TCP/IP NETWORKING

(CET 06102)

UNIT 1

Introduction

OCT 2024

- **TCP/IP** is a set of protocols (Protocol Suit) that enable communication between computers over the internet. Protocols are rules or standards that govern communications.
- If two devices in a network need to communicate, they need to use a common protocol. This can be compared with how humans speak.
- A French person cannot communicate with a Vietnamese person since they speak different languages.
- TCP/IP is known as "the language of the Internet." If you want a computer to work on the Internet, you have to use TCP/IP.

Features of TCP/IP

- **Multi-Vendor Support.** TCP/IP is implemented by many hardware and software vendors. It is an industry standard and not limited to any specific vendor.

- **Interoperability.** Today we can work in a heterogeneous network because of TCP/IP. A user who is sitting on a Windows box can download files from a Linux machine, because both Operating Systems support TCP/IP. TCP/IP eliminates the cross-platform boundaries.

Heterogeneous network *is a network connecting computers and other devices with different operating systems and/or protocols.*

- **Logical Addressing.**

An IP address is also known as a logical address and it can change over time as well as from one network to another. The Internet Service Provider will be in charge of assigning it. When a device connects to a different network, it receives a different IP address as a result of a change in Internet Service Provider.

With the help of Dynamic Host Configuration Protocol (DHCP), even in the same network, when a device wants to connect to the internet, it will acquire different addresses from the pool. There is no assurance that the device always has the same IP address. The IP address is not directly linked to any devices. As a result, it is referred to as a logical address.

However, there is a MAC address provided by the hardware interface vendor. It never changes when a device is attached to any network. As a result, it is referred to as a physical address.

Therefore:

The Logical/IP Address identifies a device in a network. But to reach and deliver data to the device, we need a MAC/Physical address.

- **Name Resolution.** IP addresses are designed for the computers and it is difficult for humans to remember many IP addresses. TCP/IP allows us to use human-friendly names, which are very easy to remember (Ex. www.omnisecu.com). Name Resolutions servers (DNS Servers) are used to resolve a human readable name (also known as Fully Qualified Domain Names (FQDN)) to an IP address and vice versa.

- **Error Control and Flow Control.** The TCP/IP protocol has features that ensure the reliable delivery of data from source computer to the destination computer. TCP (Transmission Control Protocol) defines many of these error-checking, flow-control, and acknowledgement functions.

- **Rout-ability.**

A router is a network infrastructure device which can read logical addressing information and direct data across the network to its destination. TCP/IP is a routable protocol, which means the TCP/IP data packets can be moved from one network segment to another.

- TCP protocol has methods for finding out corrupted segments, missing segments, out-of-order segments and duplicated segments.
- Error control in TCP is mainly done through the use of three simple techniques :

➢ *Checksum* – Every segment contains a checksum field which is used to find corrupted segments. If the segment is corrupted, then that segment is discarded by the destination TCP and is considered lost.

➢ *Acknowledgement* – TCP has another mechanism called acknowledgement to affirm that the data segments have been delivered. Control segments that contain no data but have sequence numbers will be acknowledged as well but ACK segments are not acknowledged.

➢ *Retransmission* – When a segment is missing, delayed to deliver to a receiver, corrupted when it is checked by the receiver then that segment is retransmitted again. Segments are retransmitted only during two events: when the sender receives three duplicate acknowledgements (ACK) or when a retransmission timer expires.

- **Multiplexing (Muxing)/De-multiplexing (De-muxing).**

Multiplexing is a way of sending multiple signals or streams of information over a communications link at the same time in the form of a single, complex signal.

Multiplexing means accepting data from different applications and directing that data to different applications listening on different receiving computers. On the receiving side the data need to be directed to the correct application, for that data was meant for. This is called De-multiplexing.

The de-multiplexer refers to the type of combinational circuit that accepts just a single input but directs it through multiple outputs.

We can run many network applications on the same computer. By using logical channels called ports, TCP/IP provides means for delivering packets to the correct application. In TCP/IP, ports are identified by using TCP or UDP port numbers.

The Benefits of Using TCP/IP

- Good failure recovery
- The ability to add networks without interrupting existing services
- High error-rate handling
- Platform independence
- Low data overhead

OSI Model

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.

Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. Its function is to transmit individual bits from one node to another over a physical medium. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

Data Link Layer

It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

- **Network Layer**

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

- **Transport Layer**

It is responsible for delivery of the entire message from the source host to destination host.

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

- **Session Layer**

It establishes sessions between users and offers services like dialog control and synchronization.

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and terminated at layer 5. Session layer services also include authentication and reconnections.

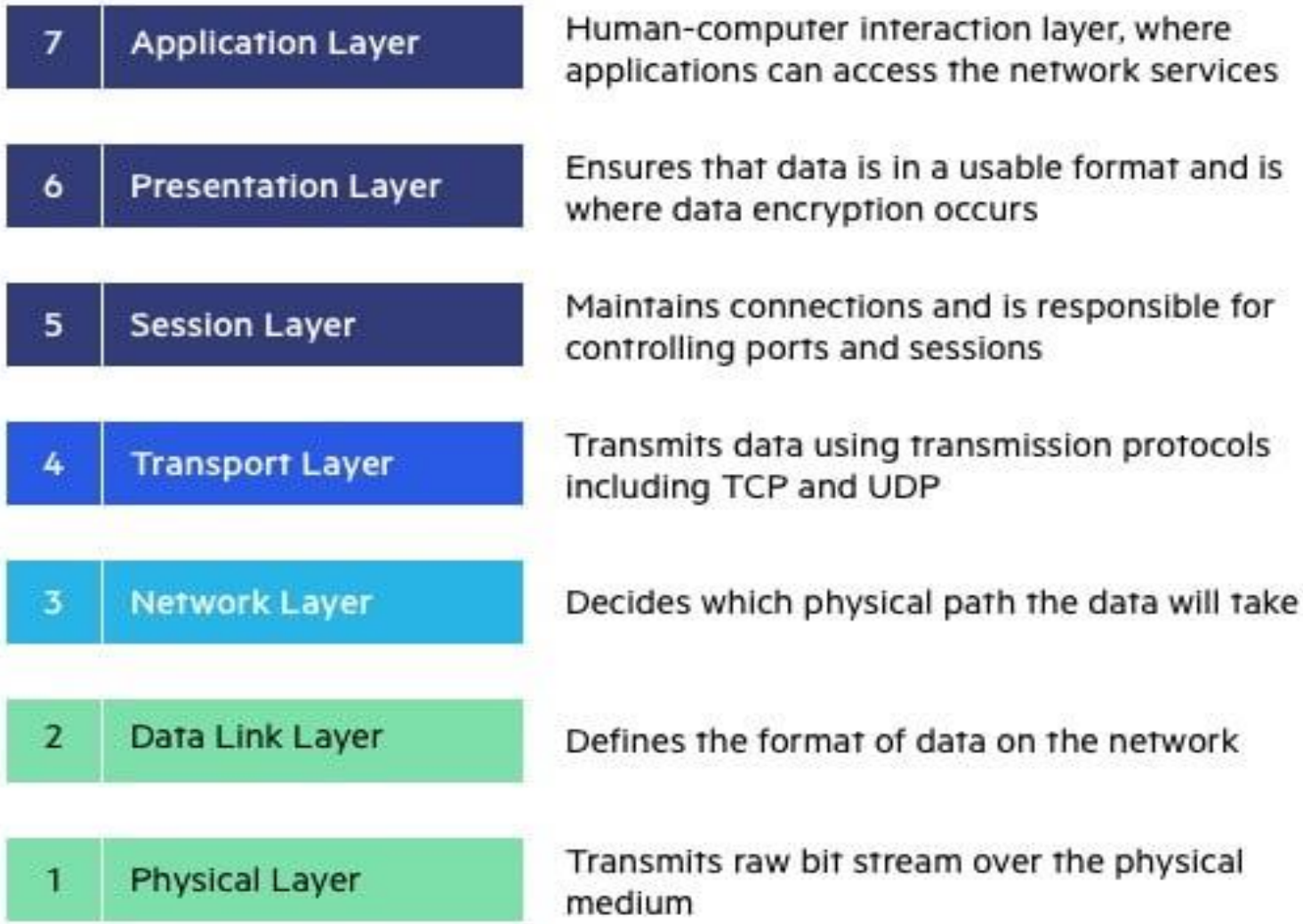
- **Presentation Layer**

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

- **Application Layer**

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

7 Layers of the OSI Model



TCP/IP Model

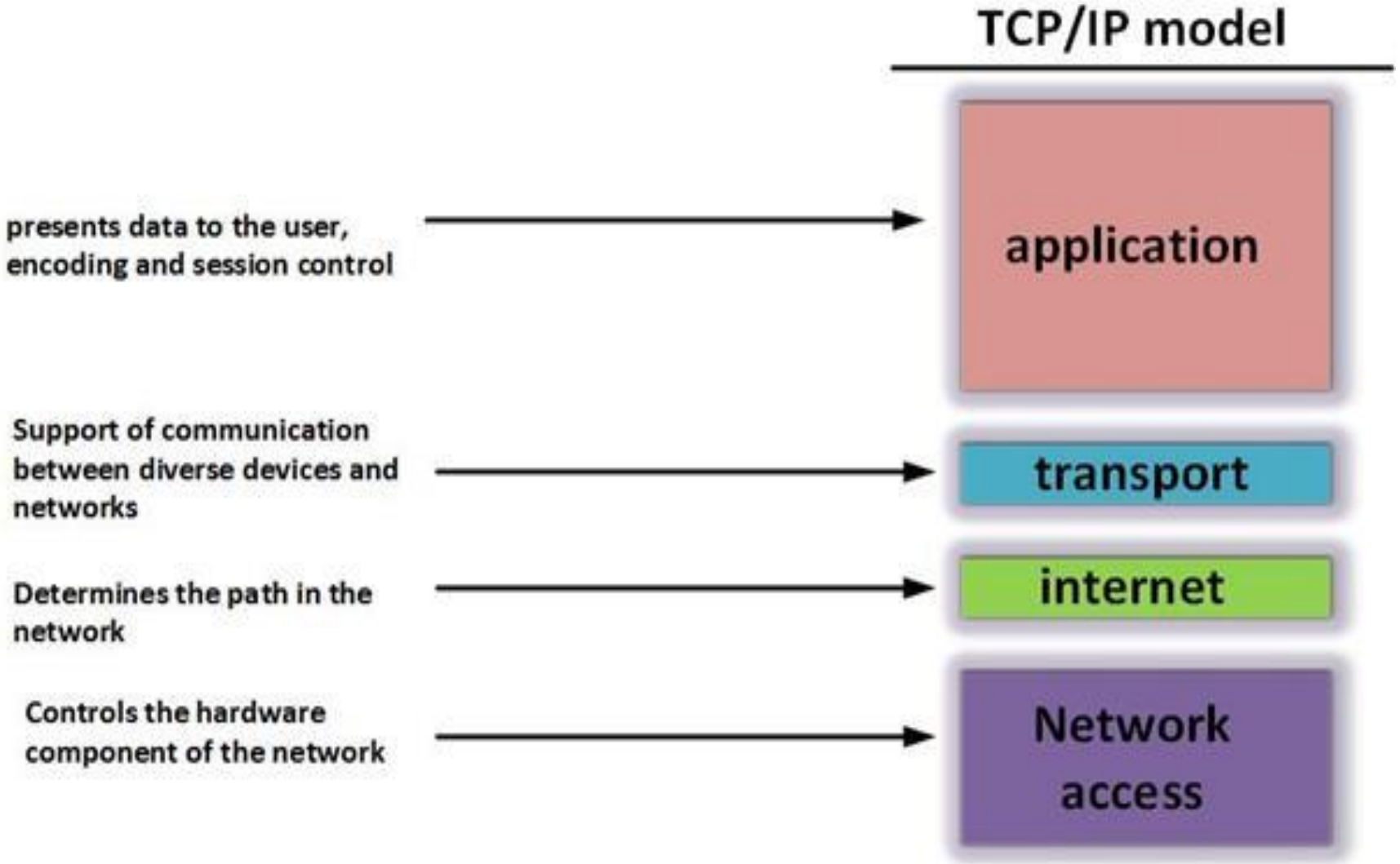
The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

TCP/IP Model helps to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together. The purpose of TCP/IP model is to allow communication over large distances. TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform.

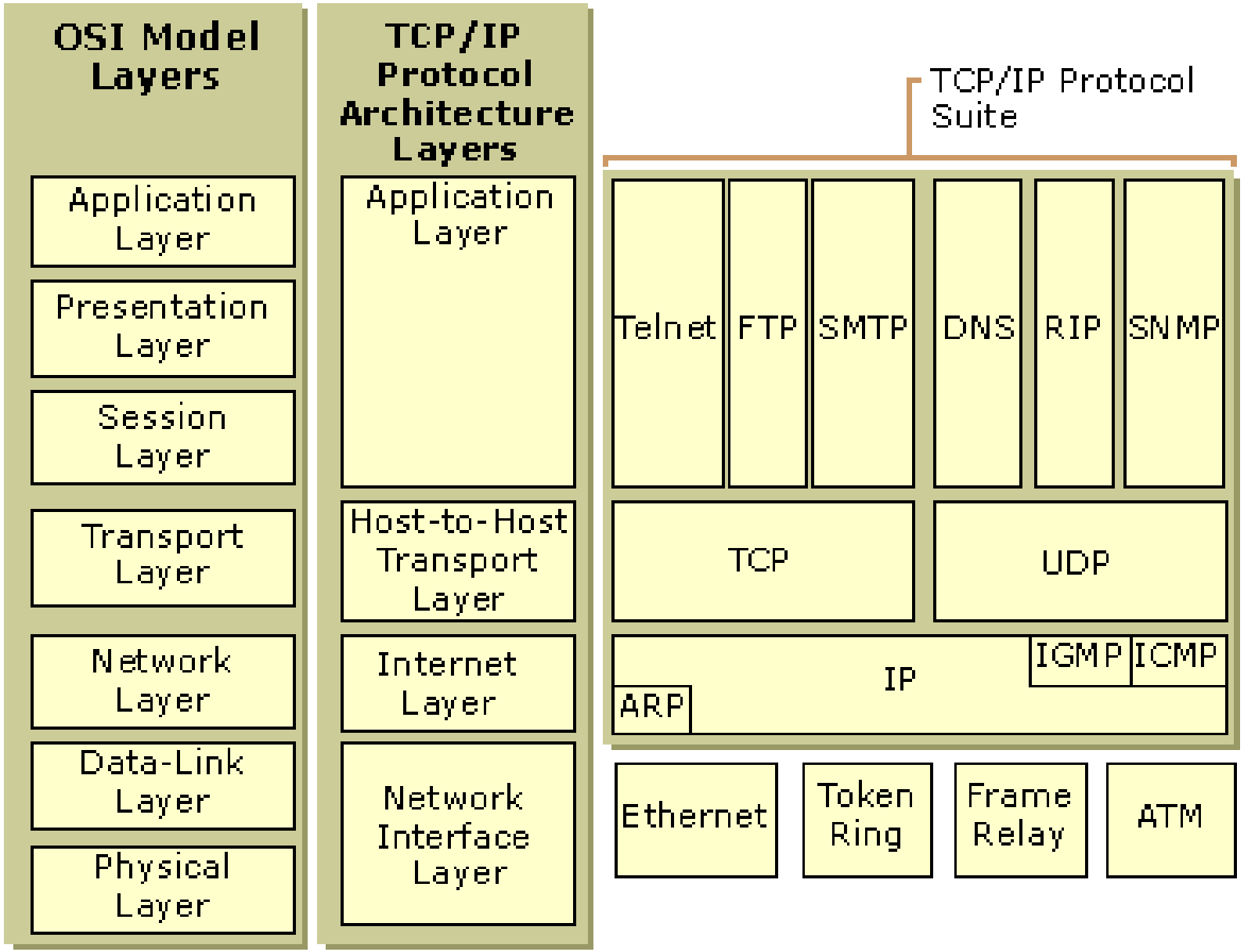
The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

4 Layers of TCP/IP Model



TCP/IP Protocol Architecture


OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IP
IGMP
ICMP
ARP
Ethernet
Token Ring
Frame Relay
ATM

- **Application Layer**

At the top of the TCP/IP protocol architecture is the Application Layer. This layer includes all processes that use the Transport Layer protocols to deliver data. There are many applications protocols. Most provide user services, and new services are always being added to this layer.

The most widely known and implemented applications protocols are:

Telnet. The Network Terminal Protocol, which provides remote login over the network.

FTP. The File Transfer Protocol, which is used for interactive file transfer.

SMTP. The Simple Mail Transfer Protocol, which delivers electronic mail.

HTTP. The Hypertext Transfer Protocol, which delivers web pages over the network.

While HTTP, FTP, SMTP, and Telnet are the most widely implemented TCP/IP applications,

you will work with many others as both a user and a system administrator.

- Some other commonly used TCP/IP applications are:

Domain Name System (DNS). It maps IP addresses to the names assigned to network devices.

Open Shortest Path First (OSPF). OSPF is used by network devices to exchange routing information.

Network File System (NFS). This protocol allows files to be shared by various hosts on the network.

Some protocols, such as Telnet and FTP, can be used only if the user has some knowledge of the network. Other protocols, like OSPF, run without the user even knowing that they exist.

- **Host-to-Host Layer Protocols**

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

Two protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are defined for transmitting datagram's.

Transmission Control Protocol (TCP)

TCP is connection-oriented in the senses that prior to transmission end points need to establish a connection first. TCP protocol data units are called segments. The sending and receiving TCP entities exchange data in the form of segments, which consist of a fixed 20-byte header followed by a variable size data field.

TCP is responsible for breaking down a stream of bytes into segments and reconnecting them at the other end, retransmitting whatever might be lost and also organizing the segments in the correct order.

- **User Datagram Protocol (UDP)**

UDP protocol consists of fewer fields compared to TCP. The reason for that is because certain data types do not require reliable delivery and extra overhead (overhead of a packet type is the amount of wasted bandwidth that is required to transmit the payload). Real-time traffic for example, needs to be transported in an efficient way without error correction and retransmission mechanisms.

UDP is considered to be a connectionless protocol. It leaves reliability to be handled by the application layer. All it cares about is fast transmission.

Which One Should You Use?

Choosing the right transport protocol to use depends on the type of data to be transferred. For information that needs reliability, sequence transmission and data integrity → TCP is the transport protocol to use. For data that require real-time transmission with low overhead and less processing → UDP is the right choice.

- **Internet Layer**

The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take. The Internet layer responsibilities include addressing, packaging, and routing functions.

Following are the protocols used in this layer are:

- IP Protocol
- ARP Protocol
- ICMP Protocol

- **Network Interface Layer**

It defines how the data should be sent physically through the network. This layer is mainly responsible for the transmission of the data between two devices on the same network. The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

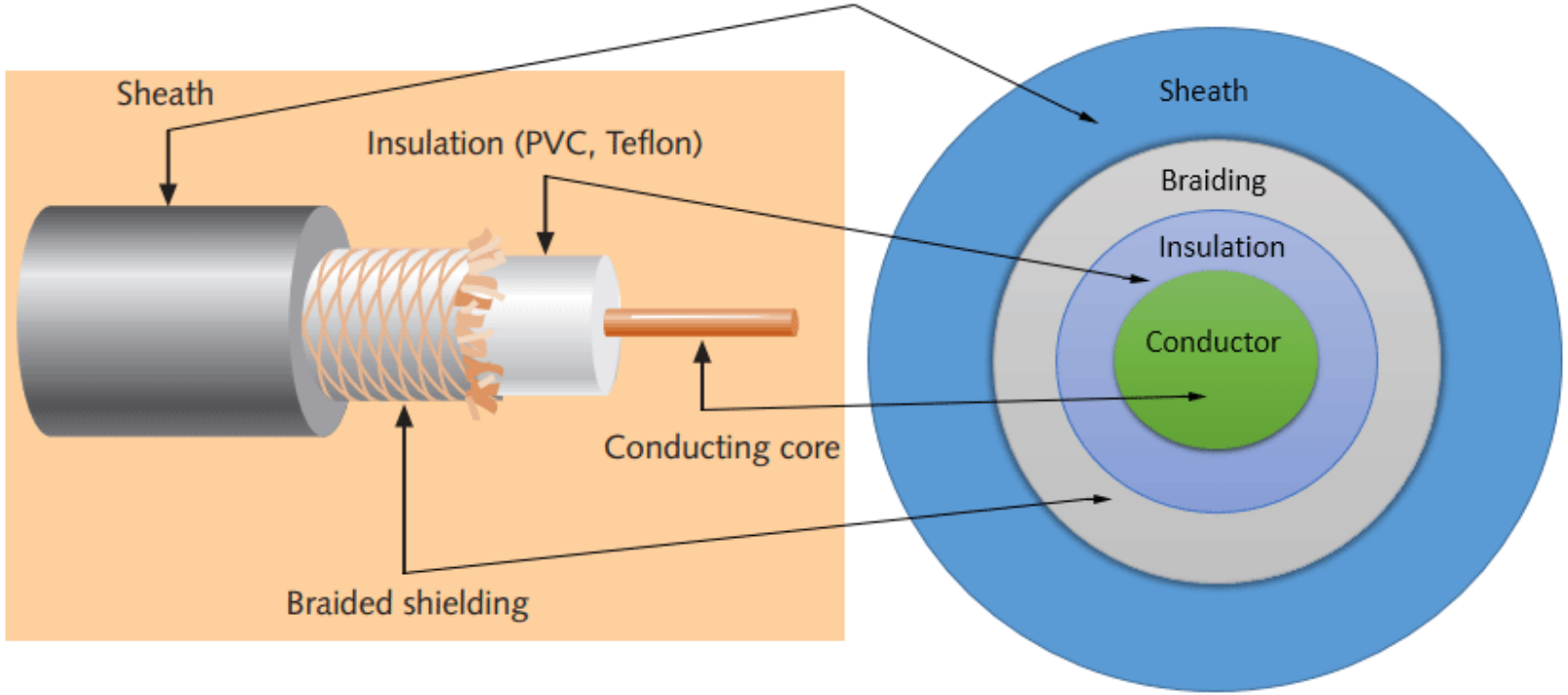
The protocols used by this layer are Ethernet, token ring, FDDI **(**Fiber Distributed Data Interface**),** X.25, frame relay.

Different Cables Configurations

▪ Coaxial cable

The great capacity of coaxial cable allows it to carry many channels simultaneously, eliminating the need for thousands of separate wires to be strung.

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.



➢*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 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 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.

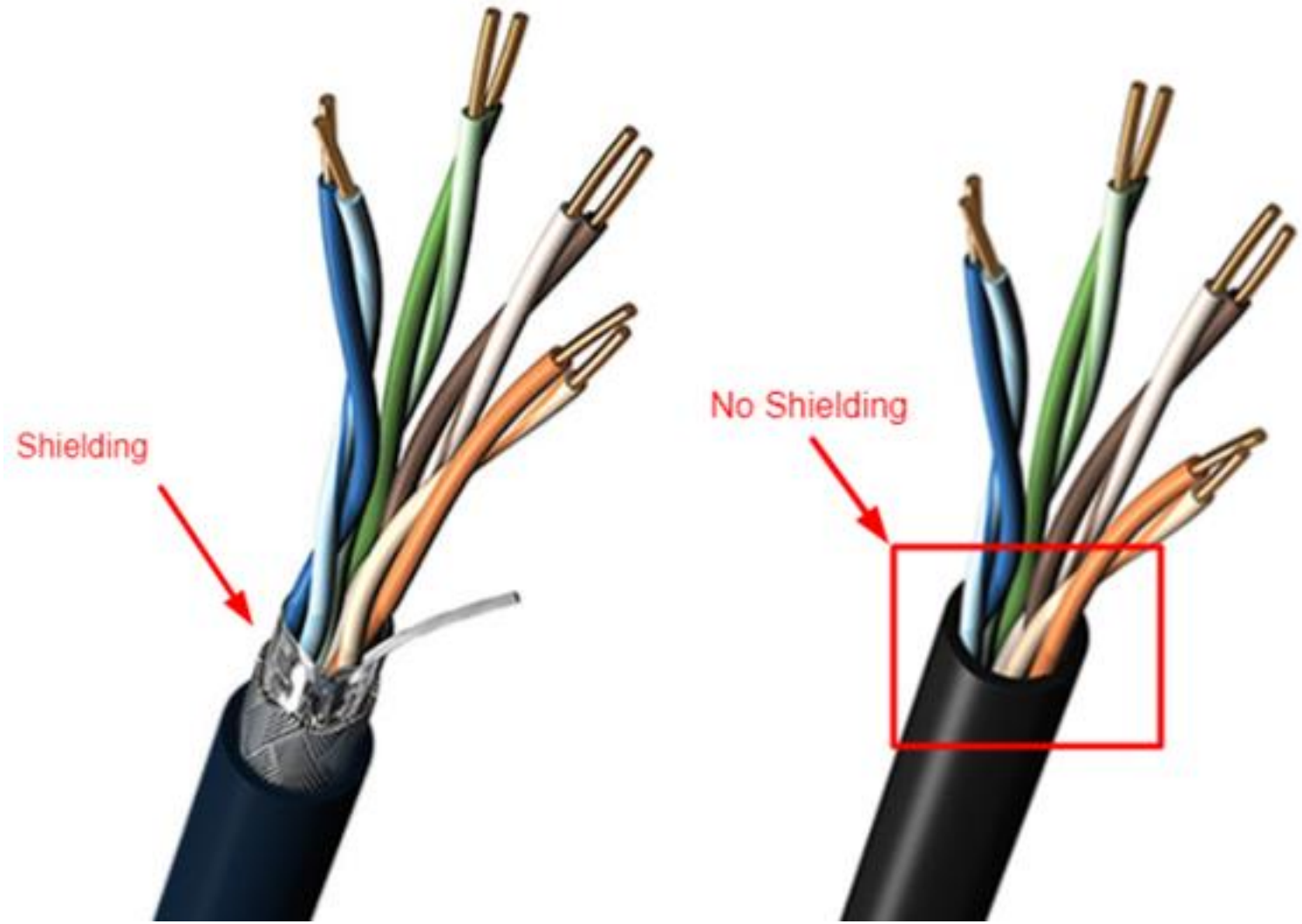
This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs.

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.


Shielding
No Shielding

▪ 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 (Electromagnetic Interference) resistance than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.

Why is UTP used more than STP?

- UTP cables contain no shields and they are thinner than STP cables, which is easier for cable installation and maintenance, particularly in limited space.
- STP cables are quite fragile and rigid. If the shield suffered damage, cabling systems are likely to be affected by interference.

Standards for the Twisted-pair Cable

The TIA/EIA specifies standards for the twisted-pair cable. The first standards were released in 1991, known as TIA/EIA 568. Since then, these standards have been continually revised to cover the latest technologies and developments of the transmission media.

The TIA/EIA 568 divides the twisted-pair cable into several categories.

- T568A and T568B standards

T568A and T568B are the wiring standards that define the pin-out (connection order) for terminating twisted-pair network cable in eight-pin modular connector plugs and jacks.

These wiring standards are one part of the TIA (Telecommunications Industry Association)/EIA (Electronic industries alliance)-568 telecommunications cabling standards.

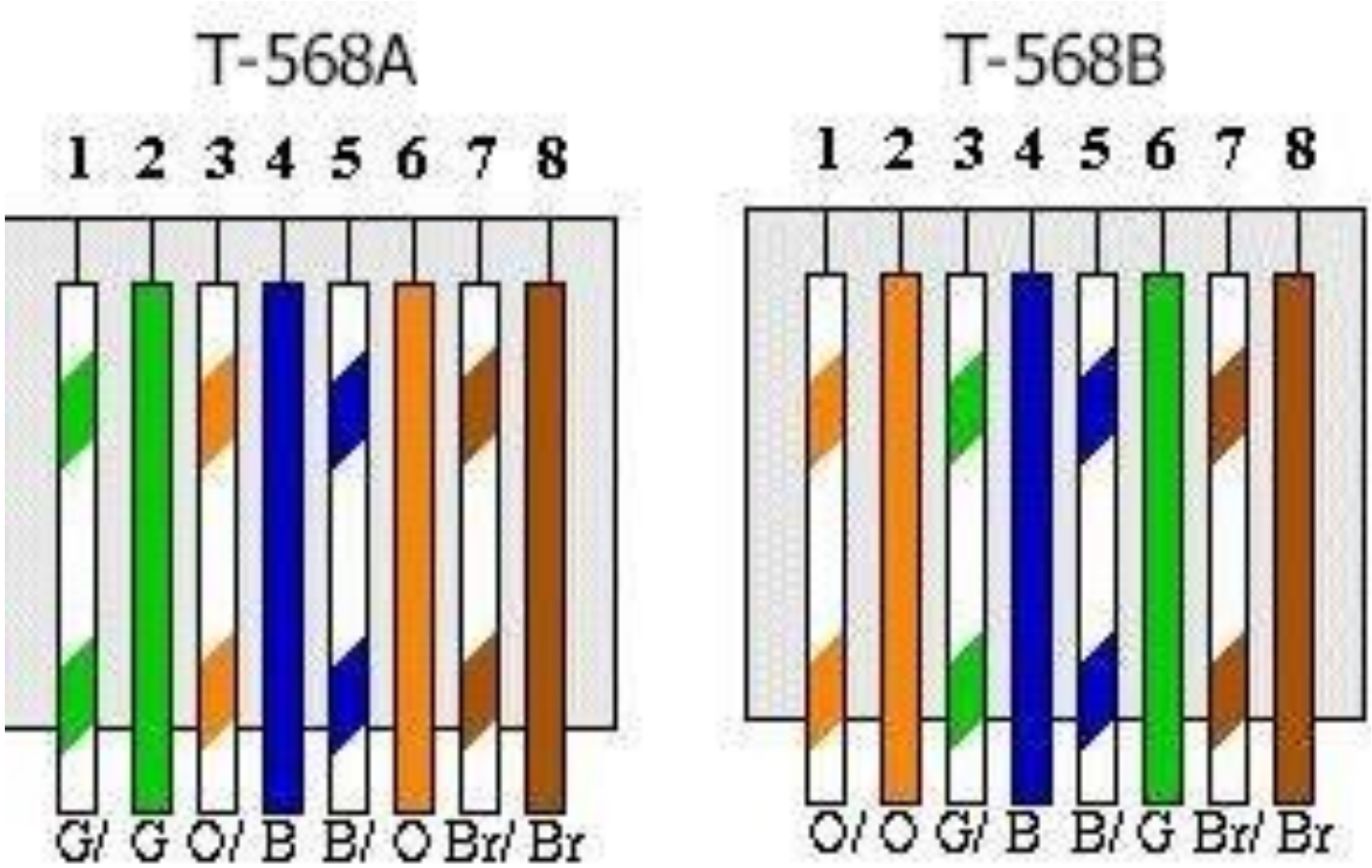
When terminating the end(s) of Ethernet cable, you have to follow a certain color code scheme, T568A or T568B. This scheme is designed to help the installer get the conductor wires into the right order so that your cable will work properly.

The only difference between T568A and T568B is that the orange and green pairs are interchanged. T568A wiring pattern is recognized as the preferred wiring pattern for this standard because it provides backward compatibility to both one pair and two pair USOC wiring schemes.

T568B is designed for better signal isolation and noise protection for newer networking systems and products and is the standard followed by the majority of Ethernet installations in the United States for RJ45 color code. It is the more common standard used when cabling for businesses.

T568A is designed for backward compatibility with older telephone wires and is the majority standard followed by European and Pacific countries.

T-568A AND T568B



Twisted-pair Cable Categories

Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4 pairs). This cable was used in the token-ring network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.
Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pair and shields each pair by its plastic sheath.

Cat 1, 2, 3, 4, 5 are outdated and not used in any modern LAN network.
Cat 7 is still a new technology and not commonly used.
Cat 5e, 6, 6a are the commonly used 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.

Fiber optic cable is completely immune to EMI (Electromagnetic Interference) and RFI (Radio Frequency Interference). 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.

Fiber optic uses light to send data. It reflects light from one endpoint to another.

▪ Two Types of Fiber Optical Cable

Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cables which are:-

➢SMF (Single-mode fiber) optical cable

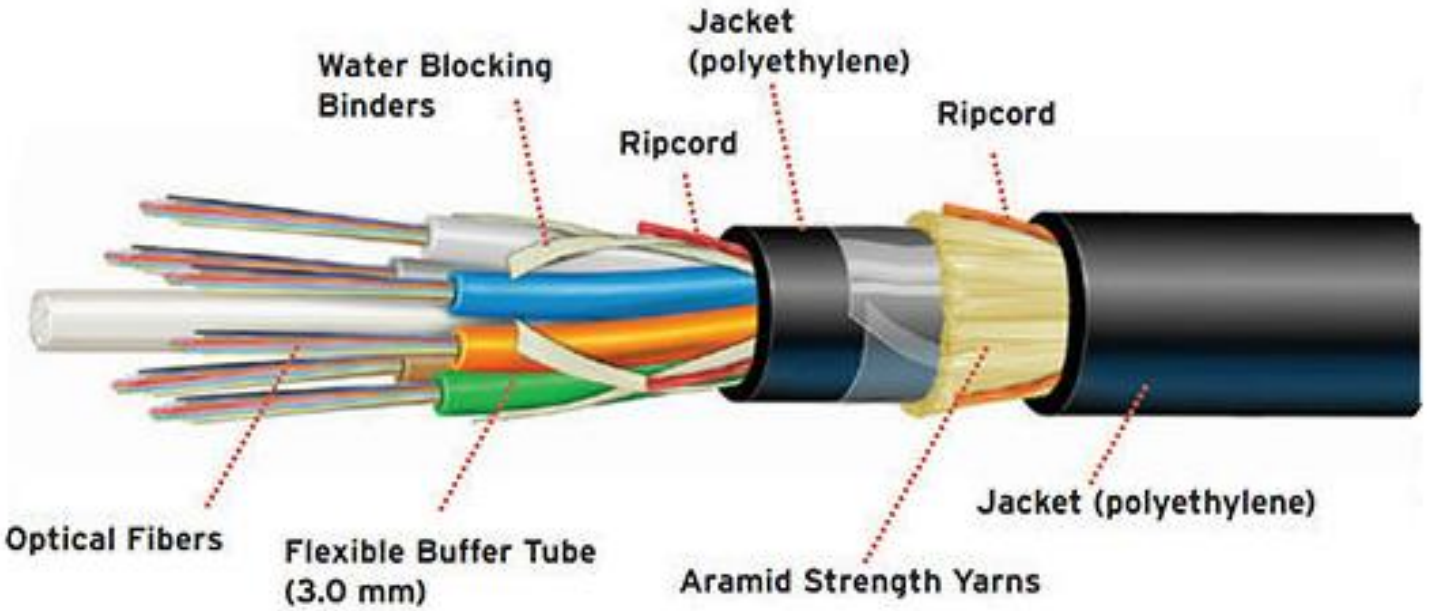
This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

➢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.

Fiber Optic Cable





Network Devices

Network devices, or **networking hardware**, are physical devices that are required for communication and interaction between hardware on a computer network.

- **Hub**

Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form.

Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model.


D-Link
FAST ETHERNET SWITCH
DES-108
D-Link

▪ Switch

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors.

You can think of a switch as a device that has some of the best capabilities of routers and hubs combined. A switch can work at either the Data Link layer or the Network layer of the OSI model. A multilayer switch is one that can operate at both layers, which means that it can operate as both a switch and a router. A multilayer switch is a high-performance device that supports the same routing protocols as routers.



▪ Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. *Routers are intelligent devices*, and they *store information about the networks they're connected to*.

Most routers can be configured to operate as packet-filtering firewalls and use access control lists (ACLs). Routers, in conjunction with a channel service unit/data service unit (CSU/DSU), are also used to translate from LAN framing to WAN framing.

This is needed because LANs and WANs use different network protocols. Such routers are known as border routers. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.

Router are also used to divide internal networks into two or more subnetworks. Routers can also be connected internally to other routers, creating zones that operate independently. Routers establish communication by maintaining tables about destinations and local connections.

A router contains information about the systems connected to it and where to send requests if the destination isn't known. *Routers usually communicate routing and other information using one of three standard protocols*: Routing Information Protocol (RIP), Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF).



▪ Bridge

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is *storing* and *forwarding frames between the different segments that the bridge connects*. They use hardware Media Access Control (MAC) addresses for transferring frames.

By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN.

Bridges work only at the Physical and Data Link layers of the OSI model. Bridges are used to divide larger networks into smaller sections by sitting between two physical network segments and managing the flow of data between the two.

▪ Gateway

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them.

Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

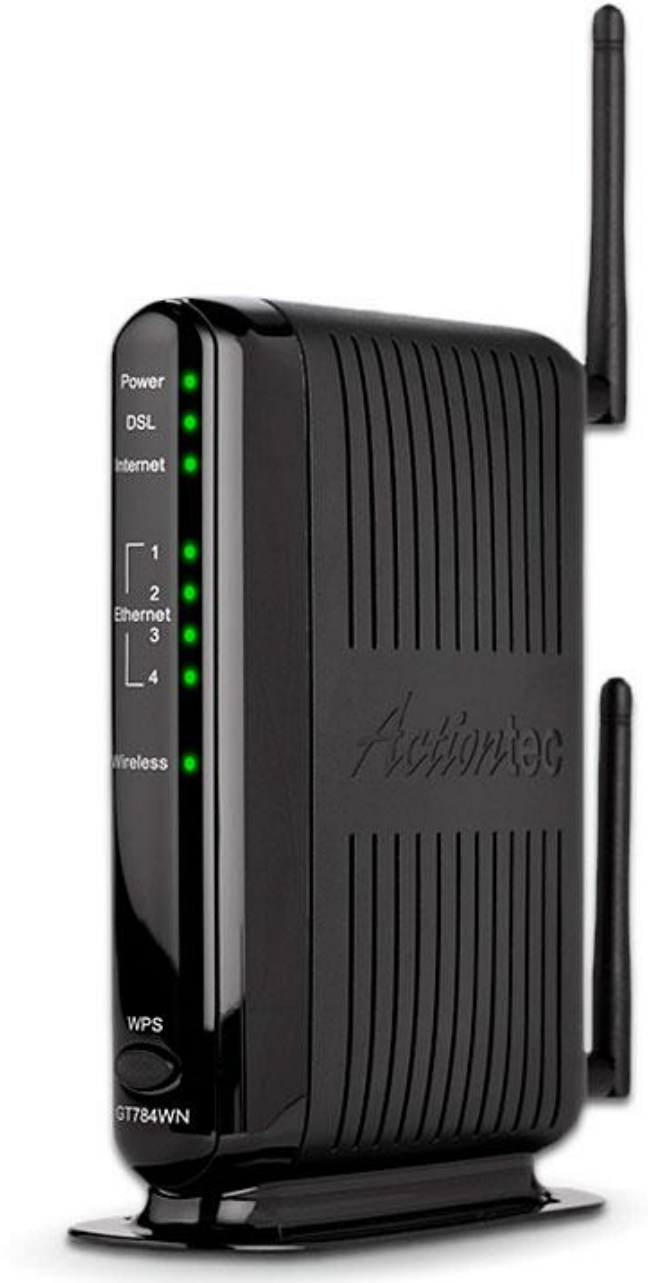
Gateways perform all of the functions of routers and more. In fact, *a router with added translation functionality is a gateway*. The function that does the translation between different network technologies is called a protocol converter.

▪ Modem

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, *digital signals are converted by the modem into analog signals of different frequencies* and *transmitted to a modem at the receiving location*.

The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The *digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232*.

Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users. Modems work on both the Physical and Data Link layers.


Power
DSL
Internet
1
2
Ethernet
3
4
Wireless
Actiontec
WPS
GT784WN

▪ Repeater

A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.

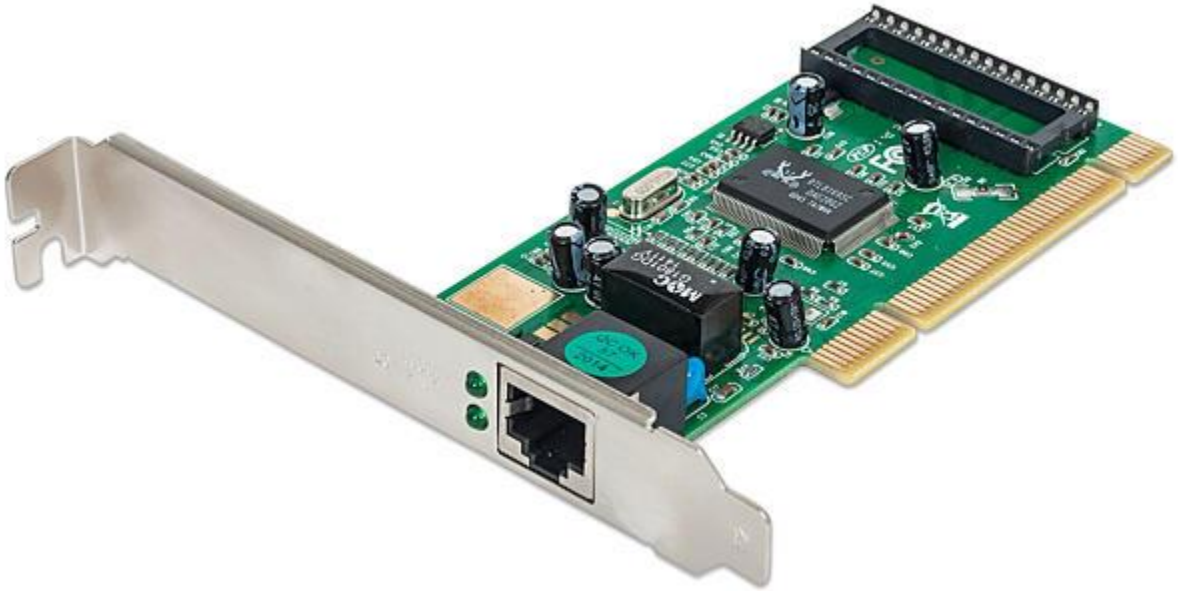
▪ Access Point

While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

▪ Ethernet Card

Ethernet card, also known as network interface card (NIC), is *a hardware component used by computers to connect to Ethernet LAN and communicate with other devices on the LAN*.

The earliest Ethernet cards were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has RJ45 socket where network cable is physically plugged in.



Network Configurations

Network configuration is the process of setting a network's controls, flow and operation to support the network communication of an organization and/or network owner.

Network configuration focuses on managing a network and its devices by applying the right set of policies, controls, and configurations. It encompasses activities from device discovery to configuration backups for efficient network administration.

Generally, network topologies denote various types of network configuration. *Network topology* refers to the systematic arrangement of nodes or devices in a network that allows them to exchange information.

Network topologies are of two types physical and logical. *Physical topology* depicts the linkages between physical devices via cables, wires, etc., in a network. In contrast, *logical topology* denotes how information is transferred through a network. The way devices interact in a network is also a part of the logical topology.

Some of the popular physical network topologies are:-

- **Bus:** Every node or device in the network is connected in a linear order with a unidirectional data flow. Bus topology is cost-effective, but it can break down quickly when there's high network traffic.
- **Ring:** Nodes are connected circularly, while data can flow in one or both directions as per needs. Ring networks are easy to set up and expand, but troubleshooting is often challenging.
- **Star:** A central server or node manages all other nodes with point-to-point communication. Star topology is commonly used in local area networks because of benefits such as centralized control, better security, and easy configuration. However, the entire network can crumble if the central server fails.
- **Mesh:** Nodes are linked in a web-like structure with point-to-point connections with every other node in the network. Data transmits through routing (shortest-path approach) and flooding methods (broadcast approach). Mesh networks are highly reliable but expensive to set up and maintain.

Network configuration key areas

- **Device discovery and management:** Configuration management discovers devices in your network and stores their critical details such as port configuration and interface details in a network inventory. Having up-to-date inventory also helps you generate reports quickly using filters such as device type, device vendor, and device location. Centralized inventory makes management easy.
- **Configuration backup and restore:** A network disaster can happen at any time, so an organization should regularly take network backups to stay future-ready. Regular backups allow you to quickly recover from unexpected scenarios such as equipment failure by uploading the most stable versions of your device settings.

- **Change management:** Maintaining accurate change records helps you identify the network engineers behind a particular configuration modification in your network. While this doesn't necessarily reduce network problems, it can accelerate the error resolution process. Standardization of change management practices, a crucial part of configuration management, ensures modifications across the network are well documented, prompt, and traceable.
- **Policy management and compliance audits:** Before making configuration changes, network administrators must formulate robust network policies to demonstrate compliance with various security standards. Network security policy creation and regular compliance audits of device settings are vital in configuration management.
- **Network automation:** Automation of network administration tasks such as device backups, firmware updates, and access rights modification is among the configuration management best practices. This boosts your network teams' productivity in addition to eliminating repetitive tasks and human errors.

Network configuration allows a system administrator to set up a network to meet communication objectives.

The process involves the following tasks:

Router configuration: Specifies the correct IP addresses and route settings, etc.

Host configuration: Sets up a network connection on a host computer/laptop by logging the default network settings, such as IP addressing, proxy, network name and ID/password, to enable network connection and communication.

Software configuration: Any network-based software, like an intrusion detection system (IDS), is allowed access and provided with the appropriate credentials to monitor network traffic.

Moreover, network configuration includes Internet/network sharing, software/application installation and firewall installation/configuration.