SD-WAN

Die Zukunft der WAN Welt

Whitepaper

ITENOS

Inhaltsverzeichnis		Seite

1 Einleitung

In diesem Whitepaper werden SD-WAN Leistungen im Grundsatz erklärt und ein Überblick zu potenziellen Lösungen für die WAN-Anforderungen von Geschäftskunden dargestellt. Außerdem werden SD-WAN-Dienste mit traditionellen MPLS-Diensten verglichen, um darzulegen, ob diese durch SD-WAN ergänzt und erweitert oder vielleicht sogar komplett ersetzt werden können.

2 Definitionen von SDN bis NFV

Bei SDN und NFV handelt es sich im Grundsatz um allgemeine technologische Konzepte und nicht um bestimmte Technologien (wie etwa bei MPLS oder LTE) oder um eine spezielle Dienstleistungskategorie für Unternehmen.
SDN und NFV tangieren alle Aspekte der klassischen IT- und Telekommunikationsinfrastruktur und Produktionsplattformen. Die ersten SDN/NFV-Implementierungen wurden vorwiegend in großen Datacentern realisiert. Zukünftig werden diese Konzepte Auswirkungen auf alle Netze und Dienste für Privat- und Geschäftskunden haben.

SDN (Software-Defined Networking) ist eine Netzkonzeption, die zwei wesentliche Funktionselemente von Netzen trennt und abstrahiert, nämlich die Control Plane (Signalisierung und Steuerung) und die Data Plane (Weiterleitung und Routing der Playload-Pakete, d.h. der tatsächlich nutzbaren Daten). Bei SDN sind Netzdesign und -administration in den zentralen Controllern implementiert (auf der Basis von universellen Hochleistungsservern), die Instruktionen an zahlreiche kostengünstigere und mit „wenig Intelligenz“ versehenen Netzknoten verteilen (beispielsweise universelle Router, Switches, Zugangspunkte usw.). Verglichen mit herkömmlichen, proprietären Netzgeräten (auch „black box“ genannt), die Software („Intelligenz“) und Hardware in einem Gerät kombinieren, wird die „Intelligenz“ hier von den Netzknoten getrennt und auf eine im Netzdesign dezentralere Ebene verschoben. Ein wesentlicher Vorteil hierbei ist die Möglichkeit, das Netzdesign inkl. Spezifikation und die Administration per Software programmieren zu können. Daher werden SDN-Konzeptionen bisweilen auch als „programmierbare Netze“ bezeichnet.

NFV (Network Function Virtualization) ist ein konzeptioneller Ansatz zur Virtualisierung von Funktionen auf einem Device. Dies ist bereits grundsätzlich eine State of the Art Technologie in der IT. In der TK Branche basieren die meisten Endgeräte heute auf proprietären Software Ansätzen auf getrennten Hardware Devices. Ein Ziel von NFV ist die Kosteneinsparung, indem preiswertere universelle Hardware bei der Netzimplementierung eingesetzt wird. Darüber hinaus gilt es bei NFV einen höheren Grad an Flexibilität zu erzielen, indem Funktionen und Features schneller geändert, hinzugefügt oder gelöscht werden können, d.h. in diesem Fall per Software (SDN), die diese Komponenten steuert. Alles in allem sind SDN und NFV unabhängige Konzepte, die aber, wenn sie optimal kombiniert werden, die Vorteile jedes einzelnen Konzeptes noch potenzieren.

Hybrid Access bezeichnet im Kontext der SD-WAN Vernetzung die parallele Nutzung „privater“ Plattformen (MPLS / Ethernet) und öffentlicher Netze (Public Internet). Mit dieser Konstellation wird dem zunehmenden Bandbreitenbedarf Rechnung getragen, der meist aber nicht geschäftskritisch ist und somit auch über qualitativ niederwertige Transportwege geleitet werden kann.

Der **Over The Top** (OTT) Ansatz legt sich „über“ die vorhandene, meist hybride Netzstruktur. Die Endgeräte werden über Ethernet „hinter“ die BestandsAccess-Abschlussrouter geschaltet und nutzen die vorhandenen Verkehrswege optimal aus. Dabei wird die Entscheidung der Verkehrsführung („Intelligenz“) aus den bisherigen Instanzen (z.B. MPLS Abschlussrouter und MPLS Plattform) an die SD-WAN fähigen Endgeräte übertragen.

Das **Dual Box Design** repräsentiert den klassischen OTT Ansatz, bei dem hinter dem Abschlussgerät des Anschlusses ein weiteres und dann SD-WAN fähiges Gerät geschaltet wird. Mit dem **Single Box Design** werden die verschiedenen Funktionen (Routing, Firewall, SD-WAN, …) in einem Gerät virtualisiert zusammengeführt. Dies bringt deutliche Kostenvorteile durch geringeren Hardwareeinsatz und verbesserte betriebliche Möglichkeiten bei jedoch höherem Integrationsaufwand in Netzplanung und Geräteentwicklung.

Mit Hilfe von **Deep Packet Inspection (DPI)** können tiefergehende Verkehrsinformationen genutzt werden und damit die Datenströme besser verstanden werden. Der Verkehr kann anhand verschiedener Parameter bewertet werden und durch das Mapping mit Vorgaben effektiver behandelt werden. So ist daraus z.B. das Setzen von DSCP Werten ableitbar. Auch die Kombination von DPI mit Firewall Lösungen erhöht die dringend benötigte erhöhte Absicherung z.B. gegen Malware oder unterstützt dabei, verhaltensauffällige Applikationen zu identifizieren und zu blockieren. Die durch diese Anwendungen benötigte höhere Rechenleistung führt heute noch zu einem signifikant höheren Hardwareeinsatz.

Auch wenn SD-WAN Technologien die Leitungsqualität aktiv auf Paketverluste und das Einhalten von SLAs überprüfen und entsprechend der Vorgaben die Verkehre leiten, kann diese Technologie jedoch keine Voraussagen über zukünftiges Verhalten machen. Genau dort setzen heutige Ansätze der **Künstlichen Intelligenz (KI)** an. Sie werten vorhandene Informationen (Statistiken, Verhaltensmuster im Netz) langfristig aus und nutzen diese, um moderne Netze besser zu steuern und zur Orchestrierung von Verbindungen. Auch kann auf neuen Anwendungsmustern oder Fehlverhalten besser und schneller reagiert werden, ohne in einen definierten ggf. aber suboptimalen Standard bzw. Notfallmodus zu fallen, bis der Mensch eingreift.

3 WAN- und SD-WAN Kundenanforderungen

Eine der wesentlichen Anforderungen, die dem SD-WAN Ansatz zugrunde liegt, ist der Wunsch nach Kostenoptimierung im WAN Umfeld. Ein wesentlicher Treiber dieses Wunsches ist das geänderte Nutzungsprofil hin zur Nutzung öffentlicher Cloud Lösungen sowie dem enorm zunehmenden Bandbreitenbedarf über das öffentliche Internet. Heute begegnet man dieser Anforderung u.a. durch eine erhöhte Flexibilität bei der Providerauswahl und zunehmender Einbeziehung von direkten, kostengünstigen Internetzugängen an den dezentralen Standorten. Gegenläufig zu diesen Einsparungen steht der erhöhte Hardwareeinsatz, weitergehende Sicherheitsmaßnahmen im Endgerätebereich oder auch die Beauftragung von Sicherheitsdienstleistern mit Internetzugängen.

Kundenrelevanz: Hoch → Gering

Anforderung an Unternehmens WAN	MPLS	SD WAN	Lösungsansatz
Kostenoptimierung	○	◑	One Box Design/Nutzung Internet
Sicherheit	●	◑	Application Firewall
Verfügbarkeit (SLA)	●	◑	Access Diversity
Bandbreite / Skalierbarkeit	●	●	Access Bundling
Flexibilität	◑	●	Service Portal/Mix Betrieb
Connectivity zu Cloud Services	◑	●	Cloud Service Connectivity
Bandbreitenbedarfsmanagement	◔	●	Dynamic Path Selection
Performance Management der Anwendungen	◑	●	Application Based Routing
Schnelle Implementierung neuer Dienste	◔	●	VNF Technologie
Schnelle Bereitstellung	◔	●	Zero Touch Provisioning

Kundenanforderungen im WAN

Zur Umsetzung der Kundenanforderungen gibt es verschiedene Lösungsansätze, die in unterschiedlichen Kundensituationen andere Gewichtung finden. So ist z.B. in kleinen Filialen der Einsatz von uCPE im klassischen OTT Ansatz (mit Dual Box Design) gegenüber einer Single Box Lösung wirtschaftlich abzuwägen, auch wenn diese ggf. nicht dem aufwändigen NFV Technologieansatz vollständig folgt.

Lösungsansatz	Beschreibung Lösungsansatz
Access Diversität	Durch den Einsatz kostengünstiger alternativer Internet Anbindung
Application Firewall	Absicherung über Firewall (UTM, Unified Tread Manager).
Lokaler Internet Break Out	Kürzester und schnellster Weg für den Internetverkehr
Access Bundling	Flexible Hinzunahme von Internetbandbreite bei Bedarf
Cloud Services Connectivity	Privat Cloud via Privat Access Carrier oder Public Cloud via Internet
Dynamic Path Selection	Application Based Routing mit Deep Paket Inspection (DPI)
Service Portal	Monitoring, aktiver rollenbasierter Anstoß von Geschäftsfällen
One Box Design	Kostenoptimierung durch Hardwareeinsparung
Zero Touch Provisioning	Kostenoptimierung durch Prozessoptimierung

Lösungsansätze zu Kundenforderungen

Bewertet man Lösungsansätze hinsichtlich ihrer Geschäftskritikalität vs. ihrer Auswirkung auf die Kosten, so ergibt sich nicht für alle Ansätze eine direkte aus Kundensicht „fühlbar“ positive Auswirkung. So hängen z.B. Zero Touch Mechanismen im Access Provisioning in erster Linie vom Automatisierungsgrad des Access Providers im Zusammenspiel mit dem OTT-Provider ab und Kosteneinsparungen bei der Hardware im Rahmen eines One Box Designs vom Zusammenspiel der Hardwarehersteller und Access/OTT Provider ab.

4 SD-WAN

SD-WAN ist keine Netztechnologie oder ein definierter Netzstandard, sondern ein Architekturansatz, der auf den oben genannten Technologieansätzen einen Endkundendienst mit den beschriebenen Vorteilen generiert. Dieser wird auf den Endgeräten beim Kunden abgebildet und „orchestriert“ den Aufbau des Verbindungsnetzes, dem Overlay, über die verschiedenen WAN Verbindungen.

Im Wesentlichen bestehen SD-WAN basierte Lösungen aus den folgenden Leistungselementen:

- **Hybrid Access im Underlay**
  Unterstützung diverser Zugangstechnologien via Kupfer, Glasfaser und Funk, nutzbar als Privat Access über L3 Anschlüsse (IP VPN-MPLS) oder L2 Anschlüsse (z.B. Ethernet PtP , PtMP) und Internetzugänge als Public Access.

- **Verbindungsorientiertes Overlay Netzkonzept**
  Aufbau eines zugangs- und plattformunabhängigen Verbindungsnetzwerkes mittels SD-WAN.

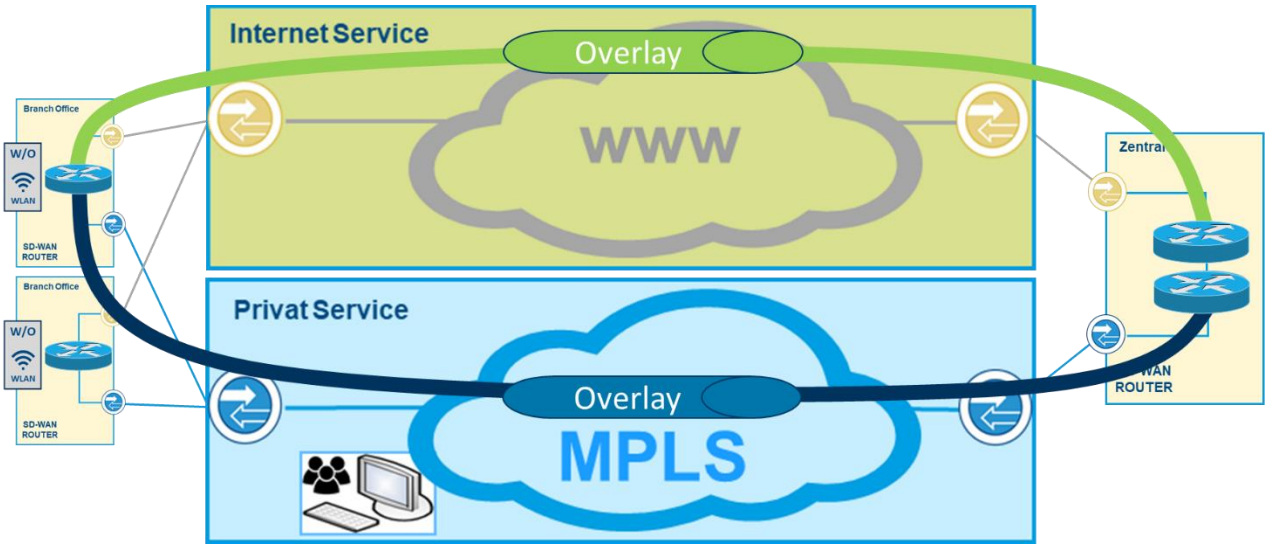
- **Dynamisches Applikation/Performance based Routing**
  Dynamische optimierte Lastverteilung über die verschiedenen Zugangstechnologien/Netze abhängig von der den Applikationen zugewiesenen Regeln und der aktuellen Performance der Verbindungen.

- **Service Portal/Zero Touch Provisioning (ZTP)**
  Bereitstellung einfacher Administrationsschnittstellen zur Steuerung der Verbindungen z.B. über Self-Care/Self-Service Portale oder die Anbindung der Kundensystems via Application Programming Interfaces (API).

- **Virtual Network Functions (VNF)**
  Implementieren von VNFs hinsichtlich Security, WAN-Optimierung oder auch Cloud-Konnektivität

Natürlich werden hybride WAN-Zugänge bereits sehr viel länger als SD-WAN am Markt angeboten und genutzt. Hierbei werden Unternehmensstandorte i.d.R. bereits heute mit zwei WAN-Verbindungen angebunden, die über verschiedene Zugangstechnologien (MPLS, Breitband-Internet, LTE usw.) realisiert werden. Der Verkehrsfluss wird dann aber meist statisch eingerichtet. Dementsprechend ist SD-WAN eine Weiterentwicklung, die dem hybriden WAN-Zugang zusätzliche Dynamik und Flexibilität verleiht. Zudem sind viele Mechanismen zur Steuerung des Verkehrsflusses heute mit den zentralen Plattformen (z.B. MPLS)

verbunden. Diese Intelligenz verlagert man nun in die SD-WAN Endgeräte und steuert und konfiguriert diese über plattformunabhänge Instanzen (SD-WAN Controller).



Beispiel SD-WAN Netz

In diesem Zusammenhang kommen auch sogenannte universal Customer Premises Equipment (uCPE) zum Einsatz. Die uCPE ist eine sogenannte White Box, also ein Universeller PC/Server ohne bekanntes Branding, die normalerweise auf einer x86-Architektur von Intel basiert. Die Hardware verwendet vorwiegend offene Standards, Komponenten und Schnittstellen. VNFs können so per Download direkt auf die uCPE des Kunden geladen werden und dort neue Funktionalitäten ermöglichen. Diese offene uCPE Konzept führt im Zielbild zu einer größeren Vielfalt an funktional hochwertigen Applikationen.

5 Die Zukunft von traditionellen MPLS-Lösungen

Die Nachfrage nach traditionellen voll gemanagten IP VPN auf Basis MPLS ist in den nächsten Jahren stagnierend bis zunehmend rückläufig prognostiziert. Grundsätzlich werden traditionelle MPLS-Offering in absehbarer Zeit weiterhin relevant bleiben und auch eine wichtige Rolle als Underlay Netz-Technologie für SD-WAN spielen.
Dies resultiert im Besonderen daraus, dass der Einsatz von heute meist Best-Effort Internetzugängen als Zugangstechnologie viele Einschränkungen hinsichtlich Servicequalität und Datensicherheit mit sich bringt. So werden bei günstigen Privatkundentarifen geschäftskundentaugliche Service Level derzeit meist nicht angeboten. Auch ist die Transportqualität aktuell oft sehr gut jedoch nicht zugesagt und für die Zukunft bei massiv steigendem Internetverkehr nicht sichergestellt.
Zudem fördert die zunehmend bessere Mobilfunkqualtität bei sinkenden Preisen den Trend ins Internet. Zukünftig werden sich LTE basierte Ansätze nicht mehr auf den Einsatz als Backup im Notfall reduzieren, sondern zu einem ernsthaften Substitut der Festverbindungen reifen.

Mit SD-WAN sind also Kosteneinsparungen möglich, jedoch nicht in jeder Kundensituation bzw. nicht an allen Standorten. MPLS ist nach wie vor hervorragend geeignet, um hochwertige Service SLAs zu vereinbaren, insbesondere für große Standorte und Schlüsselanwendungen. Weiterhin sind MPLS Netze nach wie vor prädestiniert, wenn es um die Aufteilung und Priorisierung des Verkehrs geht und somit zur Realisierung sehr guter Performance SLAs.
Daher spielt MPLS definitiv weiterhin eine wichtige Rolle für die Anbindung größerer Standorte und im Allgemeinen für Standorte mit einer komplexen Anwendungslandschaft, so z.B. bei diversen Echtzeit-Anwendungen. Zudem gibt es ganze Kundengruppen wie die öffentliche Verwaltung, Banken oder Firmen aus der Fertigungsbranche, die teilweise aus gesetzlichen Gründen bzw. auf Grund ihrer eher konservativen Haltung hinsichtlich neuer Technologien weiterhin traditionellen MPLS-Netzen den Vorzug geben.

Die Kombination aus MPLS und Internet verknüpft mit SD-WAN ist bislang eine sehr gute Option zur Optimierung traditioneller heute auf MPLS basierender IP VPNs.