

Practical 1 – Computer Networks Lab

Name: Neeraj Belsare

Roll No.: 79

Batch: A4

PRN: 202101040133

Title:

Making a patch cord

Aim:

Setup a wired LAN using Layer 2 Switch and then IP switch of minimum four computers. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrate the PING packets captured traces using Wireshark Packet Analyzer Tool.

Theory:

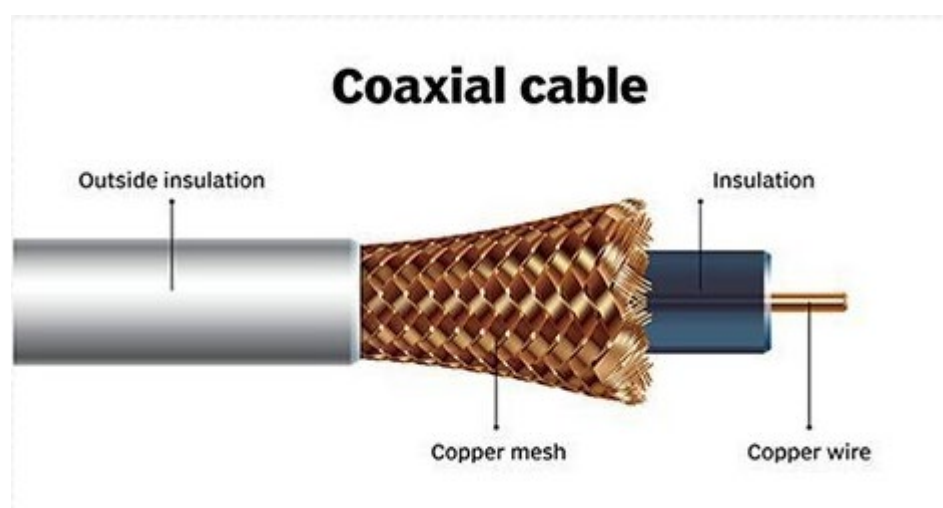
Networking Cables:

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners, etc. Different types of network cables, such as coaxial, optical fibre, and twisted pair cables, are used depending on the network's physical layer, topology, and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet). There are several technologies used for network connections. Patch cables are used for short distances in offices and wiring closets. Electrical connections using twisted pairs or coaxial cables are used within a building. Optical fibre cable is used for long distances or for applications requiring high bandwidth or electrical isolation. Many installations use structured cabling practices to improve reliability and maintainability. Power lines are used as network cabling in some home and industrial applications.

A. Coaxial Cable:

Coaxial cable, commonly known as coax cable, is an electrical cable with a unique construction featuring two concentric conductors sharing a common axis. The inner conductor carries the signal and is surrounded by dielectric insulation, ensuring electrical separation. An outer conductor, or shield, provides shielding against interference and serves as the signal's return path. A protective jacket encases the cable.

Coaxial cables are prized for their shielding capabilities, making them ideal for applications where signal integrity is vital, such as cable television and internet connections. They offer low signal loss over long distances and efficiently transmit a broad spectrum of frequencies, from analog TV signals to high-frequency digital data. Various connectors, like F-connectors or BNC connectors, ensure reliable connections.

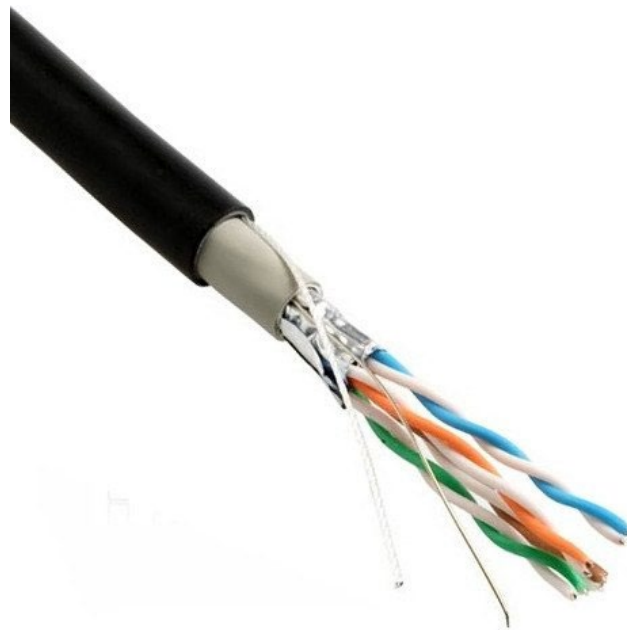


B. Twisted Pair Cable:

Twisted pair cable is a common type of electrical cable used for transmitting data and signals in telecommunications and computer networks. It consists of pairs of insulated copper wires twisted together to reduce electromagnetic interference and crosstalk. There are two main categories of twisted pair cables: Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP).

(i) Shielded Twisted Pair (STP) cable:

Shielded Twisted Pair (STP) cable is a type of electrical cable commonly employed in networking and telecommunications to transmit data and signals. What sets STP apart from its Unshielded Twisted Pair (UTP) counterpart is its additional shielding layer, usually made of metal foil or braided copper, which surrounds the individual twisted pairs of copper wires within the cable. This shielding serves a critical role in protecting the cable's signal integrity by minimizing the impact of external electromagnetic interference (EMI) and radio frequency interference (RFI).

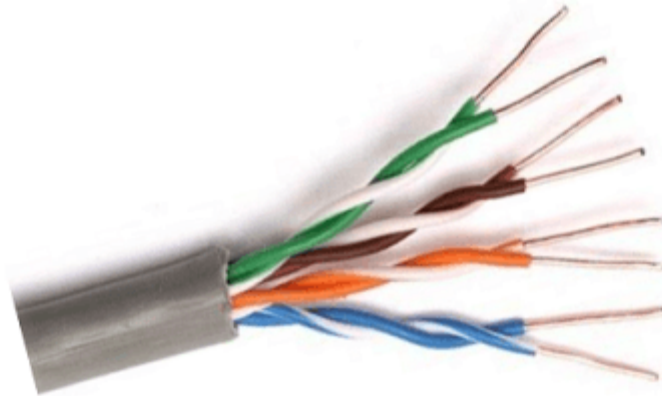


(ii) Unshielded Twisted Pair (STP) cable:

Unshielded Twisted Pair (UTP) cable is a widely used type of copper cable in networking and telecommunications. It consists of pairs of insulated copper wires twisted together. Each pair of wires is colour-coded for identification, and the entire bundle is encased in a flexible plastic sheath. UTP cables come in various categories (e.g., Cat 5e, Cat 6, Cat 6a, Cat 7), with each category offering different performance specifications.

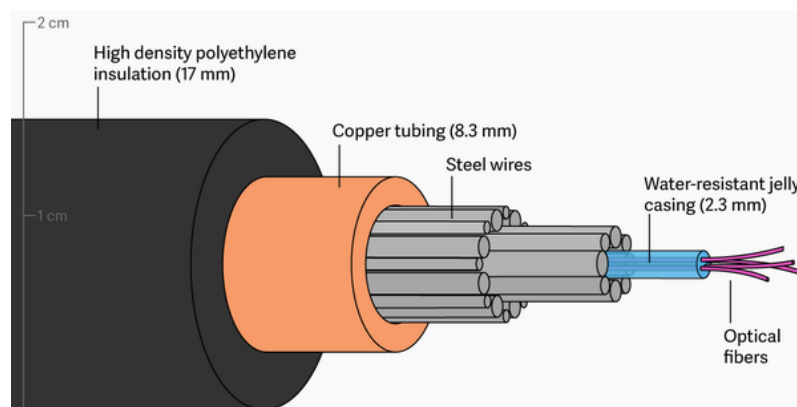
One of the key advantages of UTP cables is their cost-effectiveness. They are affordable and readily available, making them a popular choice for both residential and commercial installations. UTP cables are relatively easy to install and terminate, and they are known for their flexibility and ease of handling.

Unshielded Twisted Pair Cable



C. Fiber Optics:

Instead of insulated metal wires transmitting electrical signals, fiber optic network cables work using strands of glass and pulses of light. These network cables are bendable despite being made of glass. They have proven especially useful in wide area network (WAN) installations where long-distance underground or outdoor cable runs are required and also in office buildings where a high volume of communication traffic is common. Two primary types of fiber optic cable industry standards are defined – single-mode (100BaseBX standard) and multimode (100BaseSX standard). Long-distance telecommunications networks more commonly use single-mode for their relatively higher bandwidth capacity, while local networks typically use multimode instead due to its lower cost.



Line Tester:

A line tester, also known as a network cable tester, is a device used to check network cable integrity and connections. It verifies continuity, wiring correctness, polarity, and detects short circuits. Some models can identify cable types, generate test signals, and have remote units for distance testing. These testers are essential for maintaining reliable network connections and troubleshooting cable-related issues.

IP Address:

An IP (Internet Protocol) address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. IP addresses serve two primary functions: host or network interface identification and location addressing. There are two primary types of IP addresses:

IPv4 Address: This is the older and more common type of IP address. It consists of a 32-bit binary number, typically displayed as four decimal numbers separated by periods (e.g., 192.168.1.1). IPv4 addresses are running out due to the rapid growth of the internet, and this has led to the adoption of IPv6.

IPv6 Address: IPv6 (Internet Protocol version 6) is the next generation of IP addressing. It uses a 128-bit address format, expressed as a series of eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv6 was introduced to address the shortage of IPv4 addresses and provide a vastly larger address space.

Ping Command:

The "ping" command is a network utility tool available in most operating systems, including Windows, macOS, Linux, and others. It is used to test the reachability and responsiveness of a host or network device on an IP network. The ping command works by sending ICMP (Internet Control Message Protocol) echo request packets to the target host and waiting for ICMP echo reply packets in response.

Wireshark:

Wireshark is a widely used open-source network protocol analyzer. It is a powerful tool for capturing, inspecting, and analyzing network traffic and communication protocols in real time. Some key features and functions of Wireshark are as follows:

1. **Packet Capture:** Wireshark allows you to capture packets on a network interface in real-time. This feature is invaluable for troubleshooting network issues, monitoring network activity, and analyzing network performance.
2. **Protocol Support:** Wireshark supports a vast array of network protocols, including common ones like TCP, UDP, HTTP, DNS, and more obscure or proprietary ones. It can dissect and display packet information for hundreds of different protocols.
3. **Packet Inspection:** Users can drill down into captured packets to inspect the details of each packet, including header information, data payload, and flags. This level of granularity is essential for diagnosing network problems and understanding how protocols work.
4. **Display Filters:** Wireshark offers powerful display filtering capabilities, allowing you to filter packets based on various criteria such as source and destination IP addresses, port numbers, protocol types, and more. This helps you focus on specific traffic of interest.
5. **Color Coding:** Packets are colour-coded based on their type or significance, making it easier to spot issues or unusual behaviour in network traffic.
6. **Protocol Hierarchy:** Wireshark provides a hierarchy view of protocols used in the captured traffic, showing which protocols are encapsulated within others. This is helpful for understanding complex communication patterns.

7. **Statistics and Graphs:** It offers various statistical tools and graphical representations to analyze network traffic patterns, including conversation statistics, endpoint statistics, and round-trip time graphs.
8. **Export and Saving:** You can save captured traffic in various formats, such as PCAP, to review later or share with others. Wireshark can also export data in formats compatible with other analysis tools.
9. **Extensibility:** Wireshark is extensible through plugins and dissectors, allowing users to add support for new protocols or customize the behaviour of the application.
10. **Cross-Platform:** It is available for multiple operating systems, including Windows, macOS, and Linux, making it accessible to a broad range of users.

Wireshark is commonly used by network administrators, security professionals, developers, and anyone involved in troubleshooting or analyzing network issues. It's a valuable tool for diagnosing problems, monitoring network security, and gaining insights into network behaviour.

Procedure/code:

Step 1: Cable Preparation

Gather the necessary materials: Ethernet cables (Cat 5e or Cat 6), RJ45 connectors, a cable crimper, and a cable cutter/stripper.

Cut the Ethernet cable to the desired length for each connection, ensuring that it's long enough to reach the switch or other computers but not excessively long.

Strip about 1-2 inches of the outer cable jacket at both ends of the Ethernet cable to expose the individual twisted pairs.

Untwist the pairs and arrange them according to the T568A or T568B wiring standard. This ensures consistency in wiring across all cables.

Insert the twisted pairs into an RJ45 connector, making sure they align correctly with the connector's pins.

Use a cable crimper to secure the connector onto the cable, ensuring a proper connection.

Repeat the above steps for all the Ethernet cables needed.

Step 2: Line Testing

To ensure the cables are properly wired, use a cable line tester to verify connectivity. Connect one end of the cable to the tester's transmitter and the other end to the receiver.

Power on the tester and check for a successful connection indication. It should confirm that the cables are correctly wired and free of any shorts or open circuits.

Step 3: Setting Up the Wired LAN

Connect one end of each Ethernet cable to the Ethernet ports on each computer, and the other ends to available ports on the Layer 2 switch. Ensure a secure connection.

Step 4: Unique IP Address Configuration

On each computer, assign a unique static IP address within the same subnet. For example:

Computer 1: IP Address - 192.168.1.1

Computer 2: IP Address - 192.168.1.2

Computer 3: IP Address - 192.168.1.3

Computer 4: IP Address - 192.168.1.4

Subnet Mask - 255.255.255.0

Configure the default gateway (if needed) to point to the IP address of the Layer 2 switch.

Step 5: Ping Testing

Open the command prompt or terminal on each computer.

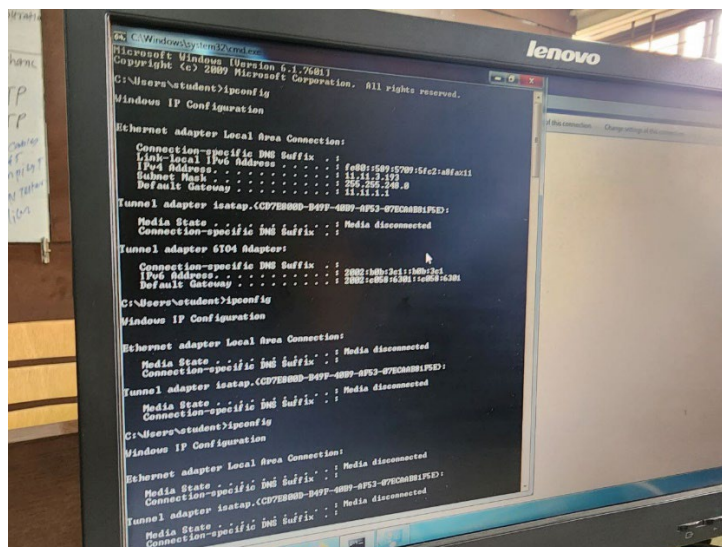
Use the PING utility to test connectivity between computers. For example, from Computer 1, you can ping Computer 2 with the following command:

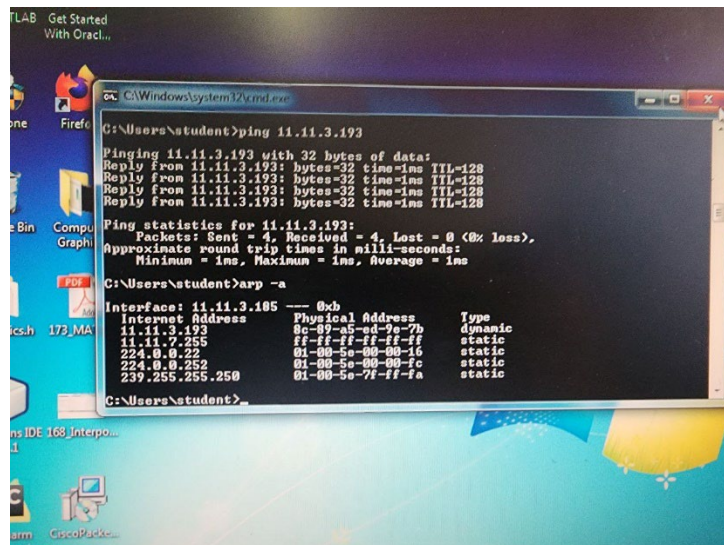
Copy code

ping 192.168.1.2

Verify that you receive replies indicating successful connectivity.

Output:





```
C:\Users\student>ping 11.11.3.193

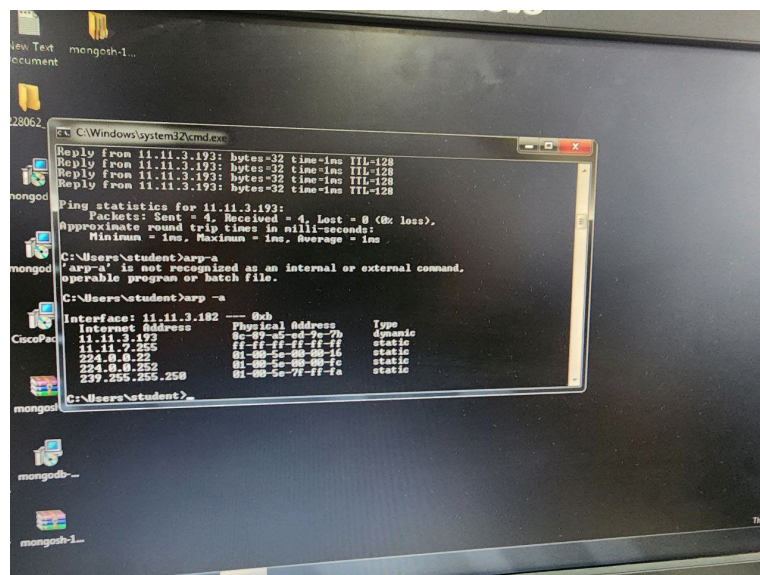
Pinging 11.11.3.193 with 32 bytes of data:
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128

Ping statistics for 11.11.3.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\student>arp -a

Interface: 11.11.3.195 --- 0xb
Internet Address      Physical Address      Type
11.11.3.193           00-00-a5-e1-9e-7b    dynamic
11.11.7.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\student>
```



```
C:\Users\student>ping 11.11.3.193

Reply from 11.11.3.193: bytes=32 time=1ms TTL=128
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128
Reply from 11.11.3.193: bytes=32 time=1ms TTL=128

Ping statistics for 11.11.3.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\student>arp -a
'arp -a' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>arp -a

Interface: 11.11.3.192 --- 0xb
Internet Address      Physical Address      Type
11.11.3.193           00-00-a5-e1-9e-7b    static
11.11.7.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\student>
```

Conclusion:

In this practical exercise, we established a wired LAN using a Layer 2 switch, connecting four computers. We prepared Ethernet cables, ensured connectivity with a line tester, configured unique IP addresses, and verified network connectivity using the PING utility. We also demonstrated the capture and analysis of PING packets using Wireshark. This hands-on experience underscores the importance of LAN setup, IP configuration, and network diagnostics.