

TEC CHANNEL *COMPACT*

IT EXPERTS INSIDE

**Optimieren,
schützen und
kontrollieren**

WLAN, LAN & DSL

Die besten Tools & Apps

Router & WLAN absichern

Netzwerk fit machen für Cloud und Mobile

ISBN 419-5-9149-1490-4



Editorial

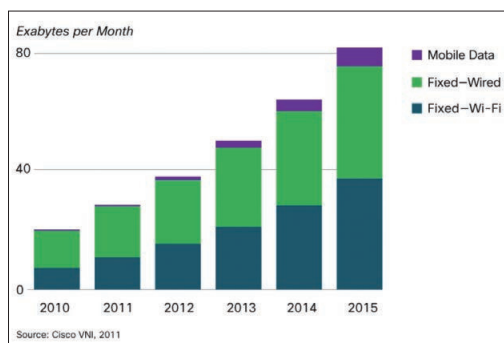
Gefangen im Netz!

Das Datennetzwerk ist allgegenwärtig und wächst unaufhörlich weiter. Dabei breitet es sich nicht nur flächenmäßig aus, sondern wird zwangsweise auch immer schneller. Forciert wird diese Entwicklung nicht zuletzt durch die steigende Anzahl mobiler Geräte und Technologien wie Cloud oder Virtualisierung. Denn ob zu Hause, unterwegs oder in der Firma, der Nutzer will oder muss überall erreichbar sein. Dieser Trend spiegelt sich auch in den aktuellen Netzwerkstatistiken wider. Laut dem Visual Networking Index 2011 von Cisco wird sich der IP-basierte Datenverkehr bis 2015 verdoppeln, und der mobile Internet Traffic soll sich noch dramatischer erhöhen.

Das schnelle Wachstum der Datenautobahnen birgt natürlich auch Gefahren. So muss der Nutzer teilweise unterschiedliche komplexe Netzwerktopologien wie LAN und WLAN gleichzeitig verwalten und dabei zusätzlich jederzeit die Sicherheit im Netzwerk gewährleisten. Das stellt sowohl den Heimanwender als auch die IT-Verantwortlichen in einem Unternehmen vor große Hürden. Neben der ständigen Überwachung des Datenverkehrs durch Monitoring-Programme ist es wichtig, geeignete Hard- und Software zu nutzen, die für den Schutz der Informationen innerhalb der verschiedenen Netzwerke sorgen. Angreifer sollten weder in ein WLAN eindringen noch ein LAN kompromittieren können. Das gilt insbesondere im Kontext mobiler Endgeräte wie Smartphones oder Tablets.

Mit diesem Compact haben wir ein Paket an Informationen geschnürt, das Ihnen eine Fülle von Beiträgen rund um das Themengebiet Netzwerk bietet. Das umfangreiche Angebot an Tools, Tipps, Ratgebern, Tests und Grundlagen soll Ihnen das theoretische und praxisnahe Rüstzeug an die Hand geben, das Sie brauchen, um die aktuellen und künftigen Herausforderungen im "Netz" zu meistern. Viel Spaß dabei!

Bernhard Haluschak
Redakteur TecChannel



Trend: Der IP-Netzwerkverkehr wird rasant weiter zunehmen.

Inhalt

	Editorial	3
	Inhalt	4
1	Netzwerk-Grundkurs	8
1.1	Ratgeber: Was ist was im Netzwerk?	8
1.1.1	Router	8
1.1.2	Switch	9
1.1.3	Hub 11	
1.1.4	Repeater	12
1.1.5	Netzwerk-Bridge	12
1.1.6	Netzwerkadapter	13
1.2	Ratgeber: Was ist was bei den Netzwerkprotokollen?	14
1.2.1	Appletalk und Ethertalk	14
1.2.2	DHCP	15
1.2.3	FTP, FTPS und SFTP	15
1.2.4	HTTP und HTTPS	16
1.2.5	IP, IPv4 und IPv6	17
1.2.6	IPX und SPX	19
1.2.7	NetBIOS und NetBEUI	19
1.2.8	SMB	19
1.2.9	SMTP	19
1.2.10	TCP/IP	20
1.2.11	UDP	20
1.3	Ratgeber: Qualifizierungsangebote für Netzwerkadministratoren	21
1.3.1	Dell	22
1.3.2	Cisco	22
1.3.3	IBM	23
1.3.4	Microsoft	24
1.3.5	Suse Linux	25
2	Netzwerk-Trends	26
2.1	Netzwerke – Trends und Herausforderungen 2012	26
2.1.1	IPv6, Cloud und Virtualisierung waren die Themen 2011	27
2.1.2	Cloud Computing und Virtualisierung werden 2012 komplexer	29
2.1.3	Einfaches Netzwerkmanagement und umfassende Sicherheitsstandards sind Pflicht	31
2.1.4	Schlüsseltechnologien wie PoE, FCoE oder IPv6 auf dem Prüfstand	33
2.1.5	Netzwerkrends, die das Jahr 2012 prägen werden	35
2.2	Ethernet-Architektur: Mit neuen Technologien fit fürs Datacenter	39
2.2.1	Mit intelligenten Switches Storage ins Netzwerk einbinden	40
2.2.2	Neue Netzwerktechnologien	40
2.2.3	Fazit	41
2.3	Netzwerkinfrastruktur: Cloud Computing ist kein Plug & Play	42
2.3.1	Kaum Problembewusstsein	42
2.3.2	Konzept für Netzwerkinfrastruktur machen	43

2.4	Die Folgen von iPhone, iPad & Co. fürs Firmennetz	45
2.4.1	Mobile Worker und Smartphones auf dem Vormarsch	45
2.4.2	Keine Konzepte für Bring your own Device	46
2.4.3	Cloud Computing spart Kosten	47
2.4.4	Wissenstransfer versus Data Loss Prevention	48
2.4.5	Compliance 2.0 für die Cloud	49
2.5	Netzwerk-Evolution: Bandbreite hat man nie genug	50
2.5.1	Aufrüsten oder bündeln?	50
2.5.2	Protokollfragen	50
2.6	Test: Breitband-Internet per Satellit in der Praxis	52
2.6.1	System und Anbieter	52
2.6.2	Planung	53
2.6.3	Lieferumfang	54
2.6.4	Außeneinheit (Outdoor-Unit – ODU) montieren	55
2.6.5	Inneneinheit installieren (Indoor-Unit – IDU)	56
2.6.6	Außeneinheit feineinstellen	56
2.6.7	Aktivieren	57
2.6.8	In die lokale Infrastruktur einbinden	57
2.6.9	Praxiserfahrungen und Bandbreiten	58
2.6.10	Von Latenzen und IP-Adressen	59
2.6.11	Fazit	60
3	Netzwerk-Monitoring	61
3.1	Mit OpenNMS Netzwerke professionell überwachen	61
3.1.1	OpenNMS versus Nagios	61
3.1.2	Server an OpenNMS anbinden	63
3.1.3	Überwachungsfunktionen in der Praxis	63
3.1.4	Integration der Systeme nicht ohne Hindernisse	64
3.1.5	Fazit	65
3.2	Test – Mit Paessler PRTG Network Monitor Netzwerke überwachen	66
3.2.1	Die Architektur von PRTG	66
3.2.2	Die Testumgebung	67
3.2.3	Setup und Inbetriebnahme	67
3.2.4	Die Verwaltungskonsole	68
3.2.5	Reichhaltiges Funktions-Set	69
3.2.6	Netzwerk analysieren	70
3.2.7	Überwachungssensoren einrichten	71
3.2.8	Einstellungen vererben	72
3.2.9	Komplexe IT-Strukturen überwachen	73
3.2.10	Fazit	74
3.3	iPhone, iPad, Android: nützliche Apps für Admins	75
3.3.1	Fing – der kostenlose Netzwerkscanner	75
3.3.2	iNet Netzwerkscanner – Netzwerk überwachen	76
3.3.3	Net Status – IP-Bereiche scannen	77
3.3.4	Nice Trace – Traceroute-Monitoring	78
3.3.5	Network Utility – Ping ganz einfach	78
3.3.6	System Status – WLAN-Informationen des iPhone	79
3.3.7	AppTicker Free – Überblick im App-Store	79
3.3.8	FileApp – Dokumente mit anderen teilen	80
3.3.9	Stundenzettel – Projektzeiten erfassen	80

3.3.10	Visitenkarten-Scanner	81
3.3.11	Dragon Dictation – Nachrichtenhilfe	81
3.3.12	Genius Scan – der Scanner für Smartphones	82
3.3.13	Faxen mit dem iPhone	82
4	LAN-Praxis	83
4.1	Ratgeber: Ausfallsicheres Netzwerk für Disaster Recovery	83
4.1.1	Das Netzwerk als Schwachstelle	83
4.1.2	Neue Wege für das Storage Backup	84
4.1.3	Im Fokus: Eigenschaften, die Sicherheit schaffen	84
4.1.4	Üben für den Ernstfall	85
4.2	Ratgeber: Standorte sicher per Remote Access vernetzen	86
4.2.1	Die alte RAS-Welt	86
4.2.2	Die Alternativen	86
4.2.3	Sicherheits-Policies durchsetzen	87
4.2.4	NAC tut not	87
4.2.5	Zukunftsmusik Ethernet-WAN	88
4.2.6	Welche Anbindung reicht aus?	88
4.3	Test: Die richtige VPN-Lösung für Ihr Netzwerk	90
4.3.1	Es ist die Soft- und nicht die Hardware ...	90
4.3.2	Checkliste für die Auswahl einer VPN-Lösung	90
4.3.3	Kostenloses VPN mit OpenVPN	92
4.3.4	Direct Access – Microsofts eigener Weg zum sicheren Zugriff	93
4.3.5	Anbindungen mit NCP	94
4.3.6	G/On – anders als die anderen	95
4.3.7	Kostenlose Fernwartung für schnelles Aufschalten	97
4.3.8	VPN-Grundlagen und -Techniken	98
4.3.9	Was bei VPN zu beachten ist	98
4.4	Mit Smartphone und Tablet sicher unterwegs arbeiten	100
4.4.1	PPTP, L2TP, IPsec und Co.	100
4.4.2	Pflegeleichte SSL-VPNs	101
4.4.3	Windows Phone ohne VPN	101
4.4.4	Sicher mobil arbeiten mit Microsoft	102
4.5	Praxis-Workshop: Windows-Firewall mit IPsec konfigurieren	103
4.5.1	Verbindungssicherheitsregeln konfigurieren	103
4.5.2	IPsec-Richtlinien über Gruppenrichtlinien erstellen	104
4.5.3	Regeln richtig konfigurieren	105
4.5.4	Netzwerkrichtlinienserver konfigurieren	107
4.5.5	Clients für die IPsec-Kommunikation konfigurieren	108
4.5.6	NAP über IPsec verwenden	109
4.5.7	Automatische Registrierung von Zertifikaten in Active Directory konfigurieren	110
4.5.8	Fehlersuche beim Einrichten von NAP über IPsec	110
4.6	Optische Netzwerke vor Hackern absichern	112
4.6.1	Optische Täuschung – typische Glasfaser-Hacks	112
4.6.2	Optimaler Schutz durch Verschlüsselung	113
4.6.3	Worauf es bei einer optischen Verschlüsselungslösung ankommt	114
4.6.4	Fazit	115
4.7	Die besten Netzwerk-Tools	117
4.7.1	Angry IP Scanner – Geräte im Netzwerk suchen	117

1 Netzwerk-Grundkurs

Netzwerke bilden die Grundlage unternehmerischer Kommunikationssysteme und ermöglichen den Zugang zu Daten unabhängig vom Standort der Mitarbeiter. Die Anforderungen an moderne LAN-Technologien steigen permanent und führen zu häufigen Änderungen und Anpassungen der Netzwerk-Infrastrukturen. Dieses Kapitel informiert über die wichtigsten Grundlagen und Fachbegriffe aus den Bereichen Netzwerktechnik sowie Protokollen. Außerdem geht es um Schulungen, Weiterbildung und Zertifizierungen für Netzwerkadministratoren.

1.1 Ratgeber: Was ist was im Netzwerk?

Ohne sie kommt kein Netzverkehr zustande: Router, Repeater, Switch und Hub machen den Datenaustausch erst möglich. Sie sind die Schaltstellen, an denen Datenpakete auflaufen. Allen gemein ist, dass sie die Daten weiterleiten. Dazu bedienen sich diese Geräte unterschiedlicher Methoden, je nachdem, auf welcher Schicht des standardisierten OSI-Referenzmodells sie arbeiten. Dass gerade Switches, Router und Hubs trotzdem häufig verwechselt werden, liegt einerseits an falsch verwendeten Begrifflichkeiten und andererseits an der sehr ähnlichen Arbeitsweise. Dieser Beitrag klärt auf über die Gerätegattungen und die unterschiedlichen Einsatzzwecke.

1.1.1 Router

Router leiten Datenpakete weiter (Routing) oder blocken sie ab. Datenpakete sind zwischen 64 und 1518 Byte lang; in den ersten sechs Byte steckt die Zieladresse, in den letzten vier Byte eine CRC-Prüfsumme. Geroutete Datenpakete kommen dann entweder direkt im Zielnetzwerk an oder bei einem anderen Router, der seinerseits die Datenpakete weiterleitet. Zum Weiterleiten der Pakete orientiert sich ein Router an einer Routing-Tabelle. Diese kann für IPv4 unter Windows ebenso wie unter Linux mit dem Befehl „netstat -r“ angezeigt werden. In IPv6-Netzwerken benutzt man unter Windows den Befehl „netsh interface ipv6 show route“, in Unix zum Beispiel „netstat -A inet6 -r“. Anhand der Routing-Tabelle bestimmt der Router, über welche Schnittstelle er die Datenpakete weiterleitet. Als Schnittstellen werden real existierende ebenso wie virtuelle in einem Router eingesetzt. Router arbeiten auf der Vermittlungsschicht (Schicht 3) des OSI-Referenzmodells, ebenso wie Layer-3-Switches. Das Weiterleiten der Datenpakete geschieht somit etwa per IP-Adressierung und nicht, wie etwa in der darunterliegenden Schicht 2, hardwareunterstützt (etwa anhand von MAC-Adressen) oder mit dem früher in Windows genutzten NetBEUI-Protokoll. Heute werden fast nur noch Router auf IP-Basis genutzt, weil die anderen Netzwerkprotokolle kaum noch eine Rolle spielen.