

TEC CHANNEL COMPACT

IT EXPERTS INSIDE

PRAXIS

RATGEBER

GRUNDLAGEN

Netzwerk

Neue Infrastruktur

- Flexibler mit Software Defined Networking
- Schneller mit Fabric-Technologie

Sicherheit erhöhen

- Linux-Distros für mehr Netzwerksicherheit
- Sicherheitslücken mit Nessus 5 aufspüren

Administration

- DNS & AD: Namensauflösung sicherstellen
- Netzwerke überwachen und inventarisieren
- NIC-Teaming: Netzwerk-Performance erhöhen

TOOLS,
TIPPS &
TESTS



TecChannel Silber-Paket

Print + iPad-Ausgabe + Premium-Zugang

nur
14,- €
monatlich
+ Prämie



- ▶ 40% Ersparnis gegenüber den Einzelpaketen
- ▶ TecChannel Compact kostenfrei auf Ihrem iPad
- ▶ 8 Ausgaben versandkostenfrei
- ▶ Alle Artikel im PDF-Format
- ▶ Exklusive Beiträge
- ▶ Eine hochwertige Prämie Ihrer Wahl



0711-72 52 276



www.tecchannel.de/silber



Inhalt

	Editorial	3
	Inhalt	4
1	Netzwerk-Trends	8
1.1	Netzwerke – Trends und Technologien 2013	8
1.1.1	Cloud Computing, ByoD und Social Media waren die Themen 2012	9
1.1.2	Herausforderungen 2013: Software-Defined Networking und Gigabit-WLAN	12
1.1.3	Cloud-Computing, Big Data, Sozial Media – und was dann?	16
1.1.4	IT-Netzwerk-Infrastrukturen richtig planen	19
1.1.5	Netzwerkrends der Zukunft	22
1.2	Software Defined Networks – Der Weg zu flexiblen IT-Netzwerken	25
1.2.1	SDN ist kein neues Konzept	26
1.2.2	Kernelement: der SDN-Controller	27
1.2.3	Die unterschiedlichen Ansätze von SDN	27
1.2.4	Das leistet SDN	27
1.2.5	Kritikpunkte von SDN	29
1.2.6	Verfügbarkeit von SDN-Controllern und Switches	29
1.2.7	SDN in der Praxis	30
1.2.8	SDN-Controller: Was zu verbessern ist	30
1.2.9	Die Open Networking Foundation	31
1.2.10	Fazit	32
1.3	OpenFlow – die Basis für Software Defined Networks	33
1.3.1	Strukturierte Verkabelung zementiert die Netze	33
1.3.2	Heutige Anforderungen verlangen nach Dynamik	34
1.3.3	Konzept des Software Defined Networks	34
1.3.4	Netzwerkconfiguration durch eine zentrale Instanz	36
1.3.5	OpenFlow – das Protokoll für Software Defined Networks	36
1.3.6	OpenFlow für vSphere	38
1.3.7	Erschwertes Monitoring	39
1.4	Software Defined Networking – Die aktuellen Strategien der führenden Hersteller	40
1.4.1	Alcatel-Lucent	40
1.4.2	Arista Networks	40
1.4.3	Big Switch Networks	41
1.4.4	Brocade	41
1.4.5	Cisco Systems	41
1.4.6	Citrix	41
1.4.7	Dell / Force10	42
1.4.8	Enterasys	42
1.4.9	Extreme Networks	42
1.4.10	Hewlett-Packard	42
1.4.11	IBM	42
1.4.12	Juniper Networks	43
1.4.13	NEC	43
1.4.14	VMware	43

1.5	Fabrics – Die Alternative zur konventionellen Netzwerkinfrastruktur	44
1.5.1	Virtual Machines erfordern neuartige Netzwerkinfrastruktur	45
1.5.2	IT-Services von der Netzwerkinfrastruktur trennen	45
1.5.3	Layer 2 Multipath: Shortest Path Bridging oder Trill	47
1.5.4	Jeder führende Netzwerkhersteller hat seine Fabric	48
1.5.5	Von flexiblen Netzen zu Virtual Application Networks	49
1.5.6	Weitere Ansätze: von Alcatel-Lucent bis Dell	50
1.5.7	Extreme und Dell/Force10: Clouds und Virtualisierung im Fokus	51
1.5.8	Hersteller zwischen Trill, SPB und eigenen Ansätzen	51
1.5.9	Virtualisierung als Schlüsselfaktor für Fabric-Architektur	52
1.5.10	Wann der Umstieg auf ein Fabric-Netzwerk sinnvoll ist	52
1.5.11	Administrationsaufwand: RSMILT und MSTP versus Shortest Path Bridging	53
1.5.12	Unbefriedigende Situation	54
1.6	Mit 100 Mbit/s ins Internet – Breitband-Hoffnung DSL-Vectoring	55
1.6.1	Doch was steckt hinter DSL-Vectoring?	55
1.6.2	DSL-Problematiken	56
1.6.3	DSL-Vectoring hat jedoch einen Haken	57
1.7	Auf dem Weg zur benutzerzentrischen IT	59
1.7.1	Unterstützung für benutzerzentrisches Computing	59
1.7.2	Neue Herausforderungen	60
1.7.3	Geänderte und zu ändernde IT-Landschaften	61
1.7.4	Fazit	61
2	Netzwerk-Praxis	62
2.1	NIC-Teaming: Netzwerkkarten unter Windows Server 2012 zusammenfassen	62
2.1.1	Ein NIC-Team erstellen	63
2.1.2	Das Team fertigstellen	64
2.1.3	NIC-Teams auf Core-Server	65
2.1.4	Teams testen und konfigurieren	66
2.1.5	Netzwerkkartenteams und Virtualisierung	67
2.2	Mehrere IP-Adressen auf einem Windows-System einsetzen	69
2.2.1	TCP/IP-Stack im Wandel: von schwachen und starken Host-Modellen	70
2.2.2	Wo und wie werden IP-Adressen auf dem System registriert?	71
2.2.3	Als Quelle überspringen: skipassource-Flag kann helfen	73
2.2.4	Hotfix bei Fehlverhalten	75
2.3	DNS und Active Directory: die Namensauflösung im Netzwerk sicherstellen	76
2.3.1	DNS in Active Directory integrieren und sichere Updates konfigurieren	76
2.3.2	Besonderheiten bei Windows Server 2012 beachten	77
2.3.3	Korrekte Namensauflösung in IPv4 und IPv6 testen	77
2.3.4	Erweiterte DNS-Einstellungen beachten	78
2.3.5	Weitere Optionen der DNS-Einstellungen	80
2.3.6	Servernamen schnell auflösen	80
2.3.7	Eine neue untergeordnete Domäne erstellen	81
2.3.8	DNS-Zonen delegieren	83
2.3.9	DNS-Server als Namensserver für die Delegierung verwenden	84

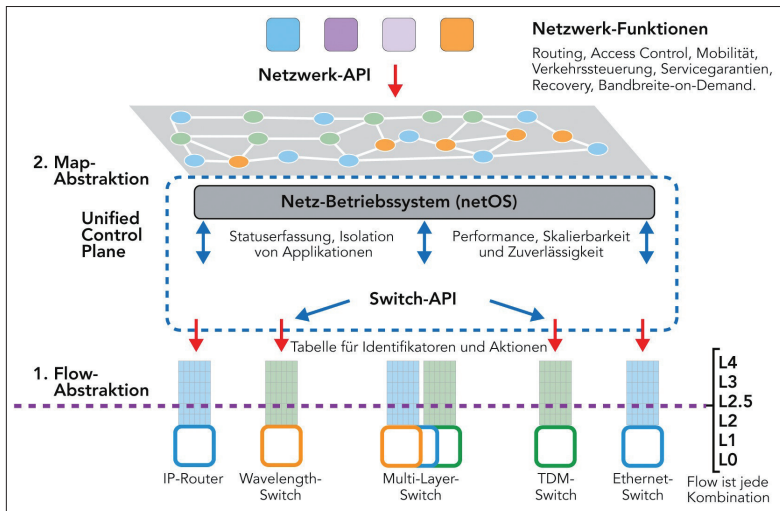
2.4	Netzwerkprotokolle SMB 3 und SMB 2 im Detail	86
2.4.1	Voraussetzungen für die Kommunikation via SMB	86
2.4.2	Vorteile von SMB 3 und SMB 2 gegenüber älteren Versionen	87
2.4.3	SMB 3/2 und andere Protokolle	87
2.4.4	Unterschiede zwischen SMB 3 und SMB 2	88
2.5	OCS Inventory NG – Netzwerke mit kostenlosem Tool inventarisieren	90
2.5.1	Welche Daten sammelt OCS Inventory NG?	91
2.5.2	Vorteile und Besonderheiten von OCS Inventory NG	92
2.5.3	Installation	93
2.5.4	Berechtigungen delegieren	93
2.5.5	Agenten im Netzwerk installieren	94
2.5.6	Netzwerkgeräte integrieren	94
2.5.7	Fazit	95
2.6	Schnelle Webseiten durch Monitoring mit AlertFox und iMacros	96
2.6.1	End-to-End-Überwachung	96
2.6.2	Der Funktionsumfang von AlertFox	97
2.6.3	iMacros automatisiert das Web-Monitoring	98
2	Netzwerk-Sicherheit	100
3.1	Empfehlenswerte Linux-Distributionen für die Netzwerksicherheit	100
3.1.1	Firewall und Router: Endian	100
3.1.2	Devil Linux: von Admins für Admins	102
3.1.3	Mit Vyatta Linux das Netzwerk schützen	103
3.1.4	Abbild unter 20 MByte: m0n0wall	104
3.1.5	Auf FreeBSD basierend: pfSense	105
3.1.6	Die Netzpolizei: IPCop	106
3.1.7	Übersichtlich: SmoothWall Express	108
3.1.8	Fazit	109
3.2	Test: Sicherheitslücken mit Nessus 5 aufspüren	110
3.2.1	Installation und Oberflächenwahl	111
3.2.2	Scan durchführen	112
3.2.3	Scan-Ergebnisse auswerten	113
3.2.4	Policies erstellen und Plugins auswählen	115
3.2.5	Fazit	116
3.3	Netzwerk in Gefahr – Wie Angreifer WLANs hacken	117
3.3.1	Die Funktechnik als Gefahrenquelle	118
3.3.2	Die Schwachstellen der WLAN-Technik	119
3.3.3	WEP, WPA, WPA2 – und was jetzt?	119
3.3.4	WPS – die trügerische Sicherheit	120
3.3.5	Die Vorgehensweise der Angreifer	120
3.3.6	Angriffe auf den WPA-Schlüssel	121
3.3.7	Empfehlungen für ein sicheres WLAN	122
3.3.8	Fazit	123
3.4	Test – Wi-Spy DBx und Chanalyzer	124
3.4.1	Preise, Software und Installation	124
3.4.2	Chanalyzer Pro und Wi-Spy DBx in der Praxis	125
3.4.3	Kombination mit WLAN-Modul	126
3.4.4	Störer aufspüren	126
3.4.5	Fazit	127

4	Netzwerk – Tipps und Tools	128
4.1	Windows Server: Befehle, die ein Admin kennen sollte	128
4.1.1	Domänencontroller überprüfen mit dcdiag.exe und Co.	128
4.1.2	Nltest und net.exe	129
4.1.3	Dateiserver und Freigaben	130
4.1.4	Windows Server 2012 aktivieren	132
4.1.5	Active Directory und PowerShell	133
4.1.6	Hyper-V und PowerShell	134
4.2	Tipps fürs Netzwerk-Outsourcing	136
4.2.1	Fünf Kriterien für die Analyse	136
4.2.2	Auf User-Entwicklung kommt es an	137
4.3	Sysinternals – Gratis-Tools fürs Netzwerk	138
4.3.1	AdExplorer (Active Directory-Explorer) – im AD navigieren	138
4.3.2	AdInsight (Insight for Active Directory) – Verbindungsanalyse	139
4.3.3	Geöffnete Ports überwachen mit TCPView	140
4.3.4	PSFile – über das Netzwerk geöffnete Dateien anzeigen	141
4.3.5	Über das Netzwerk mit Shutdown.exe und PsShutdown.exe herunterfahren	142
4.3.6	PsShutdown.exe mit mehr Optionen	143
4.3.7	ShareEnum – Freigaben im Netzwerk anzeigen	144
4.3.8	Whois	145
4.4	Praktische Netzwerk-Tools fürs WLAN	146
4.4.1	Windows-7-Rechner mit Bordmitteln als Access-Point nutzen	146
4.4.2	Virtual WiFi Router als Freeware-Alternative	147
4.4.3	Schneller Wechsel garantiert: NetSetMan	148
4.4.4	Der genaue Blick ins WLAN: WirelessNetView	149
4.4.5	Benchmark für das WLAN: NetStress	150
4.4.6	Sicherheit mit Kompromissen: Hotspot Shield	151
4.5	Test: Wireless-Controller D-Link DWC-1000	153
4.5.1	Gerätedetails und Schnittstellen	153
4.5.2	Die Konfiguration des Routers	154
4.5.3	Erste Kontaktaufnahme zum DWC-System	155
4.5.4	Übersichtliches Web-Interface	155
4.5.5	Sicherheitsfunktionen des Systems	156
4.5.6	Konfiguration und Test der Access Points	156
4.5.7	Fazit	158
4.6	Intrex Share – Informationen im Unternehmen einfach vernetzen	159
4.6.1	Feeds auf Smartphones und Tablets anzeigen	160
5	Anhang: Die beliebtesten Netzwerk-Artikel (QR-Codes)	161
	Impressum	162
	Mobile Webseite	162
	iPad Kiosk-App	162
	TecChannel-Newsletter	162

1.2 Software Defined Networks – Der Weg zu flexiblen IT-Netzwerken

IT-Verantwortliche kommen nicht zur Ruhe. Unter anderem deshalb, weil sie sich derzeit mit einer ganzen Reihe von Hype-Begriffen auseinandersetzen müssen: von Cloud Computing über den Einsatz privater, mobiler Endgeräte im Unternehmen (Bring your own Device) bis hin zu Data Center Fabrics. Und 2013 erwartet sie ein weiteres heißes Thema: Software Defined Networking (SDN). Entsprechend euphorisch geben sich einige Marktforschungsinstitute. IDC geht beispielsweise davon aus, dass der weltweite Umsatz mit SDN-Produkten 2013 bei 200 Millionen Dollar liegen wird. Bis 2016 soll er auf mehr als zwei Milliarden Dollar steigen.

Skeptischer zeigt sich dagegen Andre Kindness, Principal Analyst bei Forrester Research (www.forrester.com): „SDN-Lösungen und entsprechende Produkte benötigen noch etwa fünf Jahre, bis sie für den Einsatz in Enterprise Networks reif sind.“ Er moniert unter anderem, dass es bei SDN aufwendig sei, Netzwerkkomponenten miteinander zu koppeln, vorhandene Managementsysteme zu integrieren, die Verwaltung von Hypervisors einzubinden und das Ganze auf Netzwerk-Services abzustimmen, die auf den Ebenen 4 bis 7 des ISO/OSI-Modells angesiedelt sind.



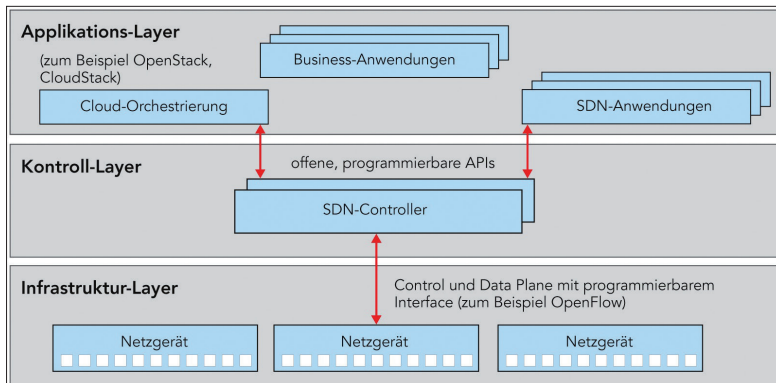
SDN-Strukturen: Über APIs lassen sich viele Netzfunktionen für Systeme und Anwendungen steuern, von der Zugangssteuerung bis hin zu Bandbreitengarantien. (Quelle: Universität Stanford)

Auch Stuart Bailey, Gründer und Chief Technology Officer von Infoblox, einem Anbieter von Produkten für die Automatisierung von Netzwerken, hält die über-

schäumende Begeisterung für SDN für wenig hilfreich: „Der Hype ist problematisch und sorgt für Verwirrung. SDN sollte vielmehr als Hilfsmittel gesehen werden, mit dem sich konkrete Herausforderungen im Netzbereich bewältigen lassen, etwa im Bereich Big Data“, so Bailey in einem Gespräch mit dem Online-Community-Portal „SDN Central“.

1.2.1 SDN ist kein neues Konzept

Software Defined Networking beziehungsweise Software Defined Networks sind kein brandneues Konzept. Es findet beispielsweise in Wireless LANs Verwendung, in denen ein WLAN-Controller vorhanden ist. Ebenso sind in MPLS-Netzen (Multi-Protocol Label Switching) SDN-Methoden zu finden. Das bestätigt Markus Nispel, Chief Technology Strategist bei Enterasys (www.enterasys.com): „Bereits in den 90er-Jahren gab es mehrere Unternehmen, die softwarebasierte Netzarchitekturen auf ihre Tragfähigkeit hin untersuchten, darunter auch Enterasys. Wir ließen das Projekt fallen, weil der damalige Ansatz nicht die erforderliche Skalierbarkeit bot.“ Im Vergleich zu herkömmlichen Netzwerk- und Switching-Architekturen weisen Software Defined Networks einige Besonderheiten auf. Die gravierendste ist die Trennung der Control Plane von der Data Plane beziehungsweise Forwarding Plane auf Layer 2 und 3 von Switches und Routern, also die Separierung von Kontroll- und Datenpfad. Die Control Plane ist für die Konfiguration eines Switches beziehungsweise Routers zuständig, außerdem für das Programmieren der Pfade, über die Daten transportiert werden. Bei SDN wird die Control Plane gewissermaßen aus Switches und Routern extrahiert und in ein separates System verlagert – den SDN-Controller.



SDN-Elemente: Über Cloud-„Betriebssysteme“ wie OpenStack und CloudStack kann ein SDN-Controller auch in eine Cloud-Computing-Umgebung eingebunden werden. (Quelle: Hewlett-Packard)

1.2.2 Kernelement: der SDN-Controller

Ein SDN-Controller ist nicht an eine bestimmte Form gebunden. Es kann sich um einen physischen Server handeln, aber auch um eine Virtual Machine oder eine Hardware-Appliance. Der Controller gibt der Forwarding Plane vor, wie sie mit Datenpaketen umgehen soll, also wohin (an welchen Port) die Pakete übermittelt werden sollen und mit welcher Priorität das erfolgen muss.

Die Forwarding Plane übermittelt diese Regeln wiederum an die applikationsspezifischen ICs (ASICs) im Router oder Switch. Vereinfacht gesagt: SDN separiert Entscheidungen, die die Weitervermittlung von Paketen und Regeln (Policies) betreffen, von der Netzwerktopologie und der Transportebene.

1.2.3 Die unterschiedlichen Ansätze von SDN

Die Kommunikation zwischen Controller und Infrastrukturebene (Data/Forwarding Plane) erfolgt über ein spezielles Protokoll. Hier kommt derzeit vor allem OpenFlow zum Einsatz, das an der Stanford University in Kalifornien entwickelt wurde. Für die Anbindung der Anwendungen sind standardisierte Application Programming Interfaces (APIs) zuständig. Derzeit favorisieren etliche Netzhersteller OpenFlow, darunter Hewlett-Packard, NEC und IBM. Allerdings gibt es auch andere Ansätze, beispielsweise Path Computation Elements (PCE), ein speziell für SDN in Weitverkehrsnetzen entwickeltes Konzept.

Die Switches und Router in einer SDN-Infrastruktur müssen das Protokoll „verstehen“, das der SDN-Controller verwendet, also etwa OpenFlow (www.openflow.org). Das bedeutet im Extremfall den Austausch von älteren Systemen gegen neue, die über entsprechende Schnittstellen verfügen. Die meisten Anbieter von Netz-ausrüstung für Enterprise Networks und Telekommunikationsnetze statten derzeit ihre Systeme mit entsprechenden Interfaces aus.

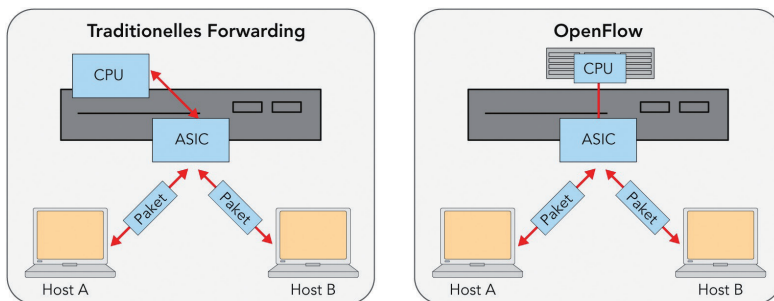
1.2.4 Das leistet SDN

Die Verfechter des Konzepts führen unter anderem folgende Vorteile von SDN an:

- Beim Controller handelt es sich um kein herstellerspezifisches, geschlossenes System. Netzadministratoren können darauf zugreifen und den Controller programmieren.
- Unterschiedliche Netzsysteme lassen sich von einer zentralen Stelle aus steuern, von physischen Switches und Routern bis hin zu virtualisierten Switches (vSwitches), WLAN-Access-Points und WAN-Optimierungssystemen.
- Anwendungen und neue Netzdienste können innerhalb von Stunden bereitgestellt werden. Derzeit erfordert dies oft mehrere Tage oder gar Monate. Bei SDN lassen sich über Einträge in Flow Tables auch Dienste und

Eigenschaften konfigurieren, bei denen das in herkömmlichen Netzen nicht mittels Scripts möglich ist, etwa Quality-of-Service-Merkmale und VLAN-Einstellungen.

- Servicedefinitionen müssen nicht mehr auf physikalische Netz-Ports „gemappt“ werden. Das verringert den Konfigurationsaufwand.
- Der Controller vermittelt dem Administrator eine „ganzheitliche“ Sicht auf die Anwendungen, Netzelemente und Datenströme (Flows).
- Laut Oracle verringert SDN die Komplexität einer Netzwerkinfrastruktur um bis zu 70 Prozent, weil weniger Switch-Ports und Kabel erforderlich sind. Bei LANs und Storage Area Networks seien es etwa 50 Prozent.



Getrennte Ebenen: Die Control- und die Forwarding-Ebene, die in einem Standard-Switch vereint sind, werden getrennt. Die Steuerung übernimmt ein externer Controller. (Quelle: Dell)

Die University of Stanford Kalifornien (www.stanford.edu) führt an, dass Software Defined Networks vor allem die Handhabung von Virtual Machines (VM) erleichtern. Demnach lassen sich in einer SDN-Infrastruktur VMs auf einfachere Weise im Netz verschieben. Der Grund ist, dass sich mit einem SDN-Controller sowohl physische als auch virtualisierte Data Planes steuern lassen.

Die genannten Faktoren schlagen sich nach Berechnungen der Beratungsgesellschaft International Strategy and Investment Group (ISI) in geringeren Kosten nieder. Durch die effizientere Auslastung der Systeme in einem typischen Server-Rack sollen sich mithilfe von SDN etwa 20 Prozent der Server-, Speicher- und Netzsysteme sowie der zugehörigen Verkabelung und Netzbandbreite einsparen lassen. In einem Rechenzentrum mit zehn Racks, die jeweils mit Ausrüstung im Wert von einer Million Dollar bestückt seien, könnten dadurch zwei Racks entfallen. Das entspricht einem Gegenwert von zwei Millionen Dollar. Zudem, so ISI, reduziert SDN die Betriebskosten. Der Grund: Im Vergleich zu einer herkömmlichen Netzinfrastruktur lassen sich mit SDN mehr Netzwerkmanagementprozesse automatisieren. Das entlastet die IT-Abteilung, vor allem bei der Migration zu einer Private-Cloud-Umgebung oder einer Hybrid Cloud, in der sowohl hausinterne IT-Systeme und -Services als auch Public-Cloud-Angebote genutzt werden.

1.2.5 Kritikpunkte von SDN

Allerdings gibt es eine Reihe von Punkten, die Fachleute am Software Defined Networking kritisieren. So steigt mit dem Konzept eines zentralen Controllers die Fehleranfälligkeit: Fällt der Controller aus, „steht“ das Netz. Dies lässt sich beheben, indem mehrere Controller zum Einsatz kommen. Das erhöht jedoch die Komplexität der Infrastruktur und damit auch den Managementaufwand.

Bedenken gibt es zudem in Bezug auf die Skalierbarkeit einer SDN-Infrastruktur. Speziell in komplexen Netzen mit vielen Switches, Servern und Virtual Machines müssen Controller mehrere hunderttausend oder Millionen Flows bewältigen. In den derzeitigen Testinstallationen der University of Stanford fallen jedoch nur mehrere hundert bis tausend Flows an.

„Neben der Standardisierung ist die Skalierbarkeit einer solchen Lösung eine Herausforderung“, bestätigt Enterasys-Technikstratege Nispel. „Eine totale Zentralisierung der Control Plane bringt zwar theoretisch Vorteile für das Management, jedoch sind Verfügbarkeit und insbesondere Skalierung ein Problem.“ Die Definition der IP-Flows in den gegenwärtig vorhandenen OpenFlow-Testumgebungen erfolge in einer groben Weise und sei statisch vordefiniert: „Das heißt, man muss sich vorher genau überlegen, wer mit wem kommunizieren möchte.“

Laut Adva Optical Networking, einem Hersteller von optischen Netzkomponenten für Weitverkehrsnetze, eignet sich SDN auf Basis von OpenFlow zudem nur unzureichend für optische Netze, in denen eine leitungsvermittelnde Übertragung stattfindet. Hier seien Erweiterungen der OpenFlow-Spezifikation erforderlich. Allerdings hat die Internet Engineering Task Force (IETF) mit Path Computation Elements eine SDN-Spezifikation zur Verfügung gestellt, die für das Software Defined Networking in Weitverkehrsnetzen auf IP-Basis zugeschnitten ist.

Weiterhin ist zu berücksichtigen, dass der Verkehr im Netzwerk durch die Kommunikation zwischen den Controllern nach ersten Erfahrungswerten um etwa drei bis vier Prozent steigt. Dies dürfte in vielen Fällen nicht problematisch sein, führt aber dennoch zu einer stärkeren Belastung des Netzes. Noch unklar ist ferner, wie sich SDN in komplexen Netzen umsetzen lässt. Dies betrifft vor allem das Management von IT-Ressourcen über mehrere Domains hinweg. Ebenfalls noch nicht zufriedenstellend gelöst ist die Frage, wie sich Verkehrsströme und Daten in Netzen trennen lassen, die auf eine „Shared Infrastructure“ zurückgreifen. Das ist beispielsweise in MPLS-Weitverkehrsnetzen (Multi Protocol Label Switching) der Fall.

1.2.6 Verfügbarkeit von SDN-Controllern und Switches

Kein Mangel herrscht an Controllern für Software Defined Networks. Derzeit sind unterschiedliche Produkte diverser Anbieter auf dem Markt. Die Palette reicht von Open-Source-Produkten wie Beacon und Floodlight bis zu kommerziellen Controllern wie ProgrammableFlow und Onix. Die meisten stammen von kleineren Unternehmen wie etwa Big Switch. Auch etablierte Netzspezialisten, beispielsweise