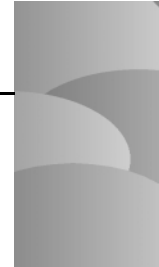


# Kapitel 3

---

## Grundlagen der Methodik



3.1	Eingrenzung von Maschine, Schicht, Ort	74
3.2	Die klassischen Netzwerkfehler	75
3.3	Erste Schritte	76
3.4	Die Windows-Registry	87
3.5	Deutung der Ereignisse und Messdaten	91
3.6	Statistik in Intervallen: Snapshots	98
3.7	Trace-Bibliotheken – ein wertvolles Gut!	100
3.8	Online-Publishing im Ernstfall	101
3.9	Psychologie und Nervenstärke!	102
3.10	Vorbeugen ist besser als Bohren	103
3.11	Permanente Qualitätssicherung	104

Wie findet man die sprichwörtliche »Nadel im Heuhaufen«?

Der eine mag es mit Magneten versuchen (scheitert aber an Alu-Nadeln), der andere mag es mit Gebläse- und Schwerkraft versuchen ... jeder mag seine eigene Idee haben, und jede Idee wird ihre eigene Berechtigung haben.

LAN-Analyse ist in gleicher Weise immer wieder auf neue Ideen angewiesen (weil sich immer wieder neue, nicht gekannte Herausforderungen einstellen): Und doch muss eine Methodik eingeübt sein, die zuverlässig auch dann funktioniert, wenn sich ein gänzlich neues, unbekanntes Fehlerszenario ereignet.

Die folgenden Ausführungen versuchen, ein solches allgemein gültiges Handlungsmuster zu entwickeln:

### 3.1 Eingrenzung von Maschine, Schicht, Ort

Als erstes werden folgende Eingrenzungen vorgenommen:

- Welche Protokolle oder Netzwerkfunktionen stehen in Verdacht, Ursache des Fehlers zu sein?
- Welche Maschinen sind betroffen bzw. stehen in Verdacht?

Es wird das beteiligte Protokoll eingegrenzt bzw. die beteiligte Netzwerkschicht (OSI-Layer). Das bedeutet etwas allgemeiner gesagt: Die beteiligte Funktion wird eingegrenzt. Zur Wahl stehen für gewöhnlich vier Kernpunkte:

- Fehler im lokalen Übertragungssystem (LAN) = physikalische Fehler
- Fehler im *Internetworking* (Vermittlung) = Routing-Fehler
- Fehler in der *Data Flow Control* (oft die Transportschicht, aber nicht nur)
- Fehler in der Namens- und Adressauflösung (ARP, DNS, WINS etc.)

Wenn sich in diesen vier Bereichen kein Fehler nachweisen lässt, liegt die Ursache meistens in einem der folgenden Bereiche:

- Fehler in der Applikation
- Fehler im Betriebssystem (bei Client oder Server)

Ob dann noch von einem »Netzwerkfehler« gesprochen werden kann, mag fraglich erscheinen.

Allgemein gilt folgende Faustregel: Je »tiefer« der Fehler liegt im System der Netzwerkschichten (also in OSI-Layer 1 oder 2), umso einfacher ist der Fehler zu finden – und umgekehrt.



Abb. 3.1: Das umgekehrte Verhältnis von Aufwand und Netzwerkschicht

Abbildung 3.1 soll das verdeutlichen: Je niedriger die Netzwerkschicht (*Physical, Data-Link, Network*), umso geringer sind Zeit und Aufwand zu veranschlagen zum Auffinden des Fehlers. Je höher die Netzwerkschicht (*Transport, Session, Presentation, Application*), umso größer muss der Aufwand veranschlagt werden, diese Fehler zu erkennen und abzustellen.

Hier ist zudem noch eine historische Komponente gegeben:

Bis Anfang der 90er Jahre galt, dass die meisten Fehler auf Layer 1,2 stattfanden – weil mit den überaus fehleranfälligen Koax-Kabeln gearbeitet wurde –, heute ist dies nicht mehr so.

Allgemein ist der *Physical Layer* mit einer fachgerecht durchgeführten Twisted-Pair-Verkabelung kaum noch stör anfällig; und wenn mal ein Fehler auftritt, so betrifft er in aller Regel nur ein Anschlusskabel und daher nur ein Endgerät. Bei einem solchen Szenario ist es oft schon unnötig, den Analyzer zu starten, da ein einfacher Kabeltausch die Vermutung bestätigt und den Fehler beseitigt.

Eher schon können sich Fehler in *Bridges* und *Switches* ereignen, also ggf. kombiniert auf den beiden OSI-Schichten 1 (*Physical Layer*) und 2 (*Data Link Layer*). Meistens ereignen sich die Netzwerkfehler in Twisted-Pair-LANs aber ab OSI-Schicht 3 (*Network Layer*) oder höher.

Gleichwohl: Die Vorgehensweise des Messtechnikers muss darauf abgestimmt sein, dass sie *jeden* Fehler erfasst.

Wichtige Abschnitte hierzu sind 3.3.4 bis 3.3.7.

## 3.2 Die klassischen Netzwerkfehler

Die häufigsten Fehler in Datennetzen lassen sich wie folgt zusammenfassen:

Grundsätzlich kann man folgende Fehlerquellen abstrakt in Klassen fassen:

	OSI Layer	Fehlerklasse, Protokolle (OSI Layer)
<b>A</b>	1,2	Broadcast-Stürme, bedingt durch Fehler in der Netzwerk-Hardware (1,2) oder in den Konfigurationen (2-7).
<b>B</b>	2,3,5,7	Adress- und Namensauflösung ( <i>Resolution</i> ) bzw. Abfragen von Namen und Adressen ( <i>LookUps</i> ): ARP-RARP (2,3), BOOTP (2,3), DHCP (2,3,5,7), WINS (3,5), DNS (3,7)
<b>C</b>	3	Fehler im Routing bzw. in der Netzwerkvermittlung Token Ring (2), IP (3), IPX (3)
<b>D</b>	4	Fehler in der Datenfluss-Steuerung ( <i>Data Flow Control</i> ) LLC (2), TCP (4), NCP (7), SMB (7)

**Tab. 3.1:** Die klassischen Fehlerquellen in LANs und WANs

Entsprechend muss auch die Vorgehensweise sein: Während grundsätzlich innerhalb des OSI-Modells die Schichten von unten nach oben auf Fehler und Auffälligkeiten hin untersucht werden, muss gleichzeitig in den hier genannten Kategorien vorgegangen werden.

Daraus ergibt sich in der Praxis ein mehrdimensionales Vorgehen, da man bei der Durchsicht von Messdaten mindestens zwei parallele Schemata abarbeitet:

- Die Vorgehensweise orientiert sich an den bekannten Schichten gemäß dem OSI-Modell (von unten nach oben).
- Die Vorgehensweise orientiert sich an Funktionen der Datenkommunikation bzw. Fehlerklassen (siehe Tabelle).

Während die Funktion »Routing« klar auf OSI-Schicht 3 liegt (wenn man mal das Token-Ring Source-Routing außer Acht lässt), ist die Funktion Datenflusskontrolle (*Data Flow Control*) bald auf jeder Schicht anzutreffen (unter Einschluss der WAN-Techniken ISDN, ATM und X.25 finden wir *Data Flow Control* tatsächlich auf mindestens fünf der sieben Schichten).

### 3.3 Erste Schritte

Die ersten Schritte hängen davon ab,

- ob ein hauseigener Techniker am LAN-Analyzer arbeitet, oder ob ein externer Dritter (Dienstleister) an die Leitung geht;
- ob die Ursache des Fehlers von vornherein einen bestimmaren Ort hat;
- ob der Fehler reproduzierbar ist (also beliebig erregt werden kann).

### 3.3.1 Interner oder externer Techniker?

Der interne Techniker »kennt« seine Server, Router, Switches ... das nehmen wir wenigstens einmal an und tun so, als sei das leidige Dokumentationsproblem gelöst oder nicht von Belang. Allerdings zeigt die Erfahrung, dass selbst interne Kräfte nicht über ausreichende Dokumentation verfügen, auch nicht über hinreichende Kenntnisse, mit welchen »Lebenszeichen« sich die verschiedenen Komponenten bemerkbar machen (AMP/SMP, BPDU, RIP, OSPF etc.).

Der externe Techniker hat dagegen erst gar keine Dokumentation; und bis sie ihm denn vorgelegt wird – sofern überhaupt vorhanden –, kann er sich längst die nötige Information weitgehend selbst besorgen.

Es sei verwiesen auf das Kapitel 6, »Die Notfallmessungen«, in dem das Zusammenspiel zwischen Auftraggeber und externem Dienstleister eigens dargestellt wird.

### 3.3.2 Dokumentation – ja oder nein?

Grundsätzlich stellt sich zum Thema »Dokumentation« eine für die messtechnische Methodik wichtige Frage:

Gesetzt den Fall, es sei eine Dokumentation gegeben: Soll man sie benutzen, sie zu Rate ziehen, sie zum Ausgangspunkt der Messungen machen? Die Antwort lautet klar und entschieden: »jein«.

- *Für* die Verwendung von Dokumentationen spricht: Es kann wichtige Zeit gespart werden, die man sonst darauf verwenden müsste, sich die benötigte Information selber zu beschaffen.
- *Gegen* die Verwendung von Dokumentationen spricht: Es kann wichtige Zeit verloren gehen, wenn man sich auf Angaben verlässt, die falsch sind – und zwar so, dass man es nicht sofort bemerkt.

Hier muss berücksichtigt werden, dass viele Fehler darin begründet liegen, dass die fürs Tagesgeschäft zuständigen Admins, Operatoren und Techniker selber aufgrund falscher Annahmen bzw. fehlender oder unzutreffender Dokumentationen gehandelt haben – und das oft über sehr, sehr lange Zeiträume.

Diese Menschen können gar nicht anders, als einem – zumal externen – Messtechniker ständig *das* zu erzählen, was sie für gegeben halten. Genau *das* aber kann völlig falsch und letztlich die Ursache des Fehlers sein.

Aus diesem Grunde ist es gut und hilfreich, sich die Aussagen anzuhören und die Dokumentation anzusehen – aber jeder Messtechniker sollte sich davor hüten, dem blind zu vertrauen.

Aus den vorgenannten Gründen hat der Autor ein festes Handlungsschema, wenn er im Notfall zu Kunden gerufen wird: Bevor er sich irgendetwas vom Kunden vorlegen lässt, und bevor der Kunde beginnt langatmig zu erzählen, hängt er sei-

nen Analyzer an die Leitung und bittet um ein bis zwei Stunden Ruhe und Einsamkeit. Dann ist eine objektive Basis für alles Weitere gegeben. Das aber setzt natürlich voraus, dass der Messtechniker in jedem Falle genau weiß, was er tut – und dass er auch die Verantwortung tragen kann.

### 3.3.3 Der erste, schnelle Überblick

Angesichts fehlender oder unzureichender Dokumentation sehen die ersten Schritte wie folgt aus:

- **Erster Schritt: Broadcasts & Multicasts**

Filter auf Broadcasts und Multicasts setzen; dann den Analyzer 60+1 Sekunden laufen lassen (oder länger). Denn so gut wie alle aktiven Komponenten geben einmal je 60 Sekunden ein Zeichen von sich:

Dies sind Router Exchange Protocols (RIP, NWRIP, OSPF, IGRP, E-IGRP, NLSP etc.), Service Advertising Protocols (NWSAP etc.), Bridge PDUs (Spanning Tree) und ähnliche Meldungen.

Ohne diese Orientierung ist eine Analyse gewissermaßen blind.

- **Zweiter Schritt: Adressen & Namen**

Filter auf alle Vorgänge setzen, die mit Namens- und Adressauflösung bzw. Adresszuweisungen zu tun haben: ARP, R/ARP, DNS, WINS, BOOTP, DHCP, ICMP, NetBIOS, AMP/SMP etc.

Die Ergebnisse dieses Schrittes vertiefen nicht nur die mit dem ersten Schritt gewonnen Erkenntnisse (zumal Protokolle wie RIP und NWSAP auch zudem erneut im zweiten Schritt betrachtungswürdig sein können); es können auch die ersten Fehler gefunden werden.

Im Falle von TCP/IP müssen die ARP-Tabellen der verschiedenen IP-Subnets vorliegen, um jeder MAC-Adresse die entsprechende IP-Adresse zuzuordnen zu können.

Welche Produkte sollte man für diese Arbeiten einsetzen?

Es gibt Werkzeuge, welche die aktiven Komponenten mit ihren Adressen und Namen automatisch sichtbar machen: Router, Bridges/Switches, RMON- und SNMP-Agenten, Server usw.

Als ein Beispiel seien der »Observer« (Network Instruments) genannt oder »What'sUp Gold« (IpSwitch).

Diese Werkzeuge können z.T. auch per »Auto-Topology«/»Auto-Map« die gefundenen Komponenten auf dem Bildschirm gemäß der Subnet-Struktur (IP, IPX) anordnen. Jedoch: So schön diese Werkzeuge auch sind, so muss man doch sehen: Sie nutzen nur in den ersten Minuten; danach weiß man, was man wissen muss, und danach wird's langweilig.

Das ist übrigens oft der ernüchternde Effekt bei Käufern: Bei der Vorführung waren sie noch durch den »Aha«-Effekt begeistert, und nach dem Kauf bzw. wenige Wochen später steht die Frage im Raum, was man denn nun damit eigentlich noch anfangen sollte.

Für einen ersten Überblick aber sind diese Werkzeuge unverzichtbar (zumindest für den Laien oder weniger erfahrenen Messtechniker). Danach ist der Messrechner mit einem qualifizierten Analyzer besser eingesetzt als mit einem solchen – zugegeben intelligenten – LAN-Monitor.

Ein gut ausgerüsteter Messtechniker muss also verschiedenen Analyseprogramme auf seinem Rechner haben: Eine Vorgehensweise Schritt für Schritt verlangt eben auch für jeden Schritt das angemessene Werkzeug.

Der Autor vollzieht sämtliche dieser Schritte regelmäßig mit dem von ihm eingesetzten *LANdecoder32* (Triticom) sowie den Add-Ons *NetSense* (Net3Group) *LANreport* (Synapse), welche die Messdaten auswerten und die gewünschten Ergebnisse druckfertig ausgeben: Server, Router, ARP-Tabellen und so weiter.

Hierauf wird an anderer Stelle noch weiter einzugehen sein.

### 3.3.4 Eingrenzung des Ortes

Manchmal ist von vornherein klar, dass der Fehler von einem Server oder Router verursacht wird. Diese Fälle sind jedoch selten; meistens zeigt sich, dass schwere Fehler mehr als nur eine Ursache haben. In den meisten Fällen, in denen der Verfasser gerufen wird, liegen mehrere Ursachen mit mehreren Wirkungen und Wechselwirkungen gleichzeitig vor – was die Arbeit nicht eben leichter macht.

Vor eiligen und leichtfertigen Schlüssen kann nur gewarnt werden!

Es muss berücksichtigt werden, dass die Tatsache, dass eine Komponente erkennbar falsch arbeitet, noch lange *nichts* über die Kernfrage aussagt, ob diese Komponente denn nun

- Täter ist,
- Opfer ist,
- oder beides zugleich.

Das heißt, es stellt sich *immer* die Frage, ob eine falsch arbeitende Komponente selber den Fehler aktiv verursacht (also Täter ist/endogene Ursache), oder ob sie passiv auf externe Ereignisse auf der Leitung reagiert (also Opfer ist/exogene Ursache).

Es ist zu berücksichtigen, dass die Hardware-/Software-Entwickler niemals alle denkbaren Fehler auf der Leitung – also etwa falsch bediente Protokolle – vorweg nehmen können, um ihre eigene Komponente zu einer fehlertoleranten Reaktion zu bringen. Dies ist nur sehr begrenzt möglich.

Angenommen, ein Arbeitsrechner sendet falsch formatierte IP-Pakete und ein Router »versteht« das nicht und »beschließt« daraufhin, sämtliche IP-Pakete in falsche Subnetze zu vermitteln – ist der Router dann Täter oder Opfer? Er wäre offensichtlich beides zugleich.

Und wenn dann aufgrund dieses Ereignisses der Nettodatendurchsatz seitens der Anwender massiv vermindert und die Antwortzeiten massiv erhöht werden, heißt es: »Das Netzwerk ist langsam«, und zugleich: »Ja, aber – wir haben doch nur 10% Netzlast!?!«

Spätestens hier wird sichtbar, dass einfache Aussagen bzw. einfache Annahmen schnell in die Irre führen können.

Wenn man dann noch hinzunimmt, dass bei einem solchen Szenario die Server wiederum auf die Idee kommen könnten, laufend den Router zu wechseln, könnte ein vorschnell urteilender Analyst sogar noch die Behauptung aufstellen, die Server seien defekt – mit der Folge, dass noch Zeit und Geld in den Umbau bzw. in die vermeintlich fällige Aufrüstung der Server gesteckt wird.

Dies sei abwegig? Mitnichten: Das ist die tägliche Praxis »da draußen«.

Die Eingrenzung des Ortes wird also schnell schwieriger, als es auf den ersten Blick erscheint.

### 3.3.5 Eingrenzung der Netzwerkschicht

Weiterhin muss Ihnen immer bewusst sein, dass die modulare Trennung der OSI-Layer reine Theorie ist. Tatsächlich kann ein Protokollfehler auf Schicht A schnell Auswirkungen auf Schicht B haben.

Ein Beispiel: Ein Routing-Fehler auf der Vermittlungsschicht (OSI Layer 3) kann sich in ReTransmissions der Transportschicht (OSI Layer 4) bemerkbar machen.

Umgekehrt können sich die auf Schicht 4 via TCP ausgehandelten Paketgrößen auf das Routing der Schicht 3 auswirken.

Es kann sogar sein, dass ein Fehler auf der Anwendungsschicht (OSI Layer 7) dazu führt, dass es Fehler im Routing gibt (OSI Layer 3), was sich dann wiederum letztlich in Ereignissen (nicht Fehlern!) der Transportschicht (OSI Layer 4) in Form von ReTransmissions niederschlagen kann; und wenn dann noch durch puren Zufall gelegentlich physikalische Fehler auftreten, wird die Situation vollends unübersichtlich.

Ursache und Wirkung sind zwar letztlich immer klar gegeben – aber das Verhältnis zwischen beiden ist eben nicht immer auf den ersten Blick klar erkennbar.

Dies führt dazu, dass man bei der Eingrenzung des Fehlers bzw. seines *logischen* Ortes im Sinne des OSI-Layers *alle* Protokollschichten zugleich im Blick haben muss sowie alle nur denkbaren Wechselbeziehungen zwischen ihnen.

Insbesondere im Kapitel zur TCP/IP-Analyse wird auf solche Wechselwirkungen hingewiesen.

### 3.3.6 Verkehrstabellen

Für das schnelle Eingrenzen des Ortes, teilweise auch der Netzwerkschicht oder des Protokolls, sind sog. Verkehrstabellen immens wichtig. Einige besondere Aspekte hierzu werden im Kapitel »Der Physical Layer« beschrieben. Hier sei allgemein Folgendes aufgeführt:

#### Schnelles Erkennen eines Dialogzustandes

Verkehrstabellen erlauben in den überwiegend meisten Fällen, schnell und zuverlässig den Status eines Client-Server-Dialoges zu ermitteln.

MAC Address[A]	MAC Address[B]	Pkts[A<=>B]	Pkts[A<B]	Octs[A<=>B]	Octs[A<B]	Errs[A<=>B]	Errs[A<B]
0050BAB1D28F	00C07B6CFFE8	1030	1135	97920	1380337	0	0
0050BAA526C7	0050BAB1D28F	295	295	162332	28880	0	0
0050BAA526C7	0050BAB1243F	200	225	47800	23416	0	0
0000E8D667F1	0050BAB1D28F	86	83	6362	6880	0	0
0050BAB1243F	0050BAB1D28F	39	49	3972	5580	0	0
0000210C072D	0000E8D667F1	32	34	2658	2684	0	0
0000210C072D	FFFFFFFFFFFF	32	0	3189	0	0	0
0000210C06FA	0050BAB1D28F	22	24	1654	1578	0	0
0000210C072D	0050BAB1243F	21	15	2292	1752	0	0
0050BAA51B70	FFFFFFFFFFFF	14	0	2366	0	0	0
0050BAA526C7	FFFFFFFFFFFF	12	0	2313	0	0	0
0000210C072D	0050BAB1D28F	12	15	1715	2167	0	0
0050BAB1D28F	FFFFFFFFFFFF	10	0	1546	0	0	0
0000210C072D	030000000001	9	0	680	0	0	0
0050BAB1D28F	030000000001	8	0	1025	0	0	0
00C085293712	FFFFFFFFFFFF	6	0	702	0	0	0
0000210C072D	01005E000116	4	0	478	0	0	0
0050BAB1243F	FFFFFFFFFFFF	4	0	679	0	0	0
0050BAA51B70	0050BAB1D28F	3	2	192	128	0	0
0000E8D667F1	0050BAA526C7	3	2	192	128	0	0
0000E8D667F1	FFFFFFFFFFFF	2	0	511	0	0	0
0000E8D667F1	030000000001	2	0	262	0	0	0
0000E8D667F1	0050BAA51B70	2	1	128	64	0	0
0000210C072D	00C07B6CFFE8	2	3	182	374	0	0
0000B4A6DBF6	030000000001	1	0	184	0	0	0
00C07B6CFFE8	FFFFFFFFFFFF	1	0	64	0	0	0
0050BAA51B70	0050BAB1243F	1	2	64	128	0	0
0000B4A6DBF6	FFFFFFFFFFFF	1	0	238	0	0	0

Abb. 3.2: Verkehrstabelle mit dem MAC-Paaren

Sowohl auf Layer 2 (MAC) wie auch auf Layer 3 (IP, IPX) werden bestimmte Fehlerklassen schnell isoliert und erkannt, wenn die folgenden Fragen durchgegangen und beantwortet werden.

Die Verkehrstabellen ermöglichen schnell und sicher die Anwendung eines effizienten Ausscheidungssystems:

Address (A)	Address (B)	Pkts(A<=>B)	Pkts(A<B)	Pkts(B<A)	Octs(A<=>B)	Octs(A<B)	Octs(B<A)	Oct/Pkt(A<=>B)
194.175.68.3	194.175.68.16	368	371	158720	34709	431	93	
194.175.68.16	206.132.185.167	267	320	21810	413698	81	1292	
194.175.68.3	194.175.68.17	164	185	39246	19246	239	104	
194.175.68.16	209.69.145.34	58	54	7389	41382	127	766	
194.175.68.4	194.175.68.16	49	54	5224	4620	106	85	
194.98.93.244	194.175.68.16	48	57	39925	7798	831	136	
194.175.68.16	194.175.68.17	39	32	4458	3302	114	103	
128.11.68.63	194.175.68.16	32	30	22926	7182	716	189	
194.175.68.2	194.175.68.16	21	24	1590	1578	75	65	
192.76.144.66	194.175.68.16	12	12	3539	992	294	82	
194.175.68.16	209.249.231.26	12	12	1240	13237	103	1103	
194.175.68.16	209.1.218.220	5	5	665	923	133	184	
194.175.68.16	207.230.126.49	5	5	688	417	137	83	
194.175.68.16	208.32.211.100	5	3	885	458	177	152	
194.175.68.16	194.175.68.31	5	0	805	0	161	0	
194.175.68.16	209.1.218.221	5	5	755	458	151	91	
194.175.68.16	207.230.126.50	5	5	665	581	133	116	
194.175.68.17	194.175.68.31	2	0	360	0	180	0	
194.175.68.16	209.92.54.201	1	2	64	128	64	64	
194.175.68.3	194.175.68.13	1	1	64	64	64	64	
194.175.68.4	194.175.68.13	1	1	64	64	64	64	
194.175.68.4	194.175.68.17	1	1	64	64	64	64	
194.175.68.13	194.175.68.31	1	0	260	0	260	0	
192.67.198.6	194.175.68.16	0	4	0	264	0	66	
192.67.198.50	194.175.68.16	0	12	0	792	0	66	

Abb. 3.3: Verkehrstabelle mit den IP-Paaren

### 3.3.7 Fragen und Antworten/Ausscheidungssystem

Eine wichtige Technik ist das schrittweise Isolieren des Fehlers, indem möglichst viele andere Varianten ausgeschlossen bzw. ausgeschieden werden.

Es ist wesentlich einfacher, in einem vorab eingegrenzten Bereich mit der Suche nach der berühmten Stecknadel zu beginnen, als den ganzen Heuhaufen nach ihr durchsuchen zu müssen!

Das folgende Frage-und-Antwort-Schema hat sich über Jahre bewährt:

#### Messpunkt bzw. Ort der Messung

Wo war der Messpunkt, an dem die Statistik erzeugt wurde?

- Hat die zur Statistik führende Messung (per Analyzer oder per SNMP+RMON) stattgefunden
  - im Client-Segment, also etwa am Arbeitsgruppenverteiler,
  - im Server-Segment, in der Server-Farm bzw. am RZ-Switch,
  - im Backbone zwischen Client und Server?

- Wenn die der Statistik zugrunde liegende Messung ...
  - im Client-Segment stattfand und mit Switches gearbeitet wird, sind angezeigte physikalische Fehler auch dort im Client-Segment zu suchen;
  - im Client-Segment stattfand und mit Repeatern (Ethernet) gearbeitet wird, sind die angezeigten physikalischen Fehler nur noch eingrenzbar, wenn bei Kollisionen zwischen *Local Collision*, *Remote Collision* und *Late Collision* unterschieden werden kann, beispielsweise durch An- oder Abwesenheit von Stopf-Bits in den *Frames* (siehe Kapitel 12, »Ethernet«); handelt es sich nicht um Kollisionen, ist der Fehler nicht ohne weitere Maßnahmen eingrenzbar;
  - im Server-Segment stattfand und mit Switches gearbeitet wird, und sofern ein Medium-Tap bzw. Medium-Splitter verwendet wurde, sind angezeigte physikalische Fehler auch dort im Server-Segment zu suchen (siehe Kapitel 5, »Switching und Mirror-Ports«);
  - im Server-Bereich an einem Mirror-Port stattfand, kann die örtliche Eingrenzung nicht ohne weiteres stattfinden, weil Messungen am Mirror-Port spezifische Probleme aufweisen (siehe Kapitel 5, »Switching und Mirror-Ports«);
  - im Backbone zwischen verschiedenen Repeatern, Switches, Routern stattfand, gilt dem Server-Bereich entsprechend das Gleiche: Bei Verwendung eines Mirror-Ports ist die örtliche Eingrenzung problematisch, bei Verwendung eines Medium-Taps ist sie zuverlässig möglich.

#### **Kontaktaufnahme/Verbindungsaufbau**

Kann etwas über den Stand der Kontaktaufnahme bzw. des Verbindungsaufbaus gesagt werden?

- Hat es zwischen zwei Rechnern (Kommunikationsendpunkten), die wegen eines Verdachts oder wegen eines Ausfalls überprüft werden, bereits Kontakt gegeben?
- Wenn es keinen Kontakt gegeben hatte: Hat der Client Broadcasts gesendet: ja/nein? Wenn ja: Kann ermittelt werden, welcher Server oder welcher Service gesucht wird? Ist es der zweite Rechner innerhalb der überprüften Paarbeziehung?
- Wenn es bereits Kontakt gegeben hatte: Laufen die Zähler weiter hoch, oder bleiben sie stehen? Wenn sie weiterlaufen: Wie oft wird der Zähler um welchen Wert erhöht?
- Wenn der Wert des Broadcast-Zählers sich in festen Intervallen mit einem festen Wert erhöht (etwa um den Wert 1 je Sekunde), so handelt es sich um Versuche der Kontaktaufnahme bzw. des Verbindungsaufbaus.

- Wenn der Wert des Broadcast-Zählers sich dagegen unregelmäßig erhöht, sind dies eher Broadcasts, die mit dem aktuellen Fehler in der überprüften Paarbeziehung nichts zu tun haben, sondern unabhängig davon gesendet werden.

### Einzelproblem vs. Gruppenproblem

Betrifft das Problem nur einen einzigen Rechner oder betrifft es mehrere, und wenn es mehrere betrifft: gehören diese in irgendeiner Weise (physikalisch, logisch) zusammen?

- Hat ein Client bzw. Server nur mit einer bestimmten Gegenstelle Probleme, oder auch mit anderen?
- Wenn Probleme nur mit einer Gegenstelle: Gibt es andere Sessions zur selben Gegenstelle, die weiterhin laufen, bei denen also weiter die Zähler hoch laufen?
- Wenn Probleme auch mit anderen Gegenstellen auftauchen: Sind es alle Gegenstellen oder nur einige?
- Wenn Probleme mit allen anderen Gegenstellen auftauchen, ist dies ein Hinweis auf Fehler in der Physik; so könnte das Anschlusskabel des Servers oder der entsprechende Switch-Port defekt sein oder der LAN-Adapter des Servers.
- Wenn Probleme nur mit einer Gruppe von Gegenstellen auftauchen, so sind die Fehler weniger im *Physical Layer* zu suchen als vielmehr in den Netzwerkschichten darüber, etwa im Routing oder in den Applikationen.
- Hat eine einzelne Station einen auffallend höheren Zählerstand bezüglich defekter Pakete als andere Stationen? Sind die Frames einer einzigen Station auffallend fehlerhafter als die Frames anderer Stationen?
- Wenn ja, so ist dies ein Hinweis auf Fehler im *Physical Layer* im Anschlussbereich dieser einen Station.
- Wenn nein, so sind die auftretenden Zählerstände insgesamt gleichmäßig verteilt oder bilden sich Gruppen?
- Wenn sich alle Zählerstände bzgl. Paketfehler gleichmäßig verteilen, so sind die auslösenden Fehler ziemlich wahrscheinlich eher normale, zum alltäglichen Betrieb gehörende Kollisionen (Ethernet) oder Relaischaltungen am Ringleitungsverteiler (Token-Ring).
- Wenn sich die Zählerstände bzgl. Paketfehler auffällig in verschiedene Gruppen gliedern (die meisten mit niedrigem Zählerstand, ein paar aber mit sehr hohem Zählerstand), so spricht dies für einen Fehler eines Verteilers (Repeater, Switch) oder seines Uplink-Kabels oder der Buchsen links und rechts vom Uplink-Kabel (Kaskadierungskabel).

**Und jetzt: gezielte Messung mit dem Analyzer!**

Wenn auf diese Weise eine hinreichende Eingrenzung des Fehlers stattgefunden hat, wird gezielt gemessen.

Hierzu müssen ggf. mehrere Analyzer zur Verfügung stehen.

**3.3.8 Drei-Punkt-Messungen**

Es ist deutlich geworden, dass der Ort der Messung von überragender Bedeutung sein kann! Eine der systematisch wichtigsten Fragen, die an Messdaten zu richten sind, lautet: Entstand die Statistik

- im Client-Segment bzw. am Arbeitsgruppenverteiler
- im Server-Segment, in der Server-Farm bzw. am Server-Switch
- im Backbone zwischen Client und Server?

Im Idealfall liegen Messungen bzw. Statistiken von allen drei Orten vor. Dies führt zum Prinzip der Drei-Punkt-Messung:

Sollte der Ort zu Beginn gar nicht eingrenzbar sein, muss an mehreren Punkten gleichzeitig gemessen werden: unmittelbar beim Client; unmittelbar beim Server; sodann auch im Netzwerk bzw. Backbone dazwischen, ggf. auch noch (als vierten Messpunkt) im WAN.

Hier wird klar, dass die Investition in nur *einen* superteuren Analyzer schon im Konzept falsch ist – sofern das Budget beschränkt ist, wovon auszugehen sein dürfte. Es bringt weit mehr, mit drei Analyzern der unteren (2.000 bis 10.000 DM) oder mittleren Preisklasse (10.000 bis 20.000 DM) an drei verschiedenen Orten zu messen, als mit nur einem einzigen Gerät der hohen Preisklasse (20.000 bis 1.000.000 DM) an nur einem einzigen Ort.

Der Hinweis auf RMON hilft hier nicht: RMON ist in aller Regel für das Vor-Checking gut; bei komplexen Fehlern aber hilft RMON nicht mehr zuverlässig genug, schon allein wegen des Zeitverlustes nicht. Das soll RMON nicht abwerten: Für Stichproben und Dauerüberwachung ist dies die richtige Technik.

Im Falle wirklich harter Fehler aber müssen »echte« Analyzer eingesetzt werden – und im Idealfall eben drei Messrechner statt nur eines Analyzers.

**3.3.9 Drei-Generationen-Messung**

Wenn schon drei Analyzer zur Verfügung stehen, lässt sich mit ihnen auch anders sinnvoll arbeiten als mit einer Drei-Punkt-Messung (s.o.), und zwar mit einer Drei-Generationen-Messung, die ihrerseits topografisch eine Ein-Punkt-Messung darstellt, da sie am selben Messpunkt erzeugt wird.

Bei einer Drei-Generationen-Messung werden die drei Messrechner wie folgt eingesetzt:

1. Der erste Analyzer ist auf langfristige Dauermessung eingestellt. Er läuft mal vielleicht eine halbe Stunde, mal vielleicht viele Stunden oder sogar den ganzen Tag durch.

Filter werden hier grundsätzlich nicht gesetzt – oder nur in wirklich begründeten Ausnahmen.

Der Grund hierfür erklärt sich aus der Verwendung der anderen zwei Analyzer, bei denen sehr gezielt mit Filtern gearbeitet wird.

Während der zweite und der dritte Analyzer niemals alle Daten aufnehmen, ist der erste Analyzer die Rückversicherung für den Fall, dass ein wichtiges Ereignis mit den beiden anderen Analyzern nicht aufgenommen wurde, weil deren Filter das nicht zuließen oder weil sie sogar offline waren.

2. Der zweite Analyzer wird auf mittelfristige, gezielte Messung eingestellt. Er läuft vielleicht mal fünf Minuten, mal vielleicht ein halbe oder ganze Stunde.

Filter werden hier sehr bewusst und sehr gezielt eingesetzt.

Die Filtereinstellungen dieses zweiten Analyzers hängen wesentlich von den Arbeiten mit dem dritten Analyzer ab.

3. Der dritte Analyzer wird für kurzfristige, sporadische Messungen eingesetzt. Er dient dazu, kurze Stichproben zu nehmen, Ideen zu entwickeln bzw. Ideen nachzugehen.

Aus den Ideen, die hier entstehen, bilden sich dann die Einstellungen für den mittelfristig laufenden zweiten Analyzer heraus.

Grundsätzlich sollte dann, wenn der zweite Analyzer zwecks Übernahme der am dritten Analyzer entwickelten Filter offline genommen wird, der dritte Analyzer seinerseits online arbeiten, auch wenn der erste Analyzer seinerseits ständig mitläuft.

Der Grund ist dieser: Sollte sich während der Umstellung am zweiten Analyzer etwas Wichtiges auf der Leitung ereignen, hilft es unmittelbar nicht, dass der erste Analyzer zuverlässig alles aufgenommen hat, da es systematisch oft unpassend ist, diesen zu unterbrechen, um an die Messdaten heranzukommen. Der erste Analyzer sollte im Normalfall den ganzen Tag durchlaufen und *nie* unterbrochen werden.

Um aber bei Eintritt des nur sporadisch auftretenden Netzwerkfehlers schnell handeln zu können, ist es wichtig, dass immer einer der beiden Analyzer (Nr. 2 oder Nr. 3) mitläuft.

Dieses Verfahren hat insgesamt seinen Grund darin,

- dass nach einem unvorhersehbaren, nur sporadisch auftretenden Fehler gesucht wird,
- dass der Fehler also nicht reproduzierbar ist (nicht beliebig erregbar).

Für Fehler, die sehr wohl gezielt hervorgerufen werden können, gibt es andere Vorgehensweisen.

### 3.3.10 Reproduktion des Fehlers

Ist ein Fehler jederzeit reproduzierbar, so ist die Analyse meistens schnell am Ziel. Es sollte daher wie folgt vorgegangen werden:

Man sucht genau *den* Mitarbeiter im Hause, der am häufigsten unter dem Fehler leidet. Neben seinem Bildschirm wird der LAN-Analysator aufgebaut und angeschlossen. Wenn möglich, wird im Rechenzentrum ein weiterer Analyzer neben den Server gestellt, ggf. wird ein dritter in das Backbone dazwischen geschaltet.

Sodann wird der/die Mitarbeiter/in aufgefordert, genau das zu tun, was für gewöhnlich im bekannten Fehler endet.

Dies hat den Vorteil, dass die Aussagen des geschädigten Mitarbeiters zur Analyse herangezogen werden können; weiterhin ist durch gleichzeitige Sicht auf den Anwendermonitor sowie Analyzer-Monitor das Verständnis der Messdaten ungleich besser, als wenn man nur – und sozusagen »blind« – im RZ am Verteilerschrank säße.

Hilfsweise kann die Kommunikation mit dem Anwender via Telefon erfolgen; dies ersetzt jedoch nicht den eigenen Blick auf den Anwendermonitor, da davon ausgegangen werden muss, dass der Anwender nicht alle Ereignisse korrekt interpretiert bzw. wiedergibt.

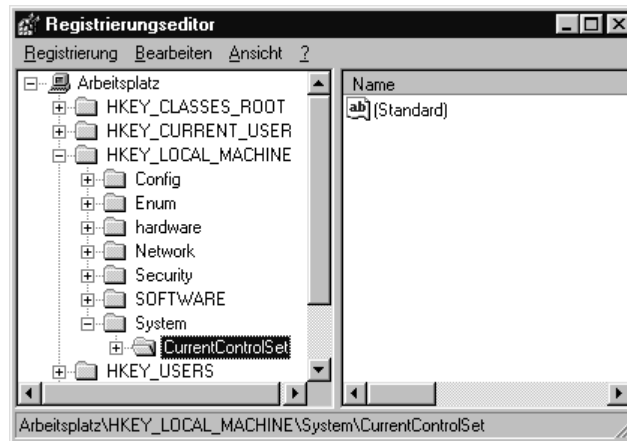
## 3.4 Die Windows-Registry

Der LAN-Analyst ist oft entweder gezwungen, sich die Registry-Einstellungen von Windows-Maschinen anzusehen, die am Fehler beteiligt sind, oder er nimmt sogar Änderungen vor (was der Autor als Externer nie selber tut, sondern nur vorschlägt).

### 3.4.1 HKLM\System\CurrentControlSet\ exportieren

Neben der Tätigkeit des LAN-Analysten sollten Mitarbeiter, die Zugang zu den WinNT-Servern bzw. den Client-PCs haben, die Registry-Daten kopieren und dem Analysten zur Verfügung stellen. Dies geschieht wie folgt:

Es wird über Start\Ausführen der Registry-Editor »RegEdit« aufgerufen.



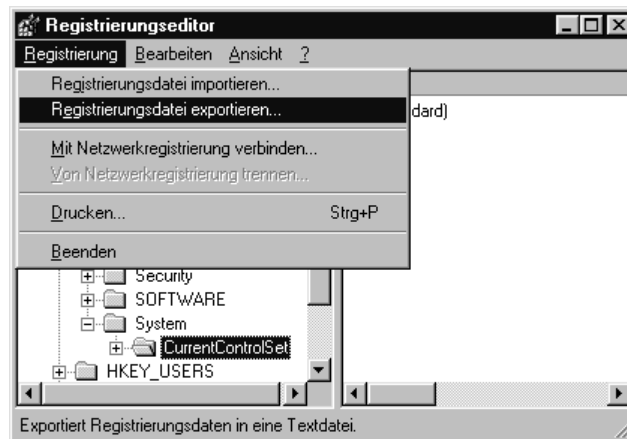
**Abb. 3.4:** RegEdit/Export von HKLM\System\CurrentControlSet (1)

Sodann muss entschieden werden, welcher Zweig exportiert werden soll:

- die gesamte Registry
- nur HKEY\_Local\_Machine
- nur HKEY\_Local\_Machine\System\CurrentControlSet

Das Wesentliche zur Datenkommunikation ist im letzten Schlüssel enthalten.

Sodann wird die Export-Funktion aufgerufen:



**Abb. 3.5:** RegEdit/Export von HKLM\System\CurrentControlSet (2)

Es wird der Name der Export-Datei abgefragt (die resultierende Datei endet auf \*.REG). Weiterhin wird hier erneut die Wahl angeboten, statt eines Unterschlüssels bzw. Zweiges die gesamte Registry zu exportieren.

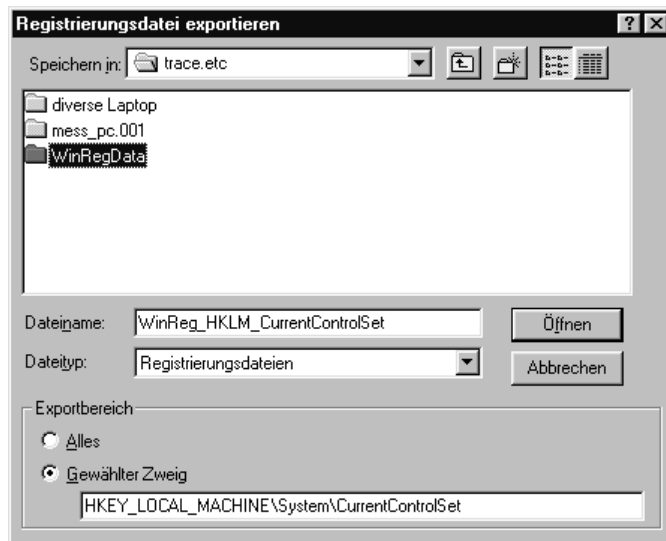


Abb. 3.6: RegEdit/Export von HKLM\System\CurrentControlSet (3)

Diese \*.REG-Datei kann später beliebig untersucht werden.

### 3.4.2 Registry-Tools zum Durchforsten der \*.REG

Es gibt Shareware-Tools, die zum Durchforsten der exportierten Registry-Dateien geeignet sind.

Auf der Beilage-CD-ROM ist das Programm »RegCheck« zu finden, das \*.REG-Dateien einlesen und deren Inhalt darstellen kann.

Wird eine Registry vollständig importiert, können mehrere 10.000 Schlüssel und Parameter in der \*.REG-Datei enthalten sein. Ein kleiner Text-Editor wie der NotePad von Windows kann diese Menge schon nicht mehr einlesen und darstellen.

Entweder nimmt man dann ausgewachsene Textverarbeitungsprogramme wie WinWord oder eben ein Registry-Tool.

RegCheck hat den Vorteil, dass es nicht die Registry direkt »anfasset«, sondern nur mit den Export-Dateien im Format \*.REG arbeitet.

Der dargestellte Registry-Path ist zugleich gewissermaßen »des Pudels Kern« für dieses Buch.

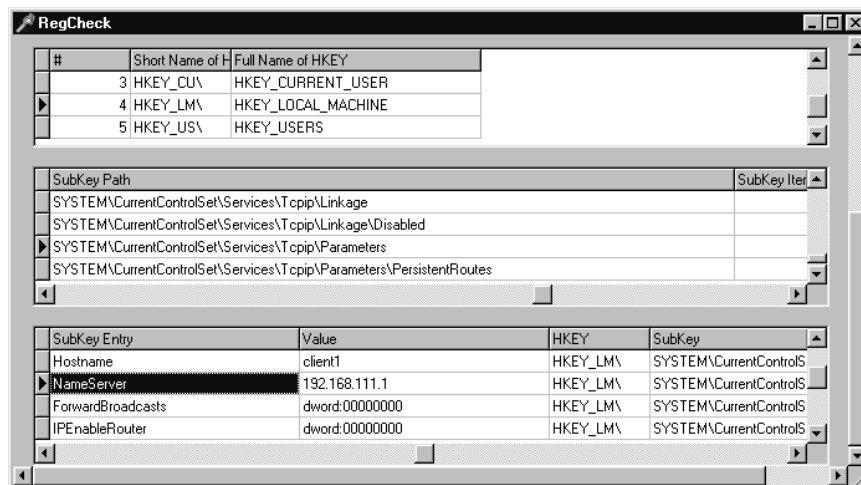


Abb. 3.7: Beispiel einer Registry-Darstellung mit RegCheck

WinNT Registry:

```
HK_Local_Machine\System\CurrentControlSet\Services
```

### 3.4.3 Systemsteuerung\Netzwerk: Vade retro!

Der vielleicht hilfreichste Satz des römischen Herrschers war ein herrisch-mürrisches »*Vade retro!*« (Weiche zurück!), wenn er niemanden an sich heranlassen wollte. Dies sollte auch Ihre Einstellung gegenüber der Windows-Systemsteuerung im Bereich »Netzwerk« sein.

Merke:

- Windows-Systemsteuerung? Das sind alles nur mehr oder weniger unverbindliche Empfehlungen oder Hinweise.
- Kein Windows-Rechner wird es sich je nehmen lassen, am Ende doch zu tun, was er will.
- Und schon gar nicht wird er Ihnen alles zeigen, was er so drauf hat.
- Nur Bruchteile dessen, was sich so in den LAN/WAN-Protokollen herumfummeln lässt, wird auch in der Systemsteuerung offenbar.
- Seine Geheimnisse bewahrt der Windows-Rechner allein in der Registry auf: Nur dort ist die volle Wahrheit zu finden!

Das ist das »Ceterum censeo ...« des Autors.

## 3.5 Deutung der Ereignisse und Messdaten

Die erste Regel des externen Analysten lautet: Höre dir an, was dir der Kunde zu sagen hat, aber misstrau, wo es nur geht!

Zu dem, was weiter oben bereits ausgeführt wurde, sei gesagt:

### 3.5.1 Misstrau dem Kunden bzw. Anwender!

Dies hat Gründe: Schnell lässt man sich durch die Erzählungen des Kunden – ihrerseits vorgetragen im Brustton der tiefsten Überzeugung – in die Irre führen. Es ist doch so: Wenn der Kunde wirklich verstanden hätte, was da auf der Leitung geschieht, hätte er den Analysten wohl kaum rufen müssen. Also: Aufgepasst!

Insbesondere muss Misstrauen herrschen gegenüber »Erkenntnissen« des Kunden, die er aus Konsolenmeldungen der Server und Router hat oder aus Fehlermeldungen der Client-PCs.

### 3.5.2 Misstrau den Fehlermeldungen der Rechner!

Ein Beispiel: Eine bei OS/2 und MS-Windows (3.x,95,98,NT) beliebte Meldung lautet:

*»Von Gerät Netzwerk kann nicht gelesen werden.«*

Schon ruft der Mitarbeiter im RZ an und sagt: *»Ich habe keine Verbindung zum Netzwerk. Meine Ethernet-Karte ist kaputt.«*

Idealerweise wird im RZ gleich weitergedacht: Entweder ist tatsächlich die Ethernet-Karte kaputt oder eben das Kabel, der Stecker, die Buchse, der Verteiler.

Dabei hat doch nur – beispielsweise – ein Server vorübergehende Überlast gemeldet oder ein Router den Umstand, dass er nicht zuständig ist (sondern ein Nachbar-Router).

Beim Weg durch die verschiedenen Protokoll- bzw. Treiberinstanzen wird fast jede objektiv korrekte Fehlermeldung derart grausam verstümmelt, dass am Ende nichts weiter übrig bleibt als:

*»Von Gerät Netzwerk kann nicht gelesen werden.«*

Insbesondere die äußerst genauen Fehlermeldungen von Routern via ICMP (*Internet Control Message Protocol*) und NetWare-Servern via NCP (*NetWare Core Protocol*) werden regelmäßig falsch ausgegeben – oder eben gar nicht.

So kommt es oft zu unbegründeten Vermutungen über Fehler in der Netzwerk-Hardware. Beispiel Ethernet: Da jeder Ethernet-Administrator weiß, dass es Kollisionen gibt, und dass bei einer Überlastung des Netzes und bei der damit ansteigenden Zahl der Kollisionen auch Client-Server-Sessions »sterben« können, fällt der Verdacht sofort dort hin, wo er durchaus nicht hingehören muss.

Auch hier wird wieder sichtbar, dass über alle Netzwerkschichten und Protokolle hinweg gemessen und interpretiert werden muss.

### 3.5.3 Wertvolle vs. wertlose Statistiken

Es soll nicht behauptet werden, dass die Statistiken der Messgeräte nicht stimmen würden. Es soll aber darauf hingewiesen werden,

- dass man Statistiken richtig lesen muss,
- dass man aus einer Vielzahl von Statistiken die für den aktuellen Zweck richtigen heraus finden muss.

Dies soll an einem der wichtigsten Beispiele überhaupt erläutert werden:

Allgemein wird schnell und gerne behauptet: »Das Netzwerk ist langsam.«

Diese Aussage hört jeder Netzwerker mehrfach am Tag. Dann ist schnell die Rede davon, die Netzlast sei zu hoch, und überhaupt müsse man wieder aufrüsten (Gigabit, Terabit, ...).

Jetzt also muss Statistik her! Schon wird das *LAN-Monitoring* angeworfen und heraus kommt dabei wahlweise folgendes:

#### Ein buntes Statistik-Placebo ...

Das zweifellos schönste, bunteste und zugleich sinnloseste Gimmick der Analyzer ist der Tachometer (siehe Abb. 3.8).

Zwar wird hier hübsch mit je einem eigenen Zeiger unterschieden zwischen ...

- aktuellem Wert
- Durchschnittswert
- Spitzenwert

... aber das sagt alles schlicht *nichts* über das Netzwerk aus. Es sind wirklich nur schöne, bunte Bilder, die sich auf dem Messestand des Herstellers ganz gut machen, damit mal jemand stehen bleibt. Die CeBIT ist jedes Jahr voll davon.

Was diese Art der Darstellung so wertlos macht, ist der völlige Verlust der zeitlichen Komponente.

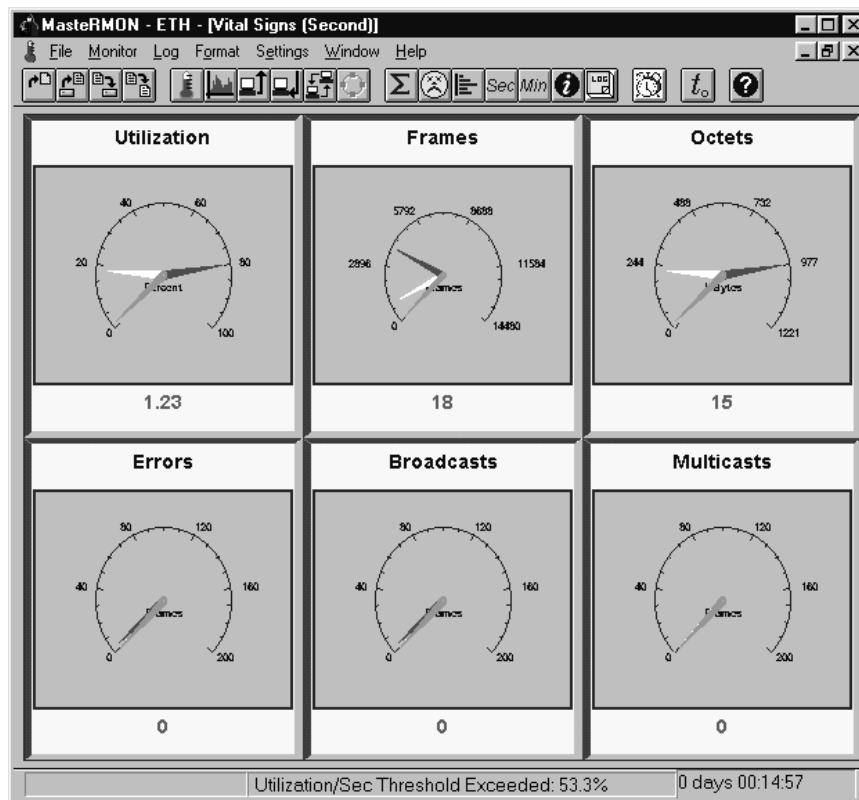


Abb. 3.8: Die berühmt-berüchtigte Tachometeranzeige

### ... und sein Gegenstück

Eine durchdachte Kurvendarstellung ist dagegen sehr viel aussagekräftiger: Im Beispiel der Abbildung 3.9 sind die Werte für »Netzlast« und »Paketfehler« übereinander gelegt – mit einem erheblichen Erkenntniswert.

Wenn die Fehlerspitzen sich zur selben Zeit ereignen wie die Lastspitzen, so sind die Fehler eine Folge dieser erhöhten Netzlast, da sich ganz natürlich dann auch die Zahl der Kollisionen erhöht – sofern es sich dabei um *Shared Media Ethernet* handelt.

Tauchen die Fehlerspitzen unabhängig von Lastverlauf auf, so ist dringend ein Fehler in der Netzwerkphysik zu vermuten.

Tauchen die Fehlerspitzen zwar abhängig vom Lastverlauf auf, aber zwischen Switches, so sind dies eben nicht normale Kollisionen, sondern vermutlich Fehler, die einer der Switches selber aktiv erzeugt.

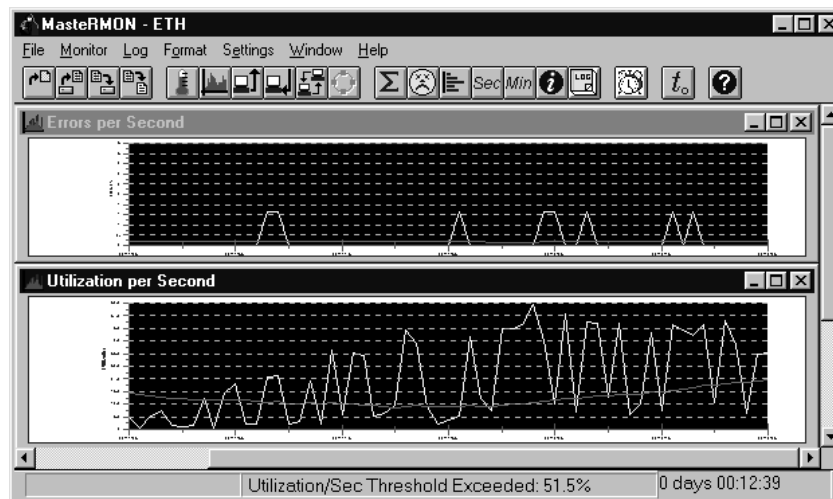


Abb. 3.9: Darstellung der Verkehrsstatistik mit Kurven im Zeitfenster

Alle diese Erkenntnisse wären aber trotz der an sich guten Kurvendarstellung nicht zu gewinnen, wenn nicht beide Kurven zugleich angezeigt würden!

Es zeigt sich also:

- Es gibt gute Statistiken mit guter Darstellung.
- Es gibt gute Statistiken mit schlechter Darstellung.
- Es gibt schlechte Statistiken mit guter, dann aber sinnloser Darstellung.
- Es gibt schlechte Statistiken mit schlechter Darstellung – aber bunten Bildern!

Das alles spielt sich ab in einer Dimension, an die Winston Churchill gar nicht dachte, als er seinen berühmten Spruch tat, dass er nur der Statistik glaube, die er selber gefälscht habe.

Die konsequente Fortentwicklung des Churchill'schen Zitats lautet:

*»Lasse nur mal einen Grafiker sich an der Statistik austoben, und es ist zukünftig ohne jeden weiteren Belang, ob diese gefälscht worden war oder nicht!«*

### Eine biedere Standardstatistik ...

Das zweite Beispiel ist ähnlich angelegt wie das erste, nur deutlich unauffälliger.

Eine völlig korrekte und unverzichtbare Statistik ist die Ausgabe von

- aktuellem Wert
- Durchschnittswert
- Spitzenwert

für die Faktoren

- Netzlast pro Sekunde (verbrauchte Sendezeit pro Sekunde)
- Pakete pro Sekunde
- Oktetts (Bytes) pro Sekunde
- defekte Pakete pro Sekunde
- Broadcast-Pakete pro Sekunde
- Multicast-Pakete pro Sekunde

So ziemlich jedes Produkt, das Netzwerkbeobachtung betreibt, gibt diese Zahlen aus.

Traffic Rate per Second			
	Current	Peak	Average
Utilization(%)	5.5	83.9	15.8
Frames	225	4068	816
Octets	69285	1048734	197133
Errors	0	3	0
Broadcasts	0	3	0
Multicasts	0	0	0

Abb. 3.10: Statistik bezüglich der Netzlast pro Sekunde

Fällt Ihnen etwas auf? Nein? Doch, vermutlich schon, aber erst auf den zweiten Blick: Was besagt denn eigentlich diese Zahl »Utilization Peak = 83,9%«?

Richtig! Sie besagt – *nichts*. Wie das? Sehen wir genauer hin:

Einerseits wird eine durchschnittliche Netzlast pro Sekunde von 15% angegeben, andererseits eine Spitzenlast von rund 84%.

Um diese Zahlen auch nur annähernd sinnhaft deuten zu können, bedürfte es zweier zusätzlicher Angaben, die hier aber völlig fehlen:

- der Beobachtungszeitraum
- weitere Ergebnisse zu diesen Faktoren zu anderen Zeitpunkten.

Ein guter Analyzer ermöglicht es, mit schnellem Blick die bisherige Messdauer zu ermitteln:

0 days 00:26:29

Abb. 3.11: Zeitanzeige in der Statuszeile von LANdecoder32

Aha. Also seit 26 Minuten lief die Messung. Ist das jetzt lang oder kurz, wenn wir auf den Wert »durchschnittliche Netzlast = 15 %« sehen? Wie sollen wir das deuten?

Wenn man das Netz, die Applikationen und das gewöhnliche Arbeitsverhalten der Teilnehmer nicht kennt, reichen auch jetzt die Daten nicht aus, um eine halbwegs sinnvolle Deutung der Zahlen vorzunehmen.

Woran hängt es denn jetzt noch?

Was uns fehlt, sind die Werte von anderen Zeitpunkten (sog. »Schnappschüsse«), oder aber dieselben Werte, nur über einen längeren Zeitraum, also längerfristig gemittelt.

Wir können nämlich bis dato nicht wissen, ob der einmal erreichte Spitzenwert von ca. 84% ein einmaliger Ausreißer war und die nächsten Spitzenwerte dahinter so etwa bei 20 oder 30% lagen, oder ob permanent Spitzen im Bereich von 70 oder 80% vorkommen.

Selbst die Zahl von rund 15% Durchschnittslast kann uns da nicht weiterhelfen. Klar: Auf den ersten Blick könnte man annehmen, dass der geringe Wert von 15% nahe legt, dass die weiteren Spitzen niedrig sein müssten. Das aber ist eine unbewiesene Annahme!

Denn nicht beantwortet bis zum gegebenen Zeitpunkt ist die Frage, ob die Datenmenge, die zu dem Wert von 15% Durchschnittslast führt, in gleichmäßigem Datenfluss entstand oder ihrerseits in höheren Spitzen.

#### Hinweis

*Wir müssen übrigens weiterhin zur Kenntnis nehmen: Auch die Statistik-pro-Sekunde ist nur eine gemittelte Statistik. Während eine einzelne Sekunde bei 10 Mbps Ethernet noch halbwegs aussagekräftig war (»nur« max. 144.000 Pakete pro Sekunde), so ist schon bei Fast Ethernet (mit max. 144.000 Paketen pro Sekunden) schon genügend Raum für eine sehr uneinheitliche Verteilung der Daten über die Sekundengrenzen hinweg.*

Wir brauchen also mehr als nur den Sekundenwert.

#### ... und ihre unverzichtbare Ergänzung

Wenn wir neben die Statistik-pro-Sekunde eine zweite legen, nämlich die Statistik-pro-Minute, wird das Ganze schon klarer.

Jetzt können wir sicher sagen: Wenn die durchschnittliche Spitzenlast pro Minute ca. 30% beträgt, dann dürfte der Wert von ca. 84% pro Sekunde ein eher seltener Ausreißer gewesen sein.

Denn würden sich Lastspitzen im Bereich von 70 oder 80% häufiger ereignen, so würde der Wert »Utilization Peak per Minute« deutlich höher ausfallen.

	Current	Peak	Average
Utilization(%)	20.2	29.1	18.9
Frames	61871	93378	58008
Octets	15141085	21818042	14171652
Errors	3	11	6
Broadcasts	2	4	2
Multicasts	0	0	0

Abb. 3.12: Statistik bezüglich der Netzlast pro Minute

Im aktuellen Fall aber ist es so, dass im Beobachtungszeitraum von rund 26 Minuten der gemittelte Spitzenwert pro Minute nur 29% beträgt, und deswegen müssen in allen anderen, vorherigen Minuten (vor der 26. Minute mit dem Mindestspitzenwert von 83,9%) die Werte umso niedriger gewesen sein.

Also kann die Belastung des Netzes mit Verkehrsspitzen so arg nicht gewesen sein. Der Wert von 18,9% für die durchschnittliche Netzlast pro Minute (gemittelt auf die bisherigen 26 Minuten) bestätigt diesen Befund.

Auch hier also hat sich gezeigt, dass die gleichzeitige Erfassung bzw. Betrachtung verschiedener, aber verwandter Statistiken von erheblichem Belang sein kann.

Und so sieht das Ganze dann tatsächlich aus (Beispiel):

The screenshot shows the MasteRMON - ETH software interface with several data windows open:

- Errors:**

CRC/Align	2
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Collision	158
- Traffic Rate per Second:**

	Current	Peak	Average
Utilization(%)	5.5	83.9	15.8
Frames	225	4068	816
Octets	69285	1048734	197133
Errors	0	3	0
Broadcasts	0	3	0
Multicasts	0	0	0
- Traffic Summary:**

Hosts	34
Conversations	57
Frames	1450904
Octets	354474539
Broadcasts	67
Multicasts	0
Errors	160
Drop Events	0
- Traffic Rate per Minute:** (This is the same table as in Abb. 3.12)

	Current	Peak	Average
Utilization(%)	20.2	29.1	18.9
Frames	61871	93378	58008
Octets	15141085	21818042	14171652
Errors	3	11	6
Broadcasts	2	4	2
Multicasts	0	0	0

At the bottom of the interface, a status bar indicates: "Utilization/Sec Threshold Exceeded: 51.1% 0 days 00:26:29"

Abb. 3.13: Statistikenfenster im LANdecoder32

Ganz nebenbei wird hier ersichtlich, dass es sinnvoll ist, mehrere Monitore mit verschiedenen Grafikanzeigen parallel laufen zu lassen.

Die hier besprochenen Formen von Statistik können online bei der Suche nach akuten Fehlern helfen.

Die folgenden Statistiken dienen der langfristigen Beobachtung des Netzwerks und sollten zur ständigen Pflege gehören.

### 3.6 Statistik in Intervallen: Snapshots

Um auch rückwirkend alle notwendigen Aussagen anhand klarer Daten machen zu können (und um nicht im Kaffeesatz lesen zu müssen), sollten die wichtigsten Kennzahlen der Netzwerkstatistik in festen Intervallen in Tabellen geschrieben werden, damit sie später wieder sichtbar gemacht werden können.

Solche Dauerstatistiken werden oft *Snapshots* und ihre Ergebnisse *Baselines* genannt.

Eine mögliche Dauererfassung der Netzwerkstatistiken könnte wie folgt eingestellt werden (Abbildung 3.14):

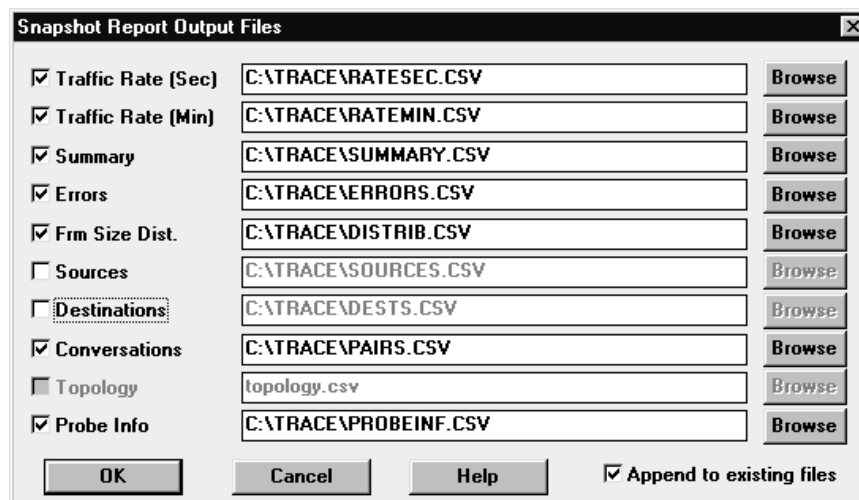


Abb. 3.14: Festlegung der Ausgabedateien für Dauerstatistiken

Jetzt muss noch das Intervall festgelegt werden, in dem die Statistikwerte in die Tabellen geschrieben werden (Abbildung 3.15).

Wenn jeweils das Erfassungsintervall abgelaufen ist, werden die Zählerwerte der angewählten Statistiken in die Tabellen (bzw. in die Dateien) geschrieben und sodann im Programm wieder auf Null gesetzt.

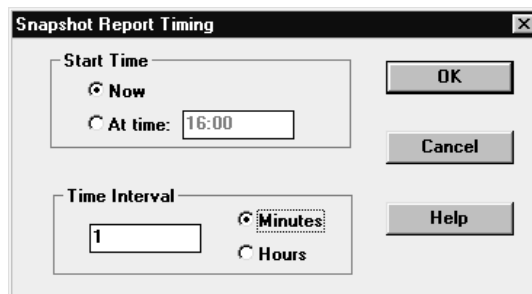


Abb. 3.15: Festlegung des Erfassungsintervalls für Dauerstatistiken

So kann jederzeit der Ereignisverlauf wieder rekonstruiert werden; mit MS-Excel oder anderen Programmen können dann wieder Kurvendarstellungen erreicht werden, wie sie auch schon online sichtbar sind (Abbildung 3.16).

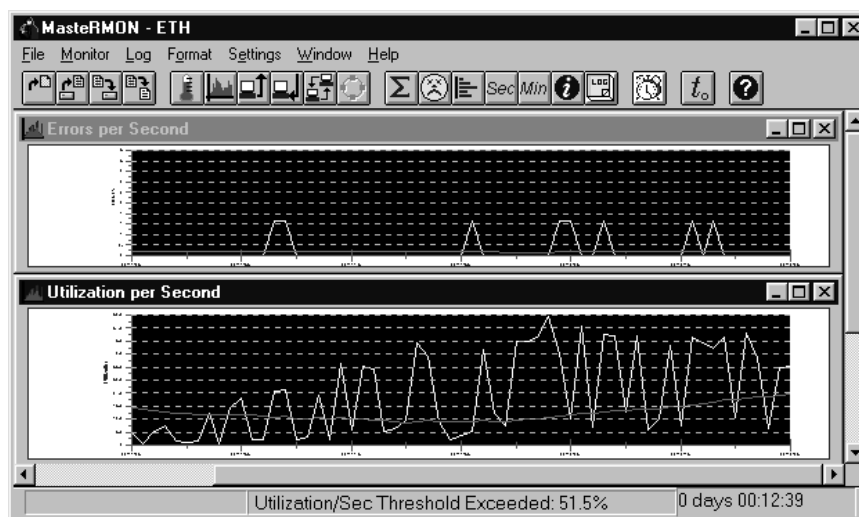


Abb. 3.16: Langzeitstatistiken in Kurvendarstellungen

### Online-Statistik vs. Offline-Statistik

Bei solchen Kurvendarstellungen wählt man bei *Online-Statistiken* für gewöhnlich Zeitfenster von jeweils einer Minute oder eine Stunde.

Bei den *Offline-Statistiken*, die aus den Intervalltabellen entstehen, wären Intervalle von vielleicht 10 oder 15 Minuten sinnvoller: Das Minutenraster wäre vielleicht zu eng, das Stundenraster vielleicht zu grob.

Hier muss die Erfahrung entscheiden, welches Zeitintervall günstig ist.

**Die Aufbereitung und Aufbewahrung**

Diese Statistiken sollten, durchaus auch optisch gut aufbereitet, ausgedruckt und abgelegt werden; ggf. sollten sie über einen Intranet-Webserver laufend publiziert werden, damit alle Dienste des Hauses darauf Zugriff haben (auf die nachbearbeiteten Statistiken, nicht auf die Geräte!).

Auch sollten diese Statistiken dem Vorgesetzten vorgelegt und von diesem abgezeichnet werden.

Die LAN-Techniker trifft oft der Vorwurf, sie hätten nicht früh genug gewarnt, wenn das »Netz mal wieder zu langsam« war. Gegen diesen ziemlich unfreundlichen, aber oft zu hörenden Vorwurf kann sich der Techniker am besten auf die beschriebene Weise zur Wehr setzen.

Außerdem helfen solche Statistiken auch dem Vorgesetzten des LAN-Technikers, notwendige Beschaffungen besser und frühzeitig zu begründen.

Somit kommen wir zum grundsätzlichen Erfordernis des Archivierens von Messdaten.

**3.7 Trace-Bibliotheken – ein wertvolles Gut!**

Zur Methodik des Analysten gehört, dass er »gut« von »schlecht« unterscheiden kann. Das aber ist nur möglich, wenn der Normalfall so gut bekannt ist (gewissermaßen im Gehirn »fest eingebrannt«), dass eine Abweichung davon sofort erkannt wird.

Dies setzt voraus,

- dass der Analyst regelmäßiges Training hat und
- dass der Analyst über umfangreiche Bibliotheken mit Messdaten (engl. »Traces«) verfügt, um im Zweifel vergleichen zu können.

Ein *externer Techniker* (Dienstleister) sollte eine gute Sammlung von CD-ROMs immer in seinem »Notarzkoffer« dabei haben.

Ein *interner Haustechniker* sollte es sich angewöhnen, seine Messergebnisse auf einem hauseigenen Intranet-Webserver zu publizieren. Dies hat viele Vorteile:

- Die Bibliotheken, welche für viele Vorgänge den jeweiligen Normalfall dokumentieren, sind stets verfügbar.
- Die Bibliotheken, welche die früher einmal erkannten und behobenen Fehler dokumentieren, helfen, (a) denselben Fehler nicht zweimal zu machen, (b) die Vorgehensweise im Fehlerfalle nicht erneut entwickeln zu müssen.

In Abschnitt 3.6 war bereits von Statistikdaten die Rede, die es aufzubereiten und aufzubewahren gilt.

Dies ist auf *Capture Data* ebenfalls anzuwenden: Beispielhafte Traces oder solche, die Fehler enthalten, sind aufzubewahren und in Auszügen mittels Intranet-Webserver bekannt zu machen.

Diese Art der Publikation hilft allen EDV-Diensten im Hause, nicht ständig das Rad neu erfinden zu müssen – Rückgriff auf Messdaten zu allen Bereichen der EDV, etwa Datenbankabfragen, Abgleich von Name-Server-Tabellen etc. gehören in die Hand aller, deren Arbeitsauftrag damit zu tun hat.

Das Online-Publishing, auf das hier abgezielt wird, ist nicht nur eine permanente Daueraufgabe, sondern zudem ein wichtiges Mittel im Notfall.

### 3.8 Online-Publishing im Ernstfall

Der Autor geht im Ernstfall sogar noch oft einen Schritt weiter: Er macht einen seiner Messrechner zum Intranet-Webserver und publiziert die Messergebnisse so, wie sie anfallen.

Den Mitarbeitern im Hause des Kunden wird der Zugriff hierauf eingerichtet und die Seite wird allen bekannt gemacht.

Sodann werden alle aufgefordert die darin aufgeworfenen Fragen zu klären. Dies sind oft einfache, aber wichtige Dokumentationsaufgaben.

Es muss ja berücksichtigt werden, dass im Hause des Kunden oft ein erschreckender Mangel an Dokumentation herrscht. Oft erfahren die hauseigenen Techniker erst durch den externen Analysten, was sie da eigentlich im Netz bzw. auf der Leitung haben.

Es ist schon vorgekommen, dass erst durch die Messung klar wurde, dass Switches als Repeater arbeiteten, weil die Konfiguration der Geräte nicht dokumentiert war; oder dass Router ungewollt im Kreisverkehr gekoppelt waren, weil die Verkabelung niemals dokumentiert worden war.

Wenn im Ernstfall extremer Zeitdruck herrscht, kann kein Einzelner alles auf einmal selber leisten. Auch der beste Netzwerk-Guru kann das nicht. Die Kunst besteht dann darin, die richtigen Arbeitsaufträge zu vergeben.

Die beste Unterstützung hierzu ist ein Intranet-Webserver, den man selber kurzfristig aufsetzt.

Alle rücklaufenden Ergebnisse werden dann sofort in die Webseiten hineingepflegt; so hat das ganze Team beste Aussichten, möglichst koordiniert und ohne Reibungsverluste voranzukommen.

Dass diese Arbeit für einen externen Analysten zu viel sein kann, liegt auf der Hand. Entsprechend fahren aus dem Hause des Verfassers je nach Vorankündigung zwei oder sogar drei Mitarbeiter zum Kunden, um möglichst synchron die größtmögliche Wirkung zu erzielen.

### 3.9 Psychologie und Nervenstärke!

Zuletzt sei darauf verwiesen, dass der externe Techniker in einer besonderen Situation ist, der er gerecht zu werden hat bzw. die er für seine Zwecke nutzen sollte.

Die folgenden Überlebensregeln für den Notfall sollen helfen.

- *Neutralität bewahren!*

Die meisten schweren Fehler sind zwar unmittelbar technisch bedingt, aber mittelbar in Fehlern der Arbeitsorganisation und Arbeitsteilung im Hause des Kunden zu suchen.

Man trifft als Externer also nicht nur auf einen technischen Defekt, sondern auch auf ein organisatorisches Umfeld, das oft davon geprägt ist, dass sich Abteilungen im Hause des Kunden schon seit Jahren gegenseitig befehlen, sich gegenseitig Dokumentationen vorenthalten etc.

Als Externer hat man die einzigartige Gelegenheit, Türen zu öffnen (z. B. zu diversen »geheimen Kommandosachen«, also bislang im Hause nicht frei zugänglichen Dokumentationen), die sich die hauseigenen Techniker anderer Abteilungen nicht hatten öffnen können.

- *Als Vermittler auftreten!*

Es sollte Aufgabe des Externen sein, alle diejenigen an einen Tisch zu bringen, deren Verantwortlichkeiten aktuell im Fehlerfalle berührt sind.

Die ggf. vorhandenen Feindschaften müssen schnell und zuverlässig überwunden werden – wenigstens für den Moment.

Hier ist hilfreich, bei einer solchen »Elefantenrunde« die notwendigen Arbeitsaufträge zu verteilen – etwa zur Nacharbeitung von Dokumentationen bzw. zur Beschaffung notwendiger Information.

Das *Online-Publishing*, das oben beschrieben wurde, ist sodann nicht nur für das eigentliche Dokumentieren wichtig, sondern hilft auch die Leute wieder zueinander zu führen.

- *Zeigen, dass auch der Helfer Hilfe braucht!*

Oft treten die Fehler nur bei wenigen, bestimmten Anwendern auf.

Dann ist es messtechnisch sehr hilfreich, unmittelbar am Arbeitsplatz eines solchen Anwenders zu messen (s. o.). Dann aber sollte man als Externer in der Lage sein, den entsprechenden Mitarbeiter davon zu überzeugen, dass es eine gute Tat ist, einen halben oder ganzen Tag dafür zu opfern, »Versuchskaninchen« zu sein.

Da Anwender oft den Netzwerkleuten skeptisch gegenüberstehen (je nach individueller Erfahrung), sollte man immer zu verstehen geben, dass man für alle da ist und allen hilft, nicht nur ausgesuchten Wenigen.

Die Hilfsbereitschaft nur einer einzigen Sekretärin kann entscheiden, ob ein Störfall in Stunden oder Tagen gelöst werden kann – entsprechend sollte man sich in seinem Verhalten auf die Situation einstellen.

- *Niemals unter Druck setzen lassen!*

Die Ursache für das messtechnische Scheitern der hauseigenen Analysten liegt oft darin begründet, dass sie nicht in Ruhe und nicht systematisch vorgehen können – eben, *weil* der Druck zu groß ist, der auf ihnen lastet bzw. der auf sie ausgeübt wird.

Es ist völlig verständlich, dass bei einem Fehler, der pro Stunde mehrere Zehntausend oder Hunderttausend Mark kostet, jeder weiß, wie groß die Verantwortung ist und schnell wird der Druck sprichwörtlich von-oben-nach-unten abgeleitet.

Mit einer solchen Situation ist aber oft der hauseigene Techniker überfordert.

Hier die Ruhe zu bewahren und sich nicht vom systematischen Vorgehen abbringen zu lassen, ist erste Analystenpflicht, zumal dann, wenn es sich um einen externen Dienstleister handelt.

Diese kleinen Regeln mögen nicht alles aufzählen, was wichtig ist, sind aber doch unverzichtbare Forderung an jeden – zumindest externen – Analysten, wenn der Notfall eingetreten ist.

Zusätzliche Hinweise zu diesem Thema sind im Kapitel »Die Notfallmessung« enthalten.

### 3.10 Vorbeugen ist besser als Bohren

Schwierig wird Netzwerkanalyse dann, wenn ein Fehler (bzw. Ereignis) nicht auf lediglich eine einzige Ursache zurückgeführt werden kann.

Tatsächlich handelt es sich bei den »ultraharten« Fehlern, die der Autor regelmäßig zu Gesicht bekommt, um multikausale Ereignisse mit einer langen Entwicklungsgeschichte. Dies muss erläutert werden.

Der Autor und seine Mitarbeiter werden in aller Regel dann gerufen, wenn alle anderen Maßnahmen und Dienstleister nicht mehr helfen konnten. In diesen Fällen stellt sich überwiegend heraus, dass viele, viele kleine Symptome (= Abweichungen von der Norm) zu finden sind, wobei jedes einzelne Symptom für sich noch keinen Fehler auslösen muss.

Im Laufe der Jahre wird hier umgebaut, dort ein neuer Treiber installiert, hier wieder ein neues Betriebssystem in Dienst genommen, dort ein Router gegen den anderen ausgetauscht. Damit schleichen sich regelmäßig kleine ... sagen wir: kleine »Unschärfen« ein, kleine »Macken«, bei denen die verwendeten Protokolle nicht ganz korrekt bedient werden oder die Konfigurationen nicht ganz sauber sind.

Diese »Macken« reichen von falsch gesetzten Timern (etwa TCP: »Wann bloß soll ich ein Paket als verloren ansehen und die Wiederholung starten?«) und falschen ARP-Table-Entries (etwa: »Wieso meldet sich der andere eigentlich nicht, wenn ich ihn mit dieser MAC-Adresse rufe?«) bis zu falschen Protokollanweisungen (etwa: »Okay, ich habe die NFS-Verbindung über UDP schon, das hindert mich aber nicht daran, sie unter TCP trotzdem noch parallel dazu aufzubauen«).

Das kann lange gut gehen. Irgendwann bringt aber ein einziger zusätzlicher Fehler die ganzen Domino-Steinchen ins Kippen. Heißt: Ein einziges *zusätzliches* Protokollereignis kann dann ausreichen, um auf einmal viele oder alle dieser »alten Macken« zu verbinden und ganze Netzwerke außer Betrieb zu setzen.

Alles das hat der Autor schon mehrfach erlebt. Die Folgerungen aus diesen Erkenntnissen sind: Protokollanalyse ist nicht nur für den Schadensfall da; sie hat ständig stattzufinden. In jedem Falle muss sie vor, während und nach einem Eingriff ins Netzwerk stattfinden (neue Router, Server, Treiber etc.).

Es darf niemals nur eine einzelne Schicht isoliert betrachtet werden. Es müssen die Ereignisse/Auffälligkeiten/Symptome aller Schichten und aller Rechner bzw. Komponenten gleichzeitig gesehen und in ihren Wechselwirkungen erkannt werden.

Da hiermit sowohl die meisten Techniker als auch die meisten Analysewerkzeuge überfordert sind, wurden die sog. Expertensysteme (Expert Diagnosis) erfunden. Leider nehmen auch diese High-Tech-Erzeugnisse die Schichten und Ereignisse überwiegend isoliert in den Blick; das Erkennen komplexer, verwobener Fehlerstrukturen wird dadurch nicht unbedingt erleichtert.

Und doch: Das verfügbare Instrumentarium sollte unbedingt ständig und gezielt eingesetzt werden. Und das Ziel muss lauten:

## 3.11 Permanente Qualitätssicherung

Netzwerkanalyse dient bei bester Anwendung und bester technischer Ausstattung

- der ständigen Dokumentation,
- der Revisionsfähigkeit des Netzwerkes,
- der Vorbeugung,
- dem notwendigen Training für den Notfall.

### 3.11.1 Kosten

Wer immer über die *Kosten* von Analysewerkzeugen oder Netzwerk-Management-Komponenten klagen möchte, sollte sich klarmachen, dass ein richtiger Einsatz dieser Technik schon binnen kürzester Zeit das dafür angelegte Geld wieder hereinholt.

### 3.11.2 Einsparungen

Schon allein die *Kostenersparnisse*, die erreicht werden können, übertreffen die Ausgaben für die Analyse bei weitem:

In vielen, wenn nicht den meisten Unternehmungen wird in oft schon unverständlicher Form eine gigantische Überrüstung betrieben, vorrangig an zwei Orten: bei den Servern und im LAN-Backbone. Die Switches sollen immer schneller sein und die Server auch.

Dagegen ist ja nichts einzuwenden: Wenn aber der Flaschenhals tatsächlich ganz woanders lag, nutzt(e) auch die teuerste Neuanschaffung bei Servern und Switches nichts.

Wer dagegen regelmäßig mit Sachverstand auf die Leitung blickt, weiß genau, wo die Leistungsverluste und die Leistungsreserven versteckt sind. Das wiederum erlaubt fortlaufendes *Tuning*, fortlaufende *Qualitätssicherung* – und es spart Kosten. Am Ende aber kommt es nur auf eines an:

### 3.11.3 Garantierte Verfügbarkeit

Was für ein Unternehmen am Ende allein zählt, ist die sichere Verfügbarkeit der EDV. Bei allen Klagen über die Kosten der EDV ist es doch so, dass die Ausfallkosten im Zweifel noch schlimmer sind als die laufenden Kosten fürs Datennetz. Spätestens in Fabriken, deren Fließbänder stillstehen, wird das klar.

Wer aber eine an 100 % heranreichende Verfügbarkeit garantieren will, muss

- messtechnisch vorbeugen und
- die Messtechnik selber permanent verfügbar machen.

Alles andere ist daneben schon eher nachrangig.

Bei der Netzwerkanalyse handelt es sich also um einen *strategischen Unternehmensdienst*, der niemals vernachlässigt werden darf.

So, wie es für die Finanzen ein *Controlling* gibt, sollte die LAN-Analyse auch eine ständige Kontrolle der Rechner und ihres Datenflusses sein.

Es gehört also auch zur Aufgabe des hausinternen Analysten, diese Sichtweise zu vertreten und populär zu machen – letztlich ist genau dies sein Auftrag.

»Klappern gehört zum Handwerk« – und mit diesem »Klappern« fängt die gute Messmethodik schon an: Denn nur wer beizeiten vorgebaut und das Geld für die richtigen Messwerkzeuge locker gemacht hat, kann im Notfall auch wirkungsvoll handeln und helfen.

Der bereits weiter vorne beschriebene Intranet-Webserver zur permanenten Veröffentlichung von Messdaten dient u.a. diesem Zweck: Wenn über Jahre die wöchentlichen Statistiken und Stichproben veröffentlicht werden, wird dies nach und nach im Unternehmen zur Kenntnis genommen; der Wert dieser Tätigkeit wird spätestens bei Nachweis der dadurch erreichten Einsparungen von niemandem mehr ernstlich in Zweifel gezogen werden.

Ein bisschen Werbung in eigener Sache kann also nicht schaden.