Nacheile auf der Datenautobahn

Kurt Jaeger, pi@LF.net
LF.net/lf/pi
LKA, Stuttgart, 8. Oktober 2003

Vorstellung

- Geschäftsführer LF.net, regionaler ISP
- Ansprechpartner von Ermittlungsbehörden
- DIHK TK-Ausschuss
- Kein Experte

Übersicht

- Was ist ein Angriff ?
- Beweissicherung
- Was ist eine IP-Adresse ?
- Probleme
- Reaktion
- Zusammenfassung

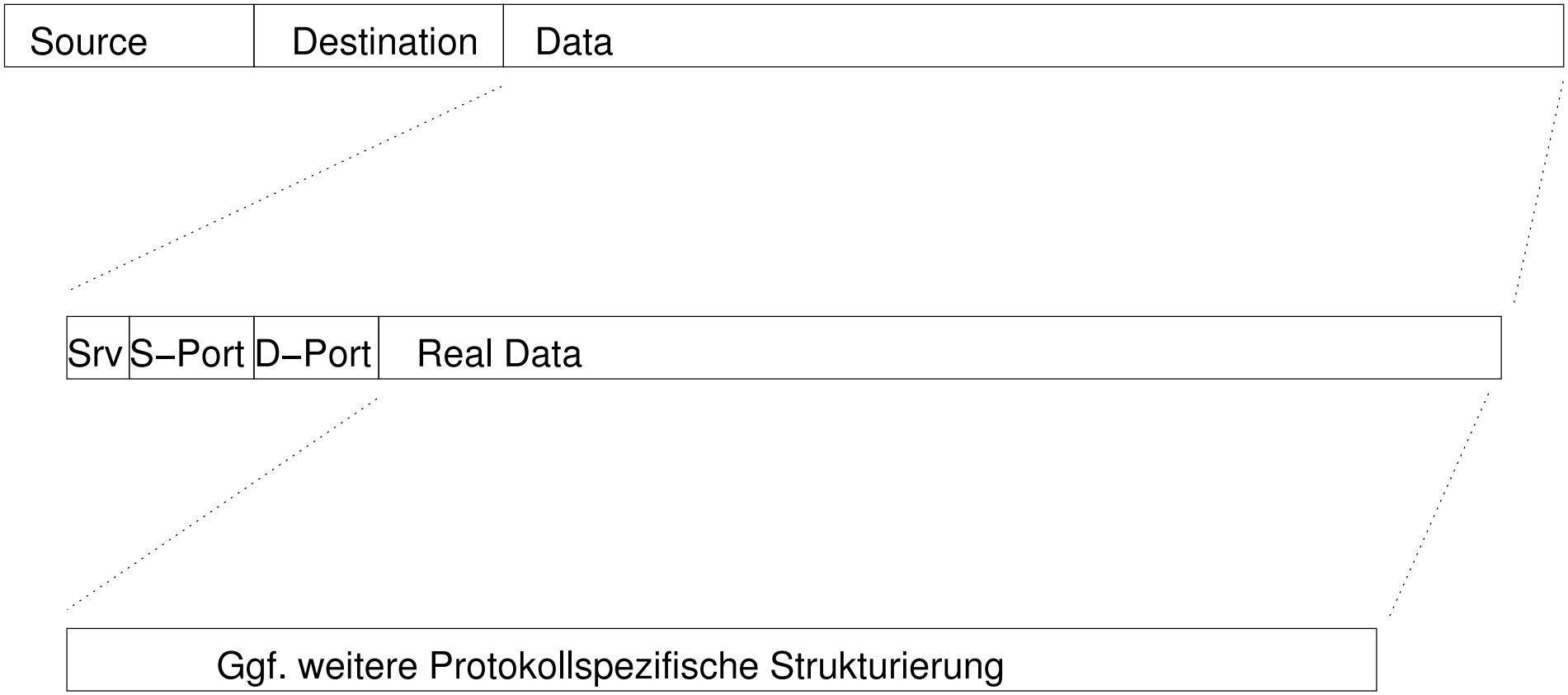
Was ist ein Angriff im Internet ?

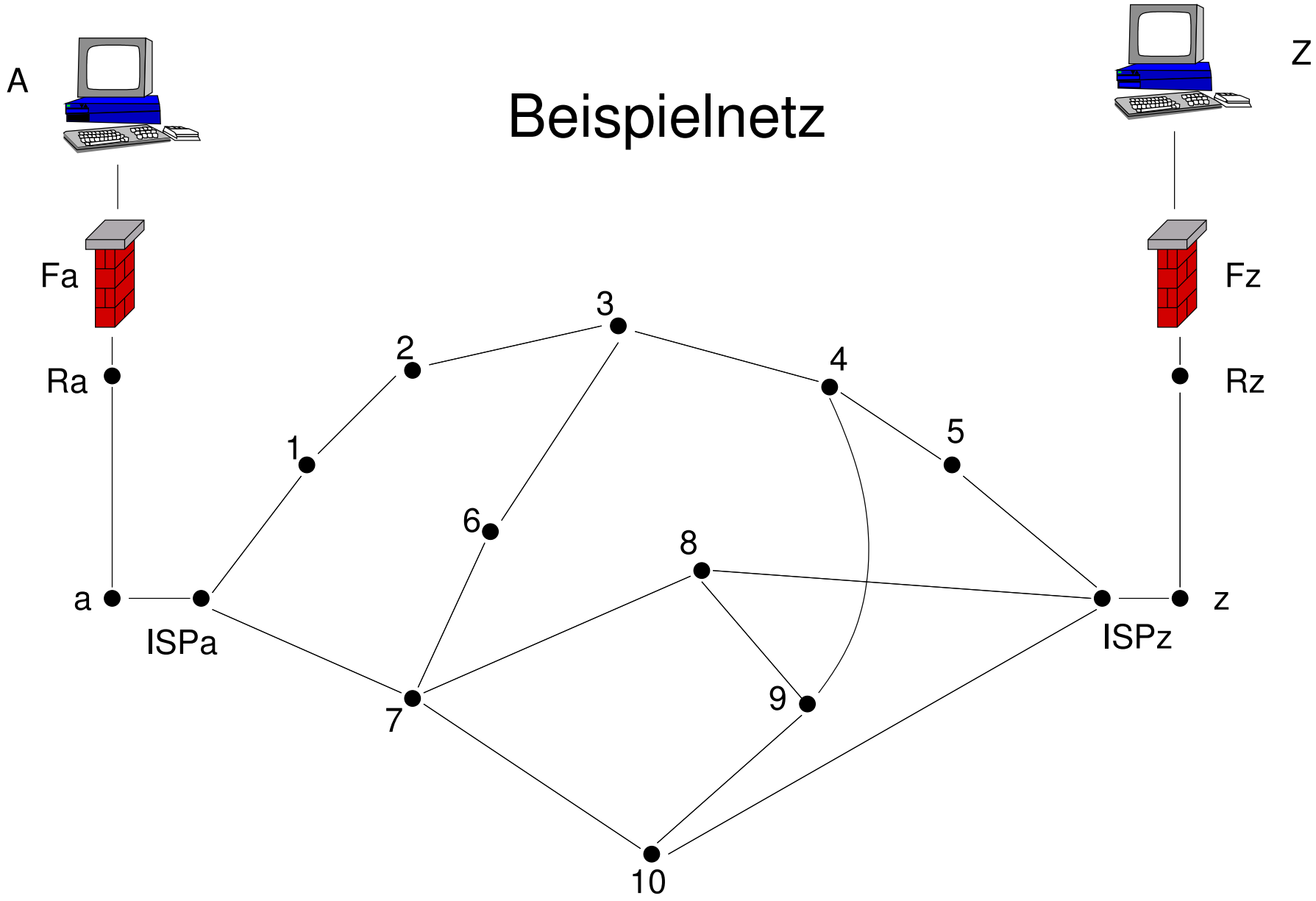
Immer: Empfangen von Datenpaketen

- Netzwerkscan (Türrütteln)
- Automatisiertes Kompromittieren von Rechnern (Script-Kiddies)
- Gezielter Angriff auf einen Rechner
- Denial-of-Service Angriff
- Distributed Denial-of-Service Angriff
- Sabotage, Spionage
- Terrorismus
- Kriegerischer Akt

Vandalismus

Was ist ein Datenpaket ?




Beispielnetz
A
Z
Fa
Fz
Ra
Rz
a
z
ISPa
ISPz
1
2
3
4
5
6
7
8
9
10

Beweissicherung

- Kopien von Datenpaketen oder Teilen (Header)
- Genaue Uhrzeit
- Digitale Daten: Quellenkritik
- Systemumfeld
- Firewall/Filter Zustand
- Routing Tabelle zu diesem Zeitpunkt: AS-Nummer

```
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.165 in via tun0
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.166 in via tun0
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.168 in via tun0
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.167 in via tun0
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.172 in via tun0
00:03:33 1000 Deny TCP 213.181.170.251:3834 213.178.180.158:135 in via tun0
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.169 in via tun0
00:03:33 1100 Deny ICMP:8.0 213.181.170.251 213.178.180.170 in via tun0
[...]
00:05:25 1000 Deny TCP 213.181.165.171:1503 213.178.180.252:135 in via tun0
00:05:26 1000 Deny TCP 203.109.159.141:4333 213.178.180.101:445 in via tun0
00:05:26 1000 Deny TCP 213.181.165.171:1507 213.178.180.253:135 in via tun0
00:05:47 1000 Deny TCP 213.106.125.211:3125 213.178.180.26:445 in via tun0
00:05:50 1000 Deny TCP 213.106.125.211:3125 213.178.180.26:445 in via tun0
00:05:51 1000 Deny UDP 80.34.20.172:3697 213.178.180.121:1434 in via tun0
00:06:01 1100 Deny ICMP:8.0 213.181.189.90 213.178.172.1 in via tun0
00:06:20 1000 Deny UDP 62.150.22.162:4325 213.178.180.68:1434 in via tun0
00:06:20 1000 Deny TCP 213.7.230.203:3506 213.178.180.126:445 in via tun0
[...]
```

```
c$ tcpdump -s 1514 -n host 213.178.180.2
tcpdump: listening on fxp0
17:34:59.855021 212.9.190.63 > 213.178.180.2: icmp: echo request
17:34:59.921414 213.178.180.2 > 212.9.190.63: icmp: echo reply
17:35:25.346271 212.9.190.63.4039 > 213.178.180.2.25: S 3624193305:3624193305(0)
 win 57344 <mss 1460,nop,wscale 0,nop,nop,timestamp 412481612 0> (DF) [tos 0x10]

17:35:25.406768 213.178.180.2.25 > 212.9.190.63.4039: R 0:0(0) ack 3624193306 wi
n 0
17:35:27.709849 212.9.190.63.4040 > 213.178.180.2.22: S 2088544484:2088544484(0)
 win 57344 <mss 1460,nop,wscale 0,nop,nop,timestamp 412481848 0> (DF) [tos 0x10]

17:35:27.773387 213.178.180.2.22 > 212.9.190.63.4040: S 330792016:330792016(0) a
ck 2088544485 win 57344 <mss 1416,nop,wscale 0,nop,nop,timestamp 18082600 412481
848> (DF)
17:35:27.773448 212.9.190.63.4040 > 213.178.180.2.22: . ack 1 win 57564 <nop,nop
,timestamp 412481855 18082600> (DF) [tos 0x10]
17:35:27.841535 213.178.180.2.22 > 212.9.190.63.4040: P 1:41(40) ack 1 win 57564
 <nop,nop,timestamp 18082606 412481855> (DF)
17:35:27.941517 212.9.190.63.4040 > 213.178.180.2.22: . ack 41 win 57564 <nop,no
p,timestamp 412481872 18082606> (DF) [tos 0x10]
17:35:28.635914 212.9.190.63.4040 > 213.178.180.2.22: P 1:7(6) ack 41 win 57564
<nop,nop,timestamp 412481941 18082606> (DF) [tos 0x10]
17:35:28.697749 213.178.180.2.22 > 212.9.190.63.4040: P 41:60(19) ack 7 win 5756
4 <nop,nop,timestamp 18082692 412481941> (DF)
17:35:28.700915 213.178.180.2.22 > 212.9.190.63.4040: F 60:60(0) ack 7 win 57564
 <nop,nop,timestamp 18082692 412481941> (DF)
17:35:28.700951 212.9.190.63.4040 > 213.178.180.2.22: . ack 61 win 57564 <nop,no
p,timestamp 412481947 18082692> (DF) [tos 0x10]
17:35:28.701037 212.9.190.63.4040 > 213.178.180.2.22: F 7:7(0) ack 61 win 57564
<nop,nop,timestamp 412481947 18082692> (DF) [tos 0x10]
17:35:28.762079 213.178.180.2.22 > 212.9.190.63.4040: . ack 8 win 57564 <nop,nop
,timestamp 18082698 412481947> (DF)
^?
212 packets received by filter
0 packets dropped by kernel
c$ exit
```

Was ist eine Adresse ?

- Postadresse
- Bank: IBAN, BLZ und Kontonummer
- Telefonnummer
- Internet: Internet Protokoll Adresse (IP-Adresse)
  Eindeutige Nummer
  - IPv4: 213.178.180.1
    3585258497 ist unleserlich
  - IPv6: v6: 3ffe:b80:3:4ed::2
    Noch viel unleserlicher
- Nicht verwechseln mit Domainnamen oder Web-Adressen

INTERNET PROTOCOL V4 ADDRESS SPACE
(last updated 2003-04-05)

The allocation of Internet Protocol version 4 (IPv4) address space to various registries is listed here. Originally, all the IPv4 address spaces was managed directly by the IANA. Later parts of the address space were allocated to various other registries to manage for particular purposes or regional areas of the world. RFC 1466 [RFC1466] documents most of these allocations.

Address Block	Date	Registry - Purpose	Notes or Reference
000/8	Sep 81	IANA - Reserved	
001/8	Sep 81	IANA - Reserved	
002/8	Sep 81	IANA - Reserved	
003/8	May 94	General Electric Company	
004/8	Dec 92	Bolt Beranek and Newman Inc.	
[...]			
200/8	Nov 02	LACNIC	(whois.lacnic.net)
201/8	Apr 03	LACNIC	(whois.lacnic.net)
202/8	May 93	APNIC	(whois.apnic.net)
203/8	May 93	APNIC	(whois.apnic.net)
204/8	Mar 94	ARIN	(whois.arin.net)
[...]			
212/8	Oct 97	RIPE NCC	(whois.ripe.net)
213/8	Mar 99	RIPE NCC	(whois.ripe.net)
214/8	Mar 98	US-DOD	
[...]			

```
inetnum:      212.118.160.0 - 212.118.160.255
netname:      OBNET-1
descr:        Oberon.net Netzwerksysteme GmbH
descr:        Duesseldorf, Germany
country:      DE
admin-c:      KJ2-RIPE
tech-c:       HON5-RIPE
status:       ASSIGNED PA
notify:       hostmaster@oberon.net
mnt-by:       OBERON-MNT
changed:      hostmaster@oberon.net 20030204
source:       RIPE

route:        212.118.160.0/19
descr:        oberon.net
origin:       AS20621
mnt-by:       OPENIT-MNT
changed:      dk@OpenIT.DE 20010503
source:       RIPE

role:         Oberon.net Hostmaster
address:      Oberon.net Netzwerksysteme GmbH
address:      Georg-Glock-Str. 8
address:      D-40474 Duesseldorf
phone:        +49 211 179253-0
fax-no:       +49 211 362146
e-mail:       hostmaster@oberon.net
trouble:      +49 171 3101372 (mobile phone)
trouble:      Information: http://www.oberon.net
trouble:      mailto:support@oberon.net
admin-c:      KJ2-RIPE
admin-c:      KN1-RIPE
tech-c:       NF1-RIPE
tech-c:       KJ2-RIPE
tech-c:       MD3114-RIPE
nic-hdl:      HON5-RIPE
notify:       hostmaster@oberon.net
mnt-by:       OBERON-MNT
changed:      hostmaster@LF.net 19980218
changed:      hostmaster@oberon.net 19990617
changed:      hostmaster@oberon.net 20020228
changed:      hostmaster@oberon.net 20020708
source:       RIPE

person:       Kurt Jaeger
address:      LF.net GmbH
address:      Ruppmannstr. 27
address:      D-70565 Stuttgart
address:      Germany
phone:        +49 711 90074 23
fax-no:       +49 711 90074 33
e-mail:       pi@lf.net
nic-hdl:      KJ2-RIPE
mnt-by:       LFNET-MNT
changed:      pi@siros.stgt.sub.org 19930531
changed:      rv@Informatik.Uni-Dortmund.DE 19930702
changed:      knocke@nic.de 19941212
changed:      jens@nic.de 19960216
changed:      hostmaster@lf.net 19980129
changed:      hostmaster@lf.net 19980414
changed:      hostmaster@LF.net 20000614
changed:      hostmaster@LF.net 20011105
changed:      hostmaster@LF.net 20021231
source:       RIPE
```

Wie genau muss die Uhrzeit sein ?

- So genau wie möglich
- Millisekunden koennen entscheidend sein, Slammer-Wurm
- Zeitsynchrone Uhren (NTP)
- Intervalle
- Versatz dokumentieren, wenn nicht synchron
- Sommer/Winterzeit nicht vergessen!
- Zeitzone nicht vergessen!

Was macht man mit der Absenderadresse ?

- Bei IANA: Wem gehört die Adresse ?
- RIPE, APNIC, ARIN, LACNIC ? durchprobieren
- Welche Organisation ?
- Welches Land ?
- Ansprechpartner ?
- Rechtlich ?

Probleme

- Dynamische IP-Adressen
- Network Adress Translation Geräte (Firewalls)
- Fälschen der Absenderadresse
- Langsame Angriffe ?
- Software-Fehler
- Rückstreuung von Angriffen
- Geklauter Adressraum
- Datenmengen: Vortrag von Herrn Pfleiderer

Reaktion

Auch auf einfache Angriffe reagieren ?

- Broken-Window-Syndrom
- Informationsflut verdeckt wirkliche Angriffe

Wie schnell reagieren ?

- Noch während der Angriff läuft
- 15 min
- Dynamische Adressen
- Geklauter Adressraum

```
c$ traceroute -n 212.118.160.1
traceroute to 212.118.160.1 (212.118.160.1), 64 hops max, 44 byte packets
 1  212.9.190.1  0.235 ms  0.218 ms  0.165 ms
 2  212.9.176.225  0.528 ms  0.435 ms  0.578 ms
 3  212.9.160.90  16.124 ms  18.126 ms  16.266 ms
 4  212.9.160.89  3.344 ms  3.185 ms  7.702 ms
 5  212.9.161.18  3.903 ms  3.729 ms  3.523 ms
 6  217.71.105.117  6.919 ms  7.324 ms  6.787 ms
 7  217.71.105.110  7.396 ms  7.211 ms  7.543 ms
 8  80.81.192.30  8.396 ms  8.918 ms  10.409 ms
 9  213.200.81.30  12.112 ms  12.591 ms  12.190 ms
10  213.200.64.130  12.063 ms  12.387 ms  11.526 ms
11  217.69.68.132  11.916 ms  13.465 ms  11.856 ms
12  217.69.64.66  11.553 ms  12.141 ms  11.476 ms
13  212.118.166.125  12.212 ms  12.762 ms  12.201 ms
14  212.118.160.1  13.293 ms  12.546 ms  12.182 ms
```

```
c$ traceroute 212.118.160.1
traceroute to 212.118.160.1 (212.118.160.1), 64 hops max, 44 byte packets
 1  core3 (212.9.190.1)  0.230 ms  0.195 ms  0.170 ms
 2  r27-gw (212.9.176.225)  0.515 ms  0.441 ms  0.516 ms
 3  atm1 (212.9.160.90)  8.130 ms  8.653 ms  8.162 ms
 4  de1.core.LF.net (212.9.160.89)  3.303 ms  3.267 ms  3.286 ms
 5  lambda.z10.LF.net (212.9.161.18)  3.677 ms  3.953 ms  3.684 ms
 6  F-2-pos030-0.de.lambdanet.net (217.71.105.117)  6.868 ms  8.524 ms  7.580 ms
 7  F-8-eth100-0.de.lambdanet.net (217.71.105.110)  7.983 ms  7.261 ms  7.062 ms
 8  de-cix.fra30.ip.tiscali.net (80.81.192.30)  8.245 ms  8.289 ms  9.642 ms
 9  so-5-0-0.dus10.ip.tiscali.net (213.200.81.30)  10.861 ms  11.003 ms  10.954
ms
10  so-0-1-0.br0.dus.openit.net (213.200.64.130)  17.416 ms  11.516 ms  12.284 m
s
11  fe5.cr1.dus.openit.net (217.69.68.132)  11.695 ms  11.751 ms  11.435 ms
12  oberon-gw.openit.de (217.69.64.66)  11.598 ms  12.702 ms  11.983 ms
13  gg8-core.oberon.net (212.118.166.125)  14.612 ms  16.341 ms  18.392 ms
14  ns.oberon.net (212.118.160.1)  12.756 ms  12.902 ms  13.519 ms
```

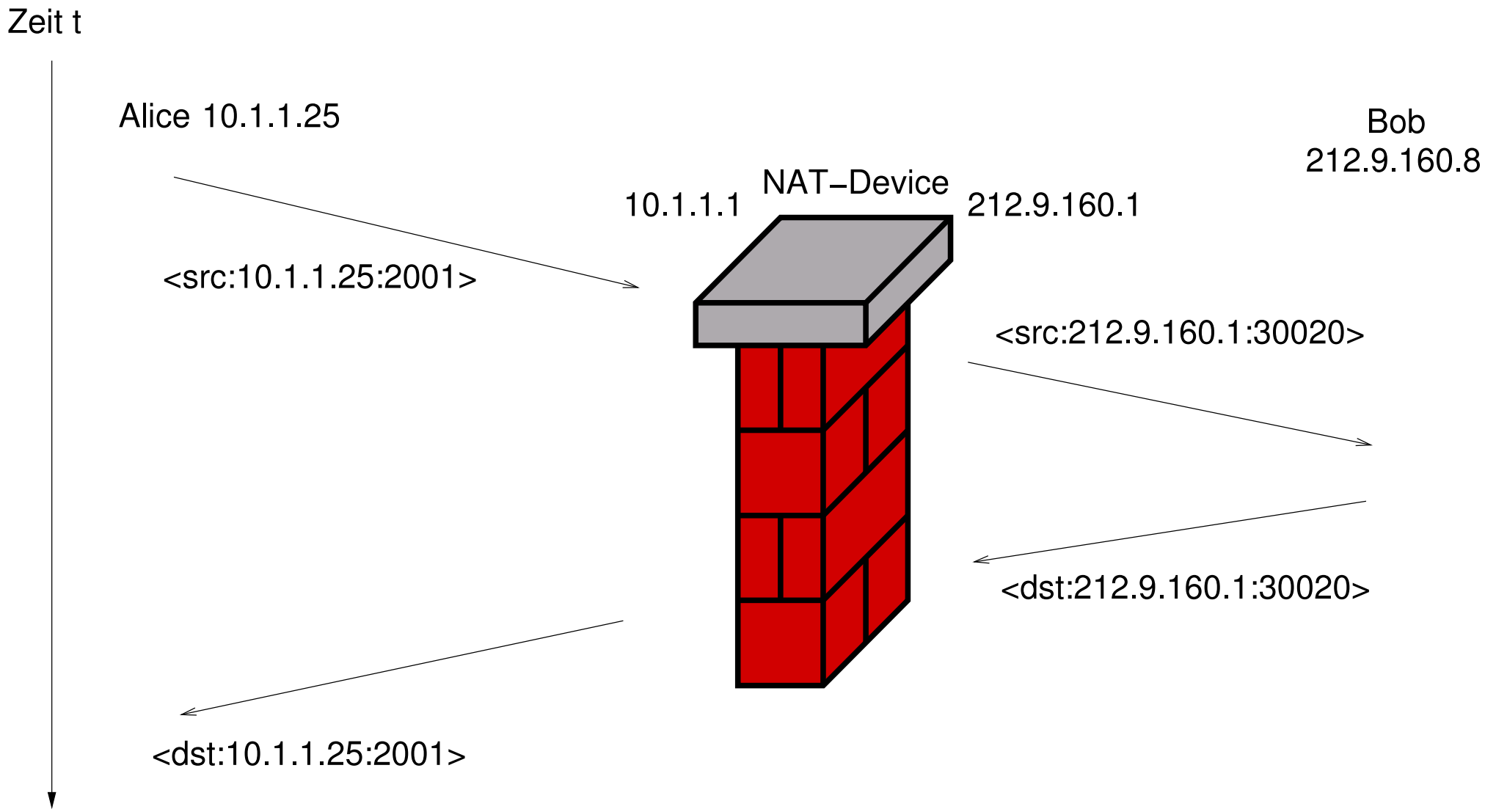
```
traceroute to ns.oberon.net (212.118.160.1) with AS and policy additions

 1 AS12374  core3                            212.9.190.1        [I]
 2 AS12374  r27-gw                           212.9.176.225      [I]
 3 AS12374  atm1                             212.9.160.90       [I]
 4 AS12374  de1.core.LF.net                  212.9.160.89       [I]
 5 AS12374  lambda.z10.LF.net                212.9.161.18       [I]
 6 AS13237  F-2-pos030-0.de.lambdanet.net    217.71.105.117     [ERROR]
 7 AS13237  F-8-eth100-0.de.lambdanet.net    217.71.105.110     [I]
 8 AS6695  de-cix.fra30.ip.tiscali.net      80.81.192.30       [?]
 9 AS3257  so-5-0-0.dus10.ip.tiscali.net    213.200.81.30      [?]
10 AS3257  so-0-1-0.br0.dus.openit.net      213.200.64.130     [I]
11 AS20621  fe5.cr1.dus.openit.net           217.69.68.132      [?]
12 AS20621  oberon-gw.openit.de              217.69.64.66       [I]
13 AS20621  gg8-core.oberon.net              212.118.166.125    [I]
14 AS20621  ns.oberon.net                    212.118.160.1      [I]

AS Path followed:  AS12374 AS13237 AS6695 AS3257 AS20621

AS12374 = LF.net Netzwerksysteme GmbH
AS13237 = LambdaNet AS for European Operations
AS6695 = DE-CIX, the German Internet Exchange
AS3257 = Tiscali Intl Network
AS20621 = OpenIT GmbH
```

Was ist NAT ?


Zeit t
Alice 10.1.1.25
Bob
212.9.160.8
10.1.1.1
NAT−Device
212.9.160.1
<src:10.1.1.25:2001>
<src:212.9.160.1:30020>
<dst:212.9.160.1:30020>
<dst:10.1.1.25:2001>

Organisatorisch

- Automatisieren
  - Wer darf melden ?
  - Was passiert dann ?
  - Art des Angriffs ?
- Enge Kopplung der Auskunftssysteme
  - Anfrage
  - Weitergabe
  - Einfrieren, Verwerfen
  - Vorgangsverfolgung
- Polizeitaktik

Juristisch

- Datenschutz ?
  - Erfassung von Datenpaketen ? Welche Teile ?
  - Von wem ?
  - Wann ?
- Fristen ?
- Ist das Versenden von Paketen strafbar ?
- Strafbarkeit:
  - Ort der Handlung ?
  - Strafhöhe ? Angemessenheit
  - Vorschlag: Strafzettel
- Kosten der Verfolgung ?
- Spam ?

Zusammenfassung

- Fleissarbeit
- Verschulden ? Die Masse machts
  SW-Hersteller ? IT-Dienstleister ? Anwender ?
- Auskunftsprozesse nicht etabliert
- Grenzüberschreitung
  rechtlich, technisch, organisatorisch, Ländergrenzen
- speed matters
- Know-How
- Werkzeuge an Bord ?
- Üben

Ausblick

- Derzeit: Risiko gering, aber langsam wachsend
- Sehr teuer: Aufräumen
- Danach: Risiko relativ gering
- Datenverkehrsordnung
- Strassenverkehrsüberwachung, Wirtschaftsprüfung
- Transparenz, denn:

Missbrauch der Überwachungsinfrastruktur: Risiko sehr, sehr hoch!

Verantwortung der Techniker, Ermittlungsbehörden

Links

- Üben:
  http://www.honeynet.org/misc/chall.html
- Wem gehören die Adressen ?
  http://www.iana.org/assignments/ipv4-address-space
- Softwarefehler erzeugen Datenverkehr
  http://www.cs.wisc.edu/ plonka/netgear-sntp/
- Slammer
  http://www.ripe.net/ripencc/mem-services/ttm/worm/
- Spam
  http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=66
- Adressraum-Diebstahl
  http://www.nwfusion.com/news/2003/1006bgp.html