AALBORG UNIVERSITY
COPENHAGEN

Semester: 4th semester

Title: Analysis of Software-Defined Wide-Area Networking

Project Period: February 2018 - June 2018

Semester Theme: Thesis

Aalborg University Copenhagen
A.C. Meyers Vænge 15
2450 København SV

Secretary: Maiken Keller

Abstract:
This thesis is going to analyze one of the hottest topics in networking today, the Software-Defined Wide-Area Networking. The research will be based on literature and standards review on the subject and it will aim to provide a comprehensive analysis with practical implications. The analysis, structured in two main parts, will explain to the reader: part 1 - what are the main principles of SD-WAN; and part 2 - how it compares to its rivals. The second part will be based on "The Art of Standards Wars" theory by Carl Shapiro and Hal R. Varian. One outcome of the research is that the fusion of SD-WAN and its major adversary - Multiprotocol Label Switching VPN will most probably represent a large part of the WAN market in the near future.

Supervisor(s):
Morten Falch
Samant Khajuria

Project group no.:
4BUS 4.13

Members
(do not write CPR.nr.):
Mario Todorov

Pages: 76
Finished: 06.06.2018

Aalborg University - Copenhagen

Master's Thesis

Analysis of Software-Defined Wide-Area Networking

Author:
Mario Todorov

Supervisors:
Morten Falch
Samant Khajuria

A thesis submitted in fulfillment of the requirements for the degree of M.Sc. in Engineering of Innovative Communication Technologies and Entrepreneurship

in the

Center for Communication, Media and Information Technologies
Dept. of Electronic Systems

June 7, 2018

“Real difficulties can be overcome; it is only the imaginary ones that are unconquerable.”

Theodore N. Vail

AALBORG UNIVERSITY - COPENHAGEN

Abstract

Technical Faculty of IT and Design
Dept. of Electronic Systems

M.Sc. in Engineering of Innovative Communication Technologies and Entrepreneurship

Analysis of Software-Defined Wide-Area Networking

by Mario Todorov

This thesis is going to analyze one of the hottest topics in networking today, the Software-Defined Wide-Area Networking. The research will be based on literature and standards review on the subject and it will aim to provide a comprehensive analysis with practical implications. The analysis, structured in two main parts, will explain to the reader: part 1 - what are the main principles of SD-WAN; and part 2 - how it compares to its rivals. The second part will be based on "The Art of Standards Wars" theory by Carl Shapiro and Hal R. Varian. One outcome of the research is that the fusion of SD-WAN and its major adversary - Multiprotocol Label Switching VPN will most probably represent a large part of the WAN market in the near future.

Acknowledgements

I would like to first express my gratitude to my supervisors - Samant Khajuria and Morten Falch for their constant support and advisory during my last semester at Aalborg University - Copenhagen. I was very fortunate to receive your guidance and use it in the creation of this master's thesis.

My deepest gratitude is for the never ending support of my family - my mother Antoaneta, my sister Natalia and my father Toshko. A very special thank you goes to my girlfriend Lina, who was an infinite source of inspiration throughout this project.

I would also like to thank my friends and colleagues - Angel, Mihail and Sorin for making this education an exciting and fun experience.

Hristo, thank you for proofreading.
Eduard, this line is for you.

Contents

List of Figures

List of Tables

List of Abbreviations

5G	5th-Generation Wireless Systems
AES	Advanced Encryption Standard
AFI	Address Family Identifier
AH	Authentication Header
AI	Artificial Intelligence
API	Application Program Interface
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
ASIC	Application-Specific Integrated Circuit
ASN	Autonomous System Number
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol version 4
BoS	Bottom of Stack
C	Checksum Present
CAPEX	Capital Expenditure
CE	Customer Edge
CEO	Chief Executive Officer
CLI	Command Line Interface
CMS	Configuration and Monitoring System
CPE	Customer-Premises Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIY	Do-it-Yourself

DMVPN	Dynamic Multipoint Virtual Private Network
DSCP	DiffServ Code Point
DSK	Dvorak Simplified Keyboard
DSL	Digital Subscriber Line
DTLS	Datagram Transport Layer Security
DWDM	Dense Wavelength Division Multiplexing
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FACTS	Framework for Analysis, Comparison, and Test of Standards
FEC	Forward Equivalence Class
ForCES	Forwarding and Control Element Separation
GRE	Generic Routing Encapsulation
HDR	Header
HMAC	Hash-based Message Authentication Code
HP	Hewlett-Packard
HPE	Hewlett-Packard Enterprise
HQ	Headquarters
IANA	Internet Assigned Numbers Authority
IBM	International Business Machines
ICV	Integrity Check Value
IDC	International Data Corporation
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPsec-v3	Internet Protocol Security version 3
IPv4	Internet Protocol version 4

IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IWAN	Intelligent Wide Area Network
IaaS	Infrastructure as a Service
IoT	Internet of Things
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LIFO	Last In First Out
LSP	Label Switched Path
LSR	Label Switched Router
MD5	Message Digest 5
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MSP	Managed Service Provider
NBMA	Non-Broadcast Multiple Access
NFV	Network Function Virtualization
NHRP	Next Hop Resolution Protocol
NIST	National Institute of Standards and Technology
NLRI	Network Layer Reachability Information
OMP	Overlay Management Protocol
ONF	Open Networking Foundation
OPEX	Operational Expenditure
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OVS	Open VSwitch
P	Provider

PE	Provider Edge
PSTN	Public Switched Telephone Network
PaaS	Platform as a Service
PfRv3	Performance Routing version 3
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RD	Route Distinguisher
REST	Representational State Transfer
RFC	Request for Comments
RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
RSVP	Resource Reservation Protocol
RT	Route Target
SA	Security Association
SAFI	Subsequent Address Family Identifier
SD-WAN	Software-Defined Wide-Area Networking
SDH	Synchronous Digital Hierarchy
SDN	Software-Defined Networking
SEN	Secure Extensible Network
SHA	Secure Hash Algorithm
SN	Sequence Number
SNMPv3	Simple Network Management Protocol version 3
SONET	Synchronous Optical Networking
SPI	Security Parameters Index
SSL	Secure Sockets Layer
SaaS	Software as a Service
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live

ToS	Type of Service
UC	Unified Communications
UDP	User Datagram Protocol
USD	United States Dollar
VC	Virtual Circuit
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPN-IPv4	Virtual Private Network - Internet Protocol version 4
VPN-IPv6	Virtual Private Network - Internet Protocol version 6
VRF	Virtual Routing and Forwarding
VSAT	Very-Small-Aperture Terminal
Ver	Version Number
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
ZTP	Zero-Touch Provisioning
mGRE	Multipoint Generic Routing Encapsulation

Chapter 1

Introduction

This thesis is going to focus on the future of Wide Area Networking (WAN) technologies and in particular on the emerging, high potential Software-Defined WAN technology. The previous and existing WAN technologies will be discussed in order to point out their weak and strong points and later compare them to SD-WAN. The technological principles of SD-WAN and its impact on the WAN market will be thoroughly analyzed to show the reader what are the possible scenarios for the evolution of this market.

In this chapter we are going to concentrate on the evolution of WAN technologies, their alternatives and how everything is moving towards cloud-based systems. The motivation for the research will be presented for the reader together with the problem definition. The limitations of the report will be discussed and the chapter will end with a conclusion, based on the aforementioned topics.

1.1 Background

1.1.1 Evolution of Wide Area Networks

Since the emergence of ARPANET in the 1960s, the first TCP/IP computer network, the world has become extremely attached to its modern version - the internet. There are some important historical events that are responsible for the internet as we see it today. The development of Ethernet in 1974 at Xerox PARC and its success as the first widely deployed LAN technology around 1980. [1] The emergence of switching in the 1990s, which replaced the low-functional bridges that were used at that time. [1] The introduction of the first commercial multi-protocol router in 1986 by Cisco, which transformed the computer networking world. [1] All of these events greatly contributed to the research and development in the computer networking field. Later, when networking became available with a commercial purpose, after 1990, there was a need for another type of technology that could connect not only local, but also remote computers. This triggered the emergence of WANs. The first form of a WAN were the so called leased lines, which were simple private connections that

required shared media, through which the individual connections of different customers were multiplexed. The first commercial packet-switched WAN technology, however, was Frame Relay. It was designed to replace leased lines and form a single protocol independent packet-switched WAN. [1] Another important WAN technology that started the shift from packet to cell-switched networks was ATM, in the late 1980s. The rivalry lasted nearly a decade until packet-switched networks took over and became the standard for the modern internet. [1] The next WAN technology that we are going to mention is still the dominant WAN technology today, from its creation in 1999. [2] This technology is named MPLS and it is standardized by IETF in RFC3031. MPLS is based on tag switching, a Cisco proprietary solution that started in 1998 and focused on labeling IP packets. [2] All of the aforementioned WAN technologies have one major similarity. They require the services of a telecom provider, which is responsible for their management and provides them as a service to potential customers. Therefore the customers depend on the specific Frame Relay, ATM or MPLS network that their ISP operates. It is important to note that these networks are not connected to the internet itself and are meant only for private communication between corporate sites.

1.1.2 Virtual Private Networks

There is, however, another way to form WAN connections between corporate sites that leverages the existing internet infrastructure and does not depend on a specific service. This method is named Virtual Private Networking. VPNs are extremely cost effective, scalable and flexible solutions that can be used as an alternative to the aforementioned WAN technologies. [3] VPNs use the available public infrastructure, the internet, to realize a virtual WAN between corporate sites. Since the internet is a global network, it provides the capability to connect sites from all around the world. VPNs also provide one other option that traditional WAN solutions don't. That is the opportunity for remote access to the company's infrastructure, which can be initialized from any location with internet access. There are also downsides of this technology. There are no current standards for the VPN solutions, which makes the choice between the abundant variations of VPN products a tough job. The biggest advantage for enterprises in using VPN solutions over traditional WAN is their price, however, benefits like traffic reliability and effective QoS are only offered from the traditional WAN solutions. [3] There are two major VPN solutions that we are going to look into in this thesis. The first one is IPsec. IPsec is a set of protocols that are used to form a secure channel over the internet at the IP layer and it is mostly used for the creation of VPNs. [4] IPsec can be used with both IPv4 and IPv6 to provide high-quality traffic security over the internet. [5] The second VPN solution is DMVPN. Dynamic

Multipoint VPN is a Cisco proprietary solution that offers highly scalable and automated VPN services. [6]

1.1.3 Going Software-Defined

It is clear nowadays that the digital world is moving towards cloud-based everything. From applications to network communication, the cloud is consuming its rivals at a rapid pace. It is especially interesting how the cloud is going to transform the WAN market with the emergence of SD-WAN - a cloud-centric networking approach, leveraging the software-defined networking principles. SD-WAN is one of the hottest topics in networking today and this is due to the fact that it combines the Software-Defined Networking, the cloud and the WAN market sectors. [7] With the increasing demand for high-bandwidth network traffic that is expected from technologies like Artificial Intelligence (AI), Internet of Things (IoT) and 5G, it is expected that by 2020 digital enterprises will need more than 5,000 terabits of interconnection bandwidth to function properly. [8] This amount of traffic will require a more scalable and cloud-friendly enterprise network model than the current market leader - MPLS. Businesses will require a flexible, cloud-ready and easily managed network communication service that is highly scalable and inexpensive. SD-WAN is designed to allow enterprises not only to connect their branch offices, as traditional MPLS WAN, but also to provide fast connectivity to all of the necessary cloud applications. Another major point of SD-WAN is its lack of configuration complexity. The separation of the control plane from the data plane, which is the major principle of SDN, allows for a centralized configuration model, which is easily administrated. But is SD-WAN going to completely replace the current MPLS and DMVPN WAN solutions? Probably not. SD-WAN, however, is capable of utilizing both the internet and the existing MPLS network in order to offer the best possible WAN optimization for the business. Therefore, SD-WAN and MPLS are able to coexist if there is sensitive traffic that can justify the MPLS cost. Another important aspect is how will this new technology affect the current WAN market. ISPs are used to being the major player in the WAN game and are certainly afraid from the numerous SD-WAN solutions that continue to emerge. Is this new technology going to take the WAN market away from ISPs and place it in the hands of cloud providers? These are certainly very important questions that people in the telecom sector are wondering about. The answers will be responsible for shaping the new look of the WAN sector and the digital world of the future with it.

1.2 Motivation

After decades of repetitive configurations, network engineers are looking forward to an approach that will ease the network management process and bring more automation into it. The software-defined approach is the closest to that idea so far. It allows for a separation between the brains and muscles of the network and brings a high level of programmability in the networking game. [9] The application of the software-defined principles in the WAN sector is realized through the SD-WAN technology. From an emerging technology in 2017, SD-WAN is rapidly becoming closer to the leadership in the sector in 2018. [10] This fast transition is the biggest change in the WAN market for its existence and deserves to be analyzed. As SD-WAN vendors are independent from telecoms and their solutions rely solely on the internet, a drastic shift in the market is expected to happen. The need for research in the field is of a great importance to networking professionals and will contribute to the better understanding of the evolution of WANs. There are already success stories with the adoption of SD-WAN that drive towards further research in the field. City and Guilds Group reported that they noticed triple improvement in the performance of their Office 365 applications across their global network infrastructure, after they have deployed a SD-WAN solution. [11] The financial expectations for the SD market are also considerable, as SD-Branch solutions are expected to reach 3 billion USD by 2022. [12] There is a need for a comparison between SD-WAN and its current rivals that is going to lay out the benefits of each technology and clear the picture for the WAN market.

1.3 Problem Definition

The purpose of this thesis is to analyze the SD-WAN technology and its impact on the WAN market. A comparison with other WAN solutions, such as MPLS VPN, IPsec VPN and DMVPN, is intended to show the reader what are the advantages and disadvantages of the SD-WAN technology. The analysis is going to bring out the current status of this new technology on the WAN market and serve as a starting point for future research about the evolution of WANs.

Problem formulation

How the Software-Defined Wide-Area Networking technology compares to the current WAN solutions? This is going to be the major question that this thesis is going to provide an answer to. The answer will be provided after analyzing and comparing the SD-WAN technology to the three major WAN technologies used today, through the use of a relevant theoretical

framework.

Sub-questions

What are the benefits of the current WAN technologies? The answer to this question will be provided in chapter 5, after introducing the three major competitors of SD-WAN in chapter 4. The intention of this question is to use these benefits to point out where SD-WAN needs to improve.

What are the benefits of SD-WAN? After extensive analysis in chapter 5, the benefits of this new technology will be examined. This will give the reader a clear view of the potential of this new technology.

Is there a chance for SD-WAN to become a major standard? After discussing the relevant theoretical framework that is going to be used for the analysis in chapter 3, it will be used to assess the market potential of SD-WAN in the analysis.

1.4 Limitations

The examined technologies in this thesis will be discussed in technical details and previous technical knowledge is required in the field of computer networking. The research is going to take a practical approach and the upcoming vendor discussion will be focused only on the major network vendors and their subsidiary companies. Since all of the SD-WAN solutions are proprietary, the most specific details around the technology are inaccessible. Therefore, the analysis will introduce SD-WAN based on general principles of operation. The thesis is solely based on literature and standards review and no expert interviews or case studies were conducted. Interviews with experts from the WAN, cloud or SDN sectors would have contributed to a better understanding of the problem and added additional value to the report. Also, interviews with experts from the marketing field would have contributed to a better understanding of the WAN market functionality and improved the quality of the market analysis. Including a case study in the thesis would have provided some inside knowledge from the business. Another limitation is that the thesis focuses on only one theoretical framework. A more detailed analysis would have been possible if multiple frameworks were introduced in the report.

1.5 Conclusion

We can see from this chapter that WAN technologies have come a long way since their invention. They are now part of a dynamic market, with strong competition between the different network vendors that continues

to evolve. Also the VPN technologies are an important part of this market. The rapid evolution of the digital world and especially the ever-increasing demand for high bandwidth is transforming the WAN industry. This transformation is aiming towards increased automation, centralized network management and flexibility. The achievement of these goals is going to be realized with the help of software-defined networks and specifically for the WAN - with the help of SD-WAN.

Chapter 2

Methodology

2.1 Introduction

This chapter focuses on the specific research and analysis methods that are used to obtain the research data, in order to provide an answer to the problem formulation. We are going to follow a pragmatism-based research philosophy throughout the thesis and focus on practical information. Both subjective and objective points of view will be considered when analyzing the SD-WAN technology. The research methods will be based on secondary data sources and no primary data will be collected.

2.2 Applied methods

The investigation part of the project is focused on the technical principles of the chosen WAN solutions and SDN. It is designed to show the reader what these technologies are and how do they function. The research forms the foundation for the theoretical framework that is to be used in the thesis. Literature and standards review is the main method for the research carried throughout the "State of the art" chapter. The research will be using a combination of descriptive, explanatory and qualitative methods for gathering data. This data is later going to serve as a foundation for the analysis, which will be based on the standards wars theory, discussed in chapter 3. The structure of the research is shown in figure 2.1.

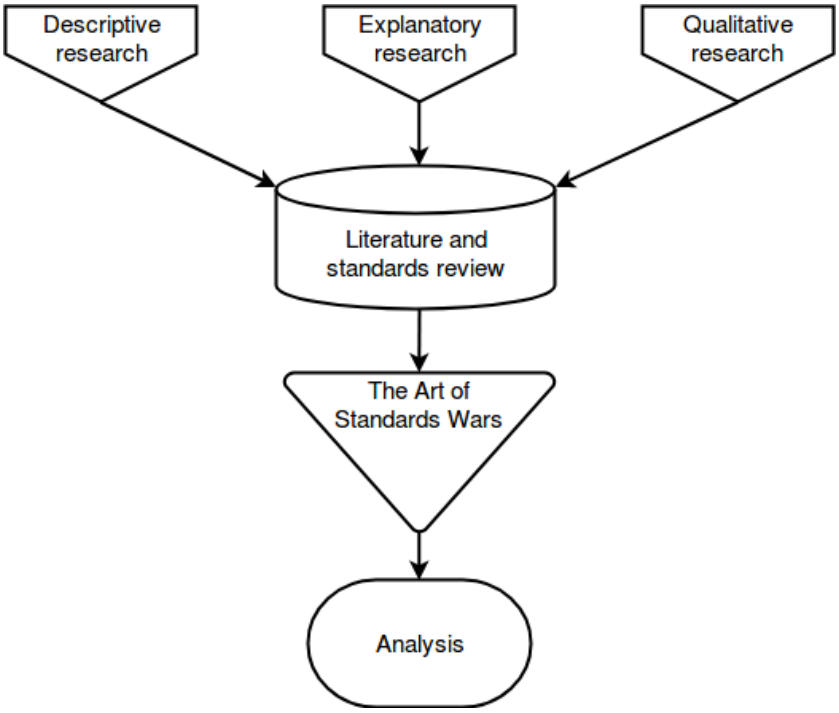

Figure 2.1: *Methodology framework*

Descriptive research

A descriptive research is mainly focused on fact-finding and interpretation. [13] One of the first examples of descriptive research - the Domesday Book, dates back to 1085 and it was used to describe England's population. [14] Throughout this thesis descriptive research is used to provide the reader with a clear understanding of the principles of the current WAN solutions. This is necessary, in order to allow for comparison between SD-WAN and other WAN solutions. However, a strict descriptive research is not enough for the purpose of this thesis. The descriptive research will be used as a starting point for its incorporation with explanatory research.

Explanatory research

Explanatory research studies focus on the correlation of different events [14], or in the particular case of this thesis - different technologies. The idea is to research a specific technology and gain the necessary knowledge for the explanation of its components and their relations. The relation between the different WAN technologies will be explained, so that SD-WAN can be analyzed on top of that. This will provide the reader with a broad view on the benefits and drawbacks of SD-WAN, in comparison with the other three technologies.

Qualitative research

Qualitative research is based on qualitative data, which represents data from all types of research that is non-quantitative. [14] By non-quantitative we refer to data that is not measured by numbers. Typical examples of qualitative data sources are questionnaires and interviews. A good strategy for qualitative research is to structure the data in specific sets and subsets. In this way, it can later be used conveniently for the analysis. According to [14], there are three major principles of qualitative data research:

- Meaningfulness
- Data classification
- Conceptual analysis

The gathered data will be based on meanings, in the specific case - technology explanations. It will also be classified into multiple sections and subsections. Different types of figures will also be used throughout the report to provide a more detailed and concept-oriented view on a specific problem, mostly technology examination. A small portion of quantitative-based data will also be used in the thesis, in order to provide relevant details for the research.

Analysis

The analysis is going to start with a detailed overview of the SD-WAN technology. Afterwards it is going to use the data gathered from the research part in order to answer the problem formulation. Standards wars, discussed in chapter 3, is the theoretical framework that will be used to compare the different WAN standards to SD-WAN and that will be the main method for conducting the analysis. A technology comparison will also be part of the analysis. It will serve as a discussion on the benefits of each of the examined standards.

2.3 Conclusion

In this chapter, we discussed the research methods that are going to be used in this thesis and uncovered the theoretical framework that will be used for conducting the analysis. The intention of the chapter is to simply provide an overview of how the research is structured and what methods are going to be used throughout the report. In the next chapter we are going to explain the principles of the chosen framework and discuss their application in the analysis.

Chapter 3

Theoretical framework

3.1 Introduction

This chapter is going to focus on the theoretical framework that is to be used in order to conduct the analysis on SD-WAN. The WAN solutions - MPLS VPN, IPsec VPN, DMVPN and SD-WAN are going to be viewed as different standards for the realization of wide area networks. This methodology is going to allow us to use the theory of standards wars [15] and analyze the potential of SD-WAN. But why did we decide to use exactly the standards wars theory for this purpose? Let us now examine some other alternatives to the chosen framework and discuss why we decided not to use them. An alternative to the standards wars framework, that is focused on the life cycle of new and innovative technologies is the hype cycle model. The hype cycle model is a framework developed by Gartner, that follows the path of a product's expectations and value over time. [16] It could have been used for the purpose of this thesis, but the hype cycle framework does not provide the detailed comparison methods found in the standards wars theory. [15] Also, there are some concerns with the consolidation of the two primary models that the hype cycle theory is based on - the hype expectations model and the technology S-curve model. [17] Another alternative is the diffusion of innovation theory by Everett Rogers. [18] This is a solid theory on technology acceptance, which main goal is to examine the growth process of a given technology, from its initial stage to its mass adoption on the market. [19] Diffusion of innovation would have served as a good framework for the research on SD-WAN's user acceptance, but it lacks the comparison methodology, intended by the author. [20] A similar standards-oriented framework - FACTS [21], developed by NIST was also considered as an alternative to the chosen one. However, in order to fully express the original idea behind this thesis, the author decided to use the standards wars theory, with one addition. A technology comparison, focused solely on the technical benefits of each of the examined solutions is intended to complement the more market-focused theory of standards wars and provide a broader view on the WAN rivalry.

3.2 Standards wars

Standards represent specific, in the case of this thesis - technological specification sets that are used for compatibility between devices manufactured by different vendors. [22] The process of adopting a standard in a given market by all of the players is referred to as standardization. [23] The battles between competing standards throughout the process of standardization is known as standards wars. These battles were always a significant part of the computer world. There are numerous examples of how one standard defeated its alternatives and started its domination on the market. For example, the QWERTY keyboard layout is a typical case, where one standard became the undisputed market leader. The QWERTY keyboard was originally created for typewriters and started to emerge in the US and British markets after 1909. [24] Although there is an alternative to the QWERTY keyboard, that is proven to be more efficient in the manner of speed - the Dvorak Simplified Keyboard (DSK), QWERTY has retained its leadership on the keyboard market. Another example, that we have already mentioned in chapter 1 is the battle between cell and packet switching that lasted almost a decade. According to [25], there are some important benefits of cell switching, regarding hardware implementation, delay and network throughput. However, cell switching has not been considered as a valid alternative since the 1990s. Why? There is apparently something more in the battles of standards, that goes beyond the standard's efficiency. Multiple factors are to be considered when discussing whether one standard is going to defeat its competitors and they are going to be examined in this part of the thesis. There are three possibilities for the end result of standards wars - truce, duopoly and fight to the death. [15]

3.2.1 Types of standards wars

There is more than one type of standards wars and usually the classification is done through comparison between the compatibility of the new and current solutions. There are six different types of standards wars - Evolution, Revolution, Rival Evolutions, Evolution versus Revolution, Revolution versus Evolution and Rival Revolutions. [15] The Evolution strategy implies that a company has created a new, superior technology that is compatible with the old one. Evolution focuses on the creation of a better product with minimum adoption costs. Revolution, on the other hand, imposes a completely new technology that is incompatible with the old one. The focus with Revolution strategies is to provide such high performance for the customer that he willingly pays the necessary cost for switching to the new standard. Rival Evolutions is considered when there are two new players in the game. The strategy is considered when both new rival technologies are compatible with the old standard, but incompatible with

each other. An important example for Rival Evolutions in the computer world is the ever lasting battle between the different Linux distributions. An interesting case is the case of Evolution versus Revolution. In this type of standards war, one of the new competitors offers backward compatibility with the old technology and the other one does not. It is a battle between the enhanced, backward compatible and cost efficient choice and the superior, backward incompatible and more expensive one. Depending on who is offering the evolution and revolution strategies, the name for this standards war type can be flipped around to Revolution versus Evolution. In the last case, Rival Revolutions are designed for wars between two new technologies that are both backward incompatible. An example for this strategy is the case of Nintendo 64 versus Sony Playstation. [15] The examined types of standards wars are shown in figure 3.1.

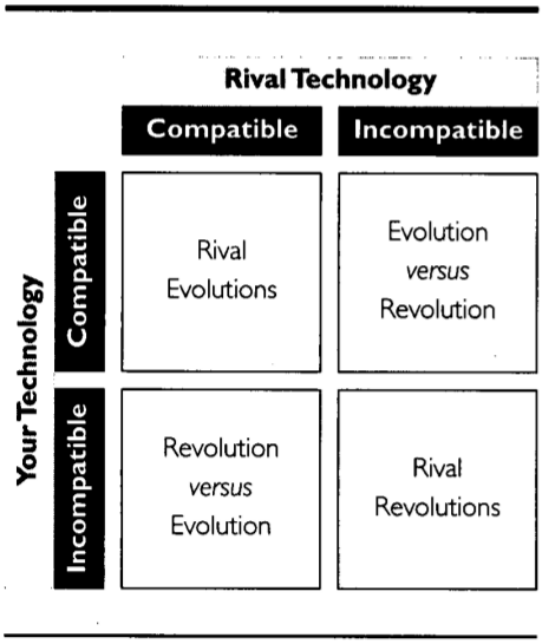

Figure 3.1: *Types of standards wars [15]*

De facto and de jure standards

Here we are going to examine two important types of standards - de facto and de jure. A standard is considered de facto, in the case where it is established on the market through a standards war. [15] An example for a de facto standard is the QWERTY keyboard layout that we mentioned in the beginning of this chapter. De jure standards, on the other hand are established through consensus between the different market players. [23] Example for a de jure standard can be the OSI reference model.

3.2.2 Key assets

There are several key assets that are considered as major points when waging a standards war - Control over an Installed Base of Customers, Intelleaual Property Rights, Ability to Innovate, First-Mover Advantages, Manufacturing Capabilities, Strength in Complements and Reputation and Brand Name. [15] According to [15], the ownership of these assets places the competitor in a high potential situation for market dominance. It is important to note that big customers and suppliers are also able to influence parts of the market.

Control over an Installed Base of Customers

This asset is to be considered when a company already owns a large part of the market and is able to influence its customers and fight off the rivals. Two specific cases deserve mentioning - Microsoft and Cisco. Both companies have established their leadership in the respective markets and can easily leverage control over their customers. In this way their rivals are forced to take the path towards a Revolution strategy, involving higher risks and costs for battling against the leaders. [15]

Intellectual Property Rights

The ownership of patents and copyrights is very important when trying to impose a new standard on the market. It provides a certain level of stability for the company and allows for blocking compatibility with rival technologies. [15] There are many big companies that rely mostly on their patent and copyright portfolios to secure their place on the market. Examples are Qualcomm, Intel, Sony, Cisco, Apple, etc.

Ability to Innovate

The ability to innovate is an important asset that focuses beyond the actual intellectual property rights. It can be viewed as the ability to create extensions for already established technologies. [15] According to [26], the measurement of innovation is a tricky business. However, one thing is certain - the goal of innovation is profit, measured by the Return on Innovation Investment (ROII).

First-Mover Advantages

This asset focuses on the importance of being first. The chances for market dominance of a company that is way ahead than its competition are significant. [15] This also requires significant resources for research and development purposes. An example for a first-mover success story is Coca-Cola. The first competitor of Coca-Cola was Pepsi-Cola, which emerged thirteen years after the establishment of Coca-Cola and by that

time Coca-Cola already controlled a large amount of the market. [27] So large that it continues to be the preferred beverage today.

Manufacturing Capabilities

The manufacturing capabilities asset focuses on saving production costs. If the new technology is being developed with low production costs, this certainly improves the company's chances for lasting in the market. Therefore, when it comes to a standards war, the company is able to afford fighting and surviving the war. HP has a long reputation of accepting open standards, because they are the key for efficient production. [15]

Strength in Complements

This asset is not focused on making a company the main product market leader, instead it focuses on using main products as vessels and transporting complementary products through them. [15] The principle here is about being the next best thing, that makes the best even better. Lets take Intel as an example. The company does not produce computers, but it produces the CPUs for most of the computer vendors across the world. This gives Intel the opportunity to create new standards for various computer components and keep its role as a component supplier for a stable customer base.

Reputation and Brand Name

The value of reputation and brand name is a significant criteria for continuous market leadership. [15] Large enterprise customers tend to prefer proven and credible companies. History has shown the importance of brand name and reputation numerous times. Examples are companies like Microsoft, Cisco, Sony, HP, IBM, etc.

3.2.3 Preemption

There are two primary methods for waging standards wars. The first one is called preemption. Preemption is all about getting an early lead in the market and using customers' feedback in your favor. [15] The simplest way of applying the preemption method is to be the first player on the market. But is it only speed that matters? A player who invades the market with a new technology will definitely receive attention from the consumer base, but that attention will only last if the quality is also there to support it. There are also other techniques that can be utilized to support preemption. Penetration pricing, a method for pricing a product below its actual cost, is a common technique for attracting more and larger customers. [15] It is highly effective, but it should only be considered when developing a proprietary solution. In this way the company invests in control over

the market and is able to regain the costs of penetration pricing once it takes over the standards battle. The use of penetration pricing with open standards is not going to justify the low costs for penetration pricing, after the product passes this phase. Another important factor for winning the war is the effective distribution of related products and services. [23] Effective distribution is considered distribution which leads to profit. This strategy is focused on maintaining the "Control over an installed base of customers" asset in order to generate as many revenue streams from the customers as possible.

3.2.4 Expectations Management

The second method for fighting the standards battles is expectations management. This is extremely important when trying to enforce a new technology on the market, since it is the consumers' expectations that are going to make them try the new technology. Expectations management is a two sided coin. As emerging companies will try to strengthen their product's expectations, market leaders will try their best to weaken the emerging rivals and keep them off the market. [15] A major tactic for managing customers' expectations is the so called vaporware. Vaporware represents a strategy for distraction of the consumer base from rival products. [28] It achieves this goal with the announcement of a new product or service, that is not intended to be created, but only to attract attention and lower competitors' sales. Another very important tactic for expectations management is the formation of coalitions. [15] This allows a company to spread the word about its product as much as possible and once enough people know about it, this can be used to support greater claims about the importance and quality of the product.

3.2.5 Once You've Won

According to [15], there are some key strategies for protecting the leadership, once a company wins the battle of standards. Since standards wars in the technology sector are a very sensitive subject in today's world, winning can be only temporary. The "Once You've Won" strategies are aimed to solve this exact problem and help a company to remain the market leader. Since this thesis is focused on analyzing a technology that is still in its early stages, none of these strategies are going to be used later in the analysis. However, we are going to present a short overview to the reader for complete understanding of the theory.

Staying on Your Guard

The first strategy to keep in mind is to always stay on your guard. Technologies and standards are all about improvement. If a company, positioned as a market leader stops investing in upgrading its technology, rival companies will notice that and start working on aggressive strategies for overtaking the market. [15]

Offer Customers a Migration Path

This strategy focuses on the anticipation of rival products and the development of migration plans for those products. The idea is that once another company develops something that the consumer base finds appealing, we should be able to provide an alternative to that solution. [15] A migration path, combined with the alternative will ensure a strategy for retaining our installed base of customers.

Commoditize Complementary Products

The commoditization of complementary products is an important step for every company. The strategy is all about maintaining a diverse set of companies for our complementary products. The integration of the core product with complementary products is considered valid only if it would add a significant value to the customers. [15] Otherwise, it is a better practice to keep those markets separate.

Competing Against Your Own Installed Base

This strategy is a very interesting one. What do we do, if we already control a large amount of the market and there are no other competitors? Who do we compete against? The answer is ourselves or our own installed base of customers. One of the ideas here is to bring more innovation in the market and try to complement the sales of our core product with another major product that depends on the core product and vice versa. [15] In this way, the sales of one of the products contributes to the sales of the other one. Other ideas that support this strategy include discount prices and renting your product, instead of directly selling it.

Protecting Your Position

Protecting your position is a strategy that is targeted towards defending our product from its competition. There are two major tactics that can be used for this strategy. The first tactic is aimed at controlling the complementary product companies, by offering them special terms and conditions if they only sell their product to our company. [15] This strategy, however, has the potential to cause legal risks and should be very

carefully considered. The other tactic is focused on avoiding the use of complementary technologies that can lead to copyright issues. [15]

Leveraging Your Installed Base

This strategy focuses on expanding our portfolio through the already established consumer base. [15] When a company becomes a leader in a specific market, this presents an opportunity for strengthening its position in other related markets as well. Buying smaller companies in order to acquire their market share and portfolio is a valid tactic for this strategy. Another one is geographic expansion.

Staying a Leader

In order to remain a leader, all of the aforementioned strategies should be combined and used wisely. However, there are some other tactics that are strictly focused on securing our position on the market. For example, to continue making proprietary extensions for our standards. [15] This can result in discovering new products, which can later turn out as a new profitable solution of our company.

3.2.6 Rear-Guard Actions

In the previous subsection we discussed strategies aimed at maintaining market dominance. But what happens if things turn out the other way around? What strategies should we consider if we have lost the battle? This is going to be the focus of this subsection and again, we are going to present a short overview of the strategies that are to be used when another player outperforms us. These strategies are not going to be included in the analysis for the same reason as with the "Once You've Won" strategies and are only presented for a holistic view on the framework.

Adapters and Interconnection

This strategy is all about keeping a fraction of the market through adaptation of our product towards the leading one. [15] Adaptation examples, in the software world, are the well-known converters and emulators. The idea here is to attract some of our competitor's customers with an alternative that is compatible with their product. This sort of interconnection will allow us to stay on the market and prepare a strategy for regaining the market back from our rival. However, creating an adapter in this case can be impossible if the leading company does not allow it. On top of that adapters are known for having performance issues, which makes them an unpopular choice.

Survival Pricing

What would a 10 year old kid answer, if we ask him how to sell more ice cream than his friends? Unfortunately we can not confirm this answer, but it is very plausible that his answer will be to cut the price. Survival pricing is a tactic for desperate moments, when we do not care so much about making a profit, but rather about staying alive. According to [15], however, survival pricing is a tactic that is unlikely to work in the software world. The main reason for this is that the cost for the software itself is considered as minor from the customers' perspective. Instead they are paying more attention to the costs for training, support and deployment.

Legal Approaches

The last strategy for rear-guard actions that we are going to discuss is about legal pressure. If everything else fails, the last option that we have is to look into our rival company's mistakes and try to exploit them in our favor through court. [15] This is the final move that we can use to remain a part of the market and should be carefully considered before we start with it.

3.3 Theory application

This framework will serve as a foundation for the comparison between SD-WAN and its rival technologies. SD-WAN will be compared to each of the three alternatives, discussed in chapter 4, separately in order to present the reader with the most comprehensive analysis. When comparing SD-WAN to each of the other standards, the discussed assets and strategies from this chapter will be examined. This will allow us to measure SD-WAN's likelihood for market dominance. A technology comparison will be added to the framework for expanding the reader's view with the technical benefits of each technology. This combination ensures that the analysis will cover both the technical and market perspectives on the subject.

3.4 Conclusion

In this chapter, we have explained the theoretical framework that will be used for the execution of our analysis on SD-WAN. A couple alternatives to the chosen theory were discussed. An overview of the standards wars theory was presented for the reader. The different types of standards wars were also explained. A layout of the key assets that a company should possess in order to dominate a specific market was included in this chapter. The two major strategies for fighting standards wars - Preemption and Expectations Management were reviewed. Strategies and tactics for

keeping the market leader position were included. The possibility for losing the battle was also taken into consideration. Different tactics for remaining part of the market after losing the standards war were discussed. The specific way of applying this theory in the thesis were examined. The chapter was intended to provide a clear understanding of the standards wars theory and prepare the reader for its purpose in chapter 5.

Chapter 4

State of the art

4.1 Introduction

In this chapter we are going to discuss more extensively the current WAN technologies that exist on the WAN market, their types and principles of operation. Internet VPNs will also be subjected to comprehensive examination. The core principles of Software-Defined Networking will also be discussed and explained. The first WAN solution that is going to be discussed is going to be MPLS VPN. The basic principles of BGP are going to be explained together with those of MPLS. The different types of this solution, Layer 2 and Layer 3 VPNs, will be examined. The second solution that is going to be considered is going to be IPsec. The general principles of IKE are also going to be explained. The third and final solution that is going to be examined is going to be DMVPN. The basic principles of GRE, mGRE and NHRP are going to be discussed as well. The chapter will finish with a comprehensive overview of SDN. Its fundamental principles and most well-known standard - OpenFlow will be included in the overview.

4.2 Wide-Area Networks

Most enterprises today use LANs for each of their offices or buildings. These LANs usually connect end devices like servers, computers, smart phones, tablets, printers and also the enterprise's network equipment such as firewalls, routers, switches and access points. LANs are usually limited by the office or building in which all of these devices are located. The dominant technology that is used inside the LAN nowadays is ethernet. [29] But what happens when an enterprise grows and has multiple branch offices across the country, or even the globe? WANs represent the technologies that are used to connect multiple branch offices and their data centers together and allow for communication between large geographical distances. [30] There can be different types of WAN services - metropolitan, regional, national or international. WAN technologies use the services of Tier 1 or Tier 2 ISPs and telephone, cable or satellite companies in order to create the communication network for the customer. [29] Also WAN technologies operate on the first three layers of the OSI

model, the physical, data-link and network layers. [31] A clear view of the separation between LAN and WAN technologies can be seen in figure 4.1.

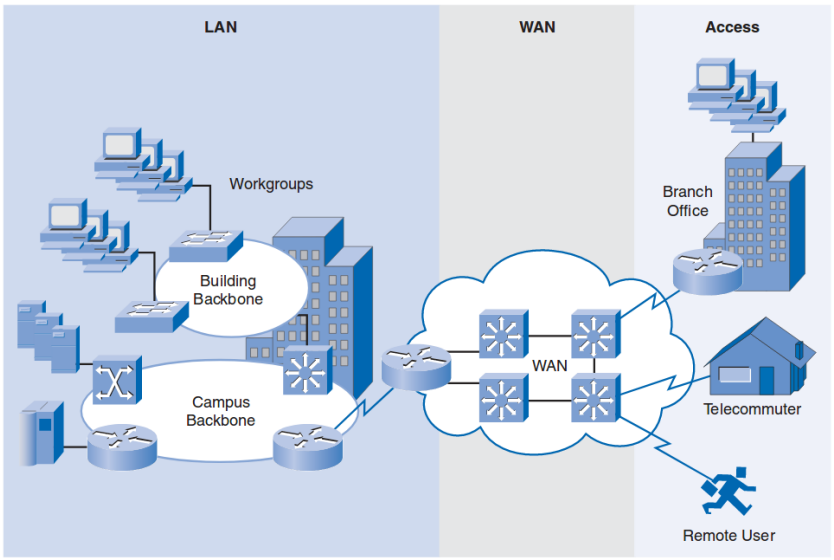

Figure 4.1: *Distinction between LAN and WAN [29]*

4.2.1 Types

There are plenty of technologies that were designed for WAN communication such as SDH, DWDM, VSAT, ISDN, Frame Relay, ATM, Metro Ethernet, MPLS, DSL. These technologies can be grouped together in two major categories, as shown in figure 4.2.

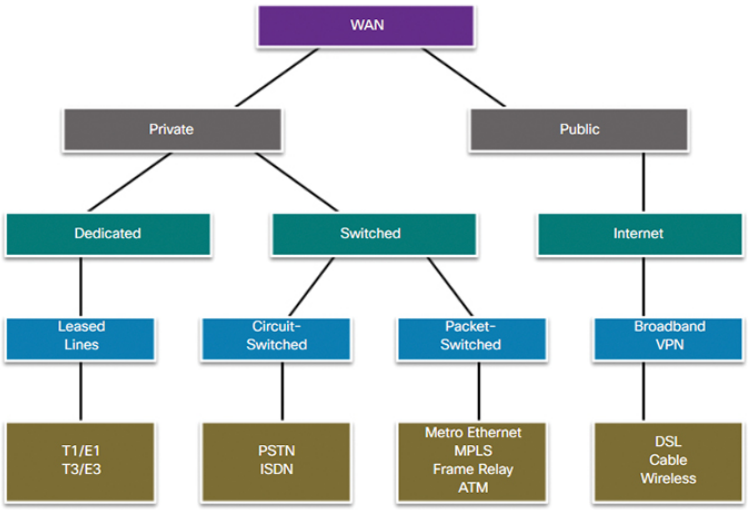

Figure 4.2: *WAN technology tree [32]*

Private WAN technologies can be further divided into dedicated and switched. An example for dedicated private WAN can be SONET/SDH or DWDM transmission. As for switched private WAN, the circuit-switched

technologies like PSTN and ISDN are considered obsolete nowadays and we will only focus on the packet-switched technologies. There is one particular technology that we will discuss more extensively later in this thesis and that is MPLS. MPLS is the most widely used private WAN technology in the world. [2] At least for now.

Public WAN technologies, on the other hand, rely on the internet. The internet provides a global network for enterprises, where they can connect all of their offices together and share information among them. There is one catch, however. Since the internet is a public network, everyone connected to it can see the information that travels through. That is certainly something that enterprises do not want. And the solution for this problem is VPN technologies.

Therefore, the choice between private and public WAN technologies can not be defined as straightforward. Where high level of security is needed, the advantage goes to the private WAN. But where low implementation costs and flexibility are more desired, public WAN should be considered. It all depends on the specific requirements of the enterprise. The same applies to the choice between dedicated or switched WAN. If there is a need for high bandwidth sensitive traffic, such as voice or video, between a bank's HQ office and its data center, the cost of leased lines can be justified. If, however, we need to connect multiple branch offices together, the more reasonable choice would be the use of packet-switched WAN. [32]

Packet switching

Since the understanding of packet switching is the foundation of the modern VPN solutions, its principle of operation will be briefly examined. The packet switching mechanism is shown in figure 4.3. This mechanism transmits data in the form of packets, which are routed or switched, depending on the network that they traverse. [29] The transport network is shared among all users, leading to low costs for the customers compared to dedicated WAN solutions. If there is a need for private communication over the packet switched network, virtual channels are formed between the points of interest and their traffic becomes hidden from the rest of the public traffic. [33] There are two primary methods for transmitting data in a packet-switched environment - connection-oriented and connectionless. [29] Example for a connection-oriented packet-switched technology can be Frame Relay or MPLS, where each packet's route is predetermined. With connectionless packet switching, each switch or router that the packet travels through is used to decide on which other interface to forward the received information. The path that packets take can

be different every time for the same source and destination adddresses. Example for connectionless packet switching is the internet. [33]

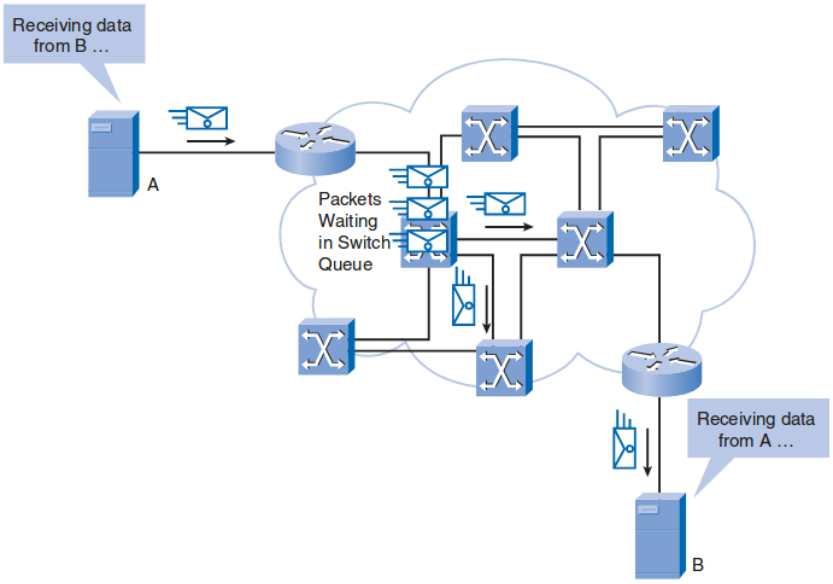

Figure 4.3: *Packet switching mechanism [29]*

4.2.2 Multiprotocol Label Switching VPN

This VPN uses the combination of two technologies. MPLS is the part which is responsible for forwarding the VPN packets through the IP backbone and BGP deals with the route distribution. [34] Other routing protocols can also be used for the realization of the MPLS VPN, but the most widely used combination is BGP and MPLS. As this technology represents the biggest competitor to SD-WAN, it will be discussed more extensively in this thesis.

Multiprotocol Label Switching

In order to fully understand the MPLS principles, we need to start with its terminology. From an ISP's perspective, the client's device that is used to connect to the ISP is referred to as customer edge (CE). On the other side, the ISP's device that is used as a connection to the client is referred to as provider edge (PE). The other routers inside the ISP's network, that are responsible only for the core operations and are not connected to external devices are simply called provider (P) routers. [35] From MPLS perspective, all routers that are running MPLS are referred to as label switched routers (LSRs). This terminology comes from the fact the MPLS architecture uses labels for forwarding packets through the network instead of IP addresses, which is the traditional forwarding method. [36] It can be stated that the P routers are actually also LSR routers. Further, the PE routers, from MPLS perspective, can also be referred to as label edge

routers (LERs). The path that MPLS packets take, from their entry point in the ISP's network to the egress LER is referred to as label switched path (LSP). It is important to note that LSPs are unidirectional. [37] The MPLS architecture can be seen in figure 4.4.

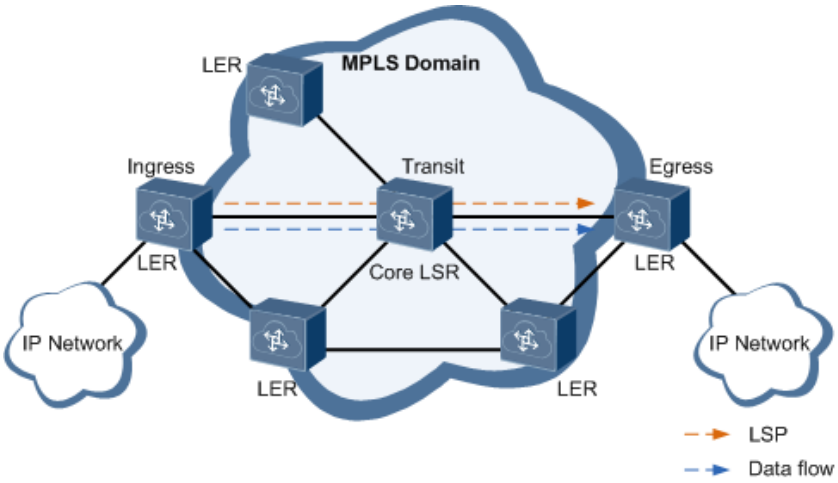

Figure 4.4: *MPLS Architecture [38]*

MPLS operates with a connection oriented mechanism, creating the communication channel before the actual communication begins. [39] The main principle of MPLS is the implementation of a differentiated services mechanism, which deals with each packet based on its traffic flow - the source and destination IP addresses. [40] When external packets enter the MPLS network, they are assigned to a Forward Equivalence Class (FEC) based on their destination IP address. [41] Then all of the packets that belong to the same FEC are assigned with the same label for further processing. The label is a local identifier that shows to which FEC does the packet belong. The FEC can be based on destination IP addresses, traffic class based on IP DiffServ Code Point (DSCP) value, multicast groups, layer 2 MPLS VPN Virtual Circuit (VC) values or IP addresses which are part of special sets of BGP prefixes used for routing purposes. [2] Packets are being labeled once they enter the ingress LER and their labels are being removed when they exit the MPLS network. Further, packets are transmitted through the MPLS network solely based on their labels, which are used to determine the next hop. (See figure 4.5)

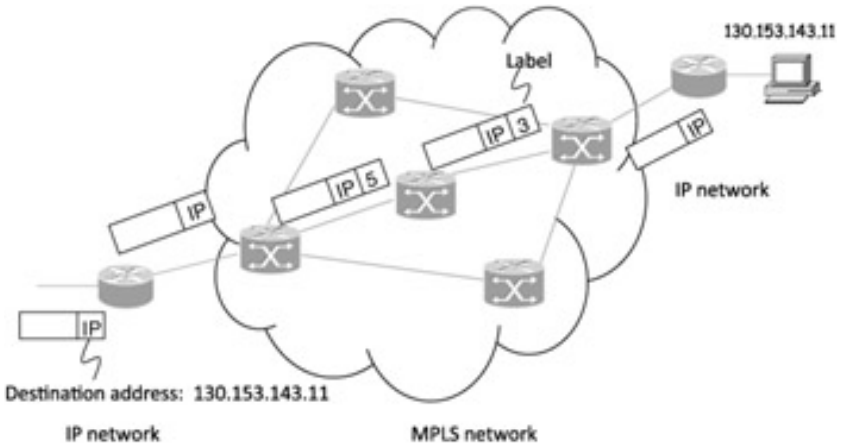

Figure 4.5: *MPLS label mechanism [39]*

The actual MPLS label can be seen in figure 4.6, where the structure of the MPLS header is shown. It consists of 32 bits, the first 20 of which represent the actual value of the label. This value is within the range $0 - (2^{20} - 1)$. The first 16 values from this range are kept for special usage and normally MPLS labels start from the value of 16. The next part of the header is the experimental field, represented in 3 bits and used for applying QoS. [2] BoS is the next field, short for Bottom of Stack, or usually referred to as the S bit. It consists of only one bit, which is used for determining the last label in a label stack. MPLS allows for flow aggregation and multiple labels can be "stacked" on the same packet. [40] This is known as label stacking and utilizes the Last In First Out (LIFO) mechanism. The BoS bit is 0 for all the labels in the stack, except for the bottom label, for which it is set to 1. The last 8 bits are used for the Time To Live (TTL) value. [2]

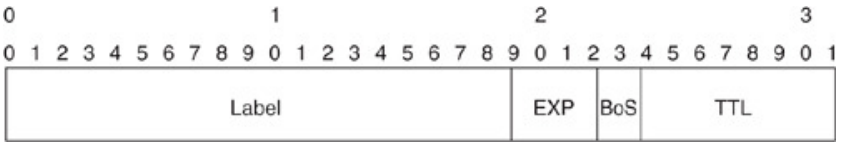

Figure 4.6: *The MPLS header [2]*

The label switching is done via the MPLS forwarding table, which contains all the necessary information for distributing labeled packets. [37] This sort of traffic differentiation allows for a high level of Quality of Service (QoS), applied through policies on the different traffic classes. [40] For the distribution of labeled packets, however, a common mechanism is needed. There are two mechanisms that can be used for distributing MPLS packets. [2] First, the labels can be placed on top of an existing IP routing protocol and second - a separate protocol can be used only for label distribution. The most common option is the use of a separate protocol and this protocol is Label Distribution Protocol (LDP). [2] There is one other protocol that is used for label distribution - Resource Reservation

Protocol (RSVP), which is used mainly for MPLS traffic engineering. One of the main advantages of MPLS is that the MPLS forwarding table consumes less processing power than the ordinary routing table and allows for faster packet processing. [37] There are currently 718,223 IP prefixes that are routed across the internet, according to [42]. Without MPLS, the calculations that each router needs to perform in order to calculate the best route to a specific IP destination address would be significant. MPLS has also other very important benefits, such as its support of multi-layer labels and its connection-oriented forwarding plane. [38] MPLS also provides intelligent traffic engineering, which is an extremely important feature for ISPs in order to allow them to manipulate customer traffic in the most suitable way. [39] These features make MPLS the dominant technology for large-scale VPN services and QoS prioritization today.

The most widely used application of MPLS is the MPLS VPN, shown in figure 4.7. This service is based on the existing MPLS network of an ISP and uses the MPLS technology to create virtual channels within that network and use them to privately transmit customer traffic between multiple locations. However, MPLS is not capable of realizing this service on its own. A routing protocol is also required and the protocol that is used for this is BGP.

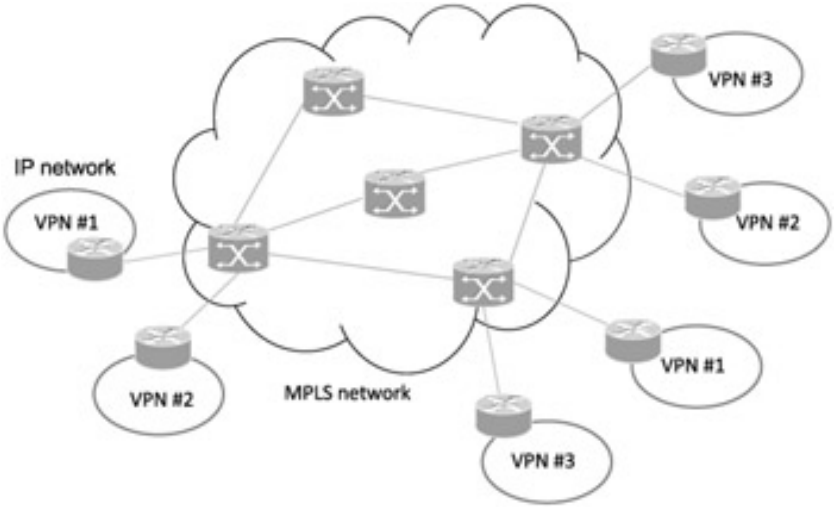

Figure 4.7: *MPLS VPN mechanics [39]*

Border Gateway Protocol

We are going to briefly discuss what BGP is and emphasise on the attributes and extensions that are necessary for the MPLS VPN in this part of the thesis. BGP, or more specifically BGP version 4 (BGP4) is the routing protocol that is responsible for the internet. [43] It is the only Exterior Gateway Protocol (EGP) that we use today and it is very different from most Interior Gateway Protocols (IGPs) like OSPF, EIGRP and IS-IS. [44]

BGP is neither a distance vector or a link state routing protocol. Instead it is referred to as path vector routing protocol and it was designed to have a lot of attributes or vectors that are able to influence traffic. [45] However, not every enterprise is connected to the internet via BGP. BGP is used when an enterprise has a more complex network with various IP routes and wants to have a main/backup internet connection through multiple ISPs. [44] There are two primary advantages of BGP that should be mentioned. The first one is its scalability. There is no other routing protocol that can handle the whole internet. [44] The second advantage is its customization. [45] When the large amount of BGP attributes gets combined with routing policies, the possibilities for traffic customization become extremely high.

The evolution of the internet is presented on figure 4.8 with the exponential growth of the world's BGP table. This can help us picture the enormous range that BGP has scaled to from 1994 to present days.

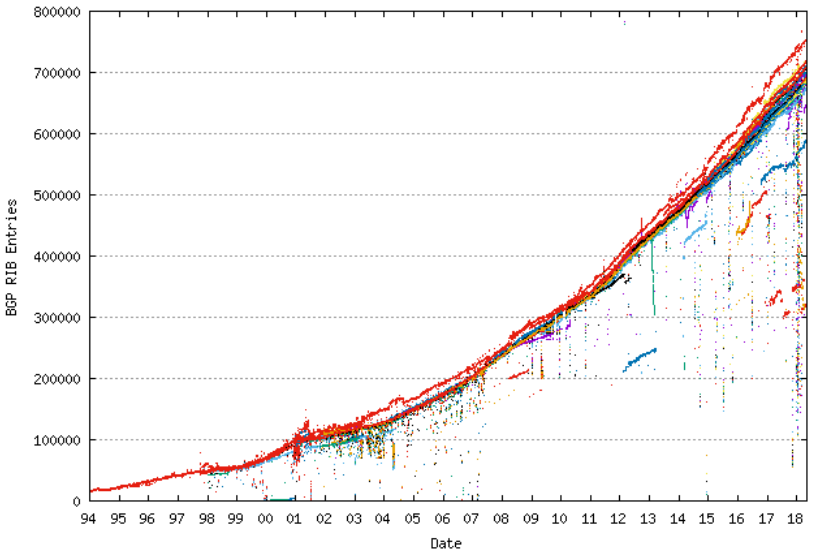

Figure 4.8: *Growth of the BGP Table - 1994 to Present [46]*

Autonomous system

The internet today is a complex network of networks that are connected through BGP. BGP looks at those networks with the concept of Autonomous Systems (ASs). Each enterprise that uses BGP to connect to the internet has its own AS Number (ASN). ASs are managed by the Regional Internet Registries (RIRs) and there are specific policies for their assignment. In Europe they are managed by Réseaux IP Européens (RIPE) and by their definition, an AS is "a group of IP networks run by one or more network operators with a single clearly defined routing policy". [47]

Attributes

As we have said earlier, BGP can use a lot of attributes to determine the best path to a destination. But for the purpose of this thesis we will cover only the most common ones.

ORIGIN
The ORIGIN attribute is mandatory and it identifies the source of a given prefix. There are three possible values for this attribute: 0 for IGP, 1 for EGP (BGP) and 3 for INCOMPLETE. The lowest value is preferred in path selection. INCOMPLETE is used when routes are redistributed into the BGP routing table from another protocol. This attribute can be manipulated through the use of route maps. [43]

AS_PATH
This is another mandatory attribute that shows in reverse order the ASs through which the selected prefix has passed, before entering the current AS. [48] AS_PATH is designed for loop prevention when doing inter-AS routing. The shortest list for AS_PATH is preferred in path selection. [43] In order to influence path selection the current ASN can be prepended into the AS_PATH list one or multiple times. [48]

NEXT_HOP
This is a mandatory attribute that is responsible for determining the next hop IP address and exit interface that should be used to reach a given prefix. Every prefix needs to have a reachable next hop in order to be considered for the best path selection. [43] Usually the NEXT_HOP is calculated so that the shortest path to the destination is chosen. [48] This attribute can be manually set through the use of route maps or additional configuration. [43]

MULTI_EXIT_DISC
MULTI_EXIT_DISC is an optional attribute that is intended for inter-AS links and its function is to segregate multiple entry or exit points to the same neighboring AS. This attribute uses a value named metric and the exit point with the lowest metric is preferred for path selection. [48]

LOCAL_PREF
This attribute is used only in iBGP communication in order to calculate the level of preference for every external route. This level of preference is later used to determine the exit point from the current AS. The higher LOCAL_PREF is preferred in the selection process and its distribution should be limited to only internal peers. [43]

COMMUNITY
The COMMUNITY is an optional value that is used to identify a group of IP prefixes with a common function. It is 32 bits long and it is possible for multiple communities to be placed on the same prefix. [43] There are two types of communities, well-known and private. Examples for well-known communities are NO_EXPORT, NO_ADVERTISE and NO_EXPORT_SUBCONFED. This attribute can be used to control the accepted, distributed and preferred routing information from other BGP peers. [49] Private communities are specifically set for their individual purpose. After prefixes are marked with a private community, they can be subjected to custom policies and the result is a very powerful tool for traffic manipulation.

Multiprotocol BGP

BGP on its own is incapable of transmitting MPLS information and therefore needs to be extended to provide multiprotocol support for the creation of MPLS VPN. Multiprotocol BGP (MP-BGP), standardized in RFC4760, along with the extended BGP attribute - Route Target - RFC4364, provide the necessary tools for realizing this VPN solution. [50] The two new attributes that MP-BGP brings are Multiprotocol Reachable Network Layer Reachability Information (NLRI) and Multiprotocol Unreachable NLRI. They both consist of the Address Family Identifier (AFI) and the Subsequent Address Family Identifier (SAFI) and are used to determine what types of routes is BGP distributing. [2] The AFI describes the specific network communication protocol - IPv4, IPv6, VPN-IPv4 or VPN-IPv6 and the SAFI shows whether the traffic is unicast, multicast or VRF. [51] The Virtual Routing and Forwarding (VRF) concept provides separate virtual routing tables for each VPN connection. The special VPN-IPv4 and VPN-IPv6 AFIs are formed with the addition of a Route Distinguisher (RD) to the selected IP prefix. [50] The RD is 8 bytes long and it is used to separate different VPN routes that use the same IP prefix. [43] In this way, unique VPN-IP prefixes are formed. When importing IP routes into the BGP address families, the extended BGP attribute Route Target (RT) is added to the prefix. [50] It is responsible for mapping the IP prefix to the specific VRF/VPN that it belongs to, and its operation is similar to the BGP COMMUNITY attribute. A given IP route can have multiple RTs but it can have only one RD. Any route that is mapped with a specific RT should be distributed to all of the other routes that are mapped with the same RT, creating the private VRF table. [52]

Layer 2 and Layer 3 VPN

The MPLS technology supports two types of VPN services, layer 2 and layer 3 VPN. [37] The layer 2 VPN, also familiar as Virtual Private LAN

Service (VPLS) is a simple, yet powerful layer 2 private carrier service. It creates a virtual channel between a customer's sites, which remains completely private from the rest of the traffic in the ISP's network. It is important to note that with layer 2 VPN, the routing occurs on the customer side, on the CE device and the ISP is "blindly" accepting the layer 2 traffic and transporting it through layer 2 interfaces in its MPLS network. [53]

With layer 3 VPN, the ISP is responsible for all the routing between the different customer sites. [36] MPLS layer 3 VPNs are based on the peer model and therefore are more scalable than other overlay based models such as IPsec. The layer 3 VPN is created with the help of VRF tables. [54] They are isolated from the other traffic in the ISP's network and the customer's traffic is completely private. When there are multiple customers connected to the same PE router, as shown in figure 4.9, each customer belongs to his own VPN and therefore has its own VRF table. A site can belong to more than one VPN, but to only one VRF. The specific VRF table will contain IP routes only to the other sites that belong to the same VPN, ensuring the privacy of traffic. [36]

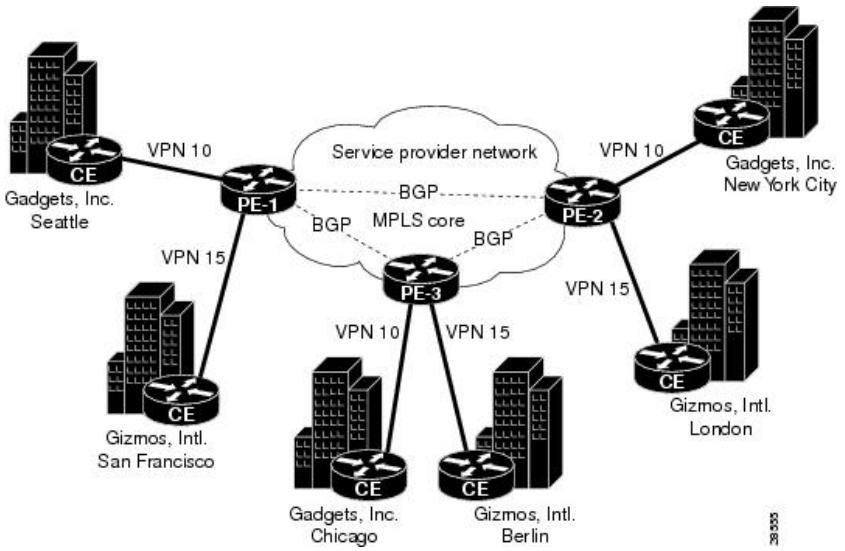

Figure 4.9: *MPLS VPN Architecture [35]*

BGP is used for distributing the VPN information through the ISP's network through the use of extended communities. When customer traffic enters the ISP's BGP/MPLS network, it is marked with a RD (10, 15 - figure 4.9). [55] All of a customer's sites must have the same RD. Then RT is used to import and export a client's IP prefixes into one or more VRF tables. Since each VPN is completely isolated, this presents the opportunity for duplicate IP address assignment. [36] VPN clients can use the same IP addresses, public or private, and be routed across the same BGP/MPLS network with the help of RDs. Each IP prefix that is used by

the customer is a member of the BGP IPv4 address family. To make the IP addresses unique, the RD is added to the IP prefix and that combination is inserted into the BGP VPN-IPv4 address family. [54] The security in MPLS VPN is designed in a decentralized approach with the separation of the control and data planes. [36] The control plane protects the network from unauthorized injection of IP prefixes in the PE devices through MD5 BGP peer authentication. The data plane is responsible for verifying packets that enter or exit the BGP/MPLS network for their authenticity with the implementation of traffic policies.

4.3 Virtual Private Networks

VPNs are virtual secure connections between two or more sites, that use the internet as a transport network. [56] They are considered secure because the information that is exchanged between the sites is protected with encryption. The virtual link that makes up the VPN from one point to the next is referred to as VPN tunnel. A VPN connection can be established between different offices of a company, also known as site-to-site VPN or between a device and an office, referred to as remote access VPN. The device that can be used to access a company's network through a VPN connection can be any type of smart device such as a laptop, tablet or phone. [57]

Site-to-site VPN

The purpose of site-to-site VPNs is to connect the networks of multiple sites together through the internet. Site-to-site VPNs require dedicated equipment such as firewalls, routers, layer 3 switches or servers. [57] The only requirement for each site is to have a connection to the internet. [56] In this way expenses are only limited to the actual devices that are used to create the VPN and the internet subscription fee. The site-to-site VPN connection is static and the end devices that reside inside the sites are unaware of its existence. Site-to-site VPNs can be further divided into intranet and extranet VPNs. When the site-to-site VPN connects offices of the same company it is considered as intranet and when it connects two different companies it is referred to as extranet. [56] Examples of solutions that can provide site-to-site VPN services are MPLS, DMVPN and IPsec. The architecture of a site-to-site VPN is shown in figure 4.10.

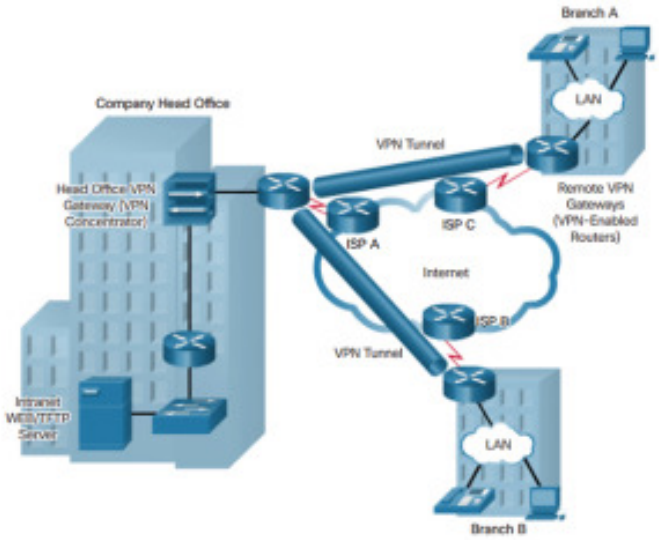

Figure 4.10: *Site-to-site VPN [32]*

Remote access VPN

The purpose of remote access VPNs is to allow employees, who are out of the office to remotely access the company's network infrastructure. Unlike site-to-site VPNs, where the VPN connection is permanent, remote access VPNs establish a connection only when it is necessary for the remote user. [56] The remote access VPN connection is dynamic and certain parameters can be changed, such as the IP address of the user that is trying to initialize the service. In order to establish a remote access VPN, the remote user needs to have a VPN client software and credentials for authentication with the VPN server. The primary remote access VPN solutions today are IPsec and SSL. [58] The architecture of a remote access VPN is illustrated in figure 4.11.

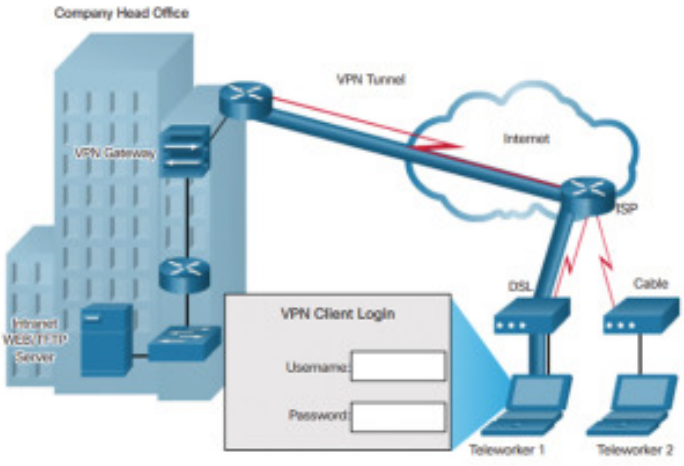

Figure 4.11: *Remote access VPN [32]*

4.3.1 Internet Protocol Security VPN

Internet Protocol Security (IPsec) is a suite of protocols and technologies that are used to provide the security for data travelling across the internet. The specifications and methods for realizing IPsec are defined in RFC4301 and RFC6071. There are two protocols that are used for the provision of security over IP networks - Encapsulating Security Payload (ESP) and Authentication Header (AH). The current version of IPsec is IPsec-v3. [5] The IPsec architecture is shown in figure 4.12. Its mechanism creates a private tunnel over the internet that is designed to securely transport customer data between the local and remote endpoints. The private tunnel actually consists of two separate tunnels, one encompassed into the other, through the use of the Internet Key Exchange (IKE) protocol which will be discussed later in this subsection. IPsec can also be used on top of MPLS VPN in order to provide the secure transmission of IP data. [59]

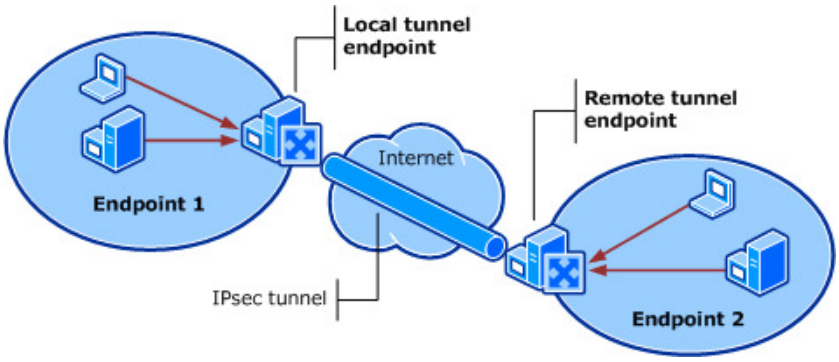

Figure 4.12: *IPsec architecture [60]*

Security Associations

Security associations (SAs) represent the toolkit that provides the necessary details for managing and monitoring the IPsec sessions. [61] Examples of SA parameters can be encryption, authentication and key management.

Internet Key Exchange

IKE is the protocol that negotiates the IPsec SAs. [4] Its process is divided in two phases. The current version of IKE is IKE version 2, as specified in RFC7296. The IKE protocol is able to provide full confidentiality and integrity capabilities. For confidentiality purposes, cryptographic algorithms like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) can be utilized. For integrity purposes, the combination of Hash-based Message Authentication Code (HMAC) and Secure Hash Algorithm (SHA) algorithms is recommended. [62]

PHASE 1
In phase 1, IKE creates a secure channel between the peers that is referred to as the IKE SA. [63] IKE authenticates the peer and the packets that the peer is sending during phase 1. [64] This is the first step of the IPsec communication and it can be performed in two modes - main and aggressive. The main parameters that the peers must agree on are authentication, encryption, diffie-hellman group and hash methods. [65]

PHASE 2
In phase 2, IKE negotiates the IPsec SAs, which are used to create the IPsec tunnel over the existing IKE phase 1 secure communication channel. [64] There is only one mode for the creation of IKE phase 2 - quick mode. The negotiated parameters for phase 2 include the selected security protocol - ESP or AH and the specific authentication and encryption parameters. [66]

The IPsec VPN can be realized in different peer types, shown in figure 4.13. The first type is a typical site-to-site VPN and because the devices that are used to create the VPN tunnel are referred to as gateways, it is considered as IPsec gateway-to-gateway VPN. [63] The second example shows a remote access IPsec VPN, realized from an end device to a security gateway. This type of IPsec VPN is referred to as host-to-gateway. The last VPN peer type is host-to-host and as shown in figure 4.13 it represents an end-to-end VPN solution from one private host to another.

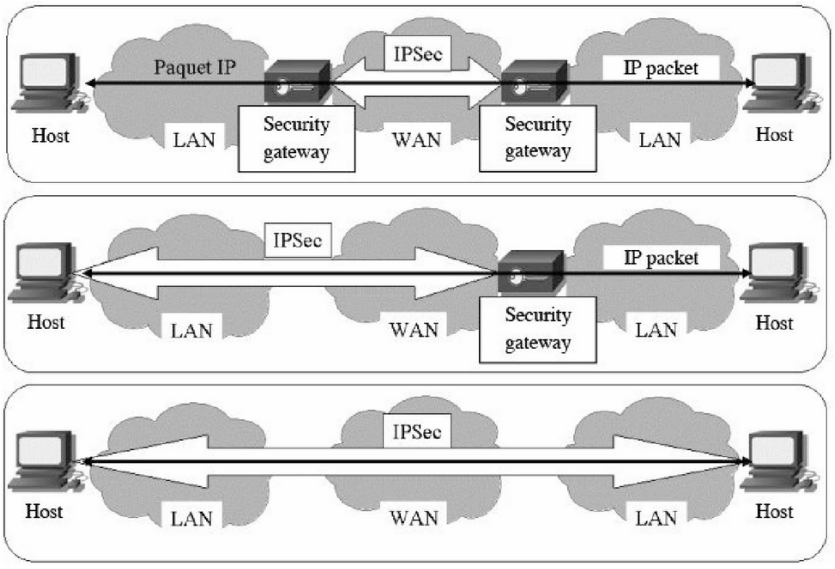

Figure 4.13: *IPsec VPN types [65]*

Encapsulating Security Payload

ESP is the security protocol that guards IP data from all the villains. It is responsible for all aspects of data security - authentication, integrity and

confidentiality. [65] The level of these security aspects depends on the specific IPsec mode that is chosen. There are two operational modes of the IPsec VPN solution - Transport and Tunnel. These two modes affect the operation of the IPsec security protocols. The difference in ESP tunnel and transport mode is shown in figure 4.14. In transport mode, the ESP header is inserted between the IP header and the data. This maintains the original IP header and allows for data to be encrypted, authenticated and forwarded with its original parameters. [63] In tunnel mode the whole IP packet is encrypted and the ESP header is placed along with a new IP header on top of the original datagram. [65] Tunnel mode is the most common implementation of IPsec VPN, especially in gateway-to-gateway communication. The tunneling mechanism allows for the transmission of protocols that a certain device can not understand through their encapsulation in another understandable protocol. [63] ESP does not provide any algorithms for authentication, integrity or confidentiality on its own. It uses the negotiated algorithms from IKE phase 2. The general principle is that ESP should be used when both authentication and confidentiality are required.

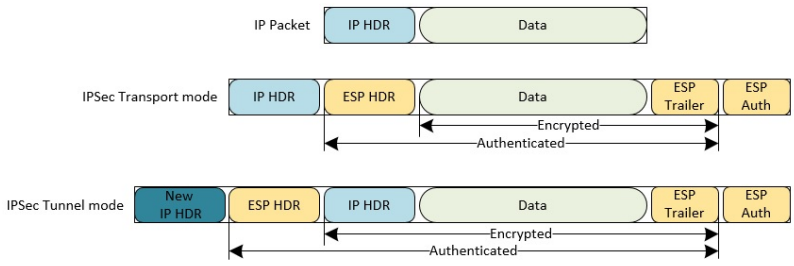

Figure 4.14: *ESP transport and tunnel mode comparison*

ESP packets are identified with IP protocol number - 50, as specified by IANA. The structure of an ESP packet is shown in figure 4.15. It consists of two parts - a header and a trailer that are attached to the payload data. The header consists of two fields - Security Parameters Index (SPI) and Sequence Number (SN). Both fields are 32 bits long. The SPI value is used to identify to which IPsec SA does a given packet belong and distinguish packets between multiple SAs. [63] The SN represents a counter value that gets incremented with each new packet and is used to mark the sequence of packets from the selected SA. [67] The ESP trailer consists of four fields - Padding, Pad Length, Next Header and Integrity Check Value (ICV). The Padding field has a special purpose. It is used to fill unused plain text in the trailer that is generated by the use of encryption algorithms, which require this plain text to be a multiple of a specific number of bytes. [67] It is also used to align the packet block with a multiple of 4 bytes. [65] The Pad Length field simply measures the used Pad bytes in the previous Padding field with values from 0 to 255. [67] The Next Header field is 1 byte long and is used to distinguish between the type of

data that is carried in the Payload Data field. Its value is used to identify whether this is an IPv4, IPv6 or another type of packet. [63] The last field - ICV is an optional field that is used only when the integrity function of ESP is required. It consists of a value that is computed over the rest of the fields and is used to verify the integrity of the packet. [67]

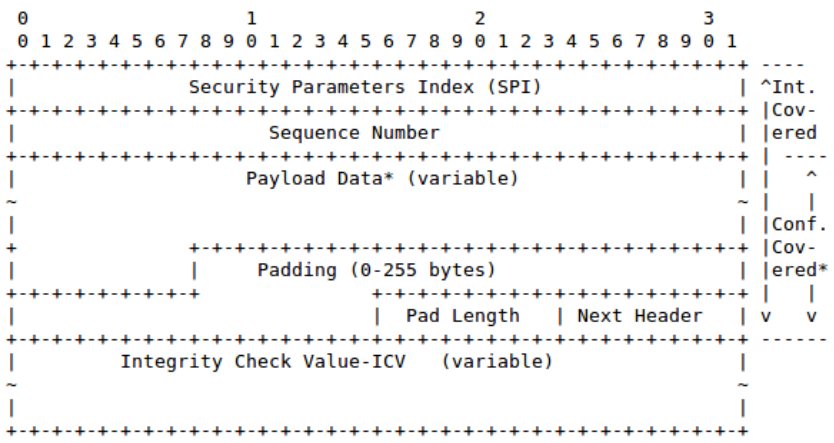

Figure 4.15: *ESP packet format [67]*

Authentication Header

AH is designed to provide authentication and integrity of IP packets, however AH does not provide data confidentiality. [68] AH can be combined with ESP in order to provide the confidentiality of data if needed. As with ESP, AH also depends on the preferred IPsec mode as shown in figure 4.16. An important benefit of AH, compared to ESP is that it provides authentication to the whole IP packet, whereas ESP authentication does not cover the first field of the datagram (IP HDR - Transport mode, New IP HDR - Tunnel mode: figure 4.16).

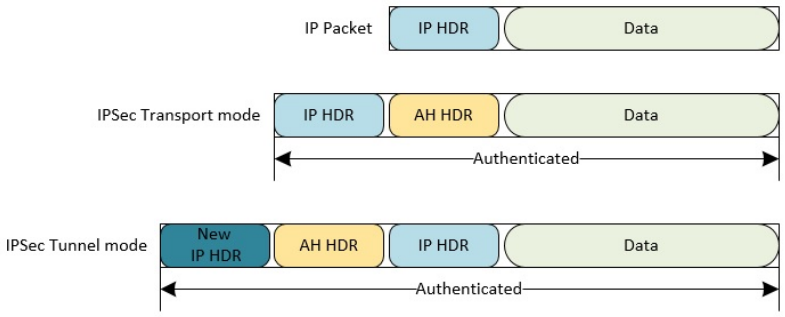

Figure 4.16: *AH transport and tunnel mode comparison*

AH packets are respectively identified with IP protocol number - 51. The format of an AH packet is shown in figure 4.17. Unlike ESP, AH consists of only a header part. The AH header has the following fields - Next Header, Payload Len, RESERVED, SPI, SN and ICV. The Next Header, SPI,

SN and ICV fields contain the same information as discussed with ESP. The Payload Len field is a 1 byte value that shows the length of the authentication block in 32-bit words. [63] The RESERVED field is always set to zero and it is left for experimental purposes. [68]

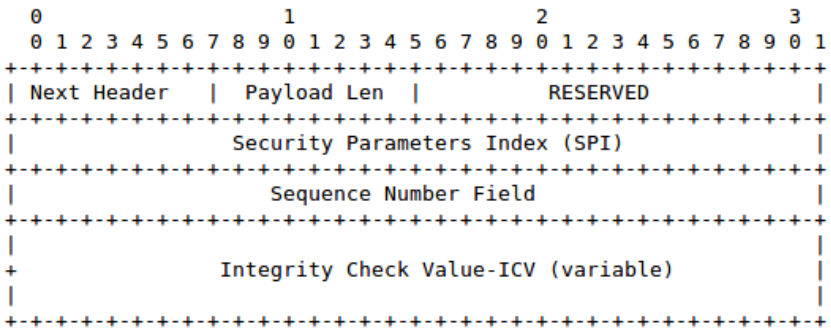

Figure 4.17: *AH packet format [68]*

4.3.2 Dynamic Multipoint VPN

Dynamic Multipoint VPN (DMVPN) is a Cisco proprietary VPN solution that is designed for flexible large-scale deployments with minimum complexity and low implementation cost, compared to MPLS VPN. [69] The architecture of a DMVPN is shown in figure 4.18. DMVPN operates with the concept of hub and spokes. There is one main router in the architecture, referred to as the hub and multiple branch office routers - spokes. The spoke routers have a permanent connection only to the central hub router and initialize on-demand connections to the other spoke routers when necessary. The DMVPN solution relies on three major technologies for its realization - Generic Routing Encapsulation (GRE), IPsec and Next-Hop Resolution Protocol (NHRP). [70] DMVPN can provide optional encryption of the VPN data with the help of IPsec.

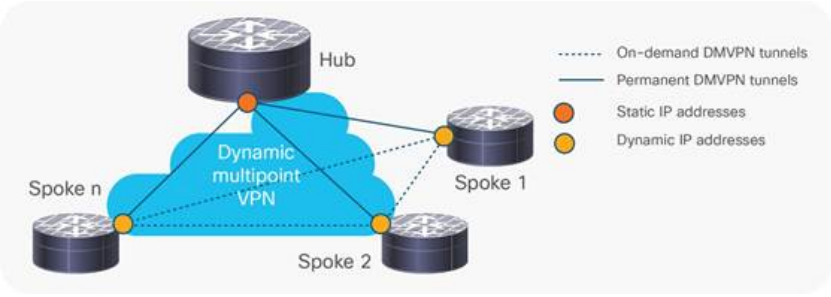

Figure 4.18: *DMVPN architecture [6]*

Generic Routing Encapsulation

GRE is defined in RFC2784 and is used for encapsulating one protocol in another by adding an additional GRE header to the IP datagram. [71] The structure of a GRE encapsulated packet is shown in figure 4.19. GRE is

simply an encapsulating protocol that is used to carry other protocols. It is also used extensively with IPsec to ensure the transmission of routing protocols through the IPsec VPN, which normally are not supported by IPsec, because it lacks the support for multicast and broadcast traffic. [63] GRE can also carry non IP protocols over IP networks and provides the ability for private IP addressing on its tunnel interfaces. [72]

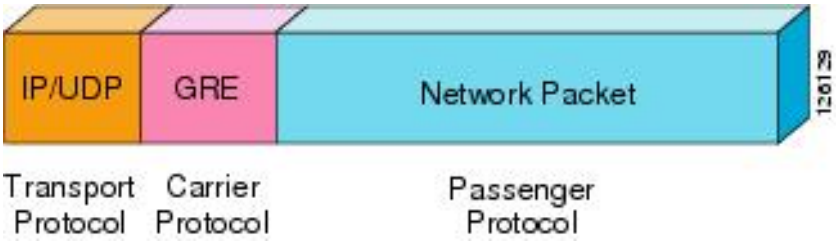

Figure 4.19: *GRE encapsulation [72]*

The GRE header is shown in figure 4.20. It consists of six header fields - Checksum Present (C), Reserved0, Ver, Protocol Type, Checksum and Reserved1. The C field is used to signal if the Checksum and Reserved1 fields are valid and present in the current GRE header. The Reserved0 field bits should always be set to zeros and their purpose is reserved for future use. The version number (Ver) field should also be set to zero and ignored on the receiver side. The Protocol Type field contains the type of the carried protocol in the payload, as specified by IANA. The optional Checksum field is used to store the calculated checksum value of the packet. Reserved1 is also a field that is meant for future purposes, but it is only present when the Checksum field is also present. It should be set to zero. [71]

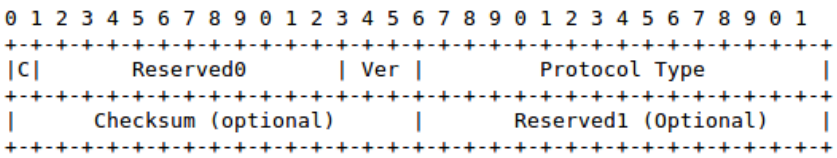

Figure 4.20: *GRE header [71]*

GRE is designed for point-to-point communication and requires a separate tunnel interface per VPN instance. [73] In the case of DMVPN, where scalability is extremely important such a behavior is insufficient. To cope with this problem, another version of GRE was designed - Multipoint GRE (mGRE). mGRE allows the hub to use one tunnel interface to connect to all of the spokes. [73] Therefore, all of the spokes appear reachable through the same tunnel interface in the routing table. There are two options for the use of mGRE in a DMVPN solution - hub-and-spoke mGRE and spoke-to-spoke mGRE. [6] The first option uses mGRE only at the hub router and normal GRE tunnel interfaces are used at the spokes. This requires all traffic to pass through the hub device and prevents direct spoke-to-spoke communication. The other option allows for traffic to be forwarded

directly from one spoke to another, eliminating the extra hop. mGRE is used at all the routers, creating a full mesh topology through dynamic tunnels. [74] Multihub design is possible if there is a need for redundancy.

This multi-tunnel approach requires a distinct method for QoS. As the communication to the different branch offices is carried through different mGRE tunnel interfaces, it requires a separate QoS policy for each interface. Cisco's answer to this problem is named per-tunnel QoS, which is designed for enforcing individual QoS policies to each tunnel instance. [75]

But what happens if the spokes have dynamic IP addresses that they receive through Dynamic Host Configuration Protocol (DHCP) from their ISP? How does the router learn the new public IP addresses in this scenario? The answer lies in the use of NHRP.

Next-Hop Resolution Protocol

NHRP is a client/server protocol, defined in RFC2332 and its purpose is similar to the Address Resolution Protocol (ARP). [76] When NHRP is configured between the hub and spokes, each time the spoke routers boot and receive a new public IP address, they map that address to their mGRE tunnel interface IP address and send the new information to the hub. [74] In this way a full mesh connectivity between the hub and spokes is formed. The hub maintains a NHRP database, where it stores the mGRE tunnel IP addresses of the spokes and their corresponding public addresses. [73] When a spoke needs to initiate a connection to another spoke, it queries the database from the hub and forms a direct tunnel with the other spoke. An example of this operation of NHRP can be seen in figure 4.21.

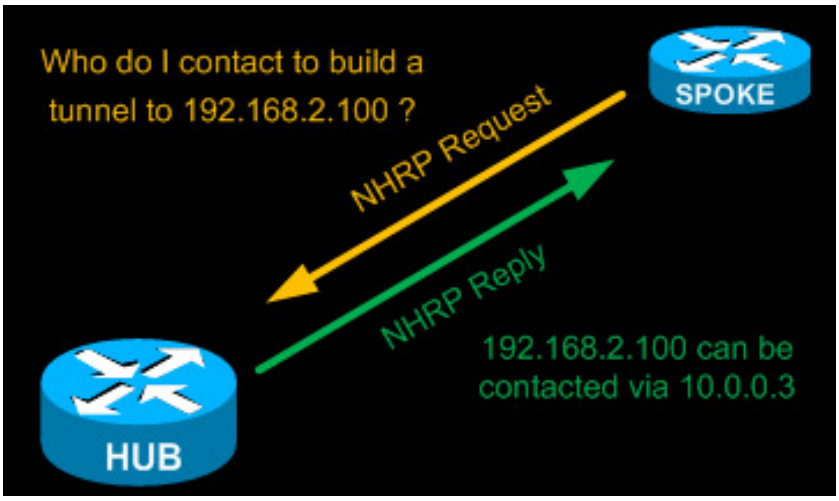

Figure 4.21: *NHRP query [69]*

The structure of the common NHRP header is shown in figure 4.22. It consists of eight fields - Src Proto Len, Dst Proto Len, Flags, Request ID, Source NBMA Address, Source NBMA Subaddress, Source Protocol Address and Destination Protocol Address. The Src and Dst Proto Len fields simply hold information about the length of the source and destination protocol addresses that are used. Flags is a field that is specific for each message type. The Request ID field is used as an identifier, grouped together with the source IP address of the packet. The Source NBMA Address and Subaddress fields carry the dynamically allocated public IP address of the source. The Source and Destination Protocol Address fields hold the value of the used protocol addresses by the sender and receiver of the packet. [76]

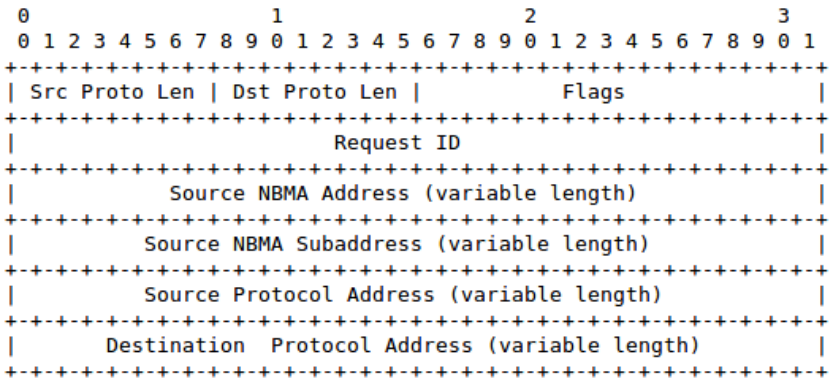

Figure 4.22: *NHRP header [76]*

4.4 Software-Defined Networking

Software-Defined Networking (SDN) is a concept that emerged around the 1990s and its main goal was to bring programmability into the networking sector. [1] Why? In order to provide the opportunity for more innovation in the field. Currently new features for network devices are being designed only by the large network vendors, such as Cisco, Juniper, Huawei, etc. It is not possible for the users to directly create a new functionality for their network device as it is with smart phones for example. What drives the need for SDN is the evolution of the cloud and virtualization technologies. [1] When discussing SDN in this thesis we are going to refer to the Open SDN and not to proprietary SDN technologies. It is important to note that SDN is not only about software, even though its name starts with this word. The importance of ASIC chips is crucial for high-speed packet switching and the need for specialized hardware will always be significant in the networking field. [77]

4.4.1 SDN Fundamentals

According to [77], there are four fundamental building blocks of SDN - plane separation; simplified device and centralized control; network automation and virtualization; and openness.

Plane separation

For a better understanding of this principle, the three levels of network abstraction are shown in figure 4.23. The data or forwarding plane is responsible for the transmission of packets based on forwarding tables. The control plane is the protocols that are used to manipulate the data forwarding mechanisms. The management plane relies on software tools that are used to influence the protocols in the control plane. [40] This level of separation is the foundation for SDN.

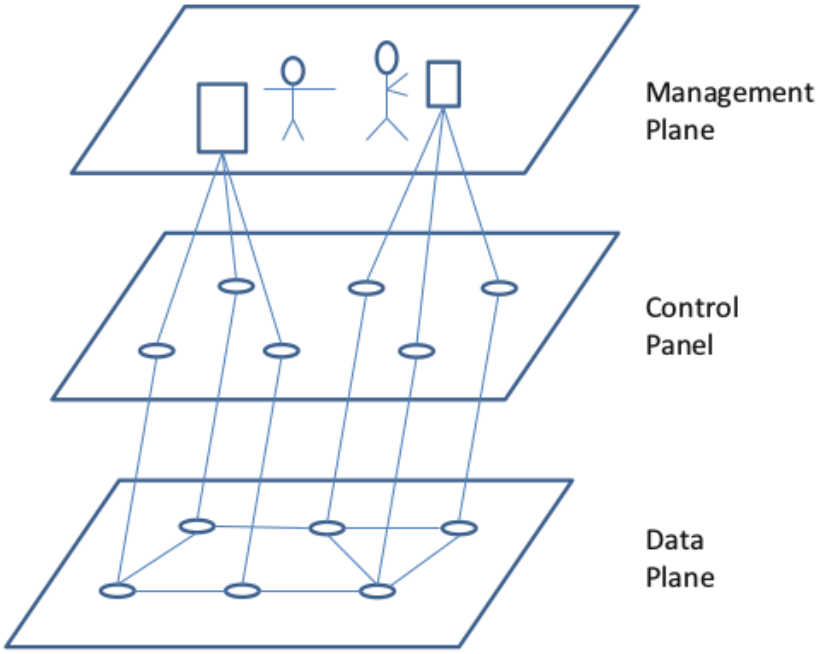

Figure 4.23: *Three network layers [40]*

Simplified device and centralized control

A comparison between the classic internet and SDN plane models is shown in figure 4.24. As we can see from the figure, the classic internet architecture (a) facilitates both the data and control planes in each device. This leads to a hardware centric approach and requires each device to be individually configured with vendor specific commands. [40] This makes the implementation of large scale network environments a difficult and time consuming job. Instead, the SDN architecture (b) provides a centralized control model, through which the controller distributes the necessary configurations to the other devices.

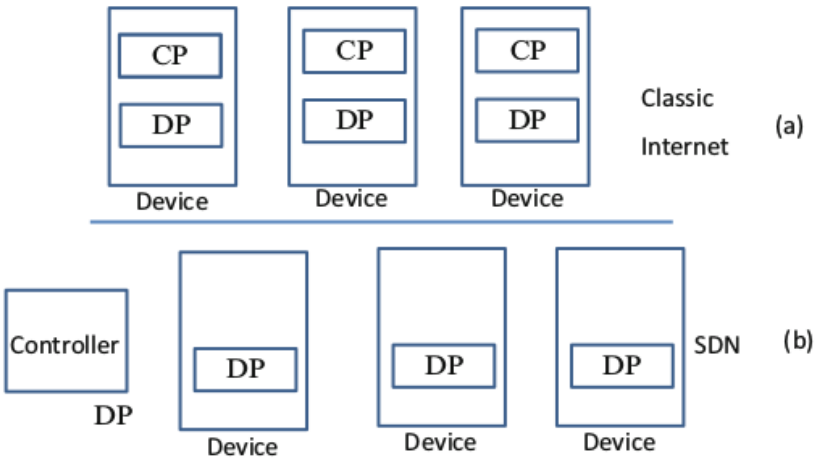

Figure 4.24: *Classic internet and SDN architectures [40]*

Network automation and virtualization

As mentioned in [77], SDN can be considered as an analogy of the evolution in programming languages, which evolved with the help of abstraction. This abstraction allows for virtualization of the network functions and leads to greater productivity. It is important to note that it is the virtualization that allows SDN to not be vendor specific. Figure 4.25 shows the SDN architecture and its two types of links - the northbound and southbound interfaces. The northbound Application Program Interface (API) is used to connect the controller to the management plane, where all the applications reside. [77] This type of interface can serve as a gateway towards high-level network automation. Example for a northbound interface is the REST API and it can be used for integration with the modern automation tools - Puppet, Chef, Ansible, etc. [78] The southbound API is the link that allows the controller to dynamically configure the forwarding network devices. [77] The most widely used and open standard for the southbound API is OpenFlow, which will be discussed later in this thesis. [79]

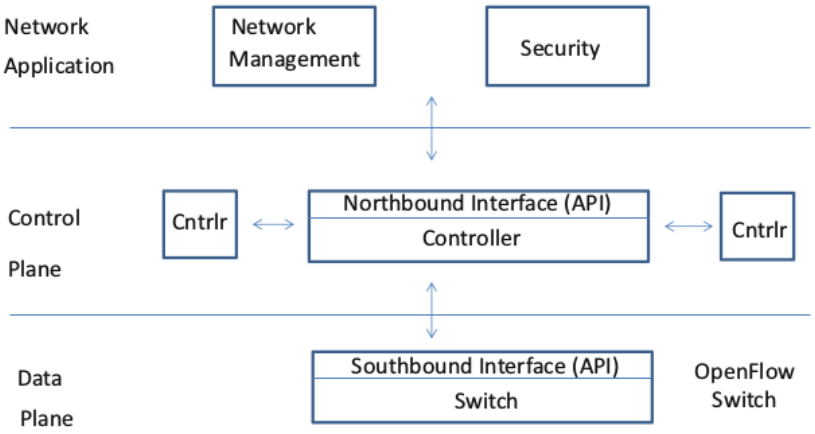

Figure 4.25: *SDN architecture [40]*

Openness

The idea behind SDN is that everything should be accomplished through the use of open standards. [77] In this way anyone can understand and contribute to the development of SDN, without the concern of proprietary secrets. The Open Networking Foundation (ONF) is a non-profit organization that is responsible for development and promotion of SDN technologies. It was created by Deutsche Telekom, Verizon, Microsoft, Google, Facebook, and Yahoo in 2011. [80] It has created the OpenFlow standard, as well as Mininet - a virtual environment for testing software-defined networks. Another important contributor is The Linux Foundation. It is responsible for creating the most widely used software for a SDN controller - OpenDaylight. [81]

4.4.2 OpenFlow

OpenFlow was originally created at Stanford for experimental purposes, around 2008, before the ONF was formed in 2011 and later became standardized and managed by the ONF in 2012 after version 1.1. [77] It is known as the major southbound API protocol. There are many flavors of OpenFlow protocols that have been developed for both controllers and switches, the most widely known among switches is the Open VSwitch (OVS). [82] By switches, in the SDN context, we refer to the simple forwarding devices that operate in the data plane. There are two types of OpenFlow switches - pure and hybrid. [83] Pure OpenFlow switches are the simplest of devices, also referred to as white box switches, and they are incapable of functioning without a controller. Hybrid switches, on the other hand, facilitate both OpenFlow and traditional forwarding methods. The current version of OpenFlow is version 1.6, as specified by the ONF but we are going to be discussing the previous 1.5.1 version due to

restricted membership access for the newest version by the ONF. The architecture of an OpenFlow switch is shown in figure 4.26. It consists of multiple flow tables, a group table and a channel. The channel represents the abstraction layer that is used to securely transmit data between the switch and the controller. [40] The flow and group tables are going to be discussed later in this section.

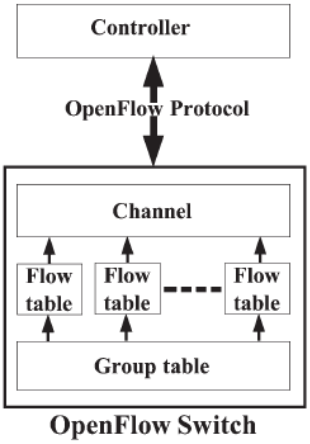

Figure 4.26: *OpenFlow switch architecture [82]*

OpenFlow ports

OpenFlow ports are the switch interfaces that are used to transmit and receive OpenFlow packets. An OpenFlow enabled port can serve as ingress or egress for a packet. OpenFlow switches support multiple packet queues per port, which allows to differentiate between packet flows with different QoS levels. [77] This principle is at the core of OpenFlow data forwarding. It allows the OpenFlow switch to map a given packet flow, with specific ingress and egress ports, to the necessary queue or QoS class. There are three types of OpenFlow ports - physical, logical and reserved. There are also standard ports, which define the combination of physical, logical and the LOCAL reserved port. The physical ports are simply the hardware switch ports that are linked to their respective interfaces. The logical ports represent custom configurable ports that can be linked to a virtual abstraction of one or more physical ports. The reserved ports are divided in two categories - required and optional. The required reserved ports are ALL, CONTROLLER, TABLE, IN_PORT, ANY and UNSET. Optional are LOCAL, NORMAL and FLOOD. [84]

Flow table

The processing of packets in the OpenFlow switch is shown in figure 4.27. There can be one or multiple flow tables, containing the specific flow entries of the switch ports. Packet processing is divided in two stages -

ingress and egress. The ingress processing occurs when the packet enters the ingress port of the switch. The switch determines whether the packet is to be forwarded by matching it to its flow tables, if so the packet is sent for egress processing. According to [77], matching criteria for the packets can be the following:

- Switch input port
- VLAN ID
- VLAN priority
- Ethernet source address
- Ethernet destination address
- Ethernet frame type
- IP source address
- IP destination address
- IP protocol
- IP Type of Service (ToS) bits
- TCP/UDP source port
- TCP/UDP destination port

The group table is used to modify the flow entries if necessary. Each flow entry consists of Match Fields, Counters, Actions and Table Miss Entry. [40] The Match Field is used to determine if a packet matches the specific flow entry. The Counter is used for gathering statistical data, such as the accepted/dropped packet rate for the flow entry. The Action specifies the instructions for handling a packet that matches the flow entry. If a packet does not match the specific flow entries from the flow table, it is considered as a Table Miss Entry. In this case the action that the switch can perform depends on custom configuration. It can include dropping the packet, transferring it to another flow table or sending it to the controller. [84]

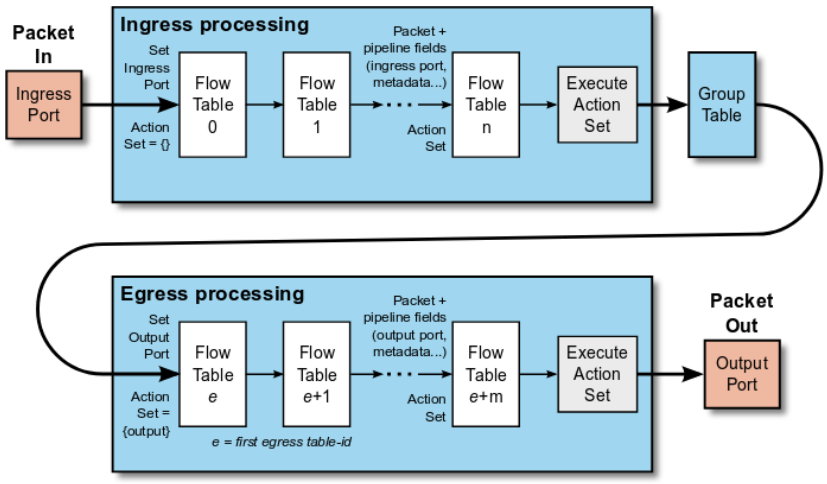

Figure 4.27: *OpenFlow switch processing [84]*

The OpenFlow protocol

The configuration of OpenFlow switches is done through the OpenFlow channel. This channel is the switches' uplink to the OpenFlow controller. For security purposes, the OpenFlow channel can be encrypted with TLS. [84] There are three types of messages that are supported by the OpenFlow protocol - controller-to-switch, asynchronous, and symmetric. Controller-to-switch messages are used only by the controller in order to query or manage OpenFlow switches. There are five controller-to-switch message types - switch configuration, command from controller, statistics, queue configuration, and barrier. [77] Asynchronous messages are triggered only by the switches to the controller, without its solicitation. They are used to update the controller's database regarding occurred changes in the switches. Symmetric messages can be initiated by both the controller and the switches without the need for solicitation.

OpenFlow is not the only standard for the southbound SDN interface, alternatives are also being developed. We are going to mention a few rivals of the OpenFlow protocol - IEEE P1520 standards initiative for programming network interfaces; Forwarding and Control Element Separation (ForCES), created by IETF; and SoftRouter. [82]

4.5 Conclusion

In this chapter we have examined in detail the principles of the MPLS, IPsec and DMVPN solutions. We have also included the fundamental principles of SDN and OpenFlow. This research is necessary to prepare us for the analysis in chapter 5. It is these examined technologies that are going to be compared to SD-WAN and it is very important to understand the

explained principles of operation. These principles will lead the analysis, together with the principles of SD-WAN that are going to be discussed in the next chapter. The use of the standards wars theory will be focused on the competition of each of the aforementioned technologies with SD-WAN.

Chapter 5

Analysis

5.1 Introduction

It is a challenge for the network to meet the current evolving application demands. Especially in the WAN sector, where the need for on-demand bandwidth and low latency, triggered by cloud applications is always rising. While enterprises are spending billions to virtualize and upgrade their data center infrastructure [85], the need for also upgrading the WAN is imminent. The revenue spent on cloud services is shown in figure 5.1, as predicted by IDC, for the time period 2015 - 2020. There are three major forms of cloud services - Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). As we can see this trend is showing exponential growth for the examined period.

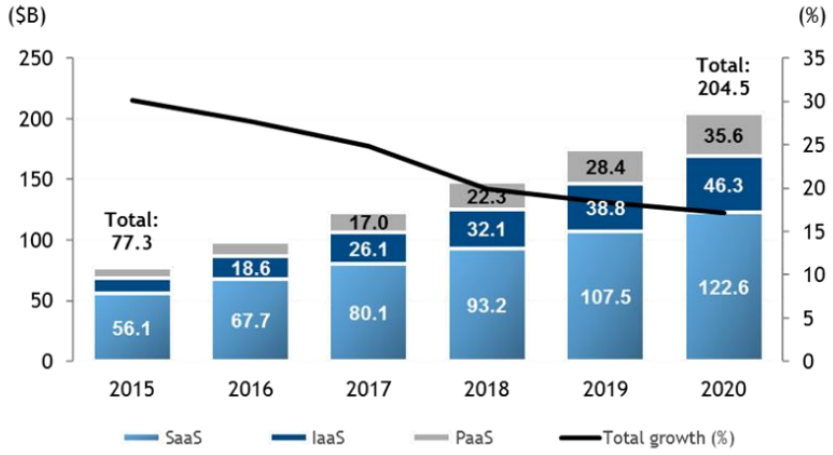

Figure 5.1: *The evolution of cloud services [86]*

It is the WAN that glues together all of the separate cloud infrastructures and creates the holistic network for the business. This effect also happens to occur in parallel with the rising adoption of SDN. Maybe the mix of these events is not a coincidence. Maybe it is especially SDN that is going to transform the WAN sector. According to [87], the most probable vast adoption of the SDN principles is expected to happen exactly in the WAN market. There are three major factors that drive the evolution of the WAN: [85]

- The cloud is transforming the network
- Unified Communications (UC) are becoming a critical part of the business
- Traditional computing is taking a network centric approach

In this chapter we are going to first introduce the SD-WAN technology and its components and then analyze it through comparison with its rival technologies. The standards wars theory will serve as a framework for conducting the comparison.

5.2 Software-Defined Wide-Area Networking

SD-WAN is a technology that has the potential to revolutionize the networking sector in the WAN area. It facilitates a new concept for the network sector - application-driven networking, where the network is expected to adjust according to application needs. [88] This concept allows SD-WAN to become a replacement of WAN optimization services, expensive MPLS VPNs and additional network automation and management costs. This new WAN concept can be seen in figure 5.2 and will be discussed more thoroughly later in this section. It is usually referred to as a hybrid WAN. The combination of all these features in one centralized solution, that is capable of outperforming the competition at an affordable price is definitely worth looking into. In this section we are going to briefly discuss some of the major SD-WAN vendors, examine the principles of operation and the different types of SD-WAN.

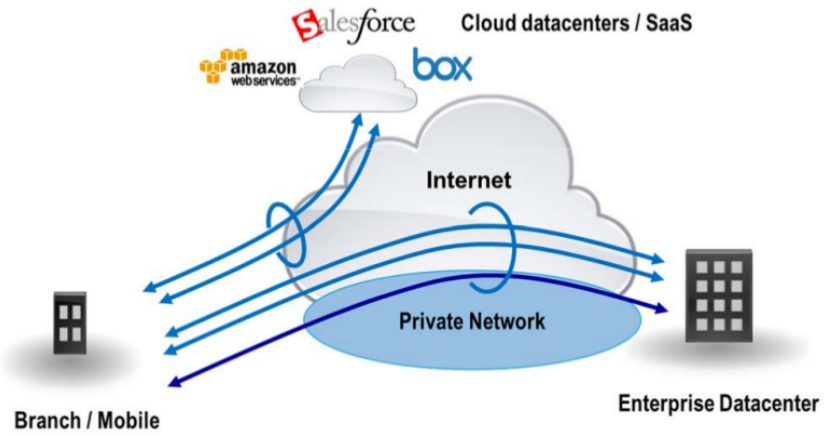

Figure 5.2: *The SD-WAN concept [89]*

SD-WAN Vendors

The current vendor situation in the SD-WAN market is a considerably interesting one. The incumbent communications vendor, Cisco, still follows

the strategy of the previous CEO of the company John Chambers. As mentioned in [15], the famous John Chambers quote "We don't do research — we buy research!" is still driving the company. Last year Cisco bought SD-WAN company Viptela for $610M and announced that it is going to work towards combining its features with Cisco's IWAN solution and provide a next-generation SD-WAN product. [90] It is interesting how much overstatement of the term next-generation is occurring in the networking field these days. Now, a year later there is an announced plan for the integration of Viptela's SD-WAN solution. According to [91], there is going to be a 3-phased plan for that integration in the next 12-24 months, where Viptela's solution is going to be completely integrated with Cisco's SD-WAN solution. Another interesting deal is the acquisition of VeloCloud by VMware. It happened also last year, shortly after Viptela's acquisition by Cisco and placed VMware as a strong competitor in the SD-WAN battle. [92] The strategy behind this deal was announced this year, resulting in a unified solution, named the Virtual Cloud Network, supporting the initial slogan of VeloCloud - "The cloud is the network.". [93] Another vendor, that is worth mentioning and has not been bought by any of the big players yet is Silver Peak. Silver Peak is a company with expertise in WAN acceleration and according to [87], Silver Peak's solution is capable of providing private line-like experience over the internet. The current SD-WAN solution provided by Silver Peak is named Unity EdgeConnect. It has a distinguishing feature - the so called First-packet iQ, which is used as an application-oriented QoS mechanism. [94] The concept behind this feature is shown in figure 5.3 and it is the fundamental building block of SD-WAN.

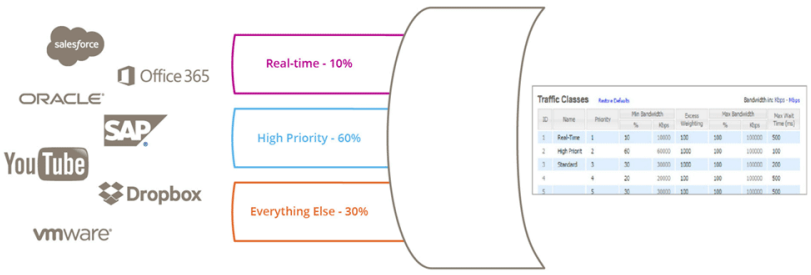

Figure 5.3: *Application-oriented QoS [95]*

Other major vendors that are involved in the SD-WAN market and deserve to be mentioned are Juniper, HPE and Riverbed. The two major acquisitions of Viptela and VeloCloud show that there is an increasing demand by the customer base for SD-WAN solutions. The competition in the SD-WAN market is only going to increase with time, as more enterprises start to explore this solution and its benefits. [91]

5.2.1 The SD-WAN Architecture

The SD-WAN architecture is shown in figure 5.4. As we can see from the figure, there are three major layers of the architecture - cloud network, virtual services and orchestration and analytics. The cloud network layer facilitates an overlay based network that is capable of establishing connections through both private and public IP infrastructures. It is designed to ease the communication to geographically separate locations, as well as to cloud applications and services. A major part of the cloud network layer is its security. [96] Given the fact that SD-WAN uses the public internet infrastructure as a transport network, security is a crucial part of its functioning. Some best practices for securing the communication channels are shown below: [97]

- Physical Security
  Prohibiting unrestricted physical access, monitoring the appliance, alarm control, protecting the physical interfaces, protecting the power supply
- Appliance Security
  Role based access control, strong password management, regular security updates, complete data erasure after decommissioning
- Network Security
  AES encryption, SHA authentication, Transport Layer Security (TLS), RADIUS and TACACS+ services, SNMPv3

Each SD-WAN device is required to authenticate itself to the controller, before it can participate in the secure cloud network. The device's authorization is controlled through the use of policies. These policies are controlled by the control plane and can be used to manipulate traffic, as mentioned in chapter 4.

The virtual services layer combines three types of services - branch services, data center services and cloud services. [96] It is responsible for optimizing the communication flow towards each of the different types of services. Branch services represent a specific service type that is located only at branch sites. A firewall is an example of a branch service, as mentioned in [96]. The firewall service can be realized through the use of Network Function Virtualization (NFV) and deployed virtually in the IT infrastructure. Data center services are usually most sensitive to WAN optimization. The firewall example that we mentioned earlier can also be used here. Its implementation in a centralized manner in the data center will allow for lower Capital Expenditure (CAPEX) costs for network devices. [96] However, this will lead to a change in the traffic patterns for the branch offices, requiring data to first pass through the data center. Cloud services represent the different aaS application solutions, provided

by cloud vendors like Microsoft, Salesforce and Amazon. This type of service is intended to be directly accessed from the internet, without the additional VPN overhead. SD-WAN aims at separating the cloud traffic from the rest and initiating direct connections to the preferred cloud provider. This allows for better utilization of its WAN services and if used together with MPLS VPN, it also utilizes MPLS traffic more efficiently.

As discussed in chapter 4, the SDN principles are based on the separation of the control and data planes. SD-WAN's principle of operation facilitates the same mechanism, isolating the control plane in the so called orchestration layer. There are three core functions of the orchestration layer - management plane, highly available and resilient control plane and business policy framework. [96] The management plane represents a high level abstraction for policy deployments, configuration management, troubleshooting, monitoring and reporting. The consolidation of these features creates a superior management interface, able to control large-scale deployments with ease. The concept behind such deployment cases is known as Zero-Touch Provisioning (ZTP). With ZTP each CPE device does not require to be individually configured, instead it downloads its configuration from the centralized control plane after authentication. [88] This form of automation removes the need for qualified personnel at each branch office. The highly available and resilient addition for SD-WAN's control plane is targeted at providing seamless transition from legacy WAN technologies to SD-WAN. [96] The control plane itself can be positioned on on-premise IT infrastructure or in the cloud. The management functions of the control plane can be accessible through web services or APIs. [88] The business policy framework is concerned with service assurance policies and business governance strategies. [96]

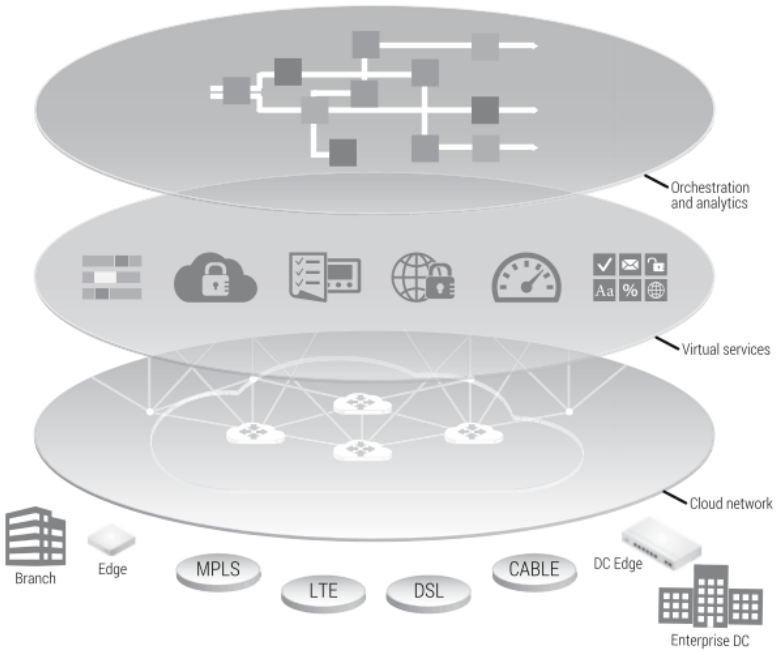

Figure 5.4: *The SD-WAN architecture [96]*

Viptela's SD-WAN solution

For an actual implementation of the SD-WAN principles, Viptela's Secure Extensible Network (SEN) solution is shown in figure 5.5. We have chosen to look into Viptela's solution based on Cisco's leading position in the networking market. There are four different components of Viptela's SD-WAN architecture - vSmart Controller, vBond Orchestrator, vEdge Router and the vManage Configuration and Monitoring System (CMS). [98] Each of the four components has its own specific functions and abilities. The vSmart Controller represents the SDN control plane, where the centralized configuration engine is running. It is responsible for the overall control of the data plane and all types of traffic manipulation. The connections between the control and data planes rely on the Datagram Transport Layer Security (DTLS) protocol. It is a special version of TLS, designed to work with UDP. [99] Its current version - version 1.2 is specified in RFC6347. The communication protocol that is used to exchange configuration information between the vSmart Controller and vEdge Routers is Overlay Management Protocol (OMP). OMP is Viptela's proprietary communication protocol for sharing information between the control and data planes. [100] The vSmart Controller is distributed as a virtual appliance, compatible with VMware hypervisors. [98]

The vBond Orchestrator is an additional software that resides on top of the vEdge Routers and is specialized in the initial process of communication between the router and the controller. [98] As we can see from figure 5.5, it is also responsible for utilizing the best possible communication

channel to the controller, whether that is the internet, an MPLS service or a mobile connection. The initial process of communication is referred to as the bringup process and it is responsible for the authentication and authorization of all participating devices in the overlay network. [101]

The vEdge Router is the next component that we are going to look into. It represents the CPE device that is to be placed at the different types of customer locations. As shown in figure 5.5 it can be used throughout all facilities, such as data centers, campus offices, branch locations and remote sites. The vEdge Routers are an upgraded version of the usual IP router that is capable of facilitating the software-defined and orchestration principles alongside traditional routing procedures. [98] They are able to provide all of the essential routing features, including routing protocols like BGP and OSPF, QoS, policy and access control, and network managemnt. [102] We mentioned that for the secure communication between the vSmart Controller and vEdge Router, DTLS is used. What about the communication between multiple vEdge Routers? Do we still remember IPsec from chapter 4? The securing of the communication between different vEdge Routers happens through IPsec tunnels. [98]

The last component of Viptela's SEN solution is the vManage CMS. The vManage CMS represents a platform for holistic configuration management and monitoring of all participating devices in the enterprise. [103] It is software based and is designed to be deployed as a virtual appliance, again compatible with VMware hypervisors. [98]

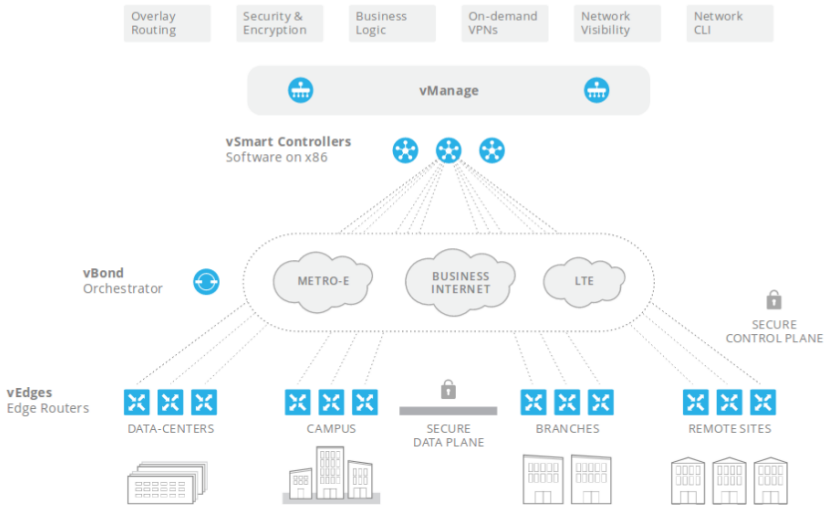

Figure 5.5: *Viptela SD-WAN architecture [98]*

5.2.2 ISPs' standpoint

Before diving into the situation of ISPs regarding the evolution of WAN services, there is one concept that we need to get familiar with. The concept of Managed Service Providers (MSPs). A MSP is responsible for delivering and supporting application, network or system services to multiple client companies, through its own IT infrastructure. [104] The process of hiring a MSP for our network infrastructure can be viewed as outsourcing it to a company that is specialized in that field and has the necessary expertise and infrastructure to support our network segment for a monthly subscription fee. Why is this important? Currently ISPs are earning a significant amount of revenue from MPLS VPN services, operating through their network infrastructures. Before the emergence of SD-WAN, a research from Radiant Insights estimated that the MPLS VPN market would be worth $26.62 billion by 2020. [105] As we can imagine, ISPs are not that thrilled with the emergence of SD-WAN, which will cause a substantial impact on their MPLS market. However, if there was a scenario in which ISPs were to gain from the SD-WAN technology, the situation would be different. Here is the place where the MSP principles come in play. ISPs are in the perfect spot to position themselves as SD-WAN MSPs.

5.2.3 SD-WAN deployment options

Every enterprise has to make the choice, whether to implement SD-WAN as a Do-it-Yourself (DIY) solution or to hire a MSP/ISP for its realization, also considered as Managed SD-WAN. Some important pros of both approaches are mentioned in table 5.1. [106] Major benefits of the DIY approach include cost savings, total control and independence. Usually the DIY solution is expected to cost less than the added subscription fees of MSPs. This is due to the fact that the most expenses with SD-WAN are spent through its deployment. [107] Also, the DIY solution offers total control of the enterprise's IT infrastructure, without involving third parties in any of the processes. This is especially important for businesses which hold sensitive information and are against the involvement of any outsider companies. Independence is a crucial factor for flexibility and should not be underestimated. [108] It consists of a company's ability to make significant changes to its IT infrastructure without waiting for complicated and time-consuming procedures from companies such as ISPs. The aforementioned benefits make a strong point for the adoption of SD-WAN as a DIY solution, but they come with a cost. [109] For a company to be able to deploy the DIY solution, it has to have significant resources and expertise in the field. This shapes the DIY strategy as most relevant for large enterprises.

Let us now examine the advantages of the Managed SD-WAN solution. Functionality, scalability and qualified personnel. By functionality, we are

referring to the time it takes for a specific feature to be implemented in the SD-WAN architecture. [106] Because ISPs are usually large enterprises, in control of multiple specialized IT departments, they are able to quickly respond and tackle complicated problems and implementations. This detail is also responsible for ensured scalability of the SD-WAN solution. The resources of ISPs can be considered as limitless, as they are always able to grow, depending on the customer demand. [109] SD-WAN as a managed service has one more very important advantage - qualified personnel. This removes the need for specialized IT professionals in the enterprise, resulting in reduced personnel costs. The listed benefits of the managed SD-WAN solution seem more appropriate for small enterprises, where the required functionality, scalability and expert-level personnel are missing.

DIY solution advantages	**Managed solution advantages**
Cost savings	Functionality
Total control	Scalability
Independence	Qualified personnel

Table 5.1: SD-WAN DIY and Managed approach advantages

There is also a third option for the deployment of SD-WAN - SD-WAN-as-a-Service. This option leverages the functionality of the cloud in order to allow SD-WAN to be used as a service and provide important benefits such as flexibility, fast deployment and low cost. [110] Some companies, like Citrix, are aiming at creating high-performance SD-WAN-as-a-Service solutions, targeted at ISPs and MSPs. [111] In this way, a reselling strategy comes in play, allowing service providers to buy the SD-WAN service as a cloud solution and resell it as an individual service to their customers. A comparison graph of the different SD-WAN solutions is shown in figure 5.6. The DIY approach is labeled as Internet-Based SD-WAN. As we can see the graph confirms our reasoning for the cost difference between the managed and DIY solutions. SD-WAN-as-a-Service is positioned somewhere in the middle, regarding cost and on top, regarding performance. Given the fact that the graph is taken from a SD-WAN-as-a-Service vendor, this performance top position is questionable, however, the cost position is in line with the rest of the conducted research.

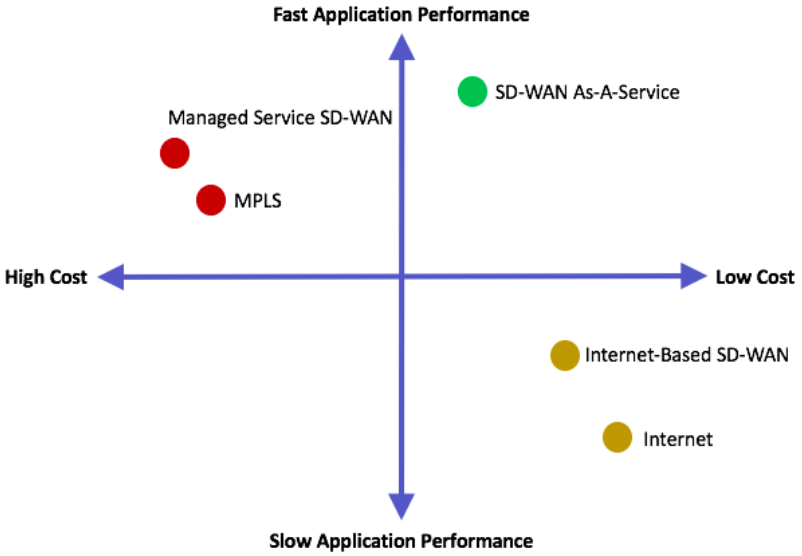

Figure 5.6: *SD-WAN deployment scenarios comparison [110]*

5.2.4 SD-WAN service types

According to [112], there are three types of SD-WAN service scenarios - prem-only, cloud-only and hybrid. These three flavors are concerned with the specific service that the client is able to use through the SD-WAN solution, rather than the deployment options which we discussed in the previous subsection. The prem-only type is the most basic type of SD-WAN service. It includes only full-mesh connectivity between the geographically separated branch offices. [112] This type of solution is designed for enterprises which do not require the use of cloud services and therefore do not need to pay the additional costs for the cloud-ready SD-WAN solution. The most important benefit of the prem-only solution is real-time traffic shaping, which utilizes the application-oriented QoS mechanism, mentioned earlier in this chapter. [113] The cloud-only service type is intended for enterprises which want to optimize their access to the cloud. [112] It provides the same application-driven QoS architecture as the prem-only solution, but specifically designed for cloud application performance. The functionality of this solution relies on the concept of the cloud gateway. The cloud gateway can be viewed as a gateway of last resort for all of the major cloud applications, such as Office 365, Salesforce, AWS, etc. [113] It provides direct access to these applications, improving their performance and reliability. This solution is designed for enterprises that have adopted a cloud-based IT infrastructure. The final type of SD-WAN service is the hybrid solution. It incorporates the prem-only and cloud-only solutions into one hybrid SD-WAN service, able to provide both - a reliable full-mesh WAN infrastructure and high-performance cloud connectivity. [112] This solution is designed for enterprises which want to

completely replace their current MPLS services with the next-generation, application-oriented WAN concept. Or for enterprises who want to utilize the SD-WAN solution together with a MPLS VPN. The hybrid SD-WAN service is the most flexible, scalable and performance-oriented WAN solution that exists in the WAN market today. [114]

5.3 SD-WAN versus Multiprotocol Label Switching VPN

In this section we are going to compare SD-WAN to its greatest competitor - MPLS VPN, from now on simply MPLS. We are going to start with a layout of the technical benefits of both technologies. Afterwards we are going to apply the standards wars framework, discussed in chapter 3 in order to determine what is the likelihood of SD-WAN replacing MPLS.

5.3.1 Technology comparison

For the technology comparison of SD-WAN and MPLS, we are going to use the examined principles of operation of MPLS, from chapter 4 and the SD-WAN principles, discussed in the beginning of this chapter. Based on that research, we are going to lay out the important advantages of both technologies. The approach for discussing the technological advantages of SD-WAN and later the rest of the rival technologies will follow a structured methodology. First we are going to display as bullet points the most relevant benefits of each technology and afterwards these bullet points will be explained.

SD-WAN advantages

- Lower costs
- Cloud-ready
- Guaranteed security
- Scalability
- Removing bandwidth limitations
- Eased network management

Maybe the most alluring advantage of SD-WAN for the enterprise is its cost. Compared to MPLS costs, which typically range between $750 and $1000 per month in the US [115], SD-WAN offers lower monthly costs, if implemented as a managed service. If implemented as a DIY solution,

the Operational Expenditure (OPEX) costs are expected to be included in the IT department personnel costs. Therefore, we can deduce that the SD-WAN DIY solution OPEX costs are equal to zero. Of course, if we are looking to deploy SD-WAN as a DIY solution in a large enterprise with a lot of branch offices, which we discussed previously as the most relevant application of the DIY approach (section 5.2), it will include large CAPEX costs. But when we split these costs in time and include the ability for total control over the network it is certain that MPLS costs will again be greater, since the subscription fee for the service is going to remain a factor throughout the whole life cycle of the company.

The cloud-ready factor is something that MPLS simply can not provide. It is especially important for enterprises which rely on the cloud for their business and want instant access to their cloud applications. It is important to remember that we need the cloud-only or hybrid type of SD-WAN in order to use this advantage. (section 5.2) The advantage is based on the next-generation application-oriented QoS mechanism that the SD-WAN solution provides. This is the new concept that emerged in the networking field after the adoption of the SDN model. This application-oriented approach is taking not only the WAN sector, but also the LAN. The evolution of SDN into intent-based networks [116] for the LAN segment is also showing us that the focus on applications in the network is spreading everywhere.

The guaranteed security of SD-WAN, which relies mostly on IPsec (section 5.2), can be considered as one of its main advantages over MPLS. As MPLS does provide a certain level of security by separating VPN traffic through the use of VRF tables, it does not encrypt that traffic. This protects the traffic from the internet, but does not protect it from the ISP. And with the ever-evolving cybersecurity threats nowadays, some enterprises which hold and transfer sensitive data can not afford to transmit that data unencrypted. SD-WAN provides full encryption of all connections, either through DTLS - from controller to edge devices, as mentioned in the Viptela case. Or through IPsec - between the different edge devices. (section 5.2) However, it is possible to apply IPsec to an existing MPLS VPN. This will remove the security issue from the table, but it also includes another one. As MPLS costs depend on the required bandwidth and IPsec is adding a significant amount of overhead to the IP packets, it can double the size of the packet, according to [117] and lead to inefficient bandwidth utilization.

The ability to scale is of a great importance to WAN technologies since that is one of their core purposes. The SD-WAN architecture allows for enhanced scalability, compared to MPLS, since each edge device represents a plug-and-play router, as discussed in section 5.2. This allows for

rapid addition of branch sites to the current WAN network of the company. Ultimate scalability of SD-WAN can be achieved when it is deployed as a DIY solution and there are no external parties involved in the process.

With MPLS, as mentioned before, the bandwidth of the communication channel is directly linked to its cost. This forces companies to use minimum capacity transmission channels and apply QoS mechanics in order to use the MPLS services in the most efficient way. With SD-WAN this is no longer the case. As discussed in section 5.2, SD-WAN uses basic internet connectivity and its service does not depend on the bandwidth. Customers are able to easily upgrade or downgrade their internet subscription based on their needs.

Network management. This is the benefit that most concerns the IT department and more specifically the network engineers and administrators. With the adoption of the software-defined principles, the centralized management system - vManage for example, from Viptela's SEN solution (section 5.2), is able to provide control over the entire WAN network through a simple web interface. This can be considered as a revolution, compared to the network management approaches that are used with MPLS VPN. There each router needs to be configured separately through complex command-driven interface, also known as the Command Line Interface (CLI). Although, the more complex part of the configuration is the ISP's concern, as it becomes clear from the research in chapter 4, enterprises will need to send qualified personnel to every new branch when deploying the MPLS solution.

MPLS VPN advantages

- Private channel reliability
- High level of QoS
- Scalability

The biggest and most important advantage of MPLS is its reliability. From the MPLS discussion in chapter 4, we have learned that it uses a connection oriented mechanism which provides a virtual private channel for the VPNs of each customer. This means that the MPLS VPN solution is highly reliable and presents the customer with private-line-like experience. This is especially important for enterprises that are in a constant use of real-time applications, such as VoIP or streaming services. Unfortunately SD-WAN can not provide the same level of reliability as MPLS, since it uses the public internet infrastructure as a transport network. This fact introduces the opportunity for reasoning whether SD-WAN is ever going

to completely replace the MPLS VPN solution. A probable scenario is that SD-WAN is going to replace MPLS only in small enterprises, where the cost is the most important factor. For large enterprises and for real-time application sensitive businesses, MPLS is still going to serve as the core WAN solution. SD-WAN, however, is able to complement it through its efficient WAN optimization and cloud-friendly behaviour.

Though MPLS does not provide application-driven QoS mechanisms, its QoS capabilities are still considered as very efficient (chapter 4) and as one of its most important advantages. The label switching mechanism, discussed in chapter 4, allows for extremely efficient traffic manipulation. Of course, it is controlled from the ISP, but so it is with the managed SD-WAN service. If customers want to be able to control their QoS policies, their options are limited to the SD-WAN DIY solution or DMVPN.

We discussed scalability as an advantage of SD-WAN. It is also an advantage of MPLS, since both technologies are able to provide worldwide connectivity. There is one catch, however. If we can deploy SD-WAN as a DIY solution and add a new branch in a day, that is certainly not the case with MPLS. As the MPLS VPN is controlled by ISPs (chapter 4), the addition of new sites to the current topology usually needs to be coordinated with multiple departments at the ISP. This introduces delay into the process with the time it takes for all the departments to synchronize their actions and perform the required procedures. Therefore MPLS as a technology is highly scalable, but its deployment as a VPN service can take more time than expected.

5.3.2 Defining the type of the war

Here we start following the standards wars framework for evaluating the competition between SD-WAN and MPLS. We will start by defining the type of the standards war, as discussed in chapter 3. Since SD-WAN is the only new standard offered in the WAN market, this narrows down the type down to two options. Evolution or revolution. SD-WAN is a new solution for the WAN market and it is designed to outperform MPLS, but it is also able to work together with MPLS - both technologies are compatible with each other. Therefore the strategy for the war that SD-WAN started, based on our research in chapter 3, is the evolution strategy.

5.3.3 Asset examination

In this part of the analysis, the discussed assets from chapter 3 will be examined from the standpoint of SD-WAN. The advantages of both technologies will be discussed, regarding each asset.

Control over an Installed Base of Customers

The first asset that we are going to examine is in favor of MPLS. Why? Because the MPLS VPN market is the biggest WAN market in the world, as mentioned in chapter 1. This places MPLS as the dictating standard in the field. Its position as a market leader allows ISPs to control the WAN market and this is why we discussed MSPs in section 5.2. ISPs have seen the potential of SD-WAN and since they are in control of the WAN market, they are trying to assimilate SD-WAN into their portfolio and continue their reign over the WAN.

Intellectual Property Rights

All SD-WAN vendors put a lot of emphasis on their intellectual property rights. There isn't a single open-source SD-WAN solution. MPLS, on the other hand is an open standard, as mentioned in chapter 1. This provides SD-WAN with the advantage of leveraging the openness of MPLS and chasing a hybrid solution (section 5.2), which can combine the benefits of both technologies. As we can see from the SD-WAN service types, discussed in the previous section, this is exactly what SD-WAN vendors are doing. Everyone of them is offering the hybrid SD-WAN solution that is capable of utilizing the existing MPLS architecture and provide optimized cloud services on top of that.

Ability to Innovate

The ability to innovate is an interesting asset when we take into account the big number of vendors in the SD-WAN market. (section 5.2) Since each solution is proprietary, the development of extensions for the SD-WAN solution is highly dependent on the vendor. We can certainly mention that there is room for extensions, when we are discussing cloud connectivity. MPLS and BGP extensions are closely related to the functionality of the technology itself, as examined in chapter 4. When talking about pure layer 2 and layer 3 VPN services, there is not a lot of room for customer focused extensions. This makes this asset in favor of SD-WAN, as software-based extensions are most probably going to become a necessary part of the SD-WAN solution.

First-Mover Advantages

None of the two technologies is to be considered as a first-mover in the WAN market. However, MPLS has been dominating the WAN market for over 15 years (chapter 1), which puts it in possession of the benefits of a first-mover standard. Based on the standards wars theory (chapter 3), this places MPLS in a strong position for continuing its market dominance. But this case is a lot more different than the Coca-Cola example, mentioned

in chapter 3, and with all of the benefits of SD-WAN, discussed previously in the technology comparison, SD-WAN has a strong chance of replacing MPLS regarding small and medium enterprises.

Manufacturing Capabilities

As we remember from chapter 3, this asset is concerned with saving production related costs. What do the costs of SD-WAN include? Manufacturing the devices, software, their implementation and support. If we take the DIY solution as an example (section 5.2), where the client company is supposed to buy the devices directly from the manufacturer, there is only the manufacturing costs that we need to consider. This is the case, because the client company is going to implement and support the devices itself. For the managed service, we can see the same outcome. The difference is that the buyer is a MSP which is then responsible for the implementation and support. So, manufacturing cutting edge devices and software for those devices is the main expenditure for SD-WAN vendors. This can be pricey! What about MPLS? Are most of the network devices out there MPLS ready? Yes. This places this asset in favor of MPLS.

Strength in Complements

SD-WAN is a main product, so is MPLS. What complements some could ask? Here is the place where we can emphasize on the cloud connectivity. SD-WAN is mostly advertised as a main product, direct competitor to MPLS, however it can also complement MPLS with its hybrid approach. As discussed in section 5.2, SD-WAN can be implemented on top of the existing MPLS network and be used as a WAN and cloud optimization solution. It works the other way around too. MPLS can complement SD-WAN for a reliable WAN backbone.

Reputation and Brand Name

Since SD-WAN is a new product, it has not gained much of a reputation yet. MPLS, on the other hand has established its name throughout the years. (chapter 1) When it comes to brand names, however, the situation gets a little more interesting. As MPLS is not a proprietary standard, there are no brands behind it. With SD-WAN, all of the major networking vendors are standing in support. Why is that? Because they can see the potential for controlling a large part of the market, in the case their product becomes the de facto standard. (chapter 3) This lays the foundations for future research on the competition between the different SD-WAN vendors. MPLS wins the reputation, but loses the brand name.

5.3.4 Strategy examination

As we mentioned earlier, SD-WAN is not a first-mover in the WAN market and therefore the preemption strategy is not applicable in this case. Nevertheless, we can not say whether SD-WAN vendors have adopted a penetration pricing scheme for competing with MPLS and the other rivals yet. The more probable strategy for SD-WAN is expectations management. We can see simply open Google, type SD-WAN and see that the vendors are spending a lot of money on advertising the expectations for the new technology. There are plenty of sponsored articles on the subject - [118] [119], just to name a few. And since MPLS is not backed up by a specific vendor, this takes away its opportunity for fighting back. The formation of coalitions between the different SD-WAN vendors is an interesting discussion. If the original strategy of expectations management fails, it is highly plausible that the individual vendors will seek coalitions in order to strengthen their position on the market. (chapter 3)

5.3.5 Outcome of the war

Based on the technology comparison and asset examination that we performed in this section, we are going to discuss the probable outcome of the standards war between SD-WAN and MPLS VPN. It is clear, from the technology comparison that SD-WAN provides more advantages to the enterprise than the traditional MPLS approach. Some of them, like the lower cost, cloud-ready factor and the guaranteed security of SD-WAN place this standard as a superior one. However, the private channel reliability of MPLS VPN is still going to attract customers who require maximum reliability for their WAN traffic. When we compare the examined assets from the standards wars framework, MPLS VPN seems to be holding one asset more then SD-WAN. Therefore, even with the superior WAN performance of SD-WAN, MPLS VPN is still in a position from which it can fight back. This is due to its established customer base, first-mover advantage, manufacturing capabilities and reputation. So the possibility of SD-WAN completely replacing MPLS is not a probable scenario in the near future. Since both standards are able to complement each other in an efficient manner, it is plausible to assume that they are going to coexist until a new, integrated solution emerges. But if SD-WAN manages to justify its expectations, triggered by the expectations management strategy, it is very likely that it will gain a significant market share in the WAN business.

5.4 SD-WAN versus Internet Protocol Security VPN

In this section we are going to examine the rivalry between SD-WAN and IPsec. But wasn't IPsec part of SD-WAN? Yes, it is. The comparison between these two technologies is going to take an interesting turn. Since IPsec is an open standard, that can be used not only with SD-WAN, but also with MPLS VPN and DMVPN, it does not appear to be a main product competitor in the WAN market. The reason for this is that IPsec is able to provide only a pure VPN tunnel service through the public internet infrastructure. There is no traffic reliability, as with MPLS, no WAN or cloud optimization as with SD-WAN, and no peer automation as with DMVPN. Instead, IPsec is to be considered as a complementary product to the other WAN solutions. This changes our methodology for applying the technology comparison and standards wars framework in this section. For the technology comparison, we are going to examine what makes IPsec valuable to SD-WAN and the other two WAN solutions. As for the standards wars framework, we are going to focus only on the "Strength in Complements" asset, discussed in chapter 3, as it is the most relevant. Since there is not much of a battle in this case, we are not going to discuss the type of standards war and the different strategy types.

5.4.1 Technology comparison

Based on the research on IPsec, conducted in chapter 4, we are going to bring out what makes this technology such a desired complement for all of the other WAN solutions. We are going to lay out the advantages of IPsec that we consider relevant for this approach, as we did in the previous example.

IPsec advantages as a complementary technology

- Confidentiality
- Integrity
- Application independence

IPsec provides three main benefits regarding data transmission - confidentiality, integrity and application independence. The technologies and protocols behind these benefits are discussed in chapter 4. It is the unmatched level of the first two benefits that makes IPsec the top security choice for internet communication. [59] We should keep in mind, that IPsec is also capable of providing the tunneling of multicast and broadcast traffic, through the use of GRE. The application independent approach

that IPsec uses is based on its core layer 3 transmission principles, discussed in chapter 4. These principles allow for no application compatibility issues through the VPN solution. [120]

5.4.2 Asset examination

As we mentioned in the beginning of this section, here we are going to examine only one asset from the standards wars framework - "Strength in Complements", due to the nature of IPsec as a complementary product to the rest of the WAN solutions.

Strength in Complements

IPsec has established its reputation as the de facto standard (chapter 3) for secure network layer communication over the internet through the years. [59] Although, as we mentioned earlier, IPsec is an open standard (chapter 4) and therefore there is no enterprise behind it, pushing for the strengthening of this asset's position, IPsec manages to push on its own. This is due to its functionality and reputation as a secure and reliable means for IP data transmission.

5.4.3 Outcome of the war

Since we made it clear that IPsec is not a main product competitor to SD-WAN, the outcome of this war is a win for SD-WAN. But IPsec remains an integral part of SD-WAN with its confidentiality, integrity and application independence advantages. As we discussed in the asset examination section, the main benefits of IPsec are in its reputation and openness, which makes the adoption of its advantages available to all of the interested parties. IPsec has been around for a long period of time [63], securing IP communications over the internet, and that does not appear to change anytime soon.

5.5 SD-WAN versus Dynamic Multipoint VPN

The final section, focused on the rivalry in the WAN market is going to examine the competition of SD-WAN and DMVPN. Since both technologies are proprietary solutions, this presents the opportunity for full asset and strategy examination (chapter 3). However, DMVPN is a solution that is offered from only one vendor in the network sector - Cisco. SD-WAN on the other hand is offered by nearly all of the major players, including Cisco. Therefore, one perspective is to look at the internal vendor strategy for product distribution, in this case Cisco's. This, unfortunately, is not possible due to the nature of this approach, as it interferes with the

confidentiality policies of the vendor. It is possible, however, to briefly examine Cisco's strategy so far, based on the company's publications on the subject. We are going to do that here and for the application of the standards wars framework, we are going to examine the rivalry of SD-WAN vs. DMVPN in the case of Cisco vs. all of the rest vendors.

Cisco's WAN strategy

According to [121], Cisco's first SD-WAN strategy was to use its DMVPN technology as a core for its IWAN solution. DMVPN, together with another Cisco proprietary technology - PfRv3 [122], were meant to provide a hybrid WAN solution, that was able to utilize both MPLS and public internet infrastructures. Later, with the acquisition of Viptela, Cisco decided to create three different SD-WAN offerings based on Viptela, Meraki and IWAN solutions, targeted at different types of customer demands. [123] This approach differs from most of the other SD-WAN vendors, as they provide only one SD-WAN solution. [124] How this strategy is going to play out, we are yet to observe.

5.5.1 Technology comparison

The technology comparison between SD-WAN and DMVPN is going to continue in the same manner as we discussed SD-WAN vs. MPLS VPN. The most important advantages of both technologies will be defined and discussed in this part of the section.

SD-WAN advantages

- Cloud-ready
- Low latency
- Scalability
- Improved QoS

As we discussed in section 5.3, the cloud-ready factor is an extremely important feature for enterprises which have adopted a cloud-centric approach for their IT infrastructure. Both DMVPN and MPLS VPN are incapable of providing this feature and therefore SD-WAN is the only solution capable of utilizing backbone WAN connectivity and cloud services in a combined, next-generation design. (section 5.2)

Because SD-WAN uses traffic optimization mechanisms, discussed in section 5.2, aimed at assuring minimum latency for corporate WAN communications, these mechanisms are able to provide a lower level of latency compared to DMVPN. This is an important benefit for enterprises that use

real-time applications, such as VoIP, which are very sensitive to the level of latency in the network infrastructure.

Once more, we are going to discuss the ability to scale. Both SD-WAN and DMVPN technologies are able to provide a scalable solution for the WAN. This is why we have placed the scalability advantage in each of them. As we have examined the principles of operation of DMVPN in chapter 4 and SD-WAN's in section 5.2, there is no question that both technologies are capable of scaling as much as necessary. This advantage places the two technologies as appropriate solutions for large enterprises, which need to maintain multinational or worldwide networks.

When discussing QoS, SD-WAN's application-oriented QoS strategy (section 5.2) offers superior performance, compared to DMVPN's per-tunnel QoS architecture, discussed in chapter 4. We do not need to discuss many technical details in order to come to this conclusion. It is based on the fact that DMVPN uses layer 3 policies in order to influence traffic prioritization, while SD-WAN goes all the way to layer 7. This fact allows for optimal QoS experience, as it provides the ability to segment and prioritize traffic down to every single application.

DMVPN advantages

- Lower cost
- Scalability

SD-WAN was offering the better cost, compared to MPLS VPN (section 5.3), but apparently that is not the case here. The DMVPN solution comes with a lower cost than SD-WAN, since it is included in most of Cisco routers and layer 3 switches. Of course, the lower pricing is related to the less amount of features that DMVPN provides. The DMVPN solution does not include any sort of traffic or cloud optimization, compared to SD-WAN. (section 5.2) But for enterprises that do not require such services and simply need a full-mesh VPN solution at an affordable price, DMVPN may be the right choice.

The scalability benefit we already discussed, while examining it in the previous SD-WAN advantages subsection.

5.5.2 Defining the type of the war

We are facing the same two options, as discussed in section 5.3, evolution or revolution. In order to define the type of standards war between SD-WAN and DMVPN, there is one question that we need to provided an answer to. (chapter 3) Are these two technologies compatible with each

other? The answer is no. It is either the one or the other. SD-WAN represents a new, next-generation approach to the WAN, which will either replace DMVPN or die trying. The definition of this war type is revolution.

5.5.3 Asset examination

Here we are going to start discussing the key assets from the standards wars theory, examined in chapter 3. We are again going to discuss the benefits of each standard throughout all of the specified assets.

Control over an Installed Base of Customers

Since SD-WAN is a new standard, pioneering in the WAN market (section 5.2), it does not have any installed base of customers to control yet. DMVPN, on the other hand, does. Its position as a renowned WAN solution, offered by the incumbent network vendor Cisco, places DMVPN on top of SD-WAN regarding this asset. Although, most of the major SD-WAN vendors are in control over a large base of customers, here we are examining the technology itself, rather than its manufacturer.

Intellectual Property Rights

In this case, as we have discussed in chapter 4 and section 5.2, both technologies are proprietary standards, the intellectual property of which is owned by corporations. This places both standards in a strong position regarding this asset. Both SD-WAN and DMVPN are able to take advantage of their individual patents and use them in their own advantage or in the other's disadvantage.

Ability to Innovate

As mentioned before, we are discussing two proprietary technologies and the ability to innovate is a plausible asset for both of them. Therefore, this becomes a challenge of which standard will introduce better and more desirable features. After our technology comparison in the beginning of this section, we are going to place this asset in favor of SD-WAN. Why? Because DMVPN (chapter 4), alike MPLS, is incapable of providing application related features, which is the most demanding place for innovation in the IT industry today. [1]

First-Mover Advantages

The situation regarding this asset is an interesting one. From historical perspective, DMVPN should have the first-mover advantage as it has been in the WAN market for a longer period of time. However, since we are discussing a revolution strategy (chapter 3) in this case and SD-WAN

is offering a completely new approach compared to DMVPN, it is to be considered as the first-mover.

Manufacturing Capabilities

DMVPN is in the same position as MPLS VPN regarding this asset. (section 5.3) Since it is a technology that is already implemented in most of Cisco's devices, through established and well-developed production cycle, it is expected to have optimized production costs. SD-WAN, on the other hand is in the beginning of this process. (section 5.2) SD-WAN vendors are yet to find the optimal manufacturing process and their position as pioneers in the market does not allow them to completely focus on that issue for the moment.

Strength in Complements

Since this is a revolution scenario, the two standards are incapable of complementing each other, as the core of revolution strategies is in the incompatibility of technologies, discussed in chapter 3. Therefore neither DMVPN or SD-WAN is focused on creating complementary products for the other rival.

Reputation and Brand Name

DMVPN is a well-known solution with established reputation and brand name. SD-WAN is lacking reputation for now, but it is a product that is being developed by most of the major network vendors. As we discussed in the beginning of this section, we are examining the case of Cisco vs. the rest of the network vendors when discussing DMVPN vs. SD-WAN. According to [125], Cisco was in control of half of the switching and routing market by the third quarter of 2017. So when we combine the reputation of DMVPN with half the market owned by its vendor to the lack of reputation of SD-WAN and the other half of the market, the result is in favor of DMVPN. But if we also consider the fact that DMVPN's vendor is also a part of the SD-WAN community (section 5.2), we can consider this asset as a tie.

5.5.4 Strategy examination

In this scenario, based on the type of the war and the asset examination, SD-WAN's strategy can be considered as a mix of the preemption and expectations management strategies. Being a revolutionary product, SD-WAN is capable of utilizing the preemption strategy (chapter 3) and getting an early lead in the software-driven WAN approach, before other similar solutions start to emerge in the market. And together with the expectations management strategy (section 5.3) that is already in play,

SD-WAN has a high chance of positioning itself as a leading WAN solution. Also, since all of the major network manufacturers, including Cisco - the only supporter of DMVPN, are offering SD-WAN solutions, there does not seem to be a strong adversary to this new standard. There is only one requirement that SD-WAN needs to manage, in order to reap the benefits of these two strategies - justify its expectations.

5.5.5 Outcome of the war

For analyzing the outcome of the battle between SD-WAN and DMVPN, we are going to discuss the already examined technology comparison and asset examination from this section. For the technology comparison, SD-WAN is clearly the standard with the better performance and features. This is due to the application-oriented approach that the SD-WAN solution is using. DMVPN's only major advantage is its cost. Regarding the asset examination we have a tie between these two standards. However, given the revolution strategy that SD-WAN is taking in this battle, it all depends on whether SD-WAN manages to justify its expectations. If a new software-driven WAN standard does not emerge, which is probably going to be the case, and SD-WAN proves its capabilities, it has the chance to not only replace DMVPN, but to secure a leading position on the WAN market for itself.

5.6 Conclusion

In this chapter we have introduced the concept of SD-WAN, some of its major vendors and its different deployment and service types. We have examined the SD-WAN architecture, together with an example of the operation of one of the leading vendor solutions - Viptela, where the general principles of abstraction in the SD-WAN architecture were shown. The ISPs perspective regarding SD-WAN was also discussed in order to show a holistic view on the market situation. We have conducted a comparison between SD-WAN and its three major rivals - MPLS VPN, IPsec and DMVPN. The examples included a technology comparison and application of the standards wars framework, introduced in chapter 3. The framework followed a structured approach by defining the type of the war and examining the necessary assets and strategies. Each comparison section ended with a probable outcome scenario, based on all of the aforementioned analysis methods.

Chapter 6

Discussion and Conclusion

6.1 Discussion

This thesis has examined the rapid evolution in the WAN market that was impelled by the emergence of SDN. SD-WAN was able to start a major transition in this market for the first time since MPLS was introduced in 1999. The three WAN technologies that served as a comparison to SD-WAN were chosen based on their prevalence in the field. The idea for the comparison was meant to provide full understanding on how this new technology is going to affect the WAN industry. After discussing the details behind WANs, the new software-defined approach and SD-WAN throughout this report, in this chapter we are going to discuss our findings and summarize the answers to the problem formulation. We are going to start from the sub-questions in our problem definition and later come to answering the major question of this thesis.

What are the benefits of the current WAN technologies?

The first sub-question that we are going to examine is about the benefits of the WAN technologies, discussed in chapter 4. After examining the benefits of MPLS VPN, IPsec and DMVPN in chapter 5, it is essential to summarize the most important benefits. The biggest advantage of MPLS VPN, without surprise, turned out to be its private channel reliability. This benefit is crucial for the transmission of real-time applications and makes MPLS VPN the preferred solution regarding traffic reliability. IPsec VPN's greatest advantage is its security, provided through the combination of encryption and authentication algorithms. The most important benefit of DMVPN turned out to be its cost. As SD-WAN was the more efficient choice regarding cost, compared to MPLS VPN, DMVPN is the technology that provides the lowest implementation and maintenance cost. We are not discussing IPsec here, which we examined only as a complementary product in this thesis.

What are the benefits of SD-WAN?

The second sub-question from the problem formulation is concerned with the advantages of the SD-WAN technology, discussed in chapter 5. The advantages of the SD-WAN technology, compared to the other WAN solutions were discussed in chapter 5 and here we are going to mention the three most important ones. The first benefit that no other solution is capable of providing is the cloud-ready factor. This advantage is expected to place SD-WAN as the preferred standard for cloud-centric enterprises. The second important benefit is SD-WAN's traffic optimization mechanisms, which lead to low levels of latency in the WAN. This advantage places SD-WAN as the second most reliable WAN solution after MPLS. Last, but not least, SD-WAN's security is an important factor for enterprises, which require their traffic to be protected at every point in the network.

Is there a chance for SD-WAN to become a major standard?

The third sub-question that we created to support the idea behind the research throughout this project is related to SD-WAN's position on the market. After discussing the three probable outcomes of SD-WAN's battles in chapter 5, here we are going to present the potential of SD-WAN to remain an integral part of the WAN market. Based on our research, SD-WAN is in possession of the necessary benefits in order to be a significant part of the WAN industry. It is capable of outperforming its rivals, which is the most important factor in the IT field. It is also capable of functioning together with its greatest competitor - MPLS VPN, which also strengthens its position on the market. It leverages the cutting-edge concept of SDN and it does not have any competitors in that regard yet. The aforementioned facts contribute to the formation of a simple, yet definitive answer to this question. Yes.

How the Software-Defined Wide-Area Networking technology compares to the current WAN solutions?

The main question that this thesis is designed to provide an answer to is concerned with the relation of the WAN technologies, examined in chapters 4 and 5. When looking into SD-WAN vs. MPLS VPN, these two technologies are most probably going to coexist on the WAN market. This is due to the evolution approach that SD-WAN is taking regarding MPLS and the effective manner in which the two standards complement each other. In the interesting SD-WAN vs. IPsec VPN case, we determined that IPsec is not a true rival in this race, since it is more of a complement to the other three technologies, rather than a main competitor. However, its complementary nature does not undermine its benefits. IPsec has proven its reputation over the years and deserves to be an integral part of the WAN. In the SD-WAN vs. DMVPN battle, we considered the internal strategy

of Cisco, DMVPN's only vendor which also provides a SD-WAN solution, and focused on the perspective - Cisco vs. the rest network manufacturers. Since this is a revolution approach and SD-WAN is offering better performance and features compared to DMVPN, everything depends on the outcome of the expectations management strategy. And since Cisco is investing a lot into its SD-WAN solution (the acquisition of Viptela, chapter 5), we can assume that the company is expecting SD-WAN to win this war. We should keep in mind that the choice between the different WAN standards depends also on the size and financial capabilities of potential customers.

6.2 Conclusion

In this project, the challenges that the current WAN technologies face today were introduced in chapter 1. These challenges are triggered by the current and forthcoming adoption of 5G, AI and IoT technologies and the drastic shift towards the cloud. An overview of the most reputable WAN technologies was presented in chapter 4. These are MPLS VPN, IPsec VPN and DMVPN. The probable successor for the WAN market was introduced in chapter 5. SD-WAN proved as a high potential standard, capable of staying long-term in the game, because of its critical advantages. The purpose of this thesis was to evaluate the feasibility of the SD-WAN technology through comparison with the current WAN standards, performed in chapter 5. The project has followed a methodological framework, introduced in chapter 2 and the performed comparison was conducted through the use of a theory, discussed in chapter 3. The summarized results of the research were presented in the beginning of this chapter.

This thesis is intended to contribute to the better understanding of the software-driven transition in the WAN segment. The analysis of SD-WAN, through the help of the standards wars theory is designed to clearly state the advantages of SD-WAN over its rivals. In this way, the SD-WAN technology is stripped off its complexity and presented in an understandable manner for the reader. This approach targets a broader audience, even though technical knowledge in the field of computer networking is required for the understanding of the investigated technologies. The report focuses on providing practical information on the subject, that can be used by networking professionals as a reference point in their exploration of SD-WAN. It can also assist IT managers in their choice regarding WAN services for their enterprise. The distinction between the enterprise's size and its IT architecture during the analysis was performed with this exact purpose. Incorporated with the main research problem, minor problems such as SD-WAN vendor discussion, service providers and deployment options were introduced specifically with practical intent. Some of these

minor problems, the vendor and service providers discussions present an excellent opportunity for future research topics and these will be elaborated in the next section.

Based on the research and analysis of this thesis, a generalization for the future of computer networking is possible. As it was discussed in the report, the adoption of the software-defined principles is not only going to affect the WAN. The efficiency of SDN is expected to invade the LAN segment as well. The concept of intent-based networks is focused on providing the same application-oriented networking approach to the internal network, as SD-WAN is for the WAN. Although an exact claim that SD-WAN and intent-based networking are going to represent the future of the network is not plausible, is is reasonable to believe that applications will. The old method of decentralized networking is slowly becoming history. The future will most certainly belong to application-driven, centralized network solutions, whether in the LAN or WAN. It is only a matter of time.

6.3 Future research recommendations

The discovered answers confirm our initial reasoning from chapter 1 that there is probably going to be a mix of SD-WAN and MPLS VPN services for the future, cloud-driven WAN. Also, we have examined how this will affect ISPs. (chapter 5) This differs from our initial reasoning in the introduction, where we stated that cloud providers are the likely successor to ISPs, regarding the provision of SD-WAN services. This, of course, remains a possibility when deploying the SD-WAN-as-a-Service solution, but for the managed SD-WAN option, the most probable type of enterprise that is going to offer this service is expected to be the MSP. Whether ISPs are going to strategically position themselves as MSPs or they are going to simply buy SD-WAN-as-a-Service from the big cloud vendors and resell it to their customers presents an opportunity for future research. Doing both is also a valid option. Another relevant research question that is worth asking is what will happen with the major network manufacturers if SD-WAN turns out as a leading standard? Maybe this will present another opportunity for applying the standards wars framework, but this time on the different flavors of SD-WAN, introduced by their respective vendors. A particularly interesting research recommendation that derives from the conclusion of this project is the alarming question "Will applications completely consume the network?".

Bibliography

[1] Marcus Oppitz and Peter Tomsu. *Inventing the Cloud Century*. Springer, 2018.

[2] Luc De Ghein. *MPLS Fundamentals*. Cisco Press, 2007.

[3] Dennis Fowler. *Virtual Private Networks — Making the Right Connection*. Morgan Kaufmann Publishers, 1999.

[4] IETF Trust. *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*. Accessed 2018-04-20. 2011. url: https://tools.ietf.org/html/rfc6071.

[5] The Internet Society. *Security Architecture for the Internet Protocol*. Accessed 2018-04-20. 2005. url: https://tools.ietf.org/html/rfc4301.

[6] Cisco Systems. *Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications Data Sheet*. Accessed 2018-04-20. 2017. url: https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html.

[7] Forbes. *SD-WAN: Entry Point For Software-Defined Everything*. Accessed 2018-04-19. 2017. url: https://www.forbes.com/sites/jasonbloomberg/2017/03/20/sd-wan-entry-point-for-software-defined-everything/#60983cd846ee.

[8] Equinix. *Global interconnection index*. Accessed 2018-04-19. 2017. url: https://www.equinix.com/resources/whitepapers/global-interconnection-index/.

[9] Networkworld. *Software-defined everything*. Accessed 2018-04-19. 2018. url: https://www.networkworld.com/article/3262993/software-defined-networking/software-defined-everything.html.

[10] Networkworld. *Why 2018 will be the year of the WAN*. Accessed 2018-04-20. 2017. url: https://www.networkworld.com/article/3237691/lan-wan/why-2018-will-be-the-year-of-the-wan.html.

[11] Networkworld. *City and Guilds Group deploys SD-WAN to improve Office 365 performance*. Accessed 2018-04-20. 2018. url: https://www.networkworld.com/article/3269049/sd-wan/city-guilds-group-deploys-sd-wan-to-improve-office-365-performance.html.

[12] Networkworld. *SD-Branch market expected to reach $3 billion by 2022*. Accessed 2018-04-20. 2018. url: https://www.networkworld.com/article/3266591/lan-wan/sd-branch-market-expected-to-reach-3-billion-by-2022.html.

[13] O.R. Krishnaswami and B.G. Satyaprasad. *Business Research Methods*. Himalaya Publishing House, 2010.

[14] Adrian Thornhill Mark Saunders Philip Lewis. *Research Methods for Business Students*. Pitman Publishing, 2009.

[15] Carl Shapiro and Hal R. Varian. *The Art of Standards Wars*. California Management Review, 1999.

[16] Dedehayir O. and Steinert M. "The hype cycle model: A review and future directions". In: *Technological Forecasting Social Change* (2016).

[17] Jackie Fenn and Mark Raskino. *Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time*. Harvard Business Press, 2008.

[18] Everett M. Rogers. *Diffusion of Innovations*. The Free Press, 1983.

[19] A. Dillon and M. Morris. "User acceptance of new information technology: theories and models". In: *In M. Williams (ed.) Annual Review of Information Science and Technology* (1996). url: https://www.ischool.utexas.edu/~adillon/BookChapters/User%20acceptance.htm.

[20] Stanford. *Review of Diffusion of Innovations, by Everett Rogers (1995)*. Accessed 2018-06-04. 2003. url: https://web.stanford.edu/class/symbsys205/Diffusion%20of%20Innovations.htm.

[21] National Institute of Standards and Technology. *FACTS: A Framework for Analysis, Comparison, and Testing of Standards*. Accessed 2018-06-04. 2013. url: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7935.pdf.

[22] National Research Council Staff. *Standards, Conformity Assessment, and Trade*. National Academies Press, 1995.

[23] Victor Stango. *The Economics of Standards Wars*. Review of Network Economics, 2004.

[24] Paul A. David. *Clio and the Economics of QWERTY*. The American Economic Review, 1985.

[25] Abtin Keshavarzian and Yashar Ganjali. *Cell Switching vs. Packet Switching*. Department of Electrical Engineering Stanford University, 2002.

[26] Harvard Business Review Scott Anthony. *How To Really Measure a Company's Innovation Prowess*. Accessed 2018-05-25. 2013. url: https://hbr.org/2013/03/how-to-really-measure-a-compan.

[27] www.study.com. *First-Mover: Advantages, Disadvantages Examples*. Accessed 2018-05-25. url: https://study.com/academy/lesson/first-mover-advantages-disadvantages-examples.html.

[28] Eirik Gaard Kristiansen Jay Pil Choi and Jae Nahm. *Vaporware*. International Economic Review, 2005.

[29] Bob Vachon and Rick Graziani. *Accessing the WAN*. Cisco Press, 2008.

[30] Jim Metzler, Ashton Metzler, and Associates. *Guide to WAN Architecture Design*. Webtorials, 2015.

[31] Cisco Systems. *Introduction to WAN Technologies*. Accessed 2018-04-19. 2012. url: http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies.

[32] Cisco Press. *WAN Concepts*. Accessed 2018-04-19. 2017. url: http://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5.

[33] Balvir Singh and Navneet Sharma. *Wide Area Network*. Laxmi Publications, 2008.

[34] SANS Institute. *Comparing BGP/MPLS and IPSec VPNs*. Accessed 2018-05-04. 2002. url: https://www.sans.org/reading-room/whitepapers/vpns/comparing-bgp-mpls-ipsec-vpns-756.

[35] Cisco Systems. *Introduction to Cisco MPLS VPN Technology*. Accessed 2018-04-19. 2007. url: https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/mpls/provisioning/guide/PGmpls1.html.

[36] SANS Institute. *What Is an MPLS VPN Anyway?* Accessed 2018-04-19. 2001. url: https://www.sans.org/reading-room/whitepapers/vpns/mpls-vpn-anyway-718.

[37] Juniper Networks. *MPLS Applications Feature Guide*. Juniper Networks, 2018.

[38] Huawei. *MPLS Overview*. Accessed 2018-04-19. url: http://support.huawei.com/enterprise/docinforeader!loadDocument1.action?contentId=DOC1000080855&partNo=10042#dc_fd_mpls_1009.

[39] Mallikarjun Tatipamula Eiji Oki Roberto Rojas-Cessa and Christian Vogt. *Advanced Internet Protocols, Services, and Applications*. John Wiley Sons, 2012.

[40] Thomas G. Robertazzi. *Introduction to Computer Networking*. Springer, 2017.

[41] The Internet Society. *Multiprotocol Label Switching Architecture*. Accessed 2018-04-19. 2001. url: https://tools.ietf.org/html/rfc3031.

[42] www.cidr report.org. *CIDR REPORT for 21 Apr 18*. Accessed 2018-04-21. 2018. url: https://www.cidr-report.org/as2.0/.

[43] Randy Zhang and Micah Bartell. *BGP Design and Implementation*. Cisco Press, 2004.

[44] SANS Institute. *Border Gateway Protocol - The Language of the Internet*. Accessed 2018-04-19. 2002. url: https://www.sans.org/reading-room/whitepapers/protocols/border-gateway-protocol-the-language-internet-379.

[45] Cisco Systems. *Introduction to Border Gateway Protocol (BGP)*. Accessed 2018-04-19. 2012. url: https://www.petri.com/introduction-border-gateway-protocol-bgp.

[46] www.bgp.potaroo.net. *BGP Routing Table Analysis Reports*. Accessed 2018-04-21. 2018. url: https://bgp.potaroo.net/.

[47] RIPE NCC. *Autonomous System (AS) Number Assignment Policies*. Accessed 2018-05-01. 2017. url: https://www.ripe.net/publications/docs/ripe-679.

[48] The Internet Society. *A Border Gateway Protocol 4 (BGP-4)*. Accessed 2018-05-01. 2006. url: https://tools.ietf.org/html/rfc4271.

[49] Network Working Group. *BGP Communities Attribute*. Accessed 2018-05-01. 1996. url: https://tools.ietf.org/html/rfc1997.

[50] Colin Bookham. *Versatile Routing and Services with BGP: Understanding and Implementing BGP in SR-OS*. John Wiley Sons, 2014.

[51] Cisco Press. *BGP Fundamentals*. Accessed 2018-05-02. 2018. url: http://www.ciscopress.com/articles/article.asp?p=2756480.

[52] The Internet Society. *BGP/MPLS IP Virtual Private Networks (VPNs)*. Accessed 2018-05-02. 2006. url: https://tools.ietf.org/html/rfc4364.

[53] Juniper Networks. *Layer 2 VPNs and VPLS Feature Guide for Routing Devices*. Juniper Networks, 2018.

[54] Cisco Systems. *MPLS: Layer 3 VPNs Configuration Guide*. Accessed 2018-04-19. 2018. url: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html?referring_site=RE&pos=2&page=https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/mpls/provisioning/guide/PGmpls1.html.

[55] Cisco Systems. *BGP-VPN Distinguisher Attribute*. Accessed 2018-04-19. url: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp-vpn-distinguisher-attribute.pdf.

[56] Cisco Systems. *How Virtual Private Networks Work*. Accessed 2018-04-19. 2008. url: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.

[57] Cisco Systems. *What Is a VPN? - Virtual Private Network*. Accessed 2018-04-19. url: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html.

[58] Cisco Systems. *Remote-Access VPNs: Business Productivity, Deployment, and Security Considerations*. Accessed 2018-04-19. 2006. url: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/prod_white_paper0900aecd804fb79a.html.

[59] Networkworld. *How IPSec Complements MPLS*. Accessed 2018-06-01. 2007. url: https://www.networkworld.com/article/2297191/lan-wan/chapter-6--how-ipsec-complements-mpls.html.

[60] www.vpnfaqs.com. *S-to-S IPsec VPN Tunnels*. Accessed 2018-05-09. url: https://www.vpnfaqs.com/s-s-ipsec-vpn-tunnels/.

[61] Cisco Press. *IPSec Overview Part Five: Security Associations*. Accessed 2018-05-07. 2002. url: http://www.ciscopress.com/articles/article.asp?p=25443.

[62] National Institute of Standards and Technology. *Guide to IPsec VPNs*. Accessed 2018-06-01. 2005. url: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-77.pdf.

[63] James S. Tiller. *A Technical Guide to IPSec Virtual Private Networks*. CRC Press, 2000.

[64] Cisco Press. *IPSec Overview Part Four: Internet Key Exchange (IKE)*. Accessed 2018-05-07. 2002. url: http://www.ciscopress.com/articles/article.asp?p=25474.

[65] André Perez. *Network Security*. Wiley, 2014.

[66] Juniper Networks. *VPN Feature Guide for Security Devices*. Juniper Networks, 2018.

[67] The Internet Society. *IP Encapsulating Security Payload (ESP)*. Accessed 2018-05-07. 2005. url: https://tools.ietf.org/html/rfc4303.

[68] The Internet Society. *IP Authentication Header*. Accessed 2018-05-07. 2005. url: https://tools.ietf.org/html/rfc4302.

[69] www.firewall.cx. *Understanding Cisco Dynamic Multipoint VPN - DMVPN, mGRE, NHRP*. Accessed 2018-05-08. url: http://www.firewall.cx/cisco-technical-knowledgebase/cisco-services-tech/896-cisco-dmvpn-intro.html.

[70] Cisco Systems. *Dynamic Multipoint VPN Configuration Guide*. Accessed 2018-05-09. 2017. url: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book.pdf.

[71] The Internet Society. *Generic Routing Encapsulation (GRE)*. Accessed 2018-05-08. 2000. url: https://tools.ietf.org/html/rfc2784.

[72] Cisco Systems. *Point-to-Point GRE over IPsec Design Guide*. Accessed 2018-05-09. 2006. url: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE.pdf.

[73] Stephen R. Smoot and Nam-Kee Tan. *Private Cloud Computing: Consolidation, Virtualization, and Service-Oriented Infrastructure*. Morgan Kaufmann Publishers, 2012.

[74] Pluralsight. *Introduction to Multipoint GRE and NHRP*. Accessed 2018-05-08. 2012. url: https://www.pluralsight.com/blog/it-ops/multipoint-gre-tunnel-introduction.

[75] Cisco Systems. *Per-Tunnel QoS for DMVPN*. Accessed 2018-06-03. 2018. url: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-per-tunnel-qos.html.

[76] The Internet Society. *NBMA Next Hop Resolution Protocol (NHRP)*. Accessed 2018-05-09. 1998. url: https://tools.ietf.org/html/rfc2332.

[77] Paul Göransson and Chuck Black. *Software Defined Networks: A Comprehensive Approach*. Morgan Kaufmann Publishers, 2014.

[78] www.sdxcentral.com. *What are SDN Northbound APIs?* Accessed 2018-05-12. url: https://www.sdxcentral.com/sdn/definitions/north-bound-interfaces-api/.

[79] www.sdxcentral.com. *What are SDN Southbound APIs?* Accessed 2018-05-12. url: https://www.sdxcentral.com/sdn/definitions/southbound-interface-api/.

[80] www.sdxcentral.com. *Who is the Open Networking Foundation (ONF)?* Accessed 2018-05-12. url: https://www.sdxcentral.com/sdn/definitions/who-is-open-networking-foundation-onf/.

[81] www.sdxcentral.com. *What are SDN Controllers?* Accessed 2018-05-12. url: https://www.sdxcentral.com/sdn/definitions/sdn-controllers/.

[82] Qi Hao Fei Hu and Ke Bao. "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation". In: *IEEE Communications Surveys Tutorials* (2014).

[83] Siamak Azodolmolky. *Software Defined Networking with OpenFlow*. Packt Publishing, 2013.

[84] Open Networking Foundation. *OpenFlow Switch Specification*. Accessed 2018-05-13. 2015. url: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.

[85] Zeus Kerravala. *A Software-Defined WAN Is a Business Imperative*. ZK Research, 2015.

[86] IDC. *SD-WAN: Enhancing the Traditional WAN for the Future*. Accessed 2018-05-26. 2017. url: https://www.business.att.com/content/whitepaper/enhancing-the-traditional-wan-white-paper.pdf.

[87] Silver Peak. *The Software-Defined WAN*. Accessed 2018-05-26. url: https://www.silver-peak.com/sites/default/files/infoctr/idg-sd-wan-whitepaper.pdf.

[88] Ralph Santitoro. *Understanding SD-WAN Managed Services*. MEF Forum, 2017.

[89] Metzler Associates Ashton. *The Need to Rethink the WAN*. Accessed 2018-05-28. url: http://www.velocloud.com/sd-wan-resources/white-papers/need-to-rethink-the-wan-jim-metzler.

[90] Networkworld. *Cisco grabs-up SD-WAN player Viptela for $610M*. Accessed 2018-05-27. 2017. url: https://www.networkworld.com/article/3193784/cisco-subnet/cisco-grabs-up-sd-wan-player-viptela-for-610m.html.

[91] Networkworld. *Cisco attacks SD-WAN with software from Viptela, Meraki acquisitions*. Accessed 2018-05-27. 2018. url: https://www.networkworld.com/article/3261549/lan-wan/cisco-attacks-sd-wan-with-software-from-viptela-meraki-acquisitions.html.

[92] Networkworld. *VMware jumps into SD-WAN with VeloCloud purchase*. Accessed 2018-05-27. 2017. url: https://www.networkworld.com/article/3235931/lan-wan/vmware-jumps-into-sd-wan-with-velocloud-purchase.html.

[93] Networkworld. *VMware and VeloCloud announce their networking and security strategy*. Accessed 2018-05-27. 2018. url: https://www.networkworld.com/article/3269769/lan-wan/vmware-and-velocloud-announce-their-networking-and-security-strategy.html.

[94] Networkworld. *Silver Peak enhances its SD-WAN edge device to improve the branch experience*. Accessed 2018-05-27. 2017. url: https://www.networkworld.com/article/3189952/lan-wan/silver-peak-enhances-its-sd-wan-edge-device-to-improve-the-branch-experience.html.

[95] Silver Peak. *Simplifying WAN Architecture*. Accessed 2018-05-27. 2018. url: https://www.silver-peak.com/use-cases/simplifying-wan-architecture.

[96] Steve Woo Sanjay Uppal and Dan Pitt. *Software-Defined WAN*. John Wiley Sons, 2015.

[97] Citrix. *NetScaler SD-WAN: Best Practices - Security*. Accessed 2018-05-27. 2017. url: https://docs.citrix.com/en-us/netscaler-sd-wan/9-2/security-best-practices.html.

[98] Cisco Systems. *The Viptela Secure Extensible Network (SEN) solution*. Accessed 2018-05-27. url: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-secure-network-data-sheet-cte-en.pdf.

[99] IETF Trust. *Datagram Transport Layer Security Version 1.2*. Accessed 2018-05-28. 2012. url: https://tools.ietf.org/html/rfc6347.

[100] Google Patents. *Overlay management protocol for secure routing based on an overlay network*. Accessed 2018-05-28. 2018. url: https://patents.google.com/patent/US9467478B1/en.

[101] Viptela. *Viptela Overlay Network Bringup*. Accessed 2018-05-28. 2018. url: https://docs.viptela.com/Product_Documentation/Getting_Started/Viptela_Overlay_Network_Bringup/01Bringup_Sequence_of_Events.

[102] Cisco Systems. *Cisco vEdge Routers Product data sheet*. Accessed 2018-05-28. 2018. url: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-vedge-routers-data-sheet-cte-en.pdf.

[103] Viptela. *Our Views On The Industry*. Accessed 2018-05-28. 2018. url: http://viptela.com/blog2/page/2/.

[104] Gartner. *Managed Service Provider (MSP)*. Accessed 2018-05-28. 2018. url: https://www.gartner.com/it-glossary/msp-management-service-provider.

[105] Radiant Insights. *MPLS IP VPN Services Market Size Worth USD 26.62 Billion By 2020*. Accessed 2018-05-28. 2015. url: https://globenewswire.com/news-release/2015/12/29/798362/0/en/MPLS-IP-VPN-Services-Market-Size-Worth-USD-26-62-Billion-By-2020-Radiant-Insights-Inc.html.

[106] Networkworld. *An essential guide to managed SD-WAN services*. Accessed 2018-05-28. 2018. url: https://www.networkworld.com/article/3250686/techology-business/an-essential-guide-to-managed-sd-wan-services.html.

[107] Gartner. *Toolkit: Calculate the Before-and-After SD-WAN Expenses*. Accessed 2018-05-29. 2018. url: https://www.gartner.com/doc/3863063/toolkit-calculate-beforeandafter-sdwan-expenses.

[108] VeloCloud. *SD-WAN: The Power to Declare Network Independence*. Accessed 2018-05-29. 2018. url: http://www.velocloud.com/sd-wan-resources/webinars/power-to-declare-network-independence.

[109] Networkworld. *SD-WAN deployment options: DIY vs. cloud managed*. Accessed 2018-05-29. 2018. url: https://www.networkworld.com/article/3243701/wide-area-networking/sd-wan-deployment-options-diy-vs-cloud-managed.html.

[110] Aryaka. *What is SDWAN and Which One is Right for Your Business?* Accessed 2018-05-29. 2018. url: https://www.aryaka.com/blog/what-is-sd-wan-which-one-right-for-your-business/.

[111] Citrix. *SD-WAN-as-a-Service: Delivering More Value to Our Service Provider Partners*. Accessed 2018-05-29. 2018. url: https://www.citrix.com/blogs/2018/02/21/sd-wan-as-a-service-delivering-more-value-to-our-service-provider-partners/.

[112] Matrix Networks. *SD-WAN Explained: The 3 Flavors of Software Defined WAN*. Accessed 2018-05-29. 2018. url: https://www.mtrx.com/blog/sd-wan-explained-the-3-flavors-of-software-defined-wan-what-is-sdwan.

[113] Networkworld. *The 3 types of SD-WAN architecture*. Accessed 2018-05-27. 2017. url: https://www.networkworld.com/article/3219653/sd-wan/the-3-types-of-sd-wan-architecture.html.

[114] SD-WAN experts. *Ultimate SD-WAN Guide*. Accessed 2018-05-29. 2018. url: https://www.sd-wan-experts.com/the-ultimate-sd-wan-guide/.

[115] Mushroom Networks. *What is the cost of MPLS?* Accessed 2018-05-31. 2018. url: https://www.mushroomnetworks.com/blog/what-is-the-cost-of-mpls/.

[116] Networkworld. *What is intent-based networking?* Accessed 2018-05-31. 2017. url: https://www.networkworld.com/article/3202699/lan-wan/what-is-intent-based-networking.html.

[117] Cisco Systems. *IPSec Overhead Calculator Tool*. Accessed 2018-05-31. 2018. url: https://cway.cisco.com/tools/ipsec-overhead-calc/.

[118] Networkworld. *SD-WAN Benefits: More Than Eliminating MPLS*. Accessed 2018-06-03. 2017. url: https://www.networkworld.com/article/3227417/sd-wan/sd-wan-benefits-more-than-eliminating-mpls.html.

[119] Networkworld. *MPLS, SD-WAN Not an Either/Or Scenario*. Accessed 2018-06-03. 2017. url: https://www.networkworld.com/article/3236492/techology-business/mpls-sd-wan-not-an-eitheror-scenario.html.

[120] Networkworld. *The pros and cons of IPSec*. Accessed 2018-06-03. 2004. url: https://www.networkworld.com/article/2326793/network-security/the-pros-and-cons-of-ipsec.html.

[121] Cisco Systems. *Cisco's IWAN (Intelligent WAN) for Your SD-WAN*. Accessed 2018-06-02. 2017. url: https://blogs.cisco.com/perspectives/ciscos-iwan-intelligent-wan-for-your-sd-wan.

[122] Cisco Systems. *PfRv3:Technology Overview*. Accessed 2018-06-03. 2015. url: http://docwiki.cisco.com/wiki/PfRv3:Technology_Overview.

[123] Cisco Systems. *Accelerating our vision with Viptela*. Accessed 2018-06-02. 2017. url: https://blogs.cisco.com/news/accelerating-our-vision.

[124] Networkworld. *Cisco's IWAN isn't dead*. Accessed 2018-06-02. 2017. url: https://www.networkworld.com/article/3220989/lan-wan/ciscos-iwan-isnt-dead.html.

[125] The Datacenter Journal. *Switching and Router Revenues Still Growing; Cisco Still Controls Half of the Market*. Accessed 2018-06-03. 2017. url: http://www.datacenterjournal.com/switching-cisco-still-controls-half-market/.