

# tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

## Unentbehrliches Netzwerk Know-how

€ 10,90

Österreich € 12,00

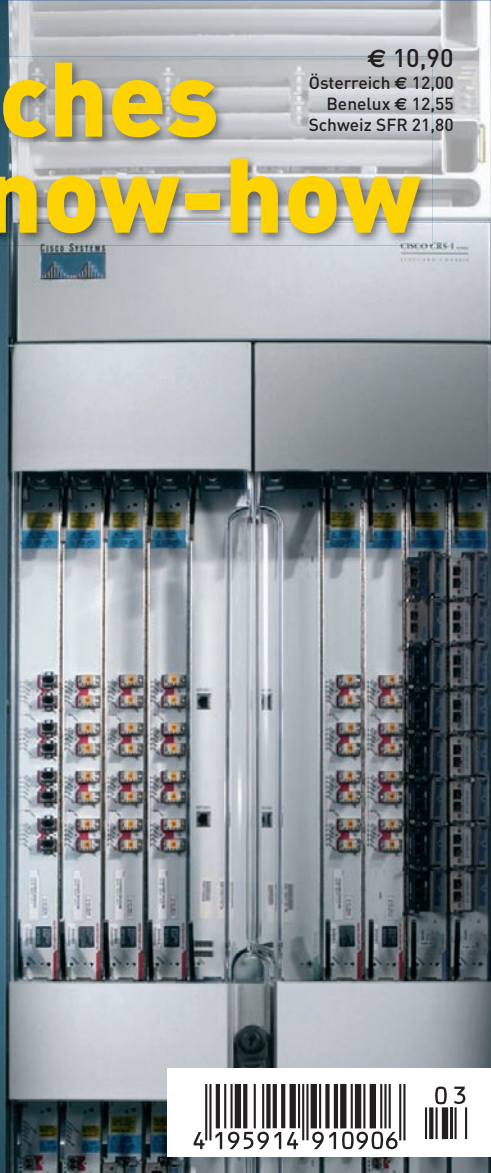
Benelux € 12,55

Schweiz SFR 21,80

- Grundlagen aus der Cisco Networking Academy
- Wissen: VLANs, Routing und Subnetze
- Praxis: LDAP & Nameserver richtig konfigurieren

## Sicherheit für Desktops und Server

- Hilfe: Katastrophenszenarien bei Active Directory
- Wissen: Zugriffskontrolle bei Samba 3
- Praxis: Linux härten



# Impressum

Chefredakteur: Michael Eckert (verantwortlich,  
Anschrift der Redaktion)  
Stellv. Chefredakteur / CvD: Albert Lauchner  
Grafik: stroemung, Michael Oliver Rupp, Yvonne Reittinger, Bernd Maier-Leppla  
Titelgestaltung: Twentyfirst Communications

## Redaktion tecCHANNEL:

Lyonel-Feiningger-Straße 26, 80807 München,  
Tel.: 0 89/3 60 86-897, Fax: -878  
Homepage: [www.tecChannel.de](http://www.tecChannel.de),  
E-Mail: [feedback@tecChannel.de](mailto:feedback@tecChannel.de)  
Autoren dieser Ausgabe: William Boswell,  
Nadine Ebel, Jochen Hein, Frank Ronneburg,  
John H. Terpstra, Jelmer R. Vernooij  
**Copyright:** Das Urheberrecht für angenommene  
und veröffentlichte Manuskripte liegt bei der  
IDG Business Verlag GmbH. Eine Verwertung  
der urheberrechtlich geschützten Beiträge und  
Abbildungen, vor allem durch Vervielfältigung  
und/oder Verbreitung, ist ohne vorherige schrift-  
liche Zustimmung des Verlags unzulässig und  
strafbar, soweit sich aus dem Urheberrechtsge-  
setz nichts anderes ergibt. Eine Einspeicherung  
und/oder Verarbeitung der auch in elektronischer  
Form vertriebenen Beiträge in Datensysteme ist  
ohne Zustimmung des Verlags nicht zulässig.

## Titelfoto:

Cisco Systems

## Anzeigen:

Anzeigenleitung: Dirk Limburg,  
Tel.: 0 89/3 60 86-871  
Leitung Anzeigendisposition: Rudolf Schuster,  
Tel.: 0 89/3 60 86-135, Fax: -99135  
Digitale Anzeigenannahme:  
Manfred Aumaier, Tel.: 0 89/3 60 86-602,  
Andreas Mallin, Tel.: 0 89/3 60 86-603

## Vertrieb / Produktion:

Vertrieb: Josef Kreitmair (leitend), Katrin Elsler  
Vertriebsmarketing: Peter Prieuwasser (leitend),  
Stefanie Kusseler

Vertrieb Handelsauflage: MZV Moderner Zeit-  
schriften Vertrieb, Breslauer Straße 5, 85386  
Eching, Tel.: 0 89/3 19 06-0, Fax: -113,  
E-Mail: [mzv@mzv.de](mailto:mzv@mzv.de), Website: [www.mzv.de](http://www.mzv.de)  
Produktionsleitung: Heinz Zimmermann

**Druck:** Schoder Druck, Gutenbergstraße 12,  
86368 Gersthofen

**Haftung:** Eine Haftung für die Richtigkeit der  
Beiträge können Redaktion und Verlag trotz  
sorgfältiger Prüfung nicht übernehmen. Veröf-  
fentlichungen in tecCHANNEL-Compact erfol-  
gen ohne Berücksichtigung eines eventuellen  
Patentschutzes. Warennamen werden ohne Ge-  
währleistung einer freien Verwendung benutzt.  
Veröffentlichung gemäß § 8, Absatz 3 des  
Gesetzes über die Presse vom 8.10.1949: Alleini-  
ger Gesellschafter der IDG Business Verlag  
GmbH ist die IDG Communications Verlag AG,  
München, eine 100-prozentige Tochter der IDG  
Inc., Boston, Mass., USA

**Verlag:** IDG Business Verlag GmbH, Lyonel-  
Feiningger-Straße 26, 80807 München,  
Tel.: 0 89/3 60 86-0, Fax: -118,

Website: [www.idg-verlag.de](http://www.idg-verlag.de)

**Handelsregisternummer:** HR 99187

**Umsatzidentifikationsnummer:** DE 181257800

**Geschäftsführer:** York von Heimbürg

**Group Publisher:** Stephan Scherzer

**Verlagsleitung:** Frank Klinkenberg

**Vorstand:** York von Heimbürg, Keith Arnot,  
Pat Kenealy

**Mitglieder der Konzerngeschäftsführung:**

Stephan Scherzer, Josef Lohner

**Aufsichtsratsvorsitzender:**

Patrick J. McGovern

Dieses tecCHANNEL-Compact wurde mit der Adobe Creative Suite CS produziert. tecCHANNEL-Compact erscheint im Verlag der PC-WELT. Zu unserer Verlagsgruppe gehören folgende Zeitschriften:

COMPUTERWOCHE

ComputerPartner

PC-WELT

DigitalWorld

Macwelt

GameStar

CIO

gamepro

## Leser- und Abo-Service:

Dialog-Service-Center GmbH, Konrad-Zuse-Straße 16, 74172 Neckarsulm, Telefon: 0 18 05/9 99-802,  
Fax: 0 71 32/9 59-166, E-Mail: [tecchannel@d-s-center.de](mailto:tecchannel@d-s-center.de)

# Inhalt

	<b>Editorial</b>	<b>3</b>
	<b>Impressum</b>	<b>4</b>
<b>1.</b>	<b>Grundlagen</b>	<b>10</b>
<b>1.1</b>	<b>Grundlagen zu Routing und Subnetzbildung</b>	<b>10</b>
1.1.1	Geroutete Protokolle und Routing-Protokolle	11
1.1.2	IP als geroutetes Protokoll	13
1.1.3	Paketübertragung und Switching im Router	14
1.1.4	Verbindungslose Netzwerkdienste	16
	Verbindungsorientierte Netzwerkdienste	17
1.1.5	Aufbau eines IP-Pakets	17
1.1.6	IP-Routing-Protokolle	19
1.1.7	Hauptfunktionen von Routern	19
1.1.8	Routing und Switching im Vergleich	21
	ARP- und Routing-Tabelle	23
1.1.9	Vergleich: Geroutete und Routing-Protokolle	24
1.1.10	Pfadermittlung	26
1.1.11	Adressierung in der Vermittlungsschicht	27
1.1.12	Routing-Tabellen	29
1.1.13	Routing-Algorithmen	30
	Metriken	31
1.1.14	Interne und externe Routing-Protokolle	31
1.1.15	Typen von Routing-Protokollen	32
	Distanzvektor-Protokolle	33
	Link-State-Protokolle	33
1.1.16	Grundlagen der Subnetzbildung	36
1.1.17	IP-Adressklassen	37
1.1.18	Subnetzbildung – Basics	37
1.1.19	Subnetzmaske erstellen	39
1.1.20	Subnetzmaske anwenden	41
1.1.21	Größe der Subnetzmaske bestimmen	42
	Subnetzmaske und IP-Adresse berechnen	43
1.1.22	Subnetze in Klasse-A- und Klasse-B-Netzwerken bilden	44
1.1.23	Netzadresse mit booleschem UND berechnen	45
1.1.24	Fazit	46
<b>1.2</b>	<b>Einführung in VLANs</b>	<b>48</b>
1.2.1	Logische Gruppen statt physikalischer Segmente	48
1.2.2	Broadcast-Domänen mit VLANs und Routern	50

1.2.3	Betrieb eines VLAN	51
	Portzentrisches statisches VLAN	53
	Ende-zu-Ende-VLANs	54
	Geografische VLANs	55
1.2.4	Vorteile von VLANs	55
1.2.5	VLANs und Sicherheit	56
1.2.6	Hubs und nicht VLAN-fähige Switches	58
1.2.7	VLAN-Typen	59
1.2.8	Kennzeichnung von VLAN-Frames	59
	IEEE 802.1Q (Frame-Tagging)	59
	ISL 60	
	FDDI 802.10	60
	LANE	61
1.2.9	VLAN-Konfiguration	62
	Statische VLANs konfigurieren	62
	Wichtige Regeln	62
1.2.10	Fehlersuche und -behebung bei VLANs	66
	Beispiel zur Fehlersuche	67
	Fehlersuche bei Endstationen	68
1.2.11	Zusammenfassung	69
<b>2.</b>	<b>Dienste und Services</b>	<b>70</b>
<b>2.1</b>	<b>Konfiguration und Betrieb eines Nameservers</b>	<b>70</b>
2.1.1	Das Konzept des Domain Name Service	71
2.1.2	Auswahl eines DNS-Servers	72
2.1.3	Allgemeines zur Konfiguration eines Nameservers	72
2.1.4	Primary Nameserver	73
2.1.5	Die Datei named.hosts	74
2.1.6	Das Masterfile-Format	75
	Start Of Authority (SOA)	76
	Nameserver (NS)	77
	Address (A)	77
	Well Known Services (SRV)	78
	Canonical Name (CNAME)	78
	Domain Name Pointer (PTR)	79
	Mail Exchange (MX)	79
	Text (TXT)	80
2.1.7	Die Datei named.local	81
	Die Datei named.rev	81
2.1.8	Slave-Nameserver	83
2.1.9	Weitere Optionen in der Datei named.boot	84
2.1.10	Steuerung des named-Prozesses	85
2.1.11	Betrieb eines Nameservers	86

---

---

2.1.12	Dynamische DNS-Updates	87
2.1.13	Sicherheit und DNS	87
	Weitere Informationen zum DNS	89
<b>2.2</b>	<b>LDAP</b>	<b>90</b>
2.2.1	LDAP-Grundlagen	90
	Abfrageoperationen	91
	Update-Operationen	91
	Authentifizierungs- und Kontrolloperationen	91
2.2.2	LDAP-Modell	94
	Funktionsmodell	95
	Informationsmodell	95
	Namensmodell	95
	Sicherheitsmodell	96
2.2.3	Schema	97
	Objekt-IDs (OIDs)	98
	Attributtypen	99
	Objektklassen	101
2.2.4	LDIF	104
	LDAP-URLs (RFC 1959):	106
2.2.5	LDAP und Sicherheit	107
	Zugriffssteuerung unter LDAP	107
	Authentifizierungsmechanismen	109
	Sicherheitsrisiken bei der Verwendung von LDAP	112
2.2.6	LDAP in der Anwendung	114
	Authentifizierung/Systemverwaltung	114
	Identity Management	115
	Adressbuch	115
2.2.7	LDAP-Tools	115
<b>2.3</b>	<b>Katastrophenszenarien bei Active Directory</b>	<b>117</b>
2.3.1	Neue Features von Windows Server 2003	117
2.3.2	Ausfall eines DNS-Servers	117
	Folgen eines DNS-Ausfalls für Windows-Clients	118
2.3.4	Ausfall eines Domänencontrollers	119
	Metadaten für einen verlorenen Domänencontroller löschen	121
2.3.5	Ausfall eines FSMO	124
	Übertragung eines FSMO-Rollenmasters	126
	Einen Rollenmaster entziehen	130
2.3.6	Verlust zentraler Replikationskomponenten	131
	Neuen bevorzugten Brückenkopfserver auswählen	132
	ISTG auswählen	133
	Ausfall einer WAN-Leitung	134
2.3.7	Sicherung von Active Directory	134

---

---

3.2.7	Mailinglisten	174
3.2.8	Absicherung des Bootloaders	174
3.2.9	Starten von Diskette	175
3.2.10	Mounten von Dateisystemen	175
3.2.11	Debian Sicherheitsupdates	176
3.2.12	Pluggable Authentication Modules (PAM)	177
	Password Required	177
	Anmeldung an Terminals	177
	PAM-Kommandos	178
3.2.13	Anpassungen der Datei /etc/inetd.conf	179
3.2.14	Die Datei /etc/login.defs	180
3.2.15	Die Datei /etc/ftpusers	181
3.2.16	Einsatz eines TCP-Wrappers	181
3.2.17	Benutzung von su und sudo	182
3.2.18	Benutzung von chroot	182
3.2.19	Kernel-Features	183
3.2.20	Benutzung der svgalib und sichere Übertragung von Dateien	184
3.2.21	Benutzung von Quota	184
3.2.22	Zugriffsrechte von Logdateien und setuid-Check	185
3.2.23	Kommandos chattr und lsattr	185
3.2.24	Integrität des Dateisystems	186
3.2.25	Die Programme locate und slocate	186
3.2.26	Secure Shell (SSH)	187
3.2.27	FTP-Server	188
3.2.28	X-Anwendungen im Netz	188
3.2.29	Display-Manager	189
3.2.30	E-Mail	189
3.2.31	Logghost – ein Server für Logdateien	190
3.2.32	BIND und Snort	191
3.2.33	Debian-Sicherheits-Updates	192
3.2.34	Austausch von Software	192
3.2.35	Kernel-Patches	192
3.2.36	Cruft	193
3.2.37	Weitere Möglichkeiten	194
3.2.38	Maßnahmen nach einem Einbruch ...	194
3.2.39	Erkennen von Rootkits	195
3.2.40	Rootkit-Tools	195
	Suckit Detection Tool	196
3.2.41	Fazit	196
	<b>Glossar</b>	<b>109</b>
	<b>Index</b>	<b>199</b>

---