NOTRE DAME UNIVERSITY
BANGLADESH

Computer Networks Hardware Lab Report

Course Code: CSE-3204
Course Title: Computer Networks Lab
Lab Task Topic: Introduction to Hardware Equipments

Submitted by:

Name: Istiak Alam
ID: 0692230005101005
Batch: CSE-20

Submission Date: April 25, 2025

Submitted to:

Dr. Fernaz Narin Nur
Adjunct Professor,
Notre Dame University Bangladesh

Table of Contents

Abstract

This lab report provides a comprehensive overview of essential computer networking hardware components and configurations encountered in practical networking environments. The main objective of this lab was to familiarize students with various networking tools and equipment such as cable testers, cable tracers, RS-232 cables, fiber optic duplex cables, SFP modules, and to understand the physical and logical aspects of network devices like switches and routers.

Through hands-on activities, we learned how to identify, test, and properly connect network cables using T-568B wiring standards, configure routers for Dynamic NAT and DHCP, and establish effective connections between switches and routers. The report also discusses the conceptual framework of the OSI Model to better understand the layer-wise interaction of network protocols and hardware.

By engaging in these exercises, students developed a strong foundational understanding of how computer networks are physically built and logically managed, which is crucial for further studies and careers in networking and IT infrastructure. The inclusion of real-world scenarios and step-by-step procedures reinforced the theoretical knowledge with practical implementation, bridging the gap between textbook learning and field expertise.

Introduction

The rapid growth of computer networks and internet-based technologies has significantly increased the demand for reliable and high-performance network infrastructure. Understanding the physical hardware components that form the foundation of such networks is essential for any networking professional or student. This lab report provides a comprehensive overview of various fundamental hardware tools and equipment used in networking environments.

In this report, we explore the practical application and functionality of essential devices such as cable tracers, cable testers, RS-232 cables, fiber optic duplex cables, and SFP modules. We also study network components like switches and routers, along with their configurations and interconnections. A key focus is placed on the T-568B Ethernet cabling standard, which defines the proper arrangement of wire pairs in twisted-pair cables for effective network communication.

Additionally, the report covers the Open Systems Interconnection (OSI) model, a conceptual framework that categorizes and standardizes the functions of a communication system into seven distinct layers. Each hardware topic is supported with descriptions and relevant images to aid in practical understanding.

This lab aims to enhance student's hands-on skills in identifying, using, and configuring networking hardware, thereby building a strong foundation for designing and managing robust network systems.

1 Cable Tracer

A **Cable Tracer** is an essential diagnostic tool used in computer networking to detect and follow the physical route of cables, especially in complex or hidden wiring environments. It is most commonly used during network installation, troubleshooting, and maintenance to identify the exact path and endpoints of cables such as twisted pair (Ethernet), coaxial, or telephone wires. The cable tracer typically consists of two main components:

- **Tone Generator (Transmitter)** – This device sends a low-voltage signal through the cable under test.
- **Probe (Receiver)** – This hand-held device detects the electromagnetic signal emitted from the cable, allowing technicians to follow its path.

Figure 1: Cable Tracer

1.1 Working Principle

The tone generator is connected to one end of the cable, and it emits a specific frequency. The technician then moves the receiver probe along the suspected cable route. The probe produces an audible tone that gets louder as it nears the cable carrying the signal, helping to trace the cable's direction through walls, ceilings, or cable trays.

1.2 Usage in Lab

In our lab exercise, the cable tracer was used to identify and trace Ethernet cables running between workstations and the central switch panel. This was particularly useful in verifying that each workstation was correctly connected to the intended switch port. We also practiced identifying disconnected or mislabeled cables using the tone and probe method. This exercise demonstrated the importance of cable management and verification in real-world networking environments.

1.3 Advantages

- Helps in quickly identifying cable paths without disconnecting network devices.
- Useful in locating broken or damaged cables within walls or conduits.
- Saves time during troubleshooting and network deployment.

2 Cable Tester

A **cable tester** is an essential diagnostic tool used in computer networking to test the physical integrity and wiring configuration of network cables, particularly twisted-pair Ethernet cables terminated with RJ-45 connectors. The main purpose of a cable tester is to identify issues such as open circuits, short circuits, crossed wires, miswiring, and split pairs that can disrupt data transmission. Cable testers typically consist of two units:

- **Main Unit (Transmitter)**: Sends electrical signals through each wire in the cable.
- **Remote Unit (Receiver)**: Receives the signal and verifies whether each wire is correctly terminated.

Figure 2: Cable Tester

The cable tester visually displays the status of each pin via a row of LED indicators. If the cable is wired correctly (e.g., using the T-568B standard), all LEDs light up in a sequential and matching order on both ends. If there is a wiring error, such as a missing connection or reversed pair, the LEDs will either not light up or show an incorrect sequence.

2.1 Usage in Lab

During our networking hardware lab session, we used the cable tester to verify the integrity of custom-made Ethernet cables. After crimping RJ-45 connectors onto CAT5e cables following the T-568B wiring standard, we connected each end of the cable to the main and remote units of the tester. The LED lights helped us confirm whether all eight wires were correctly connected. If the lights did not match the correct pattern, we identified the faulty end and re-crimped the connector.

2.2 Benefits

- Saves time during troubleshooting by quickly identifying bad cables.
- Ensures that cables meet required standards before connecting them to network devices.
- Reduces network downtime caused by faulty or miswired cables.

Overall, the cable tester is a valuable tool in both academic and professional networking environments for ensuring reliable physical layer connectivity.

3 T-568B Wiring Standard

The **T-568B Wiring Standard** is one of the two recognized wiring configurations for terminating Ethernet cables using RJ-45 connectors. It defines the pin-out order the sequence of wire colors for the eight conductors inside a twisted-pair Ethernet cable. The standard is defined by the Telecommunications Industry Association (TIA) and is used to ensure uniformity and compatibility across network devices and installations. **Color Order : wo-o-wg-b-wb-g-wc-c**

3.1 Color Code Order

The color sequence for the T-568B standard, from pin 1 to pin 8, is as follows:

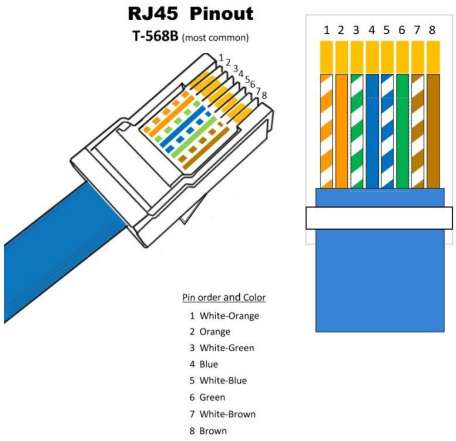

Figure 3: Wiring Standard

Each pair of colors represents a twisted pair of wires. The T-568B configuration places specific twisted pairs on specific pins to reduce cross-talk and ensure proper signal transmission.

3.2 Applications

The T-568B wiring standard is widely used in both residential and commercial Ethernet installations. It is compatible with modern networking equipment like switches, routers, and network interface cards (NICs). While both T-568A and T-568B are acceptable under ANSI/TIA standards, T-568B is more popular in the United States, especially in data installations.

3.3 Straight-Through and Crossover Cables

Straight-through Cable: Both ends of the cable use the T-568B wiring configuration. Used to connect dissimilar devices, such as a PC to a switch or a router to a modem.
Crossover Cable: One end uses T-568A and the other T-568B. Used to connect similar devices, such as switch-to-switch or PC-to-PC connections.

3.4 Importance in Lab

In our lab activities, we used the T-568B standard while crimping RJ-45 connectors onto Ethernet cables. This ensured consistency and correct connectivity throughout our network setup. The cables were then tested using a cable tester to confirm that all wires were correctly placed according to the T-568B configuration.

4 RS-232 Cable

The **RS-232 cable**, also known as a **serial cable**, is a standard communication cable used for **serial communication** between computers and peripheral devices. It is based on the **Recommended Standard 232 (RS-232)** developed by the **Electronic Industries Association (EIA)**, which defines the electrical characteristics and timing of signals, as well as the size and pin-out of connectors.

4.1 Purpose and Function

RS-232 cables are used to transmit **data serially (bit-by-bit)** between devices, typically between **Data Terminal Equipment (DTE)** like computers and **Data Communication Equipment (DCE)** like modems, printers, or routers. It is most commonly used for:

- Configuration of routers and switches via **console ports**
- Connection to serial modems
- Communication between PCs and embedded systems
- Debugging and monitoring microcontrollers

4.2 Physical Characteristics

- **Connectors**: RS-232 typically uses **DB9 (9-pin)** or **DB25 (25-pin)** connectors.
- **Cable type**: Unshielded twisted pair (UTP) or shielded cables depending on environment.
- **Voltage levels**: Logic levels are represented by **±3V to ±15V** (where +3 to +15V = logic 0 and -3 to -15V = logic 1).

4.3 Pin Configuration (DB9)

Pin	Signal Name	Description
1	DCD (Data Carrier Detect)	Detects modem connection
2	RXD (Receive Data)	Data received by DTE
3	TXD (Transmit Data)	Data sent by DTE
4	DTR (Data Terminal Ready)	DTE is ready to communicate
5	GND (Ground)	Common reference ground
6	DSR (Data Set Ready)	DCE is ready to communicate
7	RTS (Request to Send)	DTE requests transmission
8	CTS (Clear to Send)	DCE is ready to receive
9	RI (Ring Indicator)	Telephone ring indicator

Table 1: RS-232 DB9 Pin Configuration

Figure 4: RS-232 Cable

4.4 Communication Standard

- **Baud Rate**: Typically from **9600 to 115200 bps**.
- **Synchronous vs Asynchronous**: RS-232 uses **asynchronous communication**, where start and stop bits define each byte.
- **Distance Limitation**: Reliable communication is possible up to **15 meters (50 feet)**.

4.5 Use in Lab

In networking hardware labs, RS-232 cables are often used to:

- Connect PCs to routers or switches through the **console port**.
- Access command-line interfaces (CLI) using terminal software like **PuTTY**, **Tera Term**, or **Cisco Packet Tracer Terminal**.
- Perform initial configuration, IP assignment, and troubleshoot when no network access is available.

5 Fiber Optic (Duplex) Cable

Fiber optic cables are a critical component of modern high-speed communication networks. They use light signals to transmit data over long distances with minimal loss and electromagnetic interference. A **duplex fiber optic cable** consists of two optical fibers: one for transmitting (Tx) and one for receiving (Rx) data. This allows for simultaneous two-way communication, making duplex cables ideal for full-duplex networking.

5.1 Structure and Composition

Each fiber in the duplex cable is typically composed of:

- **Core:** The innermost glass or plastic region where light is transmitted.
- **Cladding:** Surrounds the core and reflects light back into the core using a lower refractive index.
- **Buffer Coating:** Protects the fiber from moisture and physical damage.
- **Outer Jacket:** Provides additional protection and structural integrity.

Duplex cables are often color-coded or labeled for easier installation and maintenance, with connectors on both ends, such as LC, SC, or ST types.

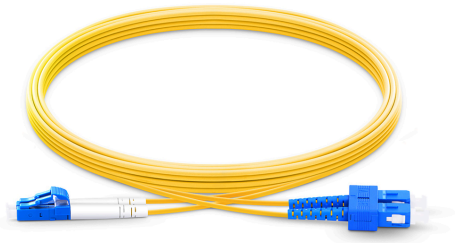

Figure 5: Fiber Optic Cable

5.2 Types of Fiber

There are two main types of fiber used in duplex cables:

- **Single-mode Fiber (SMF):** Used for long-distance communication, has a small core and transmits infrared laser light (wavelength 1310 or 1550 nm).
- **Multi-mode Fiber (MMF):** Used for short-distance communication, has a larger core and transmits LED light (wavelength 850 or 1300 nm).

5.3 Applications in Networking

- Backbone connections in LANs and WANs
- Internet Service Provider (ISP) infrastructures
- Data centers and server farms
- High-speed long-distance communication

6 SFP Module

The **Small Form-factor Pluggable (SFP)** module is a compact, hot-swappable transceiver used in network hardware for both telecommunication and data communication applications. It is designed to provide flexibility in network configuration and scalability by supporting various communication standards, such as Ethernet, Fibre Channel, and SONET/SDH.

6.1 Functionality

An SFP module acts as an interface between a network device (like a switch or router) and a fiber optic or copper network cable. It enables the device to send and receive data over different types of media by converting electrical signals to optical signals (or vice versa) depending on the media type.

Figure 6: SFP Module

6.2 Types of SFP Modules

There are several types of SFP modules available, depending on speed, range, and transmission medium:

- **SX (Short Wavelength)** – Typically used for short-range communication over multi-mode fiber.
- **LX (Long Wavelength)** – Designed for long-range communication over single-mode fiber.
- **ZX (Extended Range)** – Supports even longer distances using single-mode fiber.
- **Copper SFP (RJ-45)** – Used for Gigabit Ethernet over twisted pair copper cabling.

6.3 Applications in Networking

SFP modules are widely used in:

- Data centers
- Enterprise backbone links
- Telecommunication networks
- Campus LANs and WANs

7 Switch

A **network switch** is a fundamental device in computer networking that connects multiple devices (such as computers, printers, and servers) within a Local Area Network (LAN) and facilitates efficient data communication between them. It operates at the **Data Link Layer (Layer 2)** of the OSI model but can also support Layer 3 routing functions in advanced models.

7.1 Functionality

Unlike a hub, which broadcasts data to all ports, a switch is intelligent—it learns the MAC addresses of connected devices and forwards data only to the appropriate port based on the destination MAC address. This improves network efficiency and reduces unnecessary data traffic.

7.2 Types of Switches

- **Unmanaged Switch:** Plug-and-play device with no configuration needed; commonly used in home or small office networks.
- **Managed Switch:** Provides advanced features like VLANs, SNMP monitoring, port mirroring, and security settings; ideal for enterprise-level networks.
- **Layer 3 Switch:** Combines the functions of a router and switch, capable of performing routing functions based on IP addresses.

Figure 7: Switch

7.3 Applications in Networking

- Core component of LAN infrastructure
- Used in data centers to connect servers and storage
- Supports security and traffic management in enterprise networks

7.4 Importance in Lab

In our laboratory, network switches were used to interconnect multiple PCs and routers to form a structured LAN. We configured VLANs on managed switches to simulate departmental segmentation and observed how switches learn MAC addresses to forward frames efficiently. This provided hands-on experience in designing scalable and structured networks.

8 Router Configuration

A **router** is a networking device that connects different networks together and directs data packets between them. It operates primarily at the **Network Layer (Layer 3)** of the OSI model and is responsible for routing packets based on IP addresses. Router configuration is a critical task in network design, allowing proper communication, traffic control, and access between different segments of a network.

8.1 Basic Router Configuration Tasks

Router configuration typically involves several essential tasks, which can be performed via the router's Command Line Interface (CLI). The most common configuration steps are:

1. **Accessing the CLI:** Connect to the router using a console cable and open a terminal emulator or use console access in network simulators like Cisco Packet Tracer.
2. **Entering Privileged Mode:**

```
Router> enable
```

3. **Entering Global Configuration Mode:**

```
Router# configure terminal
```

4. **Setting the Hostname:**

```
Router(config)# hostname R1
```

5. **Configuring Interfaces:** Assign IP addresses to interfaces and enable them.

```
R1(config)# interface gig0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

6. **Setting a Default Route (Optional):** Used when the router needs to forward unknown destination packets.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.254
```

7. **Saving Configuration:**

```
R1# write memory
```

Figure 8: Router

8.2 Advanced Configuration Examples

- **Dynamic Routing Protocols (like RIP):**

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
```

- **NAT Configuration:** Configure NAT to translate private IP addresses to public ones.
- **DHCP Configuration:** Routers can be configured to act as DHCP servers in small networks.

8.3 Importance in Lab

In our Computer Network Hardware Lab, routers were configured to simulate real-world network scenarios. Tasks included setting up IP addresses on interfaces, configuring static and dynamic routing, enabling NAT, and establishing inter-VLAN routing. Through these configurations, we gained practical experience in how routers manage traffic between networks and ensure communication across different subnets.

9 Switch to Router Connection

In computer networking, connecting a switch to a router is a fundamental setup for enabling communication between local area network (LAN) devices and external networks (such as the internet). This configuration is also known as a **Router-on-a-Stick** setup when involving VLANs. The switch and router work together to forward traffic, manage network segmentation, and provide routing capabilities.

9.1 Purpose of Switch to Router Connection

- To allow hosts connected to the switch to communicate with devices in other networks.
- To route traffic between different VLANs when VLANs are configured on the switch.
- To provide internet access to LAN devices through the router.

9.2 Required Devices and Cables

- **Devices:** One router and one switch.
- **Cable:** Use a straight-through Ethernet cable for connecting a switch port to a router interface.

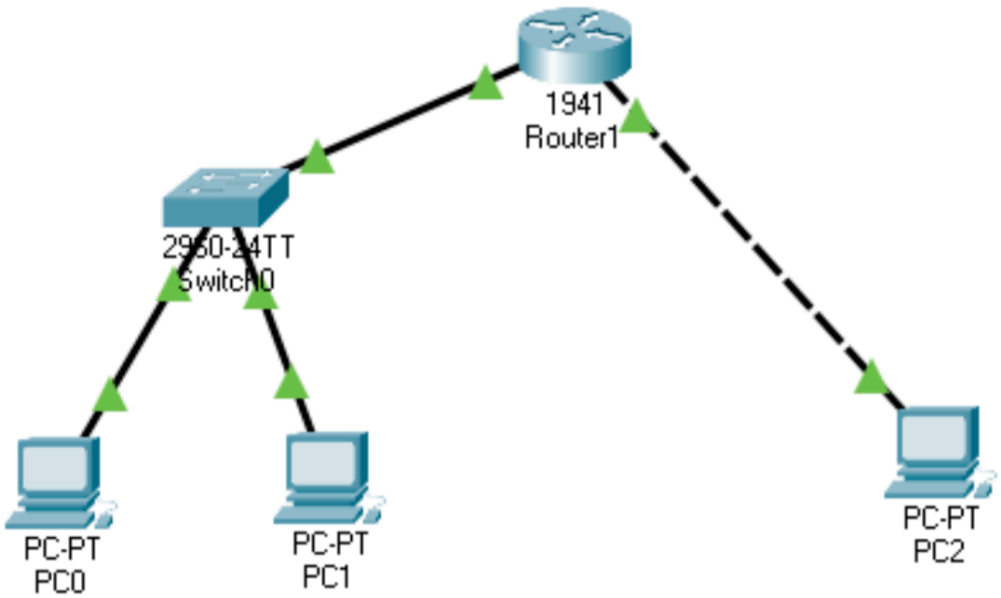

Figure 9: Switch to Router Connection in Cisco Packet Tracer

9.3 Basic Configuration Steps

Assume the following:

- Switch port: FastEthernet0/1
- Router port: GigabitEthernet0/0
- Subnet: 192.168.1.0/24

Step 1: Configure the Router Interface

```
Router> enable
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Step 2: Connect Devices

- Use a straight-through cable from the router's GigabitEthernet0/0 to the switch's FastEthernet0/1.
- Ensure devices connected to the switch (like PCs) are in the same subnet, e.g., 192.168.1.X, with default gateway set to 192.168.1.1 (router's IP).

Step 3: Test the Network

- From any PC connected to the switch, open the command prompt and ping the router's IP address:

```
ping 192.168.1.1
```

- Successful replies confirm the switch-to-router connection is functional.

9.4 Use in Lab Practice

In our lab, the switch-to-router connection was used to simulate a basic office LAN setup. By connecting the switch to a router and configuring the correct IP addressing, we enabled PCs connected to the switch to access other networks via the router. This helped us understand how routers manage traffic and how switches extend network connectivity within a LAN.

10 OSI Model

The **OSI (Open Systems Interconnection) Model** is a conceptual framework developed by the International Organization for Standardization (ISO) that standardizes the functions of a telecommunication or computing system into seven distinct layers. This model helps different networking systems to communicate with each other, regardless of their underlying architecture.

10.1 Purpose of the OSI Model

- Provides a universal standard for networking hardware and software.
- Helps in troubleshooting by isolating network problems layer by layer.
- Supports interoperability between various types of systems and technologies.

10.2 The Seven Layers of the OSI Model

1. **Application Layer (Layer 7)**
   This is the topmost layer that interacts directly with user applications. It provides services such as email, file transfer, and web browsing (e.g., HTTP, FTP, SMTP).
2. **Presentation Layer (Layer 6)**
   Responsible for translating data formats, data encryption/decryption, and compression. It ensures that data is readable by the receiving system (e.g., JPEG, MPEG, SSL/TLS).
3. **Session Layer (Layer 5)**
   Manages sessions between applications. It establishes, maintains, and terminates connections between devices (e.g., NetBIOS, RPC).
4. **Transport Layer (Layer 4)**
   Provides reliable data transfer through flow control, error checking, and segmentation (e.g., TCP, UDP).
5. **Network Layer (Layer 3)**
   Handles data routing, packet forwarding, and logical addressing (IP addressing). Routers operate at this layer (e.g., IP, ICMP).
6. **Data Link Layer (Layer 2)**
   Manages physical addressing (MAC addresses), error detection, and frame delivery. Switches operate at this layer (e.g., Ethernet, PPP).
7. **Physical Layer (Layer 1)**
   Deals with the physical connection between devices including cables, switches, voltages, and pin layouts. It transmits raw bit streams over a physical medium.

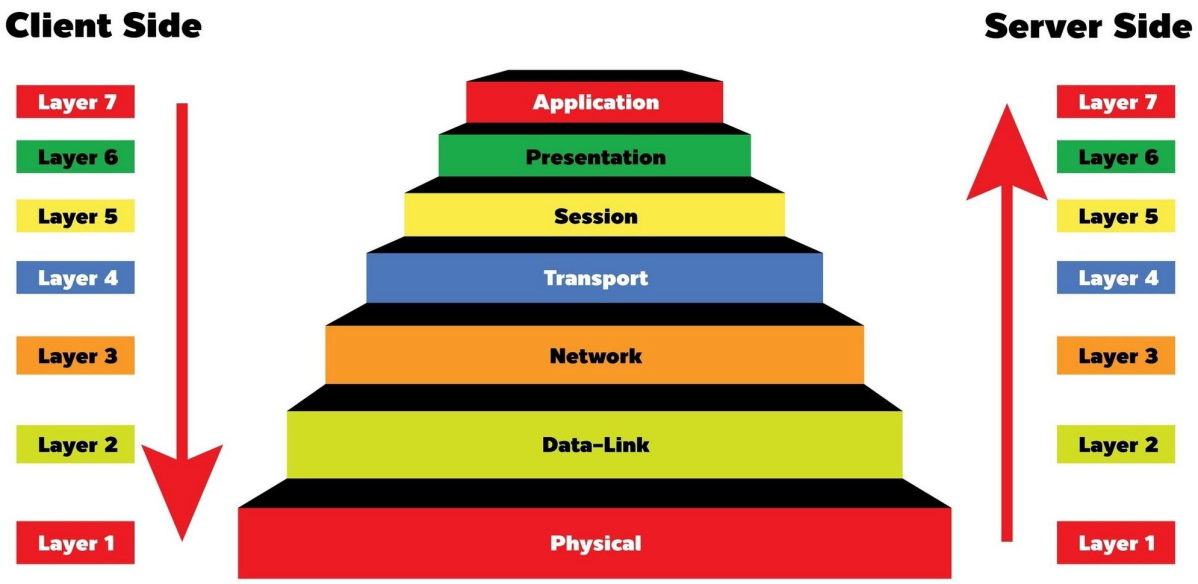

Figure 10: OSI Model

10.3 Mnemonic to Remember the Layers

"All People Seem To Need Data Processing" (from Layer 7 to Layer 1).

10.4 OSI Model in Networking Labs

In our networking lab, the OSI Model helped us to understand and troubleshoot communication between devices. For example:

- When a PC failed to ping another device, we checked Layer 1 (cable), Layer 2 (MAC), and Layer 3 (IP).
- During router configuration, we mainly worked with Layer 3 (Network Layer).
- Switch configuration tasks related to Layer 2 (Data Link Layer).

11 Conclusion

In conclusion, this lab provided a practical and insightful exploration into the foundational hardware and configurations used in modern computer networks. By working hands-on with tools such as cable tracers, cable testers, and various types of networking cables, we gained essential skills in identifying, connecting, and troubleshooting physical network components. The understanding and application of the T-568B wiring standard were especially important for ensuring correct cable assembly and communication between devices.

Moreover, the lab enabled us to explore vital networking equipment, including switches, routers, fiber optic cables, and SFP modules. Through router configurations involving Dynamic NAT and DHCP, we learned how data is dynamically translated and IP addresses are distributed, emphasizing the role of logical configurations in real-time networking. The demonstration of switch-to-router connections further reinforced our grasp of both physical and logical connectivity.

The introduction and discussion of the OSI Model allowed us to contextualize each hardware and protocol interaction within a structured framework. This layered approach to understanding network behavior proved invaluable when diagnosing connectivity issues and planning network architecture.

Overall, the lab successfully bridged theoretical networking concepts with their real-world applications, enhancing both our knowledge and confidence in setting up, maintaining, and troubleshooting basic to intermediate network infrastructures.