4 Software-defined Networking

Was ist Software-defined Networking?

Der Ansatz des Software-defined Networking (SDN) ist mehr als eine Technik, um QoS in das vorhandene Internet einzubringen, es ist eine völlig neue Definition, wie das Internet arbeitet. SDN bildet für viele neue Netzarchitekturen die Basis. Dabei umfasst SDN sehr viele Aspekte; es ist nicht nur eine neue Technik, um schnelle, hochperformante Netze zu bauen. Das Hauptziel des SDN ist die Reduzierung der Komplexität und der Kosten der Netze durch die konsequente Unterstützung der Virtualisierung von Netzfunktionen und eine Programmierbarkeit der Netzelemente durch übergeordnete Steuerfunktionen. Die Funktionen, wie Server für Signalisierung, Data Center, private Netze, Speicher oder Rechenleistung, lösen sich von der Hardware. SDN ist eine flexible Dienste-Plattform, um Leistungen von verteilten Data Center den Kunden anzubieten oder netzweite neue Funktionen vorzustellen. Daneben können SDN-Systeme einfach als flexible Netzelemente in vorhandenen Netzen eingesetzt werden. Neu sind die Rückmeldungen (Monitoring) der Netzelemente an die übergeordnete Steuerung (Controller). Über diesen Mechanismus wird die augenblickliche Netzbelastung, lokale Ausfälle oder die Nutzungsintensität von Kommunikationswegen erfasst. Der Controller kann so sehr schnell auf veränderte Situationen oder Engpässe reagieren und damit die Verfügbarkeit und die Qualität der Netze deutlich steigern.

SDN-Einsatzgebiete

Die folgenden Beispiele für die Anwendung der SDN-Technik zeigen exemplarisch die vielfältigen Einsatzgebiete:

- SDN ist eine Ergänzung vorhandener Infrastrukturen. Privatnetze können mit konventionellen Festverbindungen und speziellen SDN-Netzelementen mehrere Standorte des eigenen Unternehmens verbinden und erweiterte Funktionen und Eingriffsmöglichkeiten in ihre standortübergreifenden Netzgestaltung erreichen.

- SDN ist eine neue Netzarchitektur (SDN-Netz) und Technik, um große, komplexe und leistungsfähige Netze mit flexibler Steuerung zu bauen. Die Netzfunktionalitäten können dabei von einfachen Transportnetzen mit Festverbindungen über die Bildung kompletter Fest- oder Mobil-Netze bis hin zu einer flexiblen Transportplattform mit Rechner- und Speicherkapazitäten und ganzen Backbone-Netzen, die bedarfsgerecht Kunden zugeordnet werden können, reichen. Zusammengefasst werden diese Angebote unter den Begriffen Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (Iaas).

- SDN ist eine mögliche Plattform, um eine bessere Übertragungsqualität zu garantieren, Engpässe zu vermeiden, kurze Paketlaufzeiten und praktisch keinerlei Paketverlust in der Übertragung sowie eine sehr große Verfügbarkeit zu realisieren. Durch eine übergeordnete Steuerung und Netzelemente, die ihre augenblickliche Auslastung an diese Steuerung melden, können innerhalb der Netze Engpässe

vermieden werden und zusammen mit der Technik des Traffic Shaping Qualitäten für alle Verbindungen garantiert werden. Bei Ausfall von Verbindungsleitungen und/oder Netzelementen kann SDN automatisch Ersatzwege bereitstellen.

- SDN kann eine End-to-End-Qualität bereitstellen. Durch die Meldungen zur Auslastung von den einzelnen Netzelementen verfügt der Controller über eine komplette Netzsicht. Für die Wahl des optimalen Wegs durch das Netz kann nicht nur die direkte Umgebung eines Routers beachtet werden, sondern der Controller kann netzweit Engpässe verhindern und die optimalen Wege zum gewünschten Ziel ermitteln.

- SDN ist eine sehr flexible Plattform zur Bereitstellung von Diensten. Die Dienste oder Netzfunktionen können lastabhängig auf virtuelle Maschinen verteilt im Netz realisiert werden. Die Dienste können damit flexibel auf Netzanforderungen reagieren und sind in weiten Bereichen skalierbar, dies ermöglicht das Anbieten von ganzen Service-Plattformen (Data Center) oder ganzen Infrastrukturen (IaaS) einschließlich Rechnerleistung und Speicherbereichen. Für die Kunden dieser Plattformen bietet das SDN schnelle Reaktionen auf Kundenanforderungen, eine sehr hohe Verfügbarkeit und Performance. Die Dienste müssen nicht einem bestimmten Server mit einer festen, immer gleichen IP-Adresse zugeordnet werden, sie können (auch lastabhängig) auf mehreren Servern parallel angeboten werden. Load-Balancing-Funktionen verhindern Hotspots und Engpässe.

- SDN kann für bestimmte, einfachere Funktionen auch als eine zentrale Firewall im Netz eingesetzt werden. Spam-Mails können damit bereits im Netz erkannt und frühzeitig entfernt werden. Störer können gezielt geblockt werden, d. h., Informationen von oder zu einem bestimmten Zugang können gelöscht werden. Der Zugriff auf bestimmte Netzbereiche kann zentral kontrolliert und geregelt werden.

- SDN ist die Fortführung der Virtualisierung über Standorte hinweg im gesamten Netz. Dies ist besonders leistungsfähig, wenn eine Zusammenarbeit zwischen dem Koordinator für die virtuellen Maschinen (der Orchestrator) und dem SDN-Controller ermöglicht wird. Dadurch können virtuelle Maschinen beliebig im Netz angeordnet werden. Ein SDN-Switch kann einer logischen Adresse für einen bestimmten Service unterschiedliche Netzadressen zuordnen, um beispielsweise so ein Loadsharing eines bestimmten Services zu erreichen.

- SDN bietet einen optimierten Transport mit hoher Verfügbarkeit und Qualität sowie eine flexible Bereitstellung von Diensten, Ressourcen und virtuellen Infrastrukturen für die Kunden *ohne* ein neues, zusätzliches Protokoll oder eine weitere Netzebene einzuführen. SDN verwendet nur die bereits vorhandenen Parameter und arbeitet *gleichzeitig* in den Schichten 1 bis 4.

4.1 Der prinzipielle Ansatz

Das Netz teilt sich in eine Steuerungs- und eine Datentransport-Ebene

Ein neu eingeführtes Grundprinzip des SDN ist die Trennung zwischen der Daten- und der Steuerungsebene. Die Datenebene realisiert den Transport der Datenpakete, die Steuerungsebene macht die Vorgaben für die Wege der Datenpaketen innerhalb der Datenebene.

Der klassische Router interpretiert die in den IP-Datenpaketen enthaltenen Zieladressen und sendet das gesamte Paket dann anhand der Zieladresse und Vorgaben einer Routing-Tabelle in Richtung des gewünschten Ziels. Die Daten und die Steuerinformationen für die Daten bildeten eine Einheit, das IP-Paket. Die Steuerung in den klassischen Routern wird oft von einer firmenspezifischen Software und speziellen Integrierten Schaltungen (Application Specific Integrated Circuits – ASICs) übernommen. Mit Software-defined Networking kommt eine sehr strikte Trennung dieser beiden Informationsströme; unterschieden wird:

- Control Plane (CP), die alle Elemente und Systeme zur Steuerung der Datenpakete umfasst. Die Control Plane trifft die Entscheidungen, welche Wege die Datenpakete durch das Netz nehmen, anhand eines zentralen Netzabbilds und Informationen von den Netzelementen zu der augenblicklichen Belastung des Netzelements oder der Verbindungen zwischen den Elementen. Hierfür werden kontinuierlich Monitor-Informationen von den Netzelementen an die Steuerung gesendet.
- Data Plane (DP), die alle Netzelemente und Systeme zum eigentlichen Datentransport umfasst; sie leitet die Pakete zum gewünschten Ziel aufgrund der Vorgaben des Control Plane.

OpenFlow

Das Bindeglied zwischen beiden Ebenen bildet das *OpenFlow-Protokoll,* über das die Control Plane Instruktionen an die Data Plane senden kann und umgekehrt von der Data Plane Informationen zur Netzauslastung erhält. Die OpenFlow-Spezifikation wurde herstellerunabhängig von der Organisation Open Networking Foundation (ONF) spezifiziert, den Grundstein hierzu legten Arbeiten der Stanford University in Kalifornien, diese gemeinnützige Organisation ist ein Zusammenschluss von Anwendern, Herstellern und Netzbetreibern mit dem Ziel, den Einsatz des SDN zu fördern und offene Standards für diesen Bereich zu entwickeln. Produkte vieler Hersteller basieren auf diesen Festlegungen, daneben gibt es aber auch firmeneigene Protokolle.

OpenDaylight

Desweiteren gibt es in diesem Umfeld auch viele Open-Source-Entwicklungen wie *OpenDaylight* für die Realisierung (oder Basis dafür) des Conrollers in Software-defined Networking oder als Basis firmenspezifischer Lösungen. Die europäische Standardisierung für die Telekommunikation (European Telecommunications Standards Institute – ETSI) arbeitet mit der ONF sehr eng im Bereich des SDN und der Network Functions Virtualization (NFV) zusammen. Die *International Telecommunication Union, Telecommunication Standardization Sector* (ITU-T) stellen ebenfalls Standards in Zusammenarbeit mit ONF und ETSI zu SDN und NFV zur Verfügung (z. B. Y.330).

4.1.1 Arbeitsweise der SDN-Switche

Die Parameter für die Definition eines Flows

Die *SDN-Switche* arbeiten mit den bereits vorhandenen Parametern der Schicht 1 bis 4, d.h., die Entscheidung, welchen Weg ein eintreffendes Paket am Eingang eines Netzelements nimmt, kann beispielsweise abhängen von:

- Schicht 1: der Eingangsport: Alle Pakete, die an einem bestimmten Port eintreffen, werden ohne weitere Bearbeitung an einen anderen, vordefinierten Port gesendet. Diese Funktion entspricht einer Festverbindung zwischen zwei Anschlüssen.
- Schicht 2: Abhängig von der adressierten MAC-Adresse wird das Paket zu einem (oder mehreren) Ausgängen geschaltet. Vor dem Weiterleiten des Pakets können noch vorgegebene Parameter in Schicht 2 bis 4 vom Netzelement geändert werden, z. B. eine neue Ziel-IP-Adresse angefügt werden. Damit können viele Standorte übergreifende Schicht-2-Netze aufgebaut werden.
- Schicht 3: Anhand der Ziel-IP-Adresse wird ein bestimmter Weg durch die Netzelemente vorgegeben. Auch hier können die Netzelemente ggf. Parameter der Schichten 2 bis 4 vor dem Weiterleiten ändern.
- Schicht 4: Hier bestimmt der Source- oder Destination-Port den weiteren Pakettransport.

SDN ist kein Netz, mit SDN kann man Netze bauen

Die Bearbeitung von vielen bereits vorhandenen Parametern der Schicht 1 bis 4 ermöglicht neue, weitreichende Funktionen für die Bildung von privaten und öffentlichen Netzen. Dies ermöglicht beispielsweise virtuelle Netzstrukturen für verschiedene öffentliche und/oder private Cloud-Angebote, die sich dynamisch an die Verkehrsanforderungen angepassen können. Zusätzlich können Funktionen, wie Traffic Shaping an den Netzkanten am Eingang der Netze eingesetzt werden, die dann für ein definiertes Netzverhalten und berechenbaren Verkehr im Netz sorgen.

4.1.2 Netzstruktur und Netzelemente

Die zentrale Steuerung macht die Vorgaben für den Flow

Im grundsätzlichen Ansatz des SDN wird die Steuerung in zentrale Netzelemente, den Controller (Server) verlagert, der die Vorgaben für die Steuerung der Datenströme (dieser wird als *Flow* bezeichnet) in sog. Flow Tables definiert. Diese Vorgaben werden von einem externen Controller über eigene, gesicherte Schnittstellen in den Switch geladen. Sind die Vorgaben in der Flow Table vorhanden, wird jedes Paket, welches diesen Vorgaben (z. B. der gewünschten Zieladresse) entspricht, nach dieser Vorgabe behandelt und weitergeleitet. Der Controller macht also seine Vorgaben nicht für jedes Paket einzeln, sondern für alle Pakete, die (z. B. mit dem gleichen Anfangs- und Endpunkt) zum gleichen Flow gehören. Ein Controller ist eine zentrale Software-Applikation, die aus Sicherheits- oder Lastgründen mehrfach vorhanden sein kann oder dupliziert vorhanden ist. Wenn nur ein SDN-Controller vorhanden ist, macht dieser die Vorgaben für alle SDN-Switche. Die

Flow Tables werden in die einzelnen Netzelemente für den Datentransport geladen und dort in Forwarding Tables umgesetzt. Anhand dieser Tabellen werden dann die eigentlichen Datenpakete jeweils weitergeleitet.

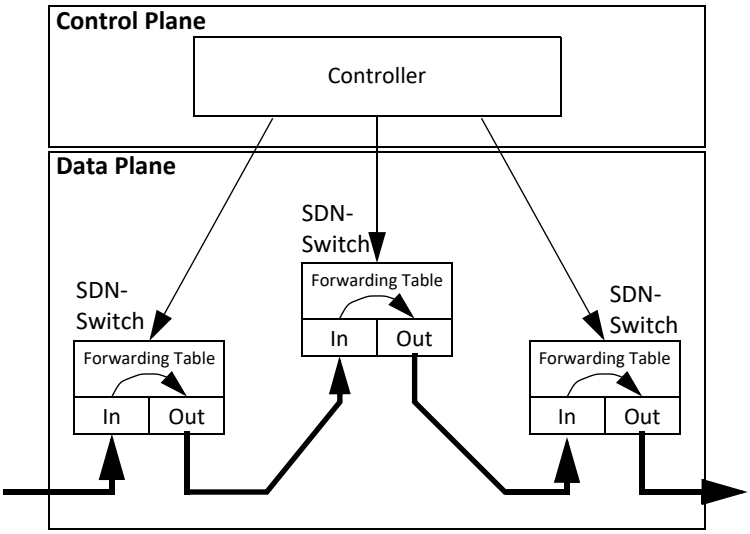


Abb. 271: *Trennung von Steuerung und Datentransport*

Aufbau eines SDN-Switch

SDN-Netzelement

Ein SDN-Switch unterscheidet sich von einem klassischen Switch dadurch, dass er nicht nur die Layer 2, sondern die Schichten 1 bis 4 (je nach Vorgaben durch den Controller) gleichzeitig bearbeiten kann. Der genaue Aufbau eines SDN-Switch hängt vom Einsatzfall, dem Leistungsumfang und den Herstellern ab. An dieser Stelle soll ein einfacher SDN-Switch (oder besser ein SDN-Netzelement) in einem LAN betrachtet werden.

Aufbau eines SDN-Netzelements

Ein SDN-Netzelement verfügt über mehrere Ethernet-Schnittstellen, im Backbone können auch direkte optische Schnittstellen mit WDM eingesetzt werden. Durch die Vorgaben des Controllers in den Flow Tables können die Funktionen des Netzelements vorgegeben und verändert werden. Die Software im Controller legt die Funktion im SDN-Switch je Flow fest – daher ein „Software-defined" Network. Neben den vielen neuen und erweiterten Funktionalitäten kann ein SDN-Switch sich auch auf einfache, konventionelle Funktionen, wie ein einfacher Layer-2-Switch oder Router beschränken. Die Vorgaben vom Controller werden über, meist gesicherte Verbindungen, an den SDN-Switch gesendet und in den Angaben der Flow Tables gespeichert. Für jede Verbindung (Flow) wird eine *Flow Table* mit den Vorgaben für die Paketbehandlung angelegt. Ist für ein eintreffendes Paket keine Flow Table vorhanden, wird das Paket zur weiteren Beurteilung an den Controller gesendet, dieser legt die weitere Behandlung für das Paket in einer Vorgabe für eine neue Flow Table fest. In einer eigenen Flow Table können die Vorgaben für Gruppenverbindungen abgelegt werden.

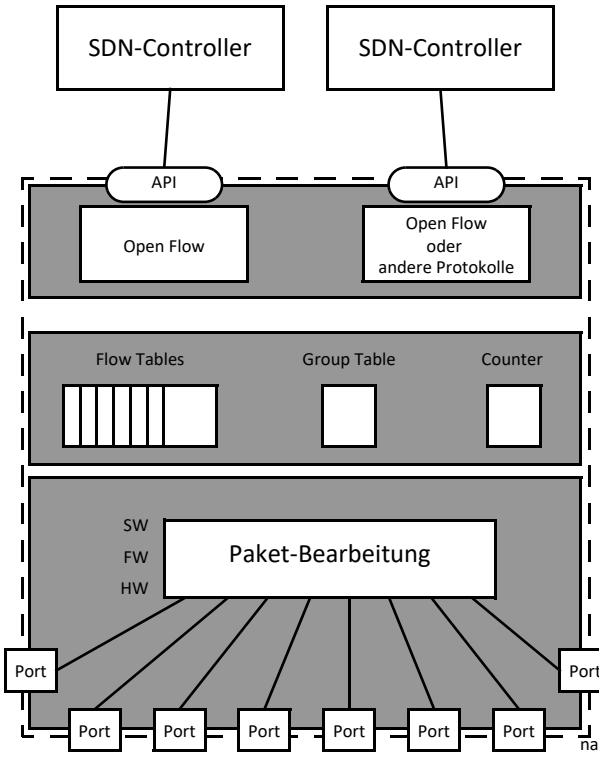
OpenFlow

Der Nachrichtenaustausch zwischen dem SDN-Switch und dem Controller basiert beispielsweise auf der OpenFlow-Spezifikation, alternativ können andere, auch firmenspezifische, Protokolle zum Einsatz kommen.

Monitoring

Der Counter zählt in jedem Switch die Nutzung der Flows, die eintreffenden Ankunftsraten und sammelt Daten zu der augenblicklichen Auslastung von einzelnen Ports und des Gesamtsystems. Diese statistischen Daten werden auf Anfrage in regelmäßigen Abständen an den Controller gesendet. Optional können auch die Anzahl der eintreffenden Pakete insgesamt oder pro vorgegebener Zeit ermittelt werden, die dann als Grundlage für eine Tarifierung (Metering) dienen können.

Abb. 272: *Aufbau eines SDN-Netzelements*



Ports

Zur Vernetzung mit anderen SDN-Netzelementen und/oder konventionellen Netzelementen (wie L2-Switchen oder Routern) verfügt der SDN-Switch über eine Anzahl von Ports. Diese Schnittstellen können als Ethernet-Schnittstellen mit den verschiedenen Geschwindigkeiten oder optische Schnittstellen mit Wellenlängenmultiplex ausgeführt sein. Aus Geschwindigkeitsgründen erfolgen die Bearbeitung der Pakete und das Weiterleiten in Richtung des Ziels in Hardware.

Weiterleitung der Pakete in HW

Die Netzelemente für den Datentransport müssen nicht mehr diverse Protokolle für das Management und Routing innerhalb dieser Netze bearbeiten und beschränken sich auf die reine Weiterleitung von Nutzpaketen (und zu einem kleinen Teil die Erkennung von Steuerinformationen und deren Weiterleitung zu dem zentralen Controller). Damit

steigt automatisch die Leistungsfähigkeit dieser Systeme und des gesamten Netzes. Anders als beim klassischen Routing wird die Wahl des besten Wegs durch das Netz nicht mehr auf viele, einzelne autonome Netzelemente (den Routern und Switchen) von Abschnitt zu Abschnitt immer wieder neu entschieden, sondern eine übergeordnete Instanz legt den Weg unter Berücksichtigung der augenblicklichen Netzauslastung von Anfang bis Ende fest. Das Konzept ist nicht ganz neu, die klassischen Telekommunikationsnetze hatten genau diesen Ansatz: eine strikte Trennung von einem Nutzwegnetz und separat behandelte Signalisierungswege mit Steuerungseinrichtung, die Vorgaben für die rein in Hardware geschalteten Nutzkanäle machten.

Die Funktion des Netzelements legt der Controller fest

In einem SDN-Netzelement können auch konventionelle Funktionen, beispielsweise eine Router-Funktion, untergebracht werden (hybrides Netzelement). Die Router-Funktionen können in der Einführungsphase mit dem klassischen Netz ohne Änderungen der klassischen Netzelemente zusammenarbeiten und bei Ausfall des zentralen Controllers Wege durch das Netz festlegen.

4.1.3 SDN-Schnittstellen

East-/West- und North-/South-Verkehr

Der Datenverkehr zwischen Netzelementen der gleichen Ebene (Data- und Control-Ebene) wird als East-/West-Verkehr (horizontal) bezeichnet. Mit dieser Schnittstelle werden Netzelemente oder Controller des gleichen oder verschiedener Netze zusammengeschaltet. Der Verkehr von einem SDN-Controller zu einer unterliegenden Ebene (Data-Ebene) läuft über die South- und der zu einer höher (Application-Ebene) liegenden Schnittstelle über die North-Schnittstelle (vertikaler Verkehr). Die Richtungen North (oben) und South (unten) beziehen sich immer auf die Sicht des Controllers.

Zentrale Steuerung

In der Abbildung 273 ist der Controller das zentrale Element. Häufig wird nur *ein* zentraler Controller dargestellt, grundsätzlich können diese Aufgabe aber auch mehrere Controller übernehmen. Zum einen muss eine solche zentrale Einheit aus Gründen der größeren Sicherheit und Verfügbarkeit mehrfach vorhanden sein. Weiterhin kann ein Betreiber ein sehr großes Netz in Abschnitte (sog. *SDN-Domäne*) aufteilen, die jeweils durch einen regionalen Controller gesteuert werden. Untereinander müssen die Controller eng miteinander gekoppelt werden. Diese Kopplung verwendet meistens Hersteller-spezifische Protokolle. In der OpenFlow-Spezifikation werden hierzu keine Vorgaben gemacht.