مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية
Bani Waleed University Journal of Humanities and Applied Sciences
تصدر عن– جامعة بني وليد – ليبيا
Website:https://jhas-bwu.com/index.php/bwjhas/index

ISSN 3005-3900 | الصفحات (143 -160) | المجلد الحادي عشر – العدد الثالث – 2026

Design, Simulation, and Implementation of a Unified Network for Computer Science Department Laboratories

Namier mohamed [1]*, Aziza Lamien [2], hasan Khaled [3], heba Ahmed [4], Hiyam Hussein [5]
[1,2,3,4,5] Computer science, Faculty of science ,Tobruk university, Tobruk, Libya
nameer.alobaidi@tu.edu.ly

تصميم ومحاكاة وتنفيذ ربط أجهزة الحاسوب في معامل قسم الحاسب الآلي في شبكة موحدة

نمير محمد[1]*، إعزيزة لامين هلال [2]، حسن خالد [3]، هبة أحمد [4]، هيام حسين [5]
[5.4.3.2.1] قسم الحاسوب ، كلية العلوم ، جامعة طبرق، طبرق، ليبيا

Received: 15-03-2026	Accepted: 20-04-2026	Published: 28-04-2026

الملخص:
يبحث هذا البحث ويقارن بين طريقتين لتصميم الشبكات للربط بين معامل الحاسوب الصغيرة. طريقة الربط الاولى عبارة عن توصيل مفتاح مركزي لتوصيل ثلاثة مفاتيح فرعية ، بينما تعتمد طريقة الربط الثانية على ثلاثة مفاتيح متصلة بشكل مباشر بدون نقطة تحكم مركزية. تم تنفيذ كل من الطريقتين ومحاكاتهما باستخدام أداة تتبع الحزم من **packet tracer Cisco** ، وكذلك تم تشغيل الشبكة على اجهزة الشبكة الحقيقة مع إجراء اختبارات عملية باستخدام أدوات فحص الشبكة، بما في ذلك **ping** و **ping -n** 10 و **tracert**. تشير النتائج إلي أن الطريقة الاولى توفر أداء أعلى من حيث الاستقرار ووقت الاستجابة وادارة الامان المركزية ، مما يسمح بتدفق حركة المرور المنظم وتطبيق الشبكات المحلية الافتراضية أو قوائم التحكم في الوصول (**ACL**). أما الطريقة الثانية ، فهي أبسط وتوفر إمكانية تفادي الأعطال ولكنها تظهر فترة استجابة أعلى قليلا، وأوقات استجابة متقلبة، وقدرة محدودة على فرض سياسات أمنية موحدة. وتشير هذه النتائج إلى ضرورة اختيار بنية الشبكة استنادا إلى متطلبات البيئة، التصاميم المركزية هي الأفضل للشبكات التعليمية أو التنظيمية المتوسطة الحجم التي تتطلب الكفاءة والأمان وقابلية التوسع، في حين أن التصاميم اللامركزية مناسبة للشبكات الأصغر أو المؤقتة. تقدم هذه الدراسة رؤى عملية حول قرارات تصميم الشبكة، وتسلط الضوء على المفاضلات بين الأداء والموثوقية وإمكانية الإدارة.

الكلمات الدالة: شبكات الحاسوب، ربط معامل الحاسوب ، تصميم الشبكات ،برنامج المحاكاة، اجهزة الشبكة المحلية.

Abstract
This research investigates and compares two network design methods for interconnecting small-scale computer laboratories. The first method utilizes a central switch to connect three access switches, while the second method relies on three directly interconnected switches without a central control point. Both methods were implemented and simulated using Cisco Packet Tracer and real machine with practical testing performed using

network diagnostic tools, including ping, ping -n 10, and tracert. The results indicate that the first method provides higher performance in terms of stability, latency, and centralized security management**,** allowing for organized traffic flow and the application of VLANs or Access Control Lists (ACLs). the second method, while simpler and offering partial fault tolerance, exhibits slightly higher latency, fluctuating response times, and limited capacity for enforcing unified security policies. These findings suggest that network architecture should be selected based on the requirements of the environment; centralized designs are preferable for medium-sized educational or organizational networks requiring efficiency, security, and scalability, whereas decentralized designs are suitable for smaller or temporary networks. This study provides practical insights into network design decisions, highlighting the trade-offs between performance, reliability, and manageability.

Keywords: Computer network, computer laboratories ,network design , Cisco packet tracer simulator software, real machine.

Introduction

A computer network is simply computers wired together in a way that lets them share data and/or devices such as hard drives, CD-ROMs, fax-modems, printers, etc. Networking facilitates communication among two or more programs operating on separate machines . In modern educational institutions, computer networks play an essential role in supporting teaching, learning, and administrative operations. A well-designed network allows students and instructors to share files, access centralized resources, and communicate efficiently within and outside the institution.

Objectives of Study.

Computer laboratories play a central role in modern academic institutions by providing hands-on access to technological resources, including networked computers, development environments, simulation tools, and shared services. These environments are essential for teaching computer science, information systems, networking, and engineering courses. However, many institutions suffer from isolated laboratory networks, where each lab operates independently. This isolation often leads to inefficient operation of technological resources, duplicated administrative efforts, and an increased cost of ownership. To address these challenges, the present project proposes the design and integration of a unified network that links multiple computer laboratories within the institution. The network is designed to improve stability and connectivity, streamline management, facilitate collaboration among stakeholders, and create a scalable infrastructure capable of accommodating future expansion.

The objectives of this study are organized into two main categories: GENERAL OBJECTIVES, which reflect the broader educational goals, and SPECIFIC OBJECTIVES, which outline the technical outcomes and operational improvements expected from the project.

- **General objectives**

The general objectives define the overarching purpose of establishing a combined laboratory network. These goals highlight the educational, collaborative, and institutional benefits expected from the project.

1. **enhance the educational environment**.
   The project aims to improve the overall teaching and learning experience by enhancing the efficiency of technological resource utilization. A centralized and well-designed network infrastructure ensures that students gain access to course materials, development platforms, and academic software in a more consistent and reliable manner.
2. **facilitate collaboration between students and faculty members**.
   Effective learning environments encourage cooperation, the exchange of knowledge, and collective problem-solving. By providing a unified network across laboratories, students and faculty members can participate in joint research projects, access shared databases, and collaborate on group assignments in real time..

- **specific objectives**

1. **Provide fast and stable connectivity between laboratories**
   A primary technical objective is to establish a network that delivers high-bandwidth and low-latency communication between all connected laboratories. Reliable connectivity is essential for software deployment, file sharing, remote access, and collaborative work. The design must balance performance with security and ensure consistent service availability.
2. **Develop a centralized management system**
   Centralizing network and device administration reduces operational complexity. Through a unified management platform, administrators can monitor device status, deploy updates, manage users, enforce security policies, and perform troubleshooting from a single interface.
3. **Reduce operational and maintenance costs**
   By replacing multiple separate laboratory networks with a single unified infrastructure, the institution can minimize resource duplication, limit unnecessary hardware investments, and streamline maintenance procedures
4. **Support future development of laboratories**
   Educational institutions develop over time, often requiring new laboratories, learning spaces, or departments. The proposed network infrastructure must therefore be modular and scalable. Supporting growth ensures that the system remains relevant, sustainable, and adaptable to changing academic demands.

Computer network

Computer networks have grown more widespread .These days, a computer network is much more than just a group of connected gadgets. Computer networks are a system of interconnected computers for the purpose of sharing digital information. The computer network enables users to analyze, organize and disseminate the information that is essential to profitability. The rise of intranets and the internet is an important aspect of computer networking. Therefore, Networking supports communication between two or more programs running on physically distant machines (Jain et al., 2015). In addition, a computer network comprises a group of computers that are interconnected in a manner that allows them to exchange data with each other and with other computers on the network. A network is established when at least two computers join together to share information and resources .A computer network is a linked group of independent computers, where "linked" indicates that the computers can share information, and "independent" signifies that no single computer can start, stop, or manage another computer within the network.

Types of Computer Networks

Computer networks have transformed how individuals and organizations communicate, share data, and access digital services. With advancements in networking technologies, a variety of network types have emerged to address different communication needs from short-range personal communication to global data exchange systems. Each network type has unique characteristics related to coverage, topology, cost, management, and performance. Understanding these network types is essential for students, IT professionals, and system designers who aim to develop efficient network infrastructures. Researchers and technology organizations have classified networks based on scale and function. According to Tanenbaum & Wetherall (2011), networks can be broadly categorized as PAN, LAN, MAN, and WAN. More recent classifications introduce WLAN, CAN, and specialized networks such as SAN and VPN (Kurose & Ross, 2021). The most used types of networks are Local area network(LAN), and wide area network WAN.

Local Area Networks(LAN)

Tanenbaum (2011) emphasizes LAN's importance in organizational environments. LANs provide high-speed communication using Ethernet cables or optical fiber, supporting resource sharing within buildings such as offices, schools, and labs. As the name implies, a Local Area Network (LAN) interconnects computers in a limited geographic area. It provides high-bandwidth communication over inexpensive transmission media (Tarkaa et al., 2017). Local Area Networks (LANs) connect electronic devices within an organization, allowing local processing and communication between devices. They enable inter-station messaging without a central host and provide access to multiple file storage systems. Some LAN architectures also support the transmission of voice and video.

Advantages of local area network

1-The basic LAN implementation is not expensive.

2. It is easy to control and manage the entire LAN as it is available in one small region.

3. The systems or devices connected to the LAN communicate at very high speed, depending upon the LAN type and Ethernet cables supported. The common speeds supported are 10 Mbps, 100 Mbps and 1000 Mbps.

4. With the help of file servers connected to the LAN, sharing of files and folders among peers will become very easy and efficient.

5. It is easy to share common resources such as printers and internet lines among multiple LAN users.

Disadvantages of Local Area Network

1. Where a lot of terminals are served by only one or two printers, long print queues may develop, causing people to have to wait for printed output.

2. Network security can be a problem. If a virus gets into one computer, it is likely to spread quickly across the network because it will get into the central backup store.

3. If the dedicated file server fails, work stored on shared hard disk drives.

Designing topology

Network topology is the geometric depiction of the connections between devices or nodes. Network topology can be represented in two ways. Physical topology refers to the physical layout of a network, while logical topology describes how data flows over it. The most popular topologies are Bus, Star, and Mesh topology.

Bus Topology

In a local area network, a single cable runs throughout the building or campus, with all nodes attached along this line, which has two endpoints called the bus or backbone. Essentially, it is a multipoint communication circuit that manages data flow efficiently, as every station can receive all transmissions sent across the network (Forouzan, 2013). To construct a bus topology, we connect three standard PCs in series using three switches, each linked by copper straight-through cables. The switches are then joined together using copper crossover cables.

Star Topology

In star topology, all the cables run from the computers to a central location where they are all connected by a device called a hub. It is a concentrated network, where the end points are directly reachable from a central location when the network is expanded (Forouzan, 2013). Ethernet 10 base T is a popular network based on the star topology. All of the cables in a star topology run from the computers to a hub, which connects them all. When the network is expanded, the endpoints can be reached directly from a central location, making it a concentrated network

Mesh Topology:

In mesh topology, each device is connected to every other device via a dedicated point-to-point link. A dedicated stand-alone link only transports data between the two devices it connects. Every node in the network is connected to every other node, making it a well-connected topology. It can involve multiple topologies and has high cable requirements (Forouzan, 2013).

- **The importance of network design and architecture**

Network design is the systematic process of planning, structuring, and implementing communication systems that connect computing resources and users. A robust design ensures reliability, scalability, security, and effective access to shared resources. In educational institutions, particularly those operating multiple computer laboratories. network architecture must support instructional needs, administrative operations, and collaborative activities (Kurose & Ross, 2021).To achieve these goals, network design integrates hardware components (switches, routers, cabling), logical topologies (VLANs, subnets), services (DNS, DHCP), management frameworks, and security mechanisms. The architecture must enable stable connectivity between laboratories, support centralized administration, and allow incremental expansion without major reconfiguration (Oppenheimer, 2010). Prepare, Plan, Design, Implement, Operate, and Optimize comprise the Cisco PPDIOO methodology. (Alarbad et al., 2024) state that The PPDIOO methodology provides a framework for ensuring an effective, well-designed network infrastructure.

Research methodology and implementation

This part of research provides a comprehensive and detailed explanation of the two designs studied in order to determine the best approach among them. This was achieved after examining the characteristics (advantages and disadvantages), similarities, and the simulation design performed by the research team using Cisco Packet Tracer network simulation software.

In this paper real machines were used to design and implement the two networks. In addition, a packet tracer used to examine the result of two networks.

- **first Method: Network Interconnection Using 4 Switches**

This method describes the design of a local area network (LAN) that consists of FOUR SWITCHES. Three of the switches function as SUB-SWITCHES, each assigned to one computer laboratory, and each sub-switch connects to two computers only. A main switch is used as the central aggregation point to interconnect all sub-switches into a unified network. The network was simulated using cisco packet tracer and was also implemented practically by using real devices to test device-to-device connectivity.

Tools and Components Used

1. Hardware

• 4 Cisco SF-1016 switches

• 6 computers (2 per sub-switch)

• Ethernet Category 6 (Cat 6) network cables

• RJ-45 con

2. Software and Commands

• Cisco Packet Tracer software for network design and simulation.

• Network command tools such as ping and ipconfig for checking connectivity.

1. General Network Structure

The network was designed according to the following arrangement:

- One central switch for the entire network

- Three access (sub) switches connected to the central switch
- Each access switch is connected to two computers only (two devices per lab network were used for practical implementation)
- All devices are within the same subnet (Flat Network)
- An Extended Star Topology was adopted
- Network cabling was implemented using both straight-through and crossover Ethernet cables

2. IP Address Allocation

IP addresses were assigned manually (Static IPv4) to all computers within the same subnet, as shown in the following table:

Table 1:IP address Allocation

Access Switch	Device	IP Address
Access Switch 1	Computer 1	192.168.1.2
	Computer 2	192.168.1.3
Access Switch 2	Computer 3	192.168.1.4
	Computer 4	192.168.1.5
Access Switch 3	Computer 5	192.168.1.6
	Computer 6	192.168.1.7

NOTE. All devices were assigned static IPv4 addresses within the same subnet (192.168.1.0/24) to form a flat network topology.
The IP addressing scheme used in this network was based on MANUAL (STATIC) IPV4 ASSIGNMENT to ensure simplicity, control, and ease of management during the practical implementation. As shown in TABLE I, all computers were configured within the same subnet (192.168.1.0/24), forming a flat network architecture without VLAN segmentation. Each access switch connects to two end devices, and each device was assigned a unique IP address to avoid address conflicts and ensure proper network communication. This addressing approach allows all hosts to communicate directly with one another through the central switch, which supports the adopted extended star topology**.** The use of static IP addresses also facilitates network testing, troubleshooting, and monitoring during laboratory exercises, making it suitable for educational and training environments.

Connectivity Testing

To evaluate the operational performance of the implemented network, a series of ICMP echo request (ping) tests were conducted to assess end-to-end connectivity between hosts connected to different access switches. These tests were designed to verify correct IP configuration, proper switch interconnection, and successful data forwarding within the flat network environment.

Specifically, a ping test was initiated from Computer 1 to the host with IP address 192.168.1.3, which produced successful echo replies. Similarly, connectivity was confirmed by issuing ping commands from Computer 2 to 192.168.1.6 and from Computer 4 to 192.168.1.7, with all tests returning positive results and no observed packet loss.

The successful outcomes of these tests, summarized in Table I, confirm that all network devices are correctly addressed within the same subnet and that the switching infrastructure is functioning as intended. Furthermore, the results demonstrate the effectiveness of the extended star topology, where the central switch efficiently manages traffic between the three access switches. Overall, the connectivity testing validates the reliability, correctness, and robustness of the network design, confirming its suitability for practical laboratory and educational use.

Network Design Using the Simulator

The following figure illustrates a two-dimensional network topology diagram designed using a network simulation tool. The diagram shows a main (central) switch, positioned at the top or center of the layout (referred as switch 1 in the figure), which serves as the core of the network. Three access switches are connected directly to the central switch, forming the backbone of the network architecture. Each access switch is connected to two end-user computers, representing the hosts within each laboratory segment (as an example, Switch 2 works as the main switch for laboratory 1, Switch 3 works as the main switch for laboratory 2, Switch 4 works as the main switch for laboratory 3). This design visually reflects the adopted extended star topology, where all access-layer devices communicate through the central switch. The simulator-based design provides a clear representation of the physical and logical structure of the network and facilitates validation, testing, and analysis of connectivity prior to real-world implementation.

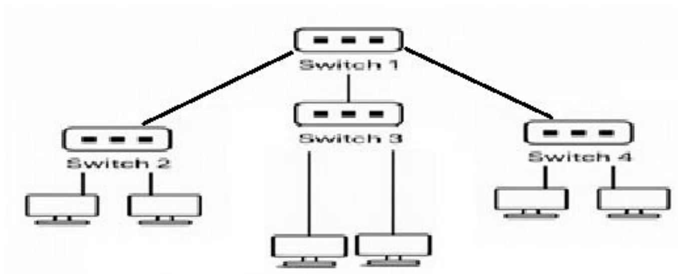


figure1: Two-Dimensional Diagram of the Structural Design of the Network Switches

The following two figures illustrate a simulation experiment performed using the network simulation software, figure 2 demonstrates successful connectivity between two devices each connected to different star topology, which represented as follows, the first device with IP address **192.168.1.1** , named PC0 , connected to Switch 0 in the figure, and the second device with IP address **192.168.1.6** , named PC5 , connected to Switch 3.

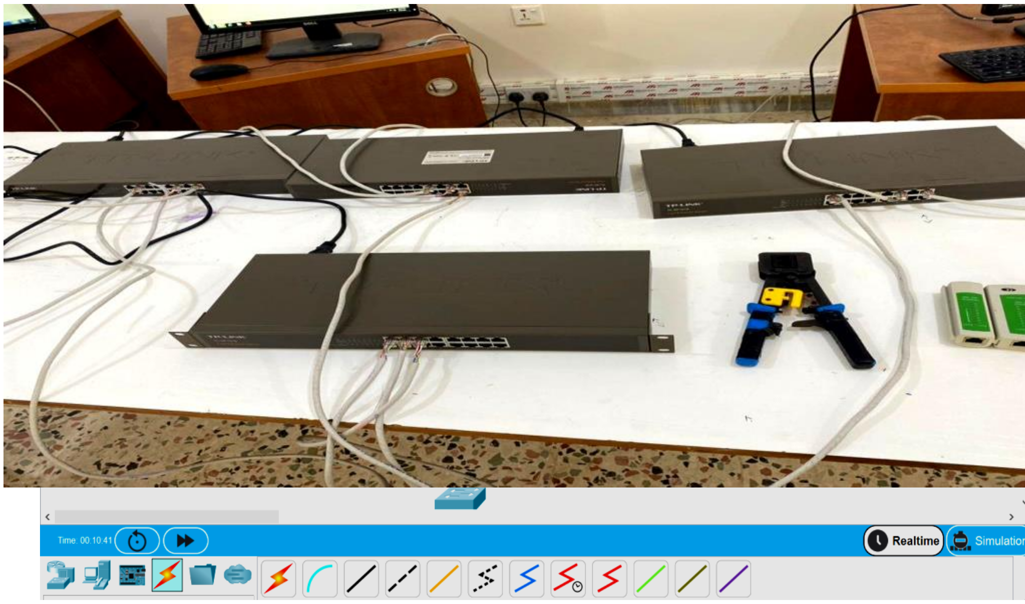


Figure 2: Network Simulation Design by the Software (Cisco packet tracer)

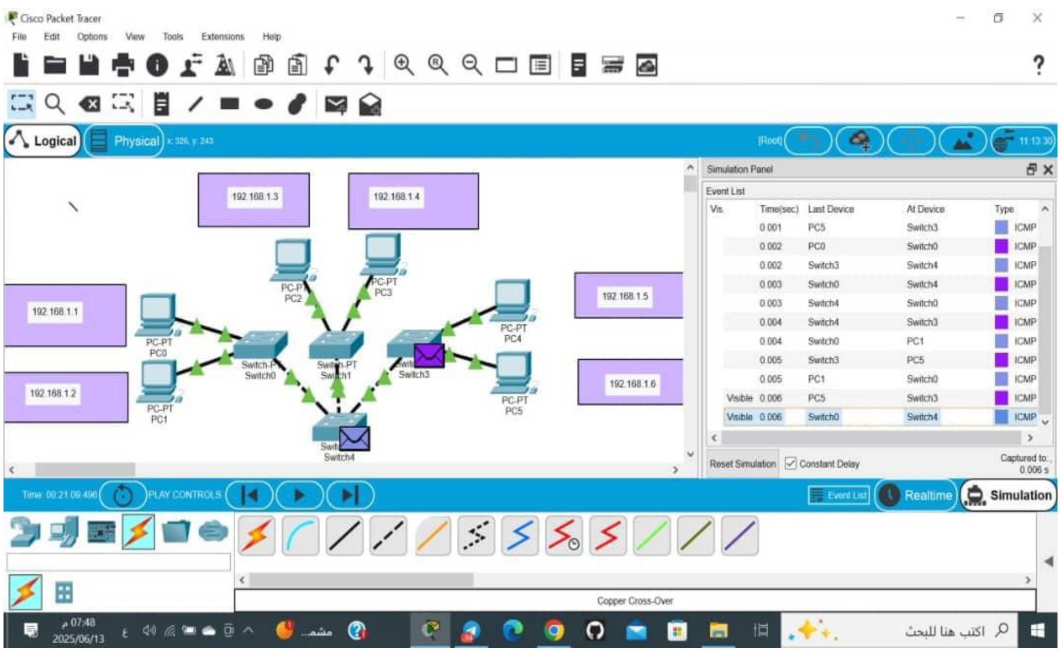
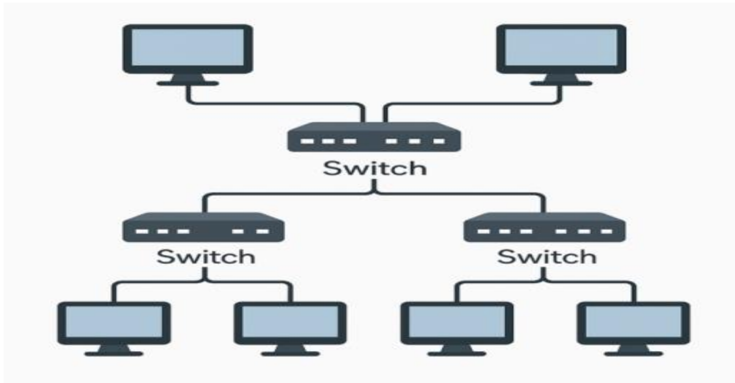


Figure3: Experiment of sending and receiving data packets between two devices on the network

Figure 4: Physical Implementation of the Network



Results and Observations of the first Method

Following the implementation and simulation of the network using specialized software, a comprehensive analysis of the operational performance yielded the following outcomes:

- **Reliable End-to-End Connectivity:** All networked computers demonstrated consistent and uninterrupted communication. This indicates that the IP addressing scheme and switch interconnections were correctly configured, ensuring proper network functionality.
- **Optimized Manageability and Scalability:** The extended star topology facilitated systematic network management and provides a framework that is readily scalable. The topology allows for the addition of new devices or switches with minimal disruption to existing configurations, thereby supporting future network expansion.
- **Low Latency and Efficient Data Transmission:** Observations confirmed that the network maintained low response times, and data packets were transmitted and received accurately. This reflects the efficiency of the switching infrastructure and the effectiveness of the adopted topology in minimizing transmission delays.
- **Centralized Control and Traffic Regulation:** The deployment of a main central switch enhanced the organization of network traffic, mitigated the risk of bottlenecks, and ensured coordinated communication between the access switches.

Collectively, these results substantiate the robustness and effectiveness of the adopted design methodology. The findings validate that this approach provides a reliable, scalable, and efficiently managed network architecture, suitable for both educational laboratory environments and small-to-medium scale organizational applications.

Second method connecting the Three Computer Laboratories Using Three Switches

This method focuses on interconnecting three computer laboratories using three **access** switches**,** with each switch connected to only two computers**,** resulting in a total of six computers. The network was implemented within a simulated environment using Cisco Packet Tracer. The design ensured full connectivity among all devices, and the process included detailed steps for cabling, configuration, and verification through practical testing**.**

Tools and Components

1. Hardware Components

- **Three switches** of type *Cisco SF-1016*
- **Six computers** (two devices connected to each access switch)
- **Ethernet Cat6 cables** for network connections
- **RJ-45 connectors** for cabling

2. Software and Commands

- **Cisco Packet Tracer**, utilized for network design and simulation
- **Network command-line tools**, including ping and ipconfig, for testing connectivity and verifying configurations

Practical Implementation Steps

General network structure

The network was designed according to the following specifications:

- **Three interconnected switches** were used to integrate all laboratory networks into a unified system.
- **Two computers per switch** were connected to facilitate practical exercises.
- All devices were configured within a single subnet**,** forming a flat network**.**
- An **extended star topology** was adopted to provide a structured and hierarchical design.
- Network cabling was implemented using both straight-through and **crossover** Ethernet cables, depending on the connection type.

This configuration ensures efficient communication between all devices while maintaining a simple, scalable, and easily manageable network architecture suitable for laboratory simulation and educational purposes.

IP Addressing Scheme

In this implementation, static IPv4 addresses were assigned to all computers to ensure predictable and stable network communication. The IP configuration maintained all devices within a single subnet (Flat Network**)**, thereby enabling direct communication between all hosts without routing requirements. Table 2 presents the IP address allocation for each computer in the network

Table 2 Static IP Address Assignment for the Laboratory Network

Access Switch	Device	IP Address
Access Switch 1	Computer 1	192.168.1.2
	Computer 2	192.168.1.3
Access Switch 2	Computer 3	192.168.1.4
	Computer 4	192.168.1.5
Access Switch 3	Computer 5	192.168.1.6
	Computer 6	192.168.1.7

Note: The static addressing scheme facilitates controlled testing, reduces the likelihood of IP conflicts, and supports efficient network troubleshooting.

Connectivity Testing

To validate the network design, ICMP echo request (ping) tests were performed between various devices across the three switches. The specific tests included:

- A ping from **Computer 1** to **192.168.1.3**, resulting in a successful response.
- A ping from **Computer 2** to **192.168.1.6**, confirming connectivity.
- A ping from **Computer 4** to **192.168.1.7**, also successful.

All tests demonstrated **reliable communication**, confirming that the switches were properly interconnected and that the network configuration was correct. The results indicate efficient packet delivery and validate the effectiveness of the extended star topology in supporting communication between all devices.

Network Design Simulation

The network was simulated using **Cisco Packet Tracer** to provide a visual representation of the logical and physical structure. The simulation included three access switches which connected as cascaded, with each access switch linked to two computers. This layout mirrors the **cascaded star topology**, which doesn't have centralized traffic management. Figures 5 and 6 illustrates the two-dimensional topology and the simulated network design, respectively.

Figure 5: Two-Dimensional diagram of the Structural design of the Network Switches

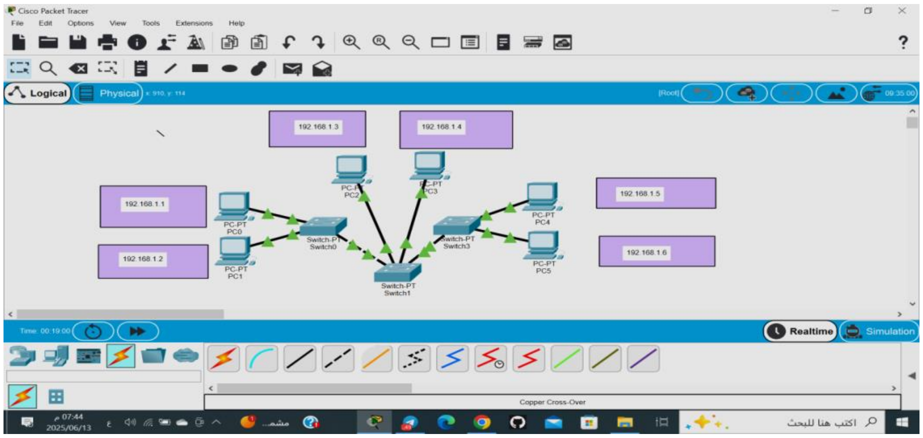


Figure 6: Network Simulation Design in Cisco Packet Tracer

Subsequent simulation experiments were conducted to verify data transmission between devices, including tests between **192.168.1.1** and **192.168.1.6** demonstrating successful packet transfer and reception which executed as follows, when the user PC0 (192.168.1.1) try to send data to user PC5 (192.168.1.6) which is outside the switch 0, the data should travel through switch 1 then arriving switch 3 which PC5 is connected (192.168.1.6)..

The following figure represents the reception of Data Packets between the two devices (192.168.1.1 and 192.168.1.2) on the same switch (Switch 0).

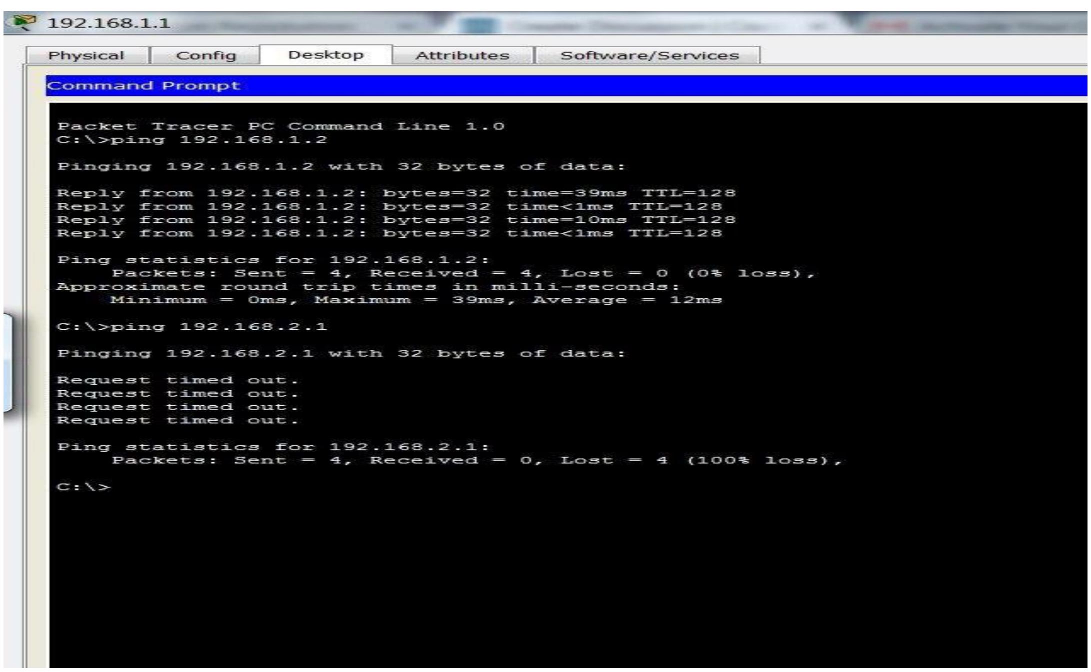


Figure 7: Reception of Data Packets Between the Two Devices

Finally, the network was implemented in a physical setup, confirming the practical feasibility of the design.

Figure 8 : Physical Implementation of the Network

Results and Observations of second method

The practical implementation and simulation of this method yielded the following findings:

1 **Reliable Connectivity:** All devices communicated successfully, indicating correct IP assignment and switch interconnection.
2 **Efficient Management and Scalability:** The extended star topology allows for organized network management and provides flexibility for future expansion.
3 **Low Latency and Effective Data Transmission:** Data packets were transmitted and received successfully with minimal delay, reflecting efficient network performance.
4 **Centralized Control:** The central switch enhanced traffic management, minimized potential congestion, and ensured smooth communication between access switches.

Overall, the outcomes confirm that this methodology provides a robust, reliable, and scalable network architecture, suitable for both laboratory simulations and small-scale educational network implementations.

Comparison Between the first Method (4 Switches) and the second Method (3 Switches)

Table 3:Comparison Between the Second Method (4 Switches) and the Third Method (3 Switches)

Parameter	First Method (4 Switches)	Second Method (3 Switches)
Number of Switches	3 access switches + 1 central switch connecting the access switches	3 interconnected switches without a central switch
Number of Computers	6 computers (2 per access switch)	6 computers (2 per switch)
Connection Method	Central switch connects the three access switches	Direct interconnection between the three switches without a central switch
Network Type	Flat network with centralized management	Flat network interconnected without a central point
Topology	Extended Star Topology	Star or simple mesh topology (depending on interconnection arrangement)
Ease of Management	Easier due to a central control point	Relatively more difficult due to absence of a clear control point
Efficiency	High – data is organized through the central switch	Good – traffic may be less organized at times

Speed	Relatively faster – data passes through a structured control center	Slightly slower – depends on the routing path between switches
Security	Better – security policies can be implemented through the central switch	Weaker – unified security policies are harder to enforce
Scalability	Flexible and easy – additional switches can be added easily	Less flexible – requires reconfiguration or additional connections
Reliability	Lower – failure of the central switch can halt the network	Higher – failure of a single switch affects only part of the network
Ping Tests	All computers communicate successfully via the central switch	All computers communicate successfully via direct interconnection
Practical Application	Suitable for medium-sized organizations requiring centralized management	Suitable for small or temporary projects

Discussion

The comparison presented in Table 3-2 highlights the fundamental differences between the first method, which employs four switches with a central control point, and the second method, which relies on three directly interconnected switches without a central switch. The results indicate that the first method provides a more structured and manageable network architecture due to the presence of a central switch, which facilitates organized traffic flow, simplified administration, and the centralized application of security policies. This design also contributes to improved performance in terms of speed and stability, as data packets are forwarded through a well-defined and controlled path.

1. Connectivity Testing Using the ping Command (Primary Evidence):

In both methods, the ping command was used as follows: > ping 192.168.1.X. The results showed successful responses for all transmitted packets (*"Reply from …"*), indicating that the network connections were correctly established and that both network designs were operational. However, practical differences between the two methods were observed:

First Method (with a central switch):

- Higher network stability
- Relatively lower response time (reply time), indicating faster and more consistent packet delivery

These observations confirm that the presence of a central switch enhances traffic organization and contributes to improved network performance and stability compared to the decentralized switch interconnection approach.

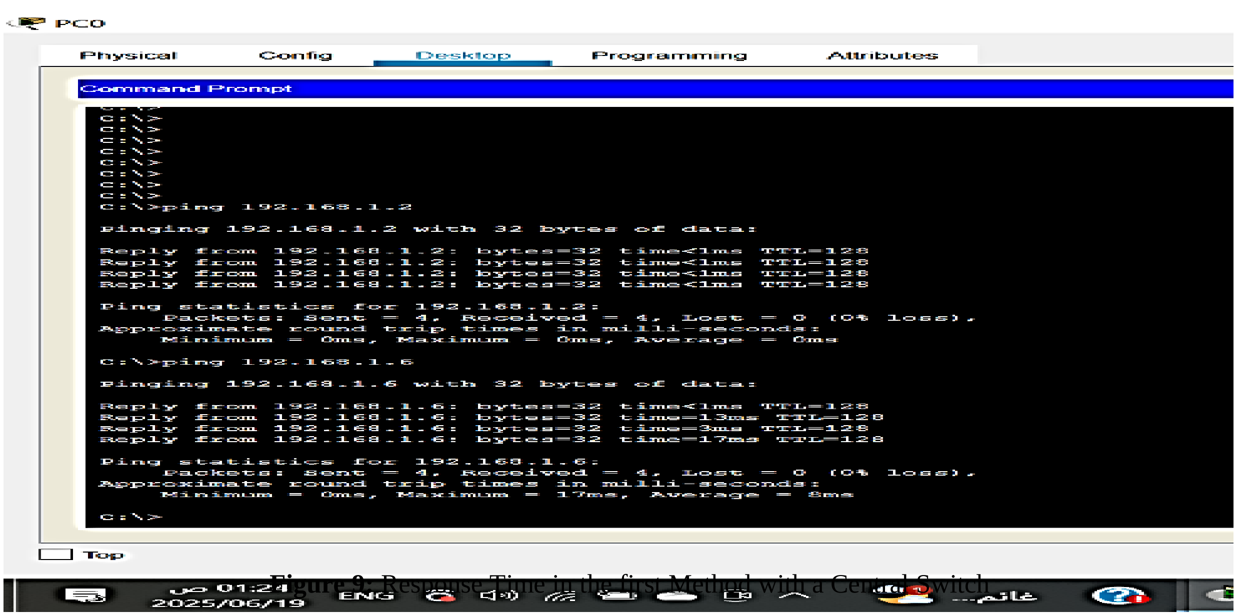


Figure 9: Response Time in the first Method with a Central Switch

Second Method (interconnected switches without a central switch):

- Slight fluctuations in response time may be observed.

- Minor delays (fractions of a millisecond) can occur, particularly under increased network load or when data traverses longer paths between devices due to multiple interconnected switches.

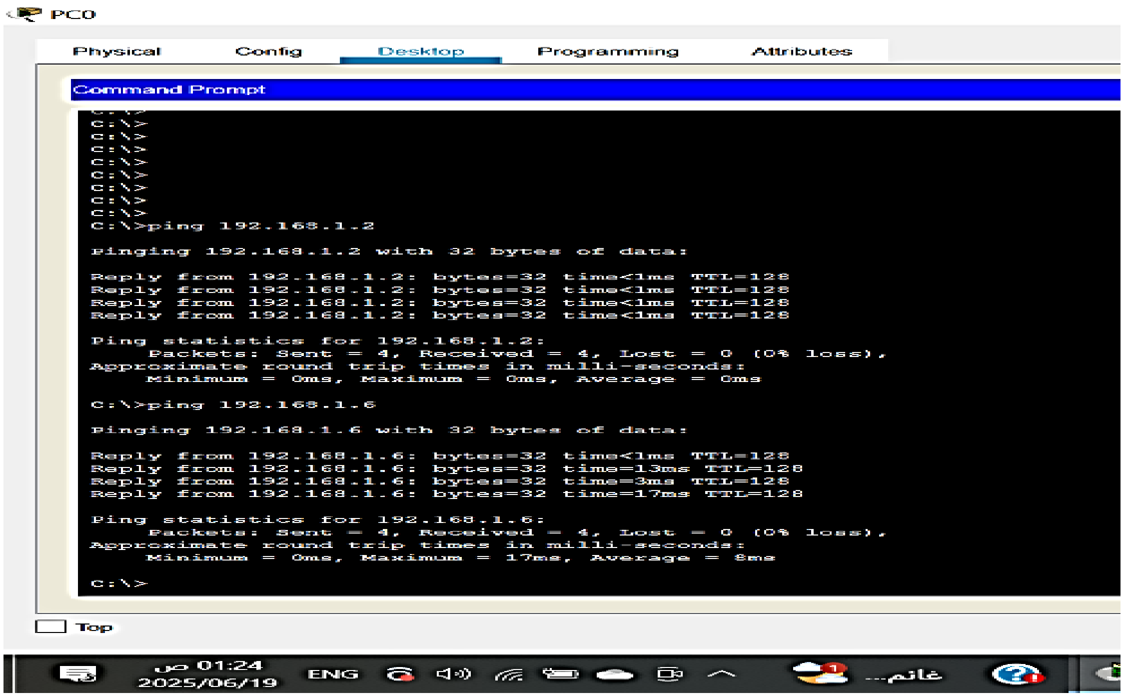


Figure 10: Response Time in the second Method (without Central Switch)

Accurate Measurement of Response Time (Latency)

When executing the following command:

> ping 192.168.1.X -n 10

the system sends 10 consecutive data packets to the destination host and displays statistical results for the round-trip time of these packets, including:

- Minimum (Minimum latency)
- Maximum (Maximum latency)
- Average (Average latency)

Using these statistical values, a more precise comparison of network latency between the two methods can be performed based on the observed results.

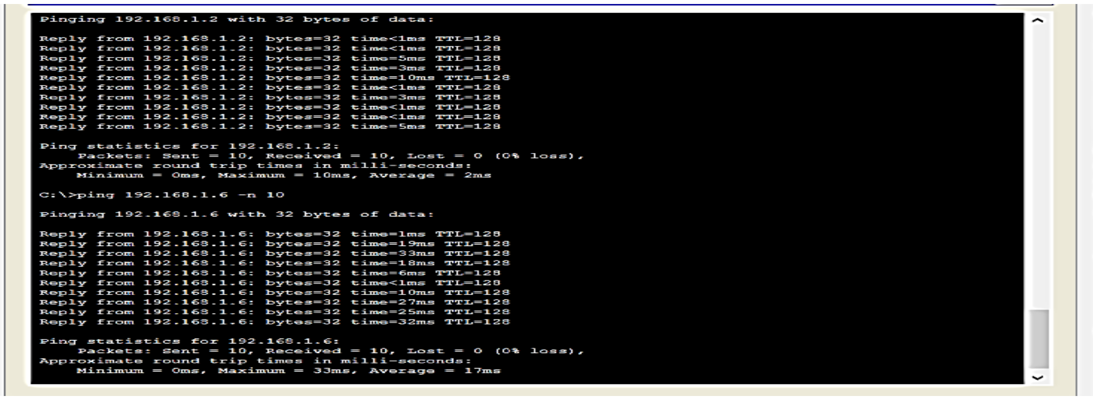


Figure 11: Response Time (Minimum, Maximum, and Average) in the first Method with a Central Switch

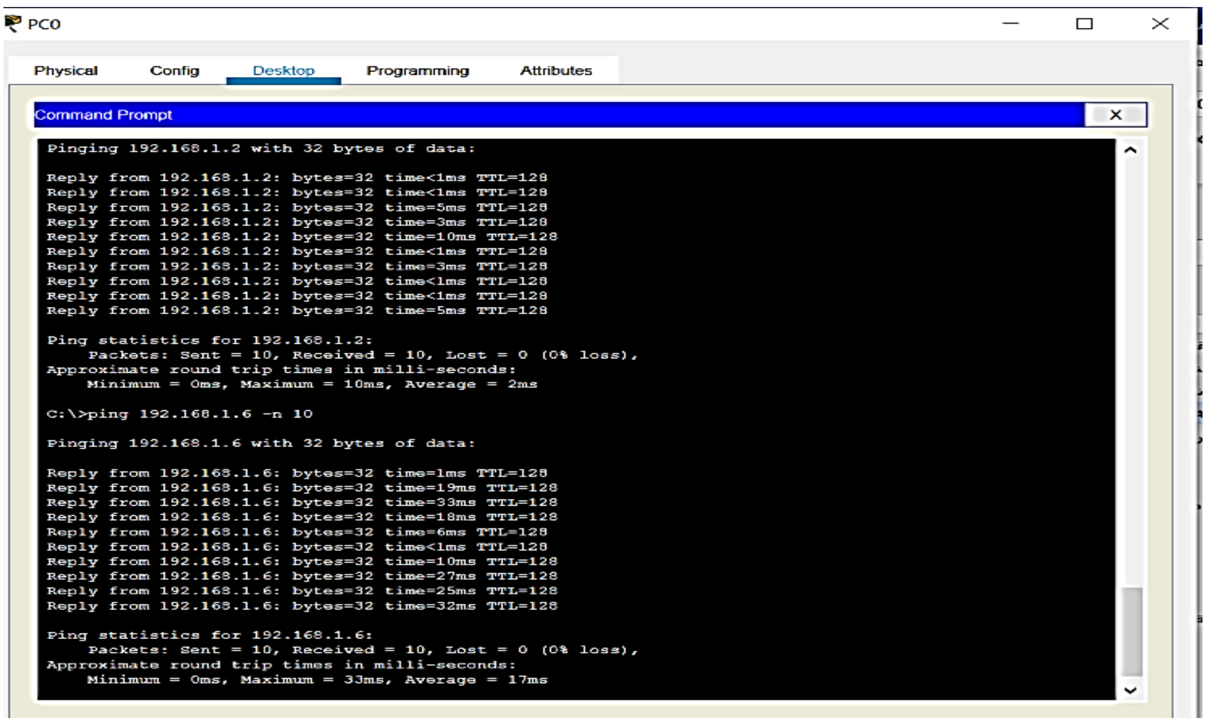
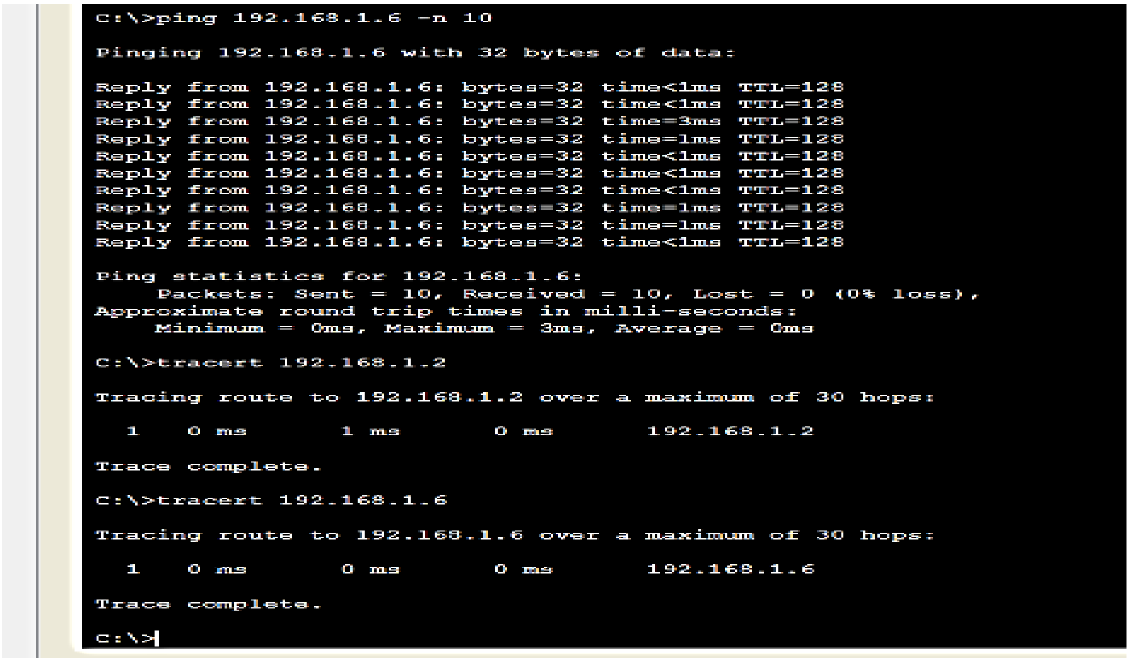


Figure 12: Response Time (Minimum, Maximum, and Average) in the second Method (without a Central Switch)

Path Analysis Using tracert

- When executing the following command: > tracert 192.168.1.X. the command displays the network path taken by packets to reach the destination host. The observed results can be summarized as follows:
- **In the network with a central switch (first Method):**
  A single, direct path is typically observed, indicating a straightforward and organized forwarding process.
- **In the network without a central switch (second Method):**
  The path may traverse multiple switches, reflecting a less centralized forwarding structure and potentially longer routing paths.



```
C:\>ping 192.168.1.6 -n 10

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=3ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms     1 ms     0 ms     192.168.1.2

Trace complete.

C:\>tracert 192.168.1.6

Tracing route to 192.168.1.6 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     192.168.1.6

Trace complete.

C:\>
```

Figure14: Tracer out Command Output in the Second Method (without a Central Switch)

Bandwidth

Network bandwidth is the maximum amount of data a network connection can transfer per second and is measured in **bits per second** (bps), or it is a capacity limit, not a performance guarantee. In other words, it's the network's maximum data sharing capacity under ideal conditions. Where Bandwidth is often confused with speed. Bandwidth describes *how much data can travel at once*. A high-bandwidth connection can support more users.

Security Considerations

Although network security is primarily an **organizational and policy-based measure** rather than a parameter directly testable via CMD commands, differences between the two methods can be observed:

- **first Method (with central switch):** VLANs and **Access Control Lists (ACLs)** can be implemented centrally, allowing effective security policy enforcement.
- **second Method (without central switch):** Absence of a central point prevents uniform application of security policies, making centralized control impossible.

Virtual Local Area Networks (VLANs)

modern institutional LANs are often configured hierarchically, with each workgroup (department/ Laboratory in our work) having its own switched LAN connected to the switched LANs of other groups via a switch hierarchy. Three drawbacks can be occurred in LAN configuration:

- Lack of traffic isolation
- Inefficient use of switches

- Managing users

Fortunately, each of these difficulties can be handled by a switch that supports virtual local area networks (VLANs). As mentioned in recommendation section.

Theoretical comparison between LANs and VLANs

Table 4: comparison between LANs and VLANs

• LAN	• VLAN
It works on a single broadcast domain	It works on multiple broadcast domain
The packet is advertised to each device	Packet is send to specific broadcast domain
Less efficient	High efficient
No information is needed to use LAN	User should know multiple commands to configure VLAN

Table 5: Summary of Experimental Results

Test	first Method (with Central Switch)	second Method (without Central Switch)
ping	Higher stability, lower response time	Good stability, slightly longer response time
ping -n 10	Lower average latency	Slight fluctuations in average latency
tracert	Single, direct path	May traverse multiple points (switches)
ipconfig	Confirms configurations	Confirms configurations
Security Policies	Applicable at central switch	Cannot be applied centrally

The results indicate that the first method provides advantages in terms of stability, performance, and security management, while the second method offers redundancy and fault tolerance but with less centralized control over traffic and security policies. Both methods successfully maintain basic connectivity, but the choice of method depends on the network size, management requirements, and desired level of security.

- **Conclusion**

This study presented a comparative analysis of two network design methods for interconnecting small-scale computer laboratories. The first method, employing a central switch to connect three access switches, and the **second method**, consisting of three directly interconnected switches without a central control point, were implemented, simulated, and evaluated through practical tests and network diagnostic tools.

The experimental results demonstrate that the first method offers superior performance in terms of stability, latency, and centralized security management**.** The presence of a central switch allows for organized traffic flow, consistent response times, and the implementation of VLANs or ACLs, providing greater control and reliability. Conversely, the second method provides fault tolerance and simplicity, as the network remains partially operational even if one switch fails, but it exhibits slightly higher latency, fluctuating response times, and limited ability to enforce unified security policies.

Ping tests, latency measurements (ping -n 10), and path analysis (tracert) confirmed that both network methods achieve basic connectivity. However, the differences in speed, stability, routing efficiency, and policy enforcement indicate that network architecture choice should be aligned with the specific requirements of the environment**,** including scalability, security, and management needs.

In conclusion, the study demonstrates that centralized network designs (such as the first method) are more suitable for medium-sized educational or organizational environments where performance, security, and manageability are priorities**,** whereas decentralized designs (like the second method) are better suited for small-scale or temporary deployments**,** where simplicity and partial redundancy are more important.

RECOMMENDATIONS

Future work could explore hybrid approaches that combine centralized management with redundancy features, or evaluate larger-scale deployments to further assess performance, scalability, and fault tolerance under higher traffic loads.

Analysis and design of VLANs for the computer department laboratories and comparison of network characteristics between the two methods in terms of bandwidth, speed, potential faults, data confidentiality, number of devices, setup costs and other network characteristics.

References

- Alarbad, A. H., Alsharif, A. M., & Sati, S. O. (2024). Campus network design for information technology faculty. International Journal of Advanced Networking and Applications, 15(6), 6211–6217. https://doi.org/10.35444/ijana.2024.15608
- Forouzan, B. A. (2013). Data communications and networking (5th ed.). Tata McGraw-Hill Education.
- Jain, G., Noorani, N., Kiran, N., & Sharma, S. (2015). Designing and simulation of topology network using Packet Tracer. International Research Journal of Engineering and Technology (IRJET), 2(2), 793–795. https://www.irjet.net/archives/V2/i2/Irjet-v2i2144.pdf
- Meelad, R. A., Mousa, M. A., & ulwahad AlSharaa, M. A. (2026). Convolutional Neural Network Models For Automated Art Style Identification: Design Training, And Evaluation. Bani Waleed University Journal of Humanities and Applied Sciences, 178-188.
- Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.
- Oppenheimer, P. (2010). Top-down network design (3rd ed.). Cisco Press.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). The network layer. In Computer networks (5th ed., pp. 343–423). Pearson.
- Meelad, R. A., Mousa, M. A., & ulwahad AlSharaa, M. A. (2026). Convolutional Neural Network Models For Automated Art Style Identification: Design Training, And Evaluation. Bani Waleed University Journal of Humanities and Applied Sciences, 178-188.
- Almarimi, A. F., & Salem, A. M. (2025). Machine Learning using Simple Linear Regression. Bani Waleed University Journal of Humanities and Applied Sciences, 10(3), 178-184.
- Dreheeb, A. M., & El Tajouri, H. (2025). Role Of Artificial Intelligence In Enhancing Cyber Security. Bani Waleed University Journal of Humanities and Applied Sciences, 10(3), 121-129.
- Elmansori, M. M., Almssmari, H. S., Salama, M. M., Khaleefah, S. S., & Albargathi, S. (2024). Improving Local Software Quality Through Process Efficiency Improving in Libyan Banks: Case Study of Derna City. Bani Waleed University Journal of Humanities and Applied Sciences, 9(5), 405-415.
- Shouran, Z., Mousa, M. A., Alatresh, S. A., & ulwahad AlSharaa, M. A. (2025). Security and Privacy in the Internet of Things: Issues, Challenges, and a Deep Learning-Based Intrusion Detection Framework. Bani Waleed University Journal of Humanities and Applied Sciences, 10(4), 225-233.
- Tarkaa, N. S., Iannah, P. I., & Iber, I. T. (2017). Design and simulation of local area network using Cisco Packet Tracer. The International Journal of Engineering and Science, 6(10), 63–77.
- James F. Kurose, Keith W. Ross. COMPUTER NETWORKING A Top-Down Approach(8th ed., 497-498).