Troubleshooting in Netzwerken

Jens Link jenslink@quux.de

jenslink@quux.de

FrOSCon 2010

Übersicht

Wer bin ich?

- Freiberuflicher Consultant
- Schwerpunkt: komplexe Netzwerke, Netzwerksecurity, Netzwerkmonitoring, Troubleshooting

Ich bin käuflich ;-)

Ziel des Vortrags

Was man als Netzwerkadmin / Firewalladmin immer wieder hört:

- “Das Netzwerk ist schult!”
- “Die Firewall ist schult”

In 98% aller Fälle liegt der Fehler woanders

Grundsätze (I)

Don’t panic!

Grundsätze (II)

Es nicht zum Problem kommen lassen ;-)

- Dokumentation
- Monitoring
- Dokumentation
- Kommunikation
- Dokumentation
- Strukturiertes Vorgehen
- Nicht mit Kanonen auf Spatzen schießen
- (Security) Features von Hardware nutzen um Probleme zu verhindern

Dokumentation

- Aktuelle Dokumentation des Netzwerks ist wichtig
- Auch Probleme **und** deren Lösung dokumentieren
- Werkzeuge: Wiki + Ticketsystem

Kommunikation

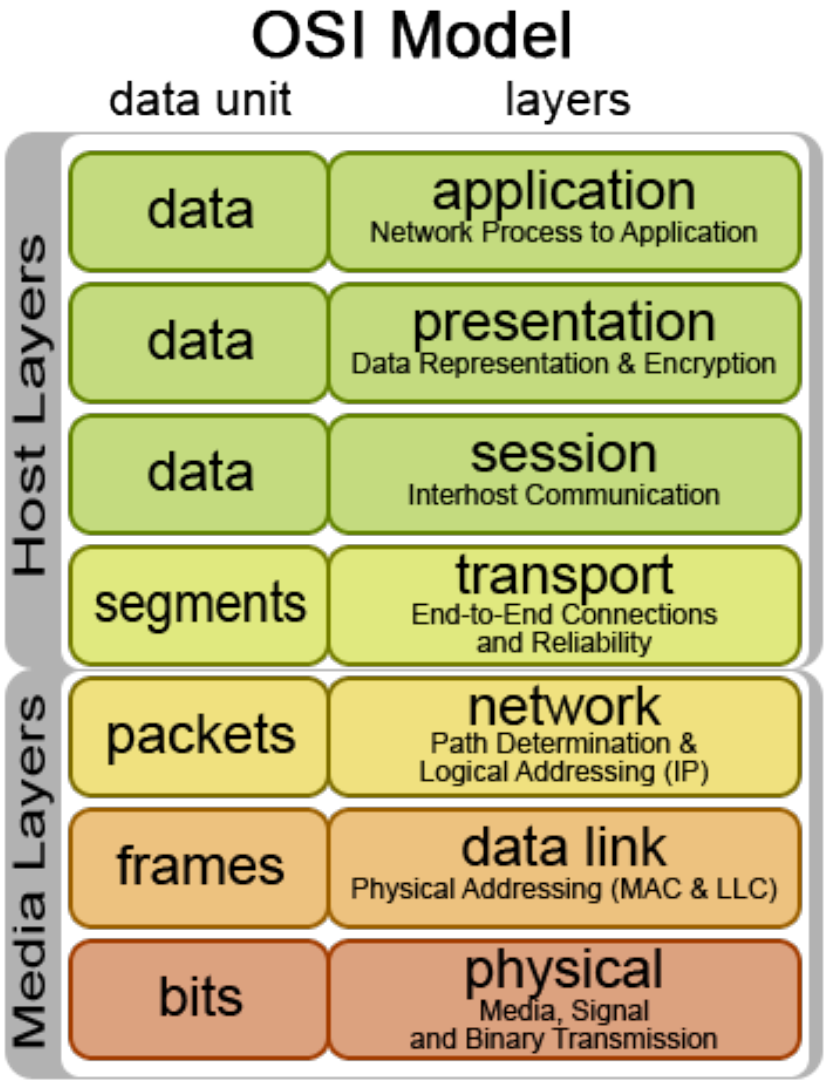
- Tickesystem nutzen
- Bei Problemen ein Ticket erstellen
- ggf. andere noch telefonisch informieren
- Vor Änderungen ein Ticket erstellen
- Bei länger anhaltenden Störungen: Regelmäßige Updates an Betroffene und Chefs

Monitoring

Probleme frühzeitig erkennen

- MRTG / Cacti
- Nagios / ICINGA
- Netflow (nfdump / nfsen)

Strukturiertes Vorgehen



Quelle: http://commons.wikimedia.org/wiki/File:Osi-model.png

Probleme mit Verkabelung

- Zu lange Kabel
- Schmutzige Stecker bei LWL, Biegeradius nicht eingehalten
- Standards einhalten
- Vernünftige Meßgeräte und Werkzeuge verwenden
- Wichtig: Meßprotokolle
- Kablesharing ist böse

Früher war alles schlimmer

Quelle: http://en.wikipedia.org/wiki/File:Ead-outlet.jpg

Switche - Interface Counter

```
switch#sh interfaces gi0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
[...]
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     11334 packets input, 735088 bytes, 0 no buffer
     Received 50 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     50 input errors, 10 CRC, 0 frame, 5 overrun, 0 ignored
     0 watchdog, 50 multicast, 0 pause input
     0 input packets with dribble condition detected
     3007014 packets output, 228157019 bytes, 0 underruns
     ...
```

Switche - Kabelmessung

`test cable-diagnostics tdr interface type number`

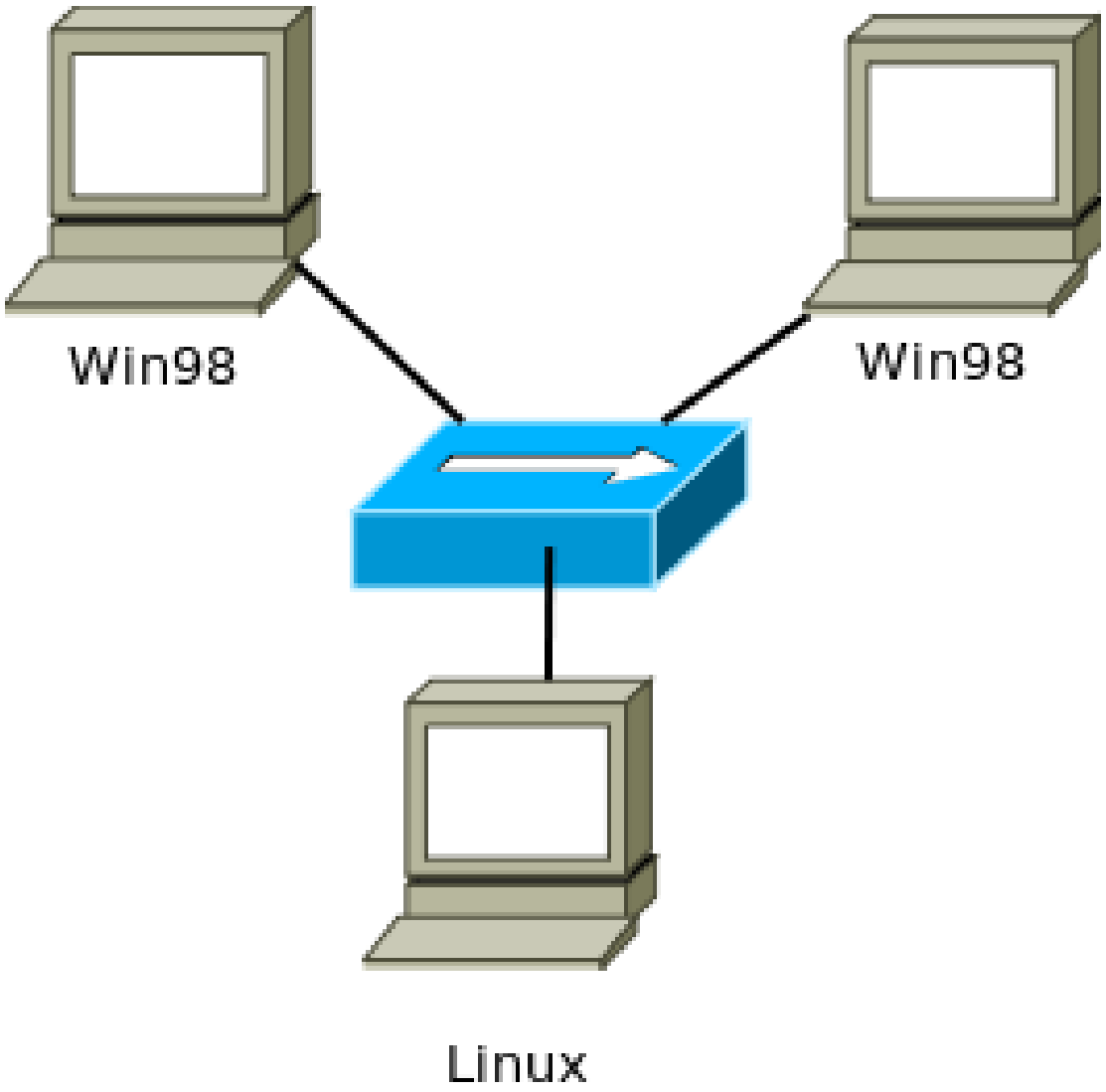
```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi0/2      auto Pair A     0    +/- 4 meters N/A         Open
                Pair B     0    +/- 4 meters N/A         Open
                Pair C     0    +/- 4 meters N/A         Open
                Pair D     0    +/- 4 meters N/A         Open
```

Tools (I)

Die meisten Betriebssysteme bringen schon ein gutes Werkzeugset mit:

- **arp**
- **ifconfig** / **ipconfig** / **ip**
- **route** / **netstat**
- **ping**
- **traceroute** / **tracert** - Der Weg zum Ziel
- **telnet** - Schnell und einfach auf prüfen ob ein TCP-Port offen ist, einfache Protokoll testen
- **nslookup** / **host** - DNS

Merkwürdigkeiten



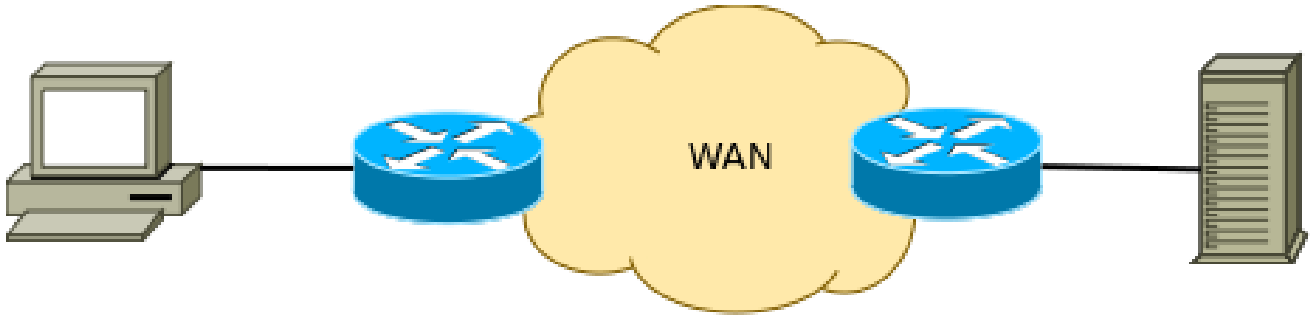
Einführung - Werkzeuge (II)

Nützliche Ergänzungen:

- **tcptraceroute**
- **mtr**
- **nmap**
- **tcpdump / Wireshark**
- **dig**
- **netcat**

Wozu tcptraceroute nützlich ist

Windows Anmeldung über das WAN schlägt fehl:



NetFlows auf Cisco Routern

```
jl-home#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Vl1           88.74.12.234    Di1*          82.113.121.164  06 01BB 0BFD    32K
Di1           82.113.121.164  Vl1           88.74.12.234    06 0BFD 01BB    10K
Vl1           88.74.12.234    Di1*          212.227.83.207  06 B137 1467   126
Vl1           88.74.12.234    Di1*          207.46.124.199  06 8E5B 0747   109
Di1           207.46.124.199  Vl1           88.74.12.234    06 0747 8E5B    60
5 of 5 top talkers shown. 6 flows processed.
```

Check Point fw monitor

- Monitoring des Pakets auf dem Weg durch die Fierwall
- Format: Erweitertes tcpdump, kann mit Wireshark gelesen werden
- 4 “Meßpunkte” können definiert werden
- Anleitung: `http://www.checkpoint.com/techsupport/downloads/html/ethereal/fw_monitor_rev1_01.pdf`

Sniffen in geswitchten Netzwerken

um in geswitchten Netzen zu sniffen, muss man den Switch entsprechend konfigurieren

Cisco:

```
SW(config)# monitor session 1 source interface
             g1/0/24 both
SW(config)# monitor session 1 destination interface
             g1/0/23
```

Andere

`http://http://wiki.wireshark.org/SwitchReference`

Panik!

Wir hindern 150 User für einen Tag an der Arbeit. . .

Kontakt

eMail	jenslink@quux.de
Jabber	jenslink@guug.de
PGP Fingerprint	D9FF E215 6686 6194 FFC8 A135 19CF A676 DB85 EF91
Blog	http://blog.quux.de