Unit 2
Networking Components (Hardware)

Meghana Palkar

Unit 2

Networking Components (Hardware)

- Networking Components (Hardware): Cables & Connectors (Coaxial, UTP/STP, Fiber Optics, Cat(x) Cables)
- Switches (Unmanaged, Smart Web Managed, Full Managed), Hardware/Software Firewall
- Study of UTM, Wireless Routers DSL/ADSL – Latest Examples and Usage
- Advances in Network Applications: Mobile as a Network Client, Types & Application of CCTV
- Network, Types and Application of Access Control Devices.

Network Cabling

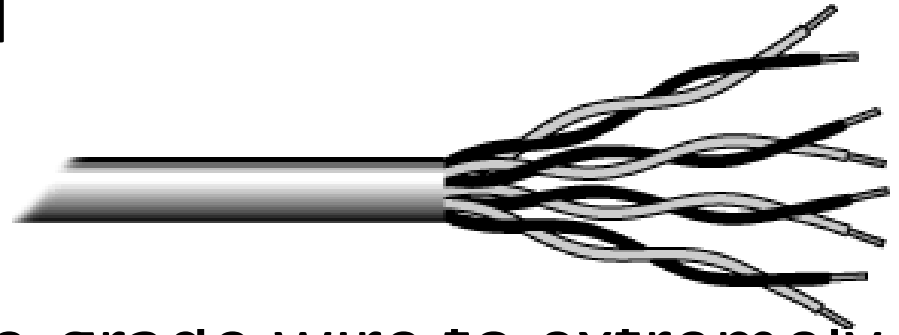
Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

Types of cables used in networks:

1. Unshielded Twisted Pair (UTP) Cable
2. Shielded Twisted Pair (STP) Cable
3. Coaxial Cable
4. Fibre Optic Cable

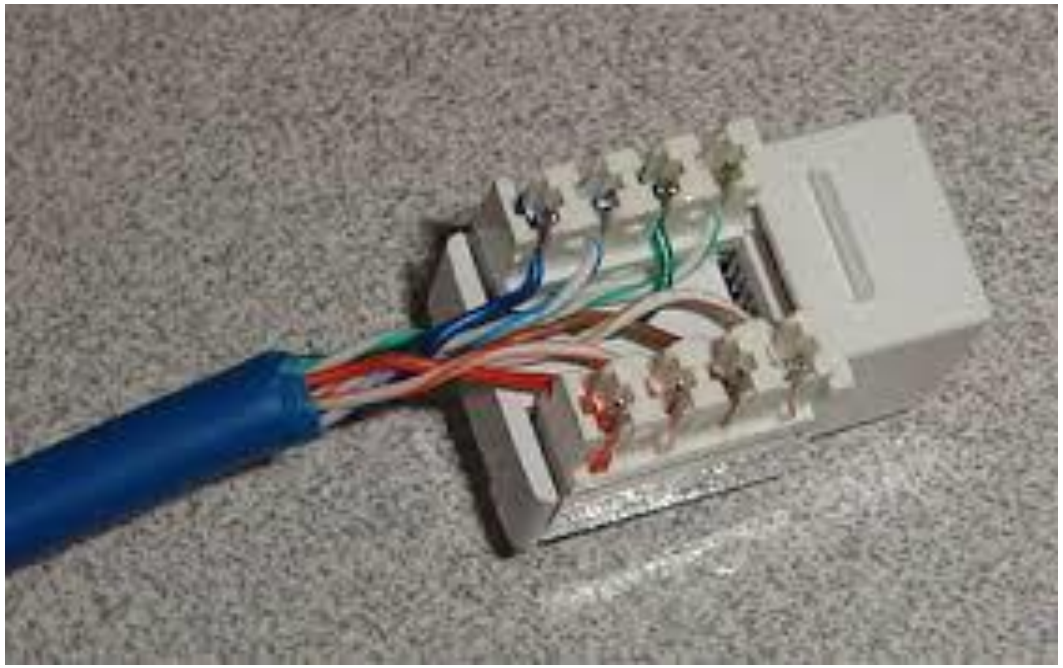
Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks. Also called

As Cat (X) cable.

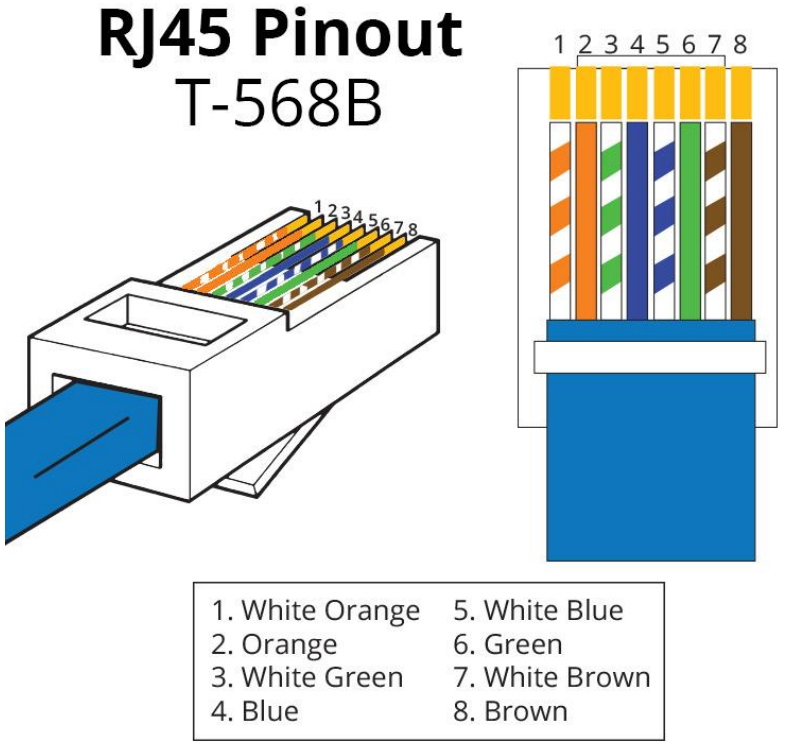


The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association / Telecommunication Industry Association) has established standards of UTP and rated six categories of wire.

Cat (x) cable connector.

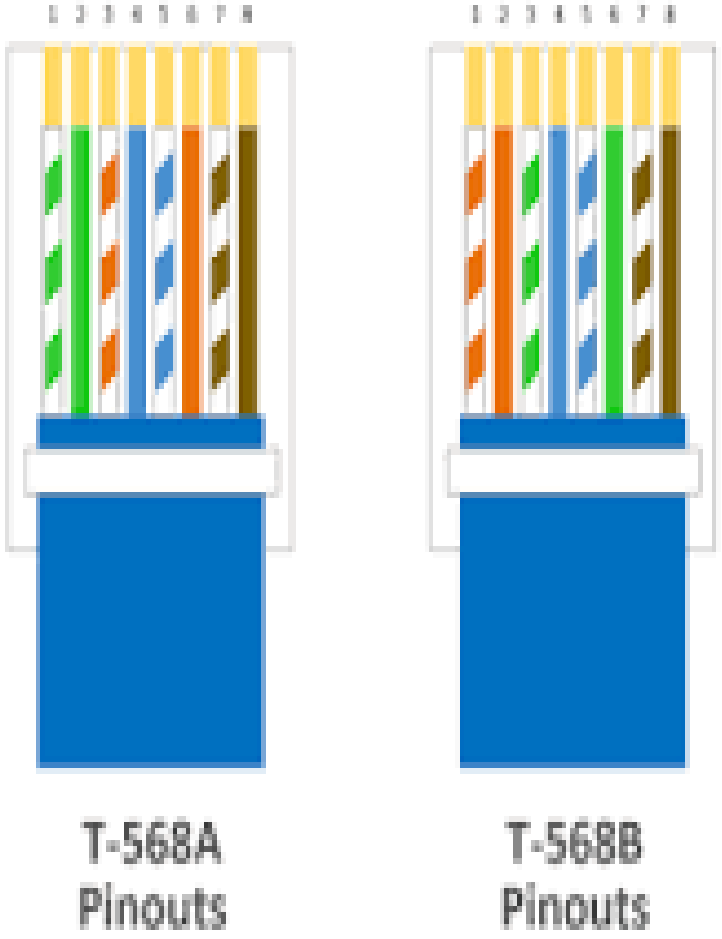


	Pair color	[cm] per turn	Turns per [m]
	Green	1.53	65.2
	Blue	1.54	64.8
	Orange	1.78	56.2
	Brown	1.94	51.7



Maximum length for a Cat X cable: A single run of Ethernet cable is designed to work at a maximum of 328 feet or 100 meters. It's entirely possible to exceed the manufacturer's specification and still maintain network connectivity. However, this greatly increases the chances of connectivity issues, reduced speeds, and lower reliability.

The cable category with the highest bandwidth is currently Cat8 with 2 billion (2 GHz) signals per second, 20 times as many as Cat5. Data Rate and Bandwidth are related terms but they are not the same. Higher frequencies carry more 1s and 0s, allowing more bits of data to be transmitted per second. CAT1 to CAT 9 different types of cables are present. CAT8 is the fastest cable.



Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
6	1000 Mbps (4 pair)	Gigabit Ethernet
7	1,000 Mbps	Gigabit Ethernet
8	10,000 Mbps	Gigabit Ethernet

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 (Registered Jack)connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. This standard designates which wire goes with each pin inside the connector.

Shielded Twisted Pair (STP) Cable

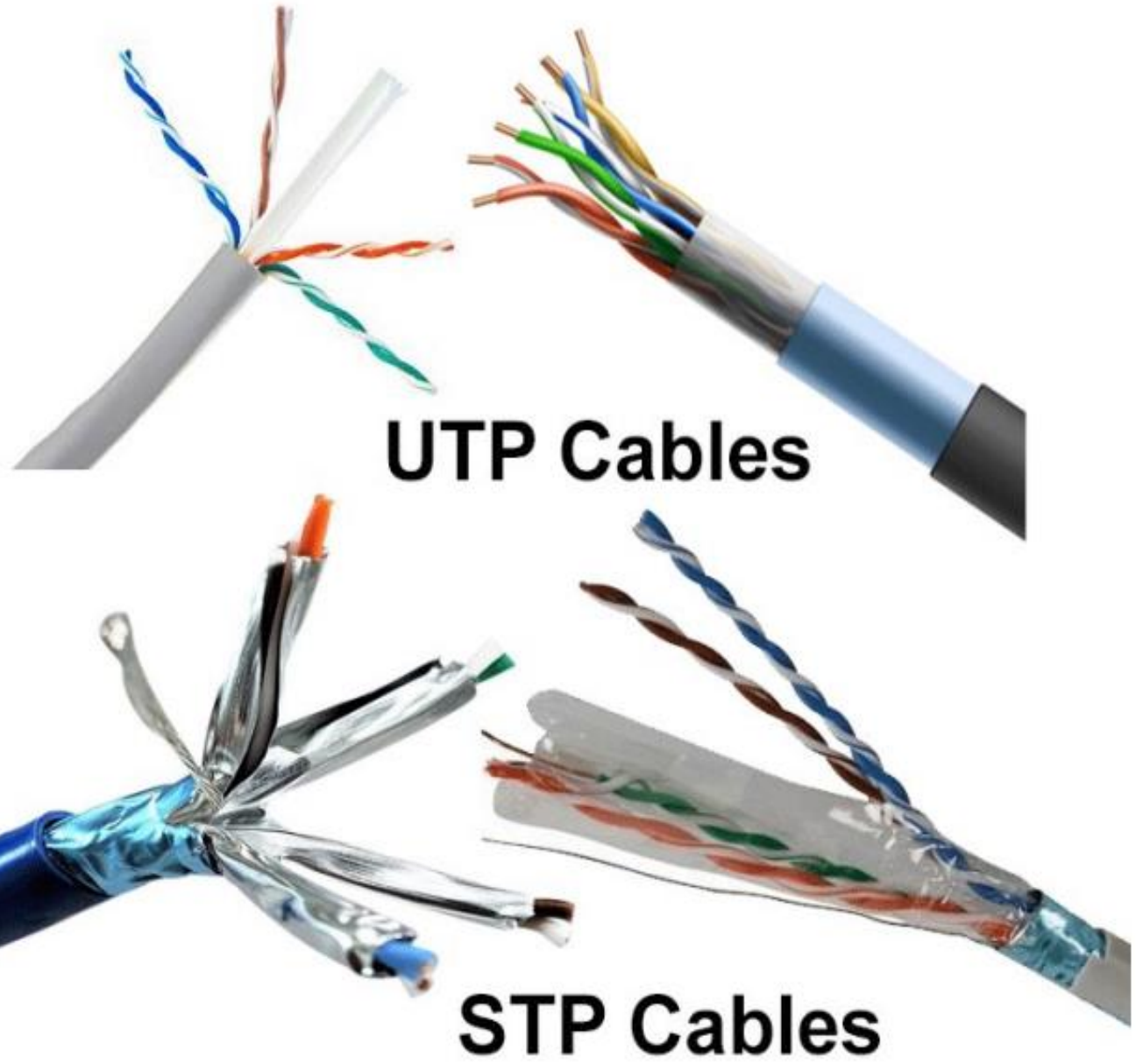
Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

- Each pair of wires is individually shielded with foil.
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

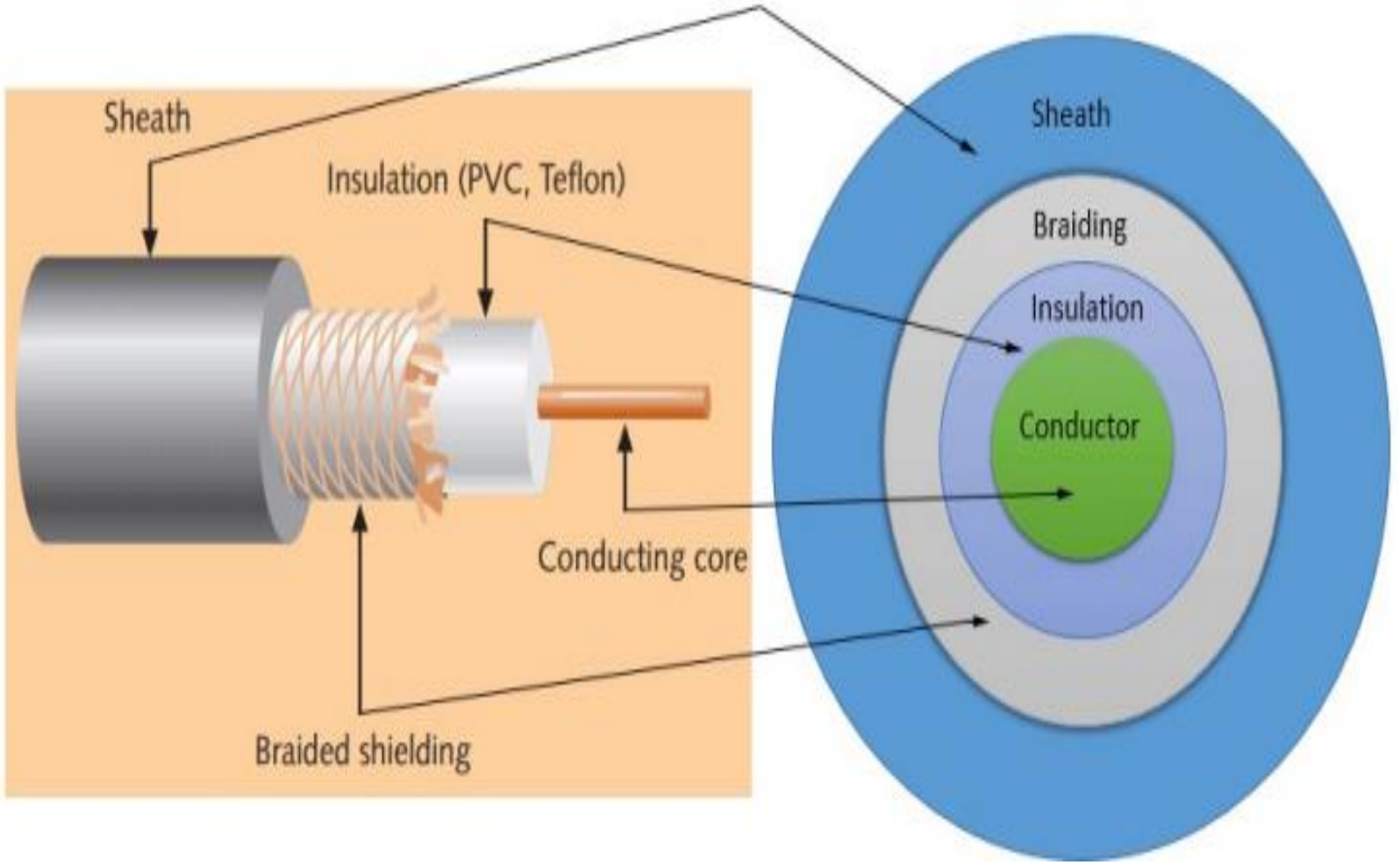
Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green and orange. In stripped color, the solid color is mixed with the white color.

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, then all pairs are wrapped in a single outer plastic sheath.



Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers. This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.



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.

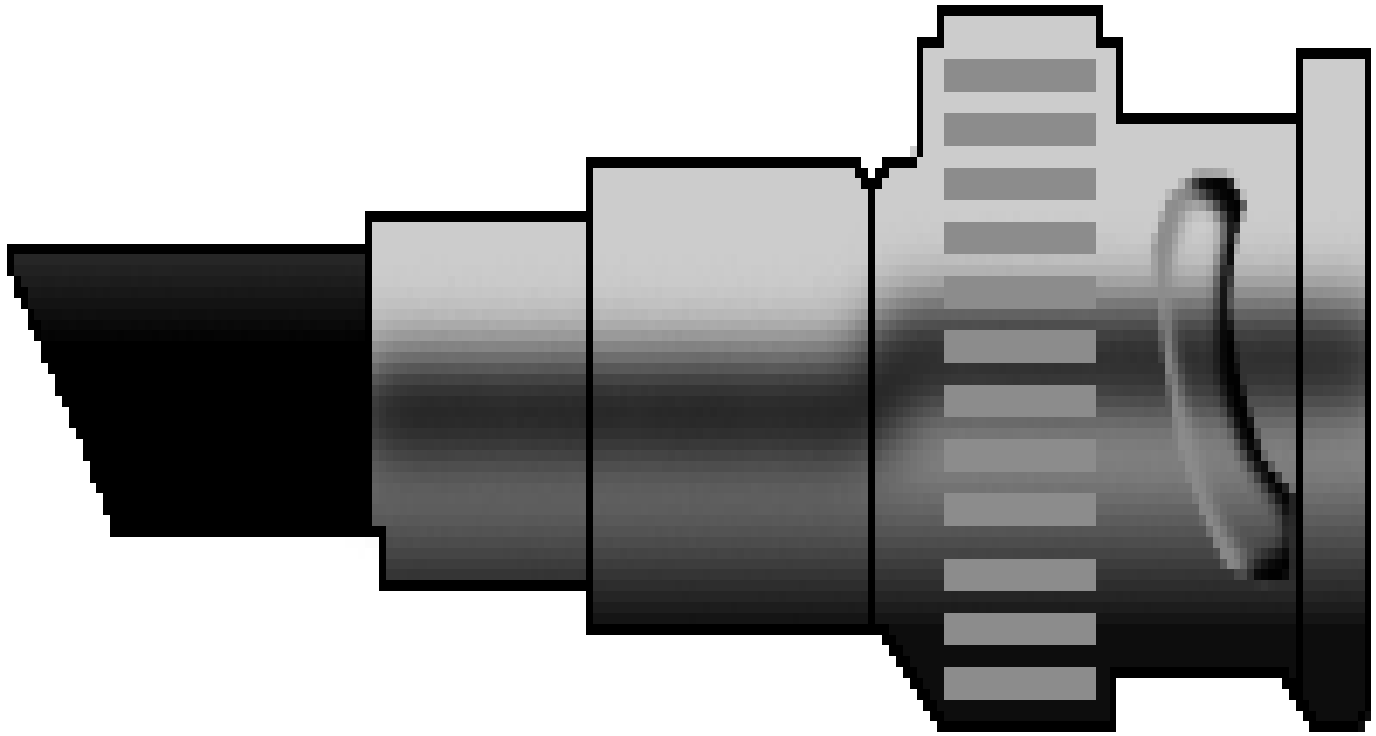
The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even their use in computer networks has been completely discontinued.

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

Coaxial cables have been in use for the last four decades. During these years, based on several factors such as the thickness of the sheath, the metal of the conductor, and the material used in insulation, hundreds of specifications have been created to specify the characteristics of coaxial cables.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.



Fiber Optic Cable

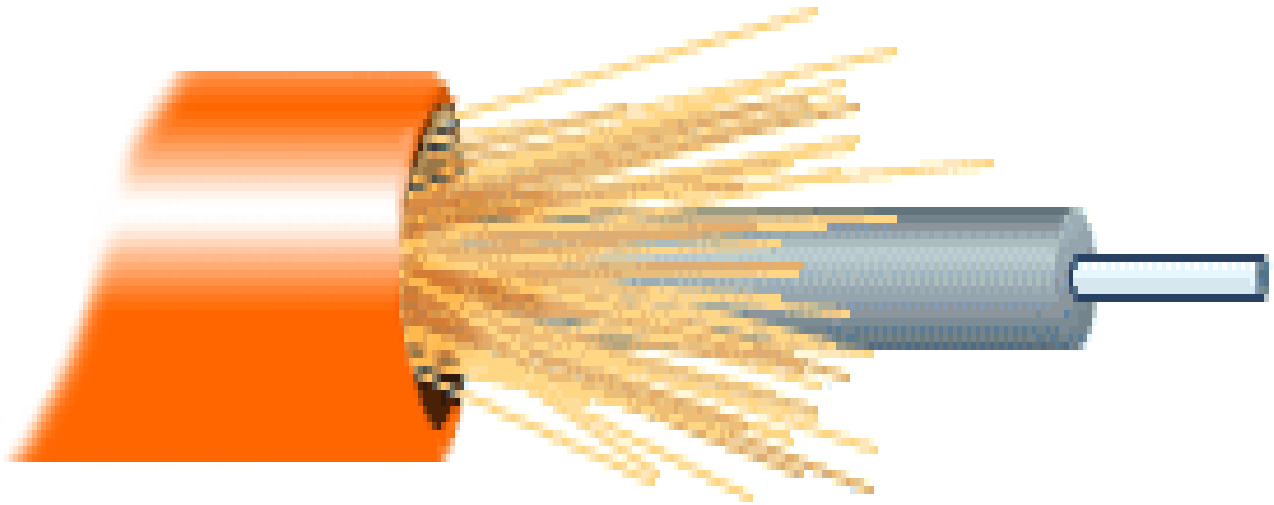
Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify.

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

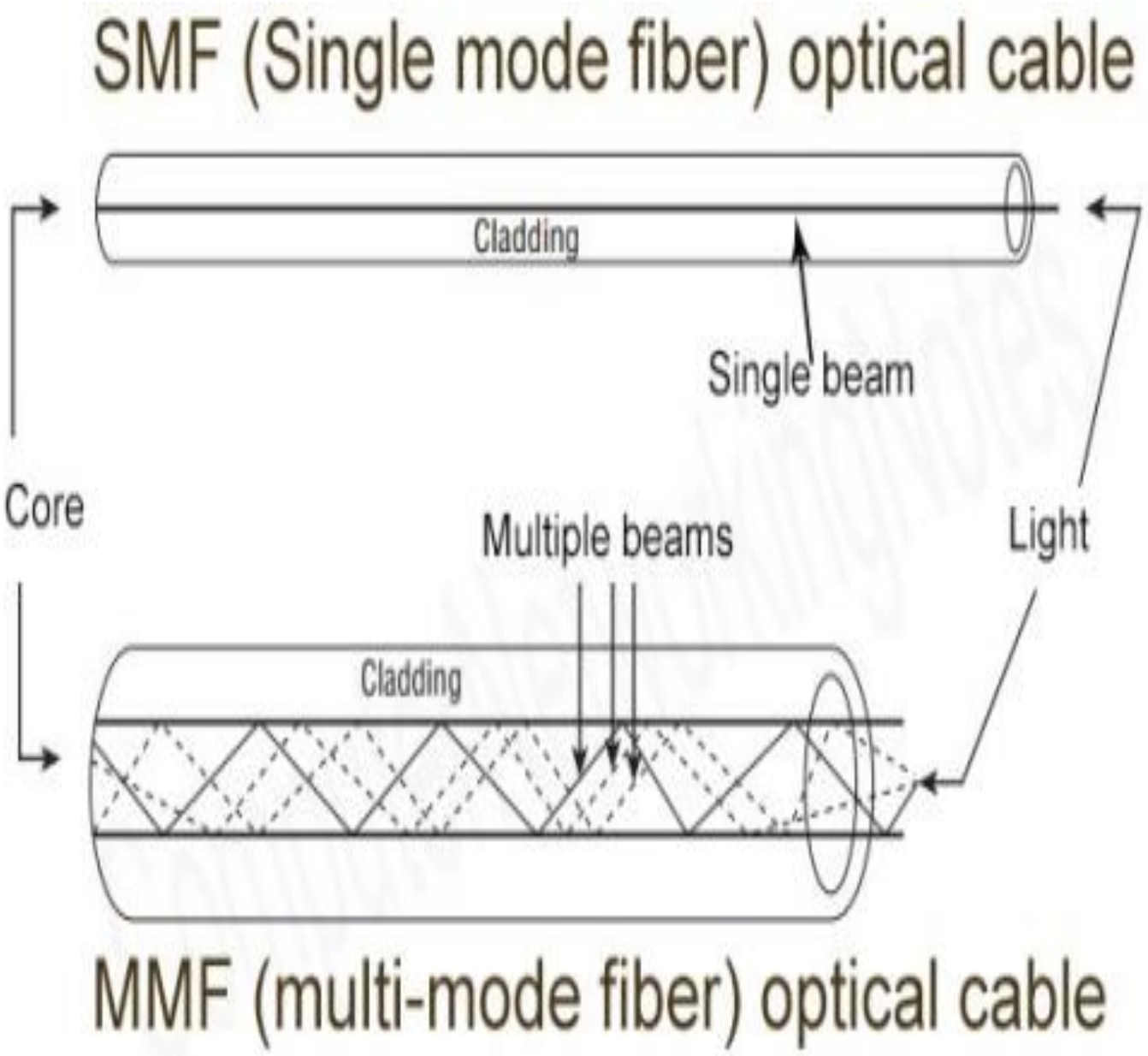
Core carries the data signals in the form of the light. Cladding reflects light back to the core. Buffer protects the light from leaking. The jacket protects the cable from physical damage.

Fiber 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 kilometers at the speed of 100Gbps.



There are two types of fiber optical cable: SMF (single mode fiber) and MMF (multi mode fiber).

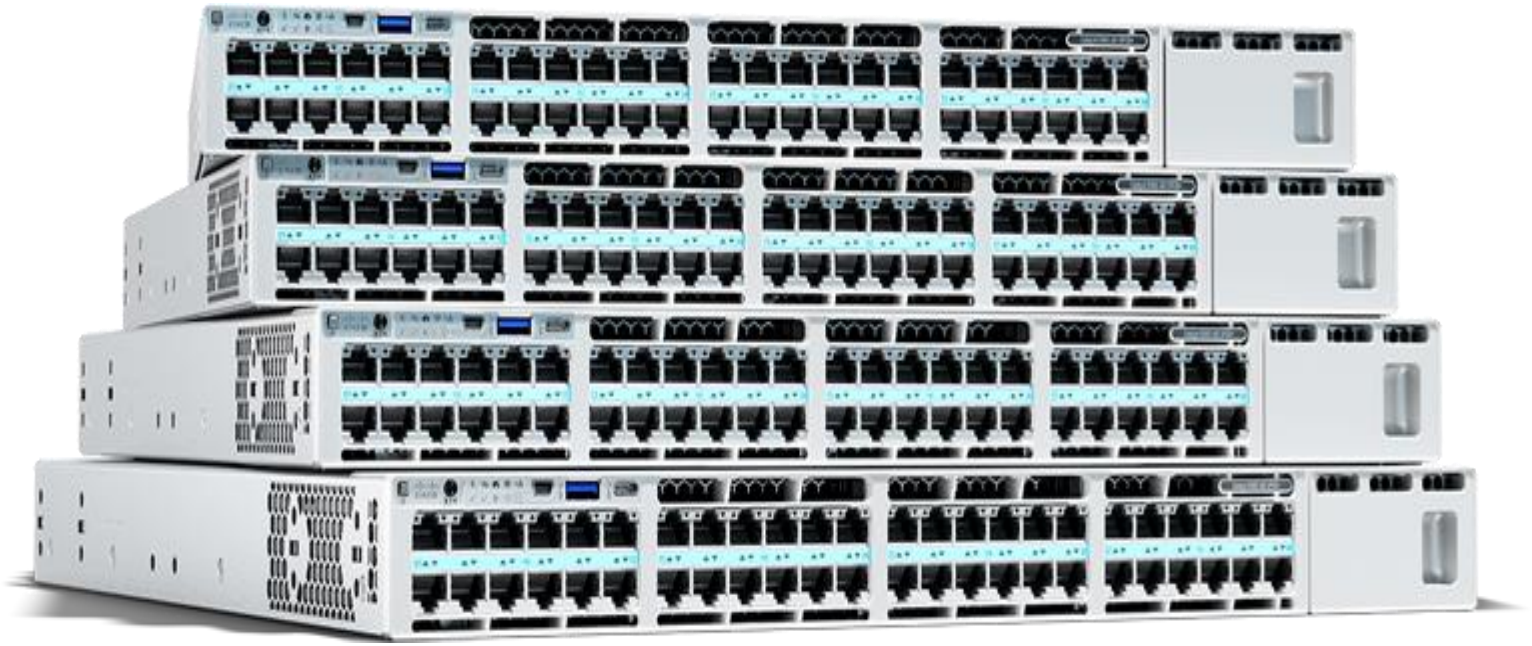
SMF (Single-mode fiber) optical cable. This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nanometer wavelengths of light. MMF (multi-mode 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 in shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nanometer wavelengths of light.



Switches (Unmanaged, Smart Web Managed, Full Managed)

When selecting the right type of switch to meet your needs, one consideration is whether to use a managed or an unmanaged switch. The key difference is in the amount of control you have over the settings of the switch.

Unmanaged switches are designed to just plug in and run, with no settings to configure. These are fine to use in small networks with only basic needs. Managed switches, however, are fully configurable, are customizable, and provide a range of data on performance. Those attributes make them more suitable for larger networks and networks supporting critical activities.



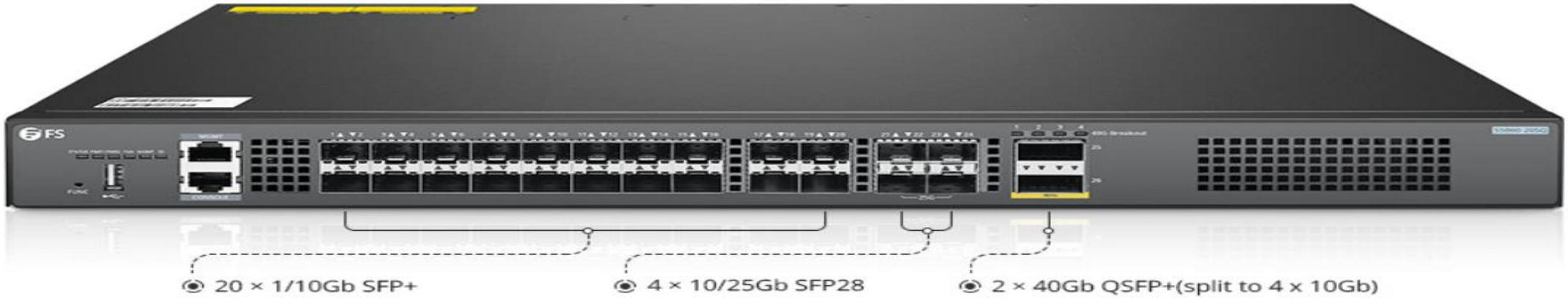
Managed switches and unmanaged switches differ in three areas: capabilities, security, and cost.

- Capabilities: Unmanaged switches immediately start forwarding traffic once users have plugged them in. They have no features besides what they need to negotiate transfer speeds and to determine each link's duplexing type. Managed switches can offer a huge number of features that can be configured by IT professionals, thus permitting a diverse array of deployment possibilities. These capabilities allow for optimization of network performance and availability.
- Security: Network security includes protection from and detection of threats to data and operability. Managed switches provide security settings that can be configured to protect the network and to help identify threats. Unmanaged switches do not offer security capabilities.
- Cost: For some users, cost is a significant choice driver. Unmanaged switches are cheap, as well as very simple to run. Managed switches, with all their additional capabilities, cost more than unmanaged switches. They also require more expertise to provision and manage, meaning added costs for staff with the skills to maintain the network

Web smart switches

Sometimes called smart switches or Web managed switches—have become a popular option for mid-sized networks that require management. They offer access to switch management features such as port monitoring, link aggregation, and VPN through a simple Web interface via an embedded Web browser. What these switches generally do not have is SNMP management capabilities. Web-smart switches must usually be managed individually rather than in groups.

A Smart Switch is a light switch that offers advanced features to help automate your home. They plug into the wall similar to normal switches. However, they have remote capabilities that help them connect to wireless networks. They may additionally include sensors to have automated operation.



Hardware/Software Firewall

A hardware firewall protects you from the outside world, and a software firewall protects a specific device from other internal systems. For example, if someone tries to access your systems from the outside, your physical firewall will block them.

But if you accidentally click on a virus-laden email that’s already managed to get into your system, your software firewall on the other computers in your office network may stop it from infecting them.

Even if you have both a hardware and software firewall, they may be useless unless you have the right people monitoring and managing them.

Hardware firewalls can be built-in a router or come as a separate gadget. Such devices have onboard memory running security policies, executing business rules, and routing network traffic. The devices themselves can range from a small tablet device to a large server.

Businesses are more likely to require a hardware firewall. It provides protection for your entire network through a single, standalone physical device, which means it also does not use server resources.

Disadvantage of a hardware firewall compared to a software firewall may include less flexibility in deployment, especially in virtualized or cloud environments, and potential higher upfront costs. However, advantages and disadvantages depend on needs and environment details.

The 3 Types of Firewalls You Need to Know

- Network-Based Firewall. A network-based firewall routes traffic between networks.
- Application Firewall. An application firewall (also called an application layer firewall) works with the TCP/IP stack to filter and intercept all traffic packets to/from apps.
- Proxy Server.

The best firewall software of 2024 is:

- Bitdefender Total Security. Best for all round security with firewall protection.
- Norton 360 Deluxe. Best multi-feature firewall protection.
- Avast Premium Security. Best multi-device firewall option.
- Panda Dome Essential.
- Webroot AntiVirus.

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

- **The main functions of a software firewall include:**
- Applying security rules to screen incoming and outgoing traffic.
- Blocking malicious programs and traffic that seek to gain access to network resources.
- Allowing authorized users to connect quickly and easily.

Study of UTM

Unified Threat Management (UTM), these capabilities better known as a Next-Generation Firewall (NGFW) today, provide multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way.

A UTM comes with antivirus software that can monitor your network, then detect and stop viruses from damaging your system or its connected devices. This is done by leveraging the information in signature databases, which are storehouses containing the profiles of viruses, to check if any are active within your system or are trying to gain access.

Some of the threats the antivirus software within a UTM can stop include infected files, Trojans, worms, spyware, and other malware.

Even though the malware is allowed to run, the UTM prevents it from interacting with other programs in the computer.

Wireless Routers DSL/ADSL: Latest Examples&Usage

DSL (Digital Subscriber Line) denotes an internet that uses digital connections between a modem and a phone line. ADSL means Asymmetrical Digital Subscriber Line where the speed of data sent is known as upstream and data received is known as downstream.

The high-speed internet that you connect to via Wi-Fi or an ethernet cable through a modem is DSL internet and it is a communication medium that receives data via a copper telephone landline.

ADSL is a popular, older type of broadband, with the term standing for Asymmetric Digital Subscriber Line. It is a broadband connection that works through the copper wires of existing phone lines and is mainly used for home broadband and within small businesses.

SHDSL: Single-Pair, High-Speed Digital Subscriber Line

Also known as G. SHDSL, this type of DSL transmits data at much higher speeds than older types of DSL. It enables faster transmission and connections to the internet over regular copper telephone lines than traditional voice modems can provide.

Network Access Control

There are two types of NAC, including the following:

- Pre-admission: evaluates access attempts and only allows entry to authorized devices and users.
- Post-admission: re-authenticates users trying to enter a different part of the network; also restricts lateral movement to limit the damage from cyber attacks.