Erzincan Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
2025,18(1), 10-23
ISSN: 1307-9085, e-ISSN: 2149-4584
Araştırma Makalesi

Erzincan University
Journal of Science and Technology
2025,18(1), 10-23
DOI: 10.18185/erzifbed.1197841
Research Article

Business Continuity Focused Hierarchic Network Topology Application for Universities

Veli ÇAPALI[1*], Ömer Faruk SAĞBAŞ[1], Kerim KARABAŞ[1], Kadir SÜMER[1]

[1] Süleyman Demirel Üniversitesi, Bilgi İşlem Daire Başkanlığı, Isparta, Türkiye

Received: 01/11/2022, **Revised:** 07/07/2023, **Accepted:** 28/11/2024, **Published:** 28/03/2024

Abstract

Today, internet and network services have become a great need with the increase in their impact and convenience in every field. Interruptions that may occur in internet and local network services in hospital automation systems are of critical importance. The demand for continuity and fast connection in internet use in distance education and health services by users has increased especially during the pandemic process. Thanks to mobile life, user patterns have changed and with the expansion of the usage areas of wireless networks, there have been changes in network topologies. Users demand uninterrupted and fast connections.

Redundancy: It has a special importance for the business processes of institutions and organizations and for services where downtime can cause serious problems. Therefore, redundancy is required to ensure that in case any of the network devices fail, it maintains the network connection with the other devices. Network redundancy is an important factor to consider maintaining network reliability and business continuity. In this study, an approach, suggestions, and a case study on how to create a redundant and hierarchical network system for large multi-user campus areas implemented in Suleyman Demirel University are presented.

Keywords: Network Planning, Hierarchical Network Topology, Business Continuity, Network Security, Network Protocols.

Üniversitelere Yönelik İş Sürekliliği Odaklı Hiyerarşik Ağ Topolojisi Uygulaması

Öz

Günümüzde internet ve ağ hizmetleri, her alanda etkisinin ve sağladığı kolaylıkların artması ile büyük bir ihtiyaç haline gelmiştir. Hastane otomasyon sistemlerinde internet ve yerel ağ hizmetlerinde oluşabilecek kesintiler kritik öneme sahiptir. Kullanıcılar tarafından uzaktan eğitim ve sağlık hizmetlerinde internet kullanımında süreklilik ve hızlı bağlantı talepleri özellikle pandemi sürecinde artmıştır. Mobil yaşam sayesinde kullanıcı şekilleri değişmiş ve kablosuz ağların kullanım alanlarının genişlemesi ile ağ topolojilerinde değişiklikler olmuştur. Kullanıcılar kesintisiz hizmet veren ve hızlı bağlantıları talep etmektedirler.

Yedeklilik; kurum ve kuruluşların iş süreçlerinde ve kesinti süresinin ciddi sorunlara neden olabileceği hizmetler için özel bir öneme sahiptir. Bu nedenle, ağ cihazlarının herhangi birinin arızalanması durumunda diğer cihazlar ile ağ bağlantısını sürdürdüğünden emin olmak için yedeklilik gereklidir. Ağ yedekliliği, ağın güvenirliliğini ve iş sürekliliğini sürdürmek için dikkate alınması gereken önemli bir faktördür. Bu çalışmada; Süleyman Demirel Üniversitesinde uygulanan ve çok kullanıcılı geniş yerleşke alanlarına yönelik yedekli ve hiyerarşik bir ağ sisteminin nasıl oluşturulacağına dair yaklaşım, öneriler ve örnek bir çalışma sunulmuştur.

Anahtar Kelimeler: Ağ Planlaması, Hiyerarşik Ağ Topolojisi, İş Sürekliliği, Ağ Güvenliği, Ağ Protokolleri.

*Corresponding Author: veli.capali@usak.edu.tr

Veli ÇAPALI, https://orcid.org/0000-0002-9045-0210
Ömer Faruk SAĞBAŞ, https://orcid.org/0000-0001-8183-950X
Kerim KARABAŞ, https://orcid.org/0000-0003-3068-6018
Kadir SÜMER, https://orcid.org/0000-0003-0994-7340

1. Introduction

Network capacity planning for institutions and organizations requires the correct placement of network resources to meet potential traffic demands and network failure scenarios. The network capacity planning process is based on very long planning cycles (e.g. annual, three-year). This is due to the inflexible nature of existing networks and areas where the topology will be applied. The inflexible main structure consists of the transport layer (fiber optic and ethernet). The protocol layer, on the other hand, should have a more dynamic and flexible structure by nature. In addition to these layers, all failure scenarios required for the estimated traffic and protection of the planned network should also be analyzed. While planning the network for possible scenarios, spare capacity planning should also be done. While planning, it is necessary to radically transform existing management architectures and create new generation flexible and manageable architectures to benefit from existing capacity, increase dynamism and create management systems in networks [1].

Expert engineers in the creation of next-generation architectures use hierarchical network models in planning and designing the network. Network installation engineers need to clearly present and explain the design of the network to determine which devices will be placed in the designed network. Likewise, network administrators and technical personnel should know the design of the network and the devices used very well to eliminate potential problems. Today, applications that are used jointly by both students and staff, especially in large campus networks, directly affect the density of the network. For this reason, it is necessary to use more effective routing and switching devices and technologies by making good planning [2]. It is not sufficient to use only network density and user statistics during this planning period. It is necessary to create a redundant architecture to provide uninterrupted service and to ensure business continuity. While planning, business continuity and risk analyzes should be done well. According to the analysis results, N+1 and/or 2N+1 network redundancy should be provided.

Network redundancy is a simple concept to understand. If the entire system fails in the topology you set up, in the event of a single point of failure, then you have nothing to rely on. Such situations require an access method with secondary (or tertiary) points and the use of main connection resources with a secondary system [3]. This is a situation that increases the uptime of the entire system but incurs a cost. There are different types of redundancy depending on the cost-performance-risk trio. For example, N+1 redundancy is when a backup of the same system is passively in the design and is activated in a way that can fulfill all functions in case of any interruption. N/2 redundancy, on the other hand, means that less equipment is spared in terms of performance by calculating the risks of the parts in the existing system separately. Here, the performance of the standby system is lower, but it is also more advantageous in terms of cost [4]. This cost-performance-risk triad should be analyzed correctly and planning should be done according to the needs. Otherwise, both the costs will increase, and the risk may become unbearable. In addition to this situation, the performance and security of a network is also very important. In investments to be made, performance and security come to the fore at least as much as redundancy and are among the factors that increase costs. Correct analysis of the needs and proper planning will prevent both time and financial losses.

In this study, the approach, and suggestions on how to create a redundant and hierarchical network system in large campus areas with multiple users for universities and a study carried out for the Süleyman Demirel University campus are presented.

2. Network Topology Planning

In the planning phase, the "System Development Lifecycle", which is widely used around the world and developed by Cisco, was used. PDIOO consists of the initials of the English words Plan, Design, Implementation, Operation and Optimization [4], [5]. PDIOO life cycle is given in Figure 1.

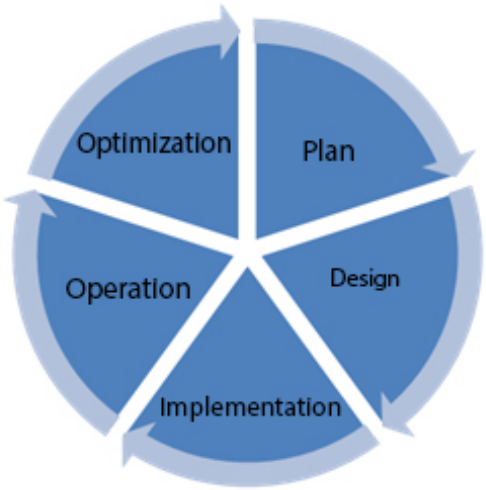

Figure 1. PDIOO System Development Lifecycle [5].

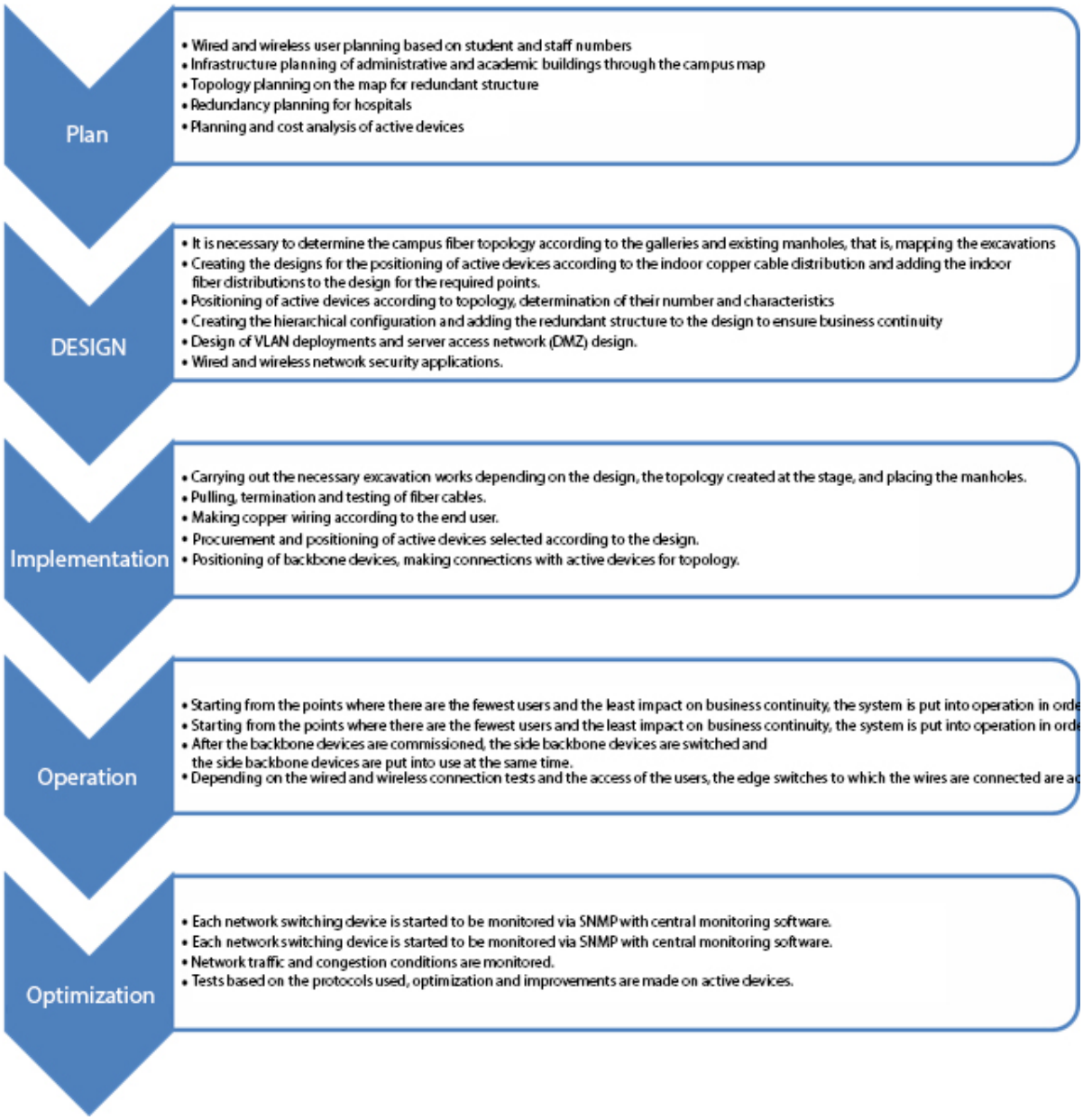

Figure 2. Süleyman Demirel University PDIOO application.

In the planning phase, the needs and the current situation are analyzed. The plan of the area to be applied is drawn and the analysis processes are completed according to the number of users and the network services to be provided over this plan. Taking advantage of the results of the analysis, the design phase is started. During the design phase, topology planning, network protocols to be used and network switching devices are decided according to the needs analysis with the technical team. Network switching devices must be capable of meeting long-term needs and supporting all application-required protocols. Likewise, at this stage, the right cabling should be selected, and infrastructure designs should be created according to the area plan to be applied. Infrastructure designs should be designed to use the existing galleries and manholes at the maximum level. Excavation and the creation of new manholes both prolong the application process and increase costs.

After the design process is completed, the installation and application process begins. In this process, fiber shooting, fiber termination, positioning of active network devices and testing processes are carried out with experienced field personnel, adhering to the design. The systems whose installation processes are completed should be put into use in order. The entire system should not be commissioned at once. By selecting the pilot areas, commissioning is done in parts in accordance with the business plan. As the systems are commissioned, the monitoring and optimization process begins with the monitoring of active devices and the monitoring of network packet traffic. Received data is analyzed and necessary optimization processes are performed on active devices. All these processes continue in cycles. PDIOO application and procedures for Süleyman Demirel University are given in Figure 2.

2.1. Determining Network Protocols

Network protocols that will operate on network switches are one of the important factors that fundamentally affect the design of a network. These protocols directly affect the speed and structured data transfer capability of the planned network. Users may encounter problems such as slowness in a network that is not configured with the correct protocols. Protocols suitable for the created topology should also be used. Some protocols used in a network structure established in a parallel and hierarchical structure for business continuity are given in Table 1.

Table 1. Network protocol table [6], [10].

Protokol	Adı	Özelliği
STP	Spanning-Tree protocol	It is a protocol that prevents loops that may occur during the communication of network switches.
VTP	VLAN Trunking Protocol	It is the second layer messaging protocol used to ensure consistency in the VLAN configuration of active devices in the network where common management is made. It manages VLAN addition, deletion and name change in multi-network switch environment.
VRRP	Virtual Router Redundancy Protocol	It is a protocol that allows multiple routers to act as a single virtual router. It is the protocol used for redundancy.
GLBP	Gateway Load Balancing Protocol	It is a business continuity redundancy network protocol that performs load balancing.
SMLT	Split Multi-link trunking	It is a split multilink channel networking protocol for both L3 and L2 that enables the exchange of information between peer nodes in a switch set for flexibility and simplicity.
DVRP	Distance-vector routing protocol	It is defined as the periodic transmission of a copy of the routing table to the router in its neighbourhood. Each router adds the distance vector value obtained as a result of the algorithm to the routing table and forwards this table to its neighbor router. Thus, while forwarding packets from one point to another, it chooses the routes with the smallest distance vector value in the routing tables, and in this way, the most suitable route between two points in the network is determined.
RIP	Routing Information Protocol	It is one of the remote vector routing portals. By calculating the number of hops (the number of passages) makes path selection with metric values.
PFC	Priority-Based Flow Control	PFC allows for prioritization of network traffic that requires lossless throughput, while other types of traffic that do not require PFC or perform better without PFC are the protocol that allows data to be transported normally.
DCB	Data center bridging	Multi-Switch Link Aggregation Groups (M-LAG) is a protocol that can address bandwidth limitations and improve network resilience, in part by routing network traffic around bottlenecks, reducing the risk of a single point of failure, and allowing load balancing between multiple switches.
MPLs	Multi-Protocol Label Switching	MPLS provides the ability to implement multi-service networks and improve network resilience. The MPLS protocol suite is a protocol whose services enable common fast redirection protocols to work together to support local convergence around the network failure.
LACP	Link Aggregation Control Protocol	It is a link aggregation technology that is used in network switches. Negotiations required for link aggregation are dynamically provided by protocols. It is used to increase bandwidth and provide redundancy of lines.
SNMP	Simple Network Management Protocol	Fault conditions, temperature, performance and used port conditions etc. from active network devices. It is the protocol used to receive and manage data such as
NTP	Network Time Protocol	It is a protocol that automatically receives time data from the date time server of active network devices over the network and provides current timing and time synchronization.

The protocols in Table 1 are currently supported or operated by almost many network switching devices. Although some protocols have different names due to the software developed by the

manufacturers of network switching devices, they perform the same function. At this point, it is important to create the right topologies for these protocols to work optimally and to run the packet traffic of active devices efficiently according to these protocols. Different active network devices and protocols are used in each layer. While some protocols are used only in backbone layer devices, some protocols are used in network devices in distribution and access layers [6].

2.2. Determining Network Security Strategies

Another important aspect in planning processes is the security of the campus network. For the campus network, which is a private network, there are many problems in its management due to the large number of users (approximately 50,000 users including students and staff) and the wide coverage of the network. Studies to solve these problems are generally divided into two parts. These are access to server systems and user security. Access to and from the campus should be defined and regulated. Access layers should be created for connections and access to these layers should be provided with authorization definitions and user authentication systems. In general, the basic structures in Figure 3 and described below should be established for campus network security.

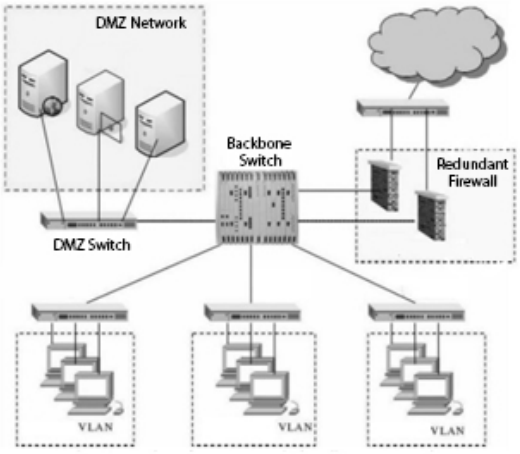

Figure 3. Topology for network security application [9].

Firewall: The overall security of the campus network, external and internal, depends on the firewall. The firewall may have a single point function depending on the campus topology, or the main firewall is at least two backups in terms of business continuity policy and redundancy. The two firewalls should be placed on different locations to work together. While the Intrusion Detection system (IDS) performs the identification and logging of malicious activity in the network, the Intrusion Prevention System (IPS) is software used to detect and prevent malicious activity or malicious links in network traffic. New generation firewall devices do not only work on a port basis like old generation devices, but also have IPS, IDS, virus protection, application security, etc. on them. contain structures.

Demilitarized Zone (DMZ): The purified network/zone for system servers is the private network created on today's firewalls, and these networks are special zones where outside

access is restricted. The main responsibility of this area is to deny unauthorized access. By switching to this network with strict rules and access control, users benefit from server services.

VLAN Planning: A virtual local area network (VLAN) is created by logically grouping network users and resources on a local area network (LAN) and assigning ports on the switching device. Types of users, buildings, floors, etc., in large campus networks. Due to the large number of structures, the management of the network is very difficult by the network administrators. With VLAN configuration, this management challenge is eased by logical separation of networks. With the logical separation of networks, a rule-governed system is provided for each network. With the use of VLAN, the security vulnerability that occurs in that logical network does not affect all networks, within the rules, and the solution process is carried out more quickly by the network and / or security administrators. In addition, switching devices can be used for management, etc. Unauthorized access to active devices is restricted by logically isolating the networks for their operations.

Network Access Control (NAC): These are the systems that allow the devices to enter the network in accordance with the rules determined by the network administrator by controlling the authorization and permission controls of the user devices that want to be included in the network using the 802.1x protocol, through the identity management system. Thanks to these systems, unauthorized access is restricted and not everyone can join the network.

Data Loss Prevention (DLP): It is a type of network data protection that is considered partially new in the field of network security and is increasing in use day by day. With DLP software, the output of unwanted data in the network can be prevented or the usage status of the determined file types can be monitored. DLP software is different from firewall and antivirus software. DLP software, as data is updated in an active multi-user system, the system must check and update the rules created for new data. DLP reports should be checked regularly, and new rules added as necessary. New reports should be created for each new rule added, and the flow of the system should be checked from these reports and rearranged. DLP software, which requires extensive work, will increase the security level within the network to a very high level, and it is a system that is very important in protecting the data of institutions and organizations.

Security Information and Event Management (SIEM): It is a management solution for threat detection, risk prevention, and cybersecurity applications for networks. These systems are It is a software that collects and processes logs and event data generated by all users, servers, network devices and firewalls in order to monitor and analyze all security-related events in the network structure [7].

Another point in ensuring network security; the correct configuration of active devices used. It is necessary to use up-to-date versions of protocols and software supported by the devices, and the ones with higher security than management protocols (SSH instead of Telnet, SNMP V3

instead of SNMP V1 etc.) should be preferred. Although an isolated network is used for the management of active devices, it is necessary to apply IP restrictions for accessing the management interfaces of the devices, and to keep track records on separate data storage areas and servers on a regular basis.

Against network attacks (DHCP Snooping, ARP Poisoning, etc.) originating from user devices in multi-user wide networks such as university campuses, it is necessary to make the necessary configurations on the switching devices. In this way, malicious packet traffic caused by one and/or more than one device is prevented, and other users are not affected by this situation.

2.3. Determination of Network Management Strategies

For network administrators today, understanding the performance and effectiveness of networks is critical to business success. At the same time, the widespread adoption of network applications, the smooth transmission of business-critical data over the same network, and the increase in performance values have increased its importance with the increasing use of mobile devices today. To provide a problem-free and uninterrupted service, the speed of response to errors is important and the determination of network management strategies plays a major role at this point. In determining the network management strategy used in our university, ISO resources, which have a major role in determining international standards, were used. FCAPS (fault-management, configuration, accounting, performance, and security) as determined by ISO model, this strategy is divided into five main areas. These fields are indicated in Table 2[8].

Table 2. FACAPS Parameters [8].

FCAPS	Explanation
Fault	Errors that occur in the network. The main purpose of error management is to detect, isolate, record and correct the error.
Configuration	It is the process of determining the operations that devices should do on the network with the management protocols of the devices and the configuration file / command strings.
Accounting	Management of data retention of consumption values of users, network usage. An example of this would be to charge the amount used by individual users.
Performance	Network performance management directly covers improving the efficiency of the network.
Security	Security management takes over the management of securing the network. We can think of its main targets as denial-of-service attacks, prevention of hackers, prevention of viruses, malware, etc. threats.

The network management architecture being used in our institution is given in Figure 4 below.

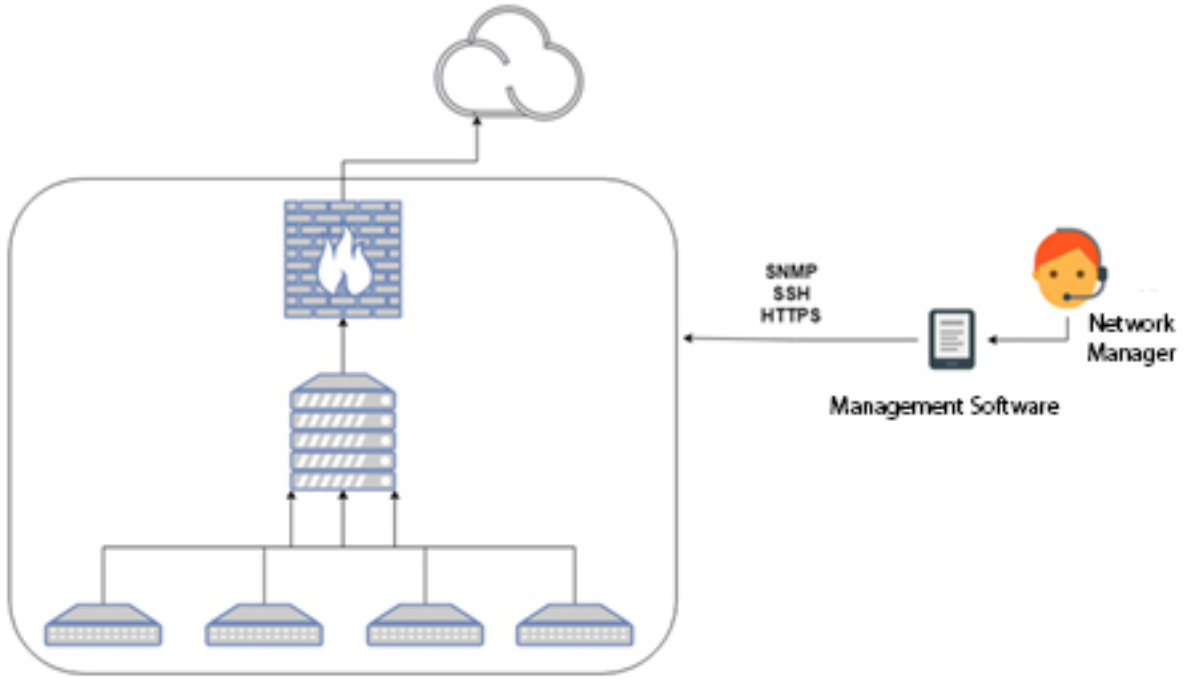

Figure 4. Network management architecture.

3. Redundant Network Topology Implement

In the campus redundant network topology application, 96 core single mode fiber cables were first installed between two separate data centers in the east and west campuses. Afterwards, 24 cores were connected to the data centers in their own campuses with single mode fiber from each edge point located in the eastern and western campuses. In order to ensure the redundancy of the edge assembly points in both campuses; Two separate main connections were made from the points in the eastern campus to the west, and from the points in the western campus to the east by making a single jump over the 96-core single mode fiber cable. Thus, each edge point is directly connected to two different data centers with fiber cables. The drawing in Figure 5 shows the fiber distribution and the redundant connection scheme of each point in the campuses.

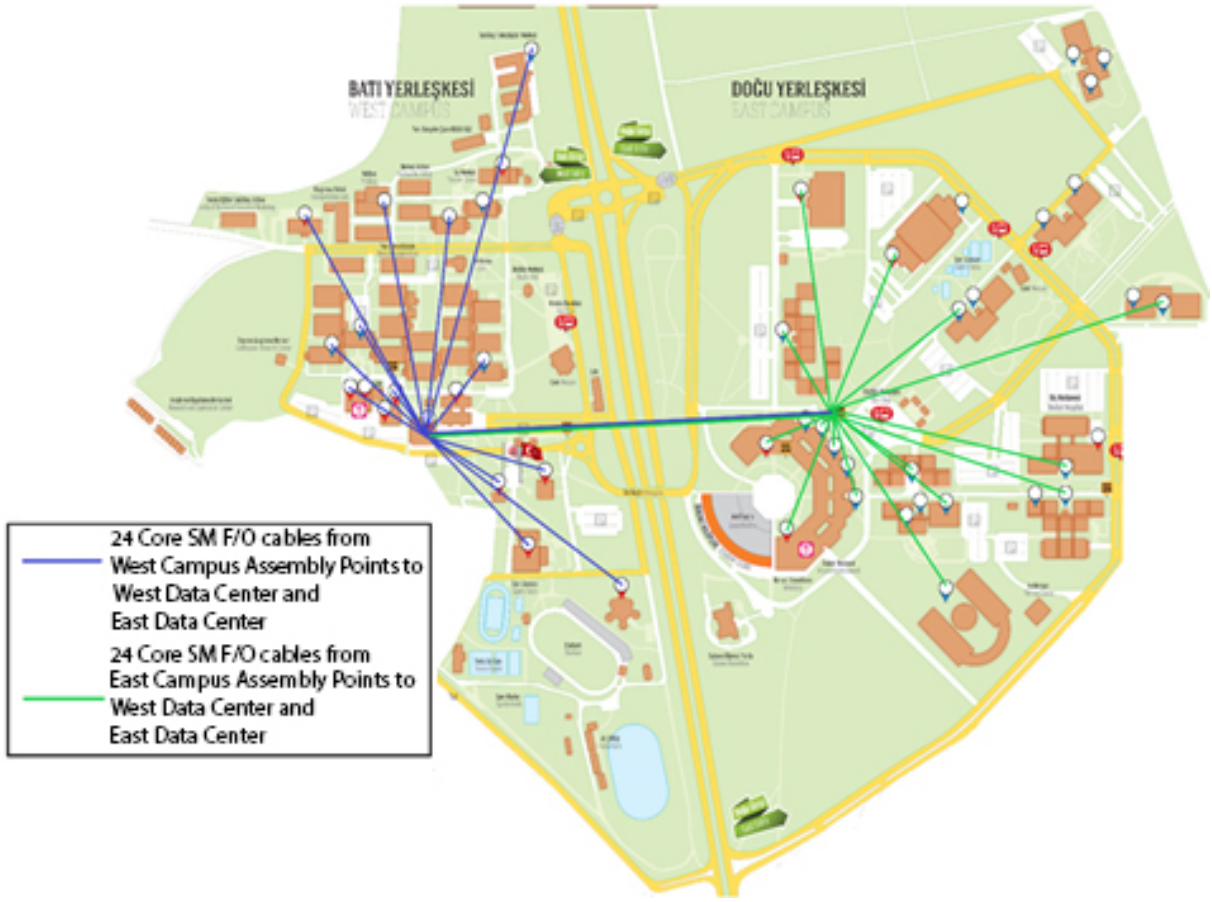

Figure 5. West and East campus fiber topology.

All fiber and copper cabling operations, fiber termination, fiber and copper cable testing operations are carried out by the personnel of Süleyman Demirel University Information Processing Department within the campus. All fibers drawn in accordance with the planned topology are terminated with a "Fujikura 70s" brand and model fusion device. After the termination process, testing processes are carried out with “Viavi Smart OTDR E126b” brand and model device for connector control and fibers. In Figure 6, the measurement performed with the OTDR device is given. Thus, loss conditions and robustness of fibers are tested and reported in digital environment. Table 3 shows the measurement and test results of the fibers drawn and terminated according to the new topology. According to the measurement values, it is decided to re-terminate and/or retract the fiber cables.

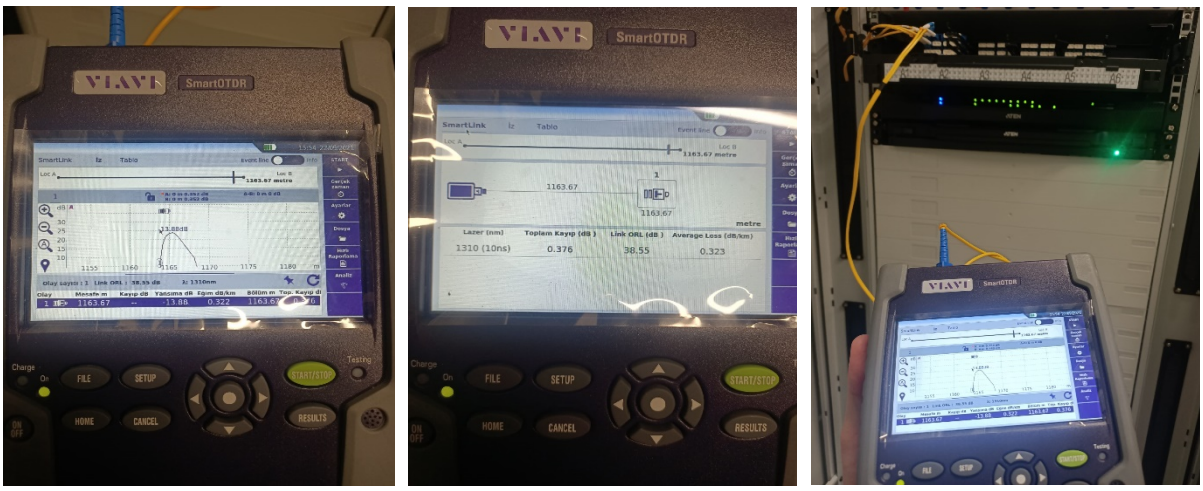

Figure 6. Fiber measurement operations performed with the OTDR device.

Table 3. OTDR results of fiber cables drawn according to the new topology.

Units	F/O Length (m)	Total Loss (DB)	Link ORL (DB)	Avr. Loss (DB/KM)
Fibers from West Campus Edge Points to West Data Center				
Rectorate Building	264,94	1,60	38,66	1,27
Faculty of Engineering- E4 Block	292,45	1,01	38,56	0,78
Faculty of Engineering- E7 Block	189,86	1,42	38,07	1,19
Faculty of Engineering- E13 Block	297,30	1,68	38,51	1,29
Faculty of Architecture	640,70	1,00	37,66	0,61
West Campus Center Classrooms	296,86	1,44	36,95	1,11
Yetem Building	937,04	2,17	36,96	1,12
Department of Administrative and Financial Affairs	157,35	1,07	38,70	0,93
Department of Construction Works	536,37	1,27	37,93	0,83
Cultural Center	286,01	1,05	38,48	0,81
Erasmus Building	1105,13	1,86	36,98	0,88
Career Center	1047,57	1,98	36,98	0,97
Fibers from East Campus Edge Points to East Data Center				
Faculty of Arts and Sciences	363,12	1,46	38,41	1,07
Faculty of Education	872,34	1,59	37,89	0,85
Faculty of Theology	616,37	2,13	36,27	0,81
Faculty of Economics and Administrative Sciences	877,90	2,04	37,43	1,09
Faculty of Law	462,72	1,55	38,09	1,06
Faculty of Fine Arts	423,93	0,93	38,25	0,65
Morphology Building	644,12	1,06	37,63	0,65
Faculty of Dentistry	631,04	1,91	37,84	1,17
Institutes Building	361,54	1,62	38,24	1,18
Swimming Pool	641,69	1,86	37,78	1,13
East Gym	865,22	1,79	37,34	0,96
Library Building	329,97	0,89	38,36	0,67

Hospital Building	889,59	1,68	37,32	0,90
96 Core SM Fibers Pulled Between West and East Data Centers				
Between West/East Data Center	1163,67	0,38	38,55	0,32

Figure 7 shows the connection topology of on-campus redundant network switching devices. A backbone network switch has been placed in each of the western and eastern campuses. Backbone network switches are connected to each other with 40Gbps + 40Gbps QSFP+ fiber as redundantly in two different ways, and backbone redundancy is created in 80Gbps bandwidth. Afterwards, each edge point (edge aggregation points located in faculties and administrative buildings) located in the eastern and western campuses was configured with a point-to-point 40Gbps QSFP+ fiber connection to the data centers. Two separate main connections are provided from the side assembly points in both campuses. One of these connections to the east data center and the other to the west data center are provided with fiber cables.

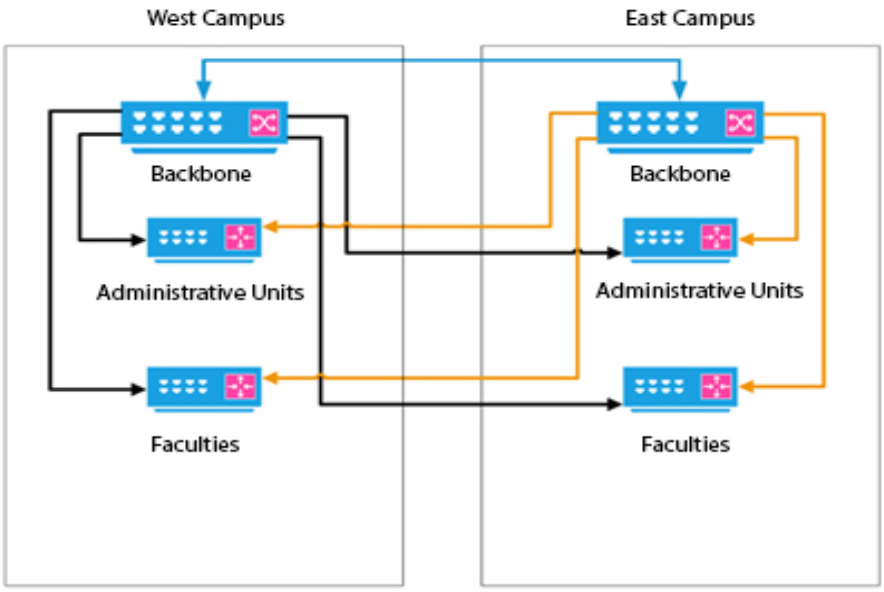

Figure 7. West and East campus switch connection topology.

Active/passive port application and port link aggregation (LACP-LAG) protocols were used on the main backbones and distribution switches in the East and West campuses of Süleyman Demirel University, as indicated in Figure 7. It is to use the ESRP protocol for load balancing on the backend connections from the access layer to the distribution layer. ESRP is a protocol like GLBP and HSRP. Also, default gateways to access layer devices are deployed with round-robin algorithm. This allows endpoints to send traffic to one of the two distribution nodes. In this way, active/passive redundancy is ensured in both the main backbones and distribution switches connected to the main backbones. In addition to these, Network switches that provide power over Ethernet (POE) at edge points for IP phones and wireless access points, and network switching devices that use redundant power supplies for backbone and distribution switches are

preferred. In addition, for network security; Tools such as 802.1x port security, DHCP snooping, dynamic ARP control, and IP resource protection are used.

4. Result and Discussion

Süleyman Demirel University's business continuity-oriented hierarchical network topology application example is presented in general terms. The business continuity situation mentioned in the network topology planning stage, the controls made after the transfer of data between the backbone and edge network devices and the creation of active-passive redundancy, have been tested with the scenarios for failure and maintenance situations and the operation of hierarchical systems. the adequacy of the structure has been revealed. The following results were obtained with this study.

- Ensuring that users are not affected by the long-term maintenance of the university in general.
- Providing a redundant connection with 40Gbps network connection to two different data centers for each building located in different campuses within the university.
- Providing redundant 10Gbps backend connectivity for each edge switch.
- Ensuring the minimization of service downtime.
- It was ensured that the efficiency of users' internet connection and access to automation systems were increased.

Having implemented this study at the Süleyman Demirel University campus has greatly contributed to the acceptability of its results, and this design will be an example for other institutions and organizations with large-scale networks. In addition to these studies, future studies are outlined below. By carrying out these studies, adding new systems will both expand the scope of this study and increase network security.

- Network access control device (NAC) installation and use.
- Establishment and implementation of data loss prevention (DLP) systems.
- Establishment and use of security information and event management (SIEM) systems

Ethics in Publishing

There are no ethical issues regarding the publication of this study

Acknowledgement

We would like to thank the Department of Information Processing of Süleyman Demirel University for their support during the implementation phase of this study.

Conflict of Interest

No conflict of interest was declared by the authors.

References

[1] Velasco, L., Castro, A., King, D., Gerstel, O., Casellas, R., Lopez, V. 2014. In-operation network planning. IEEE Communications Magazine, 52(1), 52-60.

[2] Clark, K., Hamilton, K., 1999. Cisco LAN Switching (CCIE Professional Development series). Cisco Press.

[3] TechGenix, 2022. https://techgenix.com/importance-network-redundancy, (Erişim Tarihi: 30.04.2022).

[4] Turunç, M., 2012. Paralel Hiyerarşik Dizayn Metodolojisi Kullanarak Şirket Binalarının Network Ve Alt Yapı Projelerinin Dizaynı. Yayınlanmış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, Türkiye.

[5] Oppenheimer, P., 2011. Top-Down Network Design, Indianapolis: Cisco Press.

[6] İTÜ BİDB, 2022. https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vlan-t%C3%BCrleri, (Erişim Tarihi: 1.05.2022).

[7] Bulutistan, 2022. https://bulutistan.com/blog/siem-nedir, (Erişim Tarihi: 1.05.2022).

[8] CIO-WIKI, 2022. https://cio-wiki.org/wiki/Fault_Configuration_Accounting_Performance_Security_(FCAPS), (Erişim Tarihi: 1.05.2022).

[9] Huang, M., Luo, W., & Wan, X., 2019. Research on Network Security of Campus Network. In Journal of Physics: Conference Series 1187(4), 1-6.

[10] Sahoo, K., Goswami, J. B., 2014. Redundancy Protocols For Campus Network. International journal of science invention today, 3(6), 611-624.