

# **Linux-Netzwerke**

**Aufbau, Administration, Sicherung**

**Dr. Stefan Fischer, Ulrich Walther**

**SuSE PRESS**

# Inhaltsverzeichnis

<b>I Grundlagen</b>	<b>1</b>
<b>1 Einführung</b>	<b>3</b>
1.1 Motivation	3
1.2 Aufbau des Buches.	5
<b>2 Geschichte, Entwicklung und Aufbau des Internet</b>	<b>7</b>
2.1 Entstehungsgeschichte.	7
2.2 Größenentwicklung.	9
2.3 Aufbau des Internet.	9
2.3.1 Gemeinsames Adressierungsschema	10
2.3.2 Client-Server-Modell.	.11
2.3.2.1 Server im Internet?	.11
2.3.2.2 Client-Zugriff auf Server	11
2.3.2.3 Dienste im Internet	.12
<b>3 Das Internet-Referenzmodell</b>	<b>13</b>
3.1 Schichtenmodelle für die Netzwerkkommunikation	13
3.1.1 Architektur.	.13
3.1.2 Datenfluß im Schichtenmodell	.14
3.1.3 Behandlung des Pakets während der Übertragung	15
3.2 Das ISO/OSI-Schichtenmodell	.16
3.3 Schichtenmodell des Internet	.19
3.3.1 Architektur.	.19

3.3.2	Netzzugangsschicht	19
3.3.3	Internetschicht	20
3.3.4	Transportschicht	21
3.3.5	Anwendungsschicht	22
<b>4</b>	<b>Ein paar Worte zu Linux</b>	<b>25</b>
4.1	Die Entstehung von Linux	25
4.2	Linux-Distributionen	27
<b>II</b>	<b>Internet-Technik</b>	<b>29</b>
<b>5</b>	<b>Die TCP/IP-Protokolle</b>	
5.1	Installation von Netzwerkkarten	
5.1.1	Neuinstallation	
5.1.2	Einbau einer Karte	
5.2	Internet Protocol IP	
5.2.1	Aufbau der IP-Pakete (Datagramme)	
5.2.2	Adressierung im IP	
5.2.3	IP-Subnetze und IP-Subnetzmasken	
5.2.4	Klassenlose IP-Adressen	
5.2.5	IP-Adressen für die Blumenpeter GmbH	
5.2.6	Fragmentierung von Datagrammen	
5.3	Routing	
5.3.1	Routing im Internet	
5.3.2	Direkte und indirekte Auslieferung von Paketen	
5.3.3	Routing-Tabellen	
5.3.4	Ein Routing-Beispiel	
5.3.5	Standard- und hostspezifische Routen	
5.3.6	Der Routing-Algorithmus des IP	
5.3.7	Konfiguration von Routing-Tabellen in Linux	
5.3.8	Weiterführendes	
5.4	Ausblick: IP Version 6 (IPv6)	
5.4.1	Merkmale von IPv6	
5.4.2	Das IPv6-Paket im Vergleich	

5.4.3	Syntax von IPv6-Adressen	55
5.4.4	Aktueller Status von IPv6	56
5.5	Wichtiges Konzept: Tunneling	57
5.6	Internet Control Message Protocol (ICMP)	58
5.7	Transport Control Protocol (TCP)	59
5.7.1	Überblick	59
5.7.2	Zuverlässige Übertragung	59
5.7.3	Verbindungsorientierte Übertragung	60
5.7.4	TCP-Paketformat	60
5.7.5	Verbindungsaufbau	61
5.7.6	Portnummern	62
5.8	User Datagram Protocol (UDP)	67
5.9	Zusammenfassung	69
<b>6</b>	<b>Client-Server-Kommunikation</b>	<b>71</b>
6.1	Client-Server im Internet	71
6.2	Ablauf einer Kommunikationsbeziehung	72
6.3	Lokalisierung des Servers	72
6.4	Well-Known Ports	73
6.5	Client-Server-Anwendungen selbst programmieren	73
6.5.1	Idee der Socket-Schnittstelle	74
6.5.2	Funktionen der Socket-Schnittstelle	75
6.5.3	Ablauf einer Client-Anwendung basierend auf der Socket-Schnittstelle	78
6.5.4	Ablauf eines Server-Programms	79
6.5.5	Zusammenspiel der Anwendungen	80
6.5.6	Sockets in Java	80
6.6	Zusammenfassung	84
<b>7</b>	<b>Internet-Dienste</b>	<b>85</b>
7.1	E-Mail	86
7.1.1	Simple Mail Transfer Protocol (SMTP)	86
7.1.2	Mail-Server-Programm	87
7.1.3	Mailing-Tools	89

# Inhaltsverzeichnis

7.1.4	Funktionsumfang moderner Mailprogrammen	
7.1.5	Heutige E-Mail-Programme	
7.1.6	Besonderheit: Mailinglisten	
7.2	Network News	
7.2.1	Diskussionsgruppen ( <i>Newsgroups</i> ) im Internet	
7.2.2	News-Server	
7.2.3	Funktionsweise von NNTP	
7.2.4	News-Reader	
7.2.5	Einrichten eines News-Servers unter SuSE Linux	
7.2.6	News-Clients unter Linux	
7.3	File Transfer Protocol (FTP)	
7.3.1	Aufgaben, Architektur und Eigenschaften	
7.3.2	AnonymousFTP	
7.3.3	FTP-Server	
7.3.4	FTP-Clients	
7.3.5	Eine FTP-Sitzung	
7.3.6	Konfiguration des WU-FTP-Servers für Linux	
7.4	World Wide Web (WWW)	
7.4.1	Einführung	
7.4.2	Uniform Resource Locators (URLs)	
7.4.3	HTML	
7.4.4	Hypertext Transfer Protocol (HTTP)	
7.4.5	Web-Server	
7.4.6	Web-Browser	
7.4.7	Installation und Konfiguration des Apache-Web-Server unter Linux	.114
7.5	Zusammenfassung	.115
<b>8</b>	<b>Domain Name Service (DNS)</b>	
8.1	Symbolische Namen und IP-Adressen	
8.1.1	Motivation	
8.1.2	Erste Ansätze zur Namensverwaltung	
8.2	Symbolische Namen	
8.2.1	Aufbau der DNS-Namensbereiche	

8.2.2	Einrichtung eines symbolischen Namens für einen Rechner.	.119
8.3	Aufbau der DNS-Datenbank.	.120
8.4	Nameserver.	.121
8.5	Abfrage der DNS-Datenbank.	.122
8.6	DNS und SuSE Linux.	.123
8.6.1	Szenario.	.123
8.6.2	Umsetzung in eine DNS-Datenbank für BIND v4	.125
8.6.3	Start des Systems.	.128
8.6.4	Test des Nameservers.	.129
8.6.5	BIND in der Version 8.	.129
8.7	Zusammenfassung	.135
<b>III</b>	<b>Sicherheit</b>	<b>137</b>
<b>9</b>	<b>Gefahren und Risikoabschätzung</b>	<b>139</b>
9.1	Was ist Sicherheit?.	.139
9.2	Konzeptionelle Probleme des Netzwerkbetriebs	.140
9.3	Detaillierte Kommunikations- und Risikoanalyse	.142
9.3.1	Kommunikationsbedarf.	.142
9.3.2	Wichtige Fragen bei der Risikoanalyse	.143
9.3.3	Risiken durch Benutzer.	.144
9.3.4	Risiken durch Würmer, Viren und Trojanische Pferde	.145
9.3.5	Sicherheitsrisiken der verwendeten Protokolle und Dienste.	.146
9.4	Zusammenfassung	.151
<b>10</b>	<b>Angriffe</b>	<b>153</b>
10.1	SYNFlooding	.153
10.1.1	Idee von SYN Flooding	.153
10.1.2	Funktionsweise des SYN Flooding	.154
10.2	Verteilte Denial-of-Service-Attacken.	.154
10.2.1	Idee der verteilten Denial-of-Service-Attacken	.155
10.2.2	Der Vorfall.	.156

## Inhaltsverzeichnis

10.2.3	tinOO	.156
10.2.4	Tribe Flood Network	.157
10.3	IP Spoofing/Sequence Number Attack	.157
10.3.1	Idee von IP Spoofing	.157
10.3.2	Ablauf des Angriffs	.158
10.4	DNS Spoofing	.159
10.4.1	Kurzer Rückblick: DNS	.160
10.4.2	Ziel des DNS Spoofing	.160
10.4.3	Idee des Angriffs	.160
10.4.4	Effekt des Angriffs	.161
10.4.5	Vorgehen beim DNS Spoofing am Beispiel	.161
10.5	Smurf- und Fraggle-Attacken	.162
10.5.1	Idee und Ziel des Angriffs	.162
10.5.2	Initiative gegen Smurf-Angriffe	.163
10.6	PingofDeath	.164
10.7	Internet Worm	.164
10.7.1	Der Vorfall	.164
10.7.2	Funktionsweise des Wurms	.165
10.7.3	Ziel des Angriffs	.166
10.8	Der Loveletter-Wurm	.167
10.9	Trojanische Pferde und andere Hintertüren	.169
10.10	Gegenmaßnahmen	.169
10.11	Zusammenfassung	.170

## 11 Sicherheitskonzepte

11.1	Allgemeine Sicherheitskonzepte	
11.1.1	Keine Sicherheit	
11.1.2	Sicherheit durch Verschleiern	
11.1.3	Sicherheit auf Rechnerbene	
11.1.4	Sicherheit auf Netzebene	
11.2	Sicherheitspolitik	
11.2.1	Vorgehen zur Umsetzung eines Sicherheitskonzepts	
11.2.2	Aufstellen der Sicherheitspolitik	
11.2.3	Umsetzung	

i-	11.2.4 Kontrolle	.176
.	11.3 Systemwerkzeuge zur Netzwerkd Diagnose	176
	11.3.1 ping	.177
	11.3.2 <b>tracert</b>	.179
	11.3.3 <b>ifconfig</b>	.181
	11.3.4 <b>netstat</b>	.184
	11.3.5 <b>tcpdump</b>	.188
	11.3.6 <b>ntop</b>	.191
	11.3.7 <b>bing</b>	.195
	11.3.8 <b>rpcinfo</b>	.197
	11.3.9 <b>nmap</b> und <b>xnmap</b>	.199
	11.4 Programme zur Prüfung der Netzsicherheit	204
	11.4.1 Funktionsweise von Netzwerkscannern	205
	11.4.2 Fähigkeiten von Netzwerkscannern	205
	11.4.3 SAINT unter Linux	207
	11.4.4 Nessus unter Linux	211
	11.5 Verdächtige Portnummern	215
	11.6 Zusammenfassung	222
<b>12</b>	<b>Firewalls</b>	<b>223</b>
	12.1 Eigenschaften von Firewalls	223
	12.1.1 Was ist ein Firewall?	224
	12.1.2 Was ein Firewall kann	224
	12.1.3 Was ein Firewall nicht kann	224
	12.1.4 Typen von Firewall-Komponenten	225
	12.2 Paketfilter	225
	12.2.1 Architektur	226
	12.2.2 Was Paketfilter damit beispielsweise können	226
	12.2.3 Was Paketfilter damit beispielsweise nicht können	227
	12.2.4 Vorteile von Paketfiltern	227
	12.2.5 Nachteile von Paketfiltern	227
	12.2.6 Zentrale Komponente eines Paketfilters: Filterregeln	227
	12.3 Bastion Hosts	229
	12.3.1 Grundlagen	229



## Inhaltsverzeichnis

12.3.2	Spezielle Bastion Hosts.	. . . . .
12.3.3	Eigenschaften des Bastion Host	. . . . .
12.3.4	Vorgehen beim Einrichten eines Bastion Hosts	. . . . .
12.4	Proxy Server (Application Gateways)	. . . . .
12.4.1	Architektur.	. . . . .
12.4.2	Warum Proxy Server?	. . . . .
12.4.3	Funktionsweise eines Proxy Servers	. . . . .
12.4.4	Vor- und Nachteile von Proxies	. . . . .
12.5	Firewall-Konfigurationen.	. . . . .
12.5.1	Dual-Homed Host-Architektur	. . . . .
12.5.2	Screened-Host-Architektur	. . . . .
12.5.3	Screened Subnet-Architektur	. . . . .
12.5.4	Variationen	. . . . .
12.6	Interne Firewalls	. . . . .
12.7	Auswahl und Betrieb eines Firewalls	. . . . .
12.8	Firewall unter Linux: ipchains	. . . . .
12.8.1	Arbeitsweise	. . . . .
12.8.2	ipchains	. . . . .
12.8.3	Konfiguration mit gcc	. . . . .
12.9	Application Proxy Server: Squid.	. . . . .
12.9.1	Funktionalität	. . . . .
12.9.2	Konfiguration	. . . . .
12.9.3	Zugriffskontrolle	. . . . .
12.9.4	Squid als transparenter Proxy	. . . . .
12.10	Zusammenfassung	. . . . .

## **13 Weitere Sicherheitsmaßnahmen**

13.1	Private IP-Adressen.	. . . . .
13.1.1	Idee privater IP-Adressen.	. . . . .
13.1.2	Adreßraum privater IP-Adressen	. . . . .
13.1.3	Regeln für die Verwendung	. . . . .
13.2	IP Masquerading und Network Address Translation (NAT)	. . . . .
13.2.1	Grundidee von Network Address Translation	. . . . .
13.2.2	Beispiel für NAT.	. . . . .

13.2.3	Konfiguration des Kernels.	261
13.2.4	Grundidee von IP Masquerading/PAT	263
13.2.5	Beispiel für Masquerading.	263
13.2.6	IP Masquerading in SuSE Linux.	264
13.3	Secure Socket Layer (SSL).	266
13.3.1	Ziele.	267
13.3.2	Zertifizierung in SSL.	267
13.3.3	Lage im Schichten-Modell.	268
13.3.4	Generelle Funktionsweise des Protokolls	268
13.3.5	Handshake-Protokoll.	269
13.3.6	Protokollablauf beim Handshake	269
13.3.7	Fehlerbehandlung	270
13.3.8	Sicherheit von SSL.	271
13.4	Virtual Private Networks (VPN).	272
13.4.1	Einführung.	272
13.4.2	Beispiel für ein VPN.	273
13.4.3	Motivation für den Einsatz von VPNs	273
13.4.4	Verfahren zur Abschottung von VPNs	274
13.4.5	VPN-Konfigurationen.	274
13.4.6	Typen von VPNs.	275
13.4.7	Realisierung von Network-Layer-VPNs	275
13.4.8	VPNs durch IP-in-IP Tunneling	275
13.4.9	VPNs mit Firewalls.	276
13.4.10	VPNs mit IPsec.	276
13.4.11	VPNs mit PPTP.	277
13.4.12	Konfiguration eines VPN am Beispiel der Blumenpeter GmbH.	278
13.4.12.1	Installation und Konfiguration von FreeS/WAN	279
13.4.12.2	Konfiguration von ipchains	281
13.5	Zusammenfassung	282
	Literaturhinweise	283