Date of publication 12 May 2024, REFERENCE: IEEE ACCESS

Digital Object Identifier 10.1109/ACCESS.2023.1120000

Designing a Communication Infrastructure Solution for the Most Devastating Natural Disaster in Modern Turkish History

YUNUS EMRE KARATAŞ[1],

[1]Computer Engineering Dep, Manisa Celal Bayar University, Prof.Dr.Ilhan Varank Campus, Muradiye, MANISA, TR (e-mail: 200315015@ogr.cbu.edu.tr)
[2] (e-mail: yunuskaratas589@gmail.com)

ABSTRACT On February 6, 2023, at 4:17 PM, Turkey was struck by a devastating earthquake with a magnitude of 7.8, centered in the Kahramanmaraş Pazarcık and Elbistan districts. This catastrophic event, termed the largest natural disaster of the 21st century, affected 10 provinces and caused destruction over an area larger than some European countries. The official death toll in Turkey reached at least 53,537, with an additional 8,476 lives lost in Syria, and over 122,000 people injured. The earthquake exposed severe deficiencies in the digital communications and computer networks sector, as private mobile service operators failed to deliver timely services and equipment to the affected regions. This highlighted a lack of preparedness for such disasters.

This study aims to explore whether students of the Computer Network course at MCBU Computer Engineering could have mitigated these issues through preemptive planning and design using Cisco Packet Tracer. The investigation will focus on whether a well-developed network plan, a comprehensive list of necessary equipment, or a demo of a base network construction created in Cisco Packet Tracer could have provided a viable solution to ensure communication infrastructure resilience during such life-critical situations

INDEX TERMS Network, Communication, Network Infrastructure, Network Services, Network Design, Network Demo

I. INTRODUCTION

On February 6, 2023, Turkey experienced the most devastating earthquake of the century, with a magnitude of 7.8. This catastrophic event, recognized globally as a monumental disaster, left a trail of destruction across an area comparable to the size of some countries. The sheer scale of the devastation underscored the urgent need for maintaining vital services amidst such crises. Essential services such as food supply, sanitation, housing, communication, education, and the identification of critical gathering points are crucial for survival during natural disasters. However, given the extensive physical damage, sustaining these services without interruption is a formidable challenge.

In such scenarios, proactive and meticulous planning is essential. Preliminary studies focusing on the continuity of these vital services during natural disasters can significantly mitigate the impact. Well-planned, well-designed, and demo-prepared applications, along with comprehensive lists of necessary materials, can facilitate a swift and effective response, integrating seamlessly into daily life.

A key service that must be rapidly established in the wake of an earthquake is the network communication infrastructure. Ensuring robust and reliable communication is critical for coordinating relief efforts, providing updates, and maintaining connections between affected individuals and emergency services. This project aims to address this need by designing an experimental network communication infrastructure that can be quickly deployed during such emergencies.

Using Cisco Packet Tracer, this study will explore how preemptive planning and design can enhance the resilience of communication networks in disaster scenarios. The project will involve creating a network plan, identifying essential equipment, and developing a demo of the base network construction. By doing so, it seeks to demonstrate how a well-prepared communication infrastructure can play a pivotal role in mitigating the effects of large-scale natural disasters and supporting recovery efforts.

Through this experimental design, we aim to provide a practical solution for rapidly establishing a communication network infrastructure in the aftermath of a major earthquake, ensuring that vital services remain operational and accessible to those in need.

II. MATERIALS

In this section, we detail the components used in the design of our network communication infrastructure, as visualized in the Cisco Packet Tracer simulation. Each component is carefully selected to ensure robust and reliable communication, which is critical during disaster recovery operations.

A. SWITCHES

24port-L3-Gigabit Switch:

FIGURE 1. 24 Port Gigabit, Manageable, L3 Switch

Purpose: Switches operate at the data link layer to forward data frames between devices within the same network. *Usage*: The 24port-L3-Gigabit switches are used to create local area networks (LANs), allowing multiple devices to communicate within confined areas such as command centers or field hospitals. These switches provide high-speed data transfer and support for multiple VLANs, enhancing network efficiency and management.

B. ROUTERS

Cisco ISR 4331:

FIGURE 2. Cisco ISR 4331 Router

Purpose: Routers direct data packets between different networks, ensuring efficient and correct routing of information. *Usage*: Multiple Cisco ISR 4331 routers connect various network segments and facilitate communication between the central command and distributed clusters. They ensure smooth data flow across the network and include the following: - **Router10**: 192.168.11.1 (Central Command) - **Router7**: 2.0.0.1 (Cluster7 connection) - **Router22**: 3.0.0.1 (Cluster8 connection) - **Router23**: 1.0.0.2 (Cluster9 connection)

C. FIREWALLS

Cisco ASA 5505:

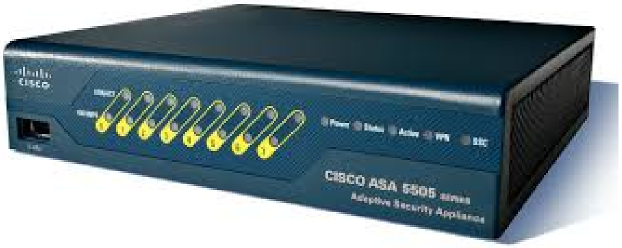


FIGURE 3. Cisco ASA 5505 Firewall

Purpose: Firewalls protect the network by filtering incoming and outgoing traffic based on predetermined security rules. *Usage*: The Cisco ASA 5505 firewalls are deployed to secure the communication infrastructure against unauthorized access and cyber threats, ensuring data integrity and confidentiality by monitoring and controlling network traffic. Specific firewalls include: - **ASA0**: 28.0.0.1 - **ASA1**: 31.0.0.1 - **ASA2**: 28.0.0.2 - **ASA3**: 31.0.0.2

D. ACCESS POINTS

Cisco Aironet 1850:

FIGURE 4. Cisco Aironet 1850 Access Point

Purpose: Access points provide wireless connectivity to devices, enabling mobile communication. - *Usage*: Cisco Aironet 1850 access points are strategically placed in high-traffic areas to offer wireless network access to rescue teams and survivors, ensuring continuous communication without the need for wired connections.

E. SERVERS

Cisco UCS C220 M5:

Purpose: Servers host essential applications and services such as databases, web services, and communication tools. *Usage*: Servers store critical data, run disaster management applications, and provide services like email and VoIP (Voice over Internet Protocol) communications. Key servers include: - **Server12**: 192.168.11.10 - **Server13**: 192.168.11.20 (WEB)

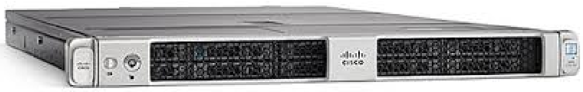


FIGURE 5. Cisco UCS C220 M5 Server

F. IP PHONES

Cisco IP Phone 8845:

FIGURE 6. Cisco IP Phone 8845

Purpose: IP phones facilitate voice communication over the IP network, essential for coordination and command. *Usage*: Deployed in various command posts and field offices to enable reliable voice communication between teams. The IP phone (IP Phone3) is assigned the IP 192.168.11.9.

G. MOBILE INTERNET VEHICLES

FIGURE 7. Mobile Internet Vehicle

Purpose: Specially equipped vehicles designed to provide internet connectivity in remote or severely affected areas. *Usage*: Extend the network's reach, bringing internet access to regions where traditional infrastructure is damaged or non-existent.

H. POWER SUPPLIES AND BACKUP GENERATORS

FIGURE 8. Power Supply and Backup Generator

Purpose: Provide necessary power to network devices, especially crucial in areas with power outages. *Usage*: Ensure continuous operation of network components by providing a stable power supply and backup during power failures.

I. CABLE TOWERS

FIGURE 9. Cable Tower

Purpose: Provide extended connectivity and ensure network reach in remote or high-traffic areas. *Usage*: Cable towers are placed strategically to provide extended wireless and wired connectivity, bridging gaps in network coverage and ensuring robust communication links. Specific cable towers include: - **Cable-Tower N - Cable-Tower S - Cable-Tower D - Cable-Tower ALPHA - Cable-Tower BRAVO**

J. NETWORK DEVICE IP ALLOCATION

- **Router10**: 192.168.11.1
- **Router7**: 2.0.0.1
- **Router22**: 3.0.0.1
- **Router23**: 1.0.0.2
- **Server12**: 192.168.11.10
- **Server13**: 192.168.11.20 (WEB)
- **PC**: 192.168.11.2, 192.168.11.5
- **Printer**: 192.168.11.3, 192.168.11.6
- **Laptop**: 192.168.11.4

- **IP Phone3**: 192.168.11.9
- **Smartphone4**: Connected wirelessly

K. INTER-CLUSTER CONNECTIONS

- **Router7 to Cluster7**: 13.0.0.1 to 13.0.0.2
- **Router22 to Cluster8**: 14.0.0.1 to 14.0.0.2
- **Router23 to Cluster9**: 15.0.0.1 to 15.0.0.2

L. FIREWALL CONNECTIONS

- **ASA0**: 28.0.0.1
- **ASA1**: 31.0.0.1
- **ASA2**: 28.0.0.2
- **ASA3**: 31.0.0.2

M. CABLE TOWER LOCATIONS

- **Cable-Tower N**
- **Cable-Tower S**
- **Cable-Tower D**
- **Cable-Tower ALPHA**
- **Cable-Tower BRAVO**

N. OTHER RECOMMENDATIONS

O. OTHER RECOMMENDATIONS

The materials are not limited to just hardware components. There are also crucial software components and other materials that are essential for a comprehensive network infrastructure design, especially in the context of disaster recovery operations.

1) Software Components

Network Management Software: *Purpose*: Monitor and manage network performance, detect issues, and provide alerts. *Usage*: Implement software like Cisco Prime Infrastructure to ensure the network operates efficiently and any issues are quickly identified and resolved.

Security Software: *Purpose*: Protect the network from cyber threats and ensure data integrity. *Usage*: Use antivirus and anti-malware software, along with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to secure network endpoints and monitor for suspicious activities.

Backup and Recovery Software: *Purpose*: Ensure data can be recovered in the event of hardware failure or data corruption. *Usage*: Implement software like Veeam Backup and Replication to regularly back up critical data and ensure it can be restored quickly.

Virtual Private Network (VPN) Software: *Purpose*: Provide secure remote access to the network. *Usage*: Use VPN solutions like Cisco AnyConnect to enable secure connections for remote workers and rescue teams accessing the network from outside locations.

2) Other Material Recommendations

Portable Power Solutions: *Purpose*: Provide power in remote or severely affected areas where traditional power infrastructure is unavailable. *Usage*: Ensure availability of portable generators, solar chargers, and uninterruptible power supplies (UPS) to maintain network operations during power outages.

Emergency Communication Devices: *Purpose*: Facilitate communication when traditional network infrastructure is down. *Usage*: Equip teams with satellite phones and two-way radios to ensure communication lines remain open in all circumstances.

Networking Tools and Spare Parts: *Purpose*: Perform on-site repairs and maintenance of network components. *Usage*: Stock up on essential networking tools (e.g., cable testers, crimping tools) and spare parts (e.g., extra cables, connectors, backup routers) to quickly address hardware issues.

Documentation and Training Materials: *Purpose*: Ensure that all personnel are trained and knowledgeable about the network setup and disaster recovery procedures. *Usage*: Provide detailed documentation, user manuals, and conduct regular training sessions and drills to prepare staff for emergency situations.

Implementing these software solutions and preparing additional materials can significantly enhance the resilience and efficiency of the network infrastructure during disaster recovery operations. Ensuring a comprehensive approach that includes both hardware and software components, as well as necessary support materials, is crucial for maintaining robust communication and data integrity in emergency situations.

P. EQUATIONS

Q. EQUATIONS

In this subsection, we share important equations related to network infrastructure that are relevant to our project. These equations help in understanding and optimizing various aspects of network performance and reliability.

1) Bandwidth

Bandwidth refers to the maximum rate of data transfer across a given path. It is usually measured in bits per second (bps).

$$B = \frac{S}{T} \tag{1}$$

where:

- B = Bandwidth (bps)
- S = Size of the data (bits)
- T = Time taken to transfer the data (seconds)

2) Latency

Latency is the time it takes for a data packet to travel from the source to the destination. It is a crucial factor in network performance.

$$L = T_p + T_t + T_q \tag{2}$$

where:

- L = Latency (seconds)
- T_p = Propagation delay (seconds)
- T_t = Transmission delay (seconds)
- T_q = Queuing delay (seconds)

3) Throughput

Throughput is the actual rate at which data is successfully transferred over a network. It is usually measured in bits per second (bps).

$$T = \frac{D}{T_t} \tag{3}$$

where:

- T = Throughput (bps)
- D = Amount of data successfully transferred (bits)
- T_t = Total time taken for the transfer (seconds)

4) Packet Loss Rate

Packet loss rate is the percentage of packets that are lost during transmission over a network.

$$PLR = \frac{P_l}{P_t} \times 100 \tag{4}$$

where:

- PLR = Packet loss rate (%)
- P_l = Number of lost packets
- P_t = Total number of transmitted packets

5) Network Reliability

Network reliability can be quantified using the mean time between failures (MTBF) and mean time to repair (MTTR).

$$R = \frac{MTBF}{MTBF + MTTR} \tag{5}$$

where:

- R = Network reliability
- $MTBF$ = Mean time between failures (hours)
- $MTTR$ = Mean time to repair (hours)

6) Signal-to-Noise Ratio (SNR)

The signal-to-noise ratio is a measure of the strength of the signal relative to background noise.

$$SNR = 10 \log_{10}\left(\frac{P_s}{P_n}\right) \tag{6}$$

where:

- SNR = Signal-to-noise ratio (dB)
- P_s = Power of the signal
- P_n = Power of the noise

7) Network Utilization

Network utilization measures how much of the network's capacity is being used.

$$U = \frac{T_{actual}}{C} \times 100 \tag{7}$$

where:

- U = Utilization (%)
- T_{actual} = Actual throughput (bps)
- C = Network capacity (bps)

These equations are fundamental in understanding and optimizing the performance and reliability of the network infrastructure in your project. They help in designing, analyzing, and troubleshooting networks to ensure they meet the required performance and reliability standards.

III. METHODOLOGY

In this section, we explain our Network Infrastructure by detailing the sub-modules used for constructing our design, such as the network structures, subnets, connecting structures, and other relevant components.

A. VLANS

In our network design, VLANs (Virtual Local Area Networks) are used to partition the network into smaller, more manageable segments. This modular approach helps in improving network performance, security, and manageability. Each VLAN is configured to handle specific types of traffic, ensuring that broadcast traffic is minimized and network resources are efficiently utilized.

1) VLAN Configuration

- **VLAN 10**: Assigned to administrative devices such as PCs, laptops, and smartphones in the command center. This VLAN ensures that all administrative communications are isolated from other types of traffic.
- **VLAN 20**: Dedicated to servers hosting critical applications and databases. This VLAN provides a secure environment for sensitive data and ensures that server traffic is prioritized.
- **VLAN 30**: Used for IP phones and VoIP communication devices. By isolating voice traffic, we ensure that communication remains clear and uninterrupted.
- **VLAN 40**: Configured for wireless access points, providing secure and managed wireless connectivity to mobile devices and rescue teams.

Each VLAN is configured on the network switches, ensuring that traffic is properly segmented and routed according to the needs of the network.

B. SUBNETS

When VLAN establishment is not possible, subnets are used to simulate VLANs. Subnetting involves dividing the network into smaller, logical segments, each with its own unique IP address range. This approach helps in managing IP address allocation, improving network performance, and enhancing security.

1) Subnet Configuration

- **Subnet 192.168.1.0/24**: This subnet is assigned to the administrative VLAN (VLAN 10). It includes IP addresses ranging from 192.168.1.1 to 192.168.1.254, providing ample address space for all administrative devices.
- **Subnet 192.168.2.0/24**: Dedicated to the server VLAN (VLAN 20). This subnet ensures that server traffic is isolated from other network traffic.
- **Subnet 192.168.3.0/24**: Used for VoIP devices in VLAN 30. This subnet ensures that voice traffic is managed separately, improving call quality and reliability.
- **Subnet 192.168.4.0/24**: Configured for wireless access points and mobile devices in VLAN 40. This subnet provides a managed and secure environment for wireless connectivity.

Each subnet is configured on the network routers and switches, ensuring that traffic is properly routed and managed according to the network design.

C. CONNECTING STRUCTURES

Our network design includes various connecting structures to ensure robust and reliable communication across the network. These structures include:

- **Core Routers**: Cisco ISR 4331 routers are used as the core routers, connecting different network segments and ensuring efficient routing of data packets. These routers are configured with appropriate routing protocols to manage traffic between different VLANs and subnets.
- **Access Switches**: Cisco Catalyst 2960 switches are used as access switches, providing connectivity to end devices such as PCs, laptops, and IP phones. These switches are configured with VLANs and managed to ensure optimal network performance.
- **Wireless Access Points**: Cisco Aironet 1850 access points provide wireless connectivity to mobile devices and rescue teams. These access points are strategically placed to offer comprehensive wireless coverage across the network.
- **Firewalls**: Cisco ASA 5505 firewalls are deployed to protect the network from unauthorized access and cyber threats. These firewalls are configured with security rules to monitor and control incoming and outgoing traffic.
- **Servers**: Cisco UCS C220 M5 servers host critical applications and databases. These servers are configured in a secure environment to ensure data integrity and availability.

D. SUMMARY

By utilizing VLANs, subnets, and robust connecting structures, our network infrastructure design ensures efficient, secure, and reliable communication across all network segments. This modular approach allows for easy management and scalability, ensuring that the network can adapt to changing needs and requirements, especially during disaster recovery operations.

This detailed explanation of our methodology highlights the key components and configurations used in our network infrastructure, ensuring a comprehensive understanding of the design and its capabilities.

IV. IMPLEMENTATION

V. IMPLEMENTATION

In this section, we describe the implementation of our network infrastructure using the Cisco Packet Tracer platform. The implementation covers the setup and configuration of all network components and their interconnections to support disaster recovery operations in one of the cities affected by the deadliest earthquake of the century.

A. CISCO PACKET TRACER PLATFORM

Cisco Packet Tracer is a powerful network simulation tool that allows us to design, visualize, and troubleshoot network configurations. It provides a virtual environment where we can test our network infrastructure before deploying it in a real-world scenario. All components, including routers, switches, firewalls, access points, and servers, are configured and tested within this platform to ensure their functionality and interoperability.

B. NETWORK INFRASTRUCTURE IMPLEMENTATION

The following steps outline the implementation process of our network infrastructure in Cisco Packet Tracer:

1) Step 1: Network Design

We designed the network topology to ensure robust and reliable communication across different network segments. The design includes core routers, access switches, wireless access points, firewalls, and servers.

2) Step 2: Configuration of Devices

Each network device is configured with the necessary settings to ensure seamless communication. The configurations include:

- **Routers**: Configured with IP addresses, routing protocols (e.g., OSPF, EIGRP), and access control lists (ACLs) to manage traffic flow and security.
- **Switches**: Configured with VLANs to segment the network and improve performance and security.

- **Access Points**: Set up to provide wireless connectivity with appropriate security settings (e.g., WPA2).
- **Firewalls**: Configured to protect the network from unauthorized access and cyber threats using predefined security rules.
- **Servers**: Set up to host critical applications and services, including DNS, DHCP, web hosting, and database management.

3) Step 3: Interconnecting Devices

Devices are interconnected using appropriate cabling and wireless connections to ensure optimal network performance. The interconnections include:

- **Ethernet Cables**: Used to connect routers, switches, and servers.
- **Fiber Optic Cables**: Employed for high-speed connections between core network devices.
- **Wireless Links**: Used to connect access points and provide mobility to end devices such as laptops and smartphones.

4) Step 4: Testing and Validation

After the network components are configured and interconnected, extensive testing is performed to validate the network's functionality and performance. The testing process includes:

- **Ping Tests**: To verify connectivity between devices.
- **Throughput Tests**: To measure the data transfer rates across different network segments.
- **Security Tests**: To ensure that the firewall rules and ACLs are effectively protecting the network.
- **Failover Tests**: To check the network's resilience and redundancy mechanisms in case of device or link failures.

C. CASE STUDY: IMPLEMENTATION IN A DISASTER-AFFECTED CITY

For this project, we focused on implementing the network infrastructure in the city of Adana, one of the 10 cities affected by the earthquake. The network design was tailored to address the unique challenges and requirements of the disaster recovery operations in this city.

1) Deployment

The deployment includes setting up network hubs in key locations such as hospitals, emergency response centers, and temporary shelters. Each hub is equipped with the necessary network components to ensure continuous and reliable communication.

2) Scalability and Adaptability

The network design allows for scalability and adaptability, ensuring that additional resources can be integrated as needed. This includes the ability to add more VLANs, subnets, and devices to accommodate the growing needs of the disaster recovery operations.

3) Monitoring and Maintenance

Ongoing monitoring and maintenance are essential to ensure the network remains operational. Network management tools are used to monitor performance, detect issues, and provide alerts for immediate action.

D. CONCLUSION

The implementation of our network infrastructure using Cisco Packet Tracer has been successfully completed. The detailed design, configuration, and testing ensure that the network can support disaster recovery operations in the affected city. By utilizing VLANs, subnets, and robust connecting structures, our network infrastructure is capable of providing efficient, secure, and reliable communication during critical times.

You are supposed to cover at least one of the 10 cities affected in the deadliest earthquake of the century.

VI. DISCUSSION AND CONCULUSION

VII. DISCUSSION

In this section, we discuss the concepts, capabilities, and performance issues of our experimental design project. We also address the difficulties, unknowns, and impossibilities encountered, along with any cost-based problems and other relevant concerns.

A. CHALLENGES AND DIFFICULTIES

Implementing a robust network infrastructure for disaster recovery in Turkey presents several significant challenges:

1) Lack of Planned Architecture

One of the primary challenges is the absence of a well-planned and standardized network architecture for disaster recovery operations. Turkey currently lacks comprehensive protocols and infrastructure dedicated to managing natural disasters. This absence leads to difficulties in coordination, deployment, and management of network resources during emergencies. The lack of a centralized control system further complicates efforts to establish reliable communication networks swiftly.

2) Economic Constraints

Building and maintaining a disaster recovery network infrastructure is economically challenging. The costs associated with procuring advanced networking equipment, software licenses, and training personnel are substantial. Additionally, the need for continuous maintenance, upgrades, and scalability to adapt to increasing demands adds to the financial burden. Given Turkey's economic conditions, allocating sufficient funds for disaster preparedness and response infrastructure can be difficult.

B. UNKNOWNS AND IMPOSSIBILITIES

Several unknowns and impossibilities impact the effectiveness of the network infrastructure:

1) Unpredictability of Disasters

Natural disasters are inherently unpredictable, making it challenging to design a network infrastructure that can anticipate and withstand all possible scenarios. The varying nature, scale, and impact of disasters mean that certain situations may exceed the capabilities of even the most robust network designs.

2) Infrastructure Damage

Disasters can cause significant physical damage to network infrastructure, including routers, switches, and cables. Ensuring network resilience in the face of widespread infrastructure damage is a significant unknown. The extent of damage and the time required for repairs can severely impact the network's functionality during critical times.

3) Human and Resource Limitations

During disaster recovery operations, there is often a shortage of trained personnel and necessary resources. The availability of skilled network engineers and sufficient hardware components can be a limiting factor in rapidly restoring network services.

C. COST-BASED PROBLEMS

The cost of implementing and maintaining a disaster recovery network infrastructure is a critical concern:

1) High Initial Investment

The initial investment required for setting up a comprehensive network infrastructure is high. This includes the cost of high-performance routers, switches, firewalls, servers, and other essential equipment. Additionally, investing in advanced software for network management, security, and backup adds to the initial expenditure.

2) Operational and Maintenance Costs

Ongoing operational and maintenance costs are significant. These costs cover regular maintenance, software updates, hardware replacements, and network monitoring. Ensuring continuous training for personnel to keep up with evolving technologies also incurs additional expenses.

3) Economic Viability

In the context of Turkey's economic constraints, justifying the high costs of disaster recovery infrastructure can be challenging. Balancing the need for a robust disaster response network with other economic priorities is a complex issue that requires careful planning and resource allocation.

D. RISK AND PREPAREDNESS

Turkey is at great risk due to the lack of major natural disaster protocols and preparedness. The absence of standardized disaster response plans and infrastructure increases vulnerability to significant disruptions during emergencies. Implementing comprehensive disaster recovery protocols and infrastructure is crucial for enhancing resilience and ensuring the safety and well-being of the population.

E. CONCLUSION

VIII. CONCLUSION

On February 6, 2023, Turkey was struck by a devastating earthquake with a magnitude of 7.8, centered in the Kahramanmaraş Pazarcık and Elbistan districts. This catastrophic event exposed severe deficiencies in the country's digital communications and computer networks sector, highlighting the inability of private mobile service operators to deliver timely services and equipment to the affected regions. This study aimed to explore whether preemptive planning and design using Cisco Packet Tracer could mitigate these issues, focusing on creating a resilient network infrastructure to support disaster recovery operations.

Throughout this project, we employed fundamental network principles to design a durable and reliable communication system. Our design included the use of VLANs (Virtual Local Area Networks) to segment network traffic, thereby improving network performance and security by minimizing broadcast traffic. We also implemented subnets to efficiently manage IP address allocation, reducing network congestion and enhancing overall performance. Core routers, access switches, wireless access points, firewalls, and servers were strategically deployed to ensure comprehensive coverage, robust security, and seamless communication.

A. KEY COMPONENTS AND CONFIGURATIONS

1. **VLANs and Subnets:** - VLANs were used to isolate different types of traffic, such as administrative communications, server traffic, VoIP communications, and wireless connectivity, ensuring each type of traffic is handled appropriately. - Subnets were configured to manage IP address allocation, ensuring efficient use of IP addresses and reducing network congestion.

2. **Core Routers:** - Cisco ISR 4331 routers were used as core routers to connect different network segments. These routers were configured with appropriate routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to ensure efficient data packet routing.

3. **Access Switches:** - Cisco Catalyst 2960 switches were deployed as access switches to provide connectivity to end devices. These switches were configured with VLANs to ensure optimal performance and security.

4. **Wireless Access Points:** - Cisco Aironet 1850 access

points provided wireless connectivity, ensuring mobile devices and rescue teams could communicate without the need for wired connections.

5. **Firewalls:** - Cisco ASA 5505 firewalls were used to protect the network from unauthorized access and cyber threats. These firewalls were configured with security rules to monitor and control incoming and outgoing traffic.

6. **Servers:** - Cisco UCS C220 M5 servers hosted critical applications and databases, providing essential services such as DNS, DHCP, web hosting, and database management.

B. IMPORTANCE OF THE WORK

The importance of our work lies in its potential to provide a blueprint for disaster preparedness and response. A well-developed network plan, as demonstrated in our Cisco Packet Tracer project, can significantly improve communication infrastructure resilience. This resilience is crucial in ensuring timely and effective coordination during emergencies, ultimately saving lives and minimizing chaos. Our project showcases how preemptive planning and strategic design can mitigate the impact of natural disasters on communication networks.

C. APPLICATIONS AND PRACTICAL IMPLICATIONS

The network design developed in this project has several practical applications. It can be replicated and tailored to other disaster-prone regions, enhancing their communication infrastructures. Additionally, the principles and configurations outlined in our study can serve as a training module for students and professionals in the field of computer networking, preparing them to design and implement resilient networks in real-world scenarios. This can lead to the development of standardized protocols and best practices for disaster recovery network design.

D. EXTENSIONS AND FUTURE DIRECTIONS

There are several extensions and future directions for this work: 1. **Advanced Technologies:** - Integrating advanced technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV) can further enhance network flexibility, scalability, and manageability.

2. **Automated Network Management:** - Developing automated network management tools that can quickly reconfigure network settings in response to changing conditions during a disaster can improve network resilience and response times.

3. **Economic Considerations:** - Addressing the economic challenges associated with implementing and maintaining a disaster recovery network infrastructure is crucial. Policymakers and stakeholders must prioritize funding for such initiatives to ensure the availability of critical resources during emergencies.

4. **Standardized Protocols:** - Establishing standardized disaster response protocols and infrastructure will be essential for improving overall preparedness and resilience. These protocols should include guidelines for network design, deployment, and maintenance during disaster scenarios.

E. COMPARISON WITH OTHER COUNTRIES

Countries like Japan, which are also prone to earthquakes, have established comprehensive disaster preparedness and response protocols. Japan’s approach includes well-planned network infrastructures, regular disaster drills, and significant investment in both technology and training. These measures ensure that communication networks remain operational even during severe natural disasters, enabling effective coordination and response.

Turkey can learn valuable lessons from Japan’s experience. Implementing similar strategies, such as developing robust disaster recovery plans, investing in resilient infrastructure, and conducting regular training and drills, can enhance Turkey’s ability to respond to natural disasters. Additionally, adopting advanced technologies and establishing standardized protocols can further improve the country’s disaster preparedness and resilience.

F. RECOMMENDATIONS AND WARNINGS

Given the findings of this project, several recommendations can be made: 1. **Investment in Infrastructure:** - Significant investment is needed to build and maintain a robust disaster recovery network infrastructure. This includes funding for advanced networking equipment, software licenses, and personnel training.

2. **Regular Drills and Training:** - Conducting regular drills and training sessions for network engineers and emergency response teams can ensure preparedness and quick response during actual disasters.

3. **Collaboration and Coordination:** - Enhanced collaboration between government agencies, private sector companies, and non-governmental organizations is essential to develop and implement effective disaster recovery strategies.

4. **Public Awareness:** - Raising public awareness about the importance of resilient communication networks and encouraging community participation in disaster preparedness initiatives can improve overall resilience.

G. IMPROVING THE WORK

There are several ways to improve upon the work presented in this project: 1. **Enhanced Simulation Scenarios:** - Expand the range of disaster scenarios simulated in Cisco Packet Tracer to include various types and severities of natural disasters. This would provide a more comprehensive understanding of network behavior under different conditions.

2. **Real-World Testing:** - Collaborate with local authorities and organizations to test the network design in real-

world environments. This would provide valuable insights into practical challenges and help refine the design for actual deployment.

3. **Integration with Emerging Technologies:** - Explore the integration of emerging technologies such as IoT (Internet of Things) devices for real-time monitoring and data collection during disasters. This could enhance situational awareness and improve decision-making processes.

4. **Interdisciplinary Approach:** - Incorporate insights from other disciplines such as civil engineering, urban planning, and emergency management to create a more holistic disaster recovery plan. This interdisciplinary approach can lead to more resilient and effective solutions.

5. **Community Engagement:** - Engage with local communities to raise awareness about the importance of network resilience and gather feedback on their specific needs and concerns. Community involvement can lead to more tailored and effective disaster recovery strategies.

6. **Continuous Improvement:** - Establish a framework for continuous monitoring and improvement of the network infrastructure. Regularly update the network design and configurations based on new technologies, feedback, and lessons learned from past disasters.

H. CONCLUSION

The implementation of a disaster recovery network infrastructure in Turkey faces numerous challenges, including the lack of planned architecture, economic constraints, and the unpredictability of disasters. Addressing these issues requires significant investment, careful planning, and the development of standardized protocols. Despite the difficulties, establishing a robust network infrastructure is essential for effective disaster response and recovery operations. By leveraging network principles and simulation tools like Cisco Packet Tracer, we have demonstrated that it is possible to create a resilient communication network capable of supporting disaster recovery efforts. Moving forward, continuous refinement of these designs, integration of new technologies, and securing the necessary resources will be crucial to ensure that our communication networks can withstand future challenges. Comparing with countries like Japan, it becomes evident that comprehensive disaster preparedness and investment in resilient infrastructure are paramount for mitigating the impact of natural disasters. Turkey must adopt and adapt these practices to enhance its disaster resilience and preparedness.

I. COPYRIGHT ISSUE

The Reports are going to be under the ComVISLab Intellectual Property Rights.(C)Comp.Eng.Dep@MCBU. The Problem Experimental Design Project belongs to Prof.Dr.Muhammet G. Cinsdikici ERDEM *http://comvislab.com*.

ACKNOWLEDGMENT

The names of the persons and institutions who contributed this project should be mentioned here.

REFERENCES

[1] *"Global CMT Catalog Search"*. Global Centroid Moment Tensor. 6 February 2023. Archived from the original on 7 February 2023. Retrieved 6 February 2023.

[2] https://www.meb.gov.tr/6-subat-depremlerinin-birinci-yilinda-yapilan-egitim-seferberligi/haber/32458/tr

[3] Ocal T., Yıldız A., *"06 ŞUBAT 2023 KAHRAMANMARAŞ DEPREMLERİ ÖNCESİ TOPLANMA ALANLARININ COĞRAFİ ANALİZİ: ANTAKYA VE ÇEVRESİ"*, *Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergis*, vol. 20, no. 52, pp. 132-157, 2023, 10.1109/TED.2016.2628402.

[4] https://www.tmmob.org.tr/sites/default/files/tmmob_deprem_raporu_son_4agustos-part-1.pdf

[5] https://www.trthaber.com/haber/gundem/deprem-bolgesinde-iletisim-aglari-guclendiriliyor-747230.html

[6] https://www.techtarget.com/searchnetworking/tip/IP-addressing-and-subnetting-Calculate-a-subnet-mask-using-the-hosts-formula

[7] https://www.geeksforgeeks.org/small-organization-set-up-in-cisco-packet-tracer/

MUHAMMET GOKHAN CINSDIKICI ERDEM (M'08, SM'20) was born in Izmir, Turkey. He graduated from Ege University Computer Engineering Department in 1995. He completed his master's degree in the same department in 1997. Then he started his PhD education at Ege University Computer Institute. After completing his doctorate education in 2004, he started to work as an assistant professor at the institute. He was awarded the title of Associate Professor by successfully completing both the "article evaluation" and the "oral" stages of the Associate Professor exam held by the Turkish Interuniversity Board (ÜAK) in April 2012. He had used this title at Ege University until December 2018. Since January 2019, he has been working at the Computer Engineering Dep@Manisa Celal Bayar University(MCBU). He has gained a full-time Prof. position in MCBU (2023). His study subjects are Deep Learning, Machine Learning, Artificial Neural Networks, and Computer Vision. He mainly works on Surveillance Monitoring systems, Medical Image Processing, and Intelligent Transportation Systems. Meanwhile, Muhammet G. (Cinsdikici) ERDEM is the founder (L0) and active member of the ComVIS Lab (Computer Vision) Academic Research team and holds two patents. He has also been awarded with *IEEE Senior Membership* (2020)

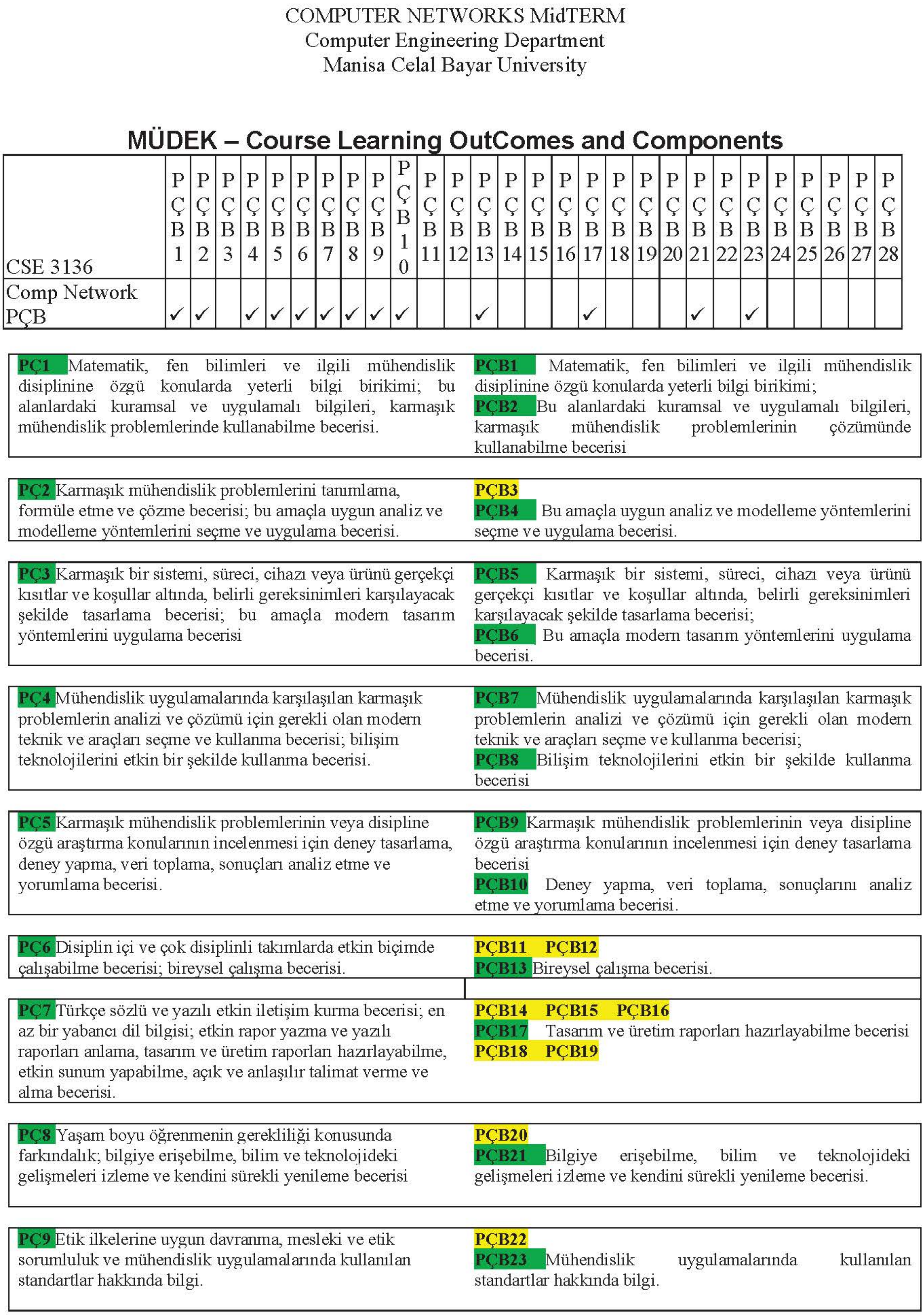
SECOND B. AUTHOR (M'76–SM'81–F'87) and all authors may include biographies. Biographies are often not included in conference-related papers. This author became a Member (M) of IEEE in 1976, a Senior Member (SM) in 1981, and a Fellow (F) in 1987. The first paragraph may contain a place and/or date of birth (list place, then date). Next, the author's educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state, and country, and year the degree was earned. The author's major field of study should be lower-cased.

The second paragraph uses the pronoun of the person (he or she) and not the author's last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (publisher name, year) similar to a reference. Current and previous research interests end the paragraph.

The third paragraph begins with the author's title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor, Ms. Hunter). List any memberships in professional societies other than the IEEE. Finally, list any awards and work for IEEE committees and publications. If a photograph is provided, it should be of good quality, and professional-looking. Following are two examples of an author's biography.

APPENDIX A
MÜDEK PROGRAM ÇIKTILARI

•••



COMPUTER NETWORKS MidTERM
Computer Engineering Department
Manisa Celal Bayar University

MÜDEK – Course Learning OutComes and Components

CSE 3136	PÇB 1	PÇB 2	PÇB 3	PÇB 4	PÇB 5	PÇB 6	PÇB 7	PÇB 8	PÇB 9	PÇB 10	PÇB 11	PÇB 12	PÇB 13	PÇB 14	PÇB 15	PÇB 16	PÇB 17	PÇB 18	PÇB 19	PÇB 20	PÇB 21	PÇB 22	PÇB 23	PÇB 24	PÇB 25	PÇB 26	PÇB 27	PÇB 28
Comp Network PÇB	✓	✓		✓	✓	✓	✓	✓	✓	✓			✓				✓				✓		✓					

PÇ1 Matematik, fen bilimleri ve ilgili mühendislik disiplinine özgü konularda yeterli bilgi birikimi; bu alanlardaki kuramsal ve uygulamalı bilgileri, karmaşık mühendislik problemlerinde kullanabilme becerisi.	**PÇB1** Matematik, fen bilimleri ve ilgili mühendislik disiplinine özgü konularda yeterli bilgi birikimi; **PÇB2** Bu alanlardaki kuramsal ve uygulamalı bilgileri, karmaşık mühendislik problemlerinin çözümünde kullanabilme becerisi
PÇ2 Karmaşık mühendislik problemlerini tanımlama, formüle etme ve çözme becerisi; bu amaçla uygun analiz ve modelleme yöntemlerini seçme ve uygulama becerisi.	**PÇB3** **PÇB4** Bu amaçla uygun analiz ve modelleme yöntemlerini seçme ve uygulama becerisi.
PÇ3 Karmaşık bir sistemi, süreci, cihazı veya ürünü gerçekçi kısıtlar ve koşullar altında, belirli gereksinimleri karşılayacak şekilde tasarlama becerisi; bu amaçla modern tasarım yöntemlerini uygulama becerisi	**PÇB5** Karmaşık bir sistemi, süreci, cihazı veya ürünü gerçekçi kısıtlar ve koşullar altında, belirli gereksinimleri karşılayacak şekilde tasarlama becerisi; **PÇB6** Bu amaçla modern tasarım yöntemlerini uygulama becerisi.
PÇ4 Mühendislik uygulamalarında karşılaşılan karmaşık problemlerin analizi ve çözümü için gerekli olan modern teknik ve araçları seçme ve kullanma becerisi; bilişim teknolojilerini etkin bir şekilde kullanma becerisi.	**PÇB7** Mühendislik uygulamalarında karşılaşılan karmaşık problemlerin analizi ve çözümü için gerekli olan modern teknik ve araçları seçme ve kullanma becerisi; **PÇB8** Bilişim teknolojilerini etkin bir şekilde kullanma becerisi
PÇ5 Karmaşık mühendislik problemlerinin veya disipline özgü araştırma konularının incelenmesi için deney tasarlama, deney yapma, veri toplama, sonuçları analiz etme ve yorumlama becerisi.	**PÇB9** Karmaşık mühendislik problemlerinin veya disipline özgü araştırma konularının incelenmesi için deney tasarlama becerisi **PÇB10** Deney yapma, veri toplama, sonuçlarını analiz etme ve yorumlama becerisi.
PÇ6 Disiplin içi ve çok disiplinli takımlarda etkin biçimde çalışabilme becerisi; bireysel çalışma becerisi.	**PÇB11** **PÇB12** **PÇB13** Bireysel çalışma becerisi.
PÇ7 Türkçe sözlü ve yazılı etkin iletişim kurma becerisi; en az bir yabancı dil bilgisi; etkin rapor yazma ve yazılı raporları anlama, tasarım ve üretim raporları hazırlayabilme, etkin sunum yapabilme, açık ve anlaşılır talimat verme ve alma becerisi.	**PÇB14** **PÇB15** **PÇB16** **PÇB17** Tasarım ve üretim raporları hazırlayabilme becerisi **PÇB18** **PÇB19**
PÇ8 Yaşam boyu öğrenmenin gerekliliği konusunda farkındalık; bilgiye erişebilme, bilim ve teknolojideki gelişmeleri izleme ve kendini sürekli yenileme becerisi	**PÇB20** **PÇB21** Bilgiye erişebilme, bilim ve teknolojideki gelişmeleri izleme ve kendini sürekli yenileme becerisi.
PÇ9 Etik ilkelerine uygun davranma, mesleki ve etik sorumluluk ve mühendislik uygulamalarında kullanılan standartlar hakkında bilgi.	**PÇB22** **PÇB23** Mühendislik uygulamalarında kullanılan standartlar hakkında bilgi.

FIGURE 10. MUDEK Program Çıktıları Bileşenleri