Hochschule Magdeburg-Stendal
Fachbereich Ingenieurwissenschaften und Industriedesign (IWID)
Institut für Elektrotechnik

Masterarbeit

zur Erlangung des Grades eines "Master of Engineering"
im Studiengang Elektrotechnik

Thema:
„Konzept zur Migration von Software-Defined-Network-Strukturen in ein zeitkritisches, hochverfügbares Datennetzwerk“

Eingereicht von: Daniel Gerlach, B.Eng.
Angefertigt für: SBSK GmbH & Co. KG
Matrikel: 2012 2075

Ausgabetermin: 04.10.2018
Abgabetermin: 18.01.2019

Schulischer Betreuer: Prof. Dr.-Ing. Dieter Schwarzenau
Betrieblicher Betreuer: Dipl.-Ing. Dirk Bartens

....
1. Prüfer 2. Prüfer

Selbstständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Masterarbeit ohne unzulässige Hilfe Dritter und nur unter Verwendung der angegebenen Hilfsmittel angefertigt habe. Die aus benutzten Quellen entnommenen Stellen wurden als solche kenntlich gemacht.

Magdeburg, den 18.01.2019

Daniel Gerlach

Vorbemerkung und Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als Berater und Projektleiter der SBSK GmbH & Co. KG sowie in Kooperation mit der Hochschule Magdeburg-Stendal. Sie ist das Ergebnis und der Abschluss einer einjährigen Entwicklung zur Migration von SDN-Strukturen in zeitkritische und hochverfügbare Netze. Parallel dazu wurde in diesem Rahmen das kooperative Forschungsprojekt „MONAT - Modellbasierte und bedarfsgerechte Netzwerkkonfiguration für Netzwerke der Automatisierung und Kommunikation“, in dankenswerter Weise gefördert durch den VDI/VDE Innovation + Technik GmbH, bearbeitet.

Angeregt und ermöglicht wurde diese Arbeit durch Herrn Prof. Dr.-Ing. Dieter Schwarzenau und Herrn Dipl.-Ing. Dirk Bartens. Ich danke Ihnen beiden für ihr Engagement und ihr reges wissenschaftliches Interesse an der hier behandelten Thematik. Herrn Dipl.-Inf. Carsten Edelberger und Herrn B.Eng. Heiko Kelling danke ich für ihre stete Diskussions- und Hilfsbereitschaft bei der Erarbeitung der Problemstellung. Gleichzeitig möchte ich mich bei meinen Kollegen und Kolleginnen der SBSK GmbH & Co. KG, sowie der I2KT GmbH & Co. KG für die tolle Zusammenarbeit bedanken. Eine solche Arbeit kann neben der täglichen Kleinarbeit nur entstehen, wenn tatkräftige und kritische Mitarbeiter zur Seite stehen. Nachdem es vollbracht ist, vergisst man die Mühen und Anstrengungen, die hinter einem liegen. Ich hoffe diese Arbeit gibt einen praxisnahen und umfassenden Bezug zu den behandelten Themen.

Weiterhin danke ich Herrn Prof. Dr. Jens Heßmann dafür, dass er mich im Jahr 2017 zurück in die Stadt Magdeburg holte und damit den Grundstein für meinen nun eingeschlagenen Berufs- und Lebensweg legte.
Ein ganz besonderer Dank gebührt meiner Partnerin, Frau M.Sc. Sandra Richter, die mich während dieser Arbeit mit ihrer objektiven und wissenschaftlichen Sichtweise vor Fehlern bewahrte und mir stets den Mut und die Kraft für neue Herausforderungen gab. Vielen Dank für dein Verständnis, die lobenswerte Unterstützung und die Investition deiner wertvollen Zeit. Dankend wende ich mich an meine Familie und meine Freunde für ihre Unterstützung und Motivation.

Magdeburg, im Januar 2019
Daniel Gerlach

Kurzfassung

Eine derzeitige industrielle Zielstellung ist die weitgehende Flexibilisierung von Produktionsprozessen und die Entwicklung cloudbasierter Industriesteuerungen. Die damit verbundene dynamische Verteilung von Daten über Weitverkehrsnetze erfordert völlig neue Denkweisen hinsichtlich der Struktur und der Steuerung dieser Netze. Dynamische Lastverteilungen und automatisierte Administrationsaufgaben stellen dabei die Kernthemen dieser Entwicklung dar. Breitbandige und gesicherte Kommunikationskanäle mit sehr geringen Latenzen dienen nicht nur industriellen Aspekten, sie sind auch Anforderungen bei der Bereitstellung medizinischer Dienste und Anwendungen. Eine derzeitige Herausforderung stellt der hohe Administrationsaufwand dar, welcher mit der hohen Dynamik des Verbindungs-aufbaus und -abbaus einhergeht. Die Kombination aus Software-Defined-Network und Network-Function-Virtualization kann diesen Anforderungen gerecht werden. Mit der Absicht diese Techniken in bestehende Netzwerkstrukturen zu integrieren, entstand im Zuge des Forschungsprojekts MONAT ein umfassendes Migrationskonzept von SDN-Strukturen in zeitkritische und hochverfügbare Netze. Das Ziel ist es, mit Hilfe professioneller SDN-Lösungen eine skalierbare Netzstruktur zu entwickeln, welche die o.g. Voraussetzungen erfüllt. Die Realisierbarkeit des Migrationskonzeptes erforderte zunächst die Entwicklung einer Zielarchitektur auf Basis von SDN. Für die Validierung kritischer Anforderungen und der Sicherstellungen grundlegender Funktionen, wurde im Rahmen eines Proof-of-Concepts eine zusätzliche Test-Struktur des Netzwerks entworfen. Anschließend wurden Handlungsempfehlungen zur schrittweisen Migration der neu entwickelten SDN-Struktur, unter Berücksichtigung bestehender Netzwerkarchitekturen, erarbeitet. Die vollständige Inbetriebnahme des Systems bedingt einen umfassenden Systemtest sowie die Systemabnahme. Hierfür wurden ebenfalls Handlungsempfehlungen aufgestellt, welche die notwendigen Abläufe beinhalten. Für die Überführung in den Regelbetrieb wurden zusätzlich die prinzipiellen Inhalte einer Systemeinweisung für zukünftige Administratoren entwickelt.

Die praktische Umsetzung dieser Netzwerkarchitektur wurde dabei in allen Punkten mit dem theoretischen Modell verglichen und bewertet. Das im Zuge dieser Arbeit entworfene Modell wird nicht nur den stetig zunehmenden Herausforderungen an Telekommunikationsnetzen gerecht, es bildet auch eine Grundlage für zukünftige Forschungsansätze, wie z.B. eines kombinierten policy- und applikationsabhängigen Forwardings.

Abstract

The current industrial aim is the extensive flexibilization of manufacturing processes as well as the development of cloud-based industrial controlling systems. The associated dynamic distribution of data by wide area networks requires completely new approaches in respect to structure and controlling levels of those networks. The distribution of traffic load has to be dynamically and administration tasks should be automated. Broadband and safe communication channels with very low latencies assist not only industrial aspects. They present also requirements to supply medical services and applications. One of the main challenges is the very high effort based on administration, which is a result of high dynamically connection and disconnection setups. The Realization of these requirements can achieved by the combination of software-defined networking and network-function virtualization. A complex migration concept was developed in the context of the research project MONAT which focuses on integration of SDN structures into existing time-critical and highly available networks. The use of professional SDN (Cisco DNA) solutions provides the development of a scalable network structure that supports the defined general requirements.

First of all, a target architecture based on software-defined networking was designed which illustrates the desired migration steps. Moreover an additional test structure as a part of a proof-of-concept of the network was introduced with the intent to gather information about detection of critical aspects and structural failures. Subsequently, recommendations for the step wise migration of the newly developed SDN structure into existing network architectures were prepared. The final implementing of the system demands a fully working system test as well as the decline of the system. For this purpose recommendations were given, which contains of necessary procedures. Finally, general hints for a system introduction into continuous networks for prospective users were established and discribed.

The practical implementation of this newly developed network architecture include all respects of the theoretical model. The presented study comply with all described challenges of telecommunications networks and enables a foundation for future research approaches, such as policy- and application-dependent traffic load forwarding.

Inhaltsverzeichnis

1 Einleitung

Gegenwärtig planen die Industrieunternehmen Deutschlands ihre Produktionsprozesse deutlich flexibler zu gestalten. Die Steuerung komplexer Auftragsabwicklungen und Produktionslinien soll zukünftig als Cloud-Dienst bereitgestellt werden können. Durch cloudbasierte Management- und Maintenance-Funktionen entstehen neue Netzwerkanforderungen. Neben einem hohen Bedarf an Bandbreite wird insbesondere eine geringe Latenz gefordert, z.B. für zeitkritische Industrieanwendungen wie Machine-to-Machine-Kommunikation (M2M), für medizinische Anwendungen und bei der Bereitstellung von Hochverfügbarkeit und Echtzeitfähigkeit der Kommunikationstechnik.

Die SBSK GmbH & Co. KG ist ein IT-Ingenieurunternehmen, dessen Hauptaufgabenfelder die Beratung, die Planung sowie die Installation komplexer und intelligenter Netzwerke sind. Die Erfahrung dieses Unternehmens umfasst u.a. innovative Lösungen aus den Bereichen der Forschung und Medizintechnik. Derzeit fungiert die SBSK als Projektleiter des Forschungsprojekts MONAT.

Im Rahmen dieses Forschungsprojektes soll ein Modell des Software-Defined-Network (SDN) als eine zukunftsweisende Netzwerktechnik erschlossen und auf bestehende zeitkritische und hochverfügbare Infrastrukturen adaptiert werden. Damit verbunden werden Kommunikationssysteme auf Sicherheit und Echtzeitfähigkeit geprüft. Bei ständig wechselnden Anforderungen an Kommunikationsbeziehungen wird eine hohe Flexibilität des Netzes gefordert, woraus ein sehr großer Administrationsaufwand resultiert. Dieser kann durch SDN reduziert werden. Das Ziel des Forschungsprojekts liegt primär in der Optimierung von Weitverkehrsnetzen. Die Ergebnisse sind jedoch auf Campusnetzwerke, z.B. in Hochschul- und Klinikumgebungen, übertragbar.

Der Fokus dieser Arbeit liegt im Erstellen eines Konzepts zur Migration von SDN-Strukturen in ein zeitkritisches, hochverfügbares Datennetzwerk. Es soll eine Handlungsempfehlung entstehen, die es IT-Unternehmen und Ingenieurbüros ermöglicht, eine SDN-Integration im unterbrechungsfreien Netzwerketrieb durchzuführen.

1.1 Status quo

Die heutigen öffentlichen Telekommunikationsnetze beschreibt man am besten als diensteintegrierte, IP-vermittelte und konvergente Breitband-Datennetze. Ein bedeutender Meilenstein für die Telekommunikationsnetze in den letzten Jahren war die Umstellung der Telefonie auf Voice-over-IP (VoIP). Die Funktion des digitalen Telefonnetzes (ISDN) wurde dabei vollständig in das IP-vermittelte Datennetz („Internet-Netz“) integriert. Die Signalisierungs- und Sprachdaten der Telefonie werden seitdem gemeinsam mit dem Internetverkehr über ein gemeinsames Netz geroutet. Seither ist das öffentliche Telekommunikationsnetz durch die Begriffe All-IP-Netz und Next-Generation-Network geprägt.

Laut der ARD/ZDF Online Studie 2017 [1] und der Studie „digital facts 2017-01“ [2] nahm die Zahl der Internetnutzer in Deutschland in den Jahren von 1997 bis 2017 um 58,3 Millionen zu. Davon benutzen 72% das Internet täglich. Einen großen Teil der Nutzung stellen Video- und Audio-On-Demand-Dienste dar, wie z.B. Netflix, Youtube und Spotify. Bereits im Jahr 2011 stand die Nutzung des Internets in 50% der Unternehmen Deutschlands im Kern des Geschäftsmodells [3]. Die Tendenz ist steigend. Dazu kommt ein zunehmender Bedarf an Datenübertragungskapazitäten im Kontext von Industrie 4.0 und dem Internet der Dinge (IoT). Zu diesen genannten Diensten kommen die Anwendungen Web-Surfen und E-Mail hinzu. Die Bereitstellung jedes einzelnen Dienstes setzt unterschiedliche Qualitätsparameter voraus. Mit jedem neu entwickelten Dienst wachsen die Anforderungen an das öffentliche Netz.

1.2 Historie der Telekommunikationsnetze

Das öffentliche Telekommunikationsnetz basiert auf physikalischer Schicht auf unterschiedlichen Techniken (LWL, Kupfer, BK-Netze, Funk). Die verschiedenen Übertragungstechniken weisen sehr unterschiedliche Qualitätsparameter (Latenzen, lastbedingter Paketverlust, Jitter) auf. In der Vergangenheit wurde dennoch eine ausreichende Ende-zu-Ende-Qualität übergreifend über komplexe Netzstrukturen erreicht, indem die Netze grundsätzlich überdimensioniert wurden. Die einzelnen Teilnetze wurden mit einer so hohen Bandbreite konzipiert, sodass der Grenzlastbereich durch die auftretenden Verkehrsströme nicht erreicht werden kann. Verbunden mit dem Anstieg der Verkehrslasten durch die o.g. Dienste (VoIP, Streaming) wurden dann Mechanismen, wie die Bandbreitenreservierung und das Warteschlangenmanagement, für zeitkritische und breitbandige Dienste eingeführt. Für das

heutige Verkehrsaufkommen, bei dem immer mehr Dienste aus der Cloud heraus bezogen werden und es z.B. eine Verlagerung des TV-Konsums weg vom öffentlichen Rundfunk über SAT und Kabel, hin zu IP-TV gibt, reichen auch diese Mechanismen nicht mehr aus. Es bedarf eines komplexen Netzwerkmanagements. Grundlegend gehören dazu Funktionen wie die Erfassung aller Netzwerkgeräte (Inventarisierung), die Überwachung dieser Komponenten (Monitoring) sowie die kontinuierliche Messung der Leistungsfähigkeit im Netzwerk (Performance). Außerdem umfasst ein Netzwerkmanagementsystem Funktionen wie Fehlererkennung, Security-Management und Accounting (Abrechnung verschiedener Dienste). Da heutige Verkehrslastaufkommen ein sehr dynamisches Verhalten aufweisen, ist eine ständige Überwachung dieser genannten Parameter sinnvoll. Das ermöglicht eine bedarfsgerechte Skalierung und Administration des Netzwerks. Dies birgt jedoch einen hohen Aufwand an Administration. Die Betriebsfähigkeit dieser Netze zur Verfügung zu stellen bedingt daher einen hohen Arbeitsaufwand. Veränderungen im Netz können nur träge umgesetzt werden, da sie einen hohen Planungs-, Umsetzungs- und Betriebsaufwand verursachen.

Zukünftig werden diese Netze vor neue Herausforderungen gestellt. Die Bestrebungen großer Industrieunternehmen, komplexe Anlagensteuerungen verschiedener Zuliefererfirmen zentral aus der Cloud heraus zu steuern, werden in Zukunft ebenfalls erhebliche Netzkapazitäten und Flexibilität erfordern. Darüber hinaus, werden sehr granulare Security-, Maintenance- und Monitoring-Funktionen benötigt. Diese Entwicklung stellt die Betreiber vor große Herausforderungen bezüglich ihrer WAN-, LAN- und WLAN-Strukturen. Es entsteht der Bedarf nach der Automatisierung der Netzkonfiguration.

In den folgenden Abschnitten 2.1 und 2.2 wird ein Ausblick auf die Weiterentwicklung der Telekommunikationsnetze, beginnend mit der Trennung von Netzsteuerung und Datentransport (Software-Defined-Network) und später mit der Virtualisierung der Netzfunktionen und Dienste (Network-Function-Virtualization) gegeben.

2 Grundlagen

Die Themen Software-Defined-Network (SDN) und Network-Function-Virtualization (NFV) entstanden in Rechenzentrumsumgebungen. Nachfolgend wird in diesem Abschnitt auf einzelne Entwicklungen eingegangen.

In klassischen Datennetzwerken wurde eine Vielzahl an Netzwerkfunktionen in dedizierten Geräten (Router, Switches, Application-Delivery-Controller) bereitgestellt. Einzelne Funktionen in diesen Geräten wurden wiederum in separaten Kontroll-Logiken (ASIC – Application-Specific-Integrated-Circiut) realisiert.

Die Hauptmerkmale klassischer Netzwerkgeräte und -strukturen sind:

- Nur langsame Entwicklung der ASICs,
- Herstellerabhängige Entwicklungen der ASIC-Funktionen,
- Proprietäre Geräte,
- Individuelle Konfiguration einzelner Geräte,
- Zeitaufwendiges und fehleranfälliges Provisioning, Change Management und De-Provisioning.

Mit der Entstehung von Server-Virtualisierungen und deren großflächige Verbreitung entstand ein Bedarf an flexibleren und effizienteren Netzwerken.

Virtuelle Maschinen (VM) stellen einen Teil dieser Server-Virtualisierungen dar. VMs können in Server-Umgebungen sehr schnell erstellt oder verlagert werden. Geschieht das über einen Layer-3-Bereich hinweg, wird eine aufwändige Konfiguration der Netzwerkkomponenten benötigt. Je nach Art und Hersteller sind die verschiedenen Netzwerkkomponenten in ihrer Funktion sehr eingeschränkt und meist genau für den jeweiligen Einsatz ausgewählt worden. Größere Veränderungen im Netzwerk erfordern dadurch neue Hardware-Anschaffungen und bedingen größere Investitionen. Auch der Betrieb einer Vielzahl an proprietärer Hardware erzeugt vergleichsweise hohe Betriebskosten. Alles in Allem sind klassische Netzwerke sehr statisch und werden nur langsam an etwaige veränderte Anforderungen angepasst. Der Einsatz von SDN und NFV soll die Beschränkungen und Abhängigkeiten aufheben. Virtualisierte Netzwerkanwendungen installiert auf standardisierter Hardware, für die Bereitstellung spezifischer Netzwerkfunktionen, sollten die Lösung dafür sein. Diese Entwicklungen von SDN und NFV in Rechenzentren sollen das Vorbild für die Innovation zukünftiger

Datennetzwerke sein. Innerhalb des Grundkonzepts der NFV werden virtualisierte Netzwerkressourcen *as a Service* betrachtet und genutzt, um Netzwerkfunktionen sowie Netzwerkapplikationen zu integrieren. [4]

Ein weiteres Merkmal klassischer Netzwerke ist die direkte Verbindung zwischen Kontrolllogik und verarbeitender Hardware. Sie besitzen somit eine „verteilte“ Control Plane. Dieses Konzept weist bezüglich der Ausfallsicherheit der Systeme Vorteile auf. Zu den Nachteilen gehört die aufwändige Umkonfiguration der Netzwerkkomponenten bei etwaigen Netzwerk-Struktur-Veränderungen. Für derartige Veränderungen stand bisher kein zentraler Controller zur Verfügung. Zur Beschleunigung und Vereinfachung dieses Vorgangs wurden verschiedene Management-Tools von namhaften Herstellern entwickelt. Diese Management-Tools beinhalten umfassende Konfigurationsmöglichkeiten. Die Kompatibilität zu Geräten verschiedener Hersteller ist jedoch auch hier begrenzt, da die Verwendung unterschiedlicher Protokolle und Schnittstellen die Entwicklung solcher Tools stets vor Hindernisse stellt. Die Weiterentwicklung der Netzwerktechniken ist aufgrund der geringen Flexibilität dieser Netzwerke sehr verlangsamt. Neue Technologien können nur mit erheblichem Aufwand in bestehenden Netzen etabliert werden. Die Umstrukturierung hin zu einem SDN behebt diese genannten Probleme und bietet Möglichkeiten zur Weiterentwicklung. [5]

2.1 Software Defined Network

Die heutigen Telekommunikationsnetze werden vor neue Herausforderungen gestellt. Kommunikationsverbindungen werden dynamisch instanziiert und durch die NFV werden neue Netzfunktionen integriert. Abhängig von Verkehrsflüssen und Netzsituationen werden die Datenpakete flexibel an die entsprechenden NFV-Strukturen weitergeleitet. Netzanwendungen können dynamisch verlagert und neu skaliert werden. SDN gilt als Schlüsseltechnik für diese Art von Datenfluss-Steuerung. Die NFV trennt die Software von der Hardware der Netzdienste. SDN entkoppelt Signalisierungsdaten und Nutzdaten in den Netzknoten durch Integration eines zentralen SDN-Controllers (Control-Plane) und mehreren dezentralen SDN-Switches (Data-Plane). Standardisiert wurde SDN von der Open Network Foundation, wie auch das hier später erwähnte Open-Flow-Protokoll. SDN kann auch mit Hilfe anderer Steuerungsprotokolle, wie ForCES (IETF) und OpFlex (Cisco), umgesetzt werden. [6]

Veränderungen in Ethernet- und IP-Netzen forderten ein neues Switching- und Routing-Konzept. Die klassischen Netzwerke sind für Client-Server-Applikationen optimiert. Durch

Kommunikationsbeziehungen zwischen Servern, Datenbanken, der Vielzahl von mobilen Endgeräten und im Kontext des Cloud Computing entstehen neue komplexe und parallel verlaufende Verkehrsmuster. Diesen neuen Verkehrsanforderungen können klassische Netzwerke nicht mehr gerecht werden. Es entsteht ein großer Bedarf an Flexibilität bedingt durch Sicherheitsanforderungen, QoS, der Konvergenz von Sprache, Video und Daten, sodass der Einsatz neuer bzw. geänderter Protokolle unabdingbar wird. Für den Betrieb von NFV-Strukturen und Cloud-Computing fehlt es den klassischen Netzen an Skalierbarkeit. Hinzu kommen die Kompatibilitäts- und Interoperabilitätsprobleme der Steuer-Software verschiedener Switch- und Router-Hersteller, welche die Netzbetreiber bei Netzkopplungen vor Herausforderungen stellt. SDN begegnet diesen Problemen mit der Nutzung des offenen Protokolls Open-Flow zur Steuerung der SDN-Switches. Switches und Router aus vorhandenen Strukturen werden durch SDN-Controller und SDN-Switches ersetzt. Die Steuerung der Datenflüsse übernimmt allein der SDN-Controller. Die Forwarding-Informationen werden dann mittels Open-Flow vom SDN-Controller an die SDN-Switches weitergeleitet. Die SDN-Switches müssen demnach keine Vielzahl an Protokollen verstehen. Somit tritt die sonst sehr herstellerabhängige Kompatibilität der Hardware in den Hintergrund. Das macht den gesamten Prozess von der Netzplanung über die Integration und Inbetriebnahme, bis hin zum Betrieb und der Instandhaltung, deutlich einfacher und senkt dazu die Investitionskosten für die Hardware. Der Vorteil von Open-Flow liegt in dem offenen Standard. Die besonders leichte Zugänglichkeit des Protokolls vereinfacht die Entwicklung für die Hersteller erheblich. Aus logischer Betrachtungsweise kann ein durch einen SDN-Controller gesteuertes Netz mit SDN-Switches als ein einzelner Switch bzw. Router betrachtet werden, was als zellulare Sichtweise bezeichnet wird. Ein weiterer Vorteil der SDN-Struktur, ist die Programmierbarkeit des SDN-Controllers durch Application-Programming-Interfaces (APIs).

Somit können schnell und einfach z.B. Änderungen am Laufzeitverhalten vorgenommen werden oder verschiedene Netzdienste integriert werden. Administratoren können eigene SDN-Applikationen integrieren und somit das Transportnetz flexibel und dynamisch verwalten. Die Konfiguration, das Management, Security-Anforderungen und die Optimierung beim Einsatz von Netzressourcen werden dadurch deutlich vereinfacht. Typische SDN-Applikationen beinhalten Funktionen wie Switching, Routing, Multicast, QoS, Bandbreitenmanagement, Traffic Engineering und Zugriffssteuerung. Weiterhin stehen SDN-Applikationen zur Steuerung bzw. Senkung des Energieverbrauchs innerhalb von software-definierten Netzwerken im Fokus der Entwicklung [7]. Außerdem können Provisioning- und Orchestrierungs-Systeme über APIs integriert werden. Die neue SDN-Architekturspezifikation

beschreibt keine Infrastructure-, Control- und Application-Layer mehr, sondern Application-Plane, Control-Plane und Data-Plane [8]. Die APIs werden nun als Application-Controller Plane Interfaces (A-CPIs) und die Controller Plane Interfaces (CPIs) als Data-Controller Plane Interface (D-CPIs) angegeben. Für jede Plane wird eine Schnittstelle zum Managementsystem (Operations Support System - OSS) beschrieben. [6]

Die Schnittstelle zwischen Data-Plane und OSS dient der Übertragung der initialen Konfiguration der Netzwerkelemente (Zuordnung von SDN-Switches zu SDN-Controller). Das OSS konfiguriert die Policies für die Control-Plane, für den Funktionsumfang der SDN-Applikationen und für das Leistungs-Monitoring. In der Application-Plane werden durch das OSS Konfigurationen für Verträge und Service-Level-Aggreements (SLA) durchgeführt. Auf diesen drei Planes werden Security-Einstellungen mit Hilfe des OSS integriert. [8]

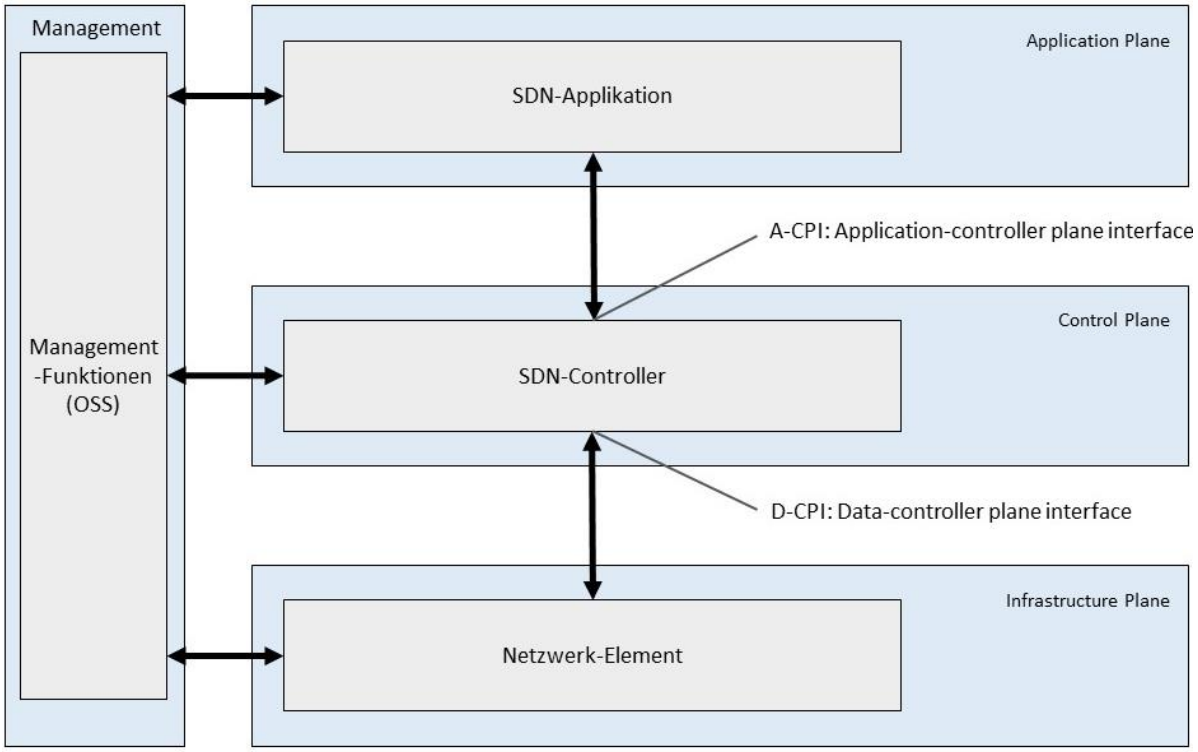

Abbildung 1: SDN Architektur mit Management (modifiziert nach [8])

Die Verwendung von SDN bietet Netzbetreibern zahlreiche Vorteile, welche z.B. für Carriernetzwerke, Campusnetzwerke oder Ähnliches genutzt werden können. Dazu gehören:

- *„zentralisierte, zeitgleiche und konsistente Steuerung aller Switches*
- *Einsatz von Switches verschiedenster Hersteller,*
- *Zentrale Gesamtsicht des Netzes*
- *Einsatz von Orchestrierungs- und Management-Tools für automatisierte und schnelle Bereitstellung, Konfiguration und System-Updates im gesamten Netz,*
- *Programmierung des Netzes in Echtzeit,*
- *Verbesserte Netzzuverlässigkeit und Sicherheit,*
- *Feingranulare Behandlung unterschiedlicher Datenflüsse*
- *Einfachere Adaption des Netzes an die Nutzeranforderungen“.* [6]

Die folgenden Erklärungen werden mit Hilfe von Abbildung 2 vorgenommen. Es wird davon ausgegangen, dass Open-Flow als Steuerungsprotokoll verwendet wird. Die Forwarding-Regeln werden in einer sog. Flow-Table abgebildet (*Tabelle 1*). Zusammengehörige Datenpakete, d.h. Pakete mit gleicher Quell- und Zieladresse, werden zu einem Flow zusammengefasst. Das Forwarding im SDN hat grundsätzlich folgenden Ablauf [6]:

1. Der SDN-Controller generiert Flow-Table-Einträge für den SDN-Switch.
2. Beim Empfang neuer Datenpakete prüft der SDN-Switch die Übereinstimmung mit vorhandenen Flow-Table-Einträgen.
3. Bei einer Übereinstimmung wird das konfigurierte Forwarding ausgeführt.
4. Wenn keine Übereinstimmung gefunden wurde, leitet der SDN-Switch das Paket zum SDN-Controller weiter.
5. Der SDN-Controller bearbeitet das Paket und versieht den SDN-Switch mit einem neuen Flow-Table-Eintrag.
6. Der „unbekannte“ Flow kann nun lokal im SDN-Switch verarbeitet werden.
7. Pauschal können auch sog. „wild cards“ gesetzt werden. Diese stellen Platzhalter für verschiedene Dienste dar.

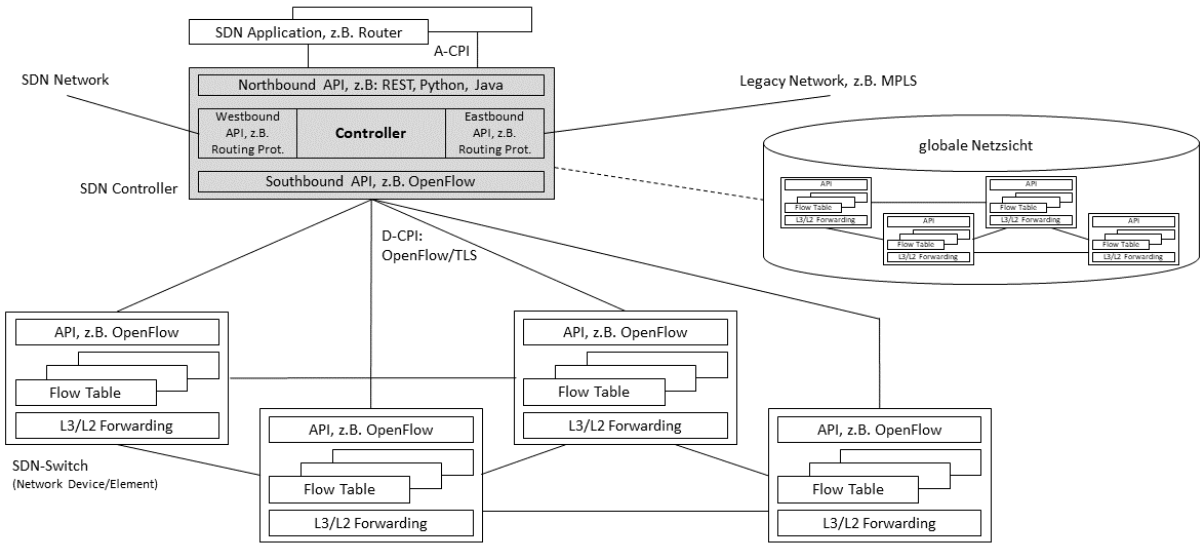

Abbildung 2: Struktur eines SDN (modifiziert nach [6])

Die *Tabelle 1* zeigt die Struktur einer Flow-Table. Wie o.g. kennzeichnet ein Flow mehrere Datenpakete mit gleichen Eigenschaften. Eine vollständige Übereinstimmung mit den Einträgen einer Flow-Table-Zeile ist dabei nicht nötig. Kennzeichnende Eigenschaften wie z.B. Quell- und Ziel-Adresse (IP Src, IP Dst) sind für eine Flow-Generierung ausreichend. Eine Flow-Table besteht grundlegend aus flow-spezifischen Zeilen (Header Fields), daraus folgenden Aktionen (actions) und Zählern (counters) für Statistiken. Eine Zeile besteht aus zwölf Header-Feldern. Die Ausführung der in *Tabelle 1* definierten Aktionen, bedingt die Implementierung der Mechanismen Forwarding und Drop (Verwerfen) im SDN-Switch. Optionale Funktionen sind Enqueue (Eintragen in eine einem Port vorangestellte Queue für z.B. QoS Support) und Modify-Field (Header-Feld modifizieren). Für das Forwarding gibt es zugleich mehrere Möglichkeiten: Forwarding an einen definierten physikalischen Port (Port 1), an alle außer den Empfangsport (All), an einen SDN-Controller (Controller) oder an den SDN-Switch selbst (local). Felder in denen beliebige Werte zugelassen sind, sind gemäß der *Tabelle 1* mit einem • gekennzeichnet. [6]

Tabelle 1: Flow Table eines SDN-Switches (modifiziert nach [6])

Header Fields												**Actions**	**Counters**
Ingress Port	Eth. Src	Eth. Dst	Eth. Type	VLAN ID	VLAN Prio	IP Src	IP Dst	IP Protocol	IP ToS Bits	TCP/UDP Src	TCP/UDP Dst	• Forward • Drop • EnQueue (An Queue eines Ports) • Modify-Fields (Header)	• Per Table • Per Flow • Per Port • Per Queue
•	•	10:20:	•	•	•	•	•	•	•	•	•	• Port 1	• 250
•	•	•	•	•	•	•	5.6.7.8	•	•	•	•	• Port 2	• 300
•	•	•	•	•	•	•	•	TCP	•	•	25	• Drop	• 892
•	•	•	•	•	•	•	192.•	•	•	•	•	• Local	• 120
•	•	•	•	•	•	•	•	•	•	•	•	• Controller	• 11

Das D-CPI (Southbound-API) stellt die Schnittstelle für die Kommunikation zwischen SDN-Controller und SDN-Switch dar. Diese Schnittstelle wird auch als Secure-Channel bezeichnet. Die Kommunikation basiert auf Open-Flow-Nachrichten, die mit TLS verschlüsselt und mittels TCP verbindungsorientiert übertragen werden. Diese Nachrichten können verschiedene Funktionen beinhalten [6]:

- Konfiguration des Switches
- Abfragen der Funktionen des Switches
- Verwaltung der Flow-Tables
- Übertragung der Pakete an den SDN-Controller, für die es keinen Flow-Table-Eintrag gibt
- Informationen über Statusmeldungen oder Fehler
- Auf- und Abbau von Open-Flow-Verbindungen.
- Überprüfung von Verfügbarkeiten

Es existieren mehrere Spezifikationen für das D-CPI (Southbound-API), hingegen keine Spezifikation für das A-CPI (Northbound-API). Es besteht die Möglichkeit Routing-Informationen mit anderen Netzen über das Westbound- und Eastbound-API auszutauschen. Dies geschieht über klassische Routing-Protokolle, wie z.B. über das Boarder-Gateway-Protocol (BGP). Wenn eine Verbindung zu einem anderen SDN-Netzwerk besteht, wird die Schnittstelle Westbound-API genannt. Ist es eine Verbindung zu einem klassischen Netz auf Grundlage von MPLS, wird die Schnittstelle als Eastbound-API bezeichnet.

Vorteilhafte Anwendungsfälle von SDN sind z.B. [6]:

- Cloud-Orchestrierung: Integration eines gemeinsamen Managements für Cloud-Server und zugehörigen Netzwerkstrukturen. Mit Hilfe von VMs wird eine automatisierte Umkonfiguration des Transportnetzes möglich. Bei Link-Überlastung können ganze VMs an einen anderen Ort im Netzwerk „umziehen“ (z.B.: Rechenzentren).
- Load-Balancing: SDN-Switches können per Open-Flow-Nachricht vom SDN-Controller als Load-Balancer konfiguriert werden, sodass bei hoher Netzlast Dienste an Server gleicher Funktionen verteilt werden können. Zusätzliche Load-Balancer werden somit nicht mehr benötigt.
- Routing-Anpassung: Die Zentralisierung der Netzfunktionen machen Routing-Anpassungen wie die Auswahl der Pfade, Verkehrsoptimierung, Redundanzen, versch. Protokollversionen (IPv4, IPv6) bzw. Routingprotokolle deutlich einfacher als bei klassischen monolithischen Routern.
- Verkehrs-Monitoring und -Messungen: Die zentrale Steuerung des Netzes erfordert eine standardmäßige Erfassung von Zustandsinformationen über das Netz. Diese können dann zu Messauswertungen zur Verfügung gestellt werden. SDN bietet außerdem Monitoring-Funktionen für Paket-Flows, sodass z.B. zu hohe Latenzen ermittelt werden können.
- Netzmanagement: Die zentrale Steuerung des SDN ersetzt aufwändige, manuelle Konfigurationen der jeweiligen Netzknoten (z.B. Aktualisierung der Access-Listen), durch eine automatisierte und optimierte adaptive Einstellung.
- Applikationsspezifische Netzoptimierung: Das Northbound-API bietet die Möglichkeit, Informationen über Eigenschaften und Zustand von Applikationen an das Transportnetz zu übermitteln und somit gezielte Forwarding-Entscheidungen und Ressourceneinsatz zu steuern.
- Testnetze für Forschung: Teststrukturen mit z.B. neuen Software- oder Protokollversionen können simpel realisiert werden.
- Mehrere virtuelle Netze können parallel betrieben und SDN-Controller für exklusive Anwendungen bereitgestellt werden. Dies kann auf Basis gleicher Hardware geschehen. Man bezeichnet diese Anwendungsfälle dann als Network-Slices.

2.2 Network Function Virtualization

Die heutigen Netzfunktionen und -dienste werden bereits als Software-Lösung realisiert. Diese Software wird jedoch auf proprietärer Hardware mit jeweils proprietären Betriebssystemen betrieben. Oftmals werden einzelne Dienste als Zusammenspiel mehrerer Network-Functions (NF) erbracht. Dazu werden die einzelnen NFs mit Hilfe einer zentralen Logik zu einem Gesamtdienst vereint. Diese Funktion wird als Orchestrierung bezeichnet. Dies gilt als gängige Praxis für die Implementierung von Netzelementen und -diensten in Kommunikationsnetzen. Die Nachteile dieses Konzepts mit proprietärer Hardware sind die relativ unflexible Netzarchitektur mit weitgehend festgelegten Funktionen und die hohen Anschaffungskosten. Das Konzept NFV begegnet diesen Nachteilen. Entwickelt und standardisiert, wurde es von dem Europäischen Institut für Telekommunikationsnormen (ETSI). Es geht dabei darum, Netzfunktionen komplett in Software zu realisieren und somit die Nutzung von Standard-Hardware zu ermöglichen. Die Nutzung virtueller Rechner (Virtual Maschine, VM) und der simultane Betrieb auf Standard-Hardware als bewährte IT-Virtualisierungstechniken, kann somit problemlos weitergeführt werden. [6]

Die Industry Specification Group for NFV (ISG NFV), als Bestandteil des ETSI, hat NFV im Jahre 2012 wie folgt definiert:

„*Network Functions Virtualization aims to transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises, ... It involves the implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment."* [9]

Die Zahl der VMs, auf denen die Software-Instanzen der NFs laufen, kann bei Bedarf erhöht sowie auch erniedrigt werden. Das ermöglicht eine bedarfsgerechte Skalierbarkeit des Gesamtsystems.

Für Netzbetreiber bietet der Einsatz von NFV zahlreiche Vorteile [6]: „…

- *Geringere Gerätekosten,*
- *Schnellere Einführung neuer Netzeigenschaften und Leistungsmerkmale, da nur noch SW, nicht mehr HW-basiert,*
- *Einsatz der selben HW-Infrastruktur für Produktions-, Test- und Referenzumgebung,*
- *Hohe Skalierbarkeit,*
- *Marktöffnung für reine SW-Hersteller,*
- *Möglichkeit, in nahezu Echtzeit die Netzkonfiguration an den aktuellen Verkehr und seine Verteilung im Netz anzupassen,*
- *Nutzung der selben HW durch mehrere Netzbetreiber,*
- *Niedrigere Planungs-, Bereitstellungs- und Betriebskosten durch homogene HW-Plattform,*
- *Automatisierung bei Installation und Betrieb durch Anwendung von IT-Orchestrierungsmechanismen und Wiederverwendung von VMs*
- *Vereinfachung des SW-Upgrades,*
- *Synergien zwischen Netzbetrieb und IT*.“

In der Vergangenheit standen hier die o.g. Vorteile, wie Offenheit der Dienste, Skalierbarkeit und Reduzierung der Investitions- und Betriebskosten, bereits im Kern der Entwicklung von Next-Generation-Networks (NGN) [10]. Die Standardisierungsarbeiten des ETSI laufen auch in der Gegenwart weiter. Im Fokus der Entwicklung einer Virtualized-Network-Function (VNF) steht, identische Funktionen wie die Physical-Network-Function (PNF), also der klassische Softwarebetrieb auf proprietärer Hardware, zu erbringen. Entgegengesetzt zum eigentlichen Ziel der NFV, also der Trennung von Software und Hardware, wird sich im Regelfall eine Kombination von VNFs und PNFs ergeben. Abstrahiert betrachtet, kann eine NF sowohl ein Netzelement mit einer bestimmten Funktion (z.B. DNS), als auch ein Subnetz mit Switches und Routern für den Nachrichtentransport darstellen. [6]

2.3 Paradigmenwechsel

Die in den Abschnitten 2.1 und 2.2 beschriebenen Entwicklungen des Netzes und der sich damit verändernde Blick auf die Verkehrslastverteilung und die Administration, kommen einem Paradigmenwechsel gleich. Die vermittlungs- und transporttechnischen Verbindungen in zeit- und businesskritischen Netzen werden häufig mit verschiedenen Routingverfahren bereitgestellt, so auch in dem im weiteren Verlauf dieser Arbeit betrachteten Netz.

Die Verkehrslenkung (engl. routing) kann abhängig von Kriterien, wie der kürzesten Strecke und Ansätzen zur Verkehrslastverteilung, sein. Routingverfahren können grundlegend in zwei verschiedene Arten klassifiziert werden, dem statischen und dem adaptiven Routing. Für die Konfiguration eines statischen Routings werden Schätzungen und Erfahrungswerte der zu übertragenden Daten zugrunde gelegt. Treten Veränderungen dieser Verkehrslasten auf, erfordert dies auch eine erneute Konfiguration der Systeme. Beim adaptiven Routing hingegen, kann das System auf sich verändernde Verkehrslasten bzw. Auslastungen einzelner Routen reagieren und eine veränderte Verkehrslenkung initiieren. Klassische Routingprotokolle sind z.B. das BGP, das Intermediate-System-to-Intermediate-System-Protocol (ISIS) und Open-Shortest-Path-First (OSPF). Die Protokolle können für statische sowie auch für adaptive Routing-Algorithmen eingesetzt werden.

Mit der Verlagerung und Zentralisierung der „Netzwerk-Intelligenz“, der Separierung von Control- und Data-Plane, erlebt das Netzwerkmanagement eine neue Denkweise. Durch SDN und NFV werden nun Funktionen, wie z.B. Analyse der Kriterien für die Verkehrslast-Aggregation, Applikationserkennung oder Administration einzelner Netzelemente, zentral von einer Schnittstelle aus bereitgestellt und mit Hilfe des SDN-Controllers automatisch an alle betroffenen Netzelemente weitergeleitet. Das QoS-Verhalten wird nicht mehr aus dem Verteilungsnetz bzw. Zugangsnetz heraus festgelegt, sondern aus der darüber liegenden Kontroll-Schicht (Control-Plane) heraus für das Zugangsnetz dynamisch festgelegt.

Wie nach *Trick und Weber im Jahr 2015* beschrieben, kann auf den SDN-Switches ein L2- sowie auch ein L3-Forwarding stattfinden. Wenn man von einem L3-Forwarding spricht, ist die Verwendung von klassischen Routing-Protokollen gemeint, welche dann jedoch reine Weiterleitungsfunktionen annehmen.

Eine Zentralisierung der „Netzwerk-Intelligenz“ (Control-Plane, SDN-Controller) bedeutet in jedem Fall eine größere Verwundbarkeit des Gesamtsystems durch Ausfälle, Missbrauche und

Sabotage. Je größer der durch die Control-Plane verwaltete Netzwerkbereich (SDN-Switches) ist, desto größer ist auch das Verwundbarkeitsrisiko. Verbunden mit einer größeren Verwundbarkeit sind auch eine höheres Ausfallrisiko des Gesamtsystems und hohe Ausfallkosten. Die Etablierung von Netzwerkanalyse- und Überwachungsmechanismen wird empfohlen, somit kann dem Verwundbarkeitsrisiko entgegen gewirkt werden. Das Verwundbarkeitsrisiko gilt gleichermaßen für Angriffe von „Außen“, wie auch für Updates oder Patches. Aus diesem Grund sollten diese Strukturen in jedem Fall redundant vorgehalten werden.

2.4 Weitere Techniken des Netzwerkmanagements

2.4.1 Locator / ID Separation Protocol

Das Locator/Identifier-Separation-Protocol (LISP) ist ein Protokoll der Vermittlungsschicht des OSI-Schichtenmodells (Layer 3 / network layer). Ziel der Entwicklung dieses Protokolls war es, Informationen über die Lokation der Hardware sowie die Identität des Clients miteinander zu verknüpfen, dem IP-Header beizufügen und für das Routing auszuwerten. Daraus entstanden der Endpoint-Identifier (EID) und der Routing-Locator (RLOC). Der EID definiert die Identität des Clients und der RLOC definiert den Ort im Netzwerk, an der der Client angeschlossen ist. Beide Werte haben das Format einer IP-Adresse und werden in fest definierten Feldern des IP-Headers eingefügt. Es besteht ein festes Header-Format für IPv4 sowie auch für IPv6.

Der Hintergrund dieser Entwicklung ist das stetige Wachsen des Internet- und Datenverkehrs und die Zunahme in der Anzahl der Endgeräte. Dies führte in der Vergangenheit zu Skalierungsproblemen aufgrund hoher Verkehrsaufkommen. Hohe Investitions- und Betriebskosten waren ein weiterer negativer Effekt dieser Entwicklung. LISP wirkt diesen Faktoren entgegen. Es ermöglicht außerdem Leistungsmerkmale wie Multihoming, also eine Any-to-Any-WAN-Konnektivität. Die erforderliche Komplexität des Netzwerkbetriebs, welche durch die Mobilität von VMs und mobiler Endgeräte erforderlich ist, wird durch LISP deutlich reduziert [11].

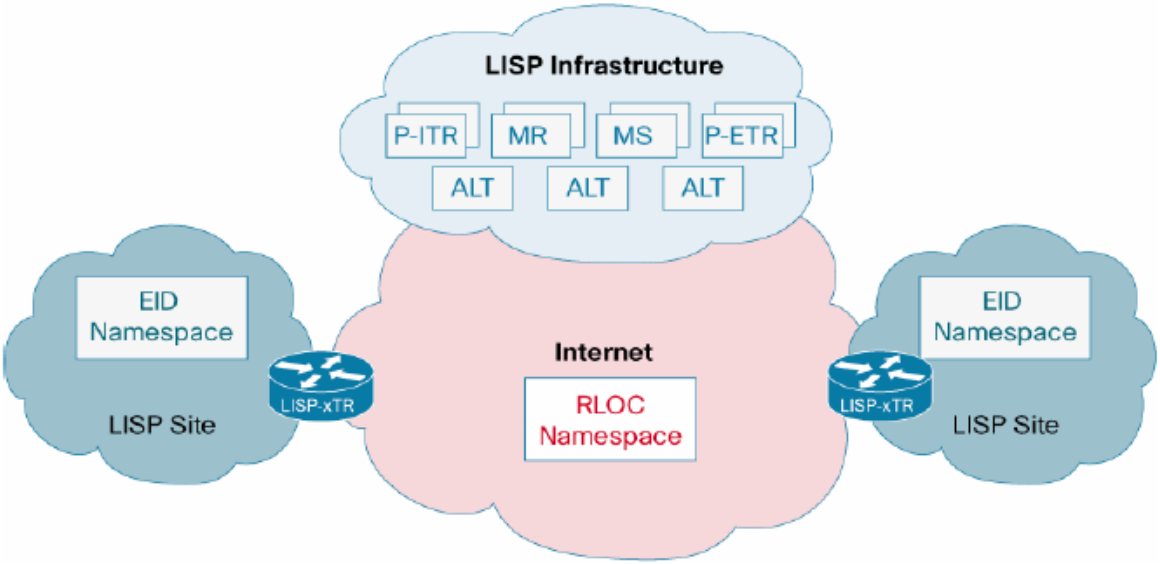

Abbildung 3: LISP Deployment Environment [12]

Die Abbildung 3 zeigt die einzelnen Funktionsbereiche von EID und RLOC. Die abgebildeten Access-Bereiche entsprechen denen, die heute in Netzwerken zu finden sind. Der einzige Unterschied besteht darin, dass die IP-Adressen (EIDs), welche innerhalb der LISP-Sites (Access-Bereiche) benutzt werden, nicht im RLOC-Namespace (äquivalent zu Internet u. Core-Netzwerk) verwendet werden. Die dargestellten Edge-Router (LISP xTR) stellen im Kontext von LISP, entweder Ingress-Tunnel-Router (ITR) oder Egress-Tunnel-Router (ETR) dar. ITRs sind Edge-Router, die Pakete aus dem LISP-Netzwerkbereich empfangen. Anschließend kapseln sie die Pakete für das Routing durch den RLOC-Netzwerkbereich in einen anderen LISP-Netzwerkbereich. ITRs fügen den Paketen EID und RLOC hinzu. ETRs sind ebenfalls Edge-Router. Sie empfangen Pakete aus dem RLOC-Netzwerkbereich, entkapseln diese und leiten sie anhand des hinzugefügten EIDs an das Ziel-Device weiter. Die in der Abbildung 3 dargestellten Edge-Router (xTR) funktionieren bidirektional und können jeweils beide Funktionen (ITR und ETR) im Netzwerk annehmen. Die Bereitstellung einer Interoperabilität zwischen xTRs und ein damit verbundenes Tunneling über einen Non-LISP-Netzwerkbereich (Internet, Core-Netzwerk), erfordert zusätzliche LISP-Komponenten. Diese zusätzlichen LISP-Komponenten sind ebenfalls in der Abbildung 3 dargestellt und funktionieren als Map-Server (MS), Map-Resolver (MR), Proxy-Ingress-Tunnel-Router (PITR) und Proxy-Egress-Tunnel-Router (PETR).

Diese LISP-Komponenten werden nun nachfolgend kurz erklärt:

- **MS:** Der Map-Server (MS) stellt die LISP-site-Policy bereit. Bei ihm registrieren sich die ETRs. Die Policy umfasst EID-Präfixe und Authorisierungsschlüssel. Diese Parameter müssen auch in der Konfiguration des ETRs vorhanden sein. ETRs senden im Zuge der Registrierung register-control-packets zum MS. Außerdem stellt der MS die Schnittstelle zu den Alternative-Topology-Devices (ALT) bereit und konfiguriert die EID-Präfixe auf den ALTs. Der MS empfängt auch map-request-control-packets von den ALTs, welche dann mit hinzugefügtem LISP-Header an den jeweiligen ETR weitergeleitet werden.
- **MR:** Der Map-Resolver (MR) empfängt map-requests und leitet sie, je nach Konfiguration, über eine Service-Schnittstelle zu den entsprechenden ALTs weiter. Außerdem senden sie, im Falle von Anfragen, welche nicht zum LISP-Bereich gehören, negative Map-requests.
- **ALT:** Ein Alternative-Topology-Device (ALT) stellt eine skalierbare Präfix-EID-Aggregation für Verbindungen in Nicht-LISP-Bereiche bereit. Da es möglich ist, Daten aus einem LISP-Bereich über ein Generic-Routing-Encapsulation(GRE)-Tunneling über BGP zu übertragen, können diese Geräte mit Hilfe einfacher Router-Hardware, welche BGP und GRE unterstützen, integriert werden.
- **PITR:** Proxy-ITRs (PITRs) stellen die Konnektivität zwischen LISP- und Nicht-LISP-Bereiche her. PITRs stellen Aggregations-Präfixe für den LISP EID-Namespace bereit. Sie empfangen Pakete aus Nicht-LISP-Bereichen, fügen entsprechende Header-Parameter hinzu und leiten sie dann an die ITRs des jeweiligen LISP-Netzwerkbereichs weiter. Mit Hilfe dieser Geräte können Leistungsmerkmale des Traffic-Engineerings auch für Nicht-LISP-Verkehrs integriert werden.
- **PETR:** Proxy-ETRs (PETRs) stellen eine Verbindung zwischen IPv6-LISP-Bereiche ohne IPv6-RLOC-Konnektivität und LISP-Bereiche her, welche ausschließlich über eine RLOC-Konnektivität verfügen. Für gewöhnlich stellen PETRs auch Funktionen von PITRs bereit und umgekehrt. Die Geräte arbeiten also in den meisten Fällen bidirektional. In diesem Fall wird die Bezeichnung PxTR verwendet.

Die vormals beschriebenen LISP-Komponenten werden häufig gemeinsam als Software-Komponente auf einem LISP-Control-Plane-Node integriert und für das Netzwerk bereitgestellt. [12]

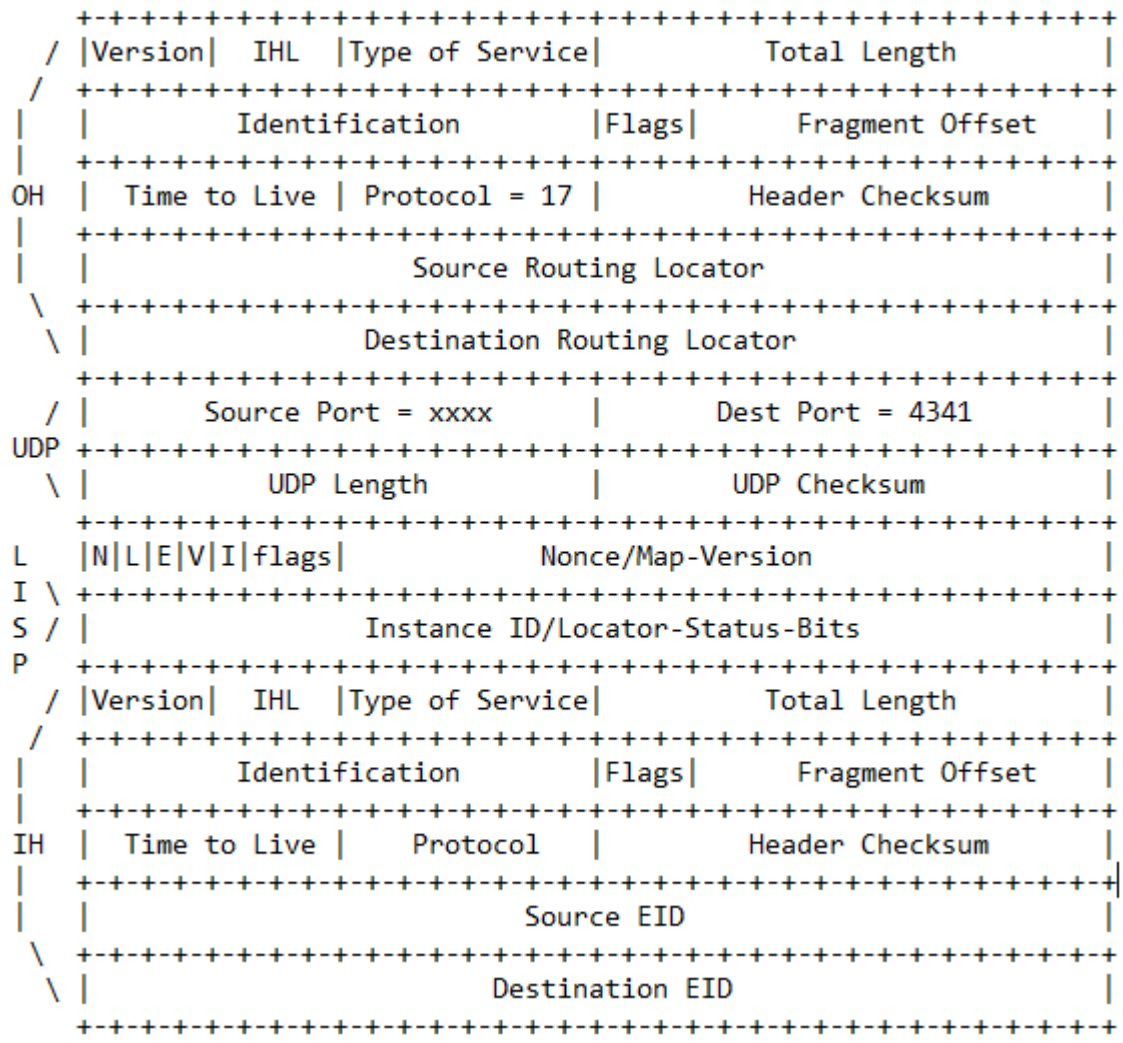

Abbildung 4: IPv4 in IPv4 Header Format [13]

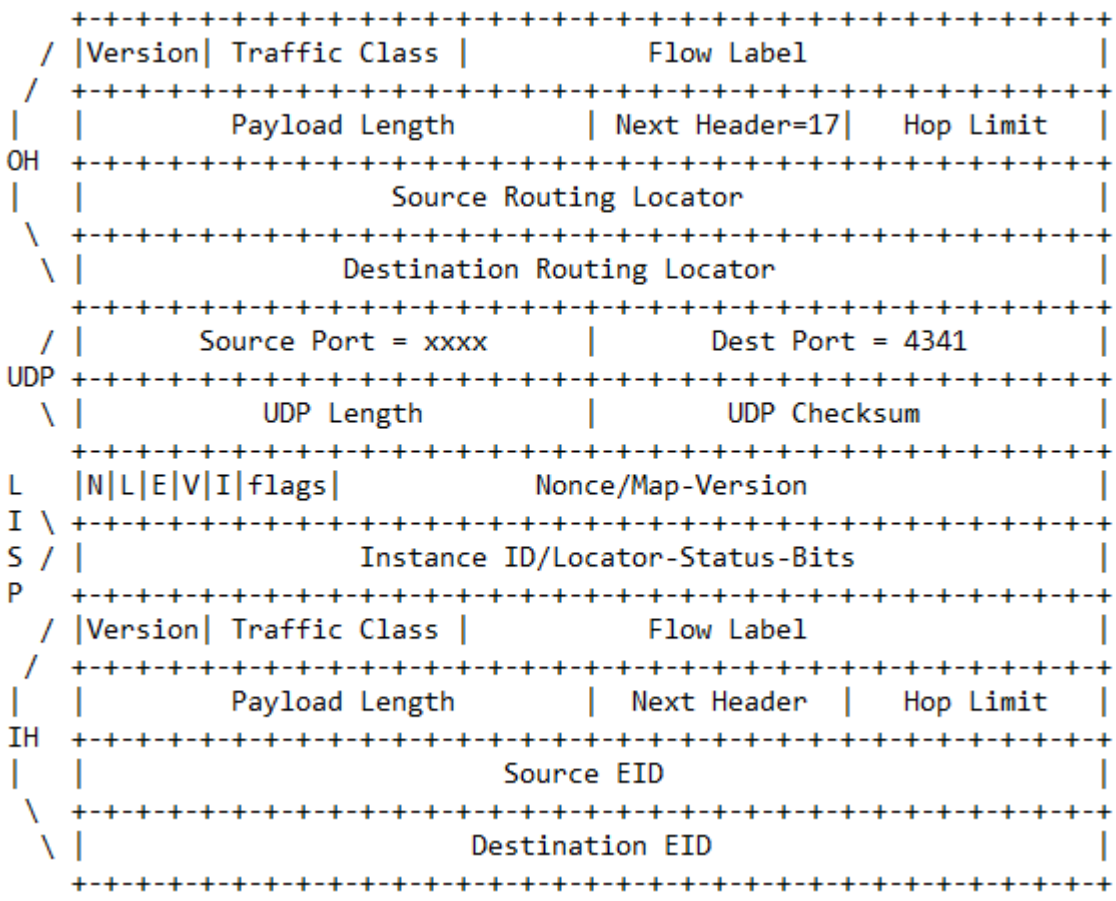

Abbildung 5: IPv6 in IPv6 Header Format (modifiziert nach [13])

Die Abbildungen 4 und 5 zeigen die LISP-Header-Formate für IPv4 und IPv6. Beide Formate verfolgen die identischen Funktionen für die jeweilige IP-Version, weshalb sie an dieser Stelle auch gemeinsam erläutert werden.

Ein LISP-gekapseltes Datenpaket besteht aus mehreren Teilen. Zunächst beinhaltet es einen IP-Header mit RLOC-Informationen über Quell- und Ziel-Adressfeldern. Darauf folgt ein UDP-Header, in dem der Ziel-Port 4341 und der Source-Port, welcher einen Hash beinhaltet, der aus Quell-, Ziel-Adressen und Port-Informationen aus dem ursprünglichen IP-Header generiert worden ist. Diese Informationen werden laut RFC6830 [13] als Outer-Header (OH) bezeichnet. Daraufhin folgt das eigentliche LISP-Datenpaket. Dieses wird vom ITR erstellt, wenn er ein Datenpaket empfängt, welches an eine LISP EID adressiert wurde. Dieses LISP-Datenpaket wird dann anhand der Destination-EID an den entsprechenden ETR gesendet. [11]

Für weitere Recherchen zum Thema LISP werden die folgenden Quellen empfohlen:

- RFC 6831 - The Locator/ID Separation Protocol (LISP) for Multicast Environments [14]
- RFC 6832 - Interworking between Locator/ID Separation Protocol (LISP) and Non-LISP Sites [15]
- RFC 6833 - Locator/ID Separation Protocol (LISP) Map-Server Interface [16]
- RFC 6834 - Locator/ID Separation Protocol (LISP) Map-Versioning [17]
- RFC 6835 - The Locator/ID Separation Protocol Internet Groper (LIG) [18]
- RFC 6836 - Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT) [19]

Das Ziel der Benutzung von EIDs und RLOCs, welches aus den vormaligen Erklärungen hervorgeht, ist die Durchführung eines Mappings zwischen beiden Bereichen. Ein LISP-Endgerät (A1), welches eine Kommunikationsverbindung zu einem anderen LISP-Endgerät (B1) aufbaut, erstellt ein Paket mit der EID von A1 als Quell-IP-Adresse und der EID von B1 als Ziel-IP-Adresse. Am Übergang in das Internet (RLOC-Namespace) ordnet der ITR dem Paket anhand seiner Ziel-EID eine Ziel-RLOC-IP-Adresse zu und kaspselt das ursprüngliche Paket mit einem zusätzlichen RLOC-Header, welcher die Quell-RLOC-IP-Adresse des ITR und die Ziel-RLOC-IP-Adresse des ETR enthält. Der Ziel-ETR stellt dann die Verbindung zum Ziel-EID her. LISP gibt an, wie die Zuordnungen zwischen EIDs und RLOCs definiert, ausgetauscht und verwendet werden. [11]

2.4.2 Virtual extensible LAN

Die Netzwerkvirtualisierungstechnik „Virtual extensible LAN“ (VxLAN) ist eine Methode zur Abbildung virtueller Layer-2-Strukturen in Layer-3-Technologien. Eingesetzt wird diese Technik in virtualisierten Rechenzentren, Cloud-Computing-Umgebungen und im SDN. [20]

Die grundlegenden Vorteile von VxLAN werden nun nachfolgend erläutert.

1. Es besteht die Möglichkeit, einzelne virtuelle Netzwerkbereiche voneinander zu isolieren und somit flexibel über den gesamten physikalischen Netzwerkbereich zu verteilen. Klassische Layer-2-Frames werden in Layer-3-Pakete gekapselt, mit einer VxLAN-ID versehen und über Layer-2-Tunneling-Verbindugen durch das Netzwerk geroutet.
2. VxLAN bietet eine höhere Skalierbarkeit in der Adressierung von Layer-2-Frames als es mit Hilfe von VLANs möglich ist. Klassische VLANs bieten die Möglichkeit, durch die Verwendung einer 12-Bit-VLAN-ID 4094 VLAN-Segmente zu adressieren. VxLAN integriert eine 24-Bit-Segment-ID, den VxLAN-Network-Identifier (VNI). Dadurch ist die Adressierung von weit über 16 Millionen Segmenten möglich. In jedem dieser VxLANs können dann wieder weitere 4094 separate VLANs gebildet werden. Diese Ressourcen sind für heutige Netzwerkarchitekturen mehr als hinreichend.
3. Es besteht eine wirtschaftlichere Nutzung des Network-Underlays durch den Einsatz von modernen Routing-Mechanismen. In klassischen VLANs wurde das Spanning-Tree-Protocol (STP) eingesetzt. Allgemein beschrieben, ermittelt STP anhand von Pfadkosten (Latenz, Übertragungsrate) die beste Verbindung zwischen zwei Netzwerkelementen auf Layer-2 und blockiert alle anderen redundanten Verbindungen für diese Kommunikation. Dadurch wird stets der beste Verbindungspfad für eine Kommunikation bereitgestellt. Durch diesen Mechanismus werden jedoch teilweise bis zu 50% der verfügbaren Pfade blockiert, sodass keine Mehrfachverbindungen entstehen. Bei breitbandigen Verkehrsaufkommen zeigt sich STP jedoch als unwirtschaftlich. VxLAN integriert mit Hilfe des Layer-3-Headers Routing-Mechanismen, wie Equal-cost-multipath (ECMP) und verschiedene Link-Aggregation-Protokolle. Diese ermöglichen es, die Verkehrsströme mit Hilfe aller verfügbaren Pfade und ganzheitlich über das Netzwerk zu verteilen. [20]

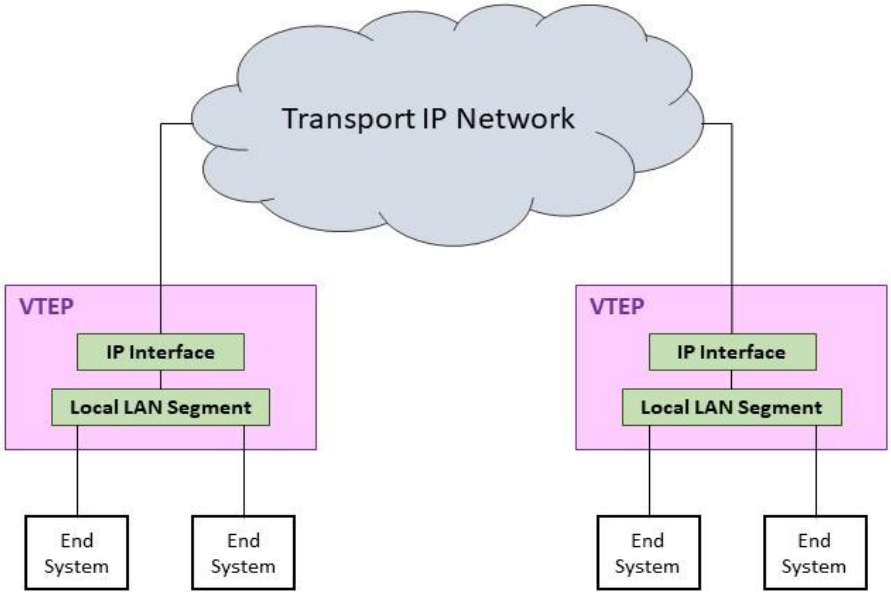

Abbildung 6: VxLAN Tunnel Endpoint, modifiziert nach [20]

Die Funktion von VxLAN wird mit Hilfe von VxLAN-Tunnel-Endpoints (VTEP) bereitgestellt. VTEPs sind VxLAN-kompatible Netzwerkkomponenten, wie Endgeräte, Router oder Switches. Sie kapseln die Ethernet-Frames in VxLAN-Segmente (Layer-3-Pakete). Jeder VTEP besitzt eine IP-Adresse. Sie stellt die Grundlage für die Übertragung der VxLAN-Segmente dar. Die VTEPs fügen den Segmenten außerdem Information über Quell- und Ziel-Ports hinzu. Dies wird später in diesem Abschnitt erläutert. Haben die Segmente ihre Zieladresse erreicht, lösen die VTEPs die VxLAN-Segmente wieder in Ethernet-Frames auf. Die vorher hinzugefügten Informationen werden an dieser Stelle wieder entfernt [20].

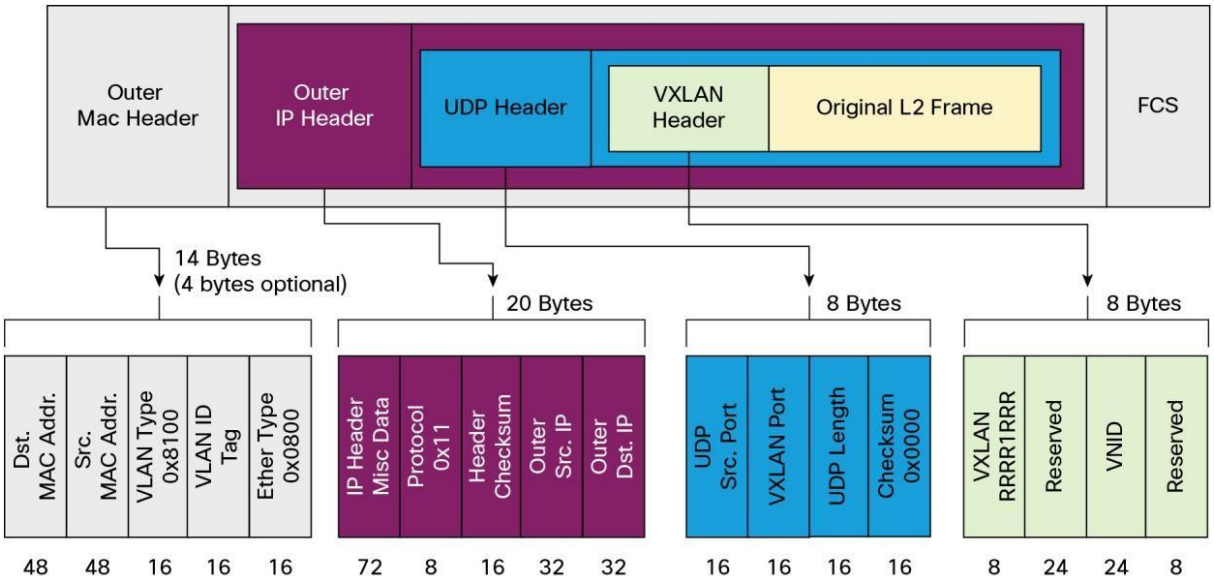

Abbildung 7: VxLAN Encapsulation and packet format [20]

Die Abbildung 7 zeigt das Format eines VxLAN-Segments. Die VTEPs fügen den Ethernet-Frames verschiedene Header und Informationen hinzu, wie z.B. folgende:

- MAC-Zieladresse (MAC des Ziel-VTEP)
- MAC-Quelladresse (MAC des Quell-VTEP)
- IP-Zieladresse (IP des Ziel-VTEP)
- IP-Quelladresse (IP des Quell-VTEP)
- UDP-Header.

Der dargestellte VxLAN-Header enthält das Feld VNI, den Virtual-Network-Identifier. Dieser ist ein Wert bestehend aus 24 Bit, welcher das jeweilige virtuelle Netzwerk identifiziert. Die Inhalte der Segmente in diesem Netzwerk bzw. Tunnel sind nicht aus anderen Netzwerken erreichbar. Zusammen mit den Quell- und Ziel-Informationen können die übertragenen Segmente eindeutig identifiziert werden [20].

Für weitere Informationen wird das Dokument RFC 7348 [21] empfohlen.

3 Zielstellung

3.1 Aktueller Stand der Technik des Campusnetzwerks

Das zu projektierende Campusnetzwerk gehört zu einem Universitätsklinikum. In diesem Abschnitt werden die technischen Anforderungen der bestehenden IT-Systeme beschrieben.

Der Campus besteht aus 26 Kliniken, 21 Instituten und 30 zentralen Dienstleistungseinrichtungen, aufgeteilt auf 56 Gebäude gemeinsam an einem Standort und in zusätzlichen Gebäuden an zwei weiteren Standorten. Insgesamt werden im Durchschnitt 3570 Mitarbeiter, 1300 Studenten und 1000 stationäre Patienten mit IT-Leistungen versorgt. Zusätzlich stehen ca. 350 Gäste-Accounts zur Verfügung. Das Netzwerksystem umfasst 120 Netzwerkverteiler-Standorte und drei Rechenzentren.

Aktuell verfügt das Netzwerk über 3800 Arbeitsplatzcomputer, 500 Netzwerkdrucker, 110 physische Server, 350 IP-Telefone und 100 Videoübertragungsgeräte. Darüber hinaus werden 300 medizinische Endgeräte und 250 IP-basierte Geräte der Gebäudeleittechnik betrieben. Derzeit werden zusätzlich ca. 1000 IPTV-fähige Patiententerminals installiert.

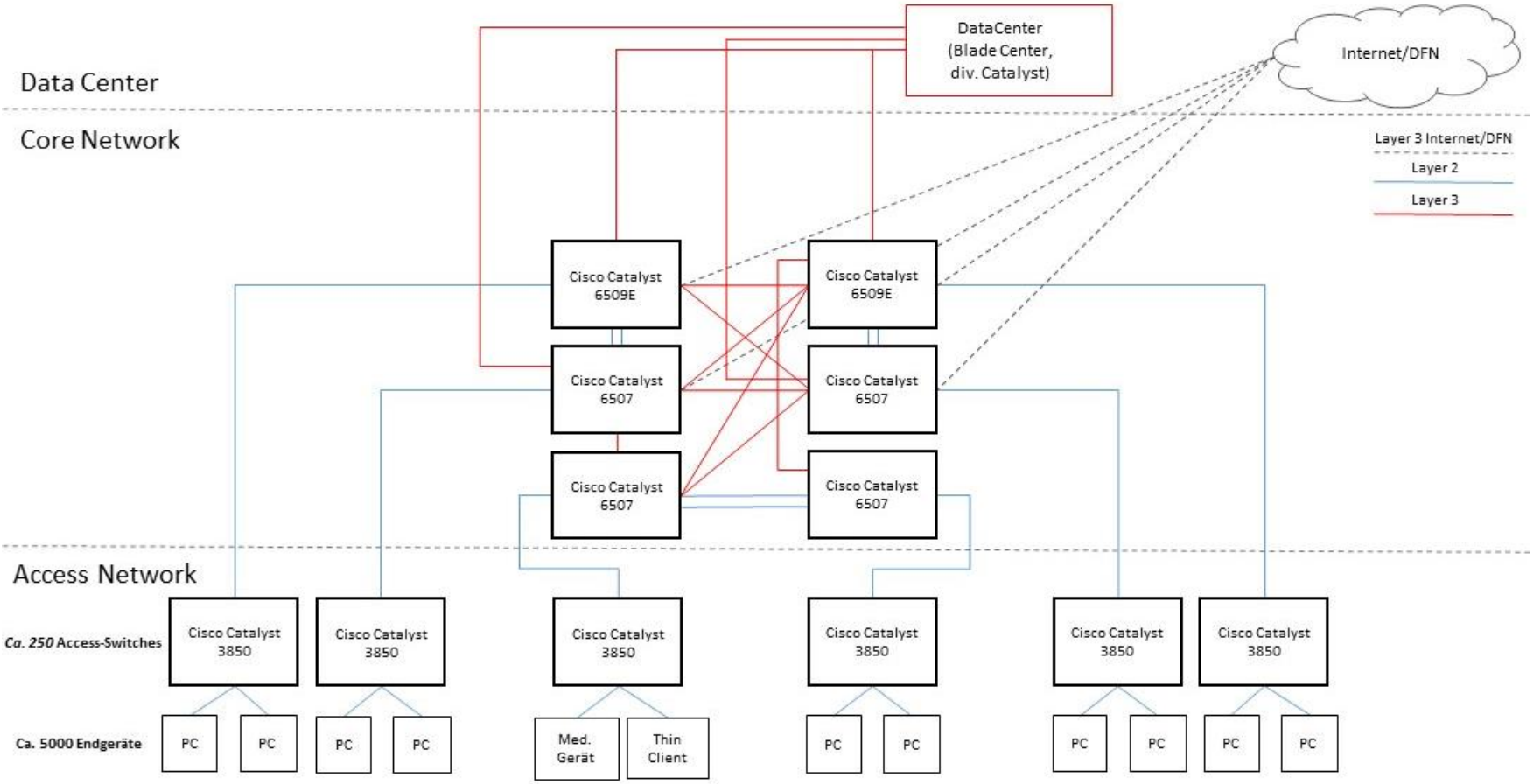

Abbildung 8: Aktueller Stand des Campusnetzwerks

Im Core-Netzwerk des Campusnetzwerks werden derzeit sechs Cisco Catalyst 65xx Systeme betrieben (Abbildung 8). Diese stellen zusammen mit 10GbE-Verbindungen und 200 Class-C-Subnetzen das geroutete IP-Backbone des Netzwerks dar. Dazu gibt es die Möglichkeit, VLANs für spezielle Anwendungsbereiche zu etablieren. Die Anbindung zum Rechenzentrum verläuft über eine ausfallsichere Switch-/Routing-Plattform vom Typ Cisco Nexus 5000 (nicht in den Abbildungen dargestellt). Die Plattform verfügt über 40GbE-Schnittstellen für die Integration spezieller Softwaresysteme. OSPF wird konsistent als Routing-Protokoll verwendet. Die Verbindung zu den Endgeräten wird mit Hilfe von ca. 150 Access-Switches vom Typ Cisco Catalyst 3850 bereitgestellt. Die Kommunikation im Access-Netzwerk wird mit Hilfe von VLANs realisiert. Für die Zugangssicherheit ist eine ausfallsichere Cisco-Network-Access-Control-Lösung (NAC) installiert. Dafür steht eine Cisco-ISE (Identity-Service-Engine), integriert im Rechenzentrum, zur Verfügung. Diese stellt rollen- und gruppenspezifische Sicherheitsrichtlinien (Policies) zur Verfügung. Für die flexible Endgerätenutzung werden definierte Policies für LAN- und WLAN-Zugangssysteme verwendet. Netzwerkdienste wie AD (Active-Directory) und DNS (Domain-Name-Service) sind ebenfalls im Rechenzentrum integriert. An den Netzkopplungen sind Firewalls vom Hersteller Palo Alto installiert. Je nach Konfigurationen beschränken die Firewalls, abhängig von Applikationen und Nutzerprofilgruppen, Verkehrsströme und Zugriffe.

Die Verbindungen in das DFN (Deutsches Forschungsnetz) und das daraus folgende Routing in das Internet, wird über diese Firewall-Strukturen realisiert. Die Firewalls sind an vier zentralen Core-Routern angebunden und aus Übersichtsgründen nicht in den Abbildungen enthalten.

3.2 Anforderungen an die neue Netzwerkarchitektur

Die grundsätzlichen Anforderungen an die neue Netzwerkarchitektur beinhalten die Automatisierung der Administration, die Erhaltung der Hochverfügbarkeit und Erhöhung des Sicherheitslevels sowie die effiziente und benutzerspezifische Verteilung der Verkehrslasten. Dafür soll die Architektur als Software-Defined-Network ausgeführt werden. Das bietet die Möglichkeit, ein zentrales Management zu etablieren. Diese Management-Architektur beinhaltet Funktionen für das Monitoring von Netzwerkressourcen sowie die Möglichkeit der Bereitstellung personalisierter Funktionsbereiche und Administrationsrechte.

Detaillierter betrachtet sollen folgende Funktionen zur Verfügung stehen:

- Hochverfügbarer Netzwerkbetrieb
- Redundante Auslegung des Core-Netzwerks
- Georedundanz-Architektur des Core-Netzwerks
- Skalierbare Leistungen im Core-Netzwerk
- Linkbündelung (Trunking)
- Overlay-Technologien VxLAN und LISP
- Group-based-Policy
- Erhöhung der zentralen Überwachungs- und Steuerungsfunktionen auf Ebene der Kommunikationsprotokolle und Teilnehmer
- Betrieb von IPv4 und IPv6 im Dual-Stack-Mode
- Richtlinienbasierte Anwendungsbereitstellung
- Telemetrie-Anwendungen für Netzwerkressourcen und Qualität

Aus Gründen der Kompatibilität und Interoperabilität sollen die künftigen Netzwerkkomponenten vom Hersteller Cisco sein.

Die Einführung von hochverfügbaren und virtuellen Server- und Storage-Architekturen in drei lokalen Rechenzentren, die zunehmende Nutzung von modernen, latenzsensitiven Softwareanwendungen und die steigende Zahl von leistungsfähigen Endgeräten bedingt eine leistungstechnische und funktionale Modernisierung der Core-Netzwerkarchitektur.

Die Netzwerkarchitektur besteht konsistent aus Produkten des Herstellers Cisco. Aufgrund der Systemerfahrung der IT-Mitarbeiter und das Vertrauen, welches gegenüber Cisco existiert, wird die zukünftige Architektur ebenfalls konsistent aus Hard- und Software-Systemen des Herstellers Cisco bestehen. Der derzeitige Aufschwung in der Entwicklung von SDN und die Ankündigung von Cisco, das DNA-Angebot (SDN) in den nächsten Jahren weiter auszubauen, ist ebenfalls ein Grund dieser Komponenten-Auswahl.

3.3 Zieldesign

Die Abbildung 9 stellt das Zieldesign der neuen Netzwerkstruktur des Campusnetzwerks dar. Die neue Architektur besteht konsistent aus SDN-fähigen Komponenten (Cisco-DNA). Alle dargestellten Verbindungen beschreiben Layer-3-Kommunikationsbeziehungen.

Cisco-DNA (Digital-Network-Architecture) ist eine Lösung zur Automatisierung von Services in Campusnetzwerken. Sie besteht aus einer offenen und erweiterbaren Plattform. Die Plattform bietet benutzer- und gruppenspezifische Access-Policies, eine automatisierte Administration und Konfiguration sowie eine hohe Skalierbarkeit der Leistungsparameter. Das DNA-Center bietet außerdem viele Möglichkeiten des Netzwerk-Monitorings.

Das Core-Netzwerk soll aus sechs Cisco Catalyst 9500 und zwei Cisco Nexus 7700 bestehen. Diese werden an sechs verschiedenen Standorten georedundant installiert. Zwischen den einzelnen Netzkomponenten bestehen jeweils zwei redundante 10GbE-Verbindungen (LWL). Diese Netzkomponenten bilden das Core-Netzwerk bzw. das IP-Backbone.

Das DNA-Center wird als proprietäreres Hardwaresystem georedundant in das Rechenzentrum integriert. Es stellt die Konfigurationsschnittstelle bzw. -oberfläche für die gesamte DNA dar. Angebunden ist das DNA-Center an das Northbound-API des SDN-Controllers. Die Funktion des SDN-Controllers wird verteilt auf den beiden rot-grün dargestellten Catalyst-9500- und auf den beiden Nexus-7700-Systemen redundant installiert. Im Gegensatz zu der theoretischen und klassischen Beschreibung des SDN-Controllers, wird diese Funktion in der Cisco-DNA auf mehrere Geräte aufgeteilt und ist rein softwarebasiert. Die Nexus-Komponenten bilden zudem die Schnittstellen zum Rechenzentrum.

Das Access-Netzwerk soll aus ca. 250 Access-Routern vom Typ Cisco Catalyst 9300 bestehen, welche die Verbindungen zu den ca. 5000 Endgeräten herstellen. Die Anbindung der Access-Geräte wird ebenfalls durch jeweils sechs redundante 10GbE-Verbindungen realisiert.

Die SDN-Struktur wird, wie nachfolgend erklärt, mit Hilfe von VxLAN und LISP konzipiert. Damit wird eine netzwerkweite Kompatibilität zu diesen beiden Techniken benötigt. Aus diesem Grund werden bei der geplanten Migration alle aktiven Komponenten des Core- und des Access-Netzwerks ausgetauscht.

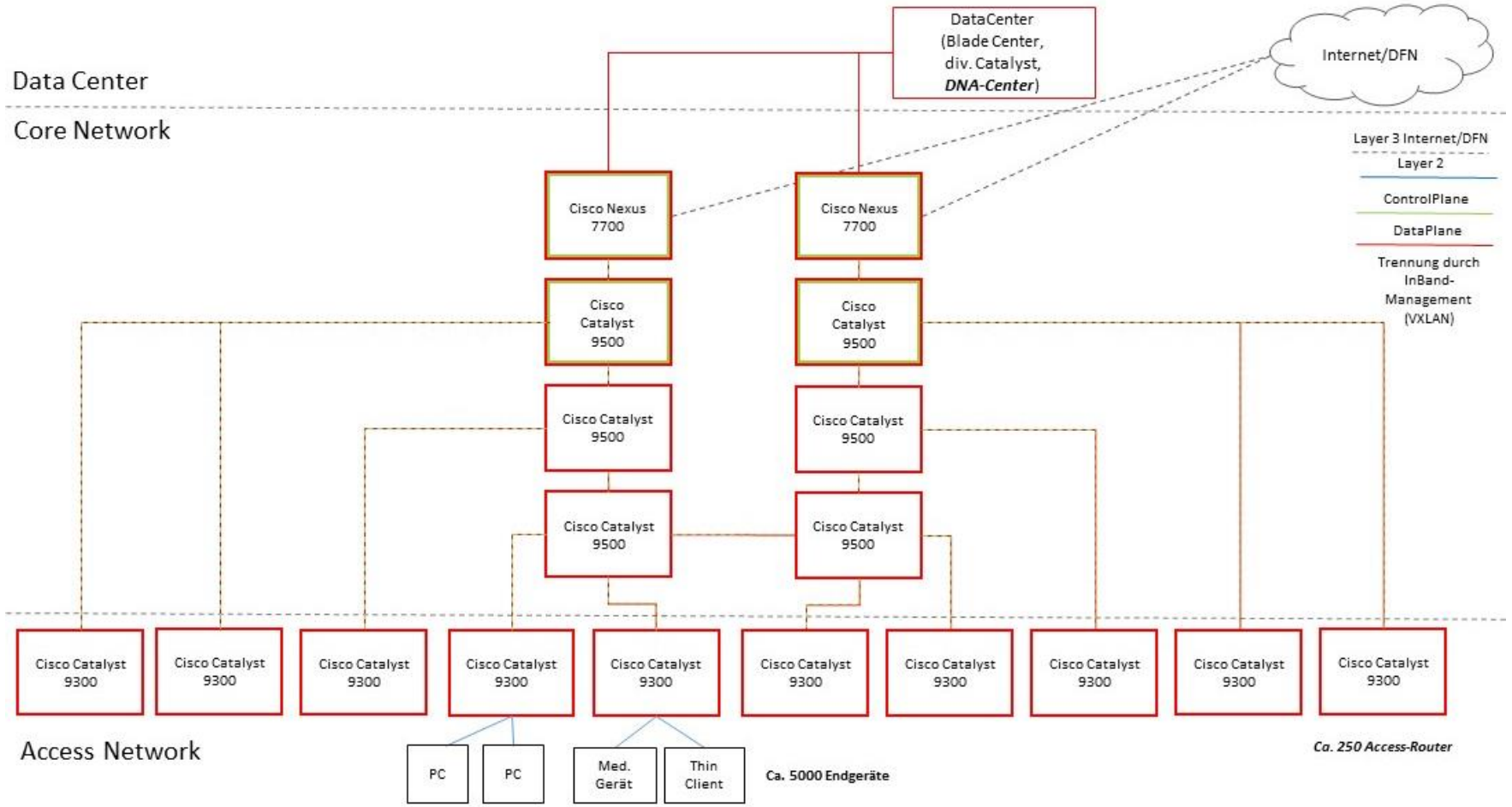

Abbildung 9: Die Netzstruktur als Ergebnis der erfolgten SDN-Migration

Die Abbildung 9 zeigt deutlich die Funktionsbereiche von der Control- und der Data-Plane. Die Trennung zwischen der Control- und der Data-Plane wird durch ein In-Band-Management über die Bildung von Virtual-extensible-LANs (VxLAN) hergestellt. Die Integration des SDN-Controllers, erfolgt nicht durch separate Hardware. Sie erfolgt in Form von Software-Modulen auf gemeinsam genutzter Hardware. Somit ist die Control-Plane nicht auf der physikalischen, sondern auf der Sicherungsschicht von der Data-Plane getrennt.

Für die Kommunikation in der Data-Plane wird das Routing-Protokoll IS-IS verwendet. Gegenüber dem vormals genutzten OSPF bietet IS-IS eine bessere Skalierbarkeit und einfachere Konfigurationsmöglichkeiten. Um die Kommunikationsbeziehungen zu vereinfachen, wurde in IS-IS eine Möglichkeit zur „Hierarchisierung“ implementiert. Das bedeutet, dass innerhalb des Netzwerks wird zwischen Level-1- und Level-2-Intermediate-Systems unterschieden wird. Level-1-IS können ausschließlich mit anderen Level-1-IS der gleichen Routing-Area kommunizieren. Level-2-IS können zwischen verschiedenen Level-1-Routing-Areas routen und bilden somit das Inter-Area-Backbone. Die Kommunikationsbeziehungen sind insofern vereinfacht, dass ein Level-1-IS nur noch Kenntnis von anderen Level-1-IS der gleichen Routing-Area hat, sowie vom nächsten Level-2-IS. Das IS-IS-Protokoll und damit verbunden die Benutzung von Area-Border-Routern führen zu einer schnelleren Konvergenz und zu stabileren Routen, als unter der Verwendung von OSPF. Verschiedene Routen von einer Level-1- zu einer Level-2-Routing-Area werden zu einer Route zusammengefasst und in die andere Richtung wieder aufgeteilt (Gateway-Funktionalität). Kommunikationsbeziehungen innerhalb der gleichen Routing-Area werden nicht zum Gateway geroutet. Änderungen innerhalb einer Routing-Area haben also keinen Einfluss auf andere Routing-Areas [22].

Für die Verbindung der Routing-Knoten (Catalyst 9500) zum Access-Netzwerk werden VxLANs gebildet. VxLAN basiert auf Layer-2 des OSI-Schichtenmodels. Die Nutzdaten werden dann in UDP-Paketen (User Datagramm Protokoll, Layer-4 OSI) gekapselt und durch das Netzwerk transportiert. Für große Netzwerkstrukturen bietet VxLAN den Vorteil gegenüber herkömmlichen VLANs, dass es möglich ist, bis zu 16.777.215 einzelne VxLANs zu erstellen. Diese können dann jeweils für sich nochmal 4094 klassische VLANs bilden [21]. Die Bildung solcher komplexen Strukturen war unter der Verwendung von VLAN nicht möglich. Da die Bereitstellung von Netzdiensten und Anwendungen benutzer-, gruppen- und geräteabhängig verlaufen soll, ist es nötig, eine große Vielzahl virtueller Netzwerke zu erstellen. Der dazugehörige Netzwerkdienst wird dann im Rechenzentrum integriert, was das

Aufrechterhalten der Kommunikation im Access-Netzwerk bei z.B. Störungsfällen in der Control-Plane ermöglicht.

Innerhalb der Control-Plane wird LISP betrieben. Das Protokoll integriert die Verknüpfung zwischen der Identität des Users und dem Installationsort im Netzwerk mit Hilfe einer zugewiesenen ID. Diese Funktion stellt die Grundlage für eine benutzer- und gruppenspezifische dynamische Konfiguration von Kommunikationsbeziehungen und Anwendungsbereitstellung dar.

Netzwerkdienste wie AD, DNS und Cisco-Identity-Services-Engine (Cisco-ISE) werden in das Rechenzentrum integriert und „klassisch“ an die Data-Plane angebunden. Somit stellt LISP im Campusnetzwerk die einzige automatisierte Funktion dar, welche über das Northbound-API an den SDN Controller angebunden ist.

Durch die „dynamische“ Zuweisung der gerätespezifischen ID über LISP wird die Grundlage für eine automatisierte Zuweisung von Policies im Netzwerk gelegt. Die Authentifizierungsinformation wird aus der AD bezogen. Die direkte Zuweisung der Policies wird dann durch die Cisco-ISE organisiert, welche die benutzer- und gerätespezifischen Zugriffs- und Sicherheitsrichtlinien auf die einzelnen Ports im Access-Netzwerk überträgt.

Die Netzwerkdienste AD und DNS sowie die Cisco-ISE sind, wie auch schon in der klassischen Struktur, in den Ressourcen des Rechenzentrums gelagert. Diese redundante zentrale Lagerung schafft sehr gute Bedingungen für einen hochverfügbaren und ausfallsicheren Betrieb des Campusnetzwerks. Außerdem sind diese Systeme relativ unempfindlich gegenüber Hard- bzw. Softwareveränderungen im Bereich des Core-Netzwerks.

4 Methoden der Migration

Die Struktur des bestehenden Campusnetzwerks wurde dokumentiert, die Anforderungen definiert und die Zielstruktur entwickelt. Das Kapitel 4 stellt nachfolgend die geplante Migration der SDN-Struktur dar. Begonnen wird in Abschnitt 4.1 mit dem Proof of Concept, welches die prinzipielle Durchführbarkeit der Migration analysieren bzw. belegen soll und stets vor dem ersten Migrationsschritt durchzuführen ist. Anschließend wird in Abschnitt 4.2 die geplante Hardware- und Software-Migration der SDN-Struktur schrittweise beschrieben und erläutert. In Abschnitt 4.3 werden die Inhalte für den Systemtest und die Systemabnahme dargestellt. In Abschnitt 4.4 werden die grundlegenden Themen der abschließenden Kundeneinweisung beschrieben. Der Vorteil dieses Migrationskonzepts besteht darin, dass es während des kontinuierlichen Betriebs des Gesamtsystems durchgeführt werden kann. Es kommt lediglich zu kurzzeitigen Unterbrechungen in der Verfügbarkeit einzelner Endgeräte. Kritische Teilschritte werden gekennzeichnet und die Vereinbarung von Wartungsfenstern empfohlen. Im Zuge der Migration wird das „alte“ sowie das „neue“ Netzwerk parallel betrieben, wobei die bidirektionale Kommunikation zwischen beiden Netzen möglich ist.

4.1 Proof of Concept

Die Validierung der Funktionen und Verfahren der zukünftigen Netzwerkstruktur erfordert die Durchführung eines Proof of Concepts (PoC). Dafür wird ein Prototyp der SDN-Netzstruktur entwickelt und auf dem Campus installiert. In diesem Prototyp sind zum finalen Campusnetzwerk identische Netzwerkkomponenten integriert. Es werden zwei Core-Router vom Typ Cisco Nexus 7700, zwei Core-Router vom Typ Cisco Catalyst 9500 und zwei Access-Router vom Typ Cisco Catalyst 9300 verwendet. Das DNA-Center wird dafür bereits in das Rechenzentrum des Campusnetzwerks integriert und mit der Teststruktur verbunden. Die Funktion des SDN-Controllers wird, wie auch im Zieldesign des Netzwerks geplant, aufgeteilt auf beiden Nexus-7700- und auf beiden Catalyst-9500-Komponenten installiert. An die zwei Access-Router, werden verschiedene Endgeräte (PCs, VoIP-Telefone, Drucker, Medizintechnik) angeschlossen.

Der Verlauf eines PoCs, also der Beweis der Funktionalitäten eines Prototyps, kann nicht allgemeingültig definiert werden. Das hier betrachtete Campusnetzwerk ist sehr komplex und

speziell auf die auftretenden Anforderungen abgestimmt, sodass eine sehr individuelle und systemangepasste Funktionsprüfung entwickelt wurde.

Das PoC wird in vier verschiedene Themen gruppiert: dem Komponentenausfall, dem Ausfall der Netzwerkverbindungen (L1 bis L3), dem Wiederanlauf nach einem Ausfall der elektrischen Versorgung und dem Replacement. Diese Gruppierungen werden nachfolgend kurz erläutert. Der Komponentenausfall umfasst drei Bereiche: das DNA-Center, die Control-Plane-Nodes (2x Nexus 7700, 2x Catalyst 9500) und die Border Nodes (Catalyst 9500). Für die Funktionsprüfungen des DNA-Centers werden folgende Punkte bearbeitet:

- Backup,
- Update,
- Downgrade (wenn technisch möglich),
- DNA-Center offline.

Für die Überprüfung der Control-Plane-Nodes und der Border-Nodes werden jeweils die Punkte:

- Reboot einzelner Systeme,
- Update,
- Downgrade (wenn technisch möglich)

bearbeitet. Außerdem wird ein möglicher Systemausfall der kompletten Control-Plane betrachtet. Das zweite Thema des PoCs ist der Ausfall einzelner Netzwerkverbindungen. Die Vermeidung eines Systemausfalls erfordert die Überprüfung der einzelnen Redundanzen der Übertragungswege. Dafür werden die folgenden Verbindungslinien nacheinander getrennt und überprüft:

- Core-Router zu Core-Router,
- Core-Router zu Rechenzentrum,
- Core-Router zu Access-Router.

Das dritte Thema des PoCs ist der Wiederanlauf nach einem Ausfall der elektrischen Versorgung. Dabei sollen Voraussetzungen für einen Neustart ermittelt und geprüft werden, wie z.B. die Dimensionierung der unterbrechungsfreien Stromversorgung (USV). Es wird eine Reihenfolge für den Neustart der Einzelsysteme festgelegt. Außerdem wird der dafür benötigte Zeitbedarf ermittelt.

Der vierte und letzte Themenbereich des PoCs ist das Replacement. Dabei wird das Systemverhalten beim Integrieren neuer Einzelsysteme in das Gesamtsystem und das Entfernen von Einzelsystemen aus dem Gesamtsystem ermittelt. Dadurch werden Systemerweiterungen simuliert, bei denen mögliche Kompatibilitäts- und Interoperabilitätsprobleme auftreten können.

Alle durchzuführenden Überprüfungen werden in ihrem Ablauf und ihren Ergebnissen protokolliert. Des Weiteren werden Notfall-Handlungsanweisungen für den Netzbetreiber erstellt, sodass eine umfassende Betriebssicherheit zu erreichen ist.

4.2 Migration der Netzwerkkomponenten

In den Abschnitten 3.1 bis 3.3 wurde das bestehende Campusnetzwerk betrachtet, die Anforderungen definiert und eine Zielstruktur entwickelt. Im Abschnitt 4.1 wurde die grundlegende Funktionalität der zu migrierenden SDN-Struktur in einem PoC untersucht. Sind die Ergebnisse dieser Analyse positiv, kann mit den Schritten der Migration fortgefahren werden.

Das Thema Netzwerkmigration umfasst drei Grundsätze: das Upgrade, den Ersatz und das Overlay [6]. Bei einem Netzwerkupgrade werden die betriebenen Netzelemente (Router, Switches, usw.) „SDN-fähig“ gemacht. Dies kann durch Software-Updates oder zusätzliche Software-Installationen passieren. Bei einem Ersatz werden klassische Netzwerkelemente durch SDN-fähige Netzwerkelemente ersetzt. Das hat den Vorteil, dass zeitgleich aktuelle und im besten Falle funktionalere Hardware eingesetzt wird. Bei einem Overlay wird eine, dem SDN-Kontext entsprechende, Control-Plane als übergeordnete Struktur zum bestehenden Netzwerk hinzugefügt. Dazu muss das klassische Netzwerk, welches zukünftig als Data-Plane funktioniert, kompatibel zu den Steuerinformationen der Control-Plane sein. In der Praxis wird meist eine Kombination aus diesen drei Möglichkeiten durchgeführt.

„*Die Ziele, die bei einer Migration verfolgt werden, sind bei allen Netzbetreibern mehr oder weniger die gleichen […]:*

- *Reduzierung der Netzinfrastrukturkosten,*
- *Reduzierung der Betriebskosten,*
- *Optimale Nutzung der Neuinvestitionen,*
- *Optimale Weiterverwendung der bereits installierten Technik,*

- *Schnellere Dienstebereitstellung,*
- *Mindestens gleich gute Quality of Service*
- *Offene Netzarchitektur bezüglich der Dienstbereitstellung.*“ [6]

Im Zuge einer schrittweisen Migration werden in dem hier betrachteten Fall einzelne neue „SDN-fähige“ Komponenten integriert. Daraufhin werden die Endgeräte in die SDN-Struktur migriert. Zum Ende jedes Migrationsschritts werden die „alten“ Komponenten aus dem Netzwerk entfernt. Ein dauerhafter Parallelbetrieb von „alten“ und „neuen“ Strukturen bleibt über den kompletten Migrationszeitraum möglich. Die konkreten Anforderungen des Netzbetreibers haben dadurch einen starken Einfluss auf den geplanten Migrationsweg. Das Campusnetzwerk wird in dem hier betrachteten Fall kontinuierlich betrieben. Die Betriebssicherheit und die Ausfallsicherheit des Gesamtsystems, der Einzelsysteme und der Dienste stehen über den kompletten Migrationszeitraum im Vordergrund.

4.2.1 Migrationsschritt 1

Die Abbildungen 10 und 11 stellen gemeinsam den ersten Migrationsschritt dar. In diesem Schritt werden dem Netzwerk zwei georedundante Core-Router vom Typ Cisco Nexus 7700 hinzugefügt. In diesen Systemen sind später Funktionen des zentralen Routings im SDN (Data-Plane) sowie Funktionen des SDN-Controllers (Control-Plane) integriert. Außerdem stellen die Geräte im späteren Parallelbetrieb das Routing zwischen „alten“ und „neuen“ Strukturen bereit. Die Anbindung zum Rechenzentrum verläuft nach abgeschlossener Migration der beiden Geräte ausschließlich über die beiden Nexus-7700-Systeme.

Die Geräte werden über Layer-3-Verbindungen angebunden (Abbildung 10, violett dargestellt). Es ist nötig eine IP-Konfiguration durchzuführen sowie OSPF und LISP auf den Geräten einzurichten. Die Erreichbarkeit der Netzwerkkomponenten in den klassischen Strukturen wird mit Hilfe von OSPF hergestellt. Die Installation des LISP wird im Bereich der Control-Plane durchgeführt. LISP erzeugt geräte- und benutzerspezifische IDs für installierte Ressourcen des Netzwerks. Durch das Zusammenspiel von LISP und der Cisco-ISE wird eine dynamische Administration und die Zuweisung spezifischer Policies campusweit ermöglicht.

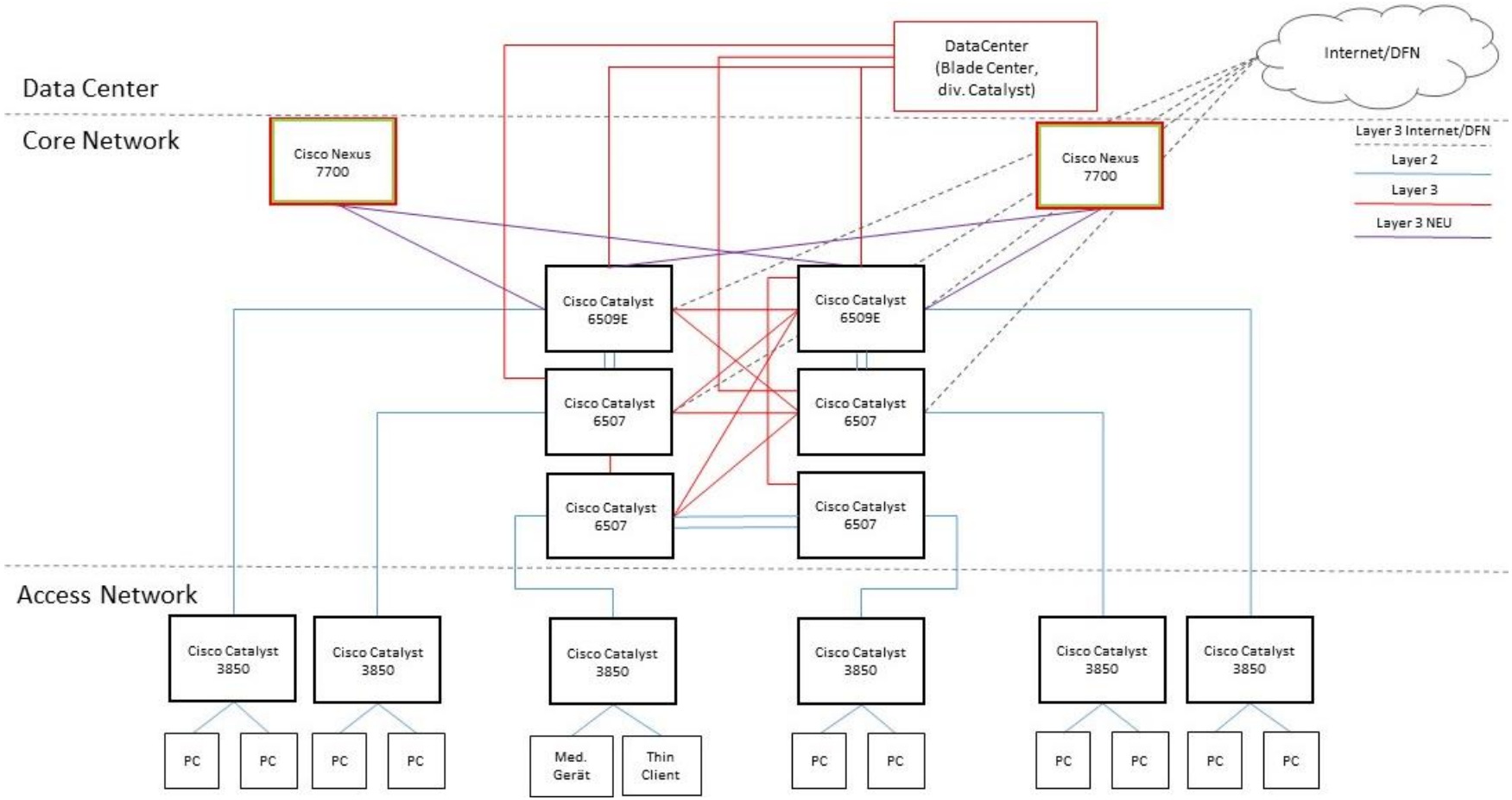

Abbildung 10: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 1.1

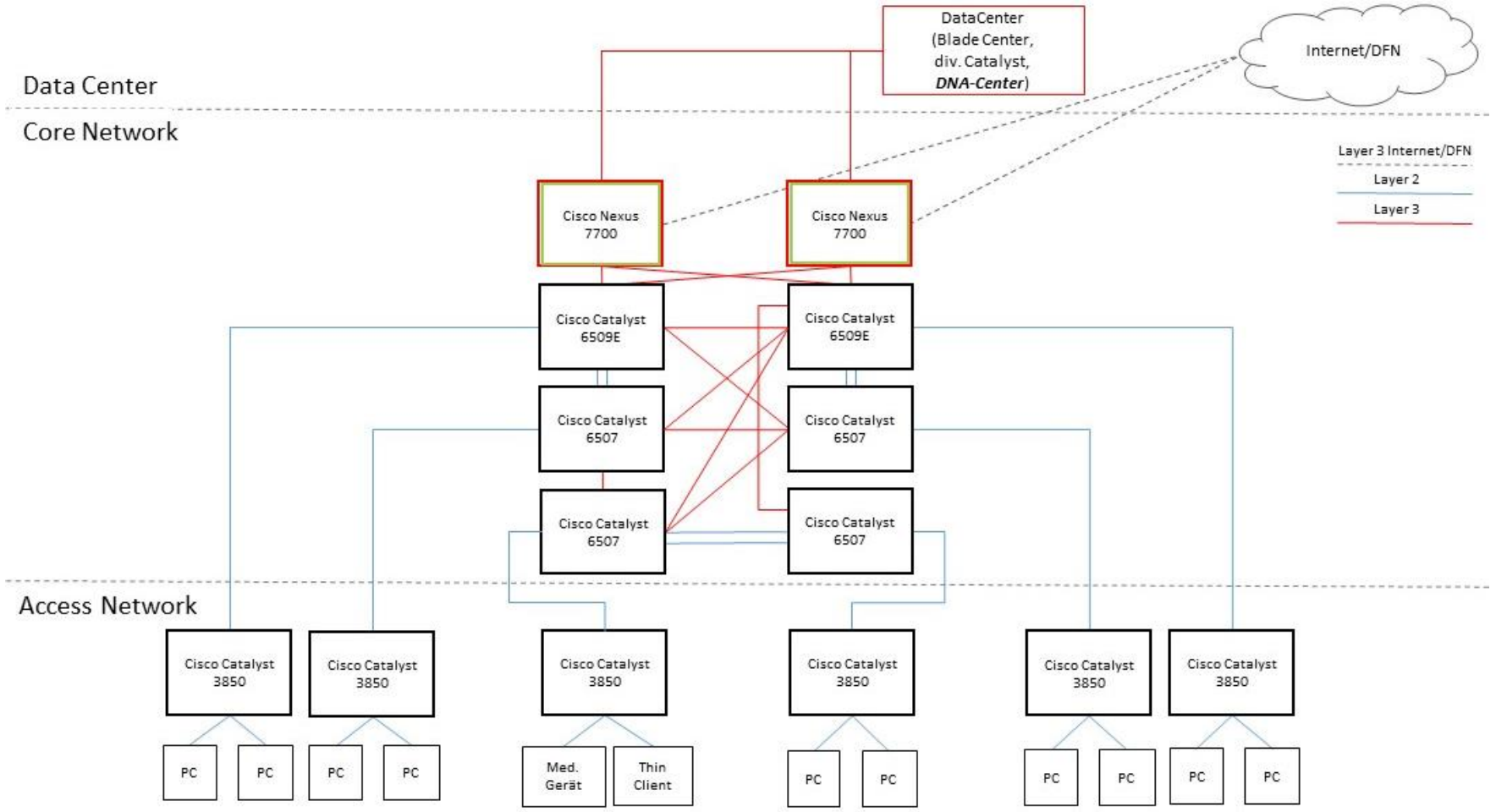

Abbildung 11: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 1.2

Sind die Geräte aus dem bestehenden Core-Netzwerk erreichbar und entsprechend per OSPF angebunden, kann mit dem zweiten Teil des Migrationsschritts fortgefahren werden (Abbildung 11).

In diesem Teilschritt werden die Layer-3-Verbindungen zwischen den Cisco-Nexus-7700-Systemen und dem Rechenzentrum hergestellt. Die Kommunikation zwischen diesen beiden Strukturen funktioniert auf Basis von BGP. Sobald die BGP-Konfiguration auf den beiden Nexus-7700-Systemen erfolgt ist und diese funktionsfähig sind, können die „alten“ Verbindungen, welche zwischen den Catalyst-6509E-Systemen und dem Rechenzentrum bestehen, entfernt werden. Da die neu integrierten Cisco-Nexus-7700-Systeme später Funktionen der Data- sowie der Control-Plane enthalten, werden sie zweifarbig gekennzeichnet (Abbildung 11, rot - Data-Plane, grün - Control-Plane). Die unterbrechungsfreie Erreichbarkeit der Netzwerkdienste im Rechenzentrum ist für den kontinuierlichen Netzwerkbetrieb von hoher Bedeutung. Aus diesem Grund wird empfohlen, für diesen Teilschritt ein Wartungsfenster mit dem Netzbetreiber zu vereinbaren.

Da noch keine weiteren SDN-Komponenten integriert wurden, können die entsprechenden Hardware-Module für das Cisco-DNA-Center wahlweise in diesem oder im nachfolgenden Migrationsschritt redundant an den Standorten des Rechenzentrums installiert werden.

Im Anschluss daran werden die Layer-3-Verbindungen den Cisco-Nexus-7700-Systemen zu den Firewall-Strukturen (Link in das DFN bzw. Internet) vorbereitet. Zu Beginn werden zwei redundante Layer-1-Verbindungen von jedem Nexus 7700 zu den Firewall-Strukturen hergestellt. Da die Kommunikation vom Campusnetzwerk in das DFN über statische Routen verläuft, müssen diese Routen auf den Nexus-Geräten sowie in den Firewalls konfiguriert werden. Nach der funktionalen Überprüfung der Kommunikationswege werden die „alten“ zentralen Core-Router umkonfiguriert, sodass die beiden zentralen Nexus-7700-Systeme als Gateway zum DFN genutzt werden.

Nach dieser Umkonfiguration werden die „alten“ Verbindungen, welche von den Firewalls zu vier zentralen Cisco Catalyst 65xx verliefen, entfernt. Dieser Teilschritt ist für den Regelbetrieb ebenfalls nicht kritisch.

4.2.2 Migrationsschritt 2

Aufgrund der paarweisen Georedundanz der Core-Router-Struktur des „alten“ Netzwerks ist in diesem sowie in den folgenden Migrationsschritten darauf zu achten, jeweils zwei Core-Router gleichzeitig zu integrieren. Die Layer-1-Verbindungen im Bereich des SDN werden dabei als einzelne Verbindungen dargestellt, bestehen jedoch konsistent aus jeweils zwei redundanten 10GbE-Verbindungen.

Im zweiten Migrationsschritt, welcher in Abbildung 12 gezeigt wird, werden die ersten beiden zentralen Core-Router vom Typ Cisco Catalyst 9500 sowie die daran angeschlossenen Access-Router vom Typ Cisco Catalyst 9300 integriert. Dafür werden an den vorhandenen Standorten der „alten“ Systeme ausreichende freie Kapazitäten in den Netzwerkschränken geschaffen, sodass die Verbindungen der Endgeräte nach erfolgtem vollständigen Migrationsschritt lediglich vom „alten“ Access-System auf das „neue“ Access-System verändert werden müssen. Dadurch werden sehr geringe Ausfallzeiten der Endgeräte erreicht. Es wird empfohlen die Migration der Endgeräte in einem mit dem Netzbetreiber abgestimmten Wartungsfenster durchzuführen.

Nachdem die „neuen“ Core- und Access-Router installiert und die notwendigen Layer-1-Verbindungen hergestellt sind, werden die erforderlichen IP- und IS-IS-Konfigurationen durchgeführt. Im SDN-Netzwerkbereich der Core-Router und der Access-Router wird das Routing Protokoll IS-IS verwendet. Zusätzlich wird nochmals eine BGP-Konfiguration auf den im ersten Migrationsschritt integrierten Cisco Nexus 7700 durchgeführt. Diese dient der Kommunikation zwischen den Nexus-7700- und den „benachbarten“ Catalyst-9500-Systemen. Nach den erfolgten IP- und IS-IS-Konfiguration, können zukünftig die Gerätekonfigurationen im Core- und Access-Netzwerk vom DNA-Center gesteuert werden. Die separate Konfiguration einzelner Netzwerkkomponenten ist damit nicht mehr notwendig. Im nächsten Teilschritt wird die VxLAN-Konfiguration für das In-Band-Management mit Hilfe des DNA-Centers auf den bereits installierten SDN-Komponenten (2x Nexus 7700, 2x Catayst 9500, Nx Catalyst 9300) durchgeführt. Durch die Bereitstellung der Netzwerkdienste im Rechenzentrum, wie z.B. AD, DNS und Lizenzservices, soll der Weiterbetrieb der Endgeräte im neuen Netzwerk problemlos verlaufen.

Nach erfolgter Überprüfung der Funktionen der neu installierten Core- und Access-Router können die einzelnen Endgeräte schrittweise vom „alten“ Netzwerk in das „neue“ Netzwerk migriert werden.

Ist diese Migration abgeschlossen, können die „alten“ Systeme abgebaut und die Layer-1-Verbindungen entfernt werden (Abbildung 13). Das Lösen der Verbindungen zu den „alten“ Netzwerkkomponenten benötigt keine zusätzliche Konfiguration in der klassischen Netzwerkstruktur. Das verwendete Routing-Protokoll OSPF erkennt durch die implementierte Nachbarschaftsdatenbank aktuelle Veränderungen in der Topologie bzw. in den Erreichbarkeiten angelagerter Netzwerkkomponenten und verändert somit dynamisch die Routingpfade im Netzwerk.

Bis zum Abschluss der SDN-Migration, bleiben die klassischen Layer-2- (klassisches Switching) und Layer-3-Strukturen (über OSPF) im Bestandsnetzwerk erhalten.

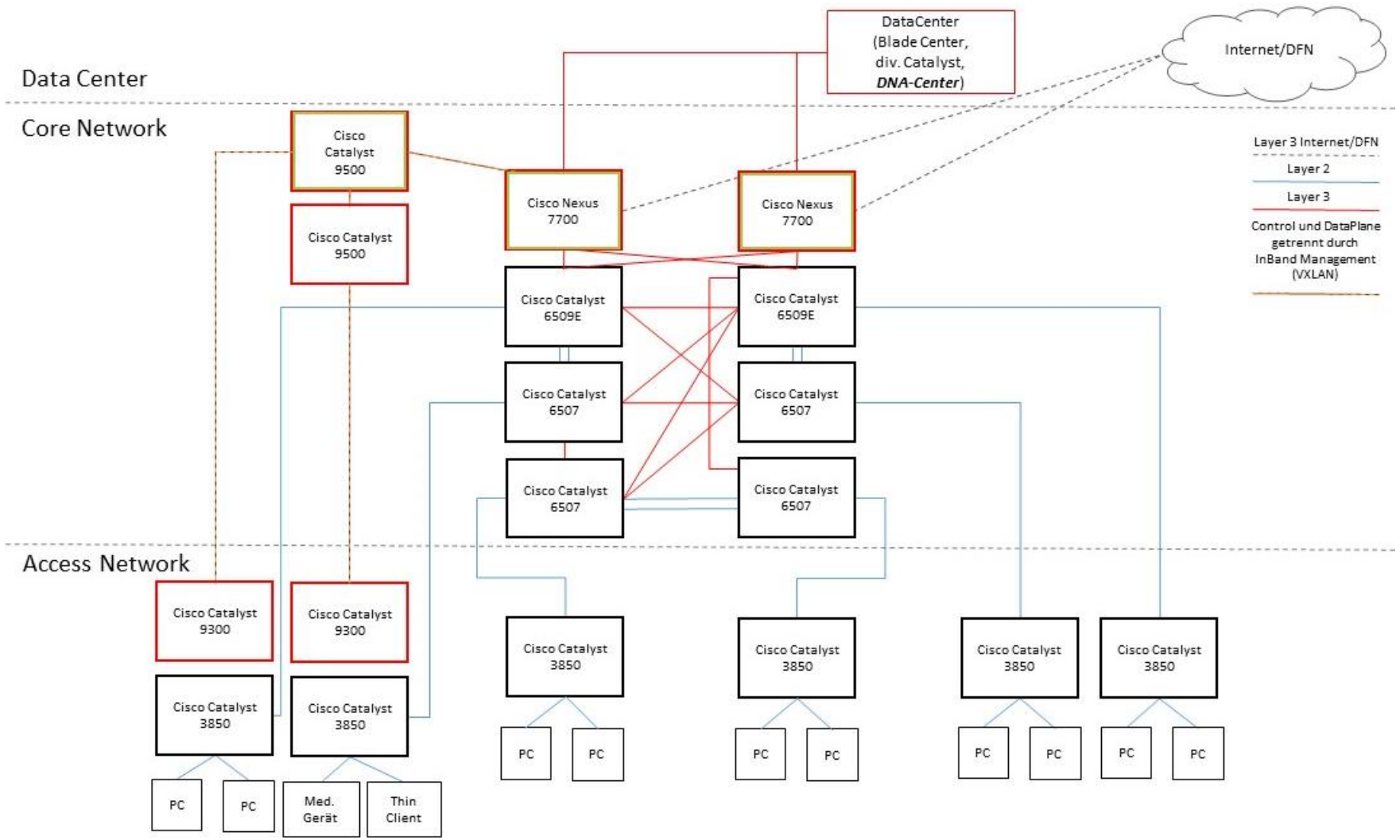

Abbildung 12: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 2.1

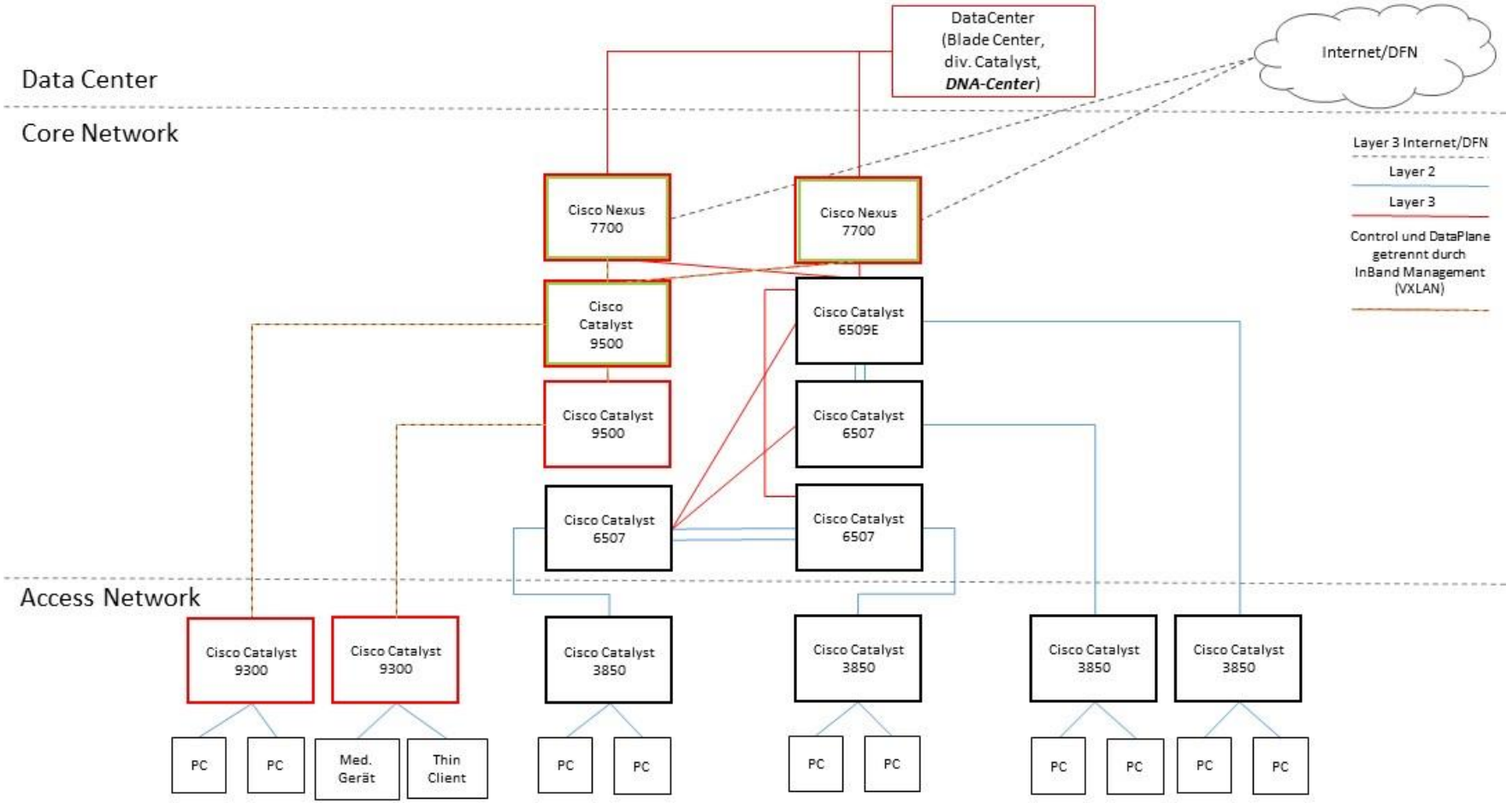

Abbildung 13: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 2.2

4.2.3 Migrationsschritt 3

Im dritten Migrationsschritt werden zunächst zwei weitere Cisco Catalyst 9500 als Core-Router in die Struktur integriert (Abbildung 14). Außerdem wird an allen Standorten der Access-Systeme zusätzlich zu jedem bestehenden Access-Switch ein SDN-fähiger Access-Router (Cisco Catalyst 9300) installiert.

Nachdem die notwendigen Layer-1-Verbindungen hergestellt sind, erhalten die installierten Geräte (2x Cisco Catalyst 9500, Nx Cisco Catalyst 9300) entsprechende IP- und IS-IS–Konfigurationen. Die Zuordnung der SDN-fähigen Geräte zu den jeweiligen VxLANs erfolgt über das DNA-Center, wobei die Control- und die Data-Plane mit Hilfe des In-Band-Managements voneinander getrennt werden.

Für den finalen Teilschritt, die Migration der Endgeräte, wird empfohlen, ein Wartungsfenster mit dem Netzbetreiber abzustimmen. Die Ausfallzeit der Netzwerkverbindungen wird dabei so gering wie möglich gehalten. Sind die betroffenen Endgeräte an die SDN-Strukturen angeschlossen und funktional überprüft, können die alten Geräte abgebaut und die Layer-1-Verbindungen zum klassischen Netz gelöst werden. Die nun entstandene Netzstruktur ist in Abbildung 15 repräsentativ dargestellt.

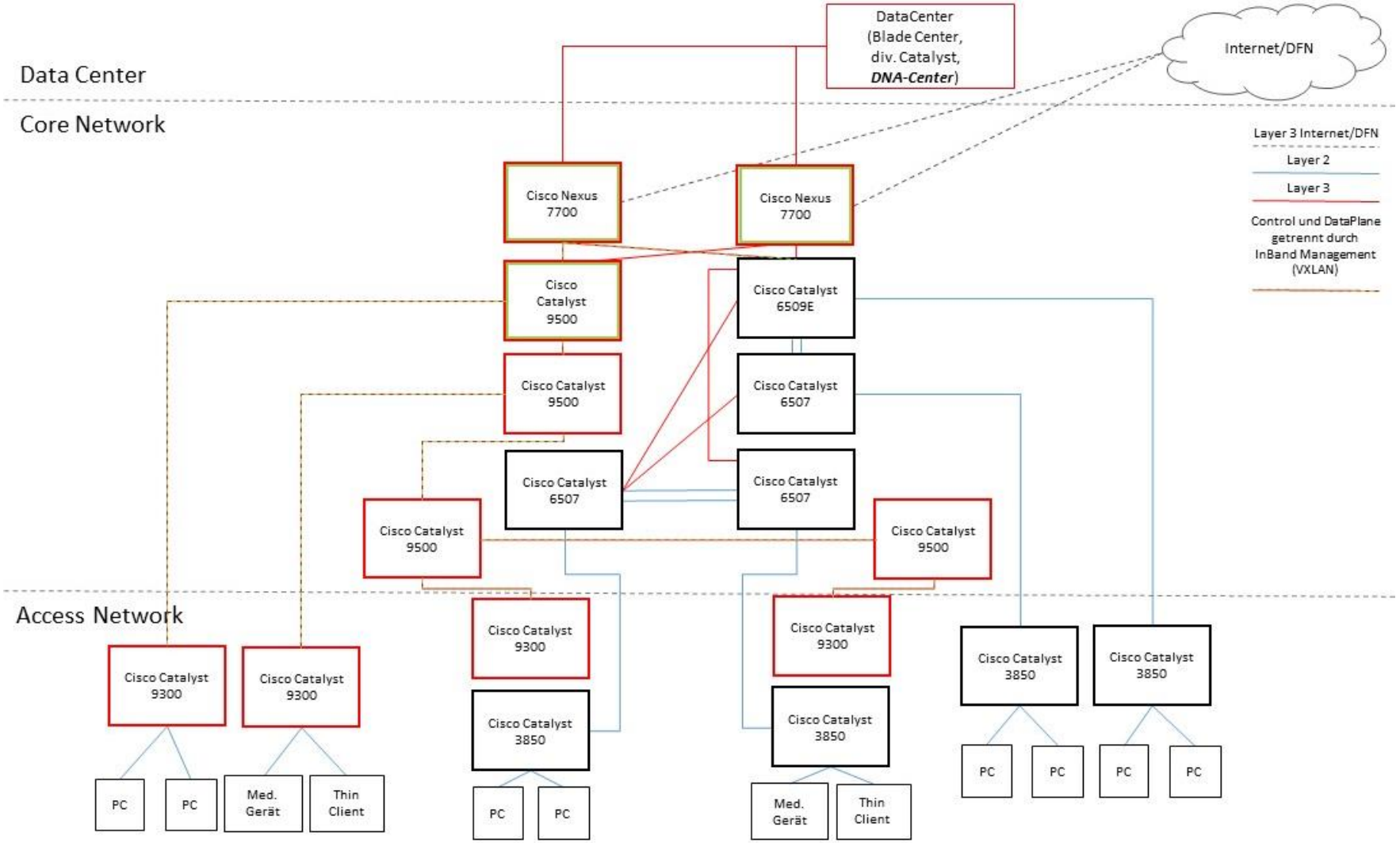

Abbildung 14: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 3.1

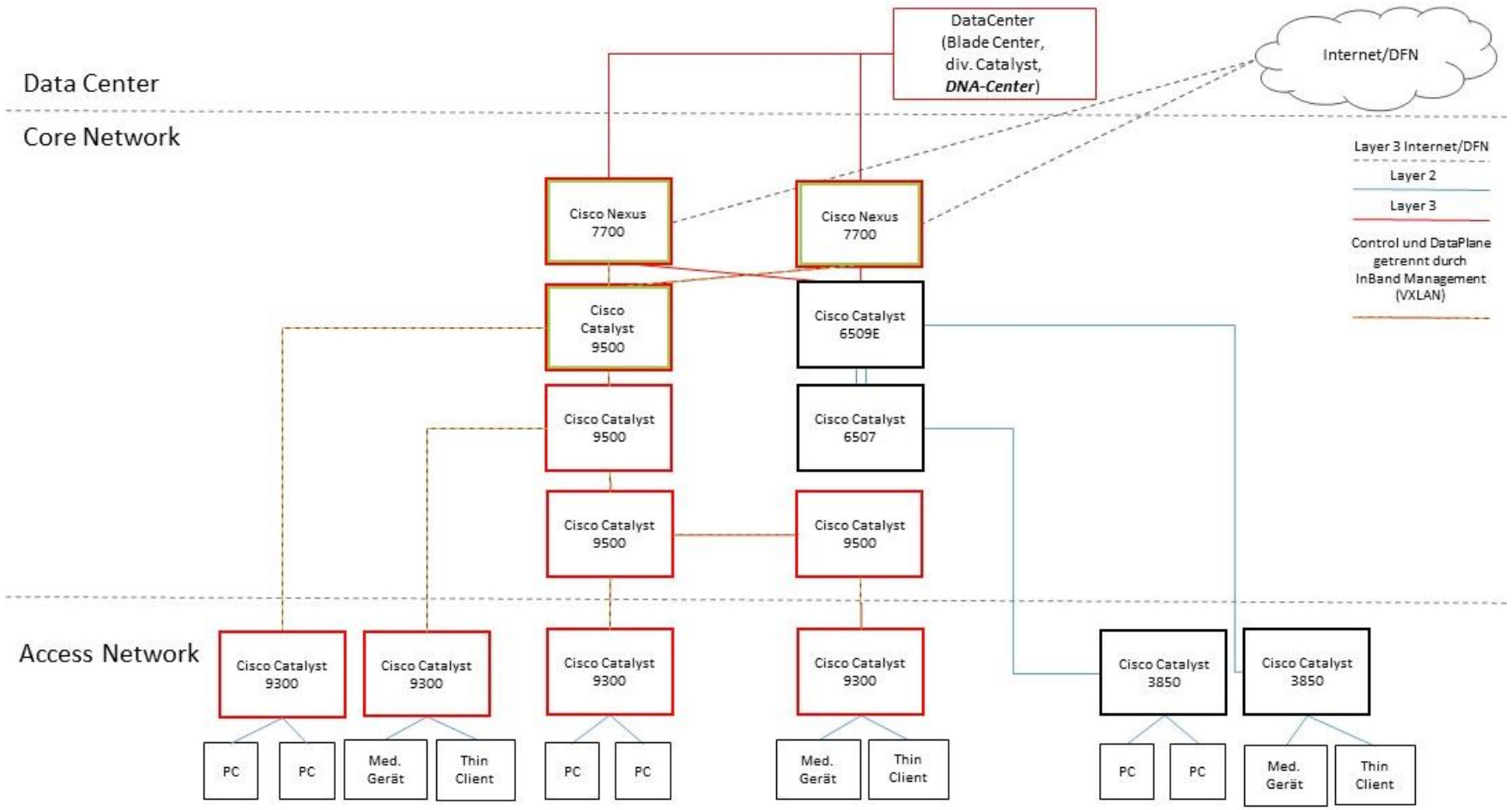

Abbildung 15: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 3.2

4.2.4 Migrationsschritt 4

Im vierten Migrationsschritt werden die letzten beiden zentralen Core-Router (2x Cisco Catalyst 9500) sowie die daran angeschlossenen Access-Router (Nx Cisco Catalyst 9300) an den gewählten Standorten zum Netzwerk hinzugefügt (Abbildung 16). Daraufhin wird die physikalische Netzstruktur hergestellt. Die Geräte erhalten die nötigen IP- und IS-IS-Konfigurationen. Über das DNA-Center erfolgt die Zuweisung der neu integrierten Geräte zu den entsprechenden VxLANs, welche das In-Band-Management für die Trennung von Control- und Data-Plane sicherstellt. Sind die Funktionalitäten überprüft, können die betroffenen Endgeräte aus der „alten“ Netzwerkstruktur in das „neue“ SDN migriert werden. Für diesen Teilschritt wird ebenfalls ein Wartungsfenster empfohlen, um die Dienstausfallzeit so gering wie möglich zu halten.

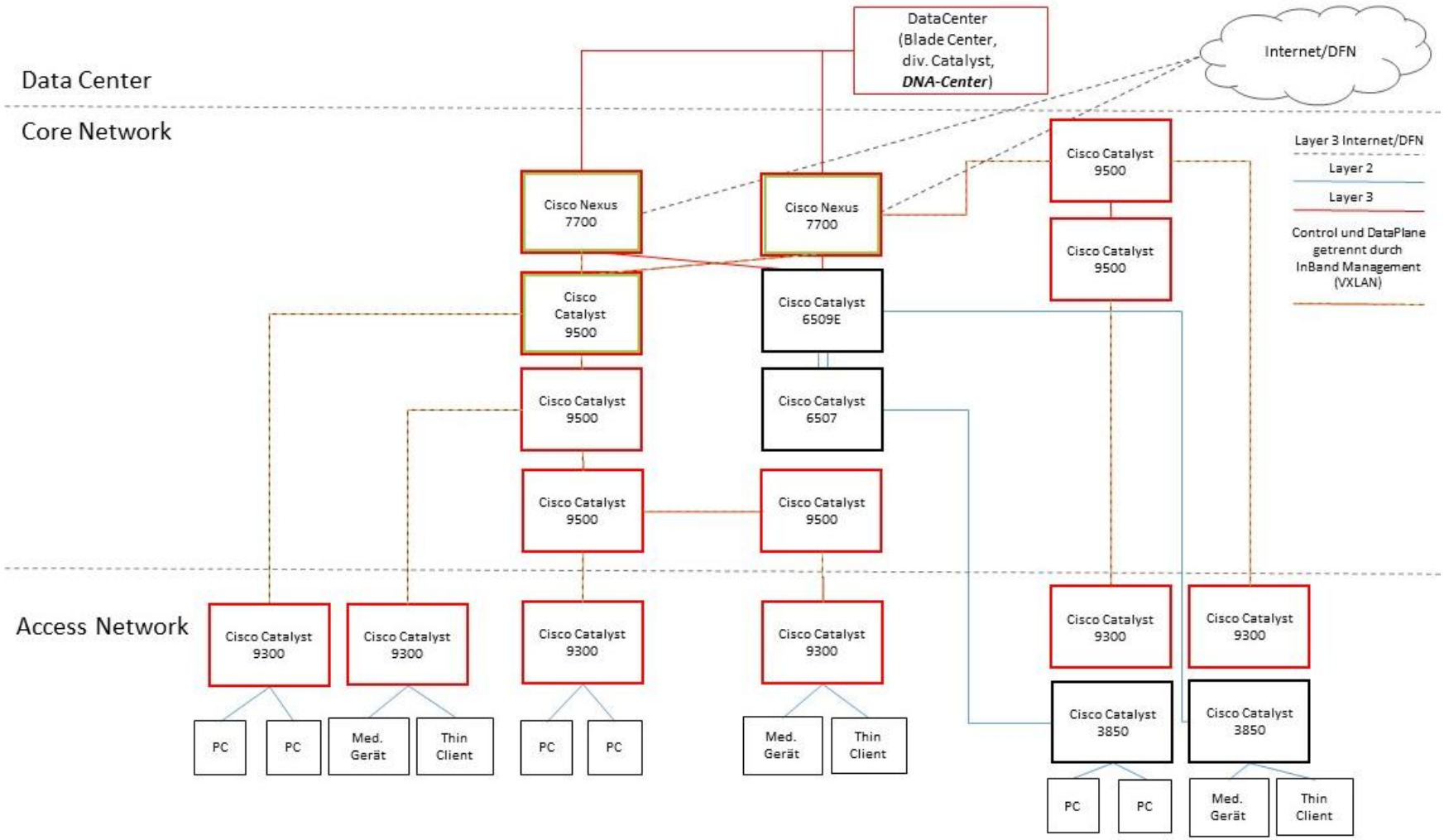

Abbildung 16: Die Netzstruktur als Ergebnis des erfolgten Migrationsschritts 4

Wie in Abschnitt 3.3 bereits beschrieben, stellt die Abbildung 9 die Zielstruktur des Campusnetzwerks nach abgeschlossener Migration dar. Das gesamte Core- und Access-Netzwerk besteht nun konsistent aus einer SDN-Struktur. Die SDN-fähigen Geräte können nun über das DNA-Center automatisiert konfiguriert werden. Das Management der benutzer-, gruppen- und gerätespezifischen Policies wird von der Cisco-ISE gesteuert und für die Endgeräte bereitgestellt. Die Benutzer können sich weiterhin an der AD anmelden und alle weiteren Netzwerkdienste, wie z.B. DNS und Lizenzservices, beziehen.

Die in diesem Kapitel mehrmals angesprochenen Systemüberprüfungen der einzelnen Migrationsschritte, sowie die Überprüfung des Gesamtsystems werden im nächsten Kapitel näher erläutert.

4.3 Systemtest und Systemabnahme

Nachdem alle erforderlichen Migrationsschritte durchgeführt sind, werden ein Test der Systeme sowie eine Abnahme des Gesamtsystems notwendig. Dieses Verfahren dient der Verifikation der Funktionen mit verschiedenen Geräten und Nutzungsklassen.

Im Abschnitt 4.1 wird empfohlen ein PoC durchzuführen. Die daraus folgenden Ergebnisse gelten als protokolliert und werden in diesem Punkt nicht weiter betrachtet. Der im Nachfolgenden beschriebene Systemtest stellt gemeinsam mit dem PoC eine zweistufige Abnahme dar, wie sie im Vorfeld mit dem Auftraggeber vereinbart wurde. Nach durchgeführtem PoC wird von einer Fehlerfreiheit der Hardware-Komponenten ausgegangen. Die folgenden Schritte der Abnahme werden gemeinsam mit dem Auftraggeber durchgeführt und sind ein Teil der Systemübergabe. Begonnen wird mit dem Liefernachweis der Einzelkomponenten, dieser beinhaltet folgende Punkte:

- Sichtprüfung auf Vollständigkeit und Beschädigungen,
- Erfassung der Seriennummern und ggf. Lizenz-Kennungen,
- Dokumentation zur Übernahme in eine Komponentenliste, die als Grundlage für den Servicevertrag benötigt wird.

Anschließend wird ein Test der Einzelsysteme durchgeführt, dazu gehören folgende Aufgaben:

- Ausführung der Selbsttestfunktionen,
- Überprüfen der Statusanzeigen,
- Nachweis über die Interoperabilität zu anderen Komponenten,
- Ausführung von systemspezifischen Funktionstests auf lokalen Komponenten,
- Test der Netzwerkverbindung (mit Hilfe des Internet-Control-Message-Protocols - ICMP),
- Dokumentation der Ergebnisse.

Als Nächstes wird ein Test des Gesamtsystems durchgeführt. Darin enthalten ist die Verifikation der Systemmerkmale und der Schnittstellenfunktionen zu den angrenzenden Kundensystemen. Im Leistungsfokus stehen folgende Aspekte:

- Feststellen der Applikationsfunktionalität,
- Failover-Test der Systeme und einzelner Systemredundanzen (bereits in PoC betrachtet),
- Feststellen der Umschaltzeiten (bereits in PoC betrachtet),
- Überprüfung der Funktionen der vereinbarten System- und Anwendungsroutinen,
- Auswertung von Log-Dateien,
- Ausführung von System-Reports des Netzbetreibers,
- Analyse der Realtime-Systemdaten des Netzmanagements,
- Durchführung von Backup- und Recovery-Funktionen,
- Dokumentation der Ergebnisse.

Des Weiteren werden Service- und Administrator-Accounts sowie Fernwartungszugänge eingerichtet und dem Netzbetreiber übergeben. Im Anschluss an die Systemabnahme wird eine Einweisung bzw. Schulung der IT-Mitarbeiter des Netzbetreibers durchgeführt.

4.4 Einweisung der Mitarbeiter in das neue Gesamtsystem

Anhand von theoretischen und praktischen Einheiten werden den IT-Mitarbeitern des Netzbetreibers Kenntnisse über die Sicherstellung des Regelbetriebs sowie die Durchführung von System- und Funktionserweiterungen im Campusnetzwerk vermittelt. Die SDN-Komponenten werden präsentiert und praktische Übungen daran durchgeführt. Nachfolgende Themengebiete stehen dabei im Fokus:

- Betriebssysteme einzelner Komponenten,
- typische Portkonfigurationen,
- der Einsatz verfügbarer Analyse- und Debugging-Funktionen zur Feststellung von Fehlerursachen,
- Betrieb des DNA-Centers (Management-Konsole),
- Implementierung von Automatisierungsroutinen,
- Etablierung der Sicherheitsfunktionen für den Regelbetrieb.

Diese Schulung vermittelt den IT-Mitarbeitern ausreichende Kenntnisse darüber, eigenständig Systemänderungen und -erweiterungen durchzuführen. Außerdem sollen sie zukünftig in der Lage sein, selbstständig Testreihen zur Fehlereingrenzung zu entwickeln und auszuführen.

5 Zusammenfassung

Das Ziel dieser Arbeit war die Erstellung eines Konzepts zur Migration einer Software-Defined-Network-Struktur in ein zeit- und businesskritisches Netzwerk. Dabei wurde eine Methode entwickelt, welche die vollständige Kompatibilität und Interoperabilität von SDN-Komponenten zueinander sowie zu klassischen Netzwerkelementen gewährleistet.
In Abschnitt 4.1 wurde ein Leitfaden erstellt, der Möglichkeiten aufzeigt, Interoperabilitäts- und Kompatibilitäts-Probleme zu erkennen und zu beheben. Außerdem wurden in diesem Abschnitt Funktionsanforderungen definiert, deren Überprüfung bei einer SDN-Migration zu empfohlen wird. Die Netzwerkmigration wurde in Abschnitt 4.2 schrittweise beschrieben. Dafür wurden in der Vorbetrachtung die einzelnen funktionalen und physikalischen (Installationsort) Abhängigkeiten analysiert und vier Migrationsschritte definiert. In diesen Schritten wurden funktionale Zusammenhänge einzelner Komponenten und Dienste dargestellt. Der entwickelte Ablauf dieser Migration schließt eine schrittweise Inbetriebnahme einzelner Komponentengruppen mit ein. Die Abschnitte 4.3 und 4.4 stellen die Übergabe des Gesamtsystems an den Auftraggeber dar. In Abschnitt 4.3 wurden die grundlegenden Inhalte der Systemabnahme und der darin enthaltenden Funktionsprüfungen beschrieben. Abschließend werden in Abschnitt 4.4 die Inhalte der fachlichen Einweisung für die IT-Mitarbeiter des Auftraggebers erläutert.
Zusammenfassend stellt sich dar, dass alle Anforderungen an die neue Netzstruktur erfüllt werden können. Auch für die im theoretischen SDN-Kontext beschriebenen Anwendungsvorteile werden Möglichkeiten der Integration geschaffen. Durch die Anbindung des Netzwerks an die vorgehaltenen Strukturen des Rechenzentrums entstehen Möglichkeiten der Cloud-Orchestrierung. Die Integration des Cisco-DNA-Centers in Kooperation mit den SDN-Controllern des Netzwerks schafft Lösungen für Load-Balancing und dynamische Routing-Anpassungen. Mit Hilfe des DNA-Centers werden Techniken des Verkehrs-Monitorings und des Netzmanagements integriert. Die Verwendung der VxLAN-Technologie erlaubt die simple Integration von Teststrukturen und virtuellen Netzen, was die Entwicklung von Test-Cases im bestehenden Netzwerk erleichtert. Die Grundlage für den Anwendungsfall der applikationsspezifischen Netzoptimierung wird in der neuen SDN-Struktur geschaffen. Abschließend ist zu erwähnen, dass dieses Dokument lediglich als Handlungsempfehlung verstanden anzusehen sein sollte und keinesfalls ein Standardkonzept für eine SDN-Migration darstellt.

6 Diskussion

In diesem Kapitel werden zwei Kern-Themen von SDN-Migrationen diskutiert: wirtschaftliche Aspekte sowie der Einsatz offener Standards.

Dazu wird die Studie „*Implications of the emerging technologies Software-Defined Networking and Network-Function-Virtualization on the future Telecommunications Landscape*“ empfohlen. Diese Studie behandelt die Themen SDN und NFV und analysiert die technologischen, ökonomischen und regulatorischen Auswirkungen unter Nutzung der Delphi-Methode. Die Delphi-Methode stellt eine systematische und mehrstufige Befragung dar und dient der Abschätzung zukünftiger Trends und Ereignisse. 700 qualifizierte Fachgrößen aus 55 Ländern nahmen an diesen Befragungen der Studie teil. In der Vergangenheit waren die Kostenersparnisse der ursprüngliche Grund für die Entstehung des Konzepts von SDN. Aufwendige proprietäre Hardware-Techniken bedingen stets hohe Investitionskosten. Die Studie konkretisiert u.a. die Auswirkungen auf die Verringerung von Capital-Expenditure (CapEx, Anlagevermögen) und Operational-Expenditure (OpEx, Betriebsausgaben). Die Ersparnisse der Gesamtkosten belaufen sich lediglich auf 3,7% bis 9%, was signifikant, aber dennoch unter den durch die Hersteller prognostizierten Bereichen liegt. [23]

Derzeit betont die Mehrheit der Hersteller von Netzwerktechniken die Offenheit ihrer SDN-Struktur. Wie im Abschnitt 2.1 beschrieben, meint der Begriff „Offenheit“ die Eigenschaften „Offenheit der Dienste“ und vorrangig die „Benutzung des offenen Standards Open-Flow“ für die Kommunikation in der Control-Plane. Diese Eigenschaften werden nur zum Teil erfüllt. Die Möglichkeit zur Integration verschiedener virtueller und skalierbarer Netzwerkanwendungen (z.B. Cloud-Applikationen medizinischer Software) und Netzwerkdienste (z.B. Domain-Controller, DNS) stellt einen sehr großen Vorteil von SDN dar und wird von allen Herstellern unterstützt. Die Verwendung von Open-Flow als Kommunikationsprotokoll in der Control-Plane wird hingegen nicht von allen Herstellern unterstützt. Viele Hersteller bemängeln, dass der Einsatz von Open-Source-Software in Kombination mit Open-Flow zu hohen Latenzen für die Kommunikation in der Control-Plane führt. Sie stellen diese Netzwerkfunktionen stattdessen, wie in Abschnitt 2 beschrieben, mit Hilfe speziell entwickelter ASICs und eigener Protokolle bereit. Diese Entwicklungen bedingen jedoch den konsistenten Aufbau innovativer Netzwerke mit Hardware-Komponenten des gleichen Herstellers. Aus Herstellersicht ist die Bindung der Kunden und Anwender an die eigene Hardware-Infrastruktur ein probates Mittel zur Erhaltung der Marktanteile. [24]

Die Praxis zeigt, dass die Auswahl des Hardware-Herstellers nicht ausschließlich wirtschaftliche bzw. technologische Hintergründe haben muss. Zusätzlich kann die Auswahl durch die eigenen Erfahrungen, das Fachwissen und evtl. durch die Zertifizierungen der Administratoren und Systemingenieure begründet sein.

Für die Entwicklung zukunftsfähiger Netzwerke und Migrationen von SDN-Strukturen in zeitkritische und hochverfügbare Netze wird für die Auswahl der Hardware-Komponenten stets die Open-Flow-Kompatibilität empfohlen. Der offene Standard dieses Protokolls stellt sehr gute Möglichkeiten der Interoperabilität von Hardware-Komponenten unterschiedlicher Hersteller bereit.

Sobald der Hersteller-Support der bestehenden Komponenten endet, wird eine Migration von SDN-Strukturen in das bestehende Netzwerk empfohlen. Eine durch SDN und NFV geprägte Telekommunikationslandschaft kann die Entwicklung und Verbreitung neuer Dienste, Anwendungen und Produkte beeinflussen sowie erheblichen ökonomischen und gesellschaftlichen Einfluss haben.

7 Ausblick

In der Zukunft sollte bezüglich der Entwicklung, Verwendung und Migration von SDN-Strukturen daraufhin gearbeitet werden, einen größeren Fokus auf die Verwendung herstellerübergreifender Protokolle, wie z.B. Open-Flow und IS-IS zu legen. Gegenwärtig finden diese Anforderungen bei nur wenigen Netzwerkausrüstern Akzeptanz. Durch die Zunahme der Endgeräteanzahl, bedingt durch Industrie 4.0 und IoT, und der damit verbundenen größer werdenden geforderten Dynamik innerhalb der Netzwerke wird die Verbreitung von SDN-Strukturen zunehmen und somit eine herstellerübergreifende Kompatibilität der SDN-Komponenten bedeutsamer. Dadurch könnten Konzeptionierungen und Inbetriebnahmen solcher Systeme planbarer gestaltet und auftretende Störungen verringert werden.
Des Weiteren arbeitet derzeit ein Forschungskonsortium in Kooperation mit der SBSK GmbH & Co. KG in dem VDI/VDE-geförderten Forschungsprojekt „MONAT“ [25] daran, neue Anforderungen, Protokoll-Unterstützungen, Anwendungen und Merkmale zu spezifizieren, wodurch die Interoperabilität zwischen SDN-Netzwerkelementen verbessert werden kann. Ein Ziel dieses Projekts ist die Entwicklung einer Möglichkeit zum kombinierten policy- und applikationsabhängigen Forwardings. Weiterhin werden Test- und Use-Cases entwickelt, welche durch eine Migration einer SDN-Struktur entstehen können.
Im Jahr 2004 wurde eine Prognose veröffentlicht [26], welche einen jährlichen Zuwachs des Bandbreitenbedarfs für Privatkunden um 60% voraus sagt. Die zu diesem Zeitpunkt prognostizierten Werte für den Bandbreitenbedarf (in 2006 – 4MBit/s; 2010 – 20 MBit/s, jeweils im Downstream) sollten sich bewahrheiten. Gegenwärtig sagt die „Breitbandstudie 2018“ [27] des Bundesverbands für Breitbandkommunikation e.V. (BREKO) einen Bandbreitenbedarf von 1000 MBit/s im Downstream und 700 MBit/s im Upstream für das Jahr 2025 voraus. Pro Privatkunden-Anschluss wird zu diesem Zeitpunkt ein monatliches Datenvolumen von 825 GByte erwartet. Diese Zahlen stellen ausschließlich die Verkehrslasten aus dem Privatkundenbereich dar. Im Geschäftskundenbereich ist durch die in dieser Arbeit erwähnten Use-Cases ebenfalls ein steigender Bandbreitenbedarf zu erwarten. Hinzu kommen Meinungen verschiedener branchenansässiger Unternehmen, die besagen, dass zukünftige Breitbandanschlüsse nicht mehr ausschließlich anhand der Brandbreite, sondern vielmehr nach Latenz-Anforderungen vermarktet werden. Diese deutlich steigenden Anforderungen sind ein Beleg für die Notwendigkeit der Weiterentwicklung von SDN im LAN-, WAN- und Cloud-

Bereich sowie für den hohen Bedarf der dienstgerechten Bereitstellung von breitbandigen, hochverfügbaren Teilnehmeranschlüssen und Netzen mit niedriger Latenz.

8 Literatur

[1] Projektgruppe ARD/ZDF-Multimedia, „ARD ZDF Onlinestudie 2017," 2017.

[2] AGOF e.V., „digital facts 2017-01," 2017.

[3] Branchenverband Bitkom, „Bedeutung des Internets für die Wirtschaft," [Online]. Available: https://www.deutschlandfunk.de/die-bedeutung-des-internets-fuer-die-wirtschaft.769.de.html?dram:article_id=114898. [Zugriff am 03 12 2018].

[4] Citrix Systems GmbH, „SDN 101: Einführung in softwaredefiniertes Networking," 2014.

[5] E. B. Schweißguth, Entwicklung und Evaluierung eines SDN-gestützten echtzeitfähigen Gerätenetzwerks, Wiesbaden: Springer Vieweg, 2016.

[6] U. Trick und F. Weber, SIP und Telekommunikationsnetze: Next Generation Networks und Multimedia over IP, München: de Gruyter Oldenburg, 2015.

[7] B. G. Assefa und O. Ozkasap, „State-of-the-art Energy Efficency Approaches in Software Definded Networking," 2015.

[8] Open Networking Foundation, „SDN architecture," 2014.

[9] M. Chiosi, D. Clarke, P. Willis, et. al., „Network Functions Virtualization," Darmstadt, 2012.

[10] G. Siegmund, Next Generation Networks, Hüthig, 2002.

[11] Cisco Systems Inc., „Locator/ID Separation Protocol Architecture," 2011.

[12] Cisco Systems Inc., „Cisco Locator/ID Separation Protocol," 2012.

[13] D. Farinacci, V. Fuller, D. Meyer und D. Lewis, „The Locator/ID Separation Protocol (LISP)," 2013.

[14] D. Farinacci, D. Meyer, J. Zwiebel und S. Venaas, „The Locator/ID Separation Protocol (LISP) for Multicast Environments," 2013.

[15] D. Lewis, D. Meyer, D. Farinacci und V. Fuller, „Interworking between Locator/ID Separation Protocol (LISP) and None-LISP SItes," 2013.

[16] V. Fuller und D. Farinacci, „Locator/ID Separation Protocol (LISP) Map-Server Interface,“ 2013.

[17] L. Iannone, D. Saucez und O. Bonaventure, „Locator/ID Separation Protocol (LISP) Map-Versioning,“ 2013.

[18] D. Farinacci und D. Meyer, „The Locator/ID Separation Protocol Internet Groper (LIG),“ 2013.

[19] V. Fuller, D. Farinacci, D. Meyer und D. Lewis, „Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT),“ 2013.

[20] S. M. H. Naqvi, „Overview and Design of VXLAN,“ 2016.

[21] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell und C. Wright, „Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks,“ 2014.

[22] V. Jung und H.-J. Warnecke, Handbuch für die Telekommunikation, Berlin: Springer Verlag, 2002.

[23] R. Arnold, et. al., „Implications of the emerging technologies Software-Defined Networking and Network Function Virtualization on the future Telecommunications Landscape,“ 2016.

[24] A. Krüger, „Kampf um den Netzwerkmarkt voll entbrannt – Cisco präsentiert seine SDN-Alternative,“ 7 1 2014. [Online]. Available: https://www.silicon.de/41593556/cisco-praesentiert-sdn-alternative-netzwerk?inf_by=54db0b770ce58a4fc15dc13d. [Zugriff am 07 12 2018].

[25] SBSK GMBH & Co. KG, „Modellbasierte und bedarfsgerechte Netzwerkkonfiguration für Netzwerke der Automatisierung und Telekommunikation,“ 01 05 2018. [Online]. Available: www.forschungsprojekt-monat.de. [Zugriff am 03 12 2018].

[26] A. Bluschke, Zugangsnetze für die Telekommunikation, München: Hanser Verlag, 2004.

[27] Bundesverband für Breitbandkommunikation e.V., „Breitbandstudie 2018,“ 2018.

9 Abbildungsverzeichnis

10 Abkürzungsverzeichnis

A-CPI	Application-Controller Plane Interface
AD	Active Directory
ALT	Alternative Topology Device
API	Application Programming Interface
ASIC	Application Specific Integrated Circiut
BGP	Boarder Gateway Protocol
BK	Breitbandkabel
BREKO	Bundesverbands für Breitbandkommunikation
CapEx	Capital Expenditure
CPI	Controller Plane Interfaces
D-CPI	Data-Controller Plane Interfaces
DFN	Deutsches Forschungsnetzwerk
DNA	Digital Network Architecture
DNS	Domain Name Service
Dst	Destination
E2E	Ende zu Ende
ECMP	Equal-cost multipath
EID	Endpoint Identifier
ETR	Egress Tunnel Router
ForCES	Forwarding and Control Element Separation
GbE	Gigabit Ethernet
GByte	Gigabyte
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IP-TV	IP-vermitteltes Fernsehen
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISE	Identity Service Engine
ISG	Industry Specification Group

ISIS	Intermediate System to Intermediate System
IT	Informationstechnik
ITR	Ingress Tunnel Router
LAN	Local Area Network
LISP	Locator/ID Separation Protocol
LWL	Lichtwellenleiter
M2M	Machine to Machine
MAC	Media Access Control
MBit/s	Megabit pro Sekunde
MONAT	Modelbasierte und bedarfsgerechte Netzwerkkonfiguration für Netzwerke der Automation und Telekommunikation
MPLS	Multi Protocol Label Switching
MR	Map Resolver
MS	Map Server
NAC	Network Access Control
NF	Network Function
NFV	Network Function Virtualization
NGN	Next Generation Network
HW	Hardware
OH	Outer Header
OpEx	Operational Expenditure
OSPF	Open Shortest Path First
OSS	Operations Support System
PETR	Proxy Egress Tunnel Router
PITR	Proxy Ingress Tunnel Router
PNF	Physical Network Function
PoC	Proof of Concept
QoS	Quality of Service
RFC	Request for Comments
RLOC	Routing Locator
SDN	Software Defined Network
SLA	Service Level Agreements
Src	Source
STP	Spanning Tree Protocol

SW	Software
TLS	Transport Layer Security
UDP	User Datagram Protocol
VDE	Verband der Elektrotechnik Elektronik Informationstechnik
VDI	Verein Deutscher Ingenieure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
VoIP	Voice over IP
VTEP	VxLAN Tunnel Endpoints
VxLAN	Virtual extensible Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network