März 2013 Deutschland € 15,90 Österreich € 17,90 Schweiz SFR 29,80
www.TecChannel.de

TECCHANNEL COMPACT

IT Experts Inside

PRAXIS
RATGEBER
GRUNDLAGEN

Netzwerk

Neue Infrastruktur

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

Sicherheit erhöhen

- Linux-Distris 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

IDG BUSINESS MEDIA GMBH

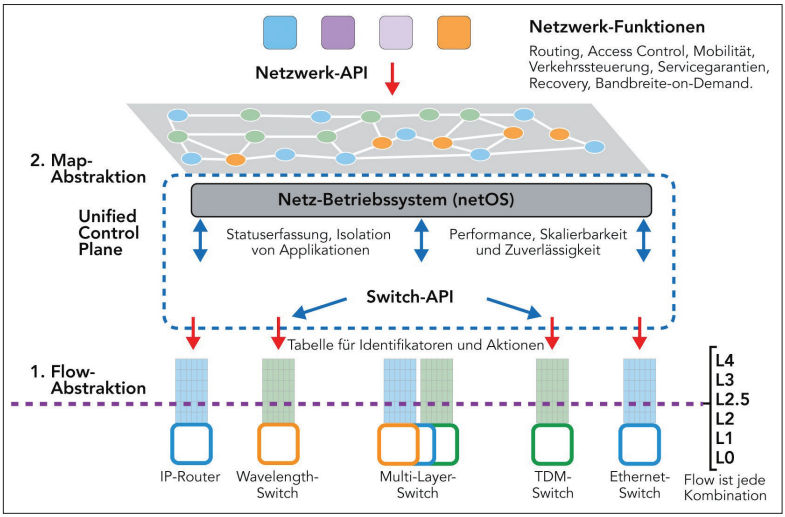
TecChannel erscheint im Verlag IDG Business Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den TecChannel Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John, Tel. 0711/72 52 276, Fax 0711/72 52 377, E-Mail: shop@tecchannel.de

Inhalt

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.



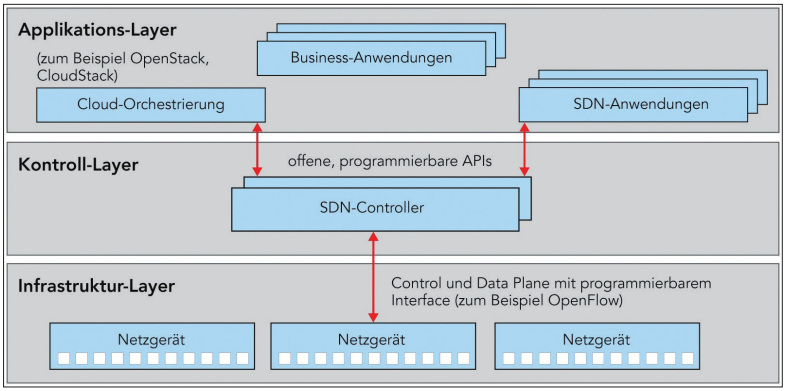
SDN-Strukturen: Über APIs lassen sich viele Netzfunktionen für Systeme und Anwendungen steuern, von der Zugangskontrolle bis hin zu Bandbreitengarantien. (Quelle: Universität Stanford)

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) SND-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 Switchs 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 Netzausrüstung für Enterprise Networks und Telekommunikationsnetze statten derzeit ihre Systeme mit entsprechenden Interfaces aus.

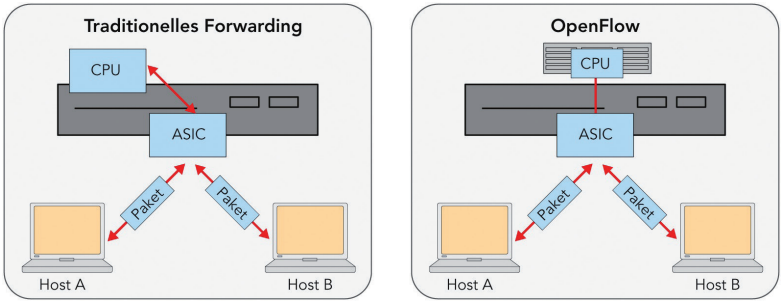
1.2.4 Das leistet SDN

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 entlaste 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