

# Inhaltsverzeichnis

	Vorwort	21
Teil I	Kritik der LAN-Analyse und Wege aus dem Zeitmengen-Dilemma	23
Kapitel 1	Der aktuelle Stand der Dinge	25
1.1	Bisherige Veröffentlichungen und das vorliegende Werk	25
1.1.1	2000 – Networker's Guide: Grundlagen der Analyse	25
1.1.2	2001 – Registry Guide: Grundlagen der Registry	26
1.1.3	2003 – das aktuelle Buch	26
1.2	Schwerpunkt: »Das Netzwerk ist langsam«	27
1.2.1	Die alte Krankheit ... da war sie wieder!	27
1.2.2	»Langsam? Wieso? Wir haben doch Gigabit!?!«	27
1.3	Schwerpunkt: OSI Layer 1/Gigabit-Ethernet	28
1.4	Schwerpunkt: OSI Layer 3-4: Routing und Transport (TCP/IP)	28
1.5	Schwerpunkt: OSI Layer 5-7: Name Services (NetBIOS, WINS, DNS etc.)	29
1.6	Schwerpunkt: OSI Layer 7: Application Layer (NCP, SMB, HTTP, VoIP etc.)	30
1.7	Schwerpunkt: neue Analyse-Techniken, neue Werkzeuge, neue Organisationsformen	30
Kapitel 2	LAN-Analyser in der Kritik	33
2.1	Der bisherige Stand der Technik	33
2.2	Die Situation des Autors bei dieser Kritik	33
2.3	Die US-Hersteller ...	34
2.3.1	... und ihre Programmierer	34
2.3.2	... und ihre Eigentümer	35
2.3.3	... und ihre Hilfslosigkeit	36
2.3.4	... und ihre Verdienste	36
2.4	Das Scheitern der LAN-Analyser	37
2.5	Online-Expertensysteme: keine Zeit für tief gehende Analyse	37

2.6	Offline-Expertensysteme: immer nur eine Datei zur selben Zeit	37
2.7	Das Problem: Wann (zu welcher Zeit) war der Fehler?	38
2.8	Das Scheitern auf OSI Layer 1 = Physical-Layer	39
2.8.1	Beispiel: Paket-Verdopplung durch Layer-3-Switches	40
2.8.2	Beispiel: defekte Pakete mit korrekter Prüfsumme	40
2.8.3	Wie kommt es zu solchen Analyzer-Fehlleistungen?	41
2.9	Das Scheitern auf OSI Layer 2 = Data Link Layer	41
2.9.1	Fehler in ATM-Netzen	42
2.9.2	MAC = 000000:000000 – ein netter, kleiner Tick von Switches	43
2.9.3	LLC bei SNA	43
2.9.4	Unicast-Pakete werden zu Multicast-Paketen verfälscht	43
2.10	Das Scheitern auf OSI Layer 3 = Network/Routing	44
2.10.1	DHCP Client Configuration	44
2.10.2	Unerkannte Verstümmelung von IP-Paketen	45
2.10.3	Unentdeckte Routing- und Verbindungsfehler im WAN	46
2.11	Das Scheitern auf OSI Layer 4 = Transport/Data Flow Control	48
2.11.1	Verschiedene Typen von TCP Retransmissions	48
2.11.2	TCP Retransmissions, die gar keine sind	49
2.11.3	TCP-Reaktionen auf Layer-3-Ereignisse	50
2.11.4	TCP Window Size = Zero	51
2.11.5	TCP Window Size = 536/576 (und ähnliche Werte)	52
2.11.6	TCP Maximum Segment Size = 536/576 (und ähnliche Werte)	53
2.11.7	TCP Reset: Verbindungsabbruch. Aber welcher?	53
2.11.8	TCP Ports: Aussagen über Applikationen insgesamt	54
2.12	Das Scheitern auf OSI Layer 5/7 = Name Services	55
2.12.1	Dateisuche via DNS: jahresbilanz.xls	55
2.12.2	Script-Abwicklung via DNS: IFMEMBEROF.LOCAL.DE	58
2.12.3	Suche nach Phantom-Namen, z. B. JSPNRMPTGSBSSDIR	59
2.13	Das Scheitern auf OSI Layer 7 = Application	61
2.13.1	Datei-Operationen: korrekt, aber wahnsinnig	61
2.13.2	Diagnose durch Quantifizierung braucht Qualifizierung	61
2.13.3	Get File Size: 3.000-mal pro Sekunde	63
2.13.4	Read File: Endlosschleife mit 100% Netzlast	64
2.13.5	Open File: Verstümmelung von Dateinamen	65
2.13.6	Open File: Dateien werden gesucht, wo sie nicht hin gehören	67
2.13.7	Applikations-Fehler im Zusammenhang mit Fehlern der Schichten 1–4	69
2.13.8	Anwenderaktionen werden falsch umgesetzt (Beispiel: SAP/R3)	70
2.13.9	Voice over IP läuft nicht richtig: versteckte Fehler im WAN	72

2.14	Das Scheitern beim Filtern	73
2.14.1	Filter auf IP-Adressen	73
2.14.2	Filter auf Textfolgen und Namen (NetBIOS, WINS, DNS etc.)	75
2.14.3	Online-Filter versus Offline-Filter	78
2.14.4	Online-Filter als Ersatz für beschränkte Offline-Filter	79
2.15	Das Scheitern des Stichprobenprinzips	81
2.15.1	Nicht gelöst: Das Problem »giga«-großer Datenmengen bzw. langer Aufzeichnungszeiträume	81
2.15.2	Nicht gelöst: Das Problem nur spontan auftretender Fehler	82
2.16	Das Scheitern bei Verifikations-Analysen	84
2.16.1	Fragen bzw. Bedingungen für eine erfolgreiche Verifikation	85
2.16.2	Hilfreich, aber bei Analyzern nicht vorhanden: ein »Gedächtnis« (Datenbank)	86
2.17	Das Scheitern mangels Datenbanken	86
2.18	Das Scheitern bei der Berichtsausgabe	87
2.18.1	Wie es (leider) bei den LAN-Analysern ist	88
2.18.2	Wie stattdessen gearbeitet werden sollte (TraceMagic)	88
2.18.3	Effizienz der Berichtsweitergabe = Effizienz der Ergebnismsetzung	89
2.18.4	Berichtswesen, Arbeitsteilung und -organisation	89
2.18.5	LAN-Analyse als permanente Qualitätssicherung (proaktiv statt reaktiv)	90
Kapitel 3	LAN-Analyzer: Anmerkungen	93
3.1	Software-Analyzer	93
3.1.1	LANdecoder32 (Triticom)	93
3.1.2	Observer (Network Instruments)	94
3.1.3	EtherPeek NX (WildPackets)	95
3.1.4	Sniffer (NAI, vormals Network General)	96
3.1.5	Surveyor (Shomiti-Finisar)	96
3.1.6	Ethereal	97
3.1.7	TcpDump	98
3.1.8	NTOP	99
3.2	Hardware-Analyzer	99
3.2.1	Hardware-Hersteller begehrt TraceMagic-Code	100
3.2.2	Agilent (Hewlett Packard)	101
3.2.3	Acterna (Wavetech Wandel Goltermann)	101
3.2.4	Shomiti-Finisar	101
3.2.5	NetTool (Fluke)	102
3.2.6	NetVCR (NikSun)	102

Kapitel 4	LAN-Analyse: Neue Wege	103
4.1	Wandel der LAN-Analyse	103
4.2	Die wichtigsten Stationen aus zehn Jahren	103
4.3	Die Ausbildung der LAN-Analysten	105
4.4	Fehler in der Arbeitsteilung der Unternehmen	107
4.5	Automatisierte Methoden in Dokumentation und Analyse	108
4.6	Verteilung der Ergebnisdaten nach erfolgter Analyse	110
4.7	Betriebliche Abläufe und ihre Forderungen an die Analyse	111
4.8	Dauerhafte Qualitätssicherung über automatische Analyse-Verfahren	113
4.9	Die Revisionsfähigkeit der Netzwerke	115
4.10	Planbarkeit und Kostenrechnung	116
Kapitel 5	TraceMagic	117
5.1	Historische Entwicklung	117
5.2	TraceMagic ist anders	118
5.2.1	Gängige LAN-Analyzer und ihre Entwicklungs-Systematik	118
5.2.2	TraceMagic und dessen Ansatz »von hinten herum«	119
5.2.3	»Beschränkung aufs Wesentliche« versus »Perfektion total«	120
5.2.4	TraceMagic in der Praxis und was Kunden sagen	121
5.3	Das Konzept von TraceMagic	122
5.4	Die vier Hauptmodule der TraceMagic-Analyse	124
5.4.1	FilterMagic	125
5.4.2	FindMagic	126
5.4.3	HostMagic	127
5.4.4	SpiderMagic	128
5.5	Installation von TraceMagic	130
5.6	Start von TraceMagic	131
5.6.1	Das Startfenster (mit Abbruchmöglichkeit)	131
5.6.2	Kleines INIT-Fenster	132
5.6.3	Lizenz-Hinweis (Demo-Version oder Lizenz-Version)	132
5.6.4	Prüfung der Datenbanken	133
5.6.5	Benutzeranmeldung	134
5.6.6	Auswahl des Analyzer-Trace-Formats	134
5.6.7	Funktionswahl: Trace-Analyse oder Report-Viewer	134
5.6.8	Datei-Auswahlmenü: Welche Traces sollen verarbeitet werden?	136
5.6.9	Trace-Menü: Die zentrale Schaltstelle	136
5.7	Der Start von SpiderMagic	136
5.7.1	Auswahl der Unterfunktionen	137
5.7.2	Start der SpiderMagic-Analyse mit TCP/IP	138

	5.7.3 Standardabfragen beim Start eines Analyse-Moduls	138
	5.7.4 Auswahl: Trace-Alias und Vorgangstitel	138
	5.7.5 Auswahl: Trace-Filter (ja oder nein)	139
	5.7.6 Auswahl: Größe der IP-Adresstabelle	141
	5.7.7 Vorbereitung der Report-Datenbanken (1)	142
	5.7.8 Auswahl: Größe der TCP History-Tabelle	142
	5.7.9 Auswahl: Trefferpakete in neue Trace-Datei schreiben?	143
	5.7.10 Auswahl: Trefferpakete in Text-Dekodierungen ausgeben?	145
	5.7.11 Vorbereitung der Report-Datenbanken (2)	146
	5.7.12 Auswahl: Endgültiger Start mit den gewählten Einstellungen	146
	5.8 Report-Dateien: Jeder Durchgang erhält sein eigenes Verzeichnis	147
	5.8.1 Die neu erzeugte Trace-Datei samt zugehörigem Event-Log	147
	5.8.2 Die Report-Datenbanken	148
	5.8.3 Die »reconstructed files«	148
	5.9 TraceMagic während der laufenden Analyse	149
	5.9.1 Trace-Analysis: Einfache Aktivitätsanzeige	149
	5.9.2 Trace-Analysis: Aufruf der Ergebnis-Datenbank	150
	5.9.3 Trace-Events: Aufruf des Event-Logs	150
	5.10 Trace-Reports: Abschlussreport-Dateien erzeugen	154
	5.11 Trace-History: Datenbank aller vergangenen Analyse-Vorgänge	155
	5.12 Die Report-Dateien und die Ergebnis-Datenbank	155
	5.12.1 TraceHistory: Summary	155
	5.12.2 TraceHistory: Details	155
	5.12.3 TraceHistory: EventFilter	159
	5.12.4 TraceHistory: Memo	160
	5.12.5 TraceHistory: History Database	160
	5.13 TraceEvents/EventFilter	161
Teil II	LAN-Analyse in den OSI-Schichten 1 bis 7	165
Kapitel 6	OSI-Schichten 1 und 2	167
	6.1 Messtechnik und Analyse auf den OSI-Schichten 1 und 2	167
	6.1.1 Was ist neu?	168
	6.1.2 Abschied von ATM, FDDI und Token-Ring im Campus-LAN	168
	6.1.3 Gigabit-Ethernet: Messungen unter Gigabit-Bedingungen	169
	6.1.4 Media-Splitter (TAP) statt Mirror-Port	170
	6.1.5 Geeignete Capture Engines für Gigabit-Messungen	171
	6.1.6 TcpDump auf dem Gigabit-Server	172
	6.1.7 Load Balancing	172

6.2	Beispiele für Fehler und ihre Diagnose durch LAN-Analyse	174
6.2.1	Erdungsfehler: Switch defekt, Frames defekt	174
6.2.2	Defekte Ethernet-Frames (1): Switch-Fehler	177
6.2.3	Defekte Ethernet-Frames (2): Switch-Fehler	189
6.2.4	Defekte Ethernet-Frames (3): Adapter-Fehler	202
6.2.5	Switch-Fehler: Paketervielfältigungen	209
6.2.6	Switch-Fehler: Spanning Tree Topology Changes	213
6.2.7	Switch-Fehler: Mirror-Port gibt Pakete falsch aus	215
6.2.8	Switch-Fehler: Pfadtabellen reichen nicht aus	218
Kapitel 7	TCP/IP-Grundlagen	223
7.1	Einführung: Was ist TCP/IP?	223
7.1.1	Sie erben TCP, Inc. und führen es zum Erfolg	223
7.1.2	Einrichtung von UDP wegen des Kostendrucks	225
7.1.3	Sie expandieren und fusionieren mit der IP, Inc.	225
7.1.4	ICMP meldet Störungen	228
7.1.5	ARP und DNS für die richtige Adresse	229
7.1.6	SNMP+RMON – Überwachung in Echtzeit	230
7.1.7	Des Rätsels Lösung	230
7.2	Die wichtigsten Protokolle der TCP/IP-Familie im Überblick	230
7.2.1	Fundstellen in der WinNT Registry	231
7.2.2	ARP – Address Resolution Protocol	232
7.2.3	IP – Internet Protocol	233
7.2.4	ICMP – Internet Control Message Protocol	235
7.2.5	TCP – Transmission Control Protocol	239
7.2.6	UDP – User Datagram Protocol	241
7.3	Vorgehensweise	241
7.4	Adress- und Namensauflösung	242
7.4.1	Betriebsphase	242
7.4.2	Die MAC-Adresse ist falsch zugewiesen (LAA)	243
7.4.3	Die IP-Adresse ist falsch zugewiesen	244
7.4.4	Die IP Subnet Mask stimmt nicht	246
7.4.5	Der NetBIOS Name stimmt nicht	248
7.4.6	Der DNS Name stimmt nicht	248
7.4.7	Die IP-Adresse des DNS-Servers stimmt nicht	248
7.4.8	Umgekehrte Namensabfragen bleiben erfolglos	249
7.4.9	Fehler im Address Resolution Protocol (R/ARP)	249
7.5	Routing-Fehler/Default Gateway	250
7.5.1	Pakete laufen über andere Wege als vorgesehen	251
7.5.2	Pakete werden von Routern verworfen	251

7.5.3	Pakete laufen doppelt: Local Loop	253
7.5.4	Router und ICMP	254
7.6	Im Fokus des Analyzers: ICMP	254
7.6.1	ICMP: »Destination Unreachable«	255
7.6.2	ICMP: »Redirection – Gateway Address«	257
7.6.3	ICMP: »Time Exceeded – TTL Expired«	258
7.6.4	ICMP: »Time Exceeded – ReAssembly Timeout«	259
7.6.5	ICMP: »Fragmentation Needed«	260
7.6.6	ICMP: »Source Quench«	261
7.6.7	ICMP: »Echo Request/Echo Reply«	261
7.6.8	Grenzen von ICMP	262
7.7	Im Fokus des Analyzers: IP	263
7.7.1	IP: Version/Header Length	264
7.7.2	IP: Type of Service (ToS)	265
7.7.3	IP: Total Length	266
7.7.4	IP: Fragment ID	270
7.7.5	IP: Fragmentation Flags	273
7.7.6	IP: Fragment Offset	275
7.7.7	IP: Time To Live (TTL)	275
7.7.8	IP: Protocol	278
7.7.9	IP: Checksum	279
7.7.10	IP: Source/Destination Address	279
7.7.11	IP Expertendiagnose	283
7.7.12	IP und NetBIOS	284
7.8	Im Fokus des Analyzers: TCP	286
7.8.1	Das Prinzip der TCP Data Flow Control	287
7.8.2	TCP: Source/Destination Port	294
7.8.3	TCP: Sequence/Acknowledge Number	298
7.8.4	TCP: Data Offset	304
7.8.5	TCP: Flags	306
7.8.6	TCP: Window Size	310
7.8.7	TCP: Checksum	313
7.8.8	TCP: Urgent Pointer	314
7.8.9	TCP: Maximum Segment Size (Option)	314
7.8.10	TCP Expertendiagnose	315
7.9	Im Fokus des Analyzers: UDP	316
7.10	BOOTP/DHCP	318
7.10.1	BOOTP – Bootstrap Protocol	318
7.10.2	DHCP – Dynamic Host Configuration Protocol	319

7.11	SNMP/RMON	324
7.11.1	SNMP: Befehls- und Abfragesprache	324
7.11.2	SNMP-over-IPX	325
7.11.3	SNMP und CMIP	325
7.11.4	SNMP Community String public/private	325
7.11.5	RMON: Ferndiagnose/Verkehrsanalyse	326
7.11.6	HS-RMON	326
Kapitel 8	OSI-Schichten 3 und 4: TCP/IP	327
8.1	Allgemeine (und fällige) Analyzer-Schelte	327
8.2	Verweis auf die anderen Kapitel	329
8.3	Vorgehensweise in diesem Kapitel	329
8.4	ICMP: Kurze Übersicht	329
8.5	IP: Fehler und Symptome	330
8.5.1	IP Corrupted Packet	330
8.5.2	IP Packet: MAC Multiple Tx/Duplicate IP Header	331
8.5.3	IP Packet: MAC Multicast/Broadcast	331
8.5.4	IP Version ungleich v4/v6	332
8.5.5	IP Header Length < 20 Octets	332
8.5.6	IP ToS / Type of Service	332
8.5.7	IP Total Length <> MAC Length	332
8.5.8	IP Packet ID = 0	333
8.5.9	IP Remote Route Change (IP Packet ID)	333
8.5.10	IP Packet ID / Duplicate ID / IP Local Loop	335
8.5.11	IP Packet ID / doppelt in verschiedenen Paketen	336
8.5.12	IP Fragmented Packets	336
8.5.13	IP Time-To-Live (TTL) / Erfassung aller Werte	337
8.5.14	IP Time-To-Live / TTL = 0	337
8.5.15	IP Local Loop/Both Packets: Before And After Hop	337
8.5.16	IP Local Loop/Single Packet: Only After Hop	338
8.5.17	IP Remote Route Change (TTL)	338
8.5.18	IP Remote Route Long Way (TTL)	339
8.5.19	IP Packet Ping-Pong (TTL)	339
8.5.20	IP Checksum	340
8.5.21	IP Source Address	340
8.5.22	IP Destination Address	340
8.5.23	IP Option / Header Extension	342
8.6	TCP: Fehler und Symptome	342
8.6.1	TCP Packet = Broadcast/Multicast	342
8.6.2	TCP Retransmission / ReTx SeqNo = PreTx SeqNo	343

8.6.3	TCP Retransmission / ReTx SeqNo <> PreTx SeqNo	343
8.6.4	TCP ReTx / Keep-Alive ReTransmission	344
8.6.5	TCP No ReTx / IP Local Loop	345
8.6.6	TCP No ReTx / IP Paketdreher	345
8.6.7	TCP No ReTx / Header Duplicate	346
8.6.8	TCP Missing Sequence	346
8.6.9	TCP Flag(s) = SYN, ACK, PSH, URG, FIN, RST	347
8.6.10	TCP Flag = RST/Abbruch	347
8.6.11	TCP Flag = SYN/ReTx	348
8.6.12	TCP Flag = FIN/ReTx	349
8.6.13	TCP Flag = RST/ReTx	349
8.6.14	TCP Window Size Low	350
8.6.15	TCP MSS Low	352
8.7	UDP: Name Services	354
8.7.1	UDP Port 53/DNS	355
8.7.2	UDP Port 137/WINS	356
8.7.3	UDP Port 138/NetBIOS Datagram	357
Kapitel 9	OSI-Schichten 5 und 7: Namensdienste	359
9.1	Dateisuche per DNS	360
9.1.1	Ergebnistabelle von TraceMagic/HostMagic	361
9.1.2	DNS-Anfragen nach SLANT010DLAKBHT01	362
9.1.3	DNS-Anfragen nach SLANT010NETLOGONCONFIG.POL	362
9.1.4	DNS-Anfragen nach SLANT011.Intern.sampleD.DE	364
9.1.5	DNS-Anfragen nach SLANT011WADLE\$BRIEFE01jhjfoo	365
9.1.6	DNS-Anfragen nach JSPNRMPTGSBSSDIR	366
9.1.7	DNS-Anfragen nach SLANT012LVSECHTSOFTWARELVS.DWX	368
9.1.8	DNS-Anfragen nach SLANT012LVSECHTSOFTWAREWinlvs5.exe	372
9.1.9	DNS-Anfragen nach MATYSDATAMAINLIST.DAT	372
9.1.10	DNS-Anfragen nach SLANT011DOKUMENTEAbteilungenDExport TrogsangDiverseCretschmar.doc	374
9.1.11	DNS-Anfragen nach SLANT011WADLE\$BRIEFE01hjhATC.doc	377
9.2	Script-Reparatur per DNS	382
9.2.1	DNS-Namen werden in der NetWare-NDS gesucht	382
9.2.2	Das Server-Login-Script als DNS-Anfrage	384
9.2.3	DNS-Anfragen nach 49	385
9.2.4	DNS-Anfragen nach MS2MAILSOFTWAREGW55ECLIENTUPDATE32.DLL	387
9.2.5	DNS-Anfragen nach NDPS01	387
9.2.6	DNS-Anfragen nach SERVER	387

9.2.7	DNS-Anfragen nach SERVERVOLUMEuser%username%	387
9.2.8	DNS-Anfragen nach www.aol.co	388
9.2.9	DNS-Anfragen nach www.kieser.com	388
9.3	Telnet-Befehle per DNS	389
9.3.1	DNS-Anfragen nach port, interfaces, configuration, admin	389
9.3.2	DNS-Anfragen nach aim1.adsoftware.com.hook.com	390
<b>Kapitel 10</b>	<b>OSI-Schicht 7: Anwendungen</b>	<b>393</b>
10.1	Applikations-Analyse in diesem Buch	393
10.1.1	TCP/IP und Appl. Layer	394
10.1.2	Typische Fehler in Client/Server-Dialogen	394
10.1.3	Fallstudie: Windows 95-Client	395
10.1.4	Fallstudie: Windows XP-Client	395
10.1.5	Fallstudie: Voice over IP und Provider-WAN	395
10.2	TraceMagic: Funktionen und Einstellungen	395
10.2.1	SpiderMagic: TCP/IP und Appl. Layer	395
10.2.2	SpiderMagic: SMB (Windows, OS/2, Samba)	397
10.2.3	SpiderMagic: NCP (Novell NetWare)	397
10.2.4	SpiderMagic: HTTP (WWW: Internet, Intranet)	399
10.2.5	SpiderMagic: Oracle – TNS	399
10.2.6	SpiderMagic: Reconstructed Files (rc.files)	400
10.2.7	SpiderMagic: VoIP (Voice over IP)	401
<b>Kapitel 11</b>	<b>TCP- und Applikations-Analyse</b>	<b>403</b>
11.1	TCP-Analyse als Teil der Applikations-Analyse	403
11.1.1	TCP-Sitzungsverhalten der Anwendungen	404
11.1.2	IP-Hosts: Teilnehmerverhalten	404
11.1.3	Event-Log: Zusammenhänge und Abläufe	404
11.1.4	Client-Zugriffe auf Server-Ressourcen: Erfolg und Misserfolg	404
11.2	Praktisches Beispiel: ICA/Citrix Metaframe	405
11.2.1	TCP-Port-Analysis (TraceStatistics, Tabelle 3)	405
11.2.2	IP-Host-Analysis (TraceStatistics, Tabelle 4)	412
11.2.3	Event-Log (Abläufe und Zusammenhänge)	418
11.2.4	File Services: Nachweis aller Dateizugriffe	421
11.2.5	SMB: Denied Resources (Zugriffsfehler)	423
11.2.6	Name Services/Tabellen	423

Teil III	Fallstudien zu den OSI-Schichten 1 bis 7	427
Kapitel 12	OSI-Schicht 7: Client/Server-Dialoge	429
12.1	TCP-Analyse als Teil der Applikations-Analyse	429
12.1.1	TCP-Analyse als Basis der Applikations-Analyse	430
12.1.2	Bedeutung einer ganzheitlichen, verknüpften Vorgehensweise	430
12.2	Mutation von Dateinamen	430
12.2.1	SAP Login	430
12.2.2	Mutationen mit Sonderzeichen	436
12.2.3	Interne Programmaufrufe des Clients als Server-Zugriffe	439
12.2.4	Aus SAMPLE.TXT wird MCF-SAMPLE.TXT	441
12.2.5	Net-Install sucht nach NiAgnt32.exe.Manifest (u. a.)	442
12.2.6	Doppelt genäht hält besser: .EXE.PIF, .EXE.COM, .EXE.BAT ...	444
12.2.7	Aus Dateien werden Verzeichnisse	446
12.3	Suche nach Dateien, die es nicht gibt	448
12.3.1	Überall ist foo	448
12.3.2	Datei-Endung, aber kein Datei-Name	449
12.3.3	%VARIABLEN% werden nicht aufgelöst	449
12.3.4	Suche mit Datei-Verkettungen als Pfadangabe	450
12.3.5	Verzeichnispfade mit Laufwerksbuchstaben	450
12.3.6	Share-Pfade werden als Verzeichnispfade missbraucht	453
12.3.7	UNC-Pfade werden als Verzeichnispfade missbraucht	454
12.4	Endlosschleifen bei Dateizugriffen	455
12.4.1	Endlossuche nach denselben Dateien	455
12.4.2	Mehrfachlesen am selben Datei-Offset	460
12.4.3	Extrem viele Zugriffe auf dieselbe Datei	461
12.4.4	Extreme Wiederholung derselben Datei-Anfrage	462
12.4.5	Extreme Suche nach DESKTOP.INI	462
12.4.6	Endlose Dateisuche in wechselnden Verzeichnissen	464
12.4.7	Extremes Öffnen/Lesen/Schließen von URL-Dateien	464
12.5	WWW: Fehler bei HTTP-Zugriffen	469
12.5.1	Einstellungen vor Beginn der Analyse	469
12.5.2	Event-Log: Ablauf und Zusammenhänge	470
12.5.3	Zugriffsstatistik: Nachweis aller Client-Requests und Server-Replies	470
Kapitel 13	OSI-Schicht 7: Fallstudie Windows 9x-Client	473
13.1	DHCP/ARP: Die neue IP-Adresse	473
13.1.1	DHCP: Request zum Bezug der eigenen IP-Adresse	473
13.1.2	ARP: zur Verifikation der IP-Adresse (»Gratuitious ARP«)	476

13.2	WINS und GETDC	477
13.2.1	WINS: Anmeldung am WINS-Server	477
13.2.2	WINS: Abfragen der IP-Adresse des PDC	481
13.2.3	SMB: GETDC-Request zur Bestätigung des PDC	482
13.2.4	WINS: Abfragen der IP-Adresse des PDC	483
13.3	SMB: NETLOGON	485
13.3.1	OSI-Schicht 4: TCP-SYN	485
13.3.2	OSI-Schicht 5: NetBIOS Session Request	487
13.3.3	OSI-Schicht 7: SMB Verify Dialect	489
13.3.4	OSI-Schicht 7: SMB Session Setup/Tree Connect	490
13.4	SMB: Create (and More)	492
13.4.1	Create – LSARPC	492
13.4.2	Create – NETLOGON	492
13.5	WINS-Refresh: irreguläre Wiederholungen	492
13.5.1	Vermutung: Die WINS Lease Time ist zu kurz	492
13.5.2	Messdaten: Filter auf WINS und DHCP	495
13.6	TraceMagic: Auswertungen und Tabellen	496
13.6.1	HostMagic/SingleHosts	496
13.6.2	HostMagic/HostPairs	496
13.6.3	HostMagic/TCP-Port Statistics	498
13.6.4	SpiderMagic/TCP/IP-Analyse (Übersicht)	499
Kapitel 14	OSI-Schicht 7: Fallstudie Windows XP-Client	503
14.1	TraceMagic: Wann welches Modul?	504
14.2	TraceMagic/HostMagic	505
14.2.1	Einstellungen vor dem Start	505
14.2.2	Ergebnisse: Device Detection (aktive Komponenten)	512
14.2.3	Ergebnisse: Name Services (WINS, UDP-138, DNS)	514
14.3	TraceMagic/SpiderMagic	520
14.3.1	Einstellungen vor dem Start	520
14.3.2	Einblicke während der laufenden Analyse	529
14.3.3	TraceReport: Erzeugung der Ergebnistabellen des Analyse-Durchgangs	533
14.3.4	TraceHistory: Datenbankfenster mit Sicht auf die Ergebnis-Dateien	534
14.3.5	TraceStatistics: Die Datenbank der TCP/IP- und SMB-Statistiken	538
14.4	TraceMagic/Event-Log und EventFilter	570
14.4.1	Event-Filter auf NiAgnt32.exe	572
14.4.2	GETDC-Befehle via Broadcast	574

14.4.3	Client ruft TCP-SYN auf Port 445, Server gibt TCP-RST zurück; SMB-IPC-Zugriff über Port 139	576
14.4.4	Mehrfaches Lesen von 1.024 Bytes am selben Offset = 0 von LSARPC und SAMR	578
14.4.5	Mehrfache Wiederholungen derselben sinnlosen DNS-Anfragen	584
14.4.6	Server-Share wird als verstümmelte Datei-Anfrage missbraucht	586
14.4.7	Zugriffe auf (und Abarbeiten von) NI5_FH.BAT und rc.files	587
14.4.8	Zugriff auf die Datei NiApMgmt.dll – verzögert durch TCP-ReTx	600
14.4.9	Verdacht: IP-Pakete treten in verdrehter Reihenfolge auf	601
14.4.10	Router meldet: TTL = 0/Paket wurde verworfen	604
14.5	Fazit der Fallstudie	607
Kapitel 15	OSI-Schicht 7: Fallstudie Voice over IP	609
15.1	Das VoIP-Projekt: Ausgangslage	609
15.2	Voice over IP: RTP und RTCP	610
15.2.1	TCP: Steuerdaten der VoIP-Endpunkte	610
15.2.2	UDP und RTP (Real Time Protocol)	610
15.2.3	UDP und RTCP (Real Time Control Protocol)	610
15.2.4	UDP-Ports für RTP und RTCP	611
15.3	Analyse in Castrop-Rauxel (Niederlassung)	611
15.3.1	Der Messpunkt	611
15.3.2	TCP Window Size/TCP Keep Alive	612
15.3.3	SNMP mit Community public	612
15.3.4	Laufzeitschwankungen: VoIP-Analyse im Observer	613
15.3.5	MAC-Fehler (und vermeintliche TCP/IP-Fehler)	615
15.3.6	IP-Pakete treffen in verdrehter Reihenfolge ein	628
15.3.7	Untersuchung der TTL-Werte	631
15.3.8	RTP-Paketverluste und RTCP-Meldungen dazu	631
15.4	Analyse in der Unternehmenszentrale	636
15.4.1	Der Messpunkt	636
15.4.2	IP-Hosts und Paketdreher	636
15.4.3	IP-Hosts und Verdopplungen von Paketen und IDs	637
15.4.4	IP-Hosts und wechselnde TTL-Werte	639
15.5	Fazit der WAN-Analyse im VoIP-Umfeld	649
15.6	FilterMagic: Der Franzose in Castrop-Rauxel	650
Kapitel 16	Schlusswort: Zeit ist Geld	663
16.1	Zeitnah und online	663
16.2	Analyse-Ergebnis: HTML-Projekt	663
16.3	WWW: Projekt-Steuerung	664

16.4	TraceMagic: LAN-WAN Information Management	664
16.5	Ausblick	668
Anhang	Internetadressen von Herstellern und Produkten	671
	Stichwortverzeichnis	673
	15 Fragen an den Autor	697
	Der Autor über sich	701