Network Security and Forensics

Lab Session 2

Submitted To:-

Dr. Lokesh Chauhan Sir

Submitted By:-

Saloni Rangari

M.Tech. AIDS

1. Study and demonstration of network Cable.

- Forming of network cable CAT-6 cables

Category 6 (CAT-6) cables are a type of twisted pair cable standard used for Ethernet and other network physical layers. CAT-6 cables are backward compatible with the Category 5/5e and Category 3 cable standards. They support Gigabit Ethernet and are capable of transmitting data at a rate of up to10 Gbps, with a maximum frequency of 250 MHz.

1. Key Features:

- Twisted Pair: Each cable contains four pairs of copper wires, each twistedtogether to reduce interference from external sources.

- Bandwidth: Up to 250 MHz.

- Speed: Supports up to 10 Gbps Ethernet (10GBASE-T).

- Distance: Maximum length of 55 meters for 10 Gbps, up to 100 meters forlower speeds (1 Gbps or 100 Mbps).

2. Materials Needed for Forming CAT-6 Cables:

1. CAT-6 Cable: Unshielded Twisted Pair (UTP) cable.

2. RJ-45 Connectors: For terminating the cable.

3. Crimping Tool: For attaching the RJ-45 connectors to the cable.

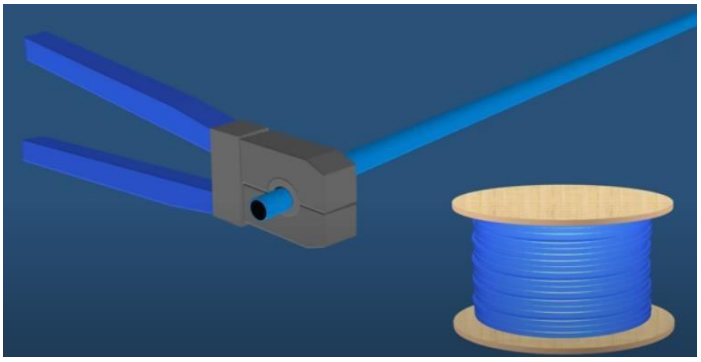
4. Cable Stripper/Cutter: For stripping the outer sheath of the cable andcutting it to length.

5. Cable Tester: To test the continuity and proper wiring of the cable.

3.Steps to Form a CAT-6 Network Cable:

1. Cut the Cable to the Desired Length:

- Use the cable cutter to cut the CAT-6 cable to the length required for yournetwork setup.

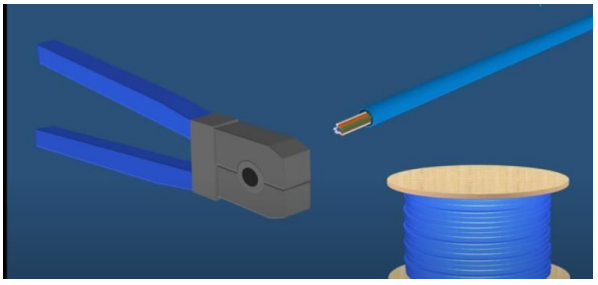


2. Strip the Cable Jacket:

- Using the cable stripper, remove about 2-3 cm of the outer jacket fromboth ends of the cable. Be careful not to nick the wires inside.

3. Untwist the Pairs:

- Untwist the pairs of wires inside the cable jacket. There are four pairs(eight wires in total), each pair twisted together.



4. Arrange the Wires:

- Align the wires according to the wiring standard you are using. The twocommon wiring standards are T568A and T568B.

- T568A Wiring Order:

1. White/Green
2. Green
3. White/Orange
4. Blue
5. White/Blue
6. Orange
7. White/Brown
8. Brown

- T568B Wiring Order:

1. White/Orange
2. Orange
3. White/Green
4. Blue
5. White/Blue
6. Green
7. White/Brown
8. Brown

- Ensure all wires are straightened and aligned before proceeding.

5. Trim the Wires:

- Trim the wires evenly so that they are about 1.5 cm long from the cablejacket.

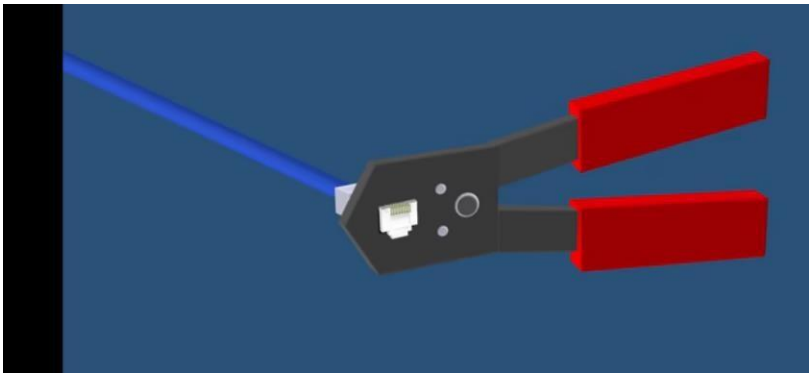
6. Insert the Wires into the RJ-45 Connector:

- Carefully insert the wires into the RJ-45 connector, making sure each wireis fully seated in the connector and in the correct order. The flat side of the RJ-45 connector should be facing you.

7. Crimp the Connector:

- Place the RJ-45 connector with the inserted wires into the crimping tool.

Squeeze the crimping tool firmly to secure the connector to the cable.



8. Repeat on the Other End:

- Repeat steps 2-7 for the other end of the cable, ensuring that both endsfollow the same wiring standard (either T568A or T568B).

9. Test the Cable:

- Use a cable tester to check for proper continuity and correct wiring. The tester will indicate if all the connections are correct and if there are any faults.

2. Study of various internetworking devices

-Hub
-Switches
-Routers

1. Hub

- A hub is a basic networking device that connects multiple devices in anetwork.

- It operates at the Physical Layer (Layer 1) of the OSI model.

Function

- Broadcasting Data: When a hub receives a data packet from one of its ports,it broadcasts the data to all other ports, regardless of the intended recipient.
This can lead to data collisions and inefficiencies.

- Half-Duplex Communication: Hubs support half-duplex communication,meaning data can be transmitted or received, but not simultaneously.

Advantages

- Simple and Cheap: Hubs are inexpensive and easy to install.

- Basic Connectivity: Suitable for small, simple networks where traffic isminimal.

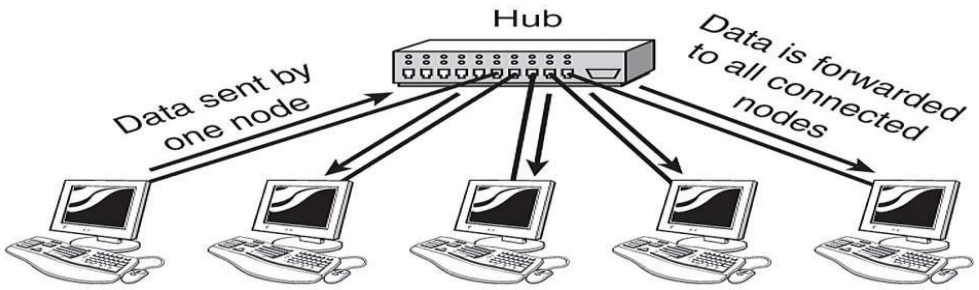
Disadvantages

- Inefficient: Broadcasting data to all devices leads to unnecessary networktraffic and potential collisions.

- No Filtering: Hubs cannot filter or manage traffic, leading to securityvulnerabilities.

Use Case

- Hubs are largely obsolete and have been replaced by more advanced deviceslike switches. They were once used in small, low-traffic networks.



2. Switch

- A switch is a more advanced networking device that connects multipledevices and manages data flow between them.

- It operates at the Data Link Layer (Layer 2), and some switches can operateat the Network Layer (Layer 3).

Function

- Data Filtering and Forwarding: Switches use MAC addresses to intelligentlyforward data to the correct device, rather than broadcasting to all devices like a hub.

- Full-Duplex Communication: Switches support full-duplex communication,allowing simultaneous transmission and reception of data.

- VLAN Support: Some switches support Virtual LANs (VLANs), allowing the segmentation of networks into different logical groups.

Advantages

- Efficient Data Handling: Reduces unnecessary traffic by only sending datato the intended recipient.

- Improved Network Performance: Minimizes data collisions and supportshigher bandwidth.

- Scalability: Suitable for larger networks with many devices.

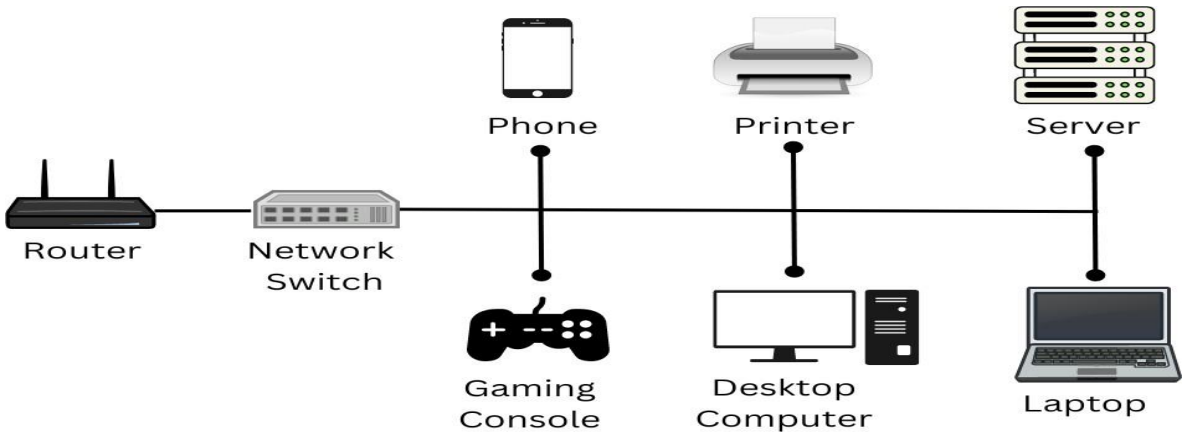
Disadvantages

- Cost: More expensive than hubs.

- Complexity: Requires more configuration and understanding of networkdesign.

Use Case

- Switches are commonly used in small to large networks, including home, office, and enterprise environments, to connect computers, printers, and otherdevices.



3. Router

- A router is a networking device that connects multiple networks together,typically connecting a local network to the internet.

- It operates at the Network Layer (Layer 3) of the OSI model.

Function

- Routing Data Packets: Routers use IP addresses to determine the best pathfor data to travel from one network to another.

- Network Address Translation (NAT): Routers can translate private IPaddresses to a public IP address for internet access.

- Firewall and Security: Many routers have built-in firewalls and securityfeatures to protect networks from unauthorized access.

- Dynamic Routing Protocols: Routers can use protocols like OSPF, BGP, orRIP to dynamically adjust routes based on current network conditions.

Advantages

- Interconnectivity: Allows different networks to communicate with eachother.

- Traffic Management: Routers can prioritize and manage traffic, improvingnetwork performance.

- Security: Provides a layer of security between networks, especially betweena local network and the internet.

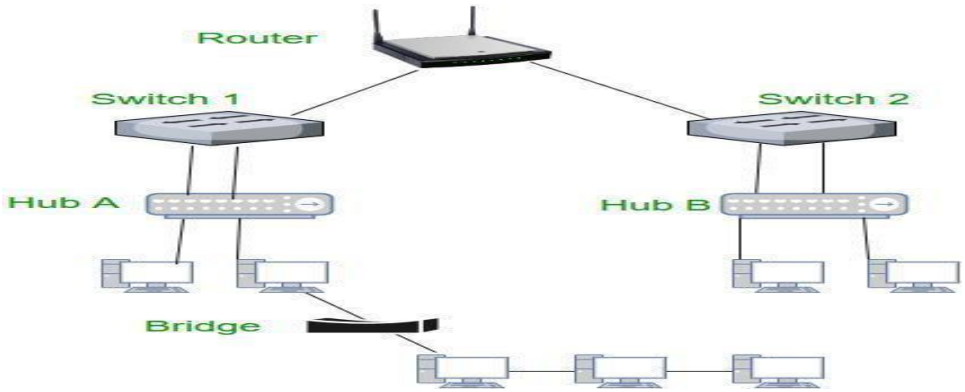
Disadvantages

- Complex Configuration: Routers can be complex to configure, especially inlarger networks.

- Cost: More expensive than hubs and switches.

Use Case

- Routers are essential in any network that connects to other networks, such ashome networks connecting to the internet, or in enterprise networks connecting multiple branches.



Comparison

- Hubs are simple and cheap but inefficient, largely replaced by switches.

- Switches offer intelligent data handling, improving network efficiency andperformance, making them suitable for most network environments.

- Routers connect different networks, providing interconnectivity, traffic management, and security, crucial for any network requiring internet accessor communication between multiple networks.

3. Demonstration of IP change and scanner.

1. IP Change Demonstration

- VPN (Virtual Private Network): The easiest way to change your IP address is by using a VPN service. A VPN masks your real IP address and assigns youa new one from the server you're connected to.

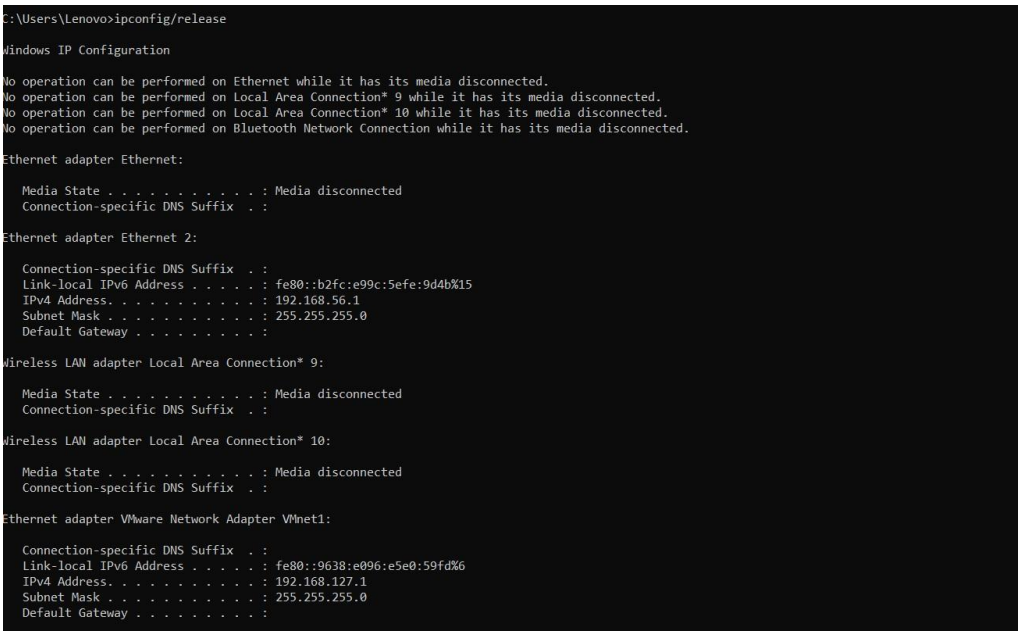
- Proxy Server: A proxy server also allows you to change your IP address. When you connect to a proxy, your internet traffic is routed through the proxyserver, making it appear as though the traffic is originating from the proxy's IP address.

- Manually Change IP (Windows):

  - Open Command Prompt.

  - Type `ipconfig /release` and hit Enter.

  - Then type `ipconfig /renew` to request a new IP address from the DHCPserver.



2. Network Scanning Demonstration

- Using Nmap:

- Nmap (Network Mapper) is a free and open-source tool used for networkdiscovery and security auditing.

- To scan a network, open a terminal and type `nmap -sn 192.168.1.0/24` to perform a ping scan on the network range.

- To scan for open ports on a specific IP, use `nmap -p 1-65535 <target_ip>`.

Network Scanning using Nmap:

- Install Nmap on your system (`sudo apt-get install nmap` for Linux).

- Run a scan on your local network: `nmap -sn 192.168.1.0/24`.

- Review the results to see the active devices on the network.

- Run a port scan: `nmap -p 22 192.168.1.1` to check if SSH port 22 is openon a specific device.