Design Of Sd-Wan On Insurance Holding Company PT. XYZ Using On-Demand Tunnel Full Mesh Connectivity

Marchand Satriawan[1], Benfano Soewito[2]

[1,2] Computer Science Department Binus Graduate Program – Master of Computer Science

e-mail: marchand.satriawan@binus.ac.id[1], bsoewito@binus.edu[2]

Abstrak

Modernisasi infrastruktur akan menjadi kebutuhan yang mendesak dan peningkatan kualitas pelayanan membuat PT. XYZ menghadapi tantangan serius dalam mencapai tujuannya untuk meningkatkan layanan asuransi dan penjamin emisi terbesar di Indonesia. Ini termasuk tantangan yang cukup kompleks dalam mengendalikan pengelolaan fasilitas dan proses bisnis yang ada. Ruang lingkup tugas akhir ini adalah untuk membandingkan kinerja sebelum dan sesudah implementasi SD-WAN pada jaringan antar anggota PT.XYZ dalam hal manajemen, biaya operasional, kemudahan kontrol, dan juga manajemen terpusat. Berdasarkan penelitian yang dilakukan dengan membandingkan hasil sebelum dan sesudah implementasi Cisco SD-WAN untuk PT. XYZ, maka dapat disimpulkan bahwa pengujian berjalan dengan baik. Dengan diterapkannya SD-WAN akan memecahkan masalah dan tantangan dalam merger IT yang baru saja dilakukan sebagai Holding BUMN Asuransi.

Kata kunci: *SD-WAN, Definisi Perangkat Lunak, Otomasi, Desain, Jaringan Area Luas*

Abstract

Modernization of infrastructure will be an urgent need and improvement of service quality makes PT. XYZ faces serious challenges in achieving its goals of improving Indonesia's largest insurance and underwriters services. This includes quite complex challenges in controlling the management of existing facilities and business processes. The scope of this thesis is to compare the performance before and after the implementation of SD-WAN on the network between members of PT.XYZ in terms of management, operational costs, ease of control, and also centralized management. Based on research conducted by comparing the results before and after the implementation of Cisco SD-WAN for PT. XYZ, it can be concluded that the test went well. With the implementation of SD-WAN, it will solve problems and challenges in an IT merger that was just carried out as an Insurance BUMN Holding.

Keywords : *SD-WAN, Software Define, Automation, Design, Wide Area Network*

INTRODUCTION

PT. XYZ is an Insurance BUMN Holding consisting of all Indonesian BUMN insurance companies which recently merged which was formed by the government to play a role in national development through the development of a complete and innovative non-bank financial industry through investment, insurance and guarantee services.

The application of information technology in a company will significantly improve performance. Increased knowledge of information technology, especially in the business processes of PT. XYZ which is a holding formed by the government to play a role in national development through the development of a complete and innovative non-bank financial industry through investment, insurance and guarantee services. With the merger of all state-owned insurance and guarantee companies, it is expected to accelerate the information system and be able to perform efficiency by integrating with one another.

Modernization of infrastructure will be an urgent need and improvement of service quality makes PT. XYZ faces serious challenges in achieving its goals of improving

Indonesia's largest insurance and underwriters services. This includes quite complex challenges in controlling the management of existing facilities and business processes.

Software Defined Networking (SDN) offers a paradigm in network control which makes it easier for network management, control, and supervision and also makes it possible to improve network performance, this is because SDN carries the concept of separating the data plane and control plane, where the existing control planes are united as a single point of control [3].

Industry 4.0 organizations adopt digital transformation to provide faster services, not only to increase employee productivity but also improve business processes, resilience, and ultimately drive rapid business growth. This trend, combined with rapid growth [5]. The Internet of Things (IoT), mobile devices, and media-rich applications place more demands on your legacy WAN infrastructure. Applications—both in the cloud and on-premises—require fast, predictable performance.

Through this case study the use of Software Defined Wide Area Network (SD-WAN) is expected to be one of the recommended solutions for PT. XYZ to be able to centralize the network to facilitate overall network management, control and supervision so as to improve services that have been adapted to the company's vision and mission. The integration of all systems into a centralized and integrated Information Technology Database will represent strong management capabilities in the areas of planning, monitoring and business execution.

RELATED WORK

Related research on Software Defined Network technology that has been carried out by entitled Software Defined Green Data Center Network with Exclusive Routing is conducting research related to how to get optimal network capacity results, many data architectures center proposed to replace traditional tree architecture, such as fat tree, Bcube, etc. because the traditional architecture is identical to many switches and data traffic is bidirectional when there is an exchange of data traffic at peak time traffic.

The results of this study show that there are 2 side effects of traditional tree architecture on data center consumption. the first can increase the consumption of electrical energy due to the use of a large number of switches. secondly, it causes inefficient network energy consumption when the switch is in low utilization, because even at low utilization the energy absorbed remains the same. With the results of the study, namely applying the flow scheduling method to reduce energy consumption in the data center network that applies Software Defined Network technology with and shortens the average traffic flow time.

Research on SDN was also conducted by entitled Research Challenge for Traffic Engineering in Software Defined Networks. In this study, SDN represents a new, flexible, and open architecture that allows dynamic and timely management of network behavior in complex and large-scale computer networks. As SDN accelerates the innovation and evolution of modern data networks, it requires a highly scalable and intelligent TE system. This article investigates SDN TE solutions from the perspective of traffic management, load balancing, fault tolerance, topology updates, traffic analysis.

Based on this background, the formulation of the problem to be solved in this research is how to do a merger of a state-owned insurance company. The purpose of this paper is to analyze the condition of the WAN used by PT. XYZ is now aware of the implications of changing current WAN solutions to SD-WAN.

THEORY METHOD

In conducting this case study, the implementation of SD-WAN is carried out using solutions that come from vendors who have a business focus in the network sector, in the end a comparison will be made with the implementation results with existing conditions, the Quality of Service (QoS) parameter that is used as a benchmark is throughput. , jitter, delay and packet loss [1]. The in-depth algorithm will not be discussed here because. are proprietary or patents of each company in developing their products, but the result to be

achieved is whether SD-WAN is suitable to be applied in the PT.XYZ environment in order to combine connectivity between members [2].

PDIOO is an abbreviation which means planning, design, implementation, operation, and optimization. It reflects the various phases of the network life cycle that are intertwined with each other. With PDIOO will find every phase in the regular operation of all networks. While each phase is important, network design is a vital phase of the PDIOO methodology. There are built-in and contingent connections between network design and every other phase of PDIOO because important designs are found in each phase and each phase is very important to consider when making network design decisions [3].

Traditional network architecture designs rely on distribution control and transport network protocols running on routers and switches that forward packets, allowing them to travel. The integration between the control plane and the data plane complicates network management. Open Flow is a standard interface designed for SDN, and is of great interest to network equipment developers and industrialists [4].

Quality of Service (QoS) is a network capability to provide better service to selected network traffic through various technologies such as frame relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1, SONET and other IP networks that use this technology [6].

Compression is essential to minimize the amount of bandwidth consumed on the link during transfer across WANs where bandwidth is quite limited. It can improve bandwidth utilization efficiency, thereby reducing bandwidth bottlenecks; it can also reduce the amount of transit time for a given data to traverse the WAN by reducing the data transmitted. Because of this, compression substantially optimizes data transmission over the network. A comparative study between various text file compression techniques reported in [8] that text files are highly effective in compression.

Caching is considered an effective approach to reduce network traffic and application response times. Based on Cache location, they can be used on client side, proxy side, and server side. Due to the limited capacity of a single Cache, Cache can also work together to serve a large number of clients. Cooperative caching can be set up hierarchically, distributively, or in hybrid mode.

METHOD RESEARCH

Research method of this paper is descriptive qualitative by referring to direct observation data and supported by relevant literature sources. The first stage in this case study begins with formulating the problems that arise after the merger of BUMN Holding. After the formulation of the problem is determined, the next step is to conduct a literature study. Literature study was conducted by collecting basic knowledge and concepts related to this research through books and journals, especially related to Software Define Network, WAN, and other studies relevant to this research [7].
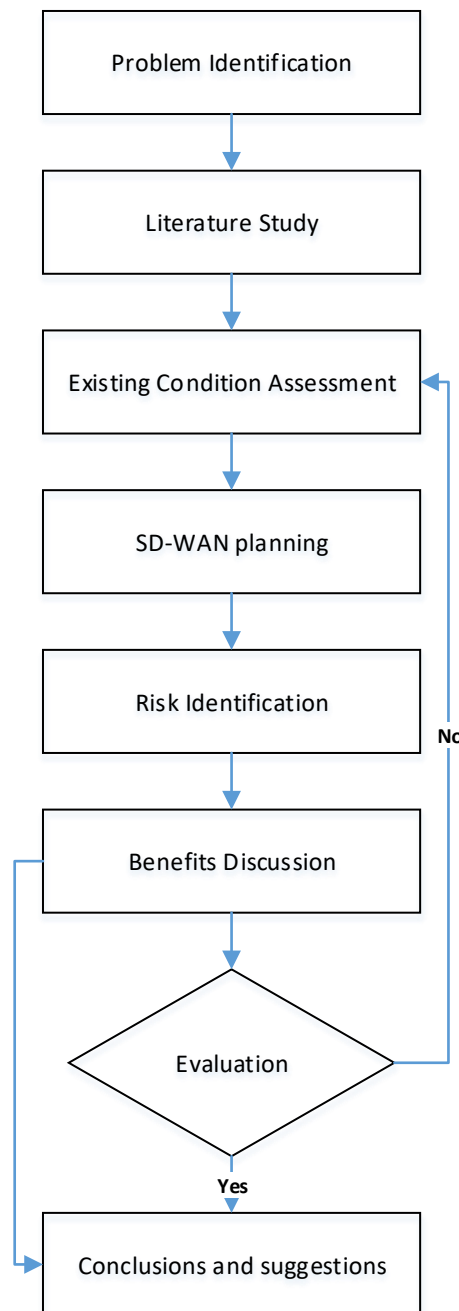
Figure 1 Conceptual Framework

Step Assessment is carried out based on the state of the results of field observations. The things that will be carried out in this assessment are as follows:

1. Recording (Inventory) all PT.XYZ group infrastructure that is part of the project and also other affected devices either in configuration or traffic flow
2. Capture all device configurations that are part of the project as well as other affected devices to be used as material for analysis and making Low Level Design
3. Conducting discussions regarding planning for the new Infrastructure including: Device Naming, IP Address Allocation, VLAN Segmentation, Routing & Switching, Policy & QoS etc.
4. Conducting discussions related to traffic flow in the new infrastructure.
5. imulating the new infrastructure that will be implemented using network emulation software SD-WAN design.

PROPOSED ARCHITECTURE

The next stage is a system recommendation which is divided into 2 main parts in the application of SDWAN technology including:

1. Functional Capability: In this section the author provides recommendations, especially on the technical function of SDWAN.
2. Operational Ability: In this section the author provides more recommendations towards the operational team of PT.XYZ
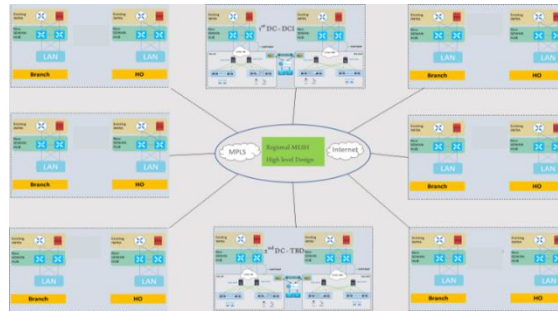

Figure 2. Proposed Design Full Mesh Connectivity

The picture below represents the points needed by PT. XYZ in implementing a good WAN in technical terms.
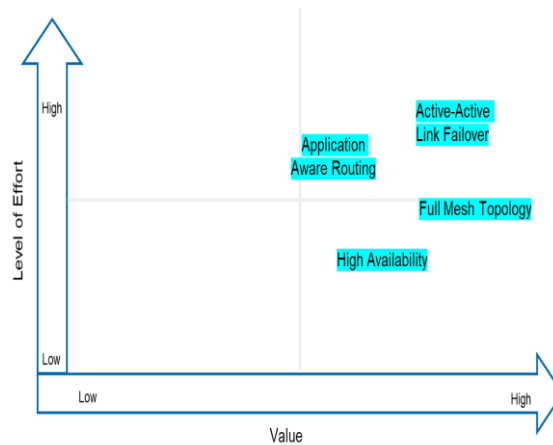

Figure 3. Comparison of Value with Technological Effort Points

If you pay attention to the diagram above, it can be concluded that the High Availability and Full Mesh Topology points are points that can be prioritized. If the prioritized points have been made then the PT.XYZ team can proceed to the other two points.
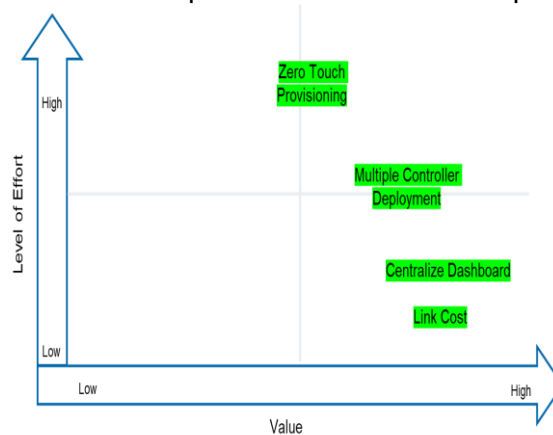

Figure 4. Comparison of Value with Operational Effort Points

If you look at the diagram above, it can be concluded that the Link Cost and Centralize Dashboard points are the points that can be prioritized. If the prioritized points have been made then the PT.XYZ team can proceed to the other two points.

Identify risks that aim to minimize the impact of migration on production and prepare curative schemes and contingency plans in case something unexpected happens. System evaluation is obtained by comparing the results of the parameters measured from the two running networks, namely the existing network that is running with the network using SD-WAN technology. Parameters that are calculated and compared are throughput, delay, packet loss and jitter. In addition, the performance of SD-WAN will also be seen using the report application of the product used

RESULTS AND DISCUSSION

Based on the results of an interview with Mr. Anjas as the project coordinator, in the discussion of this research, those configured as SD-WAN will be simulated on the Cisco cloud as identical as possible to the current conditions that are running and using devices from the Cisco brand, because of the policy of the company where the simulation is carried out. before it is implemented in production

Existing Condition Analysis

Below is a low level design that exists in the current infrastructure. All data traffic passes through DC1. DC1 has 2 Core devices using VPC technology. The branch has 2 ISP links, each connected to DC1. Branch uses fortigate devices to handle WAN connections with IPSEC and SDWAN technologies. DC1 and DC2 connections use Metro-E which is connected to the Core Switch at each site. Block 3rdpary has leased line and public ip connectivity. Connectivity to Datacenter Hub using Internet link with IPSEC technology.
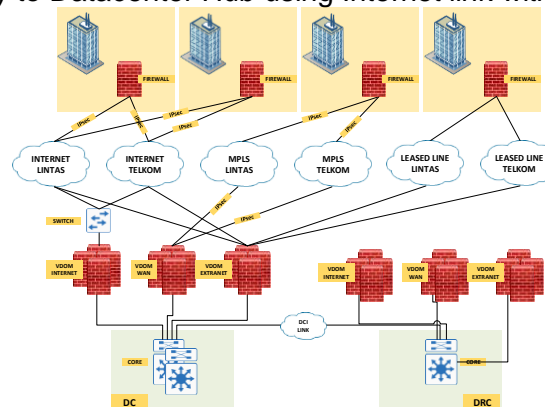

Figure 5 Existing Design

The test is carried out at the Cisco Lab by copying the existing topology for simulation in order to avoid unwanted things during testing before going up to production. Testing using a simulator provided by Cisco, namely dCloud. For the modules used in this case, several modules are:
1. Vbond – Orchestration Plane, Serves to regulate aircraft control and management.
2. vSmart – Control Plane, Serves to facilitate the discovery of new routers and also separate control plane information between vEdges.
3. vEdge – Data Plane, Vedge is a WAN router that provides a secure data plane with remote vEdge routers
4. vManage – Management Plane, Vmanage functions as a centralized management for operations from router startup to configuration
5. Trex – Traffic Generator, TRex is an open source, stateful and stateless traffic generator. It generates L3-7 . traffic

6. WanEm – Wan Emulator, WANem is a WAN Emulator, which is intended to provide real experience of mpls/Internet network, during application development/testing over LAN environment.

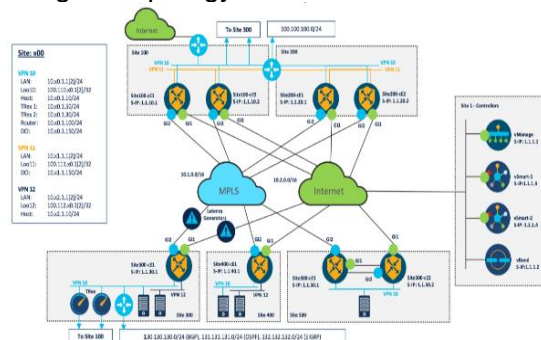The following is the logical topology used in the lab for final testing:
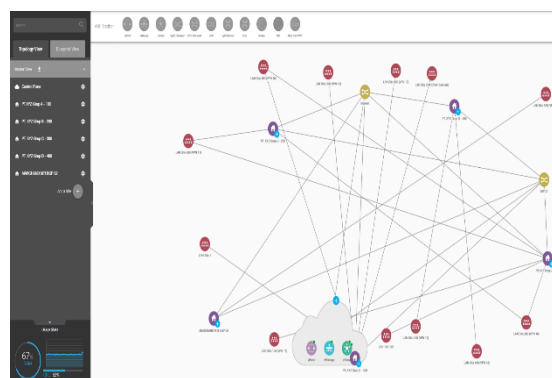

Figure 6 Logical Topology

Figure 7 Physical Topology

On Demand Tunnel Full Mesh Connectivity

With the formation of tunnels automatically automatically only when needed, it will make device utilization low and have a high scalability design. With a full mesh topology we will also test about high availability, application aware routing and also how to manage tens or hundreds of devices in one management.

When we configure the site to use dynamic tunneling, the on-demand functionality is enabled. In this mode of operation, Cisco SD-WAN routers do not carry direct tunnels to other sites that are also enabled with on-demand functionality. Cisco SD-WAN selects one or more routers (usually a centrally located router) to act as backup forwarding node(s), providing a secondary path for traffic between the two nodes. Backup nodes are not enabled for on-demand. All sites on request form a static tunnel with backup nodes.

The backup node provides a static backup route for traffic between two nodes that is enabled on demand. The first packet of traffic between the two nodes is routed through the static backup path, and triggers a tunnel request to become active between the sites. The backup line continues to forward traffic until the direct line becomes active. All on-demand sites learn the TLOC and prefix of all other on-demand remote sites. The prefix also has a backup path set through the Cisco vSmart Controller control policy. So in the control field, the on-demand tunnel network has the same status as the full mesh tunnel network, including the backup path.

The control plane downloads to data fields, routes, with backup paths and remote TLOCs representing potential direct paths between any two sites, but does not tunnel direct paths to remote TLOCs. Traffic from both ends of the tunnel on demand triggers the tunnel setup. This allows on-demand tunneling to accommodate network address translation (NAT) traversal. On-demand tunnel features:

1. Off: Tunnels on demand are not set up with remote sites. There is no active traffic to or from the remote site. Remote site TLOC is inactive - no bidirectional forwarding detection (BFD) is set up, the prefix is installed with an inactive path, and a backup path is set as the path to forward any traffic. An inactive path detects the flow and triggers a live site-to-site tunnel to set up.
2. On: Live on-demand site-to-site tunnels are set to remote sites. There is active traffic to or from the remote site. This state is identical to the typical tunnel case, where the remote TLOC has the BFD set, and the prefix is set with the direct line tunnel. In this state, tunnel activity is tracked. If there is no traffic for the duration of "idle time" (default 10 minutes), the direct site-to-site tunnel is deleted and the status changes to Inactive.

Ping from PT. XYZ Group C – 300 to PT. XYZ Group D – 400 with the datacenter position at PT. XYZ Group A – 100 and PT. XYZ Group B - 200 with full mesh connectivity request from Group C to Group D does not need to go through Group A or Group B.
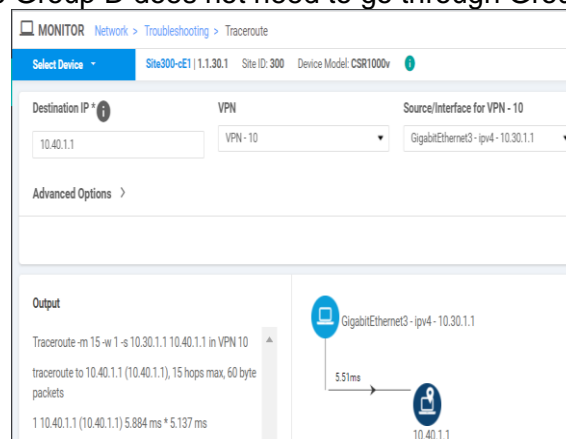

Figure 8 Hub and spoke connectivity test

It can be concluded that the hub and spoke topology is not suitable for use in the PT environment. XYZ because it is expected that the location of the datacenter can be in every member of the company.

SLA service testing based on QOS

How SD-WAN is able to improve SLA services is by using routing calculations based on application quality at each provider. In this test, the author uses a traffic generator and also a wan emulator to affect the quality of the provider both on MPLS and on the Internet
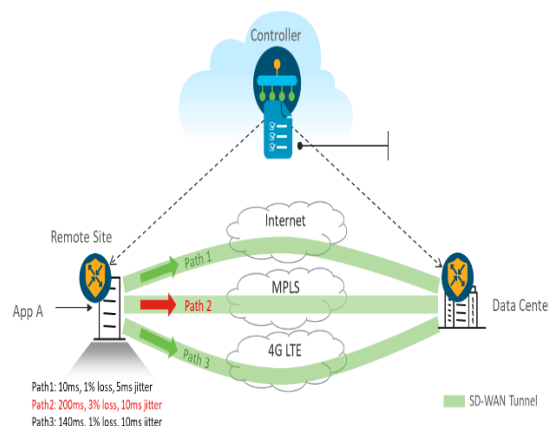

Figure 9 Application aware routing architecture (Source: Cisco_SD-WAN_Core_TDM-v8)

It looks like the picture below the system will automatically use the mpls provider path because the link quality is better than the internet. With this test successfully carried out, the system can automatically see better link quality so that the user's service is not disrupted even though one of the link providers is experiencing problems. With hybrid mpls and internet, besides being able to reduce service operational costs, it can also increase SLA by up to 99.9%.

Lower OPEX costs

When viewed from the calculation of ROI for SDWAN devices for 5 years using a hybrid Internet & MPLS connection, it is cheaper by Rp. 5,230,000,000 compared to traditional technology by using two MPLS connections. for Data Center locations. As for the implementation in branches with SDWAN devices, the difference is Rp. 116,392,000,000 cheaper than if the branch uses traditional technology and uses a two-link MPLS connection. The ROI calculation above is assumed to use the Cisco brand SDWAN type.

The total cost for a Data Center using SDWAN is Rp. 14,030,000,000 and the total cost for the Branch is Rp. 183.608 million over a period of 5 years.

CONCLUSION

It can be concluded that the test went well. With the implementation of SD-WAN, it will solve problems and challenges in an IT merger that was just carried out as an Insurance BUMN Holding. Following are the conclusions based on this research:
1. Ease of monitoring process. The use of 1 SDWAN brand will facilitate the monitoring process because the entire WAN infrastructure can be monitored in 1 dashboard.
2. Ease of setting and management process. With 1 dashboard, the WAN infrastructure management process can be done more easily.
3. High availability. With the various WAN and Internet connections used in the SDWAN solution, it can achieve high SLA Availability and can increase network user satisfaction.
4. Decreasing Opex, by reducing the use of MPLS links by conducting Hybrid MPLS and the internet, it will reduce operational costs.
    Suggestion

Suggestion

Some suggestions are given to improve this research or provide other solutions to the problems that will be faced. Some of these suggestions are as follows:
1. The research was carried out using a lab even though the topology was made as identical as possible to real conditions, it still needed to be tested directly in the field after the procurement project at PT. XYZ.
2. The research is only done by the Cisco brand.
3. The research has not done testing on IP overlaps, it is hoped that the next author can develop how if a company organization does a merger, it is certain that many IPs will overlap, one of which is to use site to site nat

REFERENCES

Ali, E. K., Manel, M., & Habib, Y. (2017). An Efficient MPLS-Based Source Routing Scheme in Software-Defined Wide Area Networks (SD-WAN). *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, https://doi.org/10.1109/aiccsa.2017.165.

Akyildiz, I. F., Lee, A., Wang, P., Luo, M., & Chou, W. (2016). Research challenges for traffic engineering in software defined networks. *IEEE Network*, https://doi.org/10.1109/mnet.2016.7474344.

Benamrane, F., Mamoun, M. B., & Benaini, R. (2017). An East-West interface for distributed SDN control plane: Implementation and evaluation. *Computers & Electrical Engineering*, https://doi.org/10.1016/j.compeleceng.2016.09.012

Pamplin, S. (2021). SD-WAN revolutionises IoT and edge security. *Network Security*, https://doi.org/10.1016/s1353-4858(21)00090-8

Troia, S., Mazzara, M., Zorello, L. M., & Pattavina, A. (2021). Resiliency in SD-WAN with eBPF Monitoring: Municipal Network and Video Streaming Use Cases. *17th International Conference on the Design of Reliable Communication Networks (DRCN)*, https://doi.org/10.1109/drcn51631.2021.9477351

Kreutz, D., Yu, J., Esteves-Verissimo, P., Magalhaes, C., & Ramos, F. M. (2018). The KISS Principle in Software-Defined Networking: A Framework for Secure Communications. *IEEE Security & Privacy*, https://doi.org/10.1109/msp.2018.3761717

Vachon, B., & Johnson, A. (2018). *Connecting Networks v6.* Cisco Press.

Al-laham, M., & Emary, I. M. (2007). Comparative Study between Various Algorithms of Data Compression Techniques. *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.4

Casado, M., Foster, N., & Arjun. (2014). Abstractions for software-defined networks. *Communications of the ACM*, https://doi.org/10.1145/2661061.2661063.

Chankhunthod, A., Danzig, P. B., Neerdaels, C., Schwartz, M. F., & Worrell, K. J. (1996). A hierarchical internet object cache. *in Proc. 1996 annual conference on USENIX Annual Technical Conference.* San Diego, CA.

Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and OpenFlow: From concept to implementation. *IEEE Communications Surveys*, https://doi.org/10.1109/comst.2014.2326417.

Hucaby, D. (2010). *CCNP SWITCH 642–813 Official Certification Guide.* Indianapolis: Cisco Press.

Jain, S., Kumar, A., Mandal, S., O, J., Poutievski, L., Singh, A., . . . Vahdat, A. (2013). B4: Experience with a Globally-Deployed Software Defined WAN. *SIGCOMM*, https://doi.org/10.1145/2534169.2486019.

Li, D., Shang, Y., He, W., & Chen, C. (2015). EXR: Greening Data Center Network with Software Defined Exclusive Routing. *IEEE Transactions on Computers*, https://doi.org/10.1109/tc.2014.2375233.

Nunes, B. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking : Past , Present , and Future of Programmable Networks, 16(3), 1617–1634. *IEEE Communications Surveys & Tutorials*, https://doi.org/10.1109/SURV.2014.012214.00180

Ravi, J., Yu, Z., & Shi, W. (2009). A survey on dynamic web content generation and delivery techniques. *Journal of Network Computer Applications*, https://doi.org/10.1016/j.jnca.2009.03.005.

Sheng, B., & Bastani, F. B. (2004). Secure and Reliable Decentralized Peer-to-peer Web Cache. *18th International Parallel and Distributed Processing Symposium*.

Szigeti, T., Hattingh, C., Barton, R., & Briley, K. (2013). *End-to-end QoS Network Design.* Cisco Press.

Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks (5th Edition) (5th ed.).* Pearson

Xu, Z., Hu, Y., & Bhuyan, L. (2004). Exploiting Client Cache: A Scalable and Efficient Approach to Build LargeWeb. *18th International Parallel and Distributed Processing Symposium*, https://doi.org/10.1109/ipdps.2004.130297