NETWORK DEVELOPMENT

Transition from Private IP (MPLS) towards Internet based solutions

Bachelor's thesis

Häme University of Applied Sciences

Information and Communication Technology

Spring 2018

Mika Lax

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka
Riihimäki

Tekijä Mika Lax **Vuosi** 2018

Työn nimi Tietoverkon kehittäminen, siirtyminen MPLS-verkoista Internet-pohjaisia ratkaisuja kohti

Työn ohjaaja/t Marko Grönfors

TIIVISTELMÄ

Tämän opinnäytetyön tilaajana toimi Konecranes. Opinnäytetyön tarkoitus oli kehittää Konecranesin tietoverkkoa uuteen suuntaan, jonka Internet-pohjaiset ratkaisut mahdollistavat. Samalla tarkoitus oli ratkaista tämänhetkisiä ongelmia, joita yksityisessä MPLS-verkossa on havaittu. Havainnoituja ongelmia olivat nopeasti kasvava Internet liikenne, liikenteen priorisointi, liikennekuorman tasaaminen sekä segmentointi. Opinnäytetyön päätavoitteena oli kerätä tietoa saavutettavissa olevista mahdollisuuksista, mitä Internet-pohjaiset ratkaisut voivat tarjota. Tässä opinnäytetyössä kuvaillaan Konecranesin tämän hetkisen verkon toimintaa, teknologioita ja mahdollisia uusia ratkaisuja. Tämä työ kattaa tietoa MPLS, SD-WAN, virtualisoinnista, pilvilaskennasta ja antaa yleiskuvan Konecranesin verkosta. Yksi päätavoitteista oli löytää ratkaisuja, jotka toisivat organisaatiolle kustannussäästöjä ja yksinkertaistavat olemassa olevaa verkkoa. Lisäksi tarkoitus oli lisätä verkon skaalautuvuutta ja joustavuutta. Opinnäytetyön lopputulos antaa hyvää tietoa Internet-pohjaisista ratkaisuista ja niiden mahdollisuuksista.

Kerättyjen tietojen perusteella Konecranesin olisi järkevintä säilyttää yksityiset MPLS yhteydet heidän kriittisimmissä sijainneissaan, kuten pääkonttoreilla, palvelinkeskuksilla ja tuotantoalueilla. Tämä takaa varman yhteyden, kaistanleveyden ja saatavuuden. Muut MPLS yhteydet olisi viisasta korvata SD-WAN ratkaisulla, joka luo kustannussäästöjä ja tekee verkosta entistä skaalautuvamman ja joustavamman. Tämä johtaa lopputulokseen, että tehokkain ratkaisu on hybridi tietoverkko, jossa voidaan hyödyntää MPLS sekä SD-WAN ratkaisun parhaita puolia.

Avainsanat Tietoverkon kehittäminen, MPLS, SD-WAN, Pilvilaskenta, Virtualisointi

Sivut 35 sivua, joista liitteitä 0 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communication Technology
Riihimäki

Author Mika Lax **Year** 2018

Subject Network development, transition from Private IP (MPLS) towards Internet based solutions

Supervisors Marko Grönfors

ABSTRACT

The commissioner of this thesis project was Konecranes. The purpose of this project was to develop the Konecranes network towards a new direction of Internet based solutions and to solve existing problems in the current Private IP (MPLS) based network. The currently identified problems include highly growing Internet traffic, traffic prioritization, offloading and segmentation. The main goal of this thesis project was to gather information on achievable opportunities which Internet based solutions could offer. This thesis describes Konecranes' current network operation, technologies and possible future solutions. This work covers information on MPLS, SD-WAN, virtualization, cloud computing and a high-level overview of the Konecranes network. One of the main objectives was to find solutions that would bring cost savings to the organization and simplify the existing network. Furthermore the intention was to introduce solutions that would make it more scalable and flexible. The outcome of this thesis gives a good knowledge of Internet based solutions and the opportunities.

Thereby the gathered information Konecranes should keep Private MPLS connections at their most critical locations such as the headquarters, data centers and production sites. This will ensure a secure connection, bandwidth and availability. It would be wise to replace the rest of the MPLS connections with a SD-WAN solution that will create cost savings and make the network more scalable and flexible. This will lead to a result where the most efficient solution is a hybrid network combining the best elements of the MPLS and SD-WAN solutions.

Keywords Network development, MPLS, SD-WAN, Cloud computing, Virtualization

Pages 35 pages including appendices 0 pages

TABLE OF CONTENTS

LIST OF ABBREVIATIONS USED

IaaS	Infrastructure as a Service
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switch Router
MPLS	Multiprotocol Label Switching
OMP	Overlay Management Protocol
PaaS	Platform as a Service
PIP	Private IP
ROI	Return on Investment
SaaS	Software as a Service
SD-WAN	Software-Defined networking in a Wide Area Network
SPCP	Service Provider’s Cloud Platform
VPN	Virtual Private Network
WAN	Wide Area Network

1 INTRODUCTION

This thesis was made for Konecranes which is the world's leading manufacturer of lifting equipment, and its customers include machinery and process industries, yards, ports and terminals. Konecranes is committed to providing lifting and maintenance services to all possible lifting needs, thus increasing the value and efficiency of its customers businesses.

Originally Konecranes was part of KONE Oy, so the history begins on year 1910 when Kone Oy was founded. Today KONE Oy is one of the most globally known elevator and escalator company industries. It was in year 1988 when KONE organized crane operations into the KONE Cranes Division of KONE Corporation. KCI Konecranes was formed on April 15, 1994, when KONE Corporation decided to sell all its other businesses except the elevator business before it was listed on Helsinki Stock Exchange. Only two years later KCI Konecranes was also listed on the Helsinki Stock Exchange. In 2006 KCI Konecranes created a new global brand strategy and identity which led to KCI Konecranes changing its name to only Konecranes. Also changing their mission statement to Lifting Businesses TM, was invented and it's still in use today. (Konecranes, 2018)

In 2017 Konecranes received orders for 3 007,4 million euros and the revenue was 3 136,4 million euros. Profit for the same year was 318,3 million euros and the result for the financial year 225,0 million euros. Konecranes growth has been mainly organic but it has also made major acquisitions. The latest major acquisition happened in 2017 when Konecranes bought Terex Corporation's MHPS (Material Handling & Port Solution) business. Now in 2018 Konecranes has 18,000 employees globally in 50 countries. Before this acquisition Konecranes had 11,000 employees and MHPS 7,000. This acquisition strengthened Konecranes position in global markets because MHPS had several operations in Central and Southern Europe, South America and South-East Asia. In turn Konecranes had focused operations in Northern Europe, North America and China. So, the companies supplemented each other in places where the other one had not focused their operations so widely. (Arvopaperi, 2018)

Now when the acquisition has happened and Konecranes has grown extensively there is need to develop their networks and reorganize the connections. The main object for this thesis is to develop Konecranes networks in the new direction of Internet based solutions and solve the existing problems in the current Private IP (MPLS) networks. Currently the main problem is highly growing Internet traffic and it will reflect straight to network connection costs because of the need of upgrading the connections to higher speeds to maintain the required quality in connections. Most common reason for this highly growing Internet traffic is that nowadays video conferencing and digital audio meetings or calls are quite common.

Konecranes is also using Office 365 which has a huge impact to the growing Internet traffic. Another major impact is that cloud services like Microsoft Azure are becoming more and more common in networking. Now the aim is to develop the company's network and to try finding Internet based solutions which can solve these problems.

2 MPLS

MPLS stands for Multiprotocol Label Switching. It is packet transmission method which is based on labels. With MPLS technique it is possible to transport data via predetermined route connections to destinations over the backbone network nodes without the need for nodes to do the complex routing. MPLS consist of multiple RFC-documents and standards.

2.1 History and development of MPLS technique

Development of the MPLS technique was started in the mid-1990s. Introduction was made by Cisco Systems and they called it “Tag Switching” because it was not restricted to ATM (Asynchronous Transfer Mode) transmission. They introduced it to IETF (Internet Engineering Task Force) and it was renamed to Label Switching. It was given to IETF for open standardization so it could be developed further to solve IP-protocols scalability problems when using ATM. In 1997 IETF founded a MPLS working group to create an interoperable multilayer switching standard. The goal of the group was to standardize the technologies for label switching and implement those methods to work with wide area network technologies SONET, Frame Relay, ATM and local area network technologies Ethernet, Token Ring etc. Originally, one of the goals was to remove a bottleneck of slow routers in the data transfer rate of ATM backbones. In practice, the purpose was to replace multiple ATM and IP routing operations with a simple data packet label based communication.

During the relatively long development of MPLS technology, information devices had also evolved as well as other network technologies, resulting in many original MPLS targets had lost their meaning. However, it was discovered during the development work, that MPLS offers more important advantages and opportunities than its original objectives. Originally MPLS was developed as a technology for network operators, it has now become more commonly used as a service offered by operators to private companies. Currently MPLS biggest benefits for companies are Layer 3 Virtual Private Network services and explicit routing. In explicit routing the route is predefined for a particular type of traffic or for a certain type of traffic service quality CoS (Class of Service) and improved QoS (Quality of Service). (Abogado, 2016)

2.2 Operation of MPLS

MPLS uses short path labels rather than long network addresses. It works by assigning labels to packets of information as they leave a network. Instead of looking up IP header information the network just reads the MPLS

label and whisks the packet along via a predetermined path. The clear advantage of the MPLS routing is that the path across the network is established before the packet starts moving. That is the reason why it is the perfect solution for prioritizing the delivery of specific types of data. The benefits of the MPLS are network scalability, security (data path protection), packet transfer rate, CoS (Class of Service), reliability and redundancy. MPLS doesn't care what underlying protocol is used. It could be Ethernet or ATM etc. It simply maps onto layer 2 protocol and provides a common fast efficient transport method over PSN (Packet Switched Network). In 7 layer OSI model MPLS works between Layer 2 and Layer 3 and is often called "Layer 2.5 protocol". Figure 1 on below shows 7 Layer OSI-Model with 2.5 MPLS Layer. (Lakshman & Lobo, 2006)

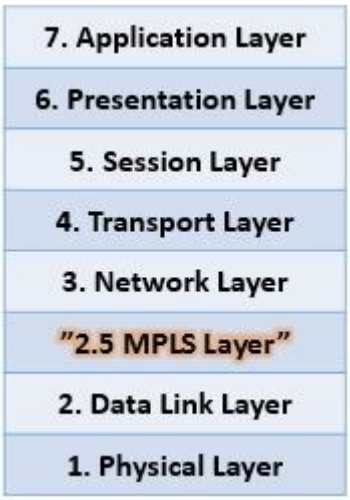


Figure 1. 7 Layer OSI-Model with "2.5 MPLS Layer"

The control and data planes are used to provide performance of MPLS. The control plane offers the intelligence within the network to let MPLS function. The data plane takes care of forwarding packets based on labels from one interface to another. RIB (IP Routing Information Base) and LIB (Label Information Base) are located in control plane. Routing tables and label binding to prefixes are built and stored in control plane but no forwarding decisions are made there. In turn FIB (IP Forwarding Information Base) and LFIB (Label Forwarding Information Base) are located in data plane and the control plane is used to create those. The forwarding decisions and lookups are done in data plane by FIB and LFIB. Figure 2 on below shows the functions of control and data planes. (Lakshman & Lobo, 2006)

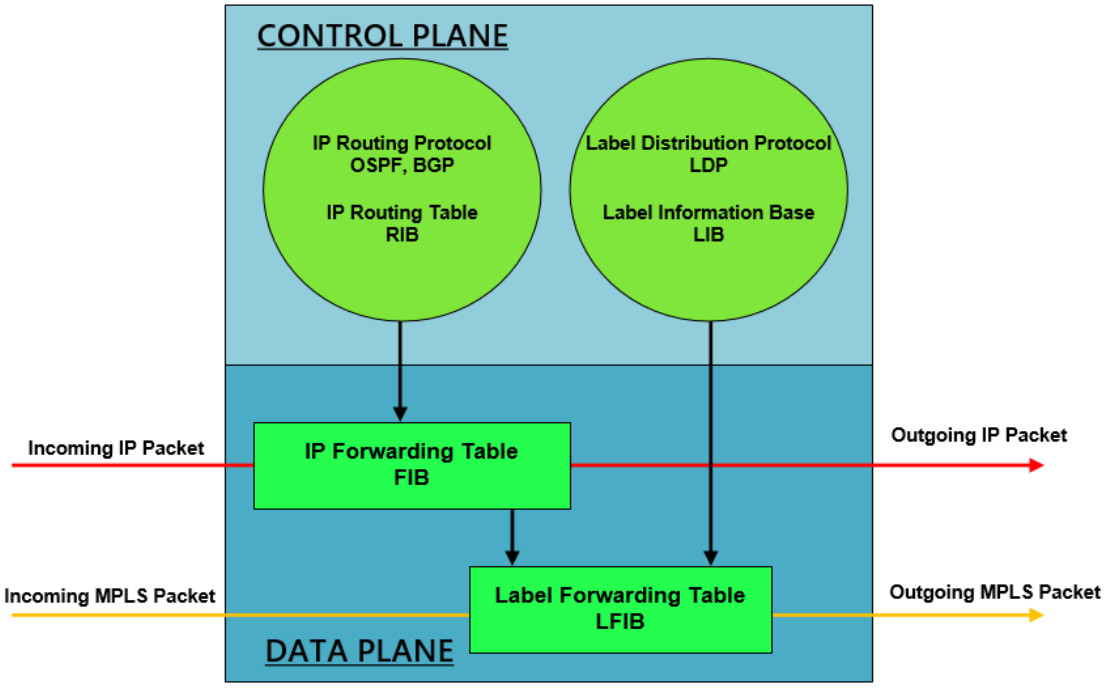


Figure 2. Function of control and data planes

MPLS network contains LSRs (Label Switch Router) and LERs (Label Edge Router). LSRs are basically any routers in the MPLS network which can process MPLS labels. LSR's main function is to receive the incoming packet and forward it out of the correct port as fast as possible. LSRs are located in the middle of the MPLS network and are connected to other LSRs but can be connected to LER as well.

LERs are located in the edge of the MPLS network and are connected to LSRs and CE (Customer Edge Router) or sometimes called CPE (Customer-Premises Equipment). LERs form one-way telecommunication paths LSPs (Label Switched Path) for MPLS network between ingress and egress devices. One-way means that the path is uni-directional and the return path can be a different LSP. LSPs are established by LDP (Label Distribution Protocol) or RSVP-TE (Resource Reservation Protocol – Traffic Engineering). The most important function of LERs is that they receive the packet from a CPE at IP network and check the layer 3 IP header info of the packet and mark it with the correct corresponding label number and then forward it to MPLS network to the LSR.

The IP header info and label numbers are stored in FEC (Forwarding Equivalence Class) table which is a set of prefixes that are treated in the same way. FEC is a group of IP packets which are forwarded in the same manner. For example, the packet payload are sent over the path with the same priority and the same label. The label is located in the MPLS Header, also called a shim header, between the IP Header in Layer 3 and Data Link header in Layer 2. The MPLS header is 32 bits long. It contains 20 bits for Label field, 3 bits for TC (Traffic Class) field, 1 bit for S (Stack) field and 8

bits for TTL (Time To Live) field. Figure 3 on below shows MPLS network devices. (Lakshman & Lobo, 2006)

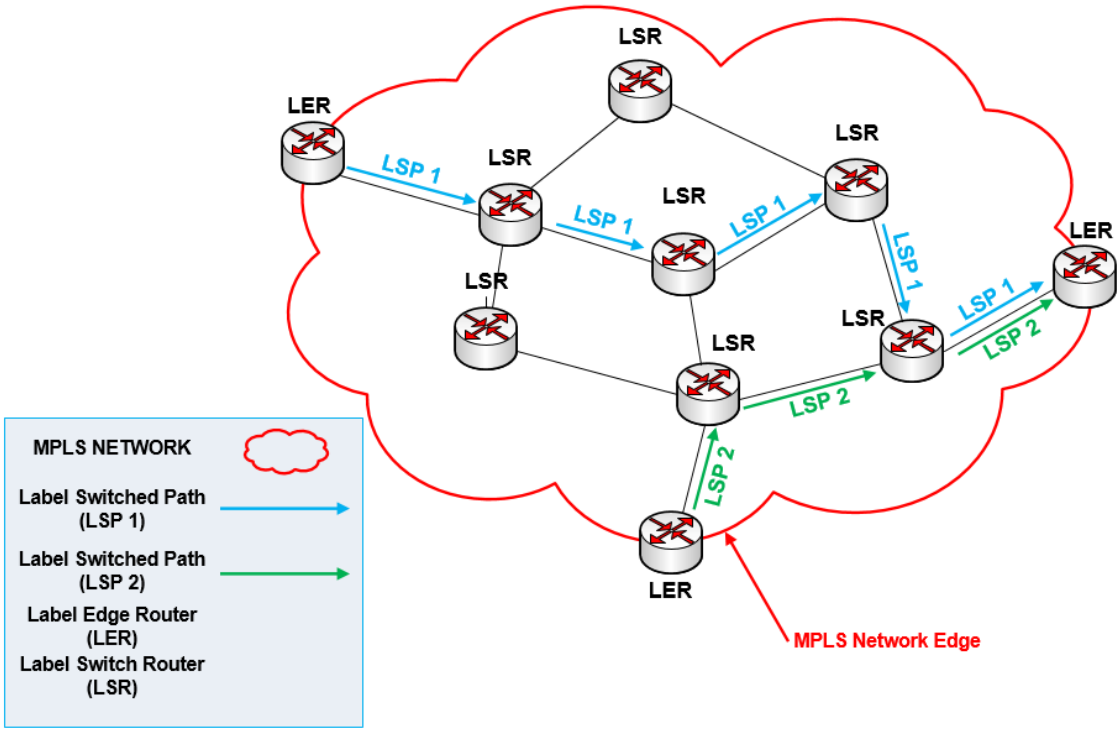


Figure 3. MPLS network devices

MPLS header consists of the following fields:

- **Label**, Label field is 20 bits long and is used for transmitting MPLS packets.

- **TC (Traffic Class)**, TC field was formerly called experimental (EXP) field, but it has been renamed to Traffic Class. It is 3 bits long and is used for QoS related functions.

- **S (Stack)**, It is possible to have multiple labels stacked on top of each other. The bottom of the label stack is called S field and is used to inform that the current label is the last in the stack when it's set.

- **TTL (Time To Live)**, TTL is 8 bits long and it functions basically the same as in IP TTL byte in the IP header. So, it will stop the packet going into an endless loop if the TTL value is decreased down to 0. When the value is 0 the packet is discarded. TTL value will always decrease by 1 when the packet moves from one router to another. Figure 4 on below shows MPLS header structure and location in Layer 2. (Juniper, 2018)

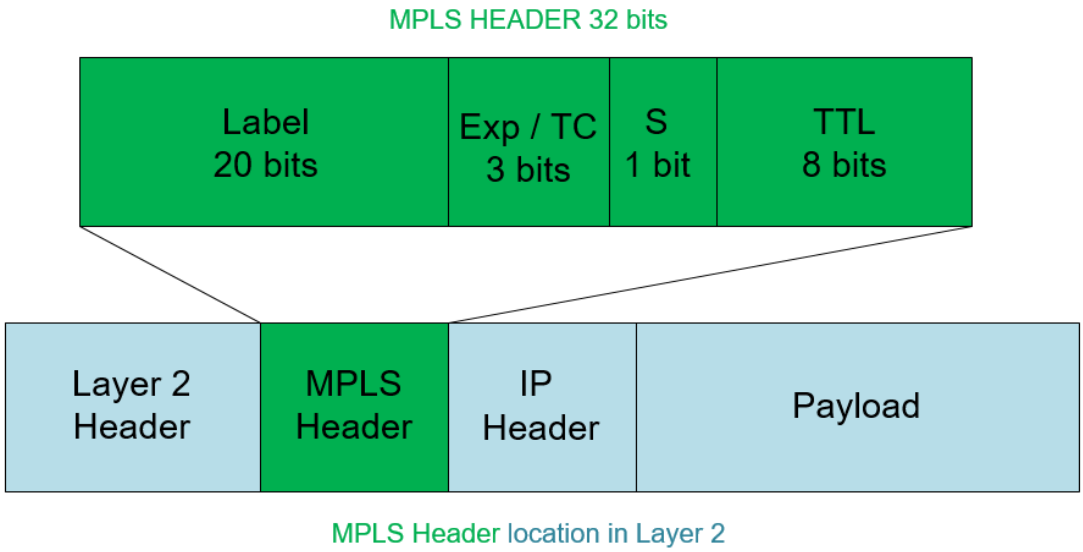


Figure 4. MPLS header structure and location in Layer 2

2.3 MPLS Label operations

In MPLS label operation there are 3 different functions which are important to know. They are called push, pop and swap. It also has operations called multiple push and swap and push. In a nutshell push means adding the label to a packet, swap means replacing the old label with a new one and pop means removing the existing label.

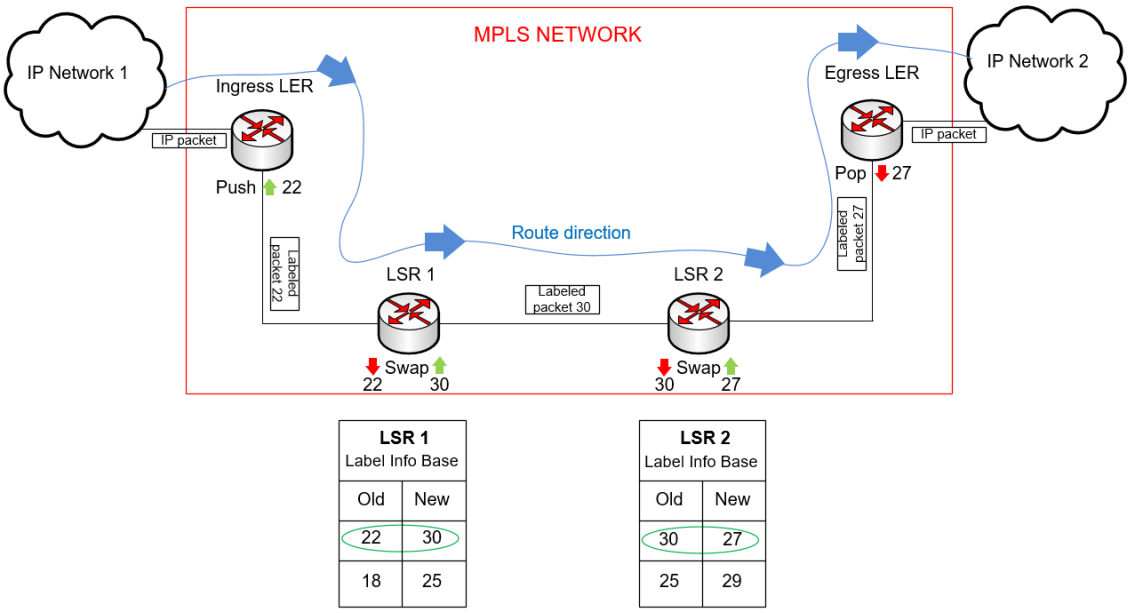
Push, is the first action when a packet is arriving from IP network to MPLS network. Ingress LER will be the first router which receives the packet and it adds a new MPLS label on it. First the LER will check the layer 3 information on the packet and after that it checks its lookup table and finds a reference FEC for that particular packet type. Then the label for that class is added or ***pushed*** on to the packet. The label is some number like 17 or 21 etc. Finally when the label is pushed on to the packet the LER will forward the packet into the MPLS network to the LSR.

Swap, When the LSR receives the packet from the LER there is already the label which the LER pushed on it. The LSR uses it's LIB (Label Info Base) to check the current label in it. When LSR finds the label from the LIB there is also information that will be the new label number for the corresponding old label number. After the LSR checks the pair of old and new label numbers from the LIB it removes or ***swaps*** the old number with new one. After this label swap the LSR will forward the packet to the next device of that LSP in the MPLS network which can be another LSR or egress LER.

Pop, Finally when the egress LER receives the packet at the edge of the MPLS network, it removes or ***pops*** the MPLS label from the packet. Then

the egress LER will forward the packet to the IP network according normal IP forwarding rules. (Juniper, 2018)

Figure 5 on below demonstrates the MPLS Label operations when data is sent from IP Network 1 to IP Network 2. The LSP (Label Switched Path) for this connection is Ingress LER -> LSR 1 -> LSR 2 -> Egress LER. First the Ingress LER receives the IP packet from IP network 1. Then it pushes the label on it with Label number 22 and after that it forwards the packet to LSR 1. Then LSR 1 receives the labeled IP packet and looks up the label on it. It finds that it is 22 and searches for the 22 label number from its LIB (Label Info Base) and finds that it needs to be swapped to label number 30. It swaps the label 22 to label 30 and forwards the packet to LSR 2. LSR 2 does the same thing as LSR 1. It uses its LIB to find the label information that it needs and swaps the label 30 to 27. Then it forwards the labeled packet with label 27 on it to the Egress LER. The Egress LER pops the label 27 off it and forwards the non labeled IP packet to IP Network 2 according to normal IP forwarding rules.



LSR 1
Label Info Base

Old	New
22	30
18	25

LSR 2
Label Info Base

Old	New
30	27
25	29

Figure 5. MPLS Label operations

2.4 Destination-based forwarding & explicit routing

PSNs (Packet Switched Networks) have been implemented on mesh topologies which means that there might be many different paths which can be used to reach the destination network. In the mesh, topology links form point-to-point connections over the network devices. The number of routers in the networks can change wildly and the paths can be different depending on the configurations and failure situations of the failed links. There are two different types of packet routing methods and they are called destination-based forwarding and explicit routing. (Sheldon, 2001)

2.4.1 Destination-based forwarding

Destination-based forwarding is usually used in more simple routing cases when one MPLS header is enough on the packet. For example, when transmitting public IP-traffic in a MPLS network which mostly relies on casual IP-Lookup for IP addresses. In destination-based forwarding the packet has a destination address and the forwarding is based on directions the packet receives as it proceeds on its path. Therefore, the path is not predefined but each router on the path looks at the address individually and makes the decision about how to forward the packet. Decisions are made until the packet has reached the destination and those decisions have been made on a hop-by-hop basis. (Sheldon, 2001)

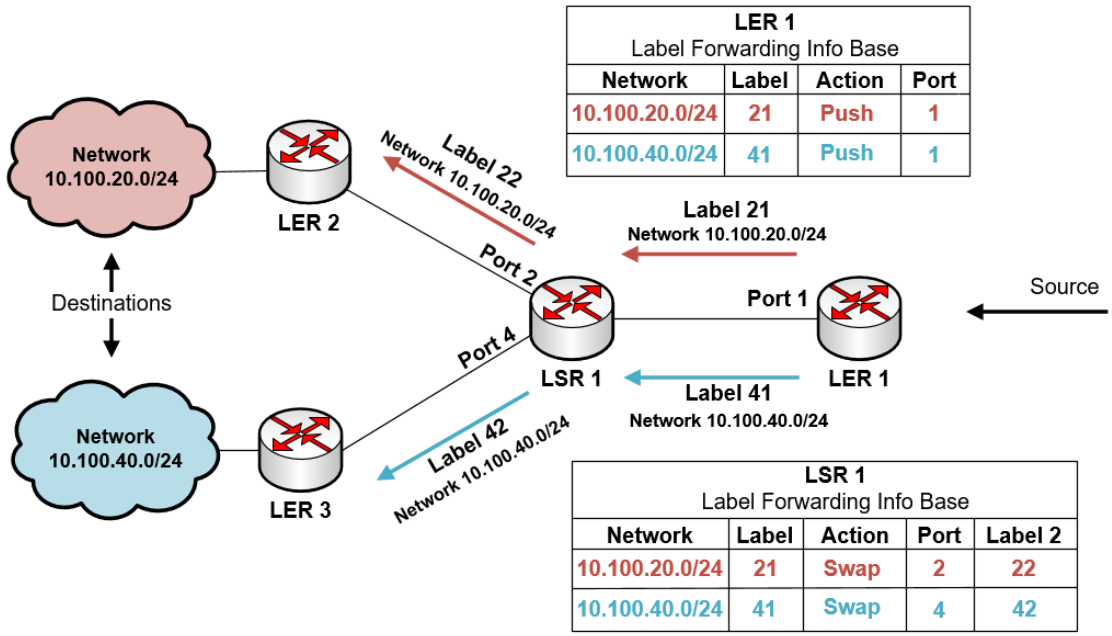


Figure 6. Destination-based forwarding

Figure 6 on above shows the example of destination-based forwarding. LER 2 is connected to network 10.100.20.0/24 and LER 3 is connected to network 10.100.40.0/24. In the MPLS network these routers will assign a label to each IP network and advertises them to their neighbors. LSR 1 and LER 1 have forwarding information in their LFIB table (Label Forwarding Info Base), therefore they know which interface / port they should use to get packets towards to the correct network destination. Firstly LER 1 receives an IP packet from some source, it examines the packet and performs the IP-Lookup action. Then LER 1 adds the label to it and notices the destination IP address 10.200.20.21 which matches the network prefix 10.100.20.0/24. From LFIB LER 1 resolves it should use Port 1 to send the packet out if it wants to reach network 10.100.20.0/24. So it forwards the packet towards LSR 1 via Port 1. After this LSR 1 receives the labeled packet and only pays attention what label is on it. It sees that the packet has been

labeled with label 21 and needs to be replaced by a new label with number 22. LSR 1 also knows that the destination network is 10.100.20.0/24 and the correct interface / port it should use is 2 to get the packet towards its destination. LSR 1 forwards the packet towards LER 2 using port 2 and label 22 as LER 2 has advertised to it. Then LER 2 receives the packet and pops off the label from it and forwards the packet to destination network 10.100.20.0/24 to reach the destination IP address 10.100.20.21.

2.4.2 Explicit routing

Explicit routing is based on networks that rely on switch routers or ATM switches. Explicit routing uses predefined paths which means that devices in the network have specific paths to specific destinations and they will use them to get the packet forwarded to its destination. Those paths are also known as a LSP's (Label Switched Paths) or virtual circuits. Because the paths are already known before sending the packet, devices only have to forward the packet towards its destination. This eliminates the routing process along the path since the route is predefined and known there is benefits, such as traffic engineering and QoS (Quality of Service). (Sheldon, 2001)

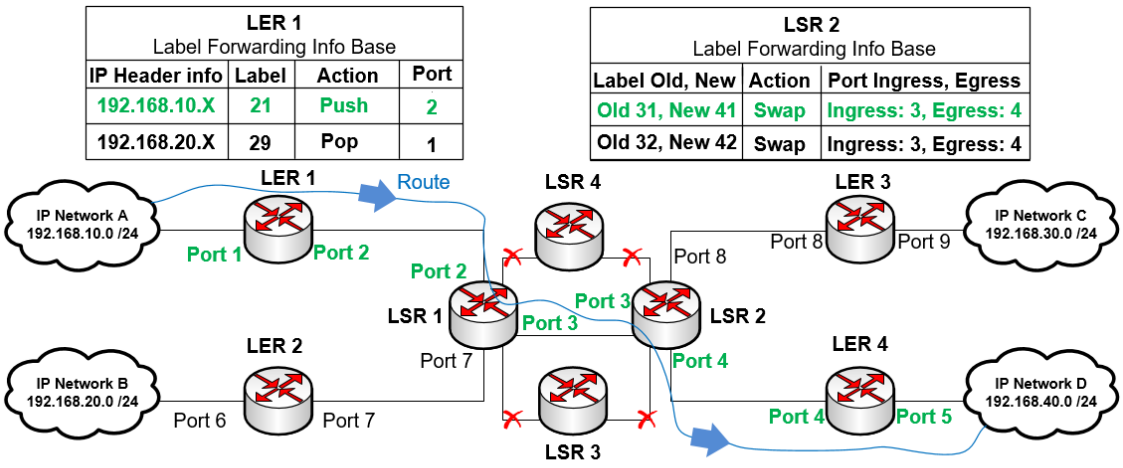


Figure 7. Explicit routing

Figure 7 on above shows the example of explicit routing. There is a predefined path from IP Network A to IP Network D. The LSP for this connection starts from LER 1 and goes to LSR 1 then to LSR 2 and finally to LER 4 which is connected to IP Network D. The routing information has been set up for each device and the forwarding information has been kept on each of their

LFIB (Label Forwarding Info Base) tables which also contains the information regarding which interface / port should be used to forward the data on correctly towards the destination. When LER 1 receives the packet from IP Network A to Port 1 it notices the IP Header Info of the packet and knows that it should push the label 21 on it and forward the packet to LSR 1 using interface port 2. LSR 1 examines the label, swaps it and forwards it to LSR 2 using the correct interface port 3. When LSR 2 receives the labeled packet, it knows it should swap the label and forward it to LER 4 via port 4. In the end LER 4 examines the packet pops the label away and forwards the packet to IP Network D. Because the path was predefined there is no chance that the packets would travel through LSR 4 or LSR 3.

2.5 **MPLS VPN**

MPLS VPN (Virtual Private Network) is a group of procedures which are used to create virtual private networks by using multiprotocol label switching. It uses a MPLS backbone to transport and route various types of network traffic. Nowadays there are three types of MPLS VPNs set up in the networks and they are Point-to-Point also known as Pseudowire, Layer 2 VPN (VPLS) and Layer 3 VPN (VPRN). There are different types of VPN protocols such as IPSec (Internet Protocol Security) which is used to secure Internet communication across an IP network, L2TP (Layer 2 tunneling protocol) is a tunneling protocol which is often combined with another VPN security protocol such as IPSec to create a highly secure VPN connection. L2TP creates a tunnel between two L2TP connection points and the IPSec protocol encrypts the data. Also, there are PPTP (Point to Point Tunneling Protocol), SSL (Secure Sockets Layer) and a few more. (Don, 2017)

2.5.1 Point-to-Point (Pseudowire)

Point-to-Point (P2P) MPLS VPNs uses Virtual Leased Lines (VLL) for supplying L2 P2P connectivity between two sites. Service providers offers VLL's to customers. Within these VLLs, Ethernet, TDM and ATM frames can be encapsulated. Typically, both sites uses their own internet connection for regular web traffic and the rest of the traffic will be routed through a VPN tunnel. (Don, 2017)

2.5.2 Layer 2 VPN (VPLS)

VPLS (Virtual Private LAN Service) is a Layer 2 multipoint VPN. With Layer 2 VPLS service providers can connect their customer Ethernet networks that are located all over the world to operate as one LAN (Local Area Network). From the client perspective, VPLS works as one big switch which connects their geographically distributed Ethernet networks to act as a

LAN. Briefly the service provider provides the backbone network and the customer uses it to connect their sites together. The service provider is responsible to take care of the backbone network which benefits the customer noticeably. This gives the customer a great asset as the complex configurations and backbone network are managed by the provider simplifying the customers responsibilities and reducing the level of knowledge the customer requires to manage their network. VPLS needs a full mesh topology to be used in its connections because it simulates a LAN. It can be done by using BGP (Border Gateway Protocol) or LDP (Label Distribution Protocol). These connections or tunnels are called pseudo wires and they are set up between all the provider edge devices which are being involved the VPLS process. VPLS provides operational cost benefits of Ethernet and QoS (Quality of Service) of MPLS. Figure 8 on below represents Layer 2 VPN. (Don, 2017)

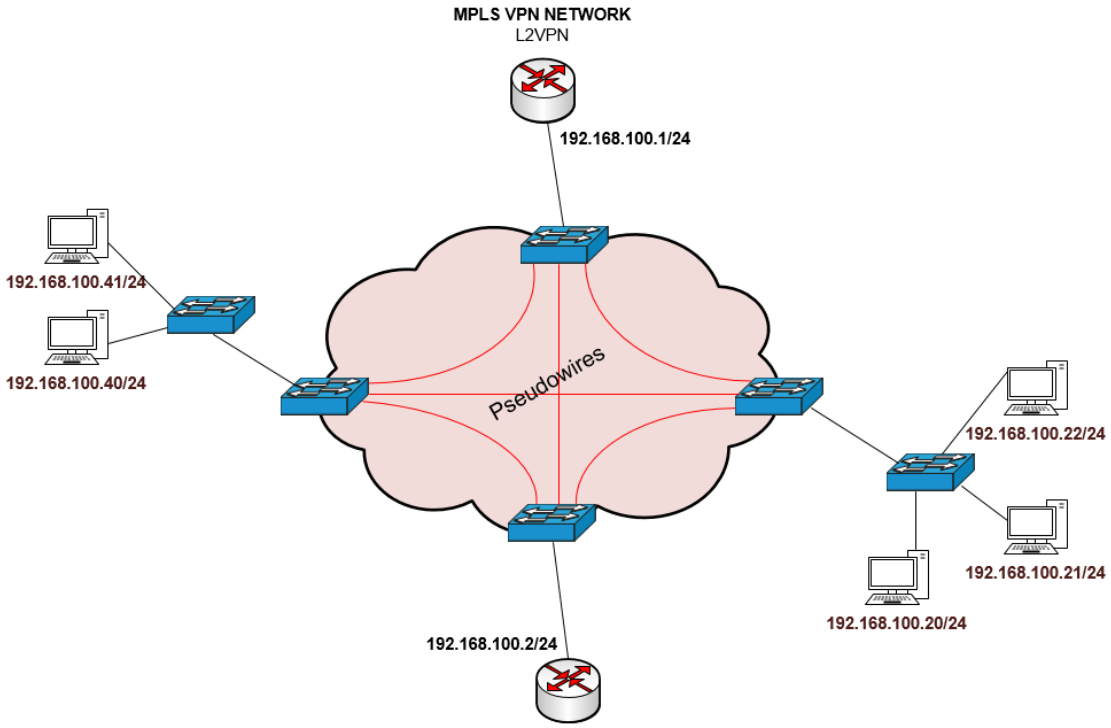


Figure 8. Layer 2 VPN (VPLS)

2.5.3 Layer 3 VPN (VPRN)

VPRN (Virtual Private Routed Network) is a Layer 3 VPN and it is also called MPLS L3VPN or L3VPN. It has grown to be one of the most commonly used network solutions. The main point of the L3VPN is that the service provider uses BGP and provides VPN routes to multiple different customers and limits VPN routing information sharing with VRF (Virtual Routing and Forwarding) technique to ISP edge routers. In L3VPN tunneling every tunnel endpoint is connected straight to the service provider's edge routers (PE) to

the backbone network. Using VRF allows PE's to handle multiple VPN connections and individual routing tables so it means that single PE can contain different routing tables for each customer. It restricts the visibility to each customer that example customer, for example A knows and sees only its own routing table and not customer B's routing information table. The fact is that the customers don't know that they are using the same PE. Because both customers A and B have their own individual routing tables it allows them to use same / overlapping network address ranges. VRF provides routing information for the same VPN connection hiding the information of internal networks and packets from the external units. The VRF-table is attached to each customer's connection interface and then when the particular interface is used the packets can be routed according to the correct VRF-table into its destination over the backbone network. (Don, 2017)

Figure 9 on below shows an example of MPLS L3VPN network. In this example there is 3 different companies and they all have their own CE routers (Customers Edge) and they all are connected into the same service provider PE router (Providers Edge). All companies have two sites and they can communicate to each other. However they doesn't know or see the others customers routers or routing information tables, only the service provider does. Company A only sees VRF table VPN A, and Company B sees VPN B and Company C sees the VPN C. Because every company has their own VRF tables they are allowed to use same or overlapping network address ranges. Company A's Site A1 CE is CE_A1 and it is connected to PE1 via IF0 interface where the VRF-table VPN A is attached to. Correspondingly VPN B Site B1 CE is CE_B1 and it is connected to PE1 via IF1. When CE_B1 a sends packet to PE1 via IF1 interface, PE1 then chooses VRF-table VPN B to be used because it uses IF1 interface. Accordingly, when CE_A1 sends the packet to PE1 via IF0, PE1 then chooses VRF-table VPN A to be used to forward the packet towards its destination which in this case is Company A's Site A2.

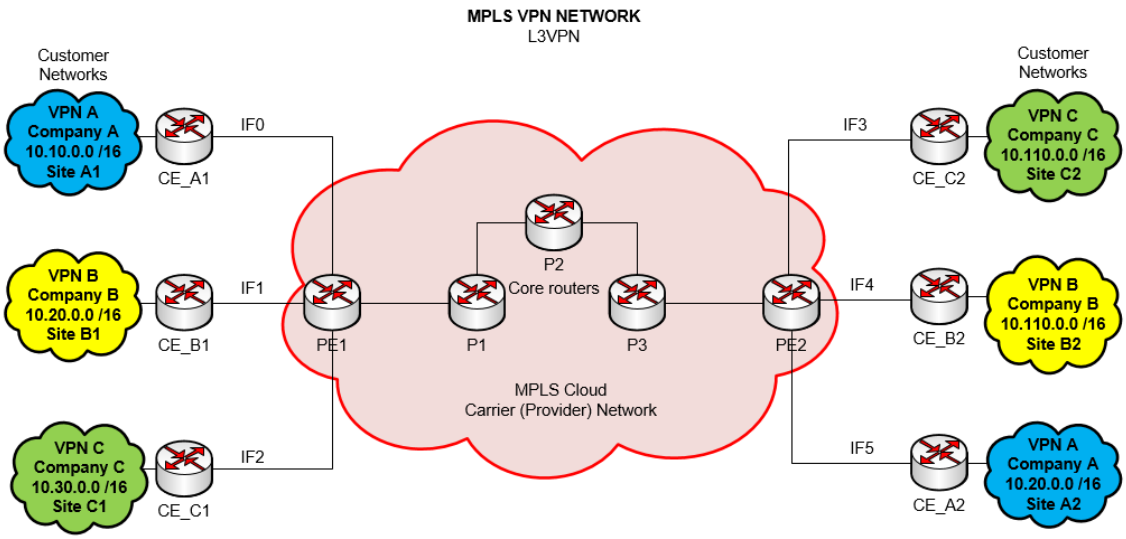


Figure 9. MPLS L3VPN network

There is another important thing related to VRF tables and L3VPN which is called RD (Route Distinguisher). The VRF tables are not enough to make sure that the traffic won't be routed into the wrong VPN group. VRF tables will prevent a conflict of using same or overlapping network address ranges but RD is required to limit the visibility of routing information. Service provider can use BGP to carry all VPN routes in their network but they need to use RD with it. Normally BGP can carry only single route to given network prefix but MPLS VPN demands that multiple companies can use their own address ranges whether they are the same or overlapping with other companies ranges. (Don, 2017)

RD works so that by adding RD to routing BGP will be forced to route multiple routes to one IP prefix. When a CE router is a sending packet to a PE router, the PE router will convert the IPv4 address prefix into VPN-IPv4 by adding the RD on it. BGP will allow this operation because it is capable to route multiple different types of prefixes. After the packet has travelled through the service provider's core network and it finally arrives to the egress PE router, it will remove the RD from the prefix. After removing the RD it will forward the packet to the CE router and this action will eliminate the need for the customer to know the VPN-IPv4 addresses, because the ingress PE adds the RD after the customer has sent the packet and the egress PE removes the RD before forwarding it to the egress CE. Therefore, the customer doesn't have to know anything about it because the service provider is taking care of transmitting packets in their own network. VPN-IPv4 address contains 12 bytes. The first 8 bytes contains RD and the last 4 bytes is the IPv4 address. RD is always unique because it makes the IP-addresses unique. It is 8 bytes long and consist of 3 different fields. (IETF, 2006)

RD's fields:

- Type (length 2 bytes)

- Administrator (length 2 or 4 bytes)

- Assigned Number (length 2 or 4 bytes)

Type field determinates the length of Administrator field and Assigned Number field. Also it defines the purpose of the Administrator field. Administrator field identifies the owner for assigned number. Assigned number field contains the numeric value which has been assigned from generally reliable source. The generally reliable source is IANA (Internet Assigned Numbers Authority) which can provide ASNs (Autonomous System Number) to service providers. For example, the RD can consist of an Administrator field which contains ASN which IANA has provided to service provider and a 4 bytes long Assigned Number field which contains the number assigned by the service provider. Every service provider manages their own

numbering area assignments of RDs preventing conflicts with other service providers. (IETF, 2006)

Figure 10 on below shows an example of AS Route Distinguisher. There are 3 different companies and they all are customers of same service provider. The service provider has assigned AS numbers for each company. Company A's AS number is 65010, Company B's is 65020 and Company C's is 65030. Service provider PE1 router has unique RD's for each customer. Company A's VPN A Site A1 RD is 65010:01, Company B's VPN B Site B1 RD is 65020:01 and Company C's VPN C Site C1 RD is 65030:01. When PE1 gets a route from VPN A CE_A1 router it converts the IPv4 address into VPN-IPv4 which means that 10.10.0.0 IPv4 will be converted to 65010:01:10.10.0.0 VPN-IPv4 form. The same thing happens with CE_B1 and CE_C1 but they will use their own unique RD's. CE_B1 will be converted from 10.20.0.0 to 65020:01:10.20.0.0 and CE_C1 from 10.30.0.0 to 65030:01:10.30.0.0.

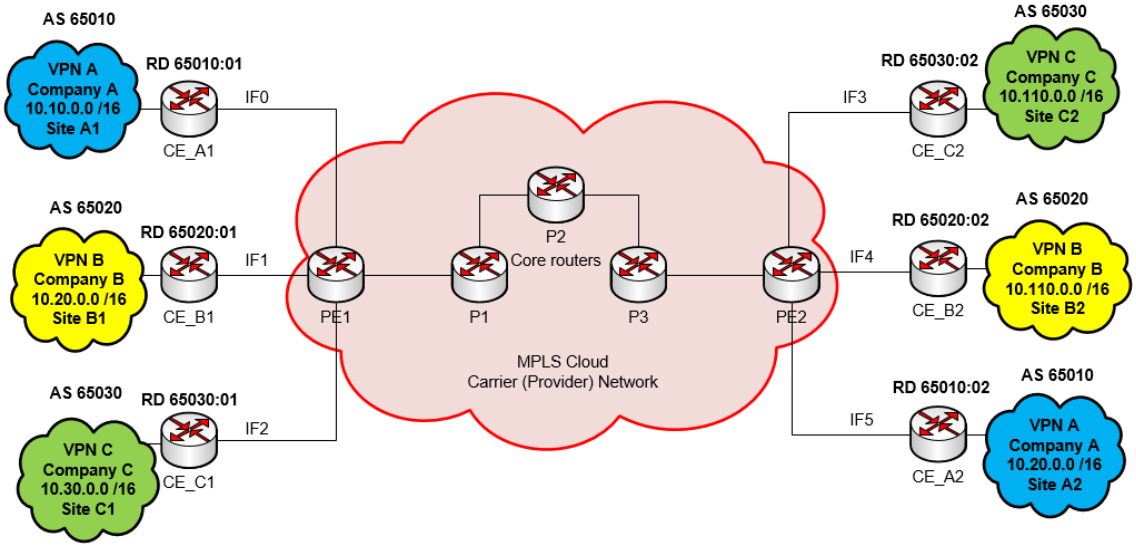


Figure 10. MPLS VPN AS Route Distinguisher

3 INTERNET BASED SOLUTIONS

SD-WAN means Software-Defined Networking in a Wide Area Network. It is quite a new thing and it is a hot topic of discussion at the moment. Lots of companies are currently considering or doing different kinds of pilot testing for SD-WAN solutions in their network to replace some traditional MPLS connections. SD-WAN's main purpose is to separate the control mechanism from its networking hardware leadings to simplified WAN management and operation. This approach is quite similar compared to SDN (Software Defined Networking) where virtualization is implemented to boost operation and management of data centers. (Butler, 2017)

3.1 **Cisco SD-WAN**

Cisco's SD-WAN solution is currently a very comprehensive product. One reason which lead to this is that Cisco acquired Viptela for 610 million dollars. SD-WAN uses software to make IT work smarter, faster and at lower cost. It will lead to the fact that long distance network building and management is more useful with SD-WAN than traditional MPLS. Because in SD-WAN parts of the control plane are centralized this leads to a simplified way to manage a network. Changes in the control plane can be grouped and managed for the whole WAN and business defined rules can be managed from a cloud-based centralized management portal. All rules and policies can be implemented and distributed easily across organization rather than using command lines for each device separately. With this simplicity, the advantage of broadband Internet connections can be utilized, instead of expensive Private IP MPLS connections. It simply lowers connections costs and increases the performance. Cisco SD-WAN provides agility, endpoint flexibility, responsiveness and cost-efficiency. It increases agility by simplifying network policy management, configuration and accelerates deployment times for new branches and applications. It also offers better performance by intelligently leveraging multiple paths including broadband connections. When these key features combine they lower IT operational costs. Cisco SD-WAN has integrated security and they have built a threat-centric security architecture which block attacks with a highly secure VPN overlay and strong encryption for end to end network protection. When running applications over internet connections the performance can be unpredictable so Cisco integrates real-time application monitoring and optimization using advanced analytics to continuously optimize the performance and user experience. Cisco SD-WAN is transport independent which means that branches can connect over any type of connection such as fiber, cable, MPLS, DSL and 4G LTE. It increases flexibility which also extends to endpoints for delivering support for physical or virtual environments, rich network services, WAN aggregation or cloud. This is intent-based networking for the WAN. Figure 11 on below shows an example of a 5-Year ROI (Return on Investment) for SD-WAN. With 100 traditional MPLS sites each having 10 Mbps bandwidth, a company can achieve up to a 76% cost reduction if it takes Cisco's SD-WAN in use. (Cisco, 2018)

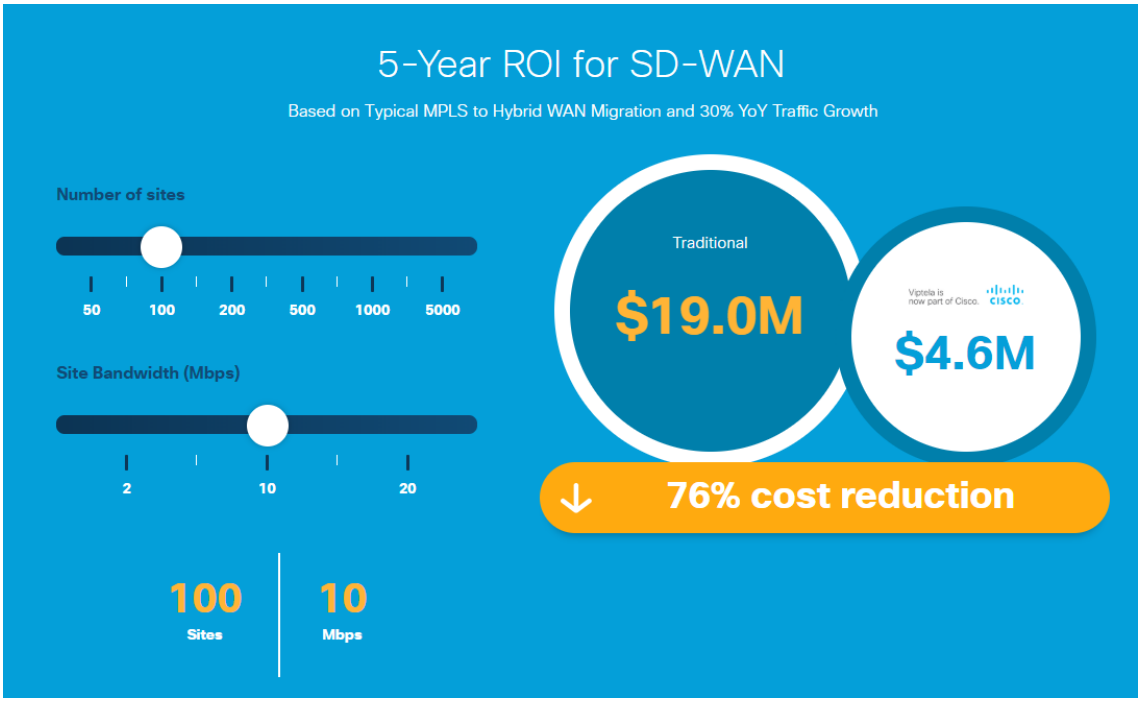


Figure 11. 5-Year ROI for SD-WAN (Cisco 2018).

3.2 **Cisco Viptela Fabric**

Companies are moving towards Internet based solutions and their network infrastructure is about to face radical changes. Cloud technologies are transforming the application world. Today applications tend to be located in the data center, IaaS (Infrastructure as a Service) or in SaaS (Software as a Service) cloud. In our modern world, people want that their enterprises can be accessed from anywhere in a consistent and secure manner. The real challenge of connectivity is adapting technology that is 20 years old (MPLS VPNs) to meet today's demands. Viptela is now part of Cisco. Viptela's focus is transforming old infrastructure to current generation fabric which overlays these underlying technologies of MPLS VPNs, Internet broadband and LTE, to provide users access to their applications in a secure way with the policies and securities defined by enterprise. Viptela's fabric contains 4 distinct layers; Data Plane, Control Plane, Management Plane and Orchestration Plane. The Data Plane is located in the customer's site or in the cloud and Control Plane is the brains of the connectivity for users and applications. The Management Plane permits users to run their policies and define their security framework. The Orchestration Plane also known as "Viptela's policy" allows them to spin up different instances of their infrastructure and allow customers to be able to integrate different services and capabilities. The Control Orchestration management plane is Viptela's host which locates in the cloud. It is divided from traditional network platform in such a way that the control plane resides in the cloud. As a result it is widely scalable and able to create an advanced architecture

for customers. Key benefits are application performance, cloud connectivity, security and scalability. Here are some great examples of the benefits Viptela fabric has brought to different enterprises.

1. **SD-WAN** has brought significant benefits to Agilent Technologies which is a large health care company. They were able to reduce the time taken to provision and deploy infrastructure by 80%. Application performance was increased five times better than previously which presents true benefits of hybrid WAN combined with cloud delivered architecture.

2. Cloud Connectivity is a really important factor in current day networking because lots of applications are moving towards the cloud from data centers. Kindred Healthcare performed a network transformation and applications migration to the cloud which improved their application experience by 4-10x on the top of the Viptela fabric. Also, Acadia Healthcare used the Viptela fabric as a key stepping-stone to enable migrating their applications to a SaaS cloud.

3. Network as a Service one great use case is enabling global service providers such as Verizon, Orange and AT&T to transform their managed services. NaaS enables them to move from connectivity providers to true experience providers.

4. Application Experience is one of Viptela's main focuses. First American Title Company is a good example of Viptela's fabric and how it was able to enable the company to deliver notably higher quality for their enterprise application suite securely. Everything from voice, video, SaaS applications, and other day to day applications. (Akkiraju, 2017)

3.3 **Virtualization**

Sometimes people may confuse virtualization and cloud computing as the same thing but they are not. They are close to each other and cloud computing always needs virtualization. Virtualization is a software which uses hardware and in turn cloud computing refers to a service that results from that usage. Virtualization software detaches compute environments from physical infrastructures. It allows various concurrent applications and operating systems to run on the same physical machine. It grant organizations cost-savings and increases existing computer hardware flexibility, utilization and efficiency. One major advantage of virtualization is server consolidation. Previously each server had their own tasks to operate and many times servers were underutilized which increased costs but with virtualization we are able to split a single server resources into multiple different usage purposes. Other benefits that can be achieved using virtualization are energy cost savings, faster deployment times, employee productivity, easier virtual machine recovery and reduced hardware costs. (Rivera, 2018)

3.4 **Cloud computing**

The Cloud computing model relies on shared computing resources of on-demand computing services like analytics, databases, networking, servers, software and storage over the cloud (Internet). All of these resources can be released and accessed with fast pace and minimum management effort or interaction with a service provider. The information is found in the cloud at all times and can be accessed from anywhere and whenever, that's why it's called cloud computing. The 5 essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. (Mell & Grance, 2011)

3.4.1 Service models

There are 3 different standard cloud computing service models which NIST (National Institute of Standards and Technology) has defined. They are called SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). They are usually presented as a stack of layers. However, these are able to work alone and they don't need each other to function. All of these models allow users to run applications and store data online. Each service model gives a different level of user flexibility and control. Figure 12 on below shows different service models. (Mell & Grance, 2011)

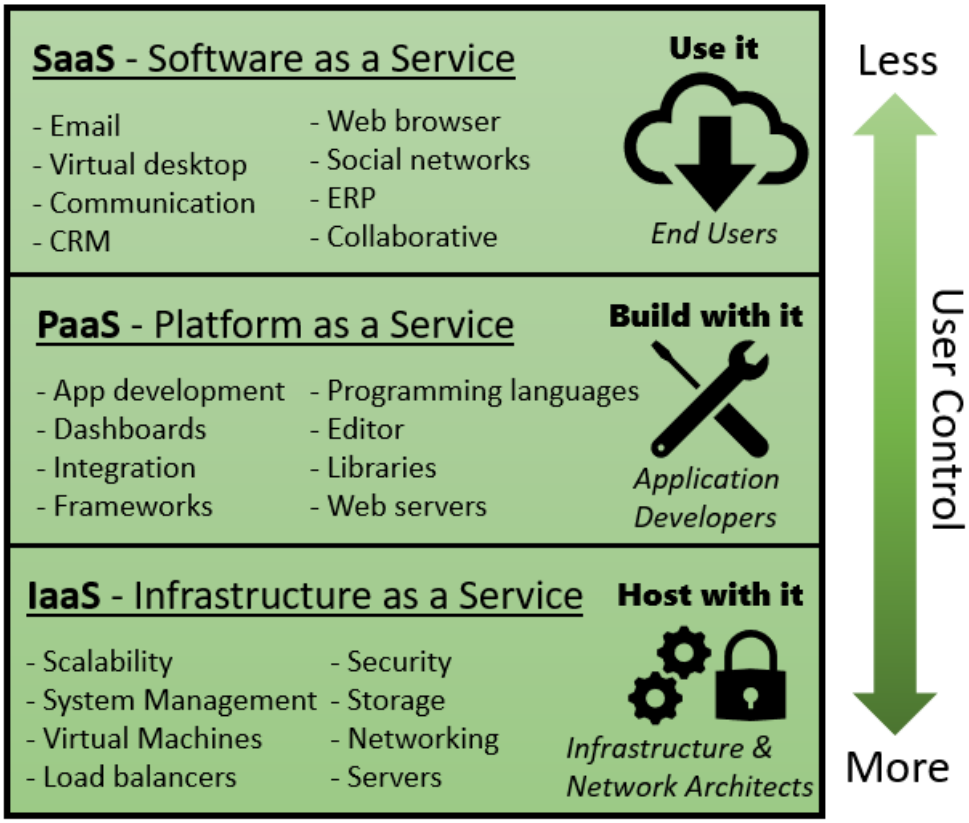


Figure 12. Service models

SaaS (Software as a Service) permits customers to run existing online applications on a cloud infrastructure. Access to these applications can be made from multiple different client devices like a web browser or a program interface. It is the service provider's responsibility to manage the underlying cloud infrastructure which includes operating systems, storage, servers and network. One well-known example of SaaS is Office 365. The biggest benefits that SaaS can provide are access flexibility, which means that applications are accessible from multiple different devices, and that it strengthens cooperation. SaaS applications can be free and some of them are paid via subscription.

PaaS (Platform as a Service) offers environment and tools for customers to enable them to create new online applications in the cloud infrastructure. In PaaS, the customers have control of their applications that they have created, and in some cases, configuration settings for the application-hosting environment. The service provider is responsible for taking care of the other parts of the underlying cloud infrastructure like servers, network etc. One great example of PaaS is the Google App Engine where anyone can make and maintain applications on Googles infrastructure. With PaaS customers are able to develop as many applications as they want with reasonable costs and deploy them on private or public cloud. My opinion is that those two factors are the best advantages of PaaS. The downside of the PaaS is that customers are limited to use the service provider programming languages and tools. Also, there might be a risk for the customers that

when they have created an application on one service provider platform they might not be able to move it to a different platform. All of these facts should be taken into consideration when customers are choosing a suitable service model and service provider for their needs.

IaaS (Infrastructure as a Service) allows customers to run and deploy applications including the operating systems on the service provider's cloud hardware. The main point is that the existing applications can be migrated into the service provider's IaaS cloud from company data centers to achieve cost savings. A good example of IaaS is AWS (Amazon Web Services) which provides on-demand cloud computing platforms. In IaaS the customers have control over operating systems, deployed applications and storage. Sometimes they can also have limited control of select networking components like host firewalls. The service provider is responsible for provision processing, networks and storage. Figure 13 on below shows customer and service provider responsibilities. (Mell & Grance, 2011)

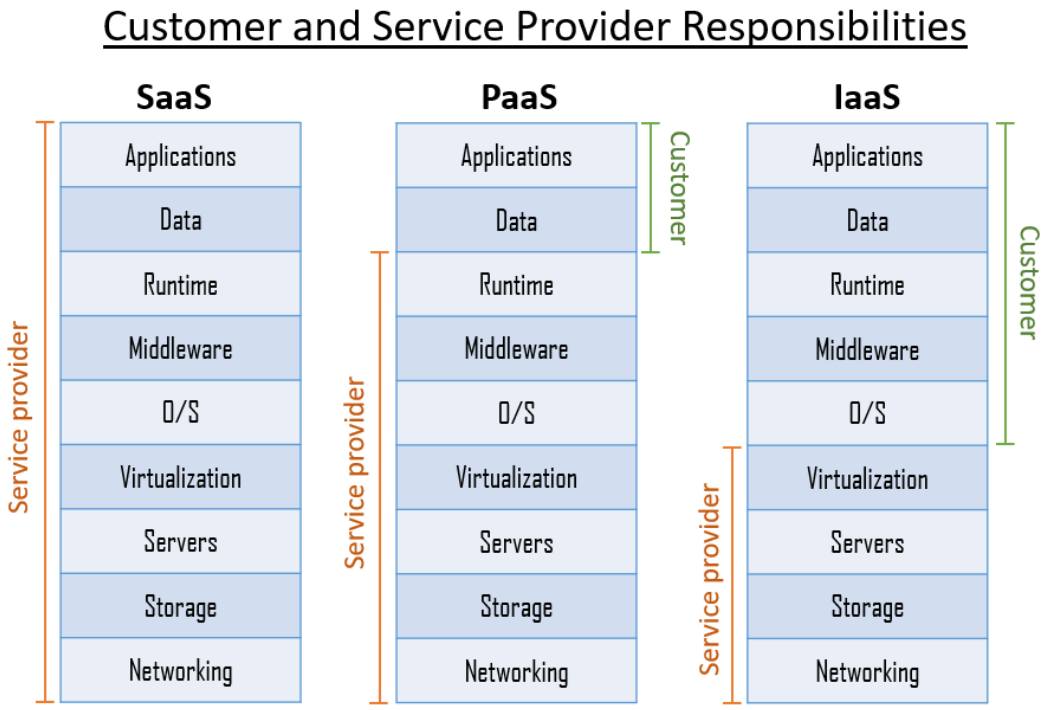


Figure 13. Customer and service provider responsibilities

3.4.2 Deployment models

There are four different deployment models which are called private cloud, community cloud, public cloud and hybrid cloud. Deployment models are determined and classified by the ownership of physical servers, virtualization software and the provider of the fault state support.

Private cloud infrastructure is private and the management and maintenance work are done by the organization, a third party, or some combination of the two. Private cloud can exist on or off premises. With private cloud infrastructure, an organization has the control to decide and perform hardware upgrades as they like. They can also verify physical security of the servers and can be absolutely confident that there are no other tenants on the service. The downside of the private cloud is that costs are higher than in public cloud and the responsibility is increased, as the organization itself is accountable for maintaining and building the services.

Community cloud infrastructure is the less known model. It is used by organizations which have shared concerns and it is for their exclusive use only. As an example, governmental organizations or research groups might have concerns related to security or policy. Community cloud is owned and managed by one or more of the organizations in the community, or a third party, or some mixture of them. It can exist on or off premises.

Public cloud deployment model is the most known cloud infrastructure deployment model. It is fully hosted on premises of the cloud service provider like Amazon and the provider is also responsible for providing the needed support. The owner can be academic, business or governmental organization or some mixture of them. They are maintained and managed by the owner. Some of the good things about public clouds are that they are highly accessible, scalable, and cost-effective. Also in fault state the cloud service provider is responsible for taking care of the problems, it allows the customer to rely on the service provider to provide the technical knowledge needed to maintain the platform allowing the customer to focus on the service and enabling it's benefits within the company or organization. The downsides of the Public cloud deployment model are that the customer is fully dependent on the provider and support costs might be considerably larger.

Hybrid cloud infrastructure is a model which combines two or more separate cloud infrastructures such as public, private or community that remain unique entities. These infrastructures are bound-together by standardized or proprietary technology which allows the portability of data and application such as load balancing between clouds. Popularity of the hybrid cloud is increasing and it might be the most popular cloud infrastructure model in future. It provides control and flexibility where it's required and enables the benefit of the public cloud model scalability and cost-efficiency. Figure 14 on below shows cloud deployment models. (Mell & Grance, 2011)

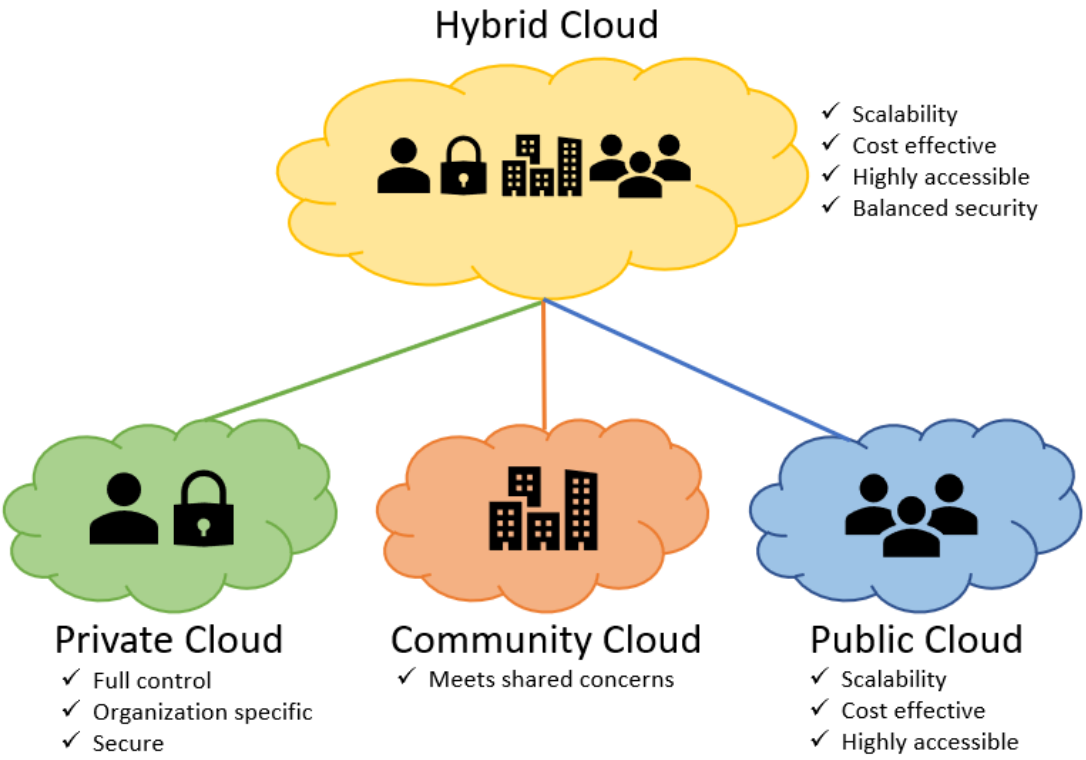


Figure 14. Cloud deployment models

3.4.3 Cloud computing services

Microsoft Azure has been established by Microsoft and is a very versatile cloud computing service. It is a public and private cloud platform. Azure has been created for building, deploying and managing services and applications through global network data centers which are managed by Microsoft. They have 54 global Azure regions which is more than any other service provider has currently. It provides SaaS, PaaS and IaaS service models and multiple programming languages and tools. Azure uses virtualization technology. Azure has hundreds of different services as AI + machine learning, analytics, compute, containers, databases, developer tools, DevOps, identity, integration, Internet of Things, management tools, media, migration, mobile, networking, security, storage and web. For example, it can be used as a platform for virtual servers or a development platform for developers. Because of Azure's wide-ranging services it is a great option for organizations to fulfill their business needs with cloud-based services. Organizations can achieve cost savings with Azure because they pay only for services they utilize. For example, if a user has a virtual machine that's usage is occasional then the user can turn off the machine when it's not needed and that will halt the costs. In turn, when the user needs it again they quickly start up the virtual machine and use it immediately with saved configurations and services. Figure 15 on below shows Microsoft Azure dashboard. (Microsoft, n.d.)

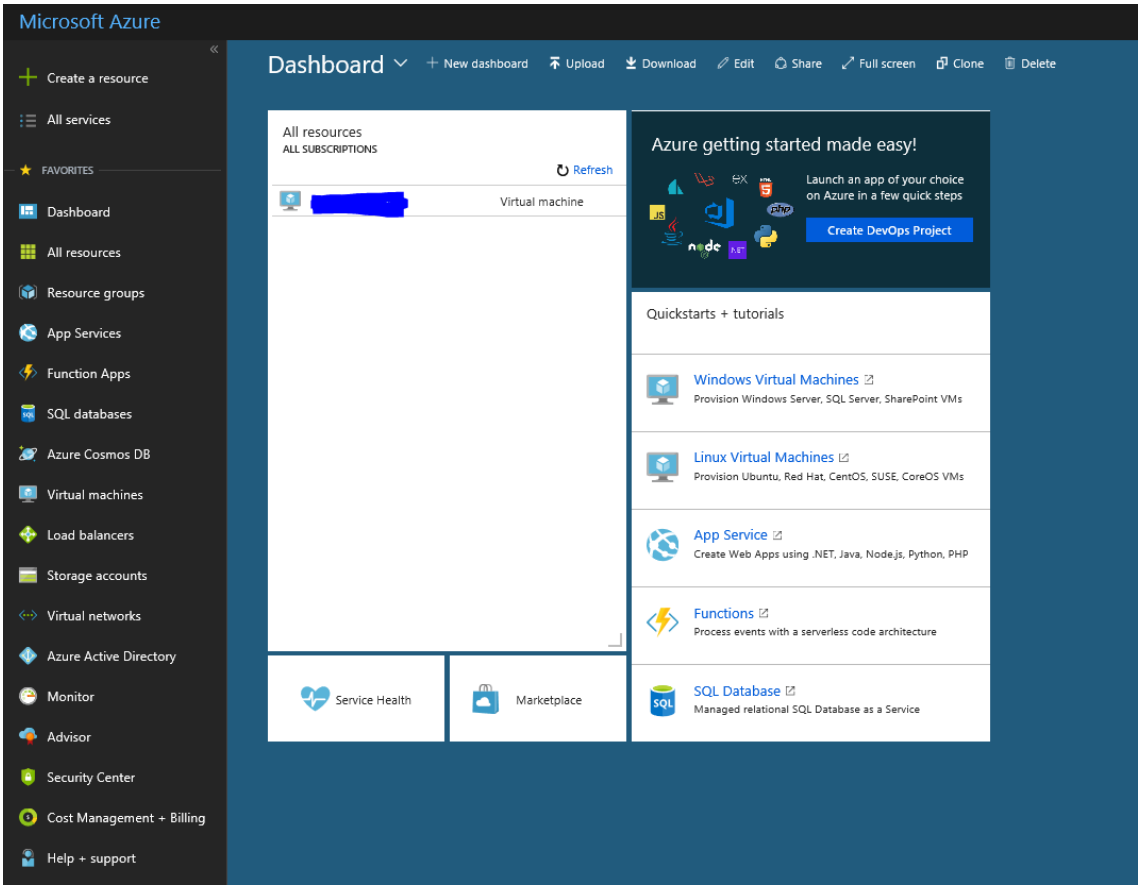


Figure 15. Microsoft Azure dashboard

Zscaler is an international cloud-based information security company which provides services such as anti-malware, application and browser vulnerability management, policy enforcement, bandwidth and QoS management, web-security, next generation firewalls, copyright and regulatory compliance in email, web and mobile computing. Zscaler security cloud allows companies to move their traditional network solutions towards the cloud based solutions in a secure manner. It provides a secure and easily deployed connection between applications and users no matter what kind of location, device or network is used. With Zscaler companies are able to simplify their network which leads to cost savings. Nowadays companies are able to move their applications from their local data centers to the cloud which leads to a situation allowings users to establish connections straight to the applications located in the cloud. Then the user connections are less resilient because the traffic is going straight to cloud and not through company's outbound gateway which have devices such as firewalls, URL filtering etc. that keeps company network safe. These kind of devices are not needed anymore because Zscaler has a full security stack as a service built inside their cloud platform. The great benefits of this type of security is that the security is brought close to the users and they are able to get a fast and secure experience regardless of location. The management of the security policies are easy to create, modify and push out in a user friendly interface. Figure 16 on below shows Office 365 traffic volume in Zscaler. (SC Media, 2013)

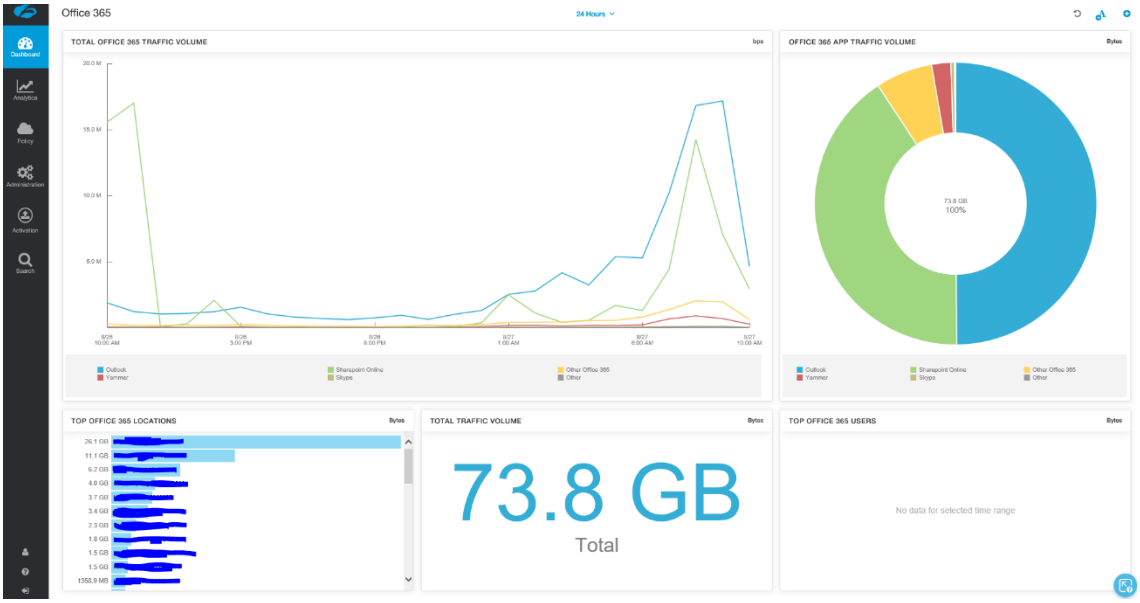


Figure 16. Zscaler displaying Office 365 traffic volume

Microsoft Office 365 provides cloud-based services and tools usually for business environments. The product works with subscriptions on a monthly or yearly basis. It contains the same familiar apps that traditional Microsoft Office provides except that it works in the cloud. Because Office 365 is license based, it supports 5 phone installs, 5 tablet installs, and 5 PC or MAC installs, a total of up to 15 installs per one user. Office 365 offers services on almost any device so people can access their Office apps across many different computing platforms such as Apple, Windows, Android, iOS etc. Microsoft Office 365 has lots of benefits compared to traditional Office. It provides a more flexible way to access office apps and helps employees to communicate and collaborate. It is also manageable, reliable, secure and always provides newest versions of apps unlike traditional office apps that can't be upgraded into the newest versions without buying a newer version of Microsoft Office. Microsoft has also added some new features to Office 365 such as Skype for Business, Yammer, and OneDrive. Skype and Yammer are used for communications, and OneDrive for the storing of files, it has space up to 1TB per user. Office 365 provides 4 core services to organizations which are: familiar Office apps, Skype for Business, SharePoint for document sharing and intranet website hosting, and finally Exchange which provides email features. Organizations can achieve great advantages through using Office 365 because it improves user productivity, simplifies IT, and services and settings are synchronized. User productivity is increased because they have latest tools for productivity and collaboration, the settings are synchronized across their different devices and they have automated updates. Figure 17 on below shows applications of Office 365 ProPlus version. (Kaelin, 2017)

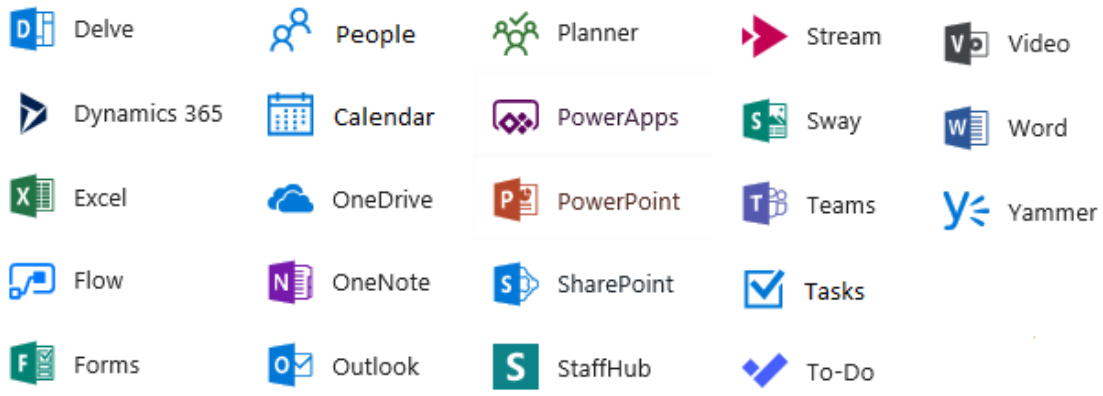


Figure 17. Microsoft Office 365 ProPlus version applications

Amazon Web Services also called AWS is a global cloud platform offerings multiple cloud computing services and products. It has a pay as you use based pricing model. AWS is suitable and fills specific needs for all sized businesses, it doesn't matter is it a big enterprise or a small start-up company. The two main products that AWS offers are EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service). EC2 is Amazon's virtual machine service where customers can get small or big machines depending their actual needs. S3 is Amazon's storage system where customer can store and share files. Amazon also offers many other services in addition to the previous ones such as VPC (Virtual Private Cloud), RDS (Relational Database Service), ELB (Elastic Load Balancing) and many others. With VPC, customers are able to create networks in the Amazon's cloud and run servers in those networks. RDS allows customers to create and manage databases. ELB provides load balancing of incoming traffic to multiple machines allowings customers to scale up their web applications regardless of the amount of users. AWS is very scalable and adaptable. Small companies can easily choose products that they need to start and keep their business running, and when they grow they can easily take more services in use. Big enterprises can use AWS, too, and they offer low-cost migration services to move their existing services to AWS. AWS is a secure and reliable solution for companies, and they have various data centers across the world to ensure data availability. Data centers are continuously monitored and their exact location information is kept in secrecy. Currently, they have data centers in 18 geographical regions, and 1 local region around the world. (Amazon, n.d.)

4 KONECRANES NETWORK

In this chapter we will take a high-level view of the Konecranes network. It will clarify the current state of the network and how it has been built. It will cover targets of the future network and my vision of the future network explaining what direction it could be developed.

4.1 **Current state**

Konecranes network is currently very large and worldwide. It is highly based on Private IP (PIP) MPLS connections. Now the plan is to develop the existing network towards Internet based solutions, to reduce network connection costs, and provide a solution for rapidly growing Internet traffic. Internet traffic has grown wildly and will continue growing because of different kinds of cloud services like Microsoft Office 365 and Microsoft Azure, also nowadays video conferences and audio meetings are common and they require reliable, high-speed network connections to work properly. Figure 18 on below shows the high-level Konecranes network diagram. As mentioned previously, the Konecranes network is based on PIP MPLS connections as can be seen in the figure. It consists of 3 different MPLS service providers that works as a backbone of the Konecranes network. Service Provider 1 is the biggest one which operates in EMEA (Europe, the Middle East and Africa) and AME (America) regions. Then there is also Service Provider 2 which operates in APAC (Asia Pacific) region and Service Provider 3 which takes care of some parts of EMEA Konecranes sites. These service providers have Peering Points which are connection points that connects their own managed network to each other and as a result they create one continous private network for Konecranes. At the moment, the Konecranes network has 3 Internet breakout points in EMEA, 1 in AME, and 1 in APAC, globally 5 breakout points in total. They are centralized Internet breakouts and these locations have been protected by firewalls, either one or a firewall cluster. The firewall cluster is a solution where 2 or more firewall nodes are working as a single logical entity to share the load of traffic processing and provide redundancy. It is transparent and guarantees the availability of network services to users. The major locations connections that are drawn in the figure are always fully redundant which ensures high availability because some services are always needed and full connection failure is not acceptable. Some cloud services like Microsoft Office 365, Zscaler, and AWS are in use as well, but in the future there will definitely be more of them because they are becoming more common and their benefits and use continues to increase. Internet traffic offloading has been implemented through Zscaler. The Konecranes network also includes a few VPN gateways and remote access points which are connected to wireless controllers.

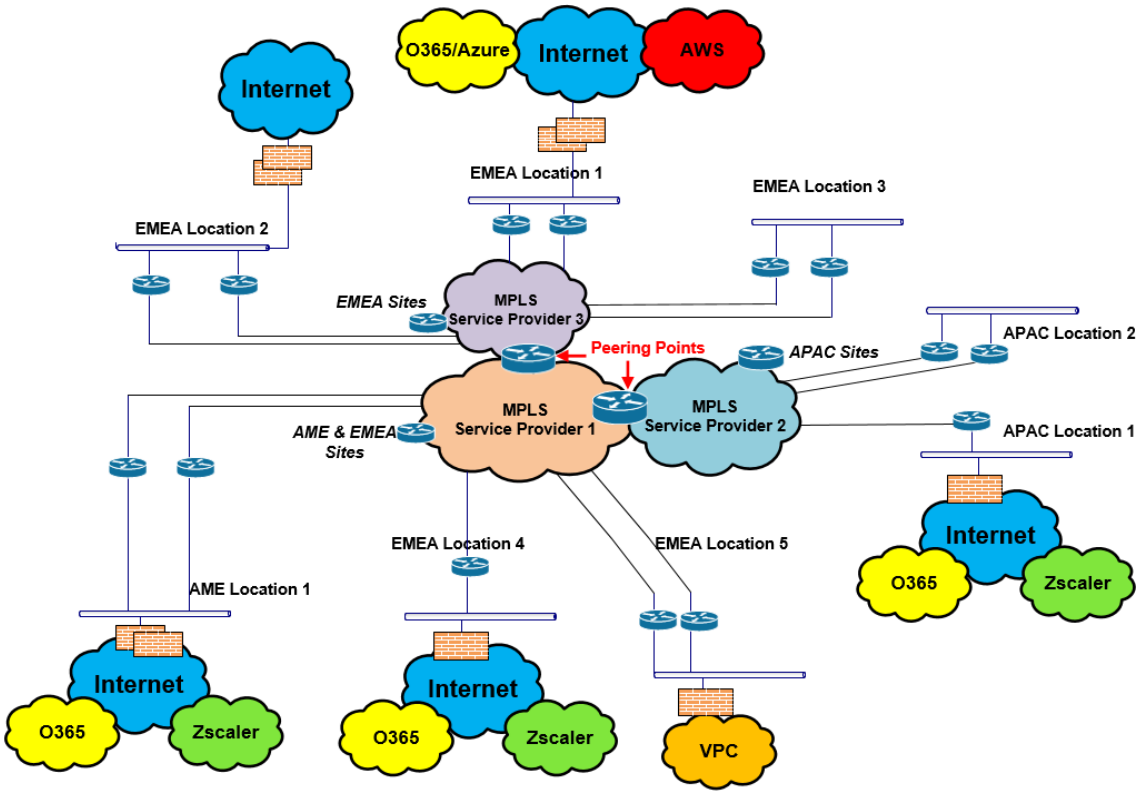


Figure 18. High-level overview of Konecranes network

4.2 Target and vision of the future network

The future network target is to develop a more agile network where Internet breakouts are more localized, and therefore closer to end users. With the increased amount of Internet breakouts, network design can be developed further and the new requirement called network segmentation or network security where the main point is to protect critical systems and data in data centers at the network level. The goal is to prevent malware and other harmful programs spreading from one site to another. From my point of view, the smartest direction where Konecranes network development should go is the hybrid solution. With the hybrid solution I mean that the future network should be built to support both MPLS and Internet based techniques such as SD-WAN in a way that Konecranes can take the best benefits from both of them. I favor a hybrid solution to be the best one because a full PIP MPLS network is expensive to upkeep but on the other hand it is very reliable and safe. In turn Internet based solutions like SD-WAN have faster deployment times and more cost-efficient than MPLS, but some risks exist when using Internet based solutions such as security and bandwidth usage. I prefer a solution where generally all the sites should use SD-WAN and it would be the main network technique in use but the largest and most important locations like production sites, distribution centers and headquarters connections should be ensured with high quality and availability at all times by MPLS connections.

Figure 19 on below shows an example of a high-level deployment of SD-WAN. In the figure there are different sized sites that are described as A,

B, C1, C2, C3 and D. The A and B sites are the largest ones such as headquarters, data centers and production sites. Their connections and devices are fully redundant and the difference between them is that A sites have fully redundant MPLS connections. There are two types of connections that are MPLS and IS (Internet Services). IS connections connected to DIAS (Dedicated Internet Access Services) that are provided by service provider where bandwidth quality is guaranteed. Then there are C1 sites that are also pretty important sites which have both MPLS and IS connections but they are not fully redundant. However C1 sites includes MPLS and IS connections, if one fails then services are automatically switched to use one of the available connections and that provides some redundancy. C2 and C3 sites are smaller sites than the previous ones and they do not require a MPLS connection. C2 sites have two IS connections but diversity is not guaranteed what makes them not fully redundant. C3 sites can manage without fully redundant IS connection. D sites can use traditional local Internet equipment and establish DMVPN connection to SPCP (Service Provider Cloud Platform). These D sites offer a cost benefit as the impact of an outage is small and the SD-WAN investment provides a poor ROI at small sites. Every site should have white box x86 network appliances or some other similar solution where SD-WAN can operate excluding smallest D sites. These appliances are managed by a SD-WAN controller or multiple controllers which simplifies deployment and maintenance of the devices. For example, access list rules or software updates can be easily distributed to all appliances in the network. Controllers can be located on-premises or they can be cloud hosted. It will lead to a network solution that is simplified, unified and cost-effective. SD-WAN traffic can cover both internal and external data traffic.

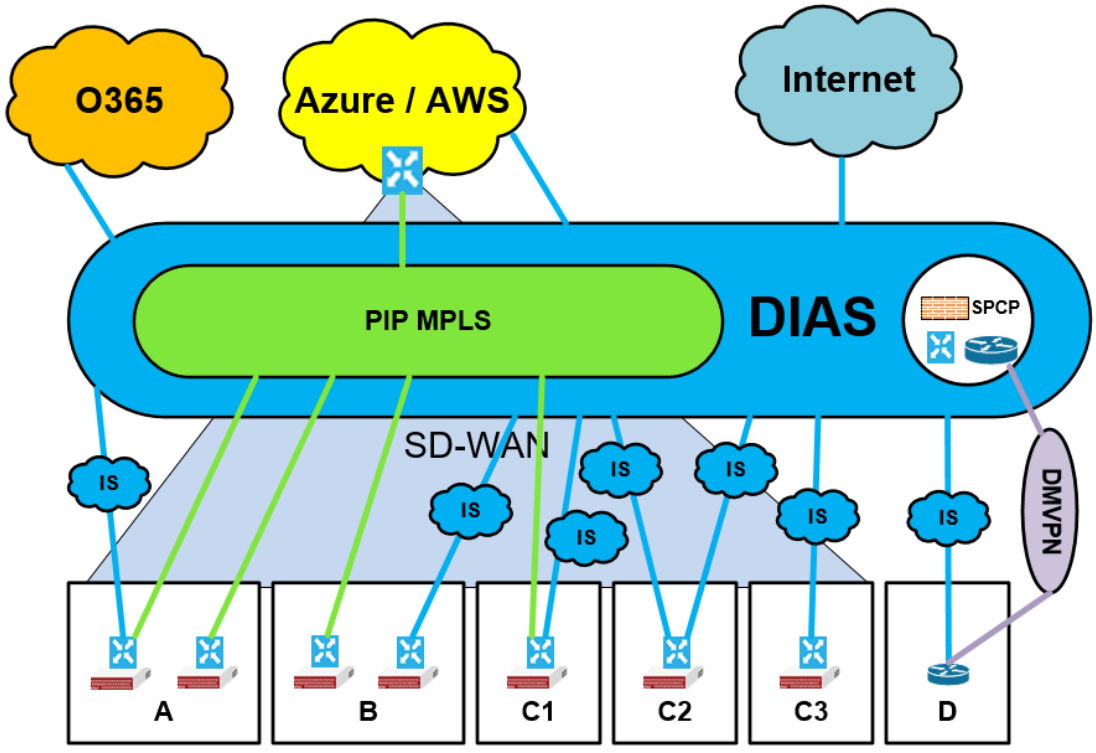


Figure 19. High-level overview of the SD-WAN deployment

Figure 20 on below demonstrates Konecranes network high-level overview of Internet and MPLS overlays. There are three different regions EMEA, AME and APAC and they all have local firewalls and Internet breakouts. Cisco SD-WAN has been implemented in all of them and they are connected to MPLS and Internet overlays through their local SD-WAN device or routers. The Internet overlay and MPLS overlay are both connected to SPCP where traffic can be manipulated or policed in numerous ways. Through utilizing a centralized SD-WAN centric design all sites are able inter-communicate across various transports in a secure manner. SPCP can contain lots of different services that the service provider is hosting. It is possible to use multiple SPCP's, as an example there could be one in each region to lower latency. There can be firewalls, Internet breakouts, SD-WAN controllers and so on. This demonstration includes Cisco's vManage, vBond, vSmart, vEdge, firewall, traditional router and the Internet breakout. Cisco vManage is located in management plane and it is like a dashboard where policies and security frameworks are defined. Cisco vSmart controllers are working in the control plane and they distribute data plane and application aware routing policies to vEdge routers. VSmart controllers will take care of connectivity for users and applications. Cisco vEdge routers are working in the data plane and they establish a secure control plane with vSmart controllers using TCP based extensible control plane protocol called OMP (Overlay Management Protocol) which advertises control plane context. It can leverage traditional routing protocols such as OSPF, BGP and VRRP in the data plane. Cisco vBond operates in the orchestration plane which can distribute list of vSmarts and vManage to all vEdge routers. It also orchestrates management and control plane.

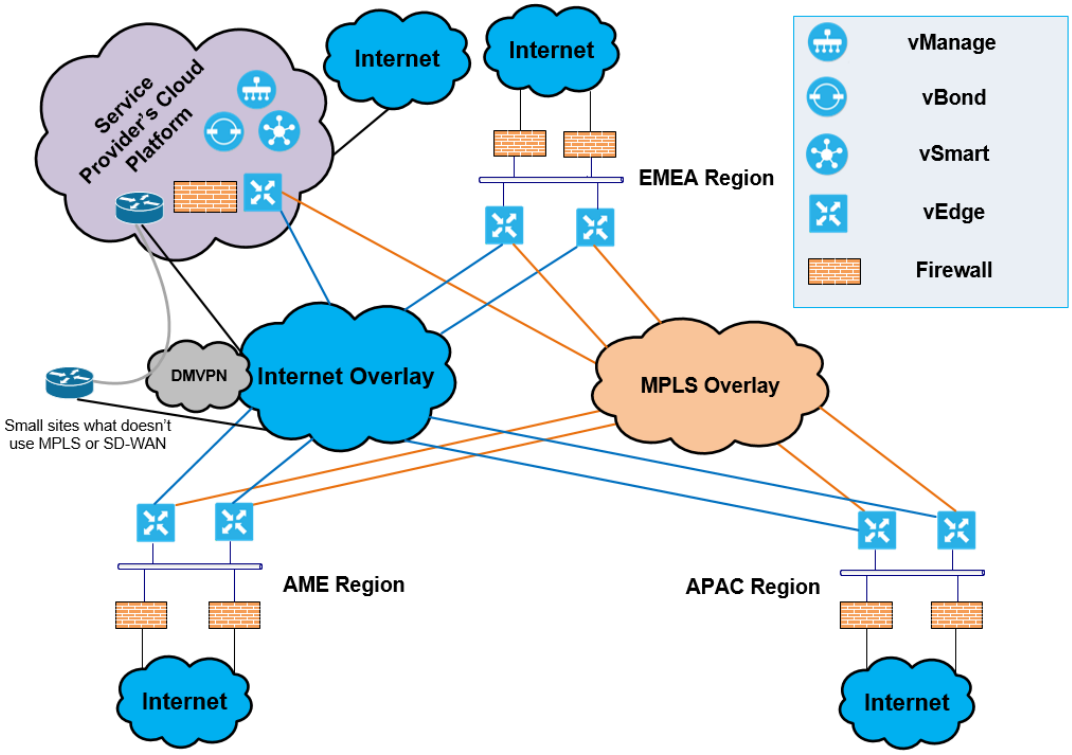


Figure 20. High-level network overview with Internet and MPLS overlays

Figure 21 on below shows pretty much the same thing as previous Figure 20 but now the regions has been replaced by different sizes of sites and connections that are the characteristic of them. There are same sites A, B, C1, C2, C3 and D that were described previously in Figure 19. Larger and more important sites have better connections than smaller sites. The order starts from most important A and ends at least important D sites. A and B sites have a local Internet breakout which they can use but there are many other sites such as C2 and C3 which don't have a local Internet breakout. These kinds of sites can use the firewall in SPCP and the Internet through it, or the other option is that they can use B site Internet breakouts if it's closer than SPCP to minimize the latency. SD-WAN is a flexible solution because we can deploy new sites faster than previously and modify the existing ones, also we are able to choose what type of routes traffic should use to reach specific destinations.

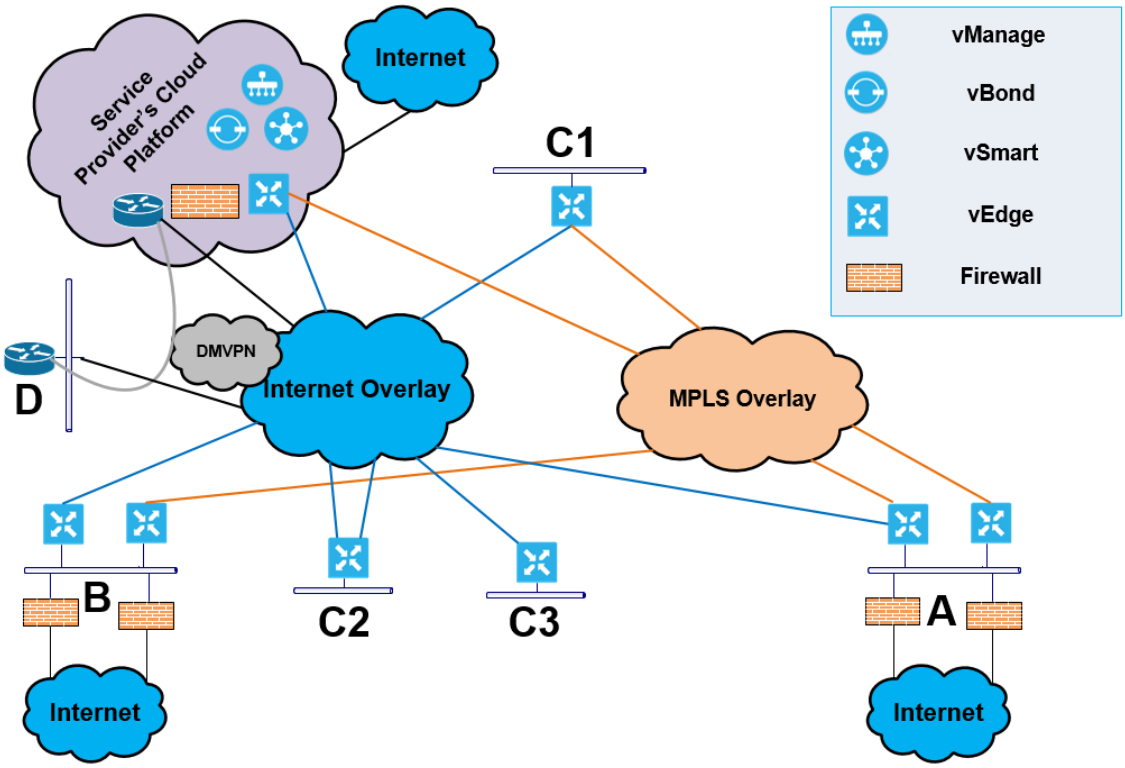


Figure 21. High-level Konecranes network overview with different sizes of sites

Figure 22 on below demonstrates segmentation opportunities with SD-WAN in the Konecranes network. The purple line displays site to site traffic between C1 and C2 sites that don't use a firewall between them. For example, VoIP Skype traffic which needs fast and stable connections to maintain the quality in the call. Red line demonstrates site to site traffic through the firewall which can be any traffic other than VoIP. When C2 site is sending traffic to B site or vice versa it will go through SPCP firewall in order to ensure that malware or other harmful items don't spread from one site to another. Both green lines are displaying different examples of traffic that

need to go to Internet. Option 1 is the darker green line where C3 site is sending traffic to Internet through A site's local firewall and Internet breakout. Option 2 is to send traffic to SPCP and use firewall and Internet breakout which are located there. It can be determined which solution should be used on a case by case basis, it may take into account distances or segmentation demands and so on. We can see that there are a lot of options regarding how different types of traffic or different sites should behave and communicate to achieve the necessary traffic segmentation and load balancing design. There are also D sites which are connected to SPCP via DMVPN.

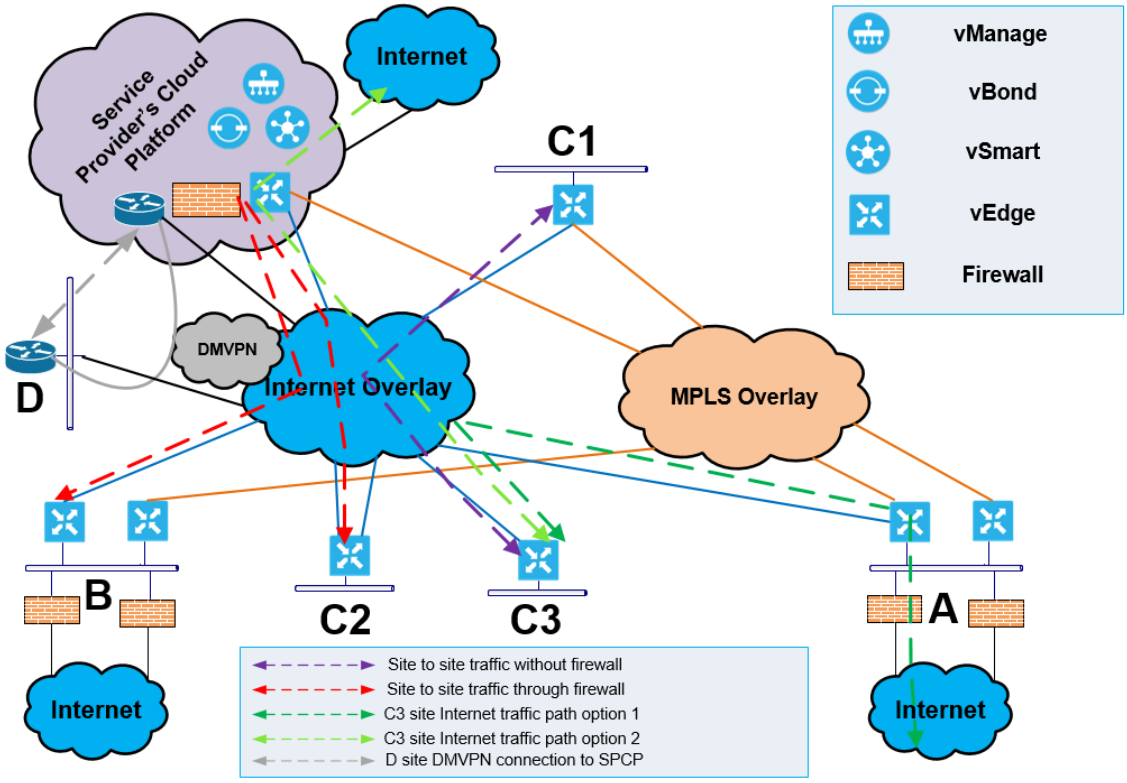


Figure 22. High-level overview of the traffic segmentation in Konecranes network

From my point of view, SD-WAN would be a great choice to implement in the Konecranes network because it allows the replacement of most of the current expensive MPLS connections. The end result of the new network design is it would be more simplified, flexible, movable, and cost-effective. New site integration to the existing Konecranes network would be faster and site moves from one location to another can be arranged faster from network point of view. Furthermore, SD-WAN provides good load balancing options for traffic and segmentation for the sites. The management and maintenance of SD-WAN locations is easier to handle because of the unified management plane which allows easy policy distribution to desired locations. MPLS connections should be kept on the most critical locations where connections must be as stable as possible around the clock where service disruptions are not acceptable. However, SD-WAN should be also implemented to those locations to provide the best possible connections,

load balancing and outcome. In the end, I would say that a hybrid network design would be the right direction for the Konecranes network to develop.

5 SUMMARY

This thesis consists of five different main chapters and those chapters are Introduction, MPLS, Internet based solution, Konecranes network and Summary. The Introduction chapter covers knowledge of Konecranes and it introduces the thesis subject, problem, and goal. The Second chapter, MPLS, covers information and operation of the MPLS technique. The Third chapter is called Internet based solutions and it covers different kinds of information regarding cloud computing, virtualization, and SD-WAN solutions. In the fourth chapter I am introducing the Konecranes network current state and my vision of the future network. The Fifth chapter is this Summary.

The purpose of this thesis was to develop the Konecranes network in a new direction of Internet based solutions. Currently Konecranes is using MPLS based network and there were some identified problems where I tried to find solutions. These problems were highly growing Internet traffic, traffic prioritization, offloading and segmentation. MPLS connections are quite expensive so it would be good to find an alternative option which could replace most of them. The main goal of this thesis was to gather information of achievable opportunities that Internet based solutions could offer. I would say that I managed to find solutions to the identified problems and also introduced Internet based solutions.

From my point of view the most reasonable way to continue Konecranes network development is to aim for the hybrid network setup which can take advantage of both MPLS and SD-WAN solutions. With SD-WAN the Konecranes network would be more simplified, flexible, movable and cost-effective. SD-WAN provides good load balancing options for traffic and segmentation for the sites. SD-WAN should replace most of the existing MPLS connections and it would lead to cost savings. This thesis gives one perspective where Konecranes could develop their network. Thesis subject is currently topical which made research work more rewarding and interesting.

REFERENCES

Abogado, N. (2016). *A Brief History of MPLS*. Retrieved June 3, 2018, from https://www.talari.com/blog/brief-history-mpls/

Akkiraju, P. (2017). *Viptela Fabric*. Retrieved August 5, 2018, from http://viptela.com/#vfabric-vid

Amazon. (n.d.). *What is AWS?* Retrieved August 24, 2018, from https://aws.amazon.com/what-is-aws/

Arvopaperi. (2018). *Konecranes Oyj tilinpäätöstiedote 2017*. Retrieved June 14, 2018, from https://www.arvopaperi.fi/porssitiedotteet/konecranes-oyj-tilinpaatostiedote-2017-6700511

Butler, B. (2017). *SD-WAN: What is it and why you'll use it one day*. Retrieved August 1, 2018, from https://www.networkworld.com/article/3031279/sd-wan/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html

Cisco. (2018). *SD-WAN: the new landscape of networking*. Retrieved August 8, 2018, from https://www.cisco.com/c/m/en_us/solutions/enterprise-networks/sd-wan/new-landscape-of-networking.html

Don, J. (2017). *A Guide to MPLS VPN Fundamentals*. Retrieved July 17, 2018, from https://www.packetdesign.com/blog/a-guide-to-mpls-vpn-fundamentals/

IETF. (2006). *RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs)*. Retrieved July 28, 2018, from https://tools.ietf.org/html/rfc4364

Juniper. (2018). *MPLS Label Operations*. Retrieved June 17, 2018, from https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-label-operations-qfx-series.html

Juniper. (2018). *MPLS Label-Switched Paths and MPLS Labels*. Retrieved June 15, 2018, from https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-label-operations-qfx-series.html

Kaelin, M. (2017). *Microsoft Office 365: The smart person's guide*. Retrieved August 22, 2018, from https://www.techrepublic.com/article/microsoft-office-365-the-smart-persons-guide/

Konecranes. (2018). *History*. Retrieved June 13, 2018, from https://www.konecranes.com/about/history

Lakshman, U., & Lobo, L. (2006). *MPLS Control and Data Plane Components*. Retrieved June 9, 2018, from https://flylib.com/books/en/2.686.1/mpls_control_and_data_plane_components.html

Lakshman, U., & Lobo, L. (2006). *MPLS Overview*. Retrieved June 9, 2018, from https://flylib.com/books/en/2.686.1/mpls_overview.html

Lakshman, U., & Lobo, L. (2006). *MPLS Terminology*. Retrieved June 9, 2018, from https://flylib.com/books/en/2.686.1/mpls_terminology.html

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud*. Retrieved August 10, 2018, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Microsoft. (n.d.). *What is Azure?* Retrieved August 19, 2018, from https://azure.microsoft.com/en-us/overview/what-is-azure/

Rivera, A. (2018). *Virtualization vs. Cloud Computing: What's the Difference?* Retrieved August 20, 2018, from https://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html

SC Media. (2013). *Zscaler Security Cloud*. Retrieved August 22, 2018, from https://www.scmagazine.com/review/zscaler-security-cloud/

Sheldon, T. (2001). *Explicit Routing*. Retrieved June 13, 2018, from http://www.linktionary.com/e/explicit_routing.html