet No Route, Reassembly Required, Reassembly Successful, Reassembly Failures, Datagrams Successfully Fragmented, Datagrams Failing Fragmentation, Fragments Created

ICMP Statistics (jeweils Received / Sent)

Messages, Errors, Destination Unreachable, Time Exceeded, Parameter Problems, Source Quenchs, Redirects, Echos, Echo Replies, Timestamps, Timestamp Replies, Address Masks, Address Mask Replies

NETSTAT: was ist los auf meinem IP-Stack? [2v2]

TCP Statistics:

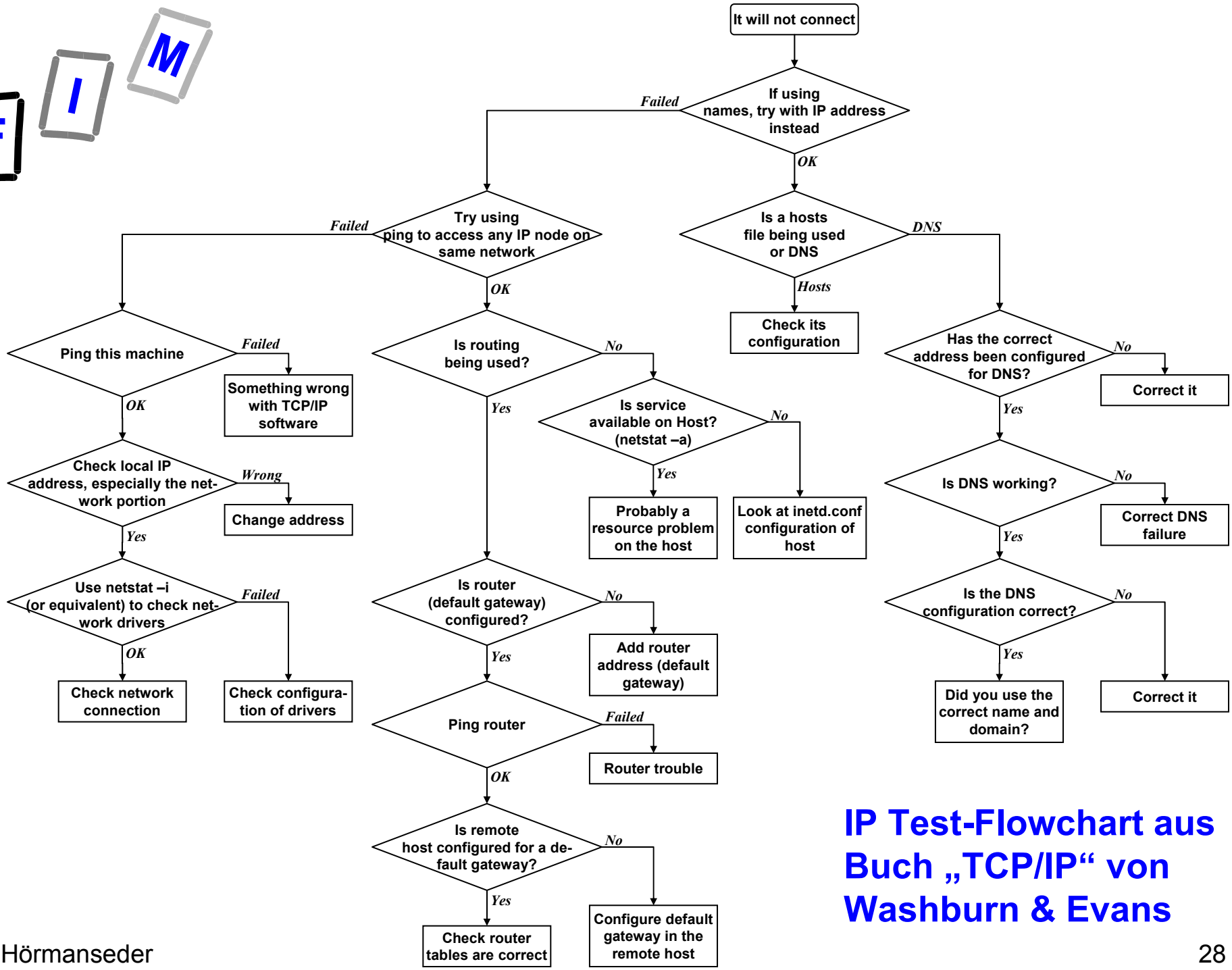
Active Opens, Passive Opens, Failed Connection Attempts, Reset Connections, Current Connections, Segments Received, Segments Sent, Segments Retransmitted

UDP Statistics

Datagrams Received, No Ports, Receive Errors, Datagrams Sent

Interface Statistics (jeweils Received / Sent)

Bytes, Unicast Packets, Non-Unicast Packets, Discards, Errors, Unknown Protocols



IP Test-Flowchart aus Buch „TCP/IP“ von Washburn & Evans