ComConsult Research

Der Netzwerk Insider

April 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

von Dipl.-Ing. Harmut Kell

Wer kennt es nicht, die Verkabelung wurde fachgerecht installiert, alles perfekt dokumentiert und die Inbetriebnahme der einzelnen Teilstrecken stehen an.

Am Anfang ist noch alles sehr übersichtlich, ein Aufschalten der Strecken geht leicht von der Hand, Erfolgserlebnisse sind schnell zu bekommen. Da verzichtet man, insbesondere aufgrund des Zeitdrucks, der bei einer Inbetriebnahme herrscht, gerne auf die Dokumentation der Rangierungen, wohlwissend, dass man ohnehin niemals wieder Zeit dafür finden wird. Doch dann kommt der Tag X: Im laufenden Betrieb müssen Änderungen an den Rangierungen durchgeführt werden, da größere Umzüge von Abteilungen oder Projektteams anstehen. Oder es ist die Suche nach einem Fehler notwendig, die ein Nutzer eines Endgerätes – oder noch schlimmer – eines Servers meldet. Spätestens in diesem Moment wird sich herausstellen, ob der Verzicht auf eine Rangierdokumentation nicht bereut wird. Im vorliegenden Artikel wird dargestellt, worauf es bei einer Dokumentation der Rangierung ankommt und wie aktuelle Techniken durch automatische Erfassung von Rangierungen das Leben einfacher machen können.

weiter auf Seite 7

Zweitthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 2

von Dipl.-Inform. Petra Borowka-Gatzweiler

1.4 OpenDaylight Projekt

Nicht zuletzt aus Unzufriedenheit mit der ONF hinsichtlich der dauerhaft verschleppten Spezifikation des Northbound Interface, aber auch mit der Motivation, eine vollständige Architektur zu spezifizieren und pragmatisch als OpenSource zu implementieren, wurde im April 2013 das OpenDaylight Consortium gegründet. Im September 2014 hatten sich 41 Mitglieder dem Consortium angeschlossen, im Februar 2014 wurde mit "Hydrogen" das erste Release, im Oktober 2014 das zweite Release "Helium" verabschiedet. (siehe Abbildungen 1.8 und 1.9)

Während sich ONF nicht wirklich entscheiden konnte, hat OpenDaylight sich für ein marktfreundliches REST API als Northbound Schnittstelle entschieden. Die Southbound Schnittstelle ist ziemlich agnostisch, hier sind verschiedenste Protokolle zugelassen, in Helium nochmals mehr als in Hydrogen. Funktionserweiterungen von Helium enthalten unter anderem Service Chaining (wird im Kapitel NFV behandelt), Föderation von SDN Controllern (East-Westbound Interface), zusätzliche Netzwerk-Virtualisierungs-Optionen und mehr Layer-4 bis Layer-7 Funktionalität.

weiter auf Seite 21

Geleit

Individuelle maßgeschneiderte Infrastrukturen für Unternehmen: der Planungs-Alptraum, aber können wir ihn verhindern?

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

ab Seite 4

Standpunkt

Nachhaltige Informationssicherheit: Ohne Druck geht es nicht

auf Seite 18

Neue Sonderveranstaltungen

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP Das neue IT-Sicherheitsgesetz

ab Seite 19

Zum Geleit

Individuelle maßgeschneiderte Infrastrukturen für Unternehmen: der Planungs-Alptraum, aber können wir ihn verhindern?

Wir erleben seit einigen Monaten einen weitgehenden Wandel in den IT-Architekturen mit erheblichen Auswirkungen auf unsere IT-Infrastrukturen. Und wir müssen feststellen, dass alte Design-Ansätze und Regeln auf einmal nicht mehr gültig sind.

Wie können wir damit umgehen und welche Ansätze gibt es, diesem Wandel sowohl in der Planung von Infrastrukturen als auch im Betrieb gerecht zu werden? Wie individuell müssen Planungen wirklich sein und welche Auswirkungen hat das auf den Betrieb?

Lassen Sie mich zuerst einige Beispiele geben, die den Wandel unterstreichen:

- bis vor Kurzem war die Welt der Server und Speicher-Architekturen zumindest zu 90% einfach in Worte zu fassen. Anwendungen mit hoher CPU- und I/O-Last und einem gleichzeitig hohen Grad an parallelen Benutzern werden am besten mit integrierten Lösungen mit Speicher und Server in einem Schrank bedient. Typische Lösungen kommen u.a. von Oracle und IBM. Alle anderen Anwendungen werden auf virtualisierten Servern mit Ost-West Architekturen zum Zugriff auf einen zentralen Speicher umgesetzt. Zentrale Speichersysteme mit 10 Gigabit Ethernet Anschluss in Kombination mit Low-Latency-Netzwerken führten dazu, dass ein Performance-Unterschied zu einer direkt im Server installierten Festplatte (Direct Attached Storage DAS) kaum feststellbar war. Nun haben PCIe-basierte SSDs zu einer deutlichen Verschiebung geführt. Mit Durchsatzwerten von 10 bis 15 Gigabit/s erreichen sie Leistungen, die über den Ost-West-Verkehr zu einem zentralen Speichersystem nicht mehr ohne erheblichen finanziellen und technischen Aufwand umgesetzt werden können. Also erleben wir eine Wiederbelebung von DAS für einen bestimmten Typ von Anwendungen. Das hat sofortige Auswirkungen auf Virtualisierung und das Wandern von Applikationen zwischen Servern sowohl in der Wahl der überhaupt in Frage kommenden Server als auch im Umfang der zu bewegenden Daten. Gleichzeitig erleben wir eine deutliche Verschiebung im Bereich

von In-Memory Computing. Bisher waren derartige Lösungen mehr in integrierten Schränken anzufinden und typischerweise große Lösungen. Einer der wesentlichen Gründe dafür war das spezielle Datenmodell, das erforderlich war und das erhebliche Anpassungsarbeiten erforderte, um eine bestehende “alte” Anwendung auf In-Memory umzustellen. Dementsprechend hat man diesen Aufwand auch nur für wenige und strategische Anwendungen ins Auge gefasst. Die neue Version von Oracle, die seit dem dritten Quartal 2014 auf dem Markt ist, hat den Umfang der Anpassungsarbeiten in sich zusammen fallen lassen. Damit ist die Tür auf für die Nutzung von In-Memory auch in kleineren und weniger strategischen Anwendungen, die in der Regel den preislichen Mehraufwand einer integrierten Schrank-Lösung nicht rechtfertigen. Hier könnten weitere Beispiele stehen, die aber alle in der gleichen Erkenntnis enden: die Zeiten der wenigen und klar angreifbaren Server-Architekturen ist vorbei. Kombiniert man das mit Anforderungen wie der schnellen Bereitstellung von Anwendungen, dann ist man schnell bei sehr individuellen Lösungen.

- wie viel Gigabit Ethernet sollen es denn nun sein? Die Auswahl der bald verfügbaren Datenraten erweitert sich fast täglich. Und natürlich gibt es irgendwie einen guten Grund für fast jede dieser Datenraten und die Nutzung von Twisted Pair ist eng damit verbunden. Aber für wen ist welche Datenrate die beste? Lässt sich das überhaupt noch sagen? Und wir können nicht pauschal auf modularer Switch-Systeme als Lösung zurück fallen, die Mehrkosten sind einfach zu hoch.

- WLANs können Gigabit. Wirklich? In der Praxis ist das verbunden mit sehr kleinen Zellen, wir sprechen von Mikrozellen-Design. Große Zellen enden da wo sie herkommen, eben nicht bei Gigabit. So weit so gut. Aber viele kleine Zel-

Kongress

ComConsult Technologie-Tage 2015
09.11. - 10.11.15 in Düsseldorf

Die ComConsult Technologie-Tage 2015 wenden sich an Entscheider in den Unternehmen. Sie liefern das Fundament zum Verständnis der aktuellsten technologischen Entwicklungen über die Grenzen der bestehenden Silos hinaus. Sie zeigen wie unsere IT in Zukunft aussehen wird.

Moderation: Dr. Jürgen Suppan
Preis: € 1.990,-- netto

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Schwerpunktthema

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Ausgangsbasis

Wie dargestellt, stellt die Ausgangsbasis ein durch das Installationsunternehmen fachgerecht installierter und dokumentierter physikalischer passiver Link im Sinne eines sogenannten Permanent Link dar, also eine Strecke zunächst ohne Anschluss- oder Rangierschnüre. In diesem Falle darf man erwarten, dass beide Enden des Links dokumentiert und vor allem beschriftet sind. Ein Ende stellt in der Regel immer ein Rangierfeld dar und das andere Ende entweder wieder ein Rangierfeld oder eine Anschlussdose. Den im industriellen Umfeld durchaus nicht ungewöhnlichen Fall eines Permanten Links ohne Abschluss in einem Rangierfeld oder einer Dose betrachten wir hier nicht. Die Beschriftung bzw. der dazugehörende Code am Rangierfeld oder Dose wird in der Regel bei den deutlich meisten Dokumentationen – falls sie gemacht wird - in irgendeiner Art in die Rangierdokumentation einfließen. Die Aufgabe der Rangierdokumentation ist es, einen Bezug zwischen dem Port des Rangierfeldes (bzw. der Dose) und dem aktiven Gerät, also z.B. dem Switch (bzw. dem PC oder auch Server) herzustellen. Dazu gibt es mehrere Möglichkeiten, auf die nachfolgend eingegangen werden soll.

Sinn und der Zweck einer Rangierdokumentation

Es darf nicht überraschen, dass es in einer nicht geringen Anzahl von Netzwerkumgebungen gar keine Rangierdokumentation gibt, dies gilt gerade für den Bereich der Endgeräteverkabelung (typischerweise Etagenverteiler mit Twisted Pair als Horizontalkabel). Auch in dem einen oder anderen Rechenzentrum wird gerne darauf verzichtet. Dagegen werden Backbone-Verbindungen - in der Regel Glasfaserstrecken - meistens dokumentiert, denn ein Ausfall einer solchen Strecke bei fehlender Dokumentation benötigt weitere zusätzliche Zeit bis zur eigentlichen Fehlerbehebung und verlängert damit die Mean Time to Repair und bei Backbone-Verbindungen betrifft das häufig größere Teile des Netzwerkes. Es geht tatsächlich in vielen Fällen auch ohne durchgängige Dokumentation, wie gut auch immer.

Mit der Dokumentation sollen insbesondere folgende Dinge vereinfacht werden:

- Bei einer Änderung der Aufschaltungen soll verhindert werden, dass irrtümlich eine falsche Aufschaltung zu einer Unterbrechung eines aktiven Links führt oder die Aufschaltung nicht zum Ziel führte und es zu Verzögerungen kommt, bis der Link aktiv wird.

- Bei einem gemeldeten Fehler auf einem aktiven Link soll nachvollzogen werden können, welche physikalischen Teile des Links, insbesondere welche Verkabelungselemente dazu gehören und weiter zu analysieren sind.

- Zusätzlich gehört natürlich im Rahmen von Change Management-Prozessen auch die Dokumentation der Anweisung an einen Techniker, wie er eine Änderung der Rangierung durchzuführen hat.

Ideal wäre es, eine End-to-End-Dokumentation vorzunehmen, die beide am aktiven Link „beteiligten“ aktiven Geräte berücksichtigt. Da der Verteiler in der Regel der Ausgangspunkt der Änderungen oder auch der Fehlersuche ist, steht dieser in den meisten Fällen im Vordergrund. Für die oben aufgeführten Fälle müssen mindestens bekannt sein:

- Name der aktiven Komponente (häufig auch als Objekt-ID bezeichnet)

- Ebenfalls Name und Einbauort des Rangierfeldes (ebenfalls Objekt-ID)

- Slot- und Port-Nummer auf beiden Komponenten

Diskutiert werden kann, ob folgende Infos ebenfalls zur Input-Dokumentation gehören müssen/sollen:

- Objekt-ID der Rangier- oder Anschlussschnur (siehe Textblock auf Seite 25)

- Übertragungstechnische Qualität der Strecke (sogenannte Channel Link Performance)

- Angaben zum „anderen“ Ende der Strecke; bei der Tertiärverkabelung wäre das z.B. der Raum der Dose oder ein Koordinatenpunkt in einem Grundriss (z.B. bei einer Dose für einen WLAN-Anschluss)

Aus der Dokumentation müssen im Idealfall über jedes bekannte Detail alle Elemente des aktiven (oder auch passiven) Links ermittelt werden können. Vereinfachend folgende Beispiele:

Beispiel Tertiärbereich: Meldet ein Nutzer mit einem kabelgebundenen Anschluss eine völlige Unterbrechung seiner

Schluss mit dem Rangierchaos: Das intelligente Rangierfeld macht alles einfacher

Netzwerk-Verbindung muss im einfachsten Falle über die Dosen/Portnummer des Anschlusses ermittelt werden können, auf welchem Switch-Port das Endgerät angeschlossen worden ist. Bei den meisten Beschriftungsrichtlinien weist die Dosen/Port-Nummer aus, in welchem Technikraum, welchem Schrank und auf welchem Rangierfeldport das Endgerät angeschlossen ist. Bis hier ist eine Rangierdokumentation noch nicht zwingend notwendig, sie vereinfacht aber die Suche bereits. Spätestens bei der Frage, auf welchen Switch-Port denn der Anschluss aufgeschaltet ist, braucht man entweder eine Dokumentation oder man muss sehr mühsam mit Hilfe von „Kabelabtasten“ die Zuordnung ermitteln.

Abbildung 1: Beschriftung mit direkter Ablesbarkeit des Ziels

Beispiel Rechenzentrum: Ein Server in einem Server-Schrank in der Mitte einer Schrankreihe wurde mit Hilfe einer Glasfaserverbindung über das Rangierfeld im Server-Schrank und dann wieder über den Kopfschrank der Reihe zu einem weiteren Netzwerk-Schrank irgendwo im Raum durchgeschaltet (siehe Abbildung 2); der Server soll in Zukunft nicht mehr benutzt werden. Diese Verbindung ist aufgrund des bereits vollständig belegten Rangierfeldes vollständig aufzulösen. Ohne eine Dokumentation der Rangierungen kann es zu einem sehr gewagten Unternehmen werden, die Rangierungen einfach zu entfernen. Selbst ein Abtasten der Rangierkabel ist mit Risiko verbunden, da Fehler auch hier nicht ausgeschlossen werden können.

Traditionelle Rangierdokumentation

Bei einer „traditionellen“ Methode erfolgt die Erfassung des rangierten Links auf Basis von einfachen Tabellen, oder bei einer „eleganteren“ Lösung auf Basis eines speziellen Dokumentations- oder Datenbanksystems. In beiden Fällen erfolgen die Erfassung der Informationen und

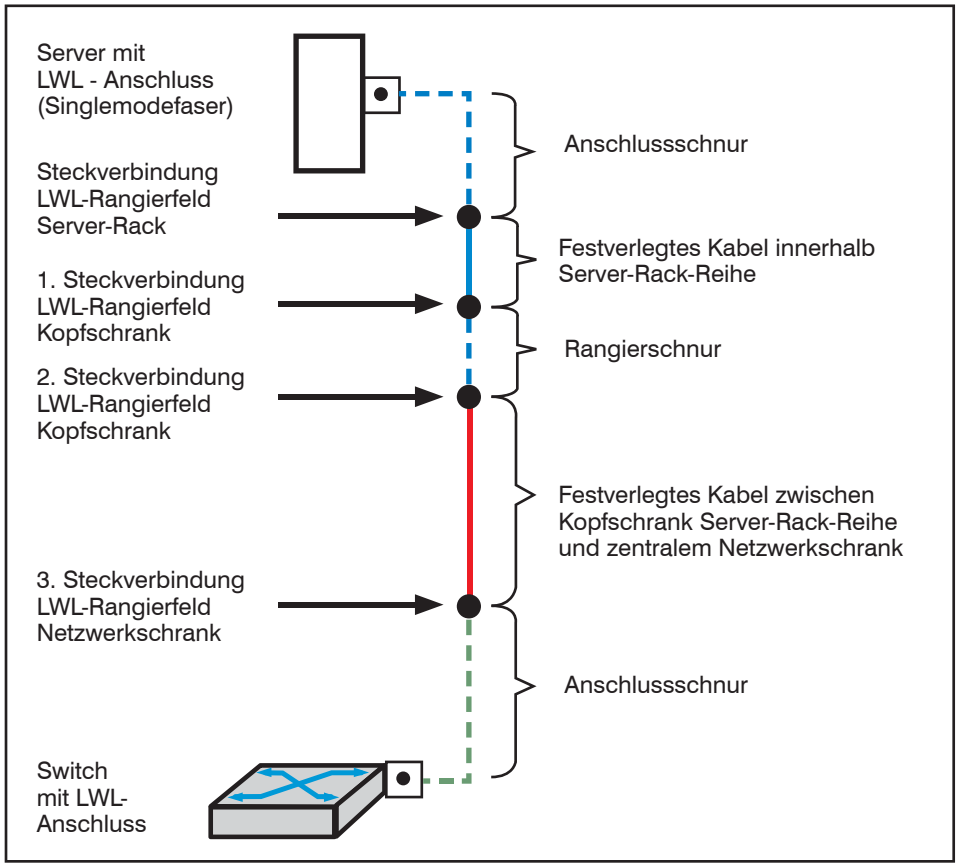

Abbildung 2: LWL-Rangierungen im Rechenzentrum

auch die Änderungen des Zustands manuell, sie muss von Personen durch eine visuelle Erfassung vor Ort aufgenommen und in den Listen / Datenbanksätzen nachgetragen werden.

ComConsult BERATUNG + PLANUNG	Rangierliste			Erfasser:_____			Datum:_____
	Gebäude:			Etage:			Verteilernr.:
Rangierkabel	von ·····			····· nach			Bemerkungen:
Typ/Nr.	Schrank	Rangierfeld Nr.	Port	Schrank	Switch	Slot	Port

Abbildung 3: Grundaufbau Rangierliste

Zweitthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz (Teil 2)

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Fortsetzung von Seite 1

Als Strategie ist klar erkennbar, ein einheitliches Northbound Interface festzulegen und vielfältige Southbound Interfaces zu unterstützen. Hier bewegt sich OpenDaylight diametral entgegengesetzt zur ONF (NBI = offen, SBI = eindeutig OpenFlow).

Somit lässt sich sagen, dass OpenDaylight klar einen breiteren Horizont als ONF SDN hat und sich hier die Grenzen zwischen SDN und NFV (Network Function Virtualisation) teilweise verwischen.

Stimmen aus dem Markt sagen: "OpenDaylight is quickly evolving into something formidable with good potential for mainstream relevancy" (Andrew Lerner, Gartner). Oder. "OpenDaylight is making steady progress cultivating a growing community of developers and users interested in adopting an open, common SDN controller platform" (Brad Casemore, IDC Research Director for Datacenter Networks).

Insgesamt hat OpenDaylight das Potenzial, sich an ONF vorbei zum de facto Standard entwickeln.

2. NFV - Network Function Virtualisation

Salopp gesagt steckt dahinter NFV die Vision, Netzwerke aus einer Ansammlung proprietärer Boxen zu einer Ansammlung von Software-Komponenten zu überführen, die auf Industriestandard-Hardware (COTS) laufen. Solche Netzkomponenten sind beispielsweise Router, Deep Packet Inspection (DPI) Komponenten, CDN Appliances, Firewalls, Load Balancer, NAT-Boxen, SBCs, WAN-Beschleuniger, Controller für Mobilnetz-Basisstationen, Mobilnetz Packet Gateways, Test- und Monitoring Komponenten usw. Bei den aufgeführten Komponenten drängt sich der Gedanke auf, dass NFV sich mit Layer-4 bis Layer-7 Diensten befasst. Dies ist aktuell tatsächlich der Fokus, grundsätzlich könnte NFV aber auch niedrigere Netzwerk-Schichten implementieren (natürlich nicht das Physical Layer …).

NFV will konventionelle Netzwerke weg von proprietären Boxen und hin zu Software-Komponenten überführen, die auf Industriestandard-Hardware (COTS) laufen.

Für NFV gilt das Motto: Cores haben wir reichlich, und Alles ist darauf lauffähig; warum also nicht auch Netzwerk-Funktionen? So weit so gut – oder auch nicht. Warum kam nicht schon früher Jemand auf die Idee NFV? Weil es erst mit den neuesten Entwicklungen Standardhardware mit ausreichend Rechenleistung, ausreichend viel und ausreichend schnellem Cache Speicher gibt. Damit hat sich die Bandbreite, die die Peripherie-Chips einer CPU unterstützen, drastisch erhöht.

Grundsätzlich gilt für Netzwerke: die Con-

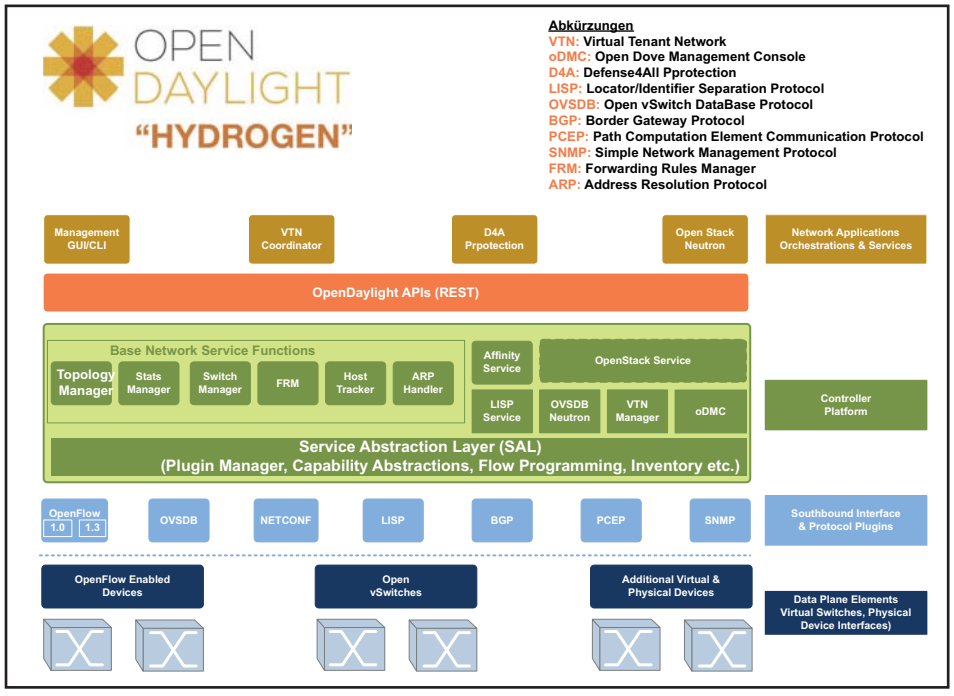

Abbildung 1.8: OpenDaylight Hydrogen Architektur

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 2

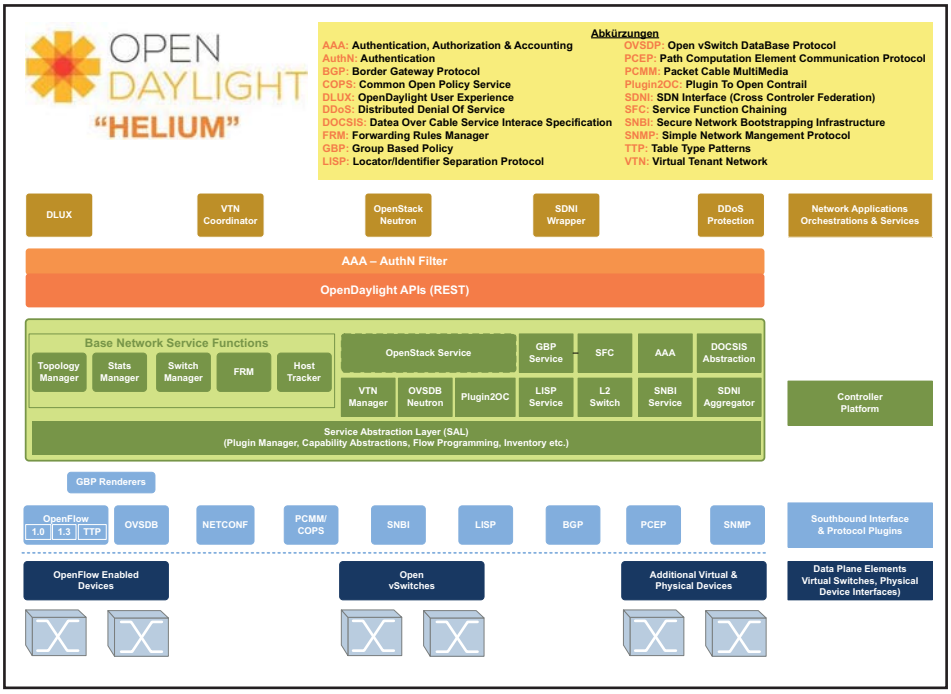

Abbildung 1.9: OpenDaylight Helium Architektur

trol Plane beschäftigt sich mit Routing- oder Signalisierungs-Protokollen, Einrichtung oder Herunterfahren von Sessions, Authentisierung und ähnlichem. Sie ist CPU-intensiv, benötigt aber wenig Bandbreite. Die Data Plane beschäftigt sich mit der Weiterleitung der realen Verkehrslast, diese ist bandbreitenintensiv, benötigt aber wenig CPU-Leistung. Ein Beispiel: Das Aufsetzen eines Telefonats in einem IMS Netzwerk benötigt typischerweise 10 bis 15 SIP Signalisierungs-Pakete aufseiten der Control Plane, während 3 Minuten Telefongespräch (Media Stream) den Austausch von 36.000 RTP Paketen erfordern. Control Planes arbeiten heute schon mit General Purpose CPUs, die Data Plane wird bislang dagegen vielfach aus Leistungsgründen mit proprietärer Hardware bestückt.

Im Bereich Network Function Virtualisation gibt es mehrere Aktivitäten. Das zur Zeit aktivste Standardisierungs-Gremium ist die ETSI mit ihrer Industry Specification Group NFV, die sich im Januar 2013 konstituiert hat. Hier wurden unter Mitarbeit von weltweit ca. 230+ Unternehmen eine Reihe Technische Spezifikationen verabschiedet, die Einsatz-Szenarien, Architektur und verschiedene Unterbereiche beschreiben. Mit Phase 1 der Arbeitsgruppe wurde die Basis-Arbeit abgeschlossen, in der jetzigen Phase 2 sollen Spezifikationen zur Implementierung erarbeitet werden.

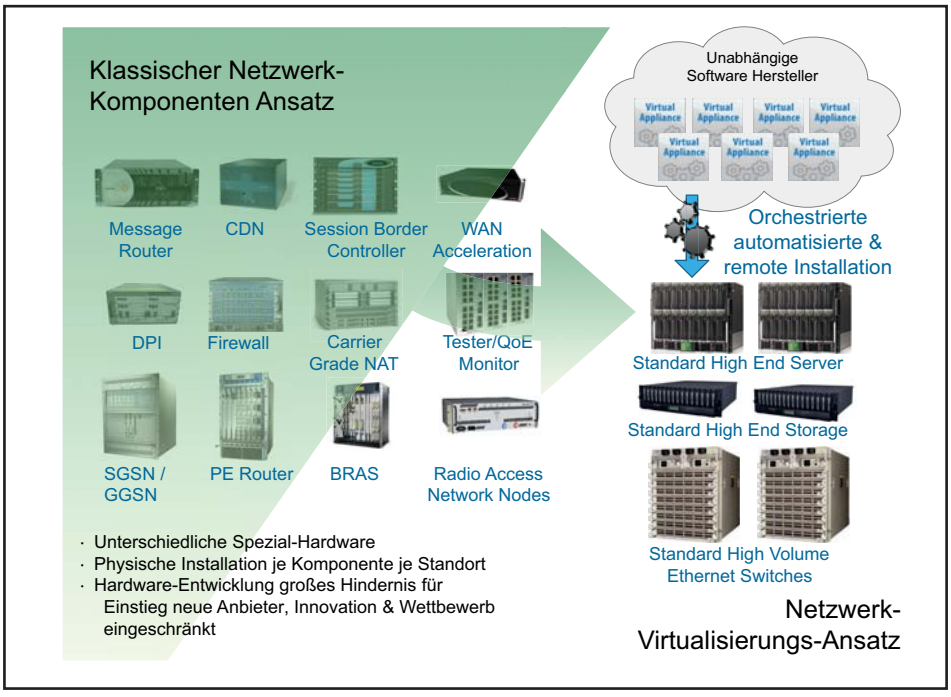

Abbildung 2.1: Vision von Network Functions Virtualisation

Im September 2014 hat die Linux Foundation ein Projekt "Open Platform for NFV" aufgelegt (OPNFV), das auf der Basis der ETSI-Spezifikationen eine NFV Referenz-Plattform entwickeln will.

Bei der IETF gibt es eine Arbeitsgruppe SFC zum Thema Service Function Chaining, die eine ähnliche Richtung wie die VNF-Forwarding Graphen der ETSI NFV Arbeitsgruppe hat.

In diesem Beitrag wird NFV in Anlehnung an die ETSI Spezifikationen betrachtet.

NFV hat das Ziel, Netzwerk-Architekturen und Netzwerk-Betrieb so zu transformieren, dass das bislang sehr vielfältige Netzwerk-Equipment durch Standard IT Virtualisierungs-Technologien auf den Einsatz von Industriestandard Hochleistungs-Servern, Industriestandard Switches und Industriestandard Speicher konsolidiert wird, wie Abbildung 2.1 zeigt.

Im Zuge der Netzwerkarchitektur-Transformation werden Netzwerkfunktionen in Software implementiert, die auf Industriestandard Serverhardware lauffähig ist, der Netzwerkbetrieb wird dahingehend transformiert, dass diese Software je nach aktuellem Bedarf dynamisch an verschiedene Lokationen migrieren oder in verschiedenen Lokationen instanziiert werden kann, ohne dass Irgendjemand hierfür physisch neue Komponenten / neues Equipment installieren und in Betrieb nehmen muss. Somit ist NFV insbesondere auf Cloud Umgebungen fokussiert. Ziel ist über die Architektur hinaus die Nutzung von IT Standardprozessen für das gesamte Netzwerk-Lifecycle Management, insbesondere auch durch den Einsatz entsprechend an NFV angepasste OSS/BSS Tools.

In der Praxis besteht eine NFV Lösung in der Regel aus drei Kernelementen: COTS Hardware, einem Hypervisor wie KVM oder ESXi, einer Cloud Management Lösung wie OpenStack oder VMware vSphere.