3 Software-defined Networking

3.1 Der prinzipielle Ansatz

3.1.1 Grundlagen

Betriebssystem für die Netze

Software-defined Networking (*SDN*) oder Software-gesteuerte Netzarchitekturen (manchmal auch als programmierbare Netze bezeichnet) vereinfachen die Netzelemente, sie lösen die Steuerungsfunktionen von den Komponenten ab, die die Pakete mit Nutzerinformationen mit großer Geschwindigkeit zum Ziel leiten. Die Technik des SDN ist nicht durchgängig einheitlich. Neben den Rahmenspezifikationen der *Open Network Foundation* (ONF), die mit dem OpenFlow Protocol (https://opennetworking.org) eine wichtige Grundlage für SDN schuf, sind andere Organisationen wie die IETF, die ITU-T und ETSI in diesem Bereich tätig, zusätzlich sind auch viele Hersteller- oder auch Kunden-spezifische Lösungen verfügbar. In der ONF sind Firmen wie Google, Facebook, Microsoft, Stanford University, UC Berkeley, Deutsche Telekom u.v.a. als Mitglieder aktiv. Mehrere Working-Groups arbeiten an Spezifikationen, Usecases und Withepapers zu speziellen Themen (Architektur, Configuration & Management, Testing & Interop., Optical Transport, Wireless & Mobile u.v.a.). In weiteren wird versucht, die Grundfunktionen und die wichtigsten Protokolle und Funktionen verständlich darzustellen. Dies kann und will daher keine umfassende und vollständige Darstellung aller Aktivitäten in diesem Bereich sein. Die Technik des SDN steht gerade erst am Anfang, vieles entwickelt sich erst noch. Dieses Buch kann daher auch kein Ersatz für die aktuellen Spezifikationen sein, hier soll vielmehr nur der Grundansatz und die prinzipielle Arbeitsweise dieser Technik dargestellt werden. In der Praxis wird man daher auch andere Realisationen, Misch- oder Migrationsformen finden, auf die hier auch nicht eingegangen werden kann.

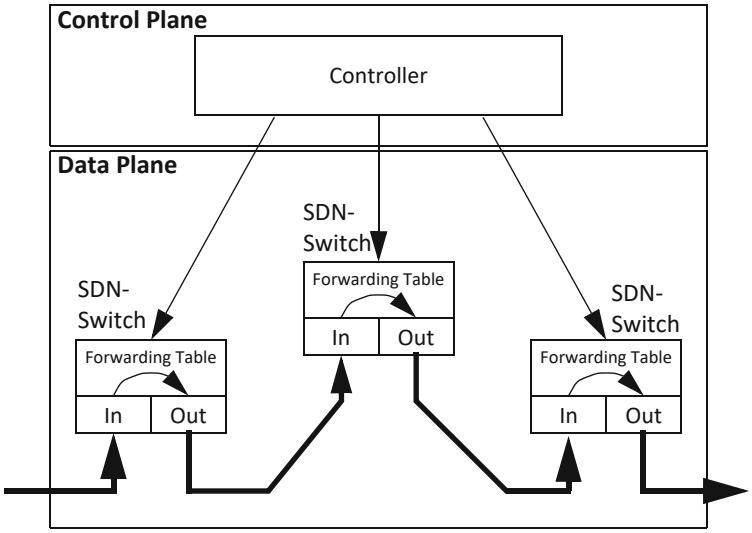
Netzstruktur und Netzelemente

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-Appli-

kation, 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. 222: *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 prinzipiell 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 Con-

troller 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.

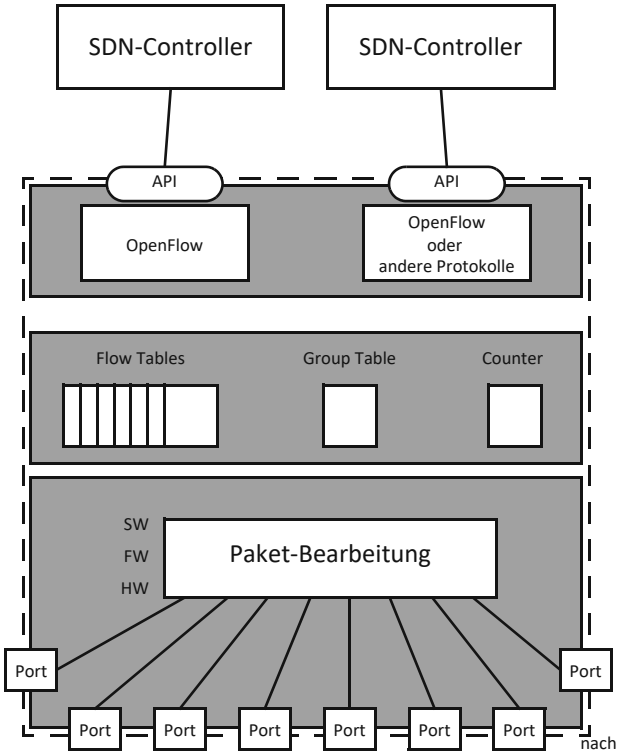


Abb. 223: *Aufbau eines SDN-Netzelements*

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-Funktion 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.

Control und Data Plane

Data und Control Plane

Der SDN-Ansatz trennt strikt die Behandlung der Pakete mit den Nutzdaten in der Data Plane und die Steuerungsebene für diese Daten-Netzelemente (*Control Plane*). Mit Hilfe des Control Plane werden sog. Flows definiert. Ein Flow ist ein Datenstrom (eine Anzahl von IP-Paketen) einer bestimmten Dienstart oder Anwendung zwischen zwei entfernten Systemen. Alle Pakete eines Flows haben den gleichen Anfangs- und Endpunkt, der durch die MAC-Adresse, die IP-Adresse und/oder den UDP/TCP-Port gekennzeichnet sein kann.

Klare Vorgaben für den Lauf der Pakete

Von einem Client können mehrere unterschiedliche Flows auch zum selben Zielgerät existieren, wenn sich beispielsweise die VLAN-Kennungen oder die TCP-Ports unterscheiden, weil beispielsweise Daten zu unterschiedlichen Anwendungen ausgetauscht werden. Für einen solchen *Flow* werden Vorschriften (rules) für die Bearbeitung der Datenpakete in einer sog. Flow Table definiert. Diese Flow Tables werden dann von dem Controller in die Netzelemente für den Transport der Nutzdaten geladen. Alle Pakete eines bestimmten Flows werden dann durch die Netzelemente, den SDN-Switchen (auch als *SDN Devices* oder als *SDN-Netzelemente* bezeichnet), nach jeweiligen Vorgaben behandelt, ggf. Parameter in den Paketköpfen geändert und die Datenpakete schließlich zum gewünschten Ziel geleitet (*paket forwarding*). Diese Weiterleitung der Daten nach festen Vorschriften erfolgt innerhalb der SDN-Netzelementen meist in Hardware.

Unbekannte Pakete werden zum Controller geleitet

Nur wenn keine Flow Table gefunden werden kann oder es sich bei dem eintreffenden Paket um spezielle Steuerpakete handelt, werden Pakete an den Controller geleitet. Für diesen neuen Flow werden dann die Vorgaben für alle beteiligten Netzelemente ermittelt und in die Netzelemente geladen. Die Vorgaben können Änderungen der über-

tragenen Parameter beinhalten (z. B. die Änderung der Zieladresse oder die Umwandlung von einer IPv4- in eine IPv6-Adresse), das Paket zu einem bestimmten Ausgang leiten oder das Paket verwerfen (Drop). Die Ermittlung der Vorgaben dauert einige wenige Millisekunden (der genaue Wert hängt von der augenblicklichen Auslastung des Controllers ab), länger als das spätere Weiterleiten der Pakete durch die Netzelemente. Ein Paketverlust tritt dabei nicht auf. Die große Menge der zu transportierenden Pakete wird durch die Switche und durch die Forwarding Tables automatisch transportiert und verbleiben damit in dem Data Plane. Die kleinste Einheit, die von dem Controller gesteuert werden kann, ist der sog. Flow, nicht das einzelne IP-Paket. Die Vorgaben, wie ein eintreffendes Paket eines bestimmten Flows zu behandeln ist und zu welchem Port mit welchen Adressen es geleitet werden soll, werden nur einmal vom Controller in den Switch geladen. Die Behandlung einzelner Pakete durch den Controller ist damit nicht notwendig.

OpenFlow oder Hersteller-spezifische Protokolle

Die Vorgaben für die Netzelemente der Data Plane werden mit der Hilfe des Protokolls *OpenFlow* von der *Open Network Foundation* (ONF) übertragen, alternativ können Hersteller-spezifische Protokolle verwendet werden. Die ONF wurde von vielen Herstellern und Netzbetreibern gegründet, daneben ist noch die OpenDayligth-Gruppe im Bereich der Software für Netzelemente aktiv. Während in der ONF, grob gesehen, mehr die Netzbetreiber und großen Anwender (z. B. die Deutsche Telekom, Microsoft, Google, Facebook und Yahoo) aktiv sind, ist OpenDayligth mehr Hersteller- und Software-orientiert (Citrix, Cisco, IBM, Red Hat usw.).

3.1.2 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 224 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. Das kann bedeuten, dass innerhalb einer Domäne nur Systeme eines Herstellers ohne Probleme zusammengeschaltet werden können.