ST. ANDREWS INSTITUTE

OF TECHNOLOGY & MANAGEMENT

Gurgaon Delhi (NCR)
Approved by AICTE, Govt. of India, New Delhi
Affiliated to Maharshi Dayanand University
‘A’ Grade State University, accredited by NAAC

Bachelor of Technology

Practical File

Computer Networks Lab

Subject Code: LC-CSE-323G

Submitted To:

Mr Puneet Garg

(Assistant Professor)

Submitted by:

Name: Gautam Tiwari

Sem: V

Roll no: 213028

Index

1. Network cable types and specifications.

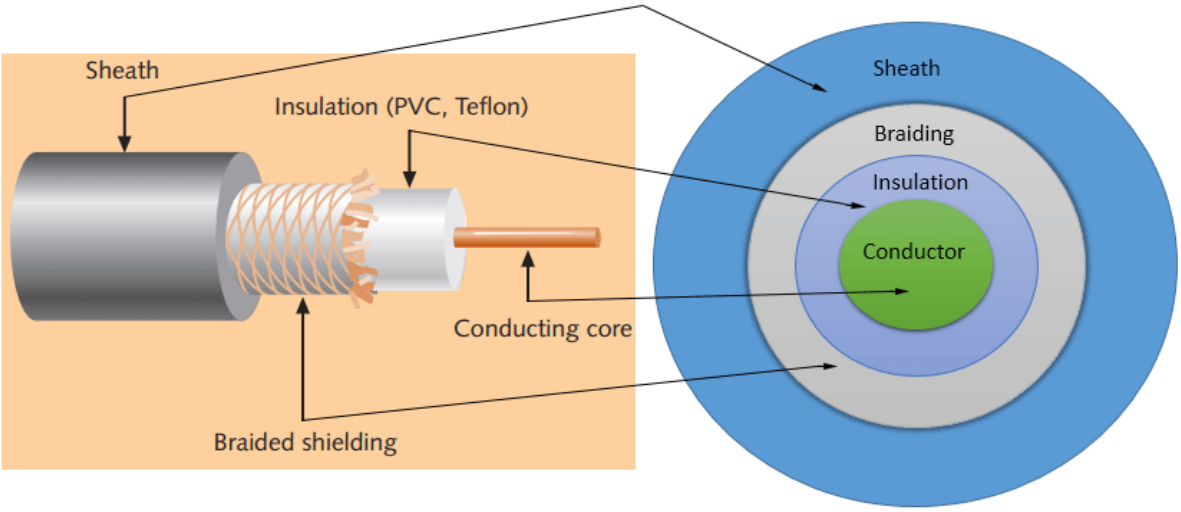
Network cables are used to connect two or more computers or networking devices in a network. There are three types of network cables:

- ❖ Coaxial
- ❖ Twisted-pair
- ❖ Fiber-optic

Coaxial cable

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, the braiding covers the insulation, and the insulation covers the conductor.

The following image shows these components.



Sheath

This is the outer layer of the coaxial cable. It protects the cable from physical damage.

Braided shield

This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.

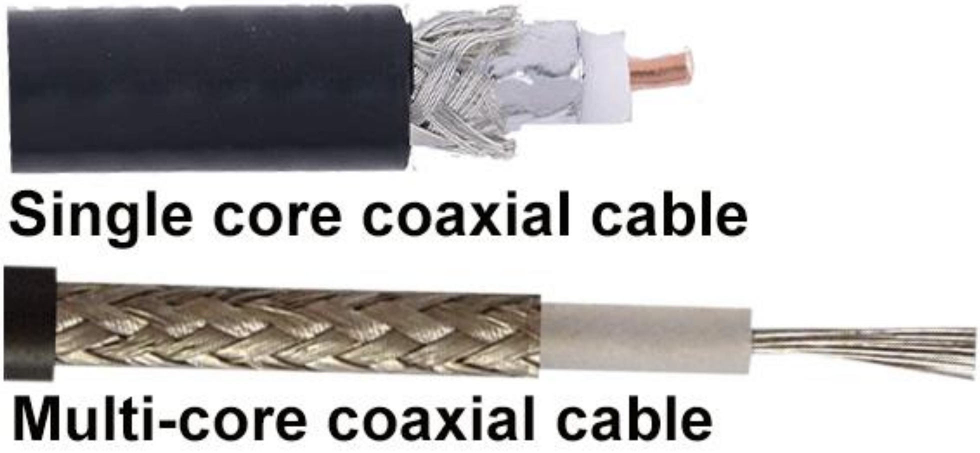
Insulation

Insulation protects the core. It also keeps the core separate from the braided shield. Since both the core and the braided shield use the same metal, without this layer, they will touch each other and create a short circuit in the wire.

Conductor

The conductor carries electromagnetic signals. Based on conductor a coaxial cable can be categorized into two types; single-core coaxial cable and multi-core coaxial cable.

A single-core coaxial cable uses a single central metal (usually copper) conductor, while a multi-core coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.



Coaxial cables in computer networks

The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even though their use in computer networks has been completely discontinued.

At the beginning of computer networking, when there were no dedicated media cables available for computer networks, network administrators began using coaxial cables to build computer networks.

Because of its low cost and long durability, coaxial cables were used in computer networking for nearly two decades (the 80s and 90s). Coaxial cables are no longer used to build any type of computer network.

Twisted-pair cables

The twisted-pair cable was primarily developed for computer networks. This cable is also known as Ethernet cable. Almost all modern LAN computer networks use this cable.

This cable consists of colour-coded pairs of insulated copper wires. Every two wires are twisted around each other to form a pair. Usually, there are four pairs. Each pair has one solid colour and one striped colour wire. Solid colours are blue, brown, green, and orange. In stripped colour, the solid colour is mixed with the white colour.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

In the *UTP (Unshielded twisted-pair) cable*, all pairs are wrapped in a single plastic sheath.

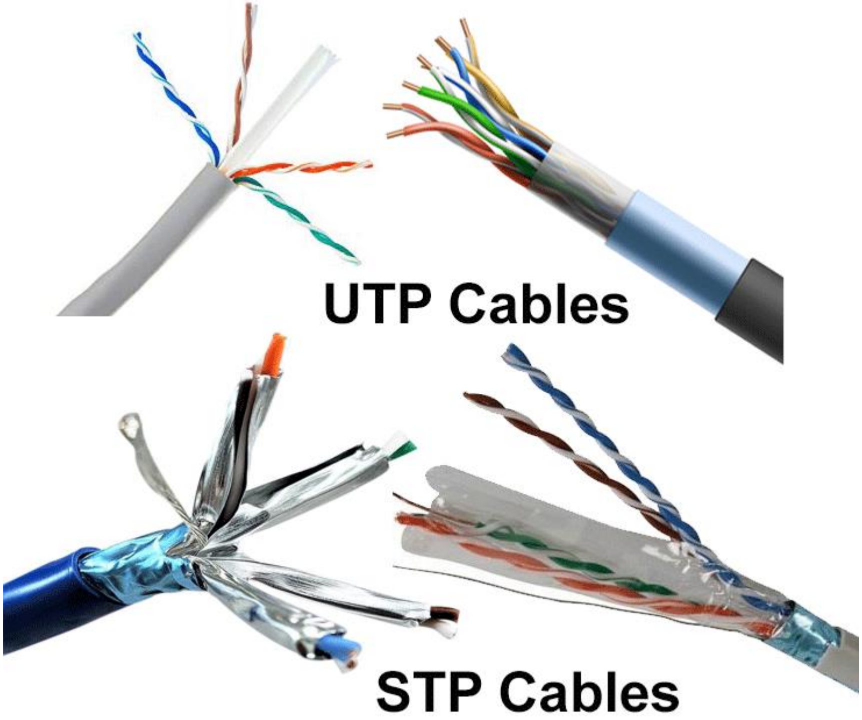
In the *STP (Shielded twisted-pair) cable*, each pair is wrapped with an additional metal shield, and then all pairs are wrapped in a single outer plastic sheath.

Similarities and differences between STP and UTP cables:

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Since the STP cable contains more materials, it is more expensive than the UTP cable.
- Both cables use the same RJ-45 (registered jack) modular connectors.

- Both cables can accommodate a maximum of 1024 nodes in each segment.
- The STP provides more noise and EMI resistance than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.

The following image shows both types of twisted-pair cables.



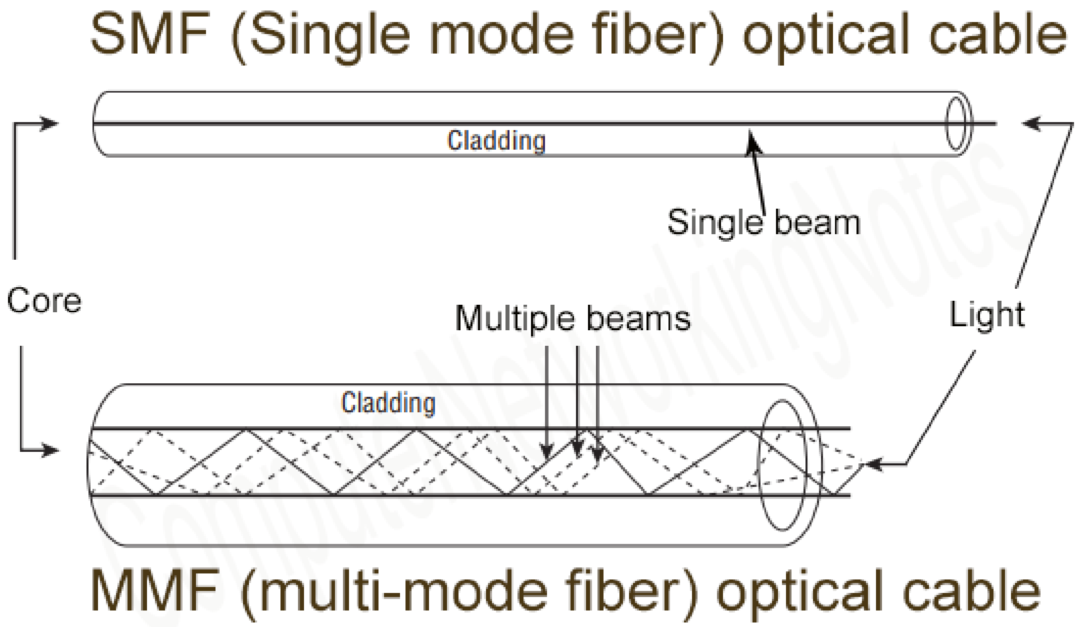
Fiber optic cable

This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

- Core carries the data signals in the form of light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

Fibre optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometres at the speed of 100Gbps.

Fibre optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.


SMF (Single mode fiber) optical cable
Cladding
Single beam
Core
Multiple beams
Light
Cladding
MMF (multi-mode fiber) optical cable

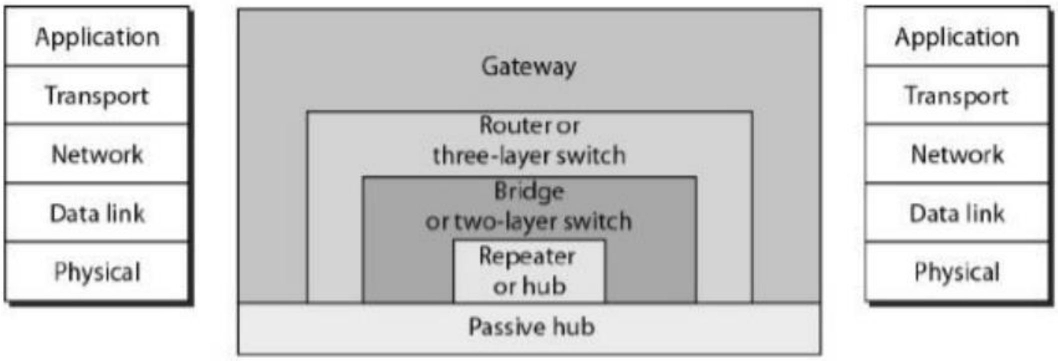
SMF (Single-mode fiber) optical cable:

This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable:

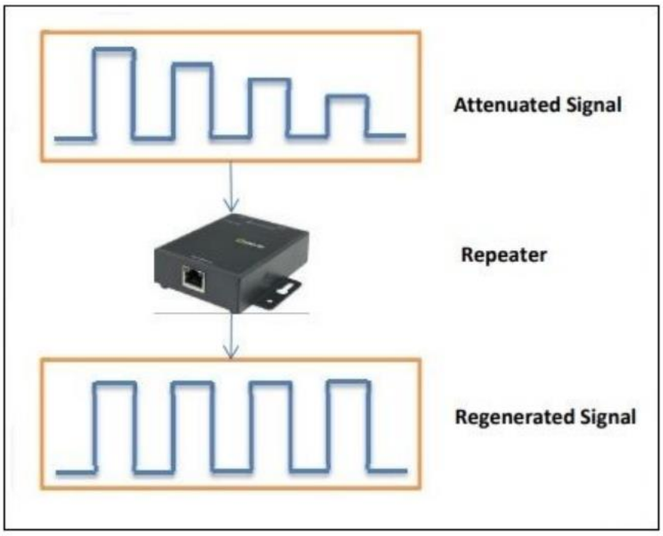
This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used for shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.

2. Study of network devices in detail.



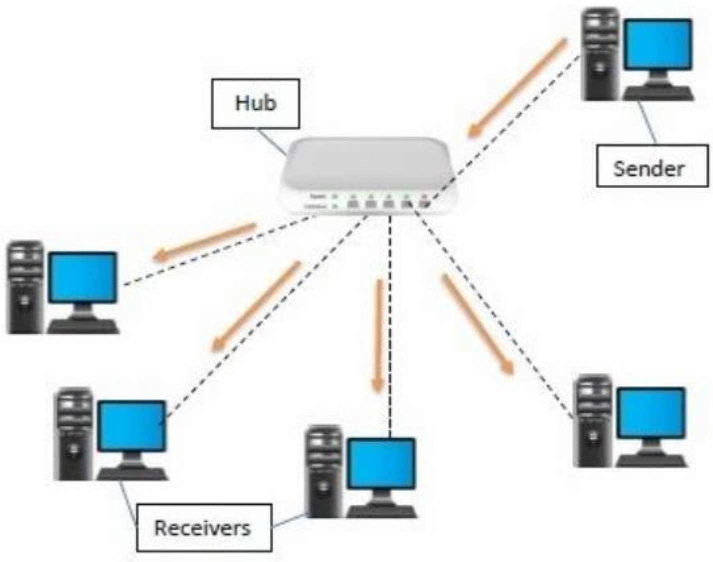
Repeaters:

- ❖ Repeaters are network devices operating at the physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.
- ❖ They are incorporated in networks to expand its coverage area. They are also known as signal boosters.
- ❖ Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
- ❖ A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern.
- ❖ The repeater then sends the refreshed signal.
- ❖ A repeater can extend the physical length of a LAN.
- ❖ The location of a repeater on a link is vital. A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits.
- ❖ If the corrupted bit travels much farther, however, accumulated noise can change its meaning completely.
- ❖ At that point, the original voltage is not recoverable, and the error needs to be corrected.
- ❖ A repeater placed on the line before the legibility of the signal becomes lost can still read the signal well enough to determine the intended voltages and replicate them in their original form.



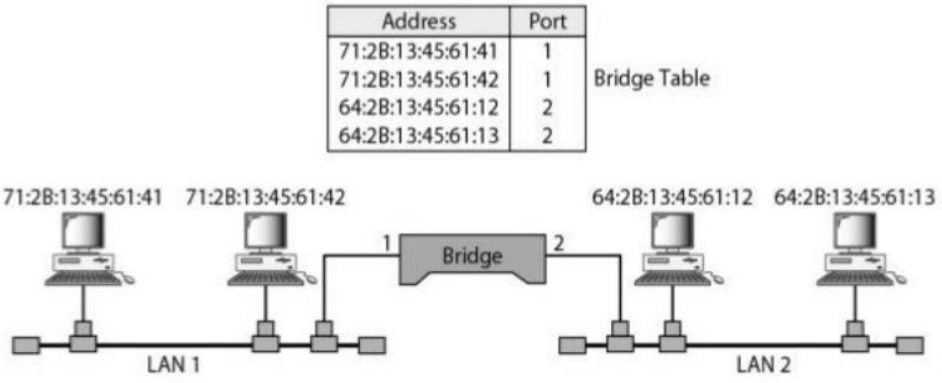
Hub:

- A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.
- A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.
- When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.



Bridges:

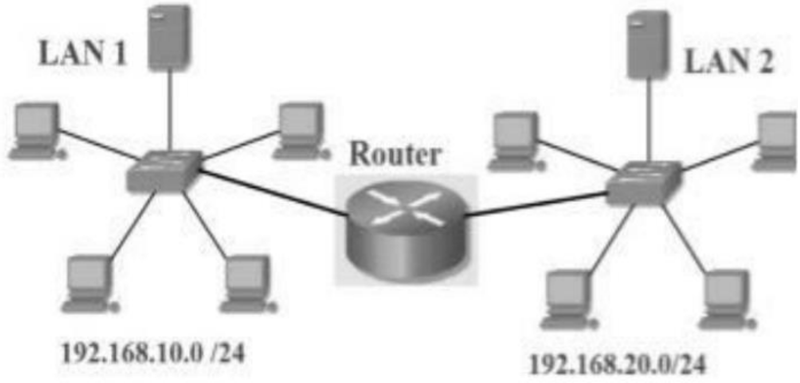
- A bridge operates in the physical layer as well as in the data link layer. It can regenerate the signal that it receives and as a data link layer device, it can check the physical addresses of source and destination contained in the frame.
- The major difference between the bridge and the repeater is that the bridge and the repeater is that the bridge has a filtering capability.
- That means it can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is forwarded, then the bridge should specify the port over which it should be forwarded.



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Router:

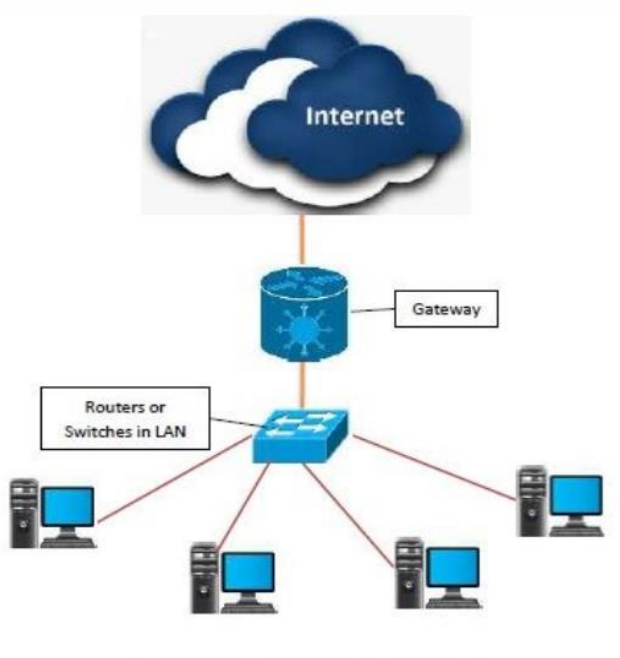
- Routers are networking devices operating at layer 3 or a network layer of the OSI model.
- They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.
- A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing).
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols. Data is grouped into packets, or blocks of data.
- Each packet has a physical device address as well as logical network address. The network address allows routers to calculate the optimal path to a workstation or computer.
- The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations.
- The router consults the routing table to determine the optimal route through which the data packets can be sent
- A routing table typically contains the following entities –
    - IP addresses and subnet mask of the nodes in the network
    - IP addresses of the routers in the network
    - Interface information among the network devices and channels



Gateway:

- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model.
- However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model.
- It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway.
- Only the internal traffic between the nodes of a LAN does not pass through the gateway.

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenarios, a gateway node may be supplemented as a proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses a packet switching technique to transmit data across the networks.

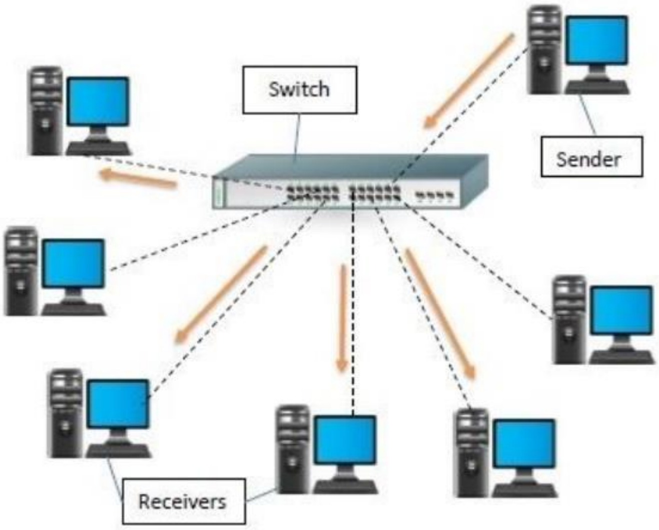


Gateway between a LAN and Internet

Switch:

- A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.
- Like a hub, a switch also has many ports, to which computers are plugged in.
- However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s).
- Thus, it supports both unicast and multicast communications.
- We can have a two-layer switch or a three-layer switch.
- A three-layer switch is used at the network layer; it is a kind of router.
- The two-layer switch performs at the physical and data link layers.
- A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance.

- A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.
- This means no competing traffic (no collision, as we saw in Ethernet).
- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC Address of the frame it received.
- However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing.
- It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.



3. Study different types of network cables and practically implement the cross-wired and straight-through cables using clamping tools.

To do these practical following steps should be done:

1) Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.
2) Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have ½ of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than ½ of an inch of un-twisted wire.
3) You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end.

Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Diagram shows you how to prepare straight through wired connection

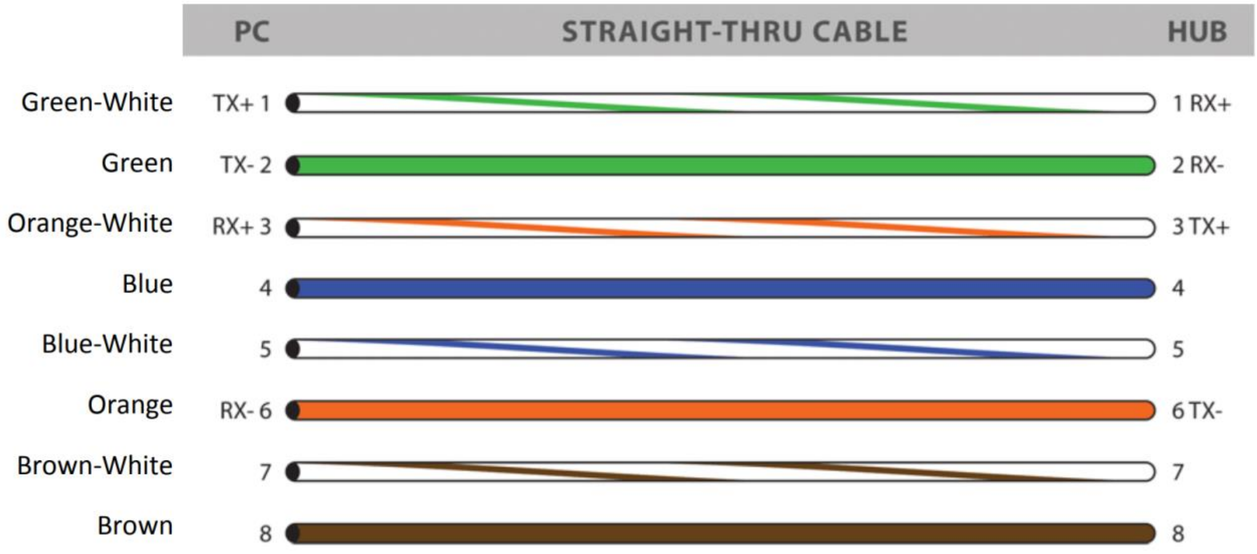
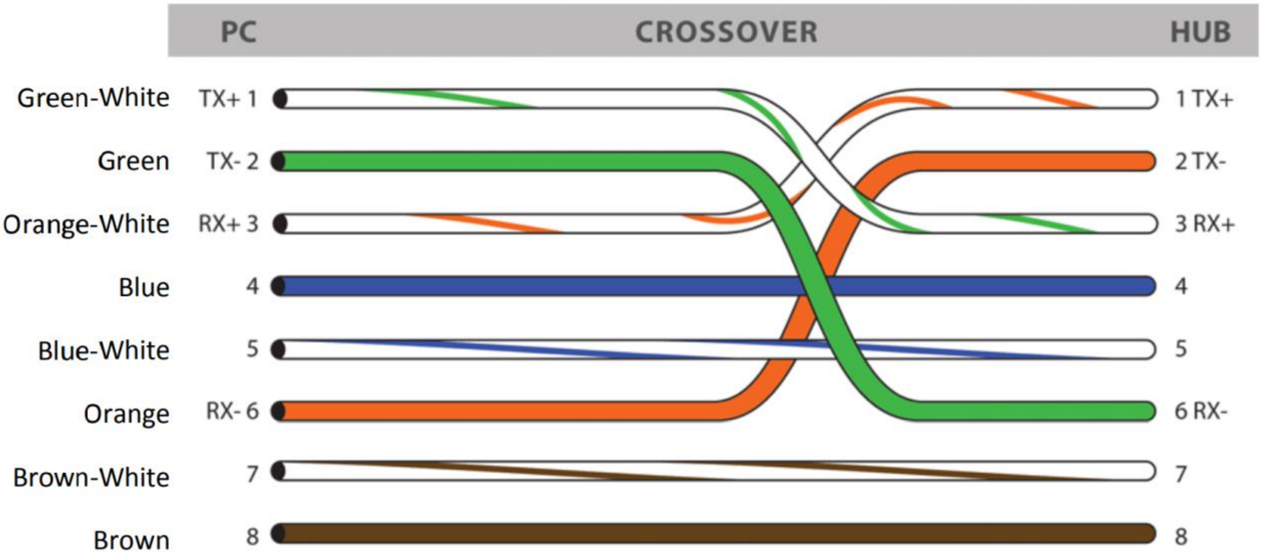


Diagram shows you how to prepare Cross wired connection



Ethernet Cable Tips:

- A straight-thru cable has identical ends.
- A crossover cable has different ends.
- A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- A crossover has one end with the Orange set of wires switched with the Green set.
- Odd numbered pins are always striped; even numbered pins are always solid coloured.
- Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left.
- No more than 1/2" of the Ethernet cable should be untwisted otherwise it will be susceptible to crosstalk.
- Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near noise inducing components.

4. Network cable crimping and testing tools.

Cables are the backbone of a wired network. The stability, reliability, and performance of a wired network depend on cables. Installing and maintaining cables in a wired network is a difficult task. To make this task easier, a variety of network cable crimping and testing tools are available.

Twisted-pair (STP and UTP) network cable crimping tools

Crimping tools are used for the following purposes:

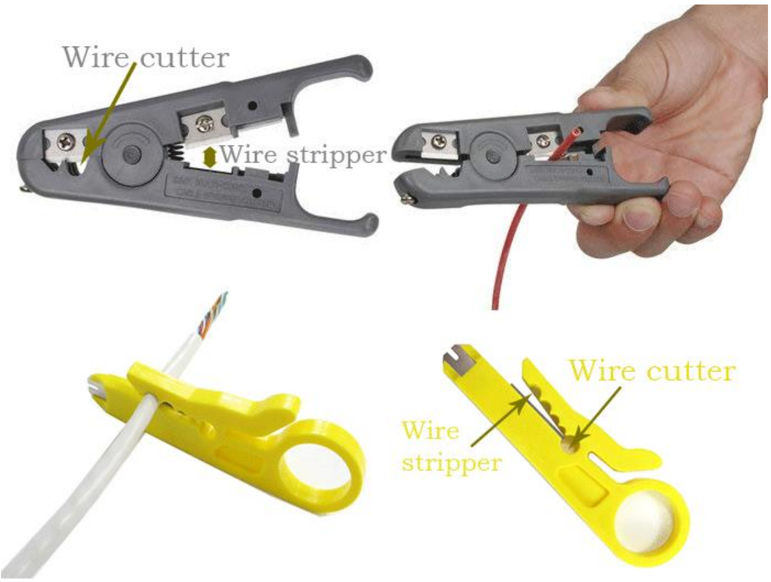
- To cut the network cable of the required length from the bundle.
- To remove the outer and inner jackets of the network cable.
- To attach the connectors on both ends of the cable.

Some crimping tools provide all the functionality while others provide one or two functionalities. The most common twisted-pair network cable crimping tools are described below.

Wire Cutter: - To cut the network cable of the required length from the bundle, you can use any standard wire cutter tool or can use a wire cutter tool that is specially designed for the twisted-pair cable. A twisted-pair wire cutter usually includes additional blades for stripping the wire.

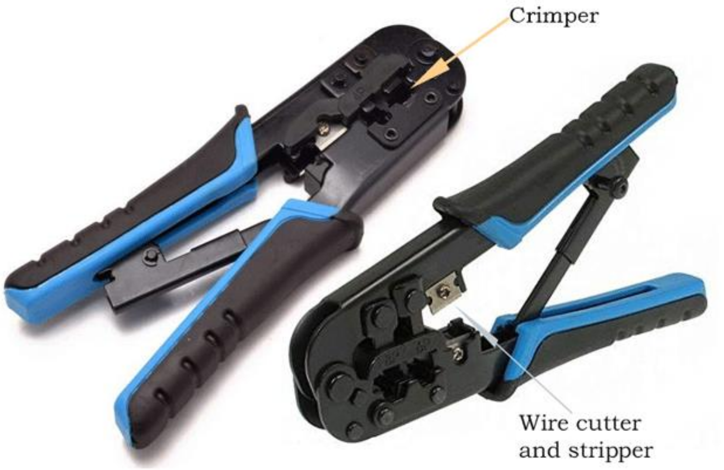
Wire Stripper: - This tool is used to remove the outer and inner jackets of the network cable. Typically, you do not need to purchase this tool separately as all standard twisted-pair wire cutters are equipped with wire-strippers.

The following image shows two twisted-pair wire cutter tools equipped with wire-strippers.



Crimp tool: - This tool is used to attach the connectors to the cable. Typically, this tool also includes a wire-cutter and wire-stripper. So if you buy a crimp tool, you don't have to buy a wire-cutter and wire-stripper separately.

The following image shows a crimping device equipped with a wire-stripper and wire-cutter.



Which tool you should buy depends on your requirements and budget. For example, if you want to install a dozen network cables, you can buy less expensive tools such as a low-cost wire stripper and a cheap crimp device. But if you are in a network cable setting-up business or have a medium or large-sized network, you should buy a crimping tool that has a built-in wire stripper and wire cutter. A high-quality twisted-pair cable crimping tool will cost you around $100 but will save you many headaches in the long run.

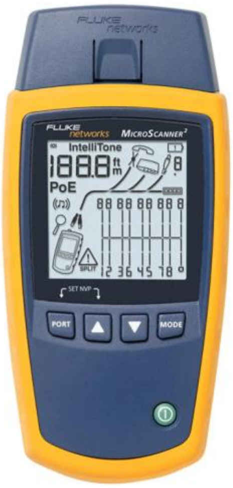
Network cable testing and troubleshooting tools

A network cable testing and troubleshooting tool is used for the following purposes.

- To measure the length of a segment or network cable.
- To detect loose connectors.
- To identify an un-labeled network cable from all network cables.
- To find a break in the network cable.
- To certify the cable installation.

Cable certifier

This device thoroughly tests a network cable and certifies that the cable installation meets a special wiring standard such as Cat 5e, Cat 6, Cat 6a, and so on. This device can check and test total segment length, crosstalk, noise, wiremap, resistance, impedance, and the capability to transfer data at the maximum frequency rated for the cable.



The image on the side shows a network cable certifier.

Since this device performs a complete test and certifies the cable installation, it will cost you more than all the other test devices listed in this section. If you have a mid-size network or if you can buy this device, then you should always buy and use this device to manage network cables.

Basic cable tester

If you can't afford a network cable certifier, you can buy and use this device to manage your network cables. Besides certifying the cable installation, this device provides all remaining functionalities of a network cable certifier. It can test cable length, cross talk, and breaks in the cable. It can also check whether the connectors on both ends of a network cable are properly attached or not.

The following image shows a basic network cable tester tool.

Tone generator and the probe

This device is used to trace the unlabeled network cables. This device comes in two pieces: the tone generator and the probe. The tone generator generates tones or signals and places them on the network cable. The probe detects these signals on the other end of the cable.

You can use this tool to identify network cables that run from a central location to remote locations. For example, if you are working on a patch-panel or a switch and trying to figure out which network cable connects back to an end-device (such as a PC), then you can use this device.

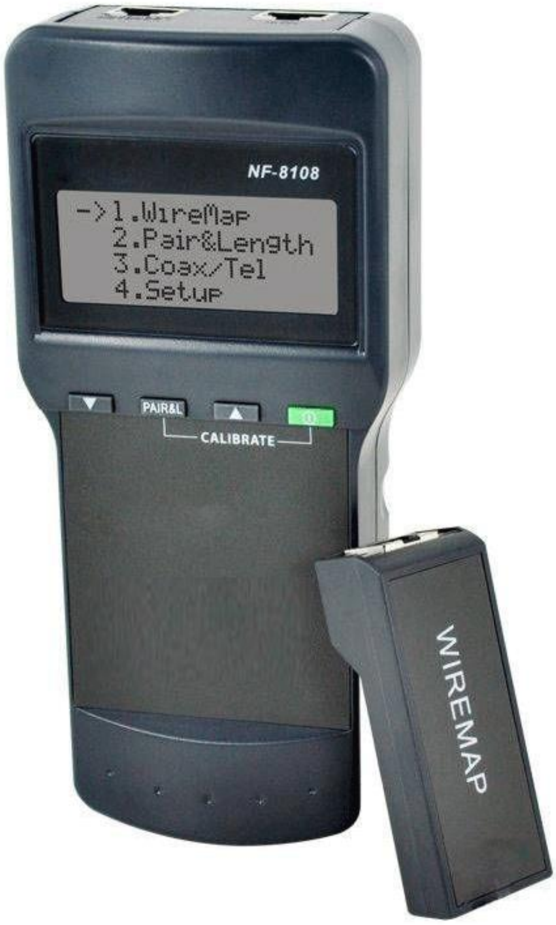
Place a tone generator at one end of the connection (end-device), and use the probe on another side (switch or patch-panel) to determine which network cable the tone generator is connected to.

The following image shows an example of a tone generator and probe.

Time domain reflectometer

This device is used to measure the length of a network cable as well as the breaks in the cable. This device transmits a signal on one end and measures the time that the signal takes to reach the end of the cable. You can also use this device to find breaks in the cable. For example, this device can tell you approximately how far the break is located in the cable.

The following image shows a time domain reflectometer.



5. Set up local area network using Packet Tracer.

On the host computer

On the host computer, follow these steps to share the Internet connection:

1) Log on to the host computer as Administrator or as Owner.
2) Click Start, and then click the Control Panel.
3) Click Network and Internet Connections.
4) Click Network Connections.
5) Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.
6) Click Properties.
7) Click the Advanced tab.
8) Under Internet Connection Sharing, select the Allow other network users to connect through this computer's Internet connection check box.
9) If you are sharing a dial-up Internet connection, select establish a dial-up connection whenever a computer on my network attempts to access the Internet check box if you want to permit your computer to automatically connect to the Internet.
10) Click OK. You receive the following message:
    When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet. Connection Sharing?
11) Click Yes.

The connection to the Internet is shared to other computers on the local area network (LAN).
The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

On the client computer

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer. To confirm the LAN adapter IP configuration, follow these steps:

1) Log on to the client computer as Administrator or as Owner.
2) Click Start, and then click Control Panel.
3) Click Network and Internet Connections.
4) Click Network Connections.
5) Right-click Local Area Connection and then click Properties.
6) Click the General tab, click Internet Protocol (TCP/IP) in the connection uses the following items list, and then click Properties.
7) In the Internet Protocol (TCP/IP) Properties dialog box, click Obtain an IP address automatically (if it is not already selected), and then click OK.
   Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254. For example, you can assign the following static IP address, subnet mask, and default gateway: IP Address 192.168.31.202, Subnet mask 255.255.255.0, Default gateway 192.168.31.111.
8) In the Local Area Connection Properties dialog box, click OK.
9) Quit Control Panel.

6. Network configuration commands.

1) Ping:

- ❖ Ping is a crucial network diagnostic tool used to determine the accessibility and round-trip time of a host on an IP network. It works by sending ICMP echo request packets to the target and measuring the time it takes for the corresponding echo replies to return. Ping is instrumental in troubleshooting connectivity issues and assessing network performance.
  - ➢ *-c:* Specifies the count of echo requests to send, allowing users to customize the number of test packets.
  - ➢ *-t:* Enables continuous ping requests until manually stopped, aiding in prolonged network monitoring.
  - ➢ *-s:* Adjusts the size of the ICMP packets, useful for simulating various network conditions.

2) Netstat:

- ❖ Netstat, short for network statistics, is a command-line utility providing a comprehensive view of network connections, routing tables, interface statistics, and more. It is invaluable for monitoring network activities and identifying potential issues.
  - ➢ *-a:* Displays all connections and listening ports, offering a complete overview of network-related activities.
  - ➢ *-n:* Shows numerical addresses instead of attempting to resolve hostnames, facilitating quicker analysis.
  - ➢ *-r:* Reveals the routing table, aiding in understanding the paths that network traffic takes.

3) Ipconfig:

- ❖ Ipconfig is a Windows command-line tool that provides detailed information about the IP configuration of a computer. It includes details such as IP address, subnet mask, and default gateway, making it indispensable for network configuration and troubleshooting.
  - ➢ */all:* Displays comprehensive information about all network interfaces, including physical and virtual ones.
  - ➢ */renew:* Initiates the renewal of IP addresses for all adapters, useful in dynamic IP environments.
  - ➢ */release:* Releases the IP addresses for all adapters, an essential step in certain network troubleshooting scenarios.

4) Tracert:

- ❖ Tracert, or traceroute, is a command-line utility that traces the route taken by packets from the source to the destination. It reveals the IP addresses of routers along the path, aiding in pinpointing network bottlenecks and identifying connectivity issues.
  - ➢ *-d:* Prevents the utility from attempting to resolve IP addresses to hostnames, expediting the tracing process.
  - ➢ *-h:* Specifies the maximum number of hops, allowing users to control the depth of the trace.
  - ➢ *-w:* A timeout value must be specified while executing this ping command. It adjusts the amount of time in milliseconds.

5) Nslookup:

- Nslookup is a versatile command-line tool used for querying DNS servers to obtain information about domain names, IP addresses, and other DNS records. It is a valuable resource for diagnosing DNS-related issues.
    - *-query:* Specifies the type of DNS record to query, enabling users to target specific information.
    - *-server:* Designates the DNS server to query, useful for troubleshooting DNS server-related problems.

6) Route:

- Route is a command-line utility that displays and modifies the IP routing table on Windows systems. It is crucial for managing network routing and ensuring efficient data transfer.
    - *-p:* Adds a persistent route to the routing table, ensuring it persists across system reboots.
    - *-f:* Clears the routing table, helpful in scenarios where a fresh start is required.

7) Pathping:

- Pathping is a hybrid command that combines features of traceroute and ping, providing a detailed analysis of the network path and latency. It is particularly useful for assessing the performance of each hop in the network.
    - *-n:* Prevents the utility from resolving addresses to hostnames, expediting the path analysis.
    - *-h:* Specifies the maximum number of hops, allowing users to control the depth of the pathping analysis.

7. LAN configuration using HUB on packet tracer.

8. LAN configuration using Switch on packet tracer.

9. LAN Configuration using Router on packet tracer.