PNS School of Engineering & Technology,

Nisamani Vihar, Marshaghai, Kendrapara

PR:3 - COMPUTER NETWORKS LAB MANUAL

Prepared By

Mr. Balaram Das

Contents

Aim The Experiment-1:

Identification of Networking Cables and Connectors

To study and clearly identify various types of networking cables and connectors used in computer networks.

Apparatus Required

- Twisted pair cables (UTP/STP – Cat5, Cat5e, Cat6)
- Coaxial cable
- Optical fiber cable
- RJ-45 connector
- RJ-11 connector
- BNC connector
- Fiber connectors (SC, ST, LC)

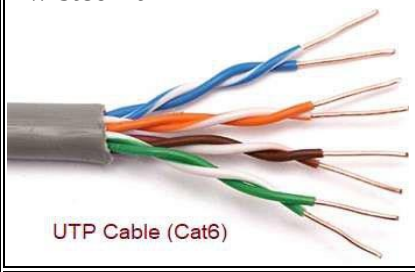
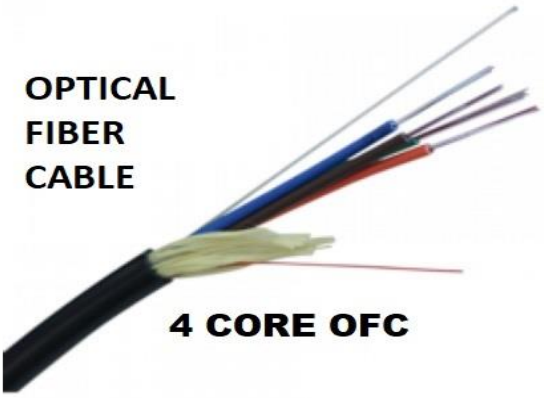
Theory

Networking cables and connectors form the physical medium through which data is transmitted in a network. Different cables are used based on bandwidth, speed, distance, and application. Connectors provide the interface between cables and networking devices.

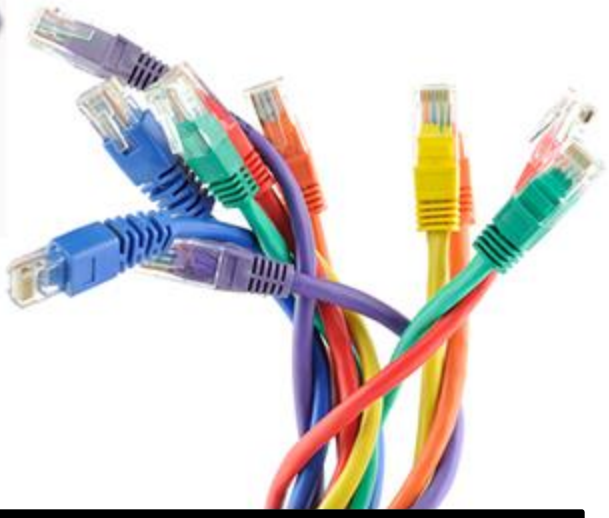
Procedure

1. Observe the given networking cables in the laboratory.
2. Identify the structure of each cable (number of wires, shielding, core).
3. Observe and identify various connectors used with each cable type.
4. Match each connector with its corresponding cable.
5. Note the typical application of each cable and connector.

Identification Table

Cable Type	Category / Type	Connector Used	Application
Twisted Pair 	Cat5 / Cat5e / Cat6	RJ-45 	LAN, Ethernet
Coaxial 	RG-6 / RG-58	BNC 	Cable TV, legacy networks
Optical Fiber 	Single-mode / Multi-mode	SC / ST / LC 	High-speed backbone

Fiber connectors (SC, ST, LC)



- Twisted pair cables use RJ-45 connectors for Ethernet communication.

Observation

- Twisted pair cables use RJ-45 connectors for Ethernet communication.
- Coaxial cables use BNC connectors.
- Optical fiber cables use specialized fiber connectors.

Conclusion

Understanding different networking cables and connectors is essential for selecting the appropriate physical medium for network installation.

Aim The Experiment-2:

Comparing Specifications of Network Cables and Connectors from Different Companies

To compare and analyze the specifications of networking cables and connectors available from different manufacturers on the internet and identify the key differences.

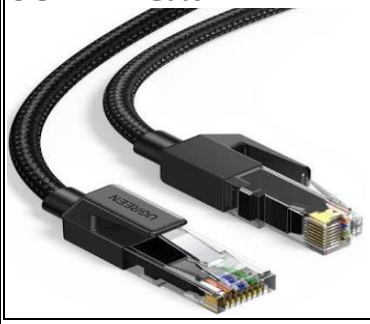
Apparatus

- **UGREEN Cat6 1000Mbps 250MHz U/UTP RJ45 Patch Ethernet Cable**
- **Terabyte Patch Cable Cat5e Lan**
- **Amazon Basics RJ45 Cat-5e Network Ethernet Patch/LAN Cable**
- **C & EC & E-RJ45 Ethernet Cable Connectors**
- **Cat5, Cat5e & Cat6 UTP RJ45 Connector 8P8C Plug**
- Internet browser for looking up product specifications

Procedure

1. **Search online** for specifications of networking cables (such as Cat5e, Cat6) from multiple brands.
2. Record key parameters for each cable, such as **bandwidth, speed rating, frequency rating, shielding type, conductor gauge**, etc.
3. **Search online** for specifications of RJ45 connectors made by different companies.
4. Compare and **note differences** between products from various brands in terms of performance, build quality, and intended application.
5. Tabulate results for easy comparison.

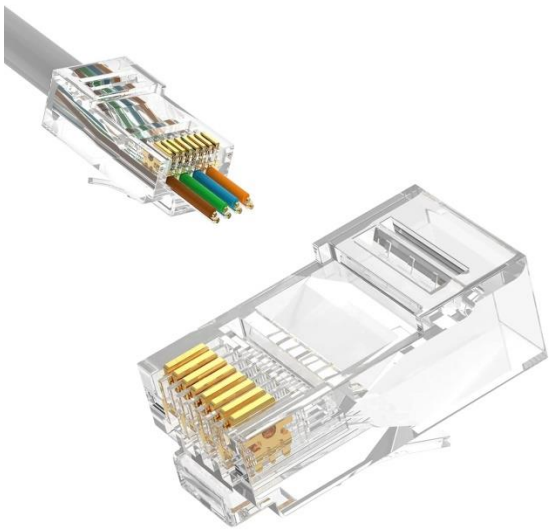
Observation & Data (Example)

Product	Cable Category	Speed Support	Frequency	Conductor	Shielding	Notes
UGREEN Cat6 	Cat6	Up to 1000 Mbps	250 MHz	Usually 23 AWG	U/UTP (Unshielded)	Higher bandwidth, suitable for gigabit networks
Terabyte Cat5e 	Cat5e	Up to 1000 Mbps	100 MHz	24 AWG	Usually UTP	Standard for most home networks
Amazon Basics Cat5e 	Cat5e	Up to 1000 Mbps	100 MHz	24 AWG	UTP	Good for general use

Connector Specifications:

- The **C & EC & E-RJ45 Ethernet Cable Connectors** and **Cat5, Cat5e & Cat6 UTP RJ45 Connector 8P8C Plug** are both RJ45 plugs designed for Cat5e/Cat6 standards, but quality of plating and build may differ.

From product pages and online specs, higher-quality cables often feature **gold-plated connectors** which improve signal integrity by reducing corrosion and contact resistance. Some connectors also offer **strain relief boots** which protect the cable termination from mechanical stress. (Network Hard wares)



C & EC & E-RJ45 Ethernet Cable Connectors

Key Differences Found

✔ Bandwidth / Frequency Differences

- Cat6 cables typically support up to **250 MHz**, while Cat5e supports **100 MHz**. Higher frequency allows more data to pass through per second. (SF Cable)

✔ Data Rates

- Cat5e cables support up to **1 Gbps** over 100 m.
- Cat6 cables can support **1 Gbps at 100 m** and **10 Gbps over shorter distances (≈55 m)**. (SF Cable)

✔ Conductor Gauge

- Cat6 often uses thicker **23 AWG** copper for improved signal quality, while Cat5e commonly uses **24 AWG**. (HeyOptics)

✔ Connector Build Quality

- Some products use **gold-plated contacts** on RJ45 plugs for better conductivity and corrosion resistance. (Network Hardwares)
- Strain relief boots vary by brand — better boots increase cable durability. (Network Hardwares)

✔ **Shielding Options**

- Some Cat6 variants may come with **shielded pairs (STP / FTP)** to reduce interference, whereas many Cat5e cables are unshielded (UTP). (SF Cable)

Conclusion

By comparing specifications of network cables and connectors from various manufacturers, we understand that:

- Higher category cables (e.g., Cat6 v/s Cat5e) offer **better performance** at higher frequencies.
- Connector quality (plating, strain relief) impacts signal reliability.
- Choose cables and connectors based on **required network speed, distance, and environment**.

Aim The **Experiment -3:**

Making Patch Cords Using Different Types of Cables and Connectors

To prepare network patch cords using different types of cables and connectors by performing crimping and splicing techniques.

Apparatus Required

- UTP cable (Cat5e / Cat6)
- RJ-45 connectors
- Crimping tool
- Wire stripper and cutter
- Cable splicing connectors (or insulation tape for demonstration)
- LAN cable tester

Theory

A patch cord is a short network cable used to connect devices such as computers, switches, and routers. Patch cords are made by terminating Ethernet cables with RJ-45 connectors using a crimping process. Proper crimping and splicing ensure reliable data transmission and reduce signal loss.

Procedure

A. Preparation of Patch Cord by Crimping

1. Cut the required length of UTP cable.
2. Strip about 2–3 cm of the outer insulation.
3. Untwist the wire pairs and arrange them according to the standard:
    - **T568B order:**
      White-Orange, Orange, White-Green, Blue, White-Blue, Green, White-Brown, Brown
4. Trim the wires evenly.
5. Insert the wires into the RJ-45 connector ensuring correct order.
6. Place the connector into the crimping tool and crimp firmly.
7. Repeat the same process on the other end of the cable to make:
    - Straight-through cable (same standard both ends)
    - Crossover cable (T568A at one end and T568B at the other)

B. Splicing of Network Cable (Demonstration)

1. Cut two Ethernet cables to be joined.
2. Strip the outer insulation from both cable ends.
3. Match and twist corresponding colored wires together.
4. Secure each joint using splicing connectors or insulation tape.
5. Cover the joint with outer insulation to protect it.

Testing of Patch Cord

- Connect the prepared patch cord to a LAN cable tester.
- Check for continuity, correct wire mapping, and absence of short circuits.

Observation

- Correctly crimped cables showed proper LED sequence in the tester.
- Incorrect wire order resulted in faulty indication.
- Spliced cables worked but showed reduced reliability compared to crimped patch cords.

Conclusion

Crimping provides a reliable and professional method for making patch cords, while splicing is useful for temporary repairs. Proper color coding and firm crimping are essential for error-free communication.

Aim The **Experiment -4:**

Demonstration and Use of Cable Testers

To study different types of network cable testers and use them to test patch cords prepared by students in the laboratory and standard cables prepared by professionals.

Apparatus Required

- Student-made patch cords
- Professionally made standard patch cords
- Basic LAN cable tester
- Advanced cable tester / cable certifier
- Power supply or batteries for testers

Theory

Cable testers are used to verify the integrity and correctness of network cables. They detect wiring faults such as open circuits, short circuits, crossed pairs, and incorrect terminations. Testing ensures reliable data transmission and helps in troubleshooting network problems.

Types of Cable Testers

1. **Basic LAN Cable Tester**
    - Checks continuity and wire mapping
    - Indicates open, short, or miswired cables
    - Commonly used in educational labs
2. **Advanced Cable Tester / Certifier**
    - Measures cable length
    - Detects attenuation and signal quality
    - Certifies cables for specific standards (Cat5e, Cat6)

Procedure

A. Testing Student-Prepared Patch Cords

1. Connect one end of the patch cord to the main unit of the tester.
2. Connect the other end to the remote unit.
3. Switch on the tester.
4. Observe the LED sequence or display output.

5. Note whether all pairs are correctly connected.

B. Testing Professionally Made Patch Cords

1. Connect the standard cable to the tester.
2. Power on the tester.
3. Observe the results.
4. Compare the readings with student-made cables.

Observation Table

Cable Type	Continuity	Wire Mapping	Fault Detected
Student-made Cable	Yes / No	Correct / Incorrect	None / Cross / Open
Professional Cable	Yes	Correct	None

Observation

- Professionally made cables showed correct wiring and stable test results.
- Some student-made cables showed wiring errors due to improper crimping.
- Advanced testers provided additional information like cable length and signal quality.

Conclusion

Cable testing is essential for verifying cable reliability. Basic testers are sufficient for checking continuity, while advanced testers ensure compliance with networking standards.

Aim The **Experiment-5:**

Configuring Computing Devices for Network Connectivity

To configure computing devices such as PC, laptop, and mobile for network connectivity and study the impact of different network configuration options like IP address, gateway, DNS, and security settings.

Apparatus Required

- PC / Laptop
- Mobile phone
- Network switch / Wi-Fi router
- Ethernet cable
- Internet connection

Theory

For a device to communicate on a network, it must be properly configured with network parameters. These include IP address, subnet mask, default gateway, and DNS server. Security options protect devices from unauthorized access and threats. Incorrect configuration can result in network failure or limited connectivity.

Procedure

A. Configuration on PC / Laptop

1. Open **Network Settings**.
2. Select **Ethernet** or **Wi-Fi** connection.
3. Choose **IP settings**:
    - **Automatic (DHCP)** or
    - **Manual (Static IP)**.
4. Enter:
    - IP Address
    - Subnet Mask
    - Default Gateway
    - DNS Server
5. Save the settings.
6. Test connectivity using:
    - `ping` command
    - Web browser

B. Configuration on Mobile Device

1. Open **Wi-Fi settings**.
2. Connect to the desired network.
3. Choose **Advanced settings**.
4. Configure:
    - DHCP or Static IP
    - DNS settings
5. Enable or disable security features (e.g., VPN, firewall apps).
6. Test connectivity by browsing or pinging (if available).

Configuration Options and Their Impact

Parameter	Description	Impact
IP Address	Unique device identifier	Incorrect IP causes network conflict
Subnet Mask	Defines network size	Wrong mask blocks communication
Default Gateway	Route to other networks	No internet if incorrect
DNS Server	Resolves domain names	Slow or no browsing if misconfigured
Security Settings	Firewall, encryption	Affects access and safety

---

Observation

- Devices configured with DHCP connected automatically.
- Static IP required correct manual entry.
- Incorrect gateway or DNS prevented internet access.
- Enabling security features improved protection but may restrict access.

Conclusion

Proper network configuration is essential for successful communication. Understanding the impact of IP addressing, DNS, gateway, and security options helps in troubleshooting and maintaining secure networks.

Aim The **Experiment-6:**

Study and Identification of Networking Devices

To study and identify various networking devices such as Network Interface Cards (NICs), Hub, Switch, Router, and Wi-Fi Access Point and understand their functions.

Apparatus Required

- Network Interface Card (wired and wireless)
- Hub
- Switch
- Router
- Wi-Fi Access Point
- Ethernet cables

Theory

Networking devices are used to connect computers and other devices in a network. Each device performs a specific function at different layers of the OSI model and plays an important role in data transmission and network management.

Procedure

1. Observe each networking device provided in the laboratory.
2. Identify physical ports, indicators (LEDs), and connectors.
3. Note the function and working principle of each device.
4. Compare similar devices such as hub v/s switch and router v/s access point.

Description of Networking Devices

1. Network Interface Card (NIC)

- Connects a device to a network.
- Can be wired (Ethernet) or wireless (Wi-Fi).
- Works at Physical and Data Link layers.

2. Hub

- Central connection device.
- Broadcasts data to all ports.
- Works at Physical layer.

3. Switch

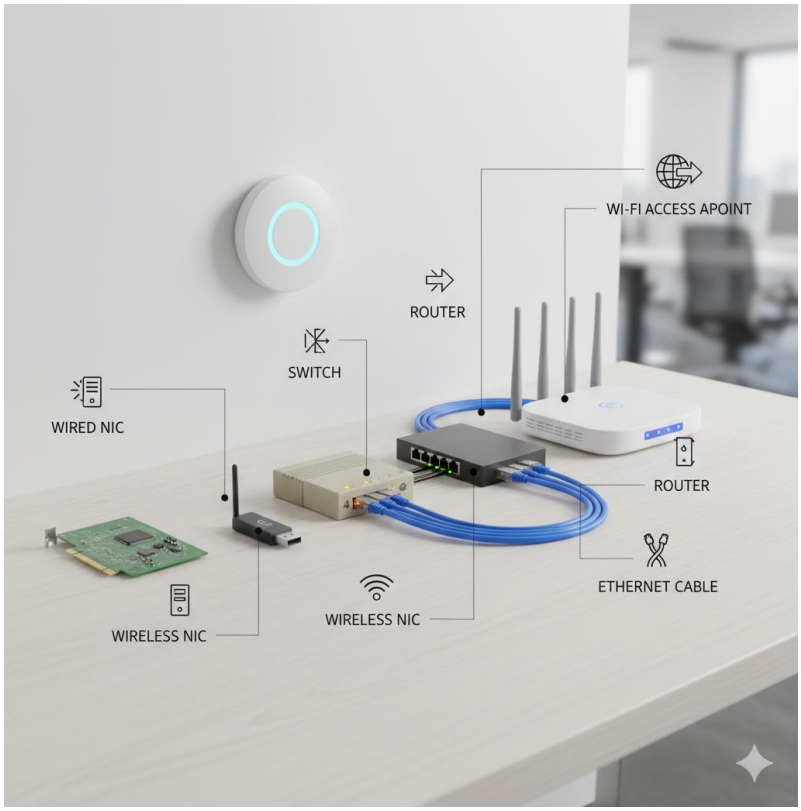
- Forwards data only to the intended device.
- Uses MAC addresses.
- Works at Data Link layer.

4. Router

- Connects different networks.
- Uses IP addresses for routing.
- Works at Network layer.

5. Wi-Fi Access Point

- Provides wireless connectivity.
- Connects wireless devices to wired network.
- Supports wireless security protocols.



Observation Table

Device	Function	OSI Layer	Key Feature
NIC	Network connection	Physical/Data Link	MAC address
Hub	Broadcast device	Physical	No filtering
Switch	Intelligent forwarding	Data Link	Reduces traffic
Router	Network routing	Network	Internet access
Wi-Fi AP	Wireless access	Data Link	Mobility

Observation

- Switches are more efficient than hubs.
- Routers enable communication between networks.
- Access points provide wireless mobility.

Conclusion

Understanding networking devices is essential for designing, installing, and troubleshooting computer networks.

Aim The **Experiment-7:**

Setting Up a Small Wired LAN in the Laboratory

To set up and configure a small wired Local Area Network (LAN) in the laboratory and test connectivity between connected computers.

Apparatus Required

- 2–4 PCs / Laptops
- Network switch
- Ethernet (UTP) patch cords
- Network Interface Cards (NICs)
- Power supply

Theory

A wired LAN connects multiple computers using Ethernet cables and networking devices such as switches. Each device is assigned an IP address to enable communication. Proper physical connections and correct IP configuration are required for successful data transfer.

Procedure

A. Physical Setup

1. Place the network switch at a central location.
2. Connect each PC to the switch using Ethernet patch cords.
3. Power on the switch and all computers.
4. Ensure link indicator LEDs glow on the switch and NICs.

B. Network Configuration

1. Open **Network Settings** on each PC.
2. Configure IP address manually (Static IP):
    - PC1: 192.168.1.1
    - PC2: 192.168.1.2
    - PC3: 192.168.1.3
    - Subnet Mask: 255.255.255.0
3. Leave Default Gateway blank (or optional).

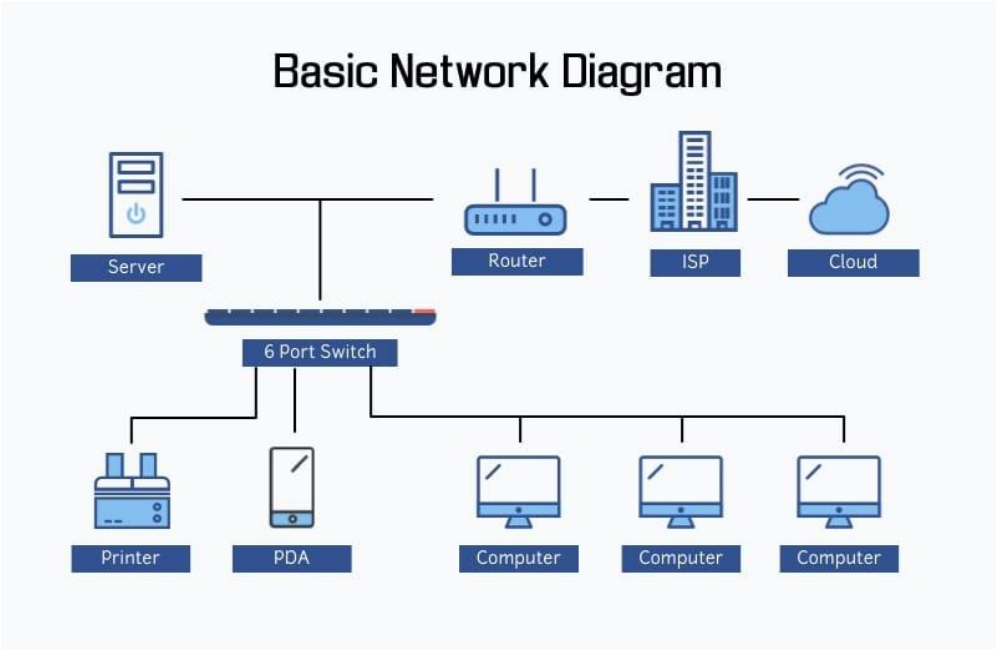
4. Save settings.

C. Testing Connectivity

1. Open Command Prompt.
2. Use the `ping` command to test connectivity:

```
3. ping 192.168.1.2
```

4. Repeat ping test between all PCs.



Observation

- Link LEDs indicated proper cable connection.
- Ping replies confirmed successful communication.
- Incorrect IP settings caused connectivity failure.

Conclusion

Wired LANs provide reliable and high-speed communication. Proper cabling and IP configuration are essential for network functionality.

Aim The **Experiment-8:**

Setting Up a Small Wireless LAN in the Laboratory

To set up and configure a small Wireless Local Area Network (WLAN) in the laboratory and test wireless connectivity between devices.

Apparatus Required

- Wi-Fi router / Wireless Access Point
- Laptop / PC with Wi-Fi adapter
- Mobile phones
- Internet connection (optional)
- Power supply

Theory

A wireless LAN allows devices to connect to a network using radio waves instead of physical cables. A Wi-Fi router or access point provides wireless connectivity by broadcasting a network name (SSID). Proper security configuration is necessary to prevent unauthorized access.

Procedure

A. Router / Access Point Configuration

1. Power on the Wi-Fi router or access point.
2. Connect a laptop/PC to the router using Ethernet or Wi-Fi.
3. Open a web browser and enter the router's IP address (e.g., 192.168.1.1).
4. Log in using administrator credentials.
5. Set:
    - **SSID (Network Name)**
    - **Wireless Mode**
    - **Security type (WPA2/WPA3)**
    - **Password**
6. Save the configuration and reboot if required.

B. Connecting Wireless Devices

1. Enable Wi-Fi on laptops and mobile devices.
2. Select the configured SSID.
3. Enter the Wi-Fi password.
4. Ensure the device obtains an IP address automatically (DHCP).

C. Testing Connectivity

1. Check IP address on connected devices.
2. Test connectivity by:
    - Pinging the router
    - Accessing shared resources or browsing the internet

Observation

- Devices connected successfully to the wireless network.
- DHCP assigned IP addresses automatically.
- Security settings prevented unauthorized access.

Conclusion

Wireless LANs provide flexibility and mobility. Proper configuration of SSID, security, and DHCP ensures secure and reliable wireless communication.