

Gerhard Lienemann

TCP/IP Praxis

Dienste, Sicherheit, Troubleshooting

3., aktualisierte Auflage

Heise Zeitschriften Verlag

Inhaltsverzeichnis

1	TCP/IP im Internet	1
1.1	Internetdomain und Subnetz	2
1.2	Einrichtung eines DNS-Servers.	3
1.2.1	Funktionsweise.	4
1.2.2	Auswahl der Betriebssystem-Plattform	7
1.2.3	Basiskonfiguration	7
1.2.4	DNS-Datenfluss	25
1.2.5	Dynamic DNS (DDNS).	27
1.2.6	Zusammenspiel von DNS und Active Directory.	30
1.3	Einrichtung eines Mailservers.	31
1.3.1	Sendmail-Konfiguration	32
1.3.2	Einrichtung der Mail-Accounts	33
1.3.3	Der MX-Record	34
1.3.4	Einrichtung des POP3-Dienstes	34
1.3.5	Konfiguration eines Mail-Clients unter Windows 2000.	35
1.3.6	Mail-Kommunikation.	37
1.3.7	Mail-Logdatei	38
1.4	Einrichtung eines Webservers.	39
1.4.1	Der »MS Internet Information Server«	40
1.4.2	Der »Apache«-Server.	44
2	Router im LAN/WAN-Verbund	55
2.1	Router-Charakteristika	55
2.1.1	Aufgaben.	55
2.1.2	Anforderungen	56
2.1.3	Funktionsweise.	58
2.2	Betrieb und Wartung	61
2.2.1	Router-Initialisierung.	62
2.2.2	Out-Of-Band-Access.	62
2.2.3	Hardware-Diagnose.	63
2.2.4	Router-Steuerung	64
2.2.5	Sicherheitsaspekte.	64
2.3	Router-Konfiguration (am Beispiel von CISCO-Routern).	65
2.3.1	Router-Modelle für unterschiedlichen Einsatz	65
2.3.2	Das Betriebssystem CISCO IOS.	70
2.3.3	Konsolenbetrieb	70

2.3.4	Router-Modi	72
2.3.5	Konfigurationsbeispiel: Internetzugang	77
3	Web-Anwendungsentwicklung	81
3.1	Basisobjekte	83
3.1.1	Statische HTML-Seiten	83
3.1.2	Dynamische HTML-Seiten	84
3.1.3	Formularverarbeitung	85
3.2	Abgrenzung	91
3.2.1	Die klassische Anwendungsentwicklung	91
3.2.2	Sequenzen, Iterationen und mehr	92
3.3	HTTP-Kommunikation	94
3.3.1	Grundlagen	95
3.3.2	Methoden zur Kommunikation	96
3.3.3	HTTP-Statusmeldungen	100
3.4	CGI-Programmierung	102
3.4.1	Das Prinzip	102
3.4.2	Umgebungsvariablen	103
3.4.3	CGI-Statusüberwachung	107
3.5	Skripting	115
3.5.1	Client-Side- und Server-Side-Skripting	115
3.5.2	Skriptsprachen	117
3.6	Active Server Pages	122
3.6.1	Allgemeine Funktionsweise	123
3.6.2	ASP-Umgebung	126
3.6.3	Variablen	127
3.6.4	Cookies	134
3.6.5	Programmsteuerung	138
4	Sicherheit im Netz	145
4.1	Interne Sicherheit	147
4.1.1	Hardware-Sicherheit	149
4.1.2	UNIX-Zugriffsrechte	149
4.1.3	Windows-Zugriffsrechte	154
4.1.4	Benutzerauthentifizierung	156
4.1.5	Die R-Kommandos	158
4.1.6	Remote Execution (rexec)	161
4.2	Externe Sicherheit	162
4.2.1	Öffnung isolierter Netzwerke	163
4.2.2	Das LAN/WAN-Sicherheitsrisiko	164
4.3	Angriff aus dem Netz	165
4.3.1	»Hacker« und »Cracker«	166
4.3.2	Scanning-Methoden	167
4.3.3	Denial-of-Service-Attacken	170
4.3.4	DNS-Sicherheitsprobleme	173
4.3.5	Betriebssystem-Schwachstellen	176
4.4	Aufbau eines Sicherheitssystems	181
4.4.1	Grundschutzhandbuch für IT-Sicherheit des BSI	182
4.4.2	Das 3-Komponenten-System	185

4.5	Firewall-System	187
4.5.1	Grundlagen	189
4.5.2	Firewall-Typen	191
4.5.3	Firewall-System »Firewall-1«	195
4.6	Content Security System	205
4.6.1	Prinzip	205
4.6.2	Produkte	206
4.6.3	Implementationsbeispiel	206
4.7	Intrusion-Detection- und Intrusion-Response-Systeme	210
4.7.1	IDS-Analyseverfahren	210
4.7.2	IDS-/IRS-Architektur	211
4.7.3	Rechtliche Situation	212
4.8	Public Key Infrastructure (PKI)	213
4.8.1	Authentifikation	213
4.8.2	Verschlüsselung	216
4.8.3	Zertifikate	221
4.8.4	Signaturen	223
4.9	Virtual Private Networks (VPN)	226
4.9.1	Grundlagen	226
4.9.2	Implementationsbeispiel: Windows 2000 IPsec	227
5	Troubleshooting in TCP/IP-Netzwerken	239
5.1	Netzwerkcharakteristika und -Symptome	240
5.1.1	Backbone-Konzept	240
5.1.2	Bridging-Mechanismen	243
5.1.3	Backup-Konzepte	246
5.1.4	Broadcast-Stürme	248
5.1.5	Retransmissions	251
5.1.6	Maximum Transfer Unit (MTU)	252
5.1.7	Buffer-Probleme	253
5.2	Netzwerkmonitoring und -analyse	253
5.2.1	Netzwerk-Design	254
5.2.2	Schwellwert-Kalibrierung	255
5.2.3	Logging mit dem syslog-daemon	256
5.2.4	Der Netzwerk-Trace	258
5.2.5	Netzwerk-Statistik	261
5.2.6	Remote Network Monitoring (RMON)	261
5.2.7	Analyse in Switched LANs	265
5.2.8	Analyse-Tool »Basic Sniffer«	265
5.2.9	Analyse-Szenario	270
	Stichwortverzeichnis	273