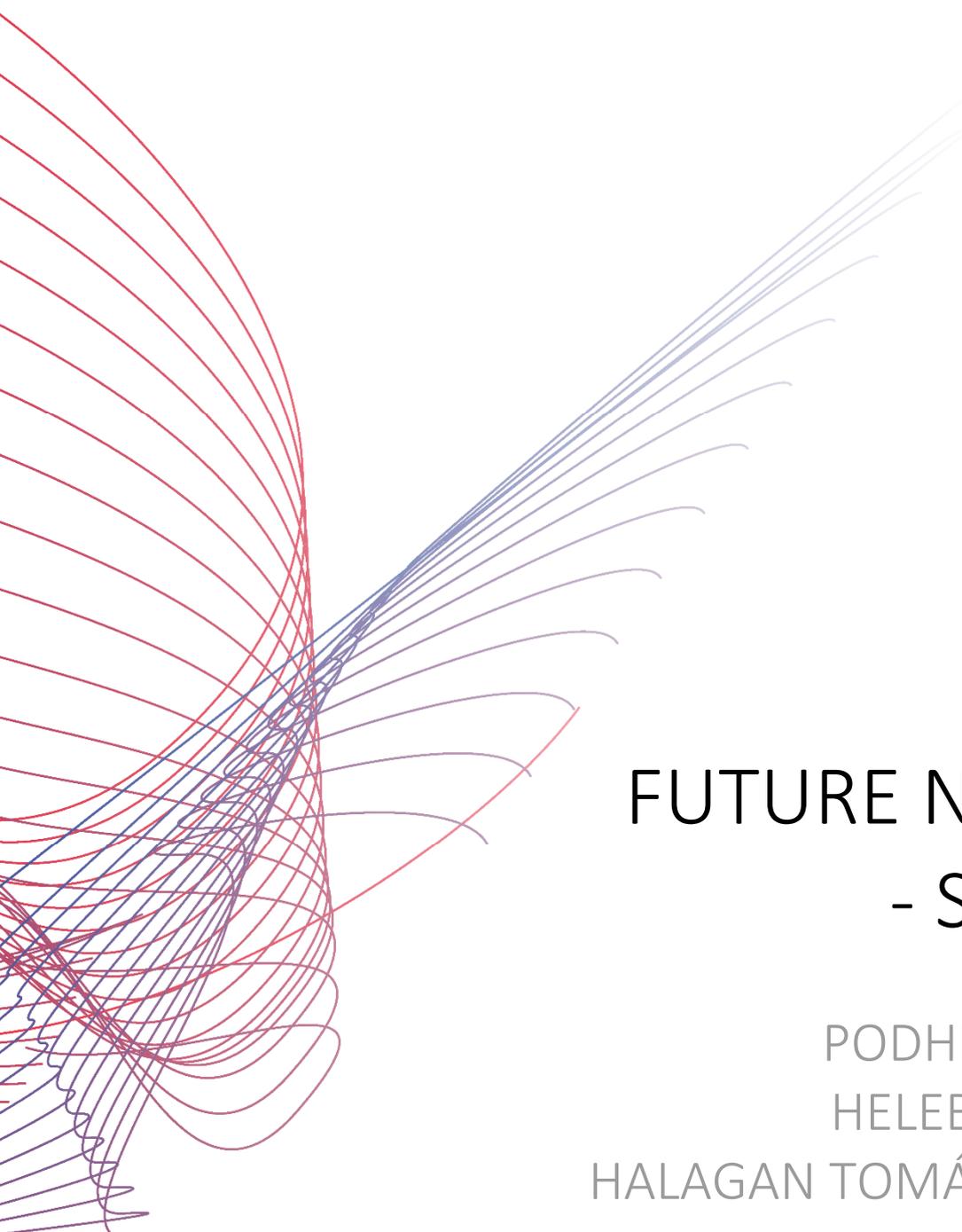




TECH pedia



FUTURE NETWORKS - SDN & NFV

PODHRADSKÝ PAVOL,
HELEBRANDT PAVOL,
HALAGAN TOMÁŠ, DROZD IVAN

Titel der Arbeit: Future Networks - SDN & NFV
Author: Podhradský Pavol, Helebrandt Pavol,
Halagan Tomáš, Drozd Ivan
Übersetzt (von): Radoslav Vargic
Veröffentlicht (von): České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktadresse: Technicka 2, Prague 6, Czech Republic
Tel.: +420 224352084
Drucken: (nur elektronisch)
Anzahl der Seiten: 41
Ausgabe: 1. Ausgabe, 2017
ISBN 978-80-01-06248-7

TechPedia

European Virtual Learning Platform for
Electrical and Information Engineering

<http://www.techpedia.eu>



Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ERLÄUTERUNG



Definition(en)



Interessantheit (Interessantes)



Bemerkung



Beispiel



Zusammenfassung



Vorteile



Nachteile

ZUSAMMENFASSUNG

Das aktuelle Internet basiert noch immer auf einem Internetprotokoll das vor mehr als 40 Jahren für bestimmte Gruppe von Diensten definiert wurde. In den zurückliegenden Jahrzehnten hat das Internet enorme Dimensionen angenommen. Man hat auch nicht mit neuen Anwendungen wie Web, Video-Streaming und Dateifreigabe gerechnet, die die Art des Internet-Verkehrs wesentlich verändert haben. Die Infrastruktur des Internets hat sich durch neue Technologien von festen optischen Netzwerken zu drahtlosen Netzwerken entwickelt. Neue Anwendungen, Dienstleistungen und Technologien sowie die Menge und Variabilität der Endgeräte erfordern flexible Lösungen. Es scheint dass die anspruchsvollsten Lösungen diejenigen sind, welche die Zusammenschaltung von Software definierten Netzwerken und die Virtualisierung von Netzwerkdiensten beinhalten. Dieses Modul konzentriert sich hauptsächlich auf diese vielversprechenden Technologien für Future Internet und gibt auch einen Überblick über die Netze der nächsten Generation.

ZIELE

Hauptziel dieses Kurses ist es, grundlegende Kenntnisse über neue Trends bei den der Informations- und Kommunikationstechnologien, vor allem über die aktuelle Entwicklung der Netze in Richtung Zukunftsnetze sowie Future Internet zu erwerben. Die Teilnehmer lernen die grundlegenden Eigenschaften der Next Generation Networks. Doch das Wichtigste ist, dass sie mit dem Wissen über modernste Technologien wie Software definierte Netzwerke und die Virtualisierung von Netzwerk-Funktionen (aus der Sicht der Grundarchitektur, das Prinzip und die Protokolle) umgehen werden. Die Aufmerksamkeit ist dabei auf aktuelle Anforderungen und Einschränkungen des Future Internet gerichtet.

LITERATUR

- [1] Mikoczy, E., Kotuliak, I., van Deventer, M. O.: Evolution of the converged NGN service platforms towards Future Networks. in Future Internet Journal, special issue Special Issue "Network vs. Application Based Solutions for NGN", 2011, ISSN 1999-5903.
- [2] Mikoczy, E.: Next Generation of Multimedia Services in Context of Future Networks. In Proceedings of ETSI Future Network Technologies Workshop, Sophia Antipolis, France, 10–11 March 2010.
- [3] Podhradský, P., Mikóczy, E., Lábaj, O., Londák, J., Trúchly, P., et al: NGN Architectures and NGN Protocols. LdV IntEleCT, Educational publication, 210 pages, Published by ČVUT Praha, ISBN: ISBN:978-80-01-04949-5, September 2011, CD version.

- [4] Podhradský, P., Mikóczy, E., Dúha, J., Trúchly, P., at al: NGN – Selected topics, LdV IMProVET.Educational publication, 137 pages, Published by ČVUT Praha, ISBN: 978-80-01-05295-2, August 2013, CD versions (SK, EN, CZ).
- [5] Nadeau, T. D., Gray, K.: SDN: Software Defined Networks. O'Reilly Media. 2013. ISBN: 978-1-449-34230-2.
- [6] Helebrandt, P., Kotuliak, I.: Novel SDN multi-domain architecture. In IEEE 12th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp.139-143, 2014.
- [7] Open Networking Foundation: Software-Defined Networking: The New Norm for Networks. White Paper, 2012
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>.
- [8] McKeown, N.: OpenFlow and Software Defined Networks. online, Presentation. 2011
http://www.openflow.org/documents/OpenFlow_2011.pps.
- [9] Open Networking Foundation. <https://www.opennetworking.org>.
- [10] McKeown, N. et al.: OpenFlow: Enabling innovation in campus networks. In: ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp.69-74, 2008.
- [11] Open Networking Foundation: OpenFlow Switch Specification version 1.3.5. 2015
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.3.5.pdf>.
- [12] Dong; L., Gopal, R., Halpern, J.: Forwarding and Control Element Separation (ForCES) Protocol Specification. IETF RFC 5810, 2010.
- [13] Chiosi, M., Clarke, D., Willis, P., Reid, A., Feger, J., Bugenhagen, M., Khan, W., at al.: Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action. SDN and OpenFlow World Congress, 2012.
https://portal.etsi.org/nfv/nfv_white_paper.pdf.
- [14] Chiosi, M., Wright, S., Clarke, D., Willis, P., at al.: Network Functions Virtualisation: Network Operator Perspectives on Industry Progress. SDN and OpenFlow World Congress, 2013. https://portal.etsi.org/nfv/nfv_white_paper2.pdf.
- [15] ETSI GS NFV-INF 001 V1.1.1, Network Functions Virtualisation: Infrastructure Overview. Specification, 2015. http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf.
- [16] ETSI GS NFV-MAN 001 V1.1.1, Network Functions Virtualisation: Management and Orchestration. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf.

- [17] ETSI GS NFV-SWA 001 V1.1.1, Network Functions Virtualisation: Virtual Network Functions Architecture. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf.
- [18] SdxCentral:Network Functions Virtualization Report. 2015. <https://www.sdxcentral.com/reports/network-functions-virtualization-report-2015/>.
- [19] Gruber C. G.: CAPEX and OPEX in Aggregation and Core Networks. In: Optical Fiber Communication, IEEE, 2009, pp. 1-3.
- [20] Strategy Analytics: Global Internet Device Installed Base Forecast. August 2014. <https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609>.
- [21] Wu, Y. et al.: CloudMoV: Cloud-Based Mobile Social TV. In: IEEE Transactions on Multimedia, vol.15, 2013, pp. 821-832.
- [22] Roberts, J.: The clean-slate approach to future Internet design: a survey of research initiatives. *annals of telecommunications - annales des télécommunications*, Volume 64, Issue 5, 2009. pp 271-276.
- [23] Banniza, T.R., Boettle, D., Klotsche, R., Schefczik, P., Soellner, M., Wuenstel, K.: A European Approach to a Clean Slate Design for the Future Internet. *Bell Labs Technical Journal - Core and Wireless Networks*, Volume 14 Issue 2, August 2009. pp. 5-22.
- [24] McKeown, N. et al.: Openflow: Enabling innovation in campus networks. In: *SIGCOMM Computer Communication Review*, vol.38, no.2, 2008, pp. 69-74.
- [25] Bashker, D., Cascio, W., Boudreau, J.: *How to Apply HR Financial Strategies (Collection)*, Addison Wesley. Chapter 1, August 2013, ISBN 9780133743173. pp. 6-10.
- [26] Barroso, L. A., Clidaras, J., Hölzle, U.: *The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines - Second Edition*. Morgan & Claypool. Chapter 6., pp. 69-71, 2013, ISBN 9781627050104.
- [27] Tits, Y.: Lack of standardization concerning interfaces between network equipments. In: *Electricity Distribution (CIRED 2013)*, 22nd International Conference and Exhibition on, IET, 2013, pp. 1-4.
- [28] McKeown, N., Girod, B.: *Clean-Slate Design for the Internet A Research Program at Stanford University*. White paper Version 2.0, 18 April 2006.

Inhaltsverzeichnis

1	Einleitung	8
2	NGN-Architektur Entwicklung in Richtung Future Network Architekturen	9
2.1	NGN-Konzepte und Architekturen	11
2.2	Schicht Konzeptmodel	13
3	Software definierte Netzwerke (SDN)	14
3.1	Einführung in die SDN	14
3.2	Die Trennung von Netzwerksteuerung und Datenweiterleitungsschicht	16
3.3	Zentrale Steuerung und Netzwerk-Programmierbarkeit	18
3.4	Vergleich der verteilten Steuerungsschicht mit traditionellen Netzwerken	19
3.5	SDN Protokolle	21
4	Network Functions Virtualisation (NFV)	25
4.1	Was hat NSF ermöglicht?	27
4.2	Anforderungen an NFV	28
4.3	NFV-Architektur	29
4.4	Infrastructure NFV – NFVI	31
4.5	Verwaltung und Orchestrierung NFV (MANO)	32
4.6	VNF-Software-Architektur	33
4.7	Anwendungsfälle für NFV	34
5	Zukunft des Internet	36
5.1	Einschränkungen des Internets	37
5.2	Eigenschaften des neuen Internet	39
5.3	Neugestaltung der Internet-Technologien	40

1 Einleitung

Ein neues Thema im Bereich der Informations- und Kommunikationstechnologien ist die Weiterentwicklung der **NGN** (*Next Generation Networks*) Technologien in Richtung zukünftiger Netze. Es gibt verschiedene Aspekte, welche die aktuelle IMS basierte NGN-Architektur beeinflussen, um zusätzliche Funktionalitäten für die nächste Generation von Multimedia-Diensten zu verbessern. Die schnelle Entwicklung von Internet-Diensten und Content-Delivery-Services über heterogene Netze ändert die Anforderungen unterschiedliche Aspekte wie zusätzliche Funktionalitäten, Mobilität, Virtualisierung und gemeinsame Nutzung von Ressourcen, Sicherheit, Vereinfachung der Architektur und der Flexibilität bei der Steuerung von Modellen mit Kontextsensitivität.

Gegenwärtig werden Diskussionen in Forschungsprojekten und dem Standardisierungs-Organisationen (ITU-T, ETSI) geführt, die zu Änderungen der Architektur des Internet auf dem Gebiet der Telekommunikation für zukünftige Netze (Future Networks - FN) führen.

2 NGN-Architektur Entwicklung in Richtung Future Network Architekturen

Es wurden zwei Hauptströme der potenziellen Entwicklung identifiziert:

1. Unbeschriebene Tafel oder revolutionäres Konzept, d.h. zukünftiges Internet, wo Architektur und Protokolle für zukünftiges Internet neu definiert und gestaltet (Netzwerkszenarien, Modelle neuer Protokolle und Prüfung der revolutionären Architektur-Modi), werden [1]. Der revolutionäre Sprung erwartet, das Internet wird technologisch neu konzipiert und wird nicht durch gegenwärtigen Konzepten begrenzt.
2. Evolutionäres Konzept, bei dem bestehende NGN Architekturen durch neue Anforderungen und Funktionen verbessert werden, die zu einem Konzept namens zukünftige Netze [1], [2] führen. NGN-Evolution kann die erwarteten Fähigkeiten zukünftiger Netze mit Hilfe von vorhandenen Protokollen und Fähigkeiten der NGN erreichen (ermöglicht durch notwendige Verbesserung von Architektur und Kontrollmechanismen).

Das zweite Konzept ist ein realistischer Ansatz für zukünftige Netzwerke aus der Sicht der Migration, in dem NGN-Netze und Technologien bereits verfügbar sind.

Es ist zweckmäßig, die Evolution anzuschauen und zukünftige Trends der NGN und die zu lösenden Fragen zu skizzieren. Migrationsszenarien der verschiedenen Arten von Netzwerk-Plattformen basieren auf der Idee, die TDM- und IP-Plattformen in eine konvergente NGN-Plattform (unter dem Aspekt von Netzwerkinfrastruktur sowie Dienstleistungen) zu integrieren. Neue Konzepte und Architekturen der zukünftigen Generation von IKT auf der Basis konvergenter IKT und NGN-Betreiber bieten neue Möglichkeiten um breites Spektrum an Multimedia-Diensten und Anwendungen zu implementieren.

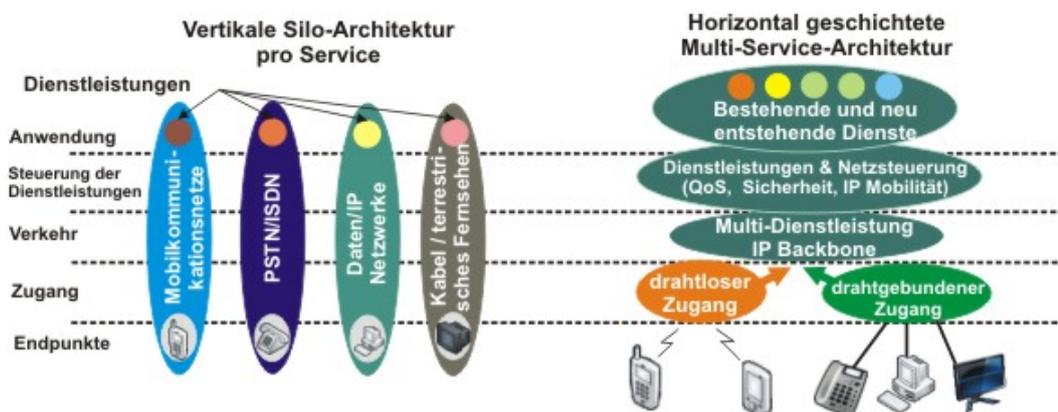


Abbildung 1 - Von vertikalen Silos auf horizontale NGN-Architektur [1]



Daher können Betreiber die vertikale Silo-Architektur, bei der jede Art von Service dedizierten Zugang, Transport, Kontrolle und Anwendungsinfrastruktur pro Dienst benötigt, unabhängig von den erbrachten Leistungen, in eine horizontal orientierte Architektur wechseln, (Abb. 1) .

2.1 NGN-Konzepte und Architekturen

Die wichtigsten Grundsätze des NGSS (Next Generation Networks) wurden festgelegt, als die Idee des NGN selbst entstand. Die nächsten beiden Definitionen von ETSI und ITU-T beschreiben die Grundlagen des NGN.



$E=m \cdot c^2$

ETSI beschreibt NGN als Konzept für die Definition und Festlegung der Netze, das die formale Verteilung von Funktionalitäten in separaten Schichten durch Verwendung von offenen Schnittstellen erlaubt. Das NGN-Konzept bietet neue Bedingungen für die Erstellung, Umsetzung und das effektive Management von innovativen Dienstleistungen. ITU-T beschreibt NGN als Netzwerk auf der Basis von Paketübertragung. Es ermöglicht den Dienstleistungsverkehr, einschließlich der Telekommunikationsdienstleistungen und ist in der Lage mit mehreren Breitband-Übertragungstechnologien zu arbeiten und inklusive einer QoS Garantie. Die Dienstfunktionen sind gleichzeitig unabhängig von den Grundübertragungstechnologien. NGN bietet unbegrenzten Benutzerzugriff auf verschiedene Dienstleistungen. Es unterstützt die allgemeine Mobilität und bietet dem Benutzer die Konsistenz und die Verfügbarkeit der Dienstleistungen.

Erwähnenswert sind einige Voraussetzungen für NGN. Sie sollten sich anpassen an:

- Hochleistungs-Paketübertragung innerhalb der Übertragungsinfrastruktur
- Trennung der Verwaltungsfunktionen von Übertragungsfunktionen
- Trennung der Dienstbereitstellung vom Netz
- Unterstützung einer breiten Palette von Dienstleistungen und Anwendungen
- Breitbandfunktionen und gleichzeitige Einhaltung der Anforderungen für **QoS** (*Quality of Services*)
- Verschiedene Arten von Mobilität (Benutzer, Terminals, Dienstleistungen)
- Konvergente Dienstleistungen zwischen Fest- und Mobilnetz (sowie Sprach-, Daten- und Video-Konvergenz)
- Übereinstimmung mit den Regulierungsanforderungen wie Notrufe und Sicherheitsanforderungen
- Billige und effektive Technologien

Innerhalb der NGN-Konzepte lösen die Normungsinstitute folgende Fragen und Probleme:

- 
- bestehende Netzwerke Migration zu NGN
 - Entwicklung auf dem Gebiet der Zugangstechnologien
 - Anschluss von anderen Netzwerken zu IP-Netzwerken

- Erbringung und die Entwicklung neuer Dienstleistungen
- Interworking im Bereich der Adressierung
- Interworking von Signalanlagen
- Roaming und Mobilität

Es gibt viele Denkmodelle und Referenzarchitekturen für, die konvergente Netzwerke und VoIP-Architekturen. Deshalb haben wir versucht, Gemeinsamkeiten zu finden und ein geeignetes Modell für NGN zu definieren. Ein Ziel des konzeptionellen Modelles ist es, Funktionsschichten (ähnlicher Funktionalitäten), ihre Einrichtungen, Referenzpunkte (Interfaces) und Informationsfluss zwischen ihnen zu bestimmen. Ein solches Modell kann dann leichter in der physikalischen Referenzarchitektur abgebildet werden (und ist unabhängig von den physikalischen Einheiten, d. h. Komponenten der Architektur).



In den meisten analysierten Fällen sind die NGN konzeptionelle Modell-Schichten, aus der Sicht der Funktionalitäten in unabhängige Teile aufgeteilt wie folgt (Abb. 2): Zugang (einige Referenzarchitekturen beinhalten den Zugang nicht direkt in dem NGN-Modell oder ersetzen ihn durch die Anpassung), Verkehr (Übertragung, Umschaltung), Kontrolle (Anruf / Sitzungskontrolle) und Anwendung (Dienstleistungen).

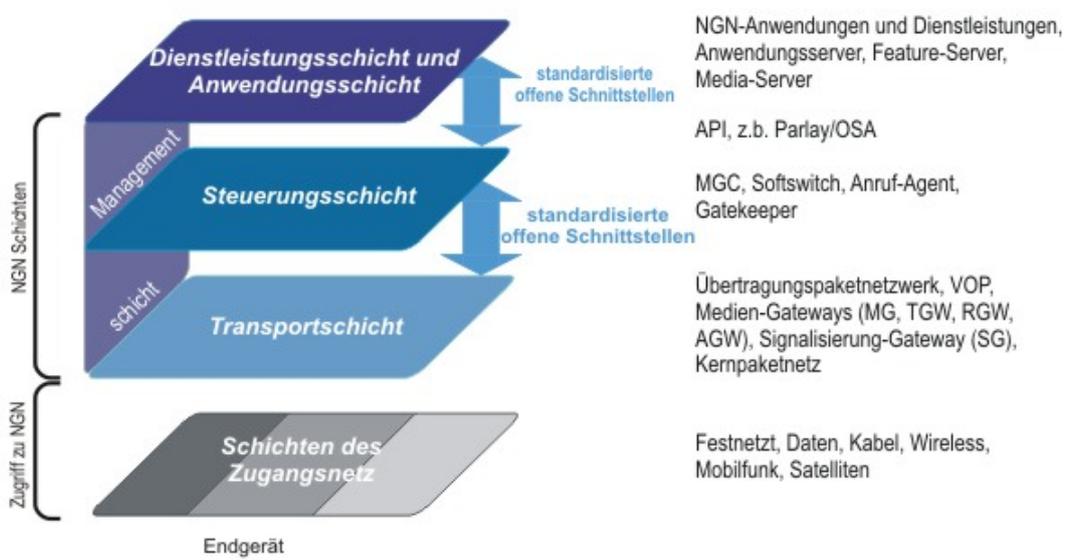


Abbildung 2 - NGN konzeptionelles Modell und seine Funktionsschichten

2.2 Schicht Konzeptmodell



Die **Zugriffsschicht** bietet die Infrastruktur an, beispielsweise ein Zugangsnetz zwischen dem Endbenutzer und dem Transportnetzwerk.

Die **Transportschicht** sorgt für den Transport zwischen den einzelnen Knoten des Netzwerks.

Die **Steuerungsschicht** umfasst die Steuerung von Dienstleistungen und Netzelementen. Diese Schicht ist für Set-up / Festlegung, Kontrolle und Rücknahme der Multimedia-Sitzung verantwortlich.

Die **Service-Schicht** bietet grundlegende Service-Funktionen, die verwendet werden können, um komplexere und anspruchsvollere Dienstleistungen und Anwendungen zu erstellen.

Im NGN ist es erforderlich, dass die Netzwerksteuerung nicht nur durch die Endgeräte-Anwendungen bestimmt ist, sondern dass die Netzwerk-Intelligenz die Kontrolle über das Netzwerk auf allen Schichten des Referenzmodells durchführen kann. Das Netzwerkmanagement-Referenzmodell beinhaltet die folgenden Aufgaben für die Netzwerk-Intelligenz hat, um sicherzustellen:

- Ressourcenmanagement (Kapazität, Ports und physikalische Elemente) und QoS beim Zugang zum Netzwerk und im Transportnetz.
- Verschiedene Arten von Medienverarbeitung, Codierung und Datenübertragung (Informationsfluss).
- Management der Anrufe und des Anschlusses. Management und Interworking aller Elemente der Referenzarchitektur.
- Dienstleistung-Kontrolle

Das NGN-Konzept und die Architekturen sind detailliert in [3], [4] beschrieben.

Es gibt verschiedene Konzepte und Entwicklungstrends, welche zu neuen Netzwerkarchitekturen führen, die in der Lage sind, das breite Spektrum / Portfolio neuer Multimedia-Dienste / Multimedia-Inhalte zur Verfügung zu stellen.

Neue Netzwerkarchitekturen auf Basis von "Software definierten Netzwerken" und "Netzwerkfunktionen Virtualisierung" werden in Kapitel 3 bzw. 4 und im "Future Internet" Konzept in Kapitel 5 dieses "Lernmoduls" vorgestellt.

3 Software definierte Netzwerke (SDN)

3.1 Einführung in die SDN

$E=m \cdot c^2$

Software definierte Netzwerke sind ein neuartiges Paradigma in der Computer-Netzwerk-Architektur mit dem Ziel, das gesamte Netzwerk mit Programmen zu steuern.

Dies ermöglicht die Lösung vieler Probleme in den traditionellen Ansätzen zur Vernetzung aber auch neue Funktionen. Die Hauptmotivation von SDN ist es, die Flexibilität, Verwaltbarkeit und Erweiterbarkeit der Computer-Verbindungen zu erhöhen und in der Folge auch die Gerätekosten zu reduzieren. Im Gegensatz zu teurer spezialisierter Netzwerkhardware wird dies durch eine schnelle Entwicklung und kurze Bereitstellungs-Zyklen, zu kostengünstigeren Software-Anwendungen führen.

Anfangs kam die Hauptmotivation für SDN von der Notwendigkeit bessere Lösungen für die Netzwerk Forschung und Entwicklung zu finden. Zu dieser Zeit gab es nur zwei verfügbare Methoden, um neue Funktionen zu testen - Softwaresimulation oder Hardware-Testumgebungen.

+

Die Simulation bietet eine gute Flexibilität und Reproduzierbarkeit.

-

Allerdings werden Simulationen in der Regel nicht in Echtzeit mit dem Produktions-Code ausgeführt, und es ist nicht leicht, ein simuliertes Netzwerk mit einem echtes Netzwerk zu verbinden und die Koexistenz der neuen Funktionen in einer realistischen Umgebung zu testen. Auf der anderen Seite sind Testumgebungen zur Implementierung benutzerdefinierter Hardware schwierig zu programmieren, und wenn sie einmal eingerichtet wurden, dann sind Änderungen schwierig und teuer.

Für die genannten Probleme sind zwei Lösungen denkbar. Entweder ein gemeinsames Testbed nutzen, welches mehrere Forschungsprojekte verwenden (wobei die Zeit für Experimente und Wiederholbarkeit begrenzt ist), oder alternativ, mit der Schaffung einer eigenen Testumgebung mit traditionellen Netzwerkgeräten von einem Equipmentanbieter. Diese werden meist als Black Box mit minimaler Anpassung geliefert. Das begrenzt allerdings die Testbed-Funktionen für neue und exotische Experimente, die für revolutionäre Innovationen erforderlich sind.

Jedoch hat sich die Rechenleistung von Mehrzweckcomputern in den späten 90er und frühen 2000er Jahren, deutlich erhöht im Vergleich mit der spezialisierten Netzwerkhardware. Dieser Umstand in Verbindung mit Fortschritten in der Virtualisierung und ein paar andern Technologien führen zu ihrer Verwendung als Software, die Kontrolle über einfache Netzwerkknoten für den schnellen Paketvermittlung implementiert. Steuersoftware kann wie in einer Simulation schnell angepasst werden. Kostengünstige Hardware mit begrenzten Funktionen für die Paketvermittlung bietet eine Paketumschlagleistung vergleichbar mit

benutzerdefinierten Hardware-Testumgebungen an. Dies ist eine der zentralen Säulen der SDN und besteht aus der Trennung von Steuer- und Weiterleitungsschicht und ist im größeren Detail im folgenden Abschnitt und [5] beschrieben.

3.2 Die Trennung von Netzwerksteuerung und Datenweiterleitungsschicht

Bevor wir die Feinheiten der SDN betrachten, müssen wir definieren, was Steuerungsschicht und Datenweiterleitungsschicht sind.

$E=m \cdot c^2$

In den meisten Routern (oder eine der diesbezüglichen Netzwerkausrüstungen) gibt es eine spezielle Hardware für den schnellen Austausch von Daten zwischen den Schnittstellen - Datenweiterleitungsschicht. Die Weiterleitung wird durch Regeln der Routing-Algorithmen realisiert,-- von einem Prozessor auf dem Betriebssystem wie die Adressübersetzung und andere höhere Funktionen -- das ist die Steuerungsschicht.

i

Im traditionellen Networking sind beide Steuerungsschicht und Datenweiterleitungsschicht in jedem Netzwerkknoten implementiert.

Dies ergibt sich aus der Herkunft des Internet - ARPANET, das zunächst durch und für das Militär konzipiert war, wobei der Schwerpunkt auf hoher Ausfallsicherheit und Überlebensfähigkeit lag. Flexibilität, einfache Änderung oder Einführung neuer Funktionen waren sekundäre Ziele.

Das Grundprinzip der SDN ist die Trennung von Steuer- und Datenweiterleitungsschicht im Netzwerk, wie in Abbildung 3 dargestellt ist. Durch die Implementierung von getrennter Steuerungsschicht (Software für Allzweckcomputer) und Daten-Weiterleitungsschicht (Netzwerk-Ausrüstung), ist es möglich, Routing- und Switching-Entscheidungen sowie die Konfiguration aller Netzwerkgeräte zu zentralisieren.

+

Die zentrale Steuerungsschicht implementiert in der Software und ausgeführt auf Allzweckprozessoren, kann viele Vorteile für die Vernetzung bringen, vor allem beschleunigte Innovation, Entwicklung und Anwendung neuer Netzwerkfunktionen.

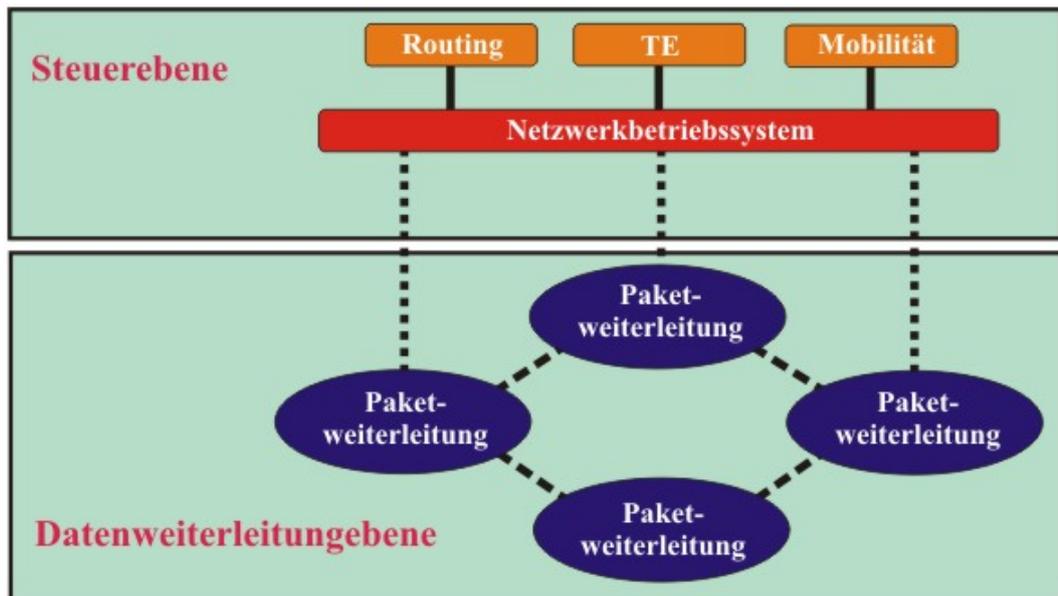


Abbildung 3 - SDN Basisarchitektur

3.3 Zentrale Steuerung und Netzwerk- Programmierbarkeit

In der modernen Netzwerktechnik sammelt die Steuerungsschicht Informationen über den Status der Verbindungen zu Nachbarn und über das Netz als Ganzes und an die Routingalgorithmen weitergeleitet. Die verteilten Algorithmen bieten eine automatische Lösung für Routing-Netzwerkverkehr, haben aber ein mögliches Problem mit der Konvergenz. Da jedes Gerät Informationen über das Netzwerk sammelt und Routing-Entscheidungen trifft, können Verzögerungen bei der Informationsausbreitung über Netzwerkänderungen zu Problemen beim Netzwerkbetrieb führen.



Die Beseitigung der Steuerungsschicht von jedem Netzwerkknoten und der Betrieb mit einer zentralen Steuerungsschicht erlaubt nicht nur die komplette Übersicht über das Netzwerk ohne Konvergenzschwierigkeiten inhärent zu verteilten Routing-Algorithmen, sondern führt auch zu einer Kostenverringerung. Ohne die Notwendigkeit verteiltes Routing zu benutzen, können neue Algorithmen verwendet, verändert und entwickelt werden. Darüber hinaus vereinfacht die Konfiguration der zentralen Steuerungsschicht das Netzwerkmanagement, wobei die Notwendigkeit für die Konfiguration jedes Knotens entfällt. Dies reduziert die Wahrscheinlichkeit für Fehlkonfigurationen und beschleunigt die Fehlersuche. Ein weiterer Vorteil der Software-Implementierung als zentrale Steuerungsschicht ist die leichte Modifikation und die Entwicklung neuer Funktionen.



Aber Gegner der SDN und einer zentralen Steuerungsschicht verweisen vor allem auf die Grenzen der Verwendbarkeit für große Netze wie das Internet. Ihre Kritik konzentriert sich auf die Steuerung, die der Single Point of Failure für das gesamte Netzwerk ist und die unzureichende Skalierung.

Die Lösung für diese Probleme ist die logisch zentralisierte, aber physisch verteilte Steuerungsschicht. Dabei verwaltet eine Reihe von Controllern einen Teil des Netzwerks und kommunizieren miteinander, um die Wartezeit der Steuerungsschicht zu reduzieren sowie eine hohe Verfügbarkeit und des einzigen logischen Verwaltungspunkts für die Netzwerkverwaltung zu bieten. Die neue Architektur für die Inter-Domain-Verbindung mit zugeordnetem Kommunikationsprotokoll für die SDN-Controller wird in [6] vorgeschlagen.

3.4 Vergleich der verteilten Steuerungsschicht mit traditionellen Netzwerken

Die traditionelle Netzwerk-Ausrüstung enthält eine Steuerungsschicht, Netzwerkanwendungen und weitere Funktionen in der Gerätefirmware. Dies bedeutet, dass alle Netzwerkknoten Routing-Entscheidungen vor Ort bilden - effektiv mit einer vollständig verteilten Steuerungsschicht (Abbildung 4). Dies kann man mit einer zentralen Steuerungsschicht vergleichen, die in der SDN-Architektur in Abbildung 3 dargestellt ist.



Die Integration vieler Funktionen bietet eine größere Funktionalität jedes Knotens, macht sie unabhängig voneinander und minimiert die Gefahr eines Single Point of Failure.



Dies wird allerdings auf Kosten einer erhöhten Komplexität erreicht. Das korreliert mit teurer Ausrüstung, höherem Stromverbrauch und kann zu Verzögerungen führen, die stammen von Notwendigkeit verschiedenen Anwendungen für Verarbeitung zu nutzen. Außerdem erfordert die Konfiguration oder Änderung des Netzwerks oft die manuelle Konfiguration vieler Geräte und die Verwendung von komplexen Management-Tools. Das Netzwerkmanagement wird zusätzlich durch die Implementierung und Konfigurationsunterschiede zwischen den verschiedenen Herstellern erschwert, weil dies Interoperabilitätsprobleme verursacht.

Wie [7] behauptet, führt diese Komplexität zu statischen Netzwerken, was aber im Gegensatz zur Notwendigkeit einer dynamischen Umgebung mit größerer Mobilität der Benutzer und Server-Virtualisierung steht. Inkonsistenzen in netzwerkweiten Richtlinien und eine begrenzte Skalierbarkeit des Netzwerks sind weitere Effekte der traditionellen Netzwerk-Feinheiten in großen Netzwerken.



Die zentralisierte Steuerungsschicht im SDN erlaubt dem befreit den Netzwerkadministrator von der Notwendigkeit, viele Geräte manuell konfigurieren zu müssen, führt also zu vereinfachtem Netzwerkmanagement und größere Flexibilität.

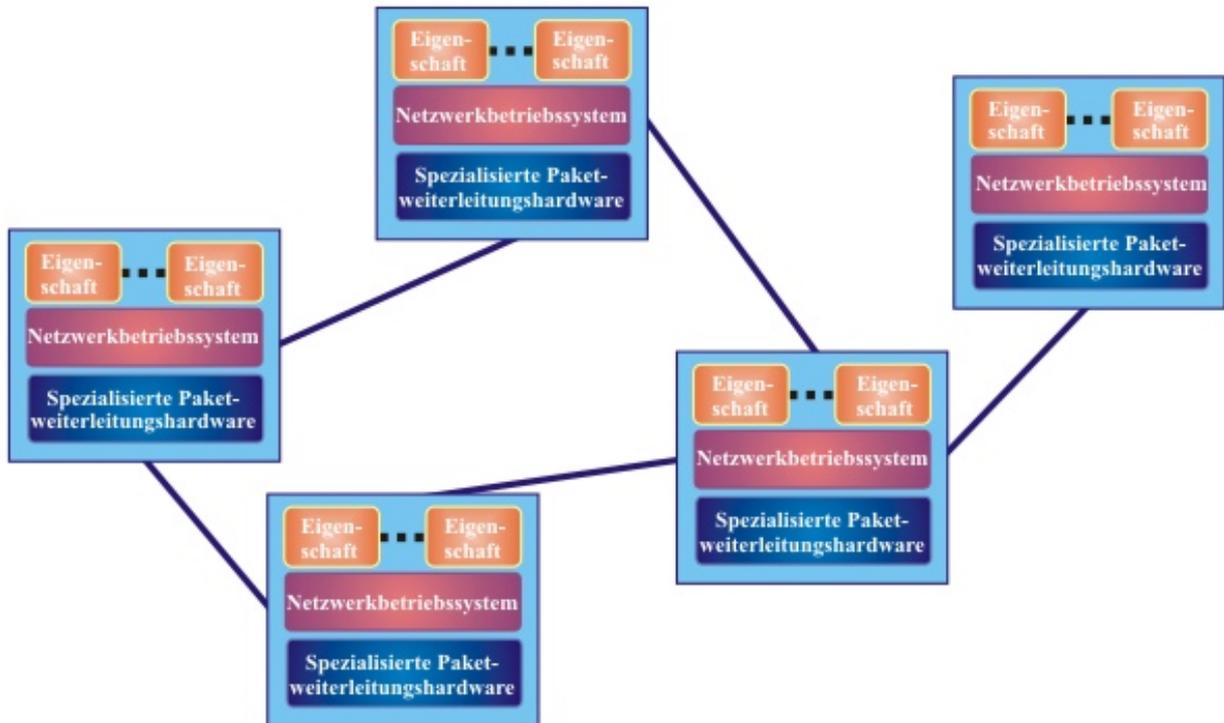


Abbildung 4 - Traditionelle Paketnetzwerkarchitektur [8]



MPLS ähnelt SDN mit schnellen Schalt der Verkehrsströme die durch Steuerungsschicht begründet ist. SDN tut dies aber auf eine andere Weise. Es gibt keine zentrale Steuerungsschicht, die in jedem MPLS-Router mit jedem LER in der Lage ist, einen Pfad zu erstellen und dann mit einem Label Distribution Protocol (LDP) zu verteilen.

3.5 SDN Protokolle

Die Trennung von Steuer- und Datenweiterleitungsschicht, (eine der zentralen Säulen SDN mit Zentralisierung der Steuerungsschicht) bedeutet, dass es einen Bedarf für Kommunikationsprotokolle gibt. In diesem Abschnitt stellen wir einige von ihnen vor, beginnend mit dem beliebtesten - OpenFlow.

OpenFlow

OpenFlow ist ein offener Standard der ursprünglich an Universitäten entwickelt und derzeit von *Open Network Foundation (ONF)* [9] entwickelt wird - eine Non-Profit-Konsortium mit der Mission, OpenFlow basierte SDN zu vermarkten und zu unterstützen. ONF ist sehr spektakulär und erfolgreich. OpenFlow ist das beliebteste Protokoll für die Kommunikation zwischen Steuerungsschicht und Datenweiterleitungsschicht – es ist ein de facto Standard. Doch die ONF-Kampagne führte oft zu der falschen Annahme, dass Openflow gleich bedeutend mit SDN ist.



Trotz bestehender Software-basierter Switching-Lösungen, die eine Erforschung neuer Methoden und Netzwerkprotokolle ermöglichen, bieten die meisten Lösungen keine ausreichende Rechenleistung und/oder Portanzahl für Großversuche an.

Die einfachsten Beispiele sind viele offene Software-basierte Implementierungen von Routing- oder Vermittlungsprotokollen die auf Universalrechnern mit mehreren Netzwerkschnittstellen laufen. Diese Techniken können in der ersten Gruppe kategorisiert werden. Dazu gehören die fehlende Leistung der Techniken, im Vergleich zu dedizierten Netzwerkausrüstungen. Am anderen Ende des Spektrums sind Hardware-basierte Netzwerkforschungs-Lösungen wie NetFPGA, die eine spezialisierte FPGA-Karte für die Line-Rate-Verarbeitung des Datenfluss benutzt.



NetFPGA wird vor allem in der Wissenschaft und beim Rapid-Prototyping verwendet, da es ein Limit von 4 Ports pro Karte gibt.

Wie in [10] erwähnt, sind dies limitierende Faktoren für die akademischen Forscher. OpenFlow ist ein Kompromiss zwischen allgemeinen, leistungsschwachen Lösungen der freien Forschung auf der einen Seite und geschlossenem, nur zum Teil modifizierbarem High-Performance-Netzwerk-Equipment kommerzieller Anbieter auf der anderen Seite.



Das OpenFlow-Protokoll definiert die Kommunikationsschnittstelle zwischen Steuerungsschicht und Datenweiterleitungsebene und muss daher von beiden Seiten implementiert werden. OpenFlow bietet eine extrem genaue Kontrolle auf Per-Flow-Basis und ermöglicht es, auf die Netzwerktopologie-, Anwendungs- oder Benutzeränderungen in Echtzeit zu reagieren.

ONF Whitepaper [9] stellt fest, dass die klassischen Netzwerk-Routing-Lösungen die Kontrolle auf dieser Schicht der Granularität derzeit nicht unterstützen.

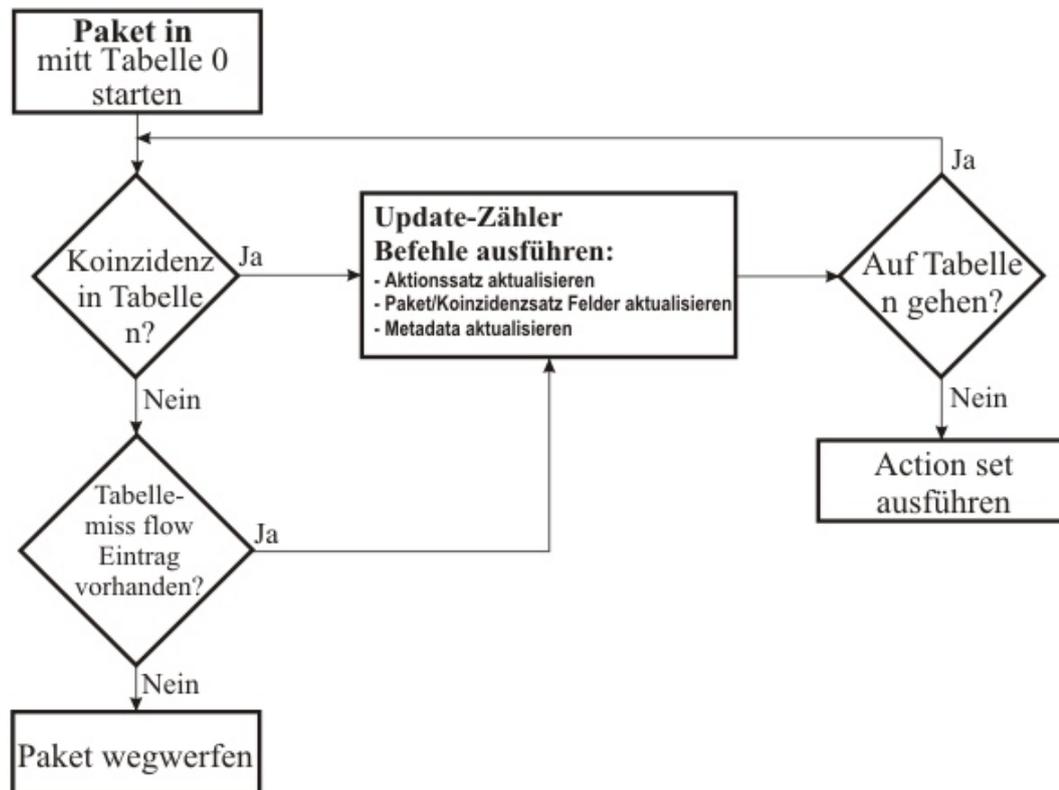


Abbildung 5 - Flussdiagramm der Paketverarbeitung in OpenFlow (logischer Schalter) [11]

Wird ein Paket von OpenFlow-Schaltern empfangen, so wird es in der OpenFlow Pipeline von einem oder mehreren Stromtabellen zusammengesetzt und bearbeitet. Stromtabellen beinhalten Einträge mit Regeln und Aktionen, die für Pakete gelten. Wenn eine Übereinstimmung für das Paket in keiner der Fluss-Tabellen gefunden wird und wird dass unbekanntes Pakete an einen Controller geschickt. Der Controller verarbeitet das Paket und entweder verwirft er das Paket oder baut einen neuen Verkehrsfluss, indem er einen neuen Eintrag in der Fluss-Tabelle erstellt. Der Handhabungsmechanismus eines empfangenen Pakets eines OpenFlow-Schalter ist in Abbildung 5 dargestellt.

ForCES



Das Protokoll *Forwarding and Control Element Separation (ForCES)* [12] definiert eine Rahmenarchitektur und die zugehörigen Protokolle, um den Informationsaustausch zwischen der Steuerungsschicht und der Weiterleitungsschicht in einem ForCes Netzwerkelement zu standardisieren.

ForCES beschreibt vor allem eine offene API und Protokolle, welches eine klare Trennung der Steuer- und Weiterleitungsschicht erlaubt.



Die große Stärke des ForCES liegt in dem Weiterleitungs-Elementmodel, das die Beschreibung der neuen Weiterleitungsschicht und deren Funktionalität ermöglicht, ohne das Protokoll zwischen Steuerungsschicht und Weiterleitungsschicht zu wechseln.

Ziel der ForCES-Entwicklung war es, das Netzwerkgerät in separate Steuer- und Weiterleitungsschichten aufzuteilen und von Hardware-Komponenten unabhängig zu werden. Daraus entstand ForCES – eine neue Architektur für Netzwerkgeräte, während OpenFlow auf eine neue Netzwerkarchitektur zielt.

NETCONF



NETCONF ist ein Netzwerk-Management-Protokoll, das Mechanismen bietet, die Remote-Installation zu manipulieren und die Konfiguration von Netzwerkgeräten zu löschen.

Das NETCONF-Protokoll selbst ist in vier Schichten mit einer Reihe von Basis-Protokoll-Operationen und verwendet **RPC** (*Remote Procedure Call*) Methoden.

Eines der Ziele von NETCONF ist es, eine programmierbare Schnittstelle zum Gerät anzubieten, die die Funktionalität der nativen Schnittstelle des Gerätes abbildet.



Obwohl NETCONF ursprünglich als Nachfolger von SNMP und einige der CLI-Protokolle für die Konfiguration der Netzwerkelemente entwickelt wurde, können NETCONF-Funktionen auch verwendet werden, um eine Form des Hybrid-SDN zu erstellen. Darüber hinaus ist NETCONF-Unterstützung eine Voraussetzung für Netzwerkgeräte, um mit dem OF-CONFIG Teil der OpenFlow-Spezifikation kompatibel zu sein.

PCE-P



Pfadberechnungselement (PCE) ist eine Einheit, die im Auftrag der Knoten, die Pfade berechnet. Das erlaubt die Verwendung optimaler Pfade für die Datenweiterleitung mittels MPLS, GMPLS P2P und P2MP durch *Label Switched Pfade* (**LSPs**).

PCE kündigt dann diesen Pfad den Netzwerkknoten mit über ein PCE-Kommunikationsprotokoll an. Dadurch erweitert es MPLS und GMPLS Endgerätfunktionen und verkleinert damit den Unterschied zwischen SDN und Standard-MPLS/GMPLS.

Obwohl PCE nicht in erster Linie als SDN-Schlüsseltechnologie entwickelt wurde, ist es logisch ein zentralisiertes Management-Modell für bestehende Technologien, das ein paar zusätzliche Verbesserungen bereitstellt.

Schnittstelle zum Routing-System

Die Schnittstelle zum Routing System (I2RS) ist eine der anspruchsvolleren Ansätze zur SDN, die von der IETF entwickelt wurde und sich noch in einem frühen Stadium der Entwicklung befindet. Die I2RS ist eine bidirektionale programmatische Schnittstelle für die Kommunikation zwischen Routingssystem und Anwendungen. Sie ermöglicht Netzwerküberwachung, Reservierung von Ressourcen und die Modifikation von Routing-Konfigurationen. I2RS konzentriert sich auf die Kommunikation zu und von Routing-Systemen. I2RS ist nicht dazu bestimmt direkte Schnittstellen zur Weiterleitungsschicht anzubieten. Die ausgewählten Strecken in die Weiterleitungsschicht zu verteilen ist Aufgabe von bestehenden Mechanismen.

Cisco ONE

Auch wenn Cisco Teil der Open Networking Foundation ist und sich aktiv an der Entwicklung von OpenFlow beteiligen, ist es nicht das einzige SDN Projekt von Cisco. Einer ihrer proprietären Alternativen ist *Open Network Environment* (Cisco **ONE**), die programmatische Schnittstellen bereitstellt, um Cisco-Geräte direkt zu steuern. Schlüsselkomponente der Cisco ONE ist das *ONE Platform Kit (onePK)* - Entwickler-Kit mit mehreren Plattform-APIs, das eine einfache Entwicklung von Netzwerk-Anwendungen mit direktem Zugang zu Netzwerkkomponenten über die Netzwerkabstraktionsschicht ermöglicht.

Nuage



Im April 2013 startete Alcatel-Lucent das Spin-out-Unternehmen „Nuage Networks“, mit der Aufgabe eine SDN-Lösung zu erstellen, die zwar auf seiner früheren Anwendung aufbaut, aber auch die Freiheit zur Nutzung alternativer, neuer Technologien bietet. Das Ergebnis dieser Entwicklung ist die „Virtualised Service Plattform“, eine Software-Lösung, die sich auf das Problem der Netzwerkvirtualisierung in Rechenzentren und auf *Cloud-Service-Provider (CSPs)* konzentriert. Weil Nuage VSP in Software implementiert ist und VXLAN als Kapselung für Hypervisor verwendet, es ist unabhängig von einem bestimmten Typ (oder einer Marke) von TOR-Schaltern.

4 Network Functions Virtualisation (NFV)

Ein integraler Bestandteil des Telekommunikationsmarktes sind proprietäre Hardware-Geräte, die für die Bereitstellung neuer Dienste erforderlich sind. Komplikationen entstehen, vor allem durch steigende Kosten und erhöhten Zeitbedarf für die Bereitstellung, wie **TTM** (*Time to Market*) und **TTD** (*Time to Deploy* Zeit zu implementieren). Diese Komplikationen sind heutzutage für Telekommunikationsunternehmen ein begrenzender Faktor zur Sicherung der Qualität ihrer angebotenen Dienstleistungen.

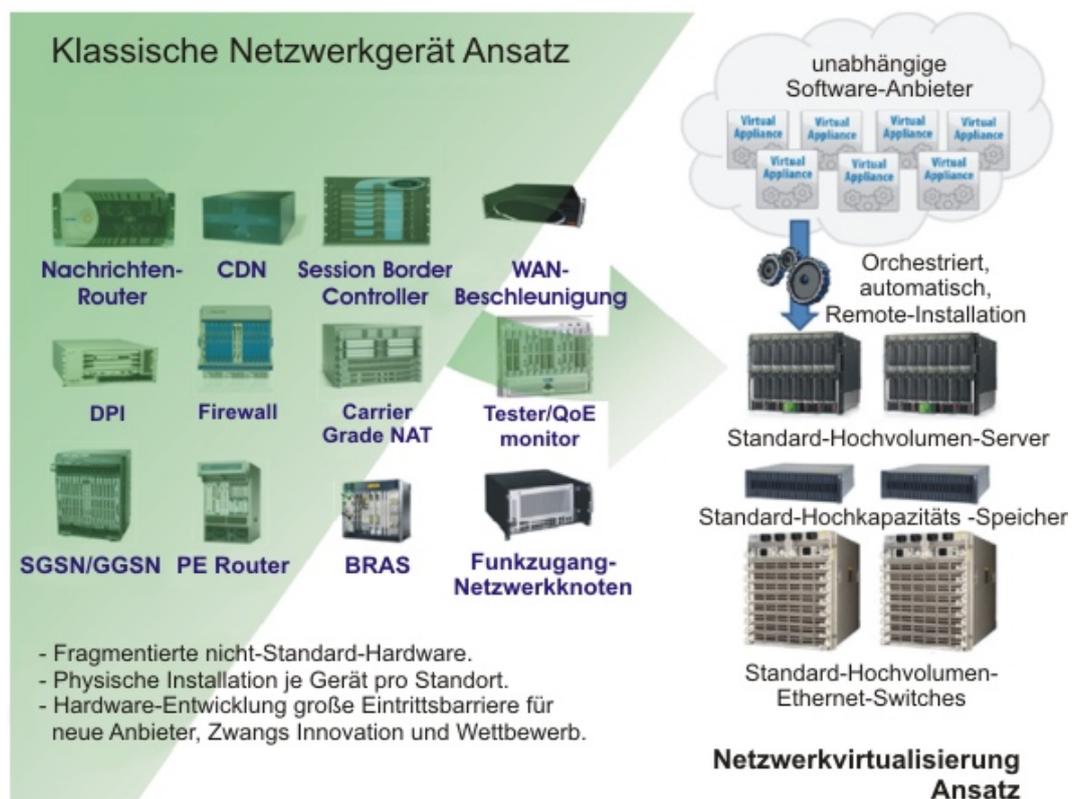


Abbildung 6 - Vision des NFV [13]



Vorteile für Netzwerk / Telekom-Betreiber

- Reduzierung von **CAPEX** (*Capital Expenditure*) und **OPEX** (Betriebsaufwand wie etwa Reparatur und Wartung) durch die Reduzierung der Kosten für die Ausrüstung und den Energieverbrauch
- kürzere Markteinführungszeit für die Bereitstellung neuer Netzwerkdienste
- bessere Rentabilität neuer Dienste
- Mehr Flexibilität für die Skalierbarkeit und die Entwicklung von Dienstleistungen

- Gelegenheit für das Testen und die Einführung neuer innovativer Dienste mit geringerem Risiko
-

Im Oktober 2012 wurde ein White Papers [13] freigegeben, das den ersten Entwurf des NFV vorgestellt. ETSI hat hier verschiedene Anforderungen an die Technologie formuliert und die Vorteile der NFV-Technologie beschrieben. Die Industrie Spezifikation Gruppe für die NFV (ISG NFV) wurde geschaffen, um alle Anforderungen an diese neue Technik zu definieren. Diese Gruppe wurde von dem Träger des European Telecommunications Standards - Europäische Institut für Telekommunikationsnormen (ETSI) gebildet. Die NFV ISG vertritt etwa 235 Unternehmen und nahm an mehreren Sitzungen in Asien, Europa und Nordamerika teil. Die ersten Dokumente der NFV ISG wurden im Oktober 2013 veröffentlicht. Die Dokumente beschreiben die Architektur der NFV, alle Komponenten und Schnittstellen. Von 2013 bis 2015 lief die zweite Phase, entsprechende neuere Dokumenten stehen direkt auf der Website NFV ISG bereit.

4.1 Was hat NSF ermöglicht?



Wenn es möglich ist, Netzwerke mit NFV-Technologie zu bauen, stellt sich die Frage, warum das Netzwerk von Anfang an mit proprietärer Hardware gebaut wurde. Die Antwort ist, dass Industriestandard-Server mit Betriebssystem und Software erst seit kurzer Zeit die Rechenleistung besitzen, um effektiv mit proprietären Geräten konkurrieren zu können. Dies gilt z. B. für Anschaffungskosten, Stromverbrauch und Zuverlässigkeit.

Mit "seit kurzer Zeit", sind die letzten vier bis fünf Jahre dieser Entwicklung definiert. In dieser Zeitspanne haben wir eine entscheidende Verbesserung beim Netzwerkdurchsatz und Paketverarbeitungsdurchsatz von x86-Prozessoren, sowie eine Erhöhung der Anzahl von Prozessorkernen auf einem einzigen physischen Industrieserver erlebt.

4.2 Anforderungen an NFV

Liste der grundlegenden Anforderungen, die NFV [1] erfüllen sollte:

- Portabilität – bei der Verteilung von NFV in unterschiedlichsten Umgebungen.
- Performance - Performance-Ziele von einzelnen Softwarefunktionen.
- Management und Orchestrierung - Mechanismen, die erforderlich sind, um Orchestrierung und Lifecycle-Management-Software-Funktionen, Ressourcen, Infrastruktur und verschiedenen Operationen zu ihrer Herstellung realisieren zu können.
- Flexibilität - die Fähigkeit, Lösungen auf einfachem Weg sowie Skalierbarkeit von Hardware-Ressourcen bieten zu können.
- Sicherheit - die festen Dimensionen, die untersucht werden müssen, da die Virtualisierungs-Umgebung von außen angegriffen werden kann.
- Kontinuität von Dienstleistungen - Funktionen, die für die weitere Erbringung von Dienstleistungen im Einklang mit dem Service Level Agreement (SLA) notwendig sind.
- Operationen - Automatisierung von betrieblichen Funktionen (z. B. Anpassung der Netzwerkkapazität, herunterladbare Software-Aktualisierung, Reparatur von Fehlfunktionen etc.).
- Energieeffizienz – Ziel ist es, den Energieverbrauch von großen virtualisierten Netzwerken zu minimieren.
- Migration und Koexistenz mit bestehenden Plattformen - Unterstützung des Übergangs von den heutigen Netzwerken, in denen nicht-virtualisierte mit virtualisierten Netzwerken koexistieren. Der Benutzer sollte bei einer Umstellung nicht betroffen sein.

Die Fähigkeit der Remote-Bereitstellung sowie des Betriebes von virtualisierten Netzwerkfunktionen auf NFV-Infrastruktur wird von verschiedenen Dienstleistern bereitgestellt und ermöglicht einen effizienten Service für Kunden in der ganzen Welt.

4.3 NFV-Architektur

Die Architektur der NFV-Technologie wurde in der zweiten Auflage des White Paper [14] konzipiert und besteht aus den folgenden Komponenten (Abbildung 7):

- NFVI (Network Functions Virtualisation Infrastructure) - bietet virtuelle Ressourcen die nötig sind zur Umsetzung der virtualisierten Netzwerkfunktionen. Sie unterstützt kommerzielle COTS Hardware-Komponenten für die Beschleunigung. Es ist eine Softwareschicht die virtualisiert und abstrahiert die darunterliegende Hardware.
- VNF (Network Functions Virtualisation) - Software-Implementierung von Netzwerk-Funktionen, die in der Lage ist, durch NFVI ausgeführt werden und kann von EMS begleitet werden - Element Management System, das die VNF verwaltet. VNF ist eine Komponente die heutigen Netzwerkknoten entspricht, die voraussichtlich als reine Software-unabhängig von der Hardware geliefert wird.
- NFV M & O (Verwaltung und Orchestrierung) - deckt Orchestrierung und Lifecycle-Management von physischen und / oder Software-Tools, die die Virtualisierung und Infrastruktur-Lifecycle-Management VNFs unterstützen. NFV M & A konzentriert sich auf die Virtualisierungsmanagement-Aufgaben, die für die NFV Rahmen notwendig ist. Es arbeitet auch mit externen NFV OSS / BSS und ermöglicht die Integration NFV in bestehende Netzwerke.

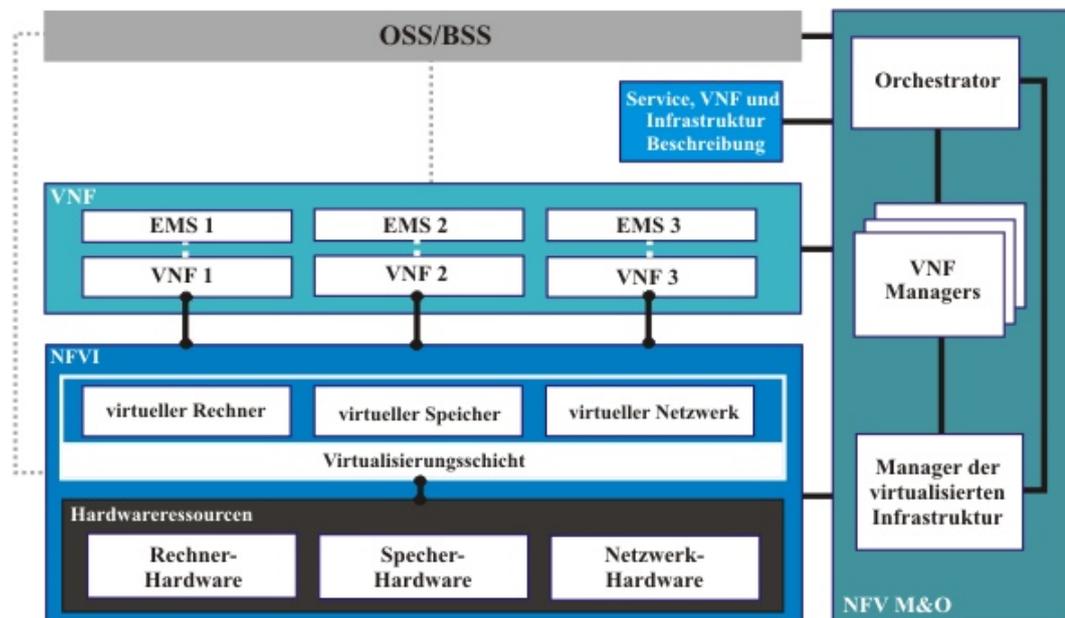


Abbildung 7 - NFV Architektur [14]

Das gesamte System wird durch eine Reihe von Metadaten unterstützt, die NFV Dienstleistungen, VNFs und Infrastrukturanforderungen zu NFV M & O beschreiben. Diese Beschreibungen zusammen mit Dienstleistungen, VNFs und

Infrastruktur können durch andere Akteure aus der Industrie zur Verfügung gestellt werden.

4.4 Infrastructure NFV – NFVI

Die NFV Infrastruktur ist in drei Domänen [15] unterteilt:

- Computer-Domäne – sie stellt Rechen- und Speicherressourcen zur Verfügung stellen und wird in Verbindung mit dem Hypervisor verwendet. Sie bietet eine Schnittstelle zu Domänennetzinfrastruktur, verbindet aber nicht zum Netz selbst.
- Hypervisor-Domäne – sie vermittelt Computer-Domäne Ressourcen der Software auf virtuellen Maschinen zu. Hypervisoren wurden für die Bedürfnisse von Cloud-Lösungen entwickelt und legen Wert auf die Verteilung der Aufgaben an die verfügbaren Hardwareressourcen. So kann man eine hohe Portabilität von virtuellen Maschinen erreichen. Der Hypervisor kann jede Art von Hardware-Plattform emulieren (nachahmen) und in einigen Fällen sogar ein komplettes Instruction Set. Damit kann die virtuelle Maschine völlig andere Prozessorarchitekturen benutzen.
- Domain-Netzwerkinfrastruktur - dieser Domäne ist zuständig für die Bereitstellung von:
 - einen Kanal für die Kommunikation zwischen mehreren VNFC (VNF Components)
 - einen Kanal für die Kommunikation zwischen mehreren VNF (network function virtualization)
 - einen Kommunikationskanal zwischen VNF und MANO (Verwaltung und Orchestrierung)
 - einen Kanal für die Kommunikation zwischen den Komponenten NFVI und deren Orchestrierung und Management
 - ein Mittel zur Fernbedienung vonVNFC
 - ein Mittel zur Verknüpfung mit dem bestehenden Netzbetreiber

4.5 Verwaltung und Orchestrierung NFV (MANO)

Die Verwaltung und Orchestrierung enthält drei Komponenten [16]:

- NFV-Orchestrator – ist verantwortlich für folgendes: die Orchestrierung (Management) der NFV Quelle an mehrere VIM (Virtualized Infrastructure Manager), die Funktionsorchestrierung von Ressourcen, Lebenszyklus-Management von Netzwerkdiensten (z. B. Verwaltungsrichtlinien erstellen, Skalierung, Leistungsmessung, Ereigniskorrelation), die Füll-Funktion Orchestrierung für Netzwerkdienste, das globale Ressourcenmanagement, die Validierung und Genehmigung von NFVI Quellen.
- VNF-Manager – ist verantwortlich für folgendes: die Verwaltung des Lebenszyklus von Instanzen der VNF. Er kann zur Verwaltung einer VNF-Instanz oder auch mehrere Instanzen des gleichen oder eines anderen Typs verwenden werden inklusive der Gesamtkoordination und der Anpassung von Konfigurationen sowie die Berichterstattung über Zwischenfälle zwischen NFVI und E / NMS.
- *Virtualized Infrastructure Manager (VIM)* - ist verantwortlich für folgendes: die Kontrolle und das Management der NFVI Berechnung, Speicher und Netzwerkressourcen innerhalb der Infrastruktur von Sub-Domains eines einzigen Betreibers, die Erfassung und Übermittlung von Performance-Messungen und Veranstaltungen.

4.6 VNF-Software-Architektur

Die „network function virtualization“ nutzt die NFV-Infrastruktur (NFVI) und wird von NFV Orchestrierung (NFV) und VNF Manager verwaltet (Abbildung 8).

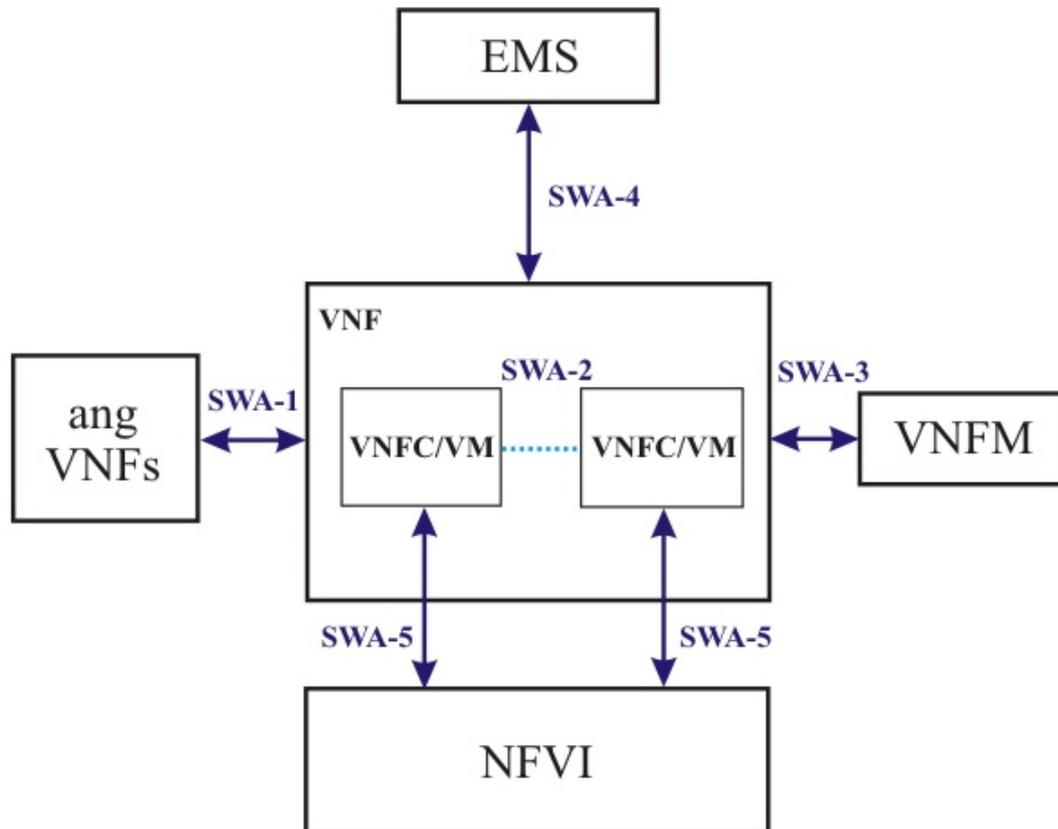


Abbildung 8 – NFV-Architektur [17]

Diese Architektur sorgt für hochwertige Verbindungen über diverse Schnittstellen:

- SWA-1 - mit dieser Schnittstelle kommunizieren mehrere VNF, sie können sie nutzen, um gemeinsam zu spielen und Aufgaben über ein Netzwerk auszuführen
- SWA-2 - verbindet Komponenten innerhalb VNF, wobei jede Komponente eine Rolle für die Ausführung von virtuellen Netzwerkfunktionen spielt.
- SWA-3 – Eine Verbindung zum VNF-Manager.
- SWA-4 - verbindet VNF mit einem EMS.
- SWA-5 - Diese Schnittstelle verbindet NFVI mit jedem VNFC.

4.7 Anwendungsfälle für NFV



NFV bietet viele Vorteile. Einerseits die Vereinfachung innovative Ansätze zur Vernetzung von Funktionen und andererseits Seite ergibt sich eine endlose Menge von Anwendungsfällen, die im realen Netzwerkverkehr mehr oder weniger nützlich sind.

Dennoch können wir sagen, dass NFV heutzutage noch keine separate, voll praktikable Lösung ist. Sogar die Organisation ETSI bemüht sich kontinuierlich darum einen starken einheitlichen Standard NFV zu erstellen. NFV beschreibt, wie von der Virtualisierung profitiert werden kann, welcher Ansatz für die Bereitstellung von Netzwerkfunktionalitäten zur Verfügung stehen und wie die Verwaltung und Orchestration durchzuführen ist.



Das Web-Portal SDxCentral veröffentlicht jährlich einen umfassenden Bericht unter dem Titel „NFV Report“ [18], der die Grundidee des NFV, seine Entwicklung und einen Überblick über Anbieter von NFV-Lösung liefert sowie vorteilhaftesten Anwendungsfälle (unten aufgeführt) beinhaltet.

Virtualisierte Netzwerkfunktionen

Gut funktionierende Cloud-Funktionen bieten viele Möglichkeiten, wie einfache, flexible und schnell zu verteilende Anwendungen und die Entwicklung von Infrastrukturen oder Plattformen. Virtualisierte Netzwerkfunktionen sind dafür ausgelegt, in vollem Umfang bereits bestehende Verfahren in der Cloud-Welt voll zu berücksichtigen. Für Cloud-Service-Anbieter sind die attraktivsten VNF: die Bereitstellung von virtuellem Routing, *Virtual Private Network (VPN)* sowie der Layer 4-7 Beschleunigungs- und Sicherheitsdienste. Sicherheitsdienste helfen, beim verbinden, schützen und skalieren der cloudbasierten Anwendungen.

Virtualisiertes Cloud Radio Access Network

Dieser Anwendungsfall ist besonders wichtig für die Mobile Service Provider, die nach Möglichkeiten zur Vereinfachung, Beschleunigung und Schaffung von neuen Funkzugangnetzen (RANS) suchen, bei gleichzeitiger Kostenkontrolle. Eine Reihe von Funktionalitäten, die sich auf proprietärer Hardware in einer Basisstation befinden, kann auf eine oder mehrere virtuelle Maschinen migriert werden. Diese können lokal auf einen COTS-Server, einem Sammelpunkt oder in der Cloud laufen.

Virtualisierte Core Mobile

Mobilfunkbetreiber sind oft konfrontiert mit Aufgaben zur Modernisierung ihrer Netze und Erweiterung ihrer Dienste und Dienstleistungen, um ländlichen Gebieten zu versorgen. Ein Anwendungsfall betrifft die Übernahme der Funktionen proprietärer Hardware im mobilen Bereich und ihren Einsatz auf einem COTS-

Server, in einer Cloud-Umgebung. Mobilfunkbetreiber suchen für die Virtualisierung Dienstleistungen die vor allem IMS, EPC MME, S-GW, P-GW, HSS und PCRF unterstützen.

Virtualisierte Begrenzung

Dienstanbieter versuchen auch eine Lösung finden wie sie ihre Begrenzung vereinfachen konnten. Die Begrenzung umfasst *Customer Premises Equipment (CPE)* und *Customer Edge (CE)*. Das Ziel ist mehr Dienstleistungen sowohl für Privat- und Geschäftskunden zu verkaufen. NFV kann eine mögliche Lösung sein, um ihre Einnahmen erhöhen. Zur Einführung der NFV-Technologie in der Welt des Service Providers, ist es notwendig, Lösungen für Virtual Customer Premise Equipment (vCPE) und VCE bereitzustellen.

5 Zukunft des Internet

Die Gegenwart kann als die Zeit der *Informations- und Kommunikationstechnologien (IKT)* charakterisiert werden. Das Internet, wie wir es heute kennen, ist ein klarer Erfolg. Doch einige Aspekte des aktuellen Internets genügen nicht derzeitigen Erwartungen an eine zuverlässige Kommunikationsinfrastruktur und zukünftigen Anforderungen, die wir gerne an ein solches Netz.



Bis zum Jahr 2015 wird das globale öffentliche Internet ca. 6 Milliarden Menschen verbinden, mehr als 4 Milliarden Menschen werden die Netzwerkdienste über mobile Geräte nutzen und mehr als 2 Milliarden Menschen werden eine freie Breitband-Verbindung zum Internet verwenden.

Diese Prognose kann man in der Arbeit von Claus G. Gruber [19] finden, sowie die Annahme, dass der Netzwerkverkehr in den kommenden Jahren eine Wachstumsrate von 40% bis 200% im Vergleich mit dem heutigen Netzwerkverkehr haben wird. Deshalb ist es wichtig zu beurteilen, in welchem Zustand sich die heutigen Computer-Netzwerke und deren Bestandteile sind. Hohe Internet-Penetration fördert und beschleunigt die Benutzung von mobilen Geräten wie Laptops, Handys und Tablets. In der Abb. 9 können wir die Prognose für die Geräte sehen, die an das globale öffentliche Internet angeschlossen sind [20].

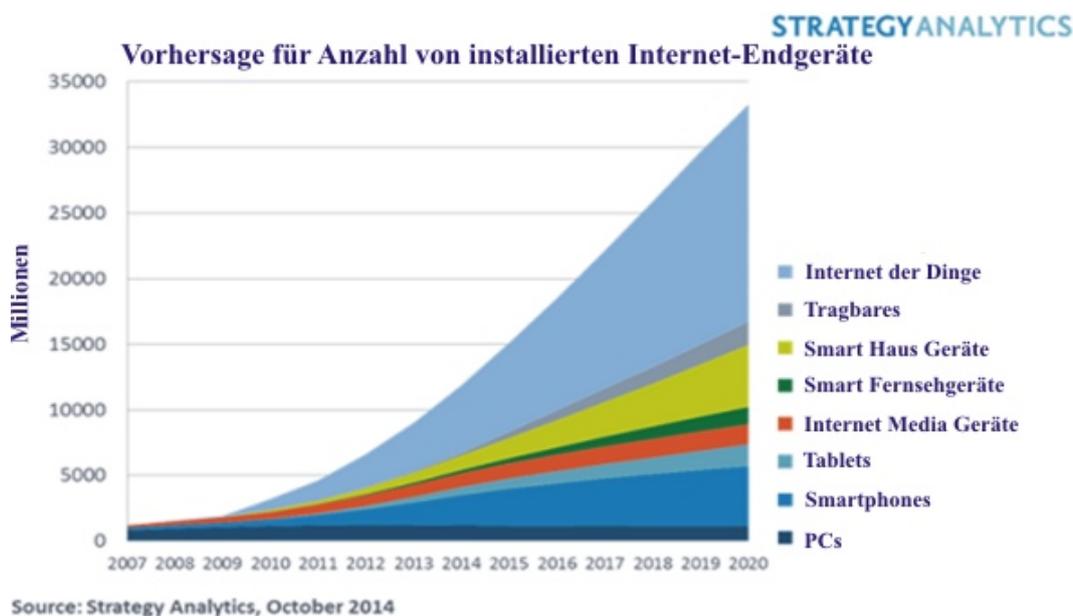


Abbildung 9 – Vorhersage für Anzahl von installierten Interne-Endgeräte

Die Anforderungen der Mobilfunknetze sind oft anspruchsvoller als die Anforderungen der Benutzer in dem drahtgebundenen Netzwerk, besonders in Bezug auf die ständige Verfügbarkeit [21]. Deshalb müssen die heutigen Netze adaptiv und agil sein und nicht nur eine hohe Verfügbarkeit der Dienste gewährleisten, sondern auch die entsprechende Qualität bereitstellen.

5.1 Einschränkungen des Internets

Das aktuelle Internet basiert hauptsächlich auf dem IP-Protokoll. Es wurde vor mehr als 40 Jahren von einer Gruppe von Wissenschaftlern für die Zusammenschaltung ihrer lokalen Netzwerke erstellt, vor allem für den Dateiaustausch, E-Mail-Kommunikation usw.

i

Das heutige Internet hat die ursprünglichen Annahmen übertroffen. Ausgehend von weniger als einigen hundert Computern sind heute mehrere hundert Millionen Rechner miteinander verbunden. Das Internet hat auch nicht mit neuen Anwendungen wie Web, Video-Streaming und Dateifreigaben gerechnet. Diese Komponenten haben die Art des Internet-Verkehrs wesentlich verändert. Die Infrastruktur des Internets wurde durch technologische Prozesse um optische, drahtlose und andere Technologien erweitert [22].

In der Abb. 10 wird die Entwicklung des Internets von der Vergangenheit bis in die Gegenwart dargestellt. Das Internetprotokoll (IP) ist in der Mitte des Schichtmodells dargestellt mit den Applikationen darüber und den Technologien im unteren Teil.

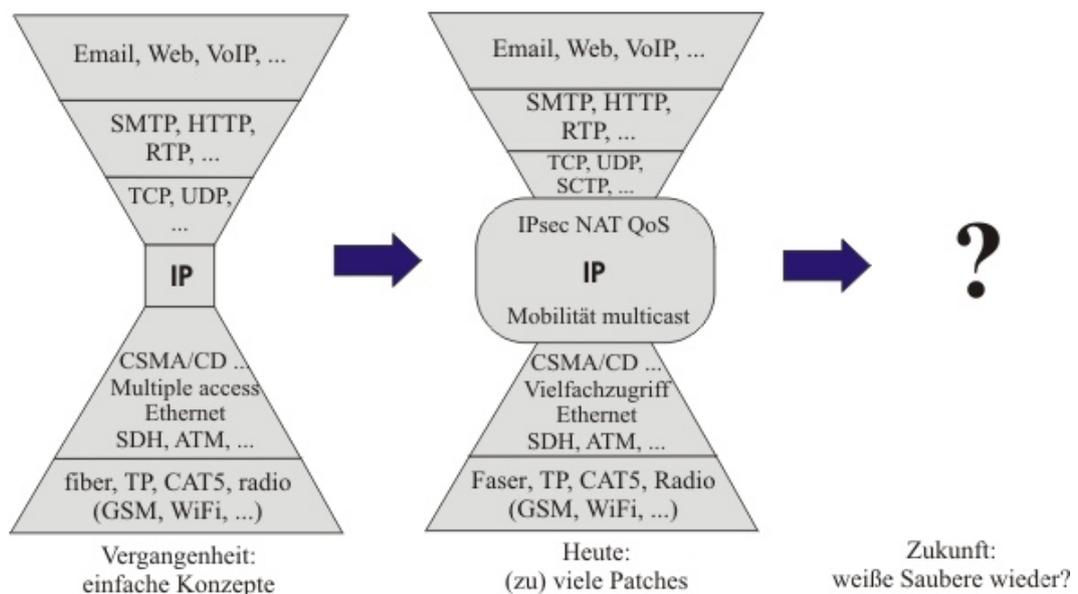


Abbildung 10 - Entwicklung des Internets [23]

Derzeit gibt es fast keine praktikable Möglichkeit, um mit neuen Netzwerkprotokollen einen experimentellen Nachweis für den praktischen Einsatz in den Netzen der *Internet Service Provider (ISP)* und *Network Service Provider (NSP)* zu erbringen.

—

Die Autoren in [24] bestätigen, dass die enorme Menge von bereits seit Jahrzehnten eingesetzten Netzwerkgeräten in der gleichen Netzwerk-Infrastruktur mit dem gleichen Netzwerkprotokoll ein riesiges Hindernis für den Zugang zu innovativen Lösungen, Forschung und Entwicklung in Computernetzwerken darstellen. Das

Ergebnis dieses Ansatzes ist auch die Tatsache, dass eine Reihe von Ideen, neue bislang ungetestet und unbewiesen sind. Die Strukturen der heutigen Computer-Netzwerke sind "erstarrten".

Es ist wichtig zu beachten, dass das Internetprojekt zum Zwecke der Forschung aufgebaut wurde. Die Architekten, der Internet-Infrastruktur haben nie die Möglichkeit eines so großen Netzwerkes, wie wir es derzeit haben, in Betracht gezogen. Aspekte wie Sicherheit, Mobilität, Flexibilität, Elastizität der Netze sind noch nie gelöst worden, weil in den Zeiten der Formalisierung des Internets, die Rechner nicht mobil waren und die Forscher neue Ideen über die offenen Umgebung verbreiten wollten. Die Vision der perfekten Internetumgebung begann mit zunehmender Zahl der Nutzer zu verblassen. Die Menge der Grundkonzepte hat sich seit dem Zeitpunkt ihrer Entstehung geändert. Mit der raschen Entwicklung der Technologien im Bereich der Informatik und Informationstechnologien, kann das öffentliche Internet nicht Schritt halten und befriedigen die damit entstehenden Anforderungen nicht befriedigen. Es ist offensichtlich, dass für die heutigen Netze neue Vorschläge gebrauchen werden, die besser an neue Trends anzupassen sind.

Der Betrieb von Computernetzwerken erfordert eine Anzahl von Ressourcen, die mit den Kosten korrespondiert. Die Kosten können in Investitionskosten (CAPEX) und Betriebskosten (OPEX) aufgeteilt werden [25]. CAPEX bezieht sich auf Investitionen, die im Voraus gemacht werden müssen und nach einer gewissen Zeit der Abschreibung unterliegen. Ein Beispiel wäre der Bau des Rechenzentrums (DC) oder der Kaufpreis für Server, Netzwerk-Ausrüstung und andere wichtige Netzwerkkomponenten. Die betrieblichen Aufwendungen OPEX sind mit wiederkehrenden monatlichen Kosten für den tatsächlichen Betrieb der Geräte, wie beispielsweise Energiekosten, Reparaturen, Wartung und Gehälter des Verwaltungspersonals verbunden.

5.2 Eigenschaften des neuen Internet

Die Eigenschaften des neuen Internet sind:

- Robustheit und Zuverlässigkeit - Zukunftsnetze sollten robust, fehlertolerant und stets verfügbar sein.
- Sicherheit - eines der größten Probleme des heutigen Internet ist die Sicherheit, vor allem die End-Host-Sicherheit. Das ist der Grund, warum beim Design der Zukunftsnetze von Anfang an größter Wert auf die Sicherheit gelegt werden muss. Das Netzwerk sollte Tools bieten, um die sich schnell verbreitenden Infektionen unter Quarantäne zu stellen, Denial of Service-Attacken zu mildern, und eine bessere Authentifizierung zu gewährleisten. [22].
- Mobile End-Host Unterstützung - Wie oben erwähnt, wird die Anzahl der Endnutzer des Internets rasch zunehmen und die Mobilfunknutzer werden dabei die Mehrheit bilden. Zukünftiges Internet sollte die Mobilität der Benutzer, der Terminals und Netzwerke und sogar der Anwendungen erleichtern, wenn sich die Kommunikation z.B. auf andere Geräte verlagert (endpoint mobility) [22].
- wirtschaftlich tragfähig und profitabel - Die Zukunftsnetze sollten profitabel für diejenigen sein, die Netzwerkdienste zur Verfügung stellen.
- Entwicklungsfähigkeit - Die Architektur des zukünftigen Internet sollte voraussetzen, dass es im Laufe der Zeit zu Änderungen und neuen Entwicklungen kommt.
- Vorhersehbar - Der Benutzer sollte wissen, welcher Service von dem Netz zu erwarten ist.
- Unterstützung der Anonymität – für Fälle, wo der Schutz des Anwenders nötig ist.

5.3 Neugestaltung der Internet-Technologien

i

Wie bereits erwähnt, gilt für eine Anzahl der an das Internet angeschlossenen Geräte ein konstantes und unaufhaltsames Wachstum, das sich Jahr für Jahr proportional vervielfacht.

Um ein stabiles, sicheres, flexibles und agiles Netzwerk zu erhalten, können wir nicht mehr bei den Standards der sechziger und siebziger Jahre bleiben. Wir sind gezwungen, uns vorwärts zu bewegen und Türen zu neuen Technologien zu öffnen. Als die größte Herausforderung erscheint hier die Zusammenschaltung von programmierbaren SDN und die Virtualisierung von Netzwerkdiensten. Eine solche neu geschaffene Architektur verspricht nicht nur eine Verbindung der unbestreitbaren Vorteile beider Technologien, sondern auch die Entstehung weiterer Verbesserungen.

+

Eine bahnbrechende Idee ist sicherlich die Architektur für die automatisierte Bereitstellung von Netzwerkdiensten in virtualisierter Form. SDN können die perfekte automatisierte Netzwerkumgebung, die das Netzwerk im Unternehmen sowie die Umgebung des Kunden automatisch konfiguriert. Darüber hinaus sind die Anwendungen, die sich auf dem SDN-Controller befinden in der Lage, dynamisch die Netzqualität auszuwerten und wenn nötig, den Netzwerkpfad zu ändern, damit die Parameter des Netzes erhalten bleiben, und können auch bei Ausfall einer bestimmten Netzwerkkomponente eingreifen.

Im Rahmen der Automatisierung können wir auch auf bestimmte Vorlagen oder Strategien für spezifische virtualisierte Dienste zugreifen und auf abgestimmte Strategien für den betreffenden Client hinweisen. Durch einen Software-orientierten Ansatz ist es möglich die gewünschte Konfiguration in einer Reihe von Netzwerkdiensten, die auch konsistent sind, zu halten - damit wird Inkonsistenz, durch Interaktionen der Benutzer vermeiden.

Die größte Herausforderung ist die Zentralisierung und Übertragung der eigenen Dienste, die so genannte „Reise mit meinen Netzwerkdiensten“. Da Dienste nicht mehr auf großen Geräten ausgeführt werden, ist jeder Kunde in der Lage, die Dienstleistungen ortsunabhängig (mobil) nutzen zu können.

+

Dank der Flexibilität dieser künftigen Netze ist es viel einfacher, ein angebotenes Produkt zu beobachten und gegebenenfalls anzupassen – eine Dienstleistung, für Erweiterungen, die es für dedizierten Geräte, bis zu diesem Zeitpunkt noch nicht gab.

-

Alle diese Ideen werden verlockend formuliert, aber der Einsatz der Architektur welche SDN und NFV Technologien verbindet, erfordert den Ersatz der bestehender Infrastruktur und das ist nicht einfach. Eine Möglichkeit für den Übergang kann in der Integration und dem Test von SDN und NFV in bestehenden Umgebung liegen, mit dem nachfolgenden Austausch veralteter Technologien.

SDN ist ein neuer Ansatz, der es uns ermöglichen sollte, das Netzwerk durch gut definierte Schnittstellen zu verwalten, zu ändern und dynamisch zu steuern. Die zentrale Steuerung enthält die ganze Intelligenz und verwaltet eine Netzwerk-weite Sicht von Datenpfad-Elemente und verbindenden Links. Durch diese zentralisierte up-to-date-Ansicht eignet sich die Steuerung für die Netzwerkmanagement-Funktionen, während die einfachen Änderungen an den Netzwerkfunktionen durch die zentrale Steuerungsschicht erlaubt sind. Mit SDN kann man das gesamte Netz, durch eine intelligente Orchestrierung und ein Bereitstellungssystem, als „On-Demand-Ressourceallocation“ verwalten.

Grundannahmen der neuen Netzwerkarchitektur [22]:

- Durchflusserkennung - Forscher halten die Durchflusserkennung für wichtig [22].
- Netzwerk-Adressierung - Adressierung sollte intuitiv sein und sich auf Dienstleistungen und Menschen beziehen und nicht auf die Schnittstellen.
- Routing-Protokolle – sie sollten zuverlässiger und stabil sein.
- Nutzung Struktur
- Dynamische Leitungsvermittlung
- Backbone-Design - Backbones sollten vorhersehbar, störungsfrei und stabil sein.
- Alle Modelle folgen dem End-to-End-Prinzip.
- Cross-Layer-Design - Es besteht kein Zweifel, dass das Schichtenmodell zahlreiche Vorteile bietet, aber es ist auch ineffizient.
- Netzwerk-Virtualisierung – Die Netzwerkinfrastruktur sollte sich im Laufe der Zeit weiterentwickeln.

In diesem Bereich wurden einige grundlegende Ideen über das Internet der Zukunft vorgestellt.



Derzeit gibt es viele Projekte, die gleichzeitig laufen und daran arbeiten, unbeschriebene Tafel Internet-Konzept zu erstellen. Diese Forschung steckt immer noch in den Kinderschuhen, daher ist es schwierig, darüber zu sprechen und die Netzarchitektur und Trends zu prognostizieren. Viele Forscher arbeiten daran und jede Forschungsgruppe hat dazu ihre eigene Sichtweise. Aber eines ist klar: Da das aktuelle Internet auf der Basis der IP mehr als 40 Jahren alt ist, müssen wir uns bereits mit seinen Grenzen und auseinandersetzen. Unbeschriebene Tafel Internet-Konzept wird sehr wichtig sein und seine Bereitstellung ist nur eine Frage der Zeit.
