

Ein typisches LAN besteht aus einer Reihe autonomer Komponenten wie Firewalls, Routern und Switches, die nach dem bekannten EVA-Prinzip (Eingabe, Verarbeitung, Ausgabe) arbeiten. Ein Datenpaket kommt rein, die Netzwerkkomponente verarbeitet es nach den konfigurierten Richtlinien und sendet es weiter. Damit die Daten von A nach B kommen, muss jedes der beteiligten Geräte die Netztopologie kennen – zumindest die direkt benachbarten Teile. Die Position einer bestimmten Komponente im Netz definiert deren Funktion.

Ein Stellungswechsel kann fatale Folgen haben. Doch damit nicht genug. Im Laufe der Zeit ratifizierte die Internet Engineering Task Force mehrere Tausend Standards in Form von Protokollen, die nicht selten Insellösungen darstellten. Kommen herstellerspezifische Implementierungen dazu, ist der Grundstein für das Chaos gelegt. Gewachsene große Netze sind unflexibel und Änderungen hochgradig komplex. Neue Herausforderungen durch Big Data oder Cloud oder die explodierende Zahl der Netzteilnehmer durch Tablet-PCs oder Smartphones können den Administrator nur noch verzweifeln lassen.

Silberstreif am Horizont

Obwohl erst seit Kurzem im Gespräch, ist die Idee von Software-Defined Networking (SDN) schon gute acht Jahre alt. Wie so oft liegen auch ihre Ursprünge im akademischen Umfeld – genauer in der Doktorarbeit von Martin Casando. Dort findet man die Idee der logischen Trennung des Datenflusses von der Steuerlogik. Heute benutzt man die Begriffe Data Plane und Control Plane. SDN bezeichnet also die Trennung von Infrastruktur und Konfiguration. Zur Ersteren gehören die Router, Switches und Firewalls. Die Con-

trol Plane kann sich außerhalb dieser Geräte befinden.

Die Aufgabentrennung hat unmittelbare Konsequenzen. Die Data Plane übernimmt quasi nur das Weiterleiten von Paketen. Ohne die notwendige Denkarbeit braucht sie weniger Rechenkraft, die zuständige Firmware kann deutlich schlichter ausfallen. Entsprechend umfangreich ausgestattet und clever muss die Control Plane sein. Hier laufen die Analysen und fallen die Entscheidungen. Von Letzteren müssen die Netzwerkkomponenten erfahren, damit sie die Datenpakete richtig weiterleiten.

Mit OpenFlow existiert eine erste standardisierte Kommunikationsschnittstelle zwischen Data Plane und Control Plane. Die Non-Profit-Organisation Open Network Foundation (ONF), die sich mit der Verbreitung und Implementierung von SDN beschäftigt, verwaltet den Standard. Das Herausziehen der Intelligenz aus den Netzwerkgeräten mindert vor allem die Abhängigkeit von Hardwareherstellern. Dabei erweist sich die Standardisierung der Schnittstellen als ausgesprochen hilfreich.

Zudem lassen sich die Lebenszyklen des Netzes einfacher von der darunterliegenden Hardware entkoppeln. Über die Control Plane hat der Administrator einen viel besseren Überblick über das Netz und kann dadurch die Datenflüsse wesentlich effizienter lenken. Da sich die Routing- und Topologie-Informationen nicht bruchstückhaft auf alle Router verteilen, sondern an einem zentralen Ort auf der separierten Steuerlogik zusammenlaufen, eröffnen sich damit neue Wege der Automatisierung, insbesondere herstellerübergreifend. Beispielsweise kann die Control Plane die Auslastung der verschiedenen Pfade vergleichen und über die Herausgabe neuer Routing-Regeln ausbalancieren. Dadurch ließe sich ein Netz auch für eine bestimmte Anwendung so weit maß-

Kurz erklärt: Software-Defined Networking

Losgelassen

Udo Seidel

Virtualisierung, Cloud-Computing und BYOD haben die Komplexität der LANs in den letzten Jahren exponentiell erhöht und das Tagesgeschäft eines Netzadministrators spürbar verändert. Software-Defined Networking soll durch die Abstraktion von der Hardware die Verwaltung wieder vereinfachen.



schneiden, dass sie sogar seine Fähigkeiten kennt.

Modelle und Varianten

Im symmetrischen SDN-Modell ist die Control Plane so weit wie möglich zentralisiert. Netzwerkübergreifend und Automatisierung sind am einfachsten, die Gefährdung durch Ausfälle aber auch am höchsten. Zusätzliche Mechanismen zum Absichern der Control Plane nehmen bei der Umsetzung dieses Modells besonders viel Raum ein. Im asymmetrischen Ansatz kennen die einzelnen Systeme die unmittelbar notwendigen Konfigurationen und funktionieren beim Ausfall der zentralen Kontrolllogik weiter. Der offensichtliche Nachteil besteht in unnötigen Redundanzen der Informationen.

Eine andere Kategorisierung von SDN basiert auf dem Sitz der Control Plane. In einer hochgradig virtualisierten Umgebung ist der Virtualisierungshost die offensichtliche Wahl. Als Alternative gilt das Betreiben sogenannter dedizierter SDN-Controller. Eine dritte Methode, die SDN-Modelle

zu unterscheiden, legt den Fokus auf die Verteilung der Informationen. Die Control Plane kann die notwendigen Informationen per Multi- oder Broadcast verteilen. Gegner dieses Ansatzes befürworten dagegen eher verteiltes Hashing oder verteilte Nachschlagetabellen. Eine Verwandtschaft zur zentralen Control Plane ist leicht erkennbar.

Auf dem Papier klingt SDN wie der heilige Gral. In der Realität gibt es aber Misstöne, weil die Hersteller unterschiedliche OpenFlow-Versionen implementieren. Control Planes gibt es als Open Source genauso wie als kommerzielles Produkt. Bei der Data Plane hat man eine deutlich geringere Auswahl. Dennoch, die Trennung von Konfiguration und Infrastruktur ist der Weg in die Netz-Zukunft. (sun)

Dr. Udo Seidel

studierte Mathe und Physik und leitet das Linux-Strategie-Team sowie die „Server Automation“-Gruppe bei der Amadeus Data Processing GmbH in Erding.

