

Gerhard Lienemann

TCP/IP-Praxis

Design, Management, Analyse

Verlag Heinz Heise

Inhaltsverzeichnis

Vorwort – 13

1	Integration heterogener Netzwerke – 15
1.1	Problemszenario – 15
1.1.1	Historisch gewachsene LAN-Vielfalt – 15
1.1.2	Das Problem eines effektiven Netzwerkmanagements – 16
1.1.3	Anwendungsisolation in isolierten Netzwerken – 17
1.2	Lösungsansätze – 17
1.2.1	Schaffung einheitlicher Protokollstrukturen – 18
1.2.2	Einsatz zentraler Netzwerkmanagement-Tools – 19
1.2.3	Nutzung vorhandener LAN/WAN-übergreifender Software – 21

2	Netzwerkdesign: Integration – 23
2.1	Der SNA-Interconnect-Controller IBM 3172 – 24
2.1.1	SNA und TCP/IP – 24
2.1.2	Die technischen Details – 25
2.1.3	Konfiguration mit OF/2 – 28
2.1.3.1	Installation des OF/2 – 28
2.1.3.2	Das OF/2-Menüsystem – 29
2.1.3.3	Definition eines 3172-Controllers – 31
2.1.3.4	Remote Management – 38
2.1.4	VTAM-Definitionen – 40
2.1.5	TCP/IP-Profile unter MVS – 44
2.2	LAN-WAN-Integration durch Data Link Switching (DLSw) – 60
2.2.1	DLSw-Konzeption – 61
2.2.2	Das Switch-to-Switch Protocol (SSP) – 63

2.3	Router im LAN/WAN-Verbund	- 66
2.3.1	Router-Charakteristika	- 66
2.3.2	Der Time-To-Live-Wert (TTL)	- 68
2.3.3	Funktionsweise des Transportalgorithmus	- 68
2.3.3.1	Allgemeines	- 69
2.3.3.2	Unicast	- 69
2.3.3.3	Multicast	- 70
2.3.3.4	Broadcasts	- 71
2.3.4	Betrieb und Wartung	- 71
2.3.4.1	Router-Initialisierung	- 72
2.3.4.2	Out-Of-Band-Access	- 73
2.3.4.3	Hardware-Diagnose	- 74
2.3.4.4	Router-Steuerung	- 74
2.3.4.5	Sicherheitsaspekte	- 75
2.4	Router-Konfiguration	- 75
2.4.1	Beispiel: PROTEON	- 75
2.4.1.1	Die Prozesse	- 76
2.4.1.2	Das PROTEON-Menüsystem	- 78
2.4.1.3	Konfigurationsbeispiel: Einrichtung einer IP-Adresse	- 83
2.4.1.4	Konfigurationsbeispiel: Definition einer statischen Route	- 84
2.4.1.5	Konfigurationsbeispiel: Aktivierung von Protokollfiltern	- 84
2.4.1.6	Konfigurationsbeispiel: Aktivierung des dynamischen Routings	- 85
2.4.2	Beispiel: CISCO	- 86
2.4.2.1	Die Bedieneroberfläche	- 87
2.4.2.2	Erstkonfiguration und Inbetriebnahme	- 95
2.4.2.3	Konfigurationsänderungen	- 100
2.4.2.4	CISCO Works	- 101

3

Netzwerkmanagement - 102

3.1	Einfachstes Netzwerkmanagement	- 107
3.1.1	Das „ping“-Kommando	- 108
3.1.2	Das „traceroute“-Kommando	- 110
3.1.3	Das „netstat“-Kommando	- 111
3.2	NetView for AIX	- 114
3.2.1	Herkunft und Vererbung des Produkts	- 115
3.2.2	Management-Applikationen	- 116
3.2.2.1	Drop-in-applications	- 117
3.2.2.2	Tool Applications	- 127
3.2.2.3	Map Applications	- 128
3.2.3	Installation	- 128

3.2.3.1	Systemvoraussetzungen	– 128
3.2.3.2	Installation über das SMIT	– 130
3.2.4	Die Komponenten	– 132
3.2.4.1	Submap-Window	– 132
3.2.4.2	Control Desk Window	– 134
3.2.4.3	Tools Window	– 136
3.2.4.4	Navigation Tree Window	– 137
3.2.5	Map-Konfiguration	– 137
3.2.5.1	NetView „lernt“ die Topologiestruktur	– 138
3.2.5.2	Manuelle Modifikation der Topologie	– 139
3.2.5.3	Die Topologieobjekte und ihr Status	– 140
3.2.5.4	Die Management Information Base (MIB)	– 141
3.2.6	Management mit SNMP	– 142
3.2.6.1	SNMP-Konfiguration im NetView	– 143
3.2.6.2	Herstellung der Funktionsfähigkeit von SNMP-Agenten	– 145
3.2.6.3	SNMP-Kommandos	– 147
3.2.7	Monitoring – Event Log	– 148
3.2.8	Schwellwerte für die Management-Sensibilität	– 150
3.2.9	Produktübersicht: Management-Anwendungen	– 150

Troubleshooting in TCP/IP-Netzwerken – 152

4.1	Netzcharakteristika und -symptome	– 153
4.1.1	Backbone-Konzept	– 153
4.1.1.1	Collapsed Backbones	– 155
4.1.2	Bridging-Mechanismen	– 156
4.1.2.1	‘All Routes Broadcast – Non-broadcast return	– 156
4.1.2.2	Single Route Broadcast – All Routes Return	– 158
4.1.3	Backup-Konzepte	– 159
4.1.3.1	Individuelle ISDN-Backups	– 160
4.1.3.2	Vermaschte Netzstruktur	– 161
4.1.4	Broadcast-Stürme	– 161
4.1.4.1	Broadcast-Filter	– 162
4.1.4.2	Broadcasts im Routing Information Protocol	– 162
4.1.4.3	Broadcasts im Address Resolution Protocol	– 163
4.1.4.4	Broadcasts im BOOT-Protokoll	– 163
4.1.4.5	Remote Polling	– 163

4.1.5	Retransmissions	- 164
4.1.6	Maximum Transfer Unit (MTU)	- 165
4.1.7	Buffer-Probleme	- 166
4.2	Netzwerkmonitoring	- 167
4.2.1	Netzwerkdesign	- 167
4.2.2	Schwellwert-Kalibrierung	- 168
4.2.3	Logging mit dem Syslog-Daemon	- 169
4.3	Netzwerkanalyse	- 172
4.3.1	Die Wahl des Standorts	- 173
4.3.2	Der Netzwerk-Trace	- 174
4.3.3	Netzwerkstatistik	- 175
4.4	Netzwerkanalyse-Tools	- 175
4.4.1	Remote Network Monitoring (RMON)	- 176
4.4.1.1	Konzeption	- 176
4.4.1.2	Die RMON-MIB	- 177
4.4.2	Network General: Distributed Sniffer Server (DSS)	- 194
4.4.2.1	Konzeption	- 195
4.4.2.2	Die Software-Komponenten	- 197
4.4.2.3	Token-Ring-II Analyzer	- 198
4.4.2.4	Übersicht: Symptome	- 214
4.4.2.5	Übersicht: Diagnosen	- 217
	Netzwerkprogrammierung	- 218
5.1	Client-Server-Prinzip	- 219
5.1.1	Client-Server-Typen	- 220
5.1.2	Client-Server-Kommunikation	- 221
5.2	Socket-Programmierung	- 222
5.2.1	Socket-Typen	- 222
5.2.1.1	Stream-Sockets	- 223
5.2.1.2	Datagramme	- 223
5.2.1.3	Raw-Sockets	- 223
5.2.2	Kriterien zur Wahl des Socket-Typs	- 223
5.2.3	TCP-Socket-Session	- 224
5.2.4	Datenstrukturen	- 225
5.2.4.1	Port-/Socket-Nummern	- 225
5.2.4.2	Klassendefinitionen der IP-Adressen	- 226
5.2.4.3	Socket-Adresse	- 227
5.2.4.4	Adreßfamilien	- 227
5.2.4.5	Protokollfamilien	- 227
5.2.4.6	Prototypen der Socket-Funktionsaufrufe	- 228
5.2.5	Systemaufrufe	- 231
5.2.6	Programmbeispiel	- 236

5.3	Remote Procedure Calls (RPCs)	– 242
5.3.1	Konzept der RPCs	– 243
5.3.1.1	Transport	– 244
5.3.1.2	Aufrufsemantik	– 244
5.3.1.3	Verteiltes RPC-Programmkonzept	– 245
5.3.1.4	RPC-Request und RPC-Response	– 246
5.3.1.5	External Data Representation (XDR)	– 248
5.3.1.6	Portmapper	– 253
5.3.2	RPC-Programmlogik	– 254
5.3.2.1	RPC-Client	– 254
5.3.2.2	RPC-Server	– 255
5.3.3	RPC Application Program Interface	– 256
5.3.4	Programmbeispiel	– 257

XWindows – OSF/Motif – 262

6.1	Konzeption – Übersicht	– 263
6.1.1	X Display Server	– 263
6.1.2	Display-Manager	– 265
6.1.3	Window-Manager	– 269
6.1.4	X-Clients	– 270
6.2	Beschreibung der X-Client-Anwendungen	– 270
6.2.1	Hilfsmittel des Desktops	– 270
6.2.2	Anwendungen für Anzeige und Tastatur	– 271
6.2.3	Anwendungen zur Verwaltung von Schriftarten	– 271
6.2.4	Grafikanwendungen	– 271
6.2.5	Druckeranwendungen	– 272
6.2.6	Resource Management	– 272
6.2.7	Diverse Anwendungen	– 272
6.3	Der Window-Manager (mwm)	– 273
6.3.1	Das Standard-Root-Menü	– 273
6.3.2	Erstellung individueller Root-Menüs (.mwmrc)	– 274
6.4	Die XTerm-Konfiguration	– 280
6.4.1	XTerm-Parameter	– 281
6.4.2	Umleitung der Anzeige (DISPLAY)	– 282
6.4.3	XClipboard	– 283
6.5	Weitere X-Clients	– 284
6.5.1	XClock und XCalc	– 284
6.5.2	Die Printer-Clients	– 286
6.6	X-Security	– 287
6.6.1	Hostbasierte Zugriffskontrolle (xhost)	– 287
6.6.2	Userbasierte Zugriffskontrolle (xauth)	– 288

6.7	Das X-Protokoll	- 297
6.8	XDisplay-Server-Produkte	- 298
6.8.1	Digital Excursion Version 1.1	- 298
6.8.2	Hummingbird eXceed Version 5	- 302
Security in IP-Netzen - 308		
7.1	Internal Security	- 309
7.1.1	Hardware Security	- 309
7.1.2	UNIX-Zugriffsrechte	- 310
7.1.2.1	Standard-UNIX-Rechte	- 310
7.1.2.2	SVTX (Sticky Bit)	- 313
7.1.2.3	SUID (Set User Id) und SGID (Set Group Id)	- 313
7.1.2.4	ACL (Access Control List)	- 314
7.1.3	Benutzerauthentifizierung	- 315
7.1.4	Die R-Kommandos	- 317
7.1.4.1	Rlogin	- 319
7.1.4.2	Rsh	- 319
7.1.4.3	Rcp	- 320
7.1.5	Das Remote-Execution-Kommando (rexec)	- 321
7.1.6	Trojanische Pferde	- 322
7.2	External Security	- 323
7.2.1	Öffnung isolierter Netzwerke	- 323
7.2.2	Das LAN-WAN-Sicherheitsrisiko	- 324
7.2.3	Firewall-Konzepte	- 326
7.2.3.1	Screening-Router	- 326
7.2.3.2	Application Level Gateway	- 327
7.2.3.3	Circuit Level Gateway	- 328
7.3	Die Sicherheitsalternative: Isolation?	- 329
Das „Internet“ - 331		
8.1	Warum „Internet“?	- 331
8.1.1	Der Internet-Kunde	- 332
8.1.2	Der „virtuelle Marktplatz“	- 337
8.1.3	„Internet-Netiquette“	- 339
8.1.4	Das Internet-Risiko	- 340
8.2	Internet-Service-Provider (ISP)	- 340
8.2.1	Service-Provider: Leistung und Kosten	- 341
8.2.1.1	EUnet	- 342
8.2.1.2	NTG/Xlink	- 343
8.2.1.3	MAZ	- 344
8.2.2	Tarifbeispiele einiger Service-Provider	- 344
8.3	Dienste im Internet	- 346
8.3.1	Electronic-Mail	- 346

8.3.2	NetNews/UseNet	- 350
8.3.3	Gopher	- 352
8.3.4	FTP	- 355
8.3.4.1	FTP-Sessionaufbau	- 360
8.3.4.2	FTP-Dateiübertragung	- 361
8.3.5	Archie	- 363
8.3.6	World Wide Web (WWW)	- 364
8.3.7	Weitere Dienste	- 366
8.3.7.1	WAIS	- 367
8.3.7.2	IRC	- 367
8.3.7.3	Prospero	- 367
8.3.7.4	Alex	- 367
8.3.7.5	WhoIs	- 368
8.3.7.6	X.500	- 368
8.3.7.7	NetFind	- 368
8.3.7.8	Finger	- 368
8.3.7.9	Veronica	- 369
8.3.7.10	TELNET	- 369
8.4	WWW-Publishing	- 369
8.4.1	Publishing Guidelines	- 370
8.4.2	Einführung in HTML	- 371
8.4.3	Erstellung einer Homepage	- 373
 Anhang - 377		
A.1	Windows-Socket-1.1 – Funktionsaufrufe	- 377
A.2	RPC-Aufrufe	- 378
A.3	Abkürzungen aufgelöst	- 381
A.4	Literaturverzeichnis	- 384
A.5	Register	- 386