SITE 1101: Principles of Information Systems

Week 08

Telecommunications & Computer Network

Authors: Rahida Asadli, Ismayil Shahaliyev

Created / Updated: Nov 23 2025 / Dec 20 2025

Teleecommunications

Telecommunications at its core, is the long-distance transmission of information using electronic or electromagnetic signals. Whenever two devices exchange information (e.g. voice call, video stream, bank transaction) some form of telecommunications is functioning in the background. Telecommunications allows communication to happen without the sender and receiver being physically close. A phone call from one country to another, a university campus connecting its buildings, or a satellite sending weather data to Earth are all examples of telecommunications enabling interaction across space.

Every telecommunication system follows the same basic structure: *sender → channel (medium) → receiver*. The *sender* is where information originates. For example, when you type a message on a smartphone, the phone acts as the sender by converting your text into a digital signal suitable for transmission. The signal then travels through the *channel*, which is the path between sender and receiver. This path may be a physical medium, such as a copper or fiber-optic cable, or a wireless medium using electromagnetic waves, as in Wi-Fi or mobile networks. Different channels have different characteristics, affecting speed, cost, and resistance to interference. At the *receiver*, the incoming signal is converted back into a form the user can understand, such as readable text on a phone screen. For communication to work, both sender and receiver must follow shared rules called *protocols*, which define how data is formatted, transmitted, and interpreted. Without protocols, devices would not be able to understand each other.

Glossary

Before starting our discussion, it is important to understand some of the technical terms used in telecommunications and networks. These terms appear frequently in networking and telecommunications, and knowing them makes it easier to understand more advanced concepts.

Attenuation refers to the weakening or loss of a signal as it travels through a transmission medium. All signals gradually lose strength the farther they move, but the amount of loss depends on the cable type. Electrical signals traveling through copper wires, for example, lose strength much more quickly than light signals traveling through fiber-optic cables. If attenuation becomes too high, the receiver may get a distorted or unreadable signal, which is why long cables often require repeaters or amplifiers.

Electromagnetic Interference (EMI) describes the effect that external electrical or magnetic sources have on a cable's signal. Nearby power lines, motors, electronic devices, and even fluorescent lights create electromagnetic fields that can disturb data transmission. Copper-based cables are especially vulnerable to EMI because they carry electrical signals.

Fiber-optic cables, on the other hand, use light instead of electricity and therefore cannot be influenced by electromagnetic fields at all.

Bandwidth is the *maximum* amount of data that a communication medium or network can carry per second. It is similar to the width of a water pipe: the wider the pipe, the more water can flow through it at once. In the same way, a cable or wireless link with higher bandwidth can carry more bits of data every second. Bandwidth is usually measured in *Mbps* (megabits per second) or *Gbps* (gigabits per second). Bandwidth is not about how fast each bit moves – because all electrical or light signals always travel extremely fast – but about how much data can move at the same time.

Example. Imagine two Internet connections: one with *10 Mbps* and another with *100 Mbp*s. If you try to download a 100 MB video file, the 100 Mbps connection can transfer far more data per second, so the file will download much faster. In cables, the same logic applies. A twisted-pair cable with a bandwidth of 100 Mbps per 100 meters can only carry a moderate amount of information at once. A coaxial cable can support around 500 Mbps, so it can transfer several times more data in the same timeframe. Fiber-optic cable can carry gigabits of data every second, meaning it has an extremely wide "data highway" that can support huge amounts of information without slowing down.

Throughput is the actual amount of data that successfully travels through the network per second. While bandwidth is the theoretical maximum capacity, throughput represents what you really experience in real conditions. Many factors can reduce throughput, such as interference, cable quality, distance, network congestion or equipment limitations. *Network congestion* happens when more data is trying to pass through the network than the network can handle at that moment. Because the "data highway" is full, everything slows down.

Example. Suppose your Wi-Fi connection has a bandwidth of 300 Mbps, but your laptop receives only 80 Mbps during real usage. This difference comes from obstacles like walls, other Wi-Fi networks nearby, or older hardware. Although the network *could* support 300 Mbps in ideal conditions, the throughput is only 80 Mbps because that is the actual rate at which data is being delivered. Throughput is always equal to or lower than bandwidth. It can never be higher because you cannot exceed the maximum capacity of the medium. When people complain that their "Internet is slow," they are not complaining about bandwidth itself, they are complaining about reduced throughput caused by delays, interference, or congestion.

Signal type indicates the physical form of the transmitted data. Twisted-pair and coaxial cables both carry electrical signals, meaning electrons move through a copper conductor. Fiber-optic cables carry light signals, where small, rapid flashes of light encode the data. The physical difference between electrons and light explains why fiber performs better in speed, distance, and reliability, as well as why they are more expensive.

Properties/Type	**Twisted pair**	**Coaxial cable**	**Fiber-optic cable**
Cost	Low	Medium (≈2–3× twisted pair)	High
Installation	Easy	Easy	Difficult
Attenuation	High	Moderate	Very low
Signal type	Electrical	Electrical	Optical (light)

Bandwith	~1–100 Mbps	Hundreds of Mbps to Gbps	Gbps to Tbps
Distance	~100 m	~100 m	Kilometers
EMI effect	High	Low	None

Latency is the time it takes for a piece of data to travel from one point to another. Even if the bandwidth is high, high latency can make communication feel slow. Local networks have low latency, long-distance communication may have higher latency.

Exercise. Determine bandwidth and throughput of your device’s connection.

Direction

Communication systems can be classified by the direction in which data flows between sender and receiver. In practice, information may flow in only one direction, alternate between directions, or move in both directions at the same time. These differences affect how interactive a system feels and what it can be used for. The three basic types are *simplex*, *half-duplex,* and *full-duplex* communication.

Simplex communication is one-way only. Data flows from sender to receiver, and the receiver cannot respond over the same channel. There is no interaction. This model is used when feedback is unnecessary and the goal is simply to distribute information. A television broadcast is a classic example: the station sends signals, and TVs only receive them. Digital billboards and public display screens work the same way – they show information but send nothing back.

Half-duplex communication allows data to flow in both directions, but not simultaneously. A device can either send or receive at any given moment, and communication happens by taking turns. This is simpler and cheaper than full-duplex but slower and less natural. Walkie-talkies are the typical example: one person speaks while the other listens, then they switch. Older shared-cable Ethernet networks and many radio systems for taxis or emergency services also use half-duplex communication.

Full-duplex communication allows simultaneous two-way data transfer. Both sides can send and receive at the same time, creating smooth and natural interaction. This requires more complex system design but provides the best user experience. Phone calls are a clear example: both people can speak and hear each other at once. Modern mobile networks, video calls, and Internet connections also rely on full-duplex communication, enabling fast, continuous exchange of data.

Time

Communication systems can also be classified based on the time relationship between the sender and the receiver. Timing determines whether both parties must be active at the same moment, and it influences how quickly information travels and how interactive the communication feels. When timing is strict and aligned, communication becomes immediate and *real-time*. When timing is flexible, systems allow delays and do not require participants to respond instantly. This distinction shapes the design of many modern technologies, from video calls to email platforms.

Synchronous communication requires both endpoints to be active at the same time and to exchange data immediately. This model tightly *couples* the sender and receiver in time and often in execution flow. It assumes low latency, predictable availability, and sufficient resources on both sides. Synchronous communication is therefore appropriate when results are needed immediately or when later processing would be incorrect, such as real-time control systems, live audio/video streaming, or interactive remote procedure calls where the caller blocks until a response arrives.

Asynchronous communication removes this temporal coupling. Asynchronous communication is not primarily about delayed human interaction. It is a core architectural choice used to handle latency, partial failure, load imbalance, and limited resources in scalable and resilient systems.

The sender and receiver do not need to be active simultaneously, and the sender does not block waiting for the receiver to process the message. Instead, data is buffered, queued, or persisted until it can be handled. This model exists primarily to improve scalability, fault tolerance, and resource utilization in technical systems.

Asynchronous communication is essential when workloads are sudden or unpredictable. For example, email servers process messages asynchronously so that incoming traffic spikes do not overload delivery or storage systems. Messages are queued and processed in batches, allowing throughput to be optimized independently of arrival time. Asynchronous execution is also critical for efficient use of computational resources. Long-running tasks such as data processing jobs, model training, video transcoding, or backup operations are executed asynchronously so they do not block user requests or real-time services. Task schedulers and job queues distribute work when CPU, memory, or GPU resources become available.

Range

Another important way to understand communication systems is by the physical range they cover. Distance determines how far signals must travel and what types of technologies or transmission media are required. A small-scale personal network inside a room operates very differently from massive global networks that span oceans and continents. As the distance grows, the complexity, infrastructure, cost, and technologies involved grow as well.

Personal Area Network (PAN) covers only a very small area, usually within a few meters around a single person. PANs connect personal devices such as smartphones, smartwatches, earbuds, fitness trackers, and laptops. The purpose of a PAN is to allow an individual user's devices to communicate with each other seamlessly and wirelessly.

Local Area Network (LAN) covers a limited geographic area such as a home, office, school building, or university campus. LANs are designed to connect multiple devices so they can share resources like printers, databases, internet access, and internal applications. LANs usually rely on Ethernet cables, Wi-Fi access points, switches, and routers to ensure reliable communication among devices within the same location.

Example. A typical example of a LAN is the network inside your home. Your router distributes internet access to your phone, laptop, smart TV, and gaming console. All these devices are part of the same LAN, which allows them to communicate with each other efficiently. Another example is an office network where dozens of computers connect to a central server, shared printers, and company databases. University labs, libraries, and academic buildings also rely on LANs to allow students and staff to access educational resources. LANs are known for high speed, low cost, and strong control since everything is located in a confined area.

Metropolitan Area Network (MAN) spans a larger area than a LAN, typically a city or a large campus consisting of multiple buildings. MANs are used when organizations need to connect several LANs together across a broader space while maintaining high-speed communication.

Wide Area Network (WAN) covers extremely large geographic areas, such as multiple cities, countries, or even entire continents. WANs are designed to support long-distance communication across thousands of kilometers. Because of the enormous distances involved, WANs use advanced technologies such as satellite links, undersea fiber-optic cables, high-speed backbone networks, and powerful routers capable of long-distance routing.

Example. The most significant example of a WAN is the Internet itself, which links billions of devices across the planet. When someone in Azerbaijan visits a website hosted in the United States, the data travels through a WAN that spans multiple networks, undersea cables, and data centers. International banking networks are also WANs because they allow ATMs and bank branches around the world to access the same financial systems. Global shipping companies, airlines, and multinational corporations rely on WANs to connect their offices across continents. No matter the scale, a WAN always involves long-distance communication that joins many smaller networks into one vast global system.

Computer Networks

A computer network is a collection of devices connected so they can exchange data. Devices communicate by sending small units of information across cables or wireless signals. To make this possible, each device must use specific hardware and addressing methods. The following terms describe the key building blocks of any network.

Glossary

MAC (Media Access Control) address is a unique, hardware-based identifier for network devices, like a serial number for your Wi-Fi or Ethernet card, used to identify them on a local network segment (like your home Wi-Fi) for data delivery, often shown as 12 hexadecimal digits (e.g. 00:1A:2B:3C:4D:5E) and sometimes called a physical or burned-in address. It is crucial for network communication, ensuring data packets reach the correct device, and can be found in device settings or using command-line tools like `ipconfig /all` on Windows.

IP (Internet Protocol) address is a logical address assigned to a device so it can communicate across different networks. Unlike the MAC address, an IP address can change depending on the network you connect to. Routers use IP addresses to determine the correct path for data across wider networks such as the internet.

Hub is a simple device that connects multiple computers but does not analyze or direct data intelligently. When it receives data from one device, it copies that data to all connected devices. Hubs do not read addresses, which creates unnecessary traffic and makes them inefficient.

Switch is a more advanced version of a hub. It learns the MAC addresses of connected devices and forwards data only to the specific device that should receive it. This reduces traffic and increases network performance. Switches operate inside a local network.

Router connects different networks together. It reads IP addresses in the data and chooses the best route for packets to reach their destination. A home router connects your local network (your devices) to your internet service provider and then to the wider internet.

Modem connects a local network to the physical infrastructure of the internet service provider (ISP). It modulates discrete digital data from a computer into a continuous physical signal suitable for transmission over the communication medium, and then converts the received continuous signal back into discrete digital data. This process is called **mo**dulation and **dem**odulation. The modem does not route traffic, it provides access to the ISP network. In practice, many home devices combine modem, router, and switch functionality into a single unit, but these are logically distinct components.

Frame is the unit of data used inside a local network when switches forward information. Frames carry MAC addresses. When data leaves the local network and moves through routers, it becomes packets that carry IP addresses.

Packet is a small unit of data that travels across a network. Each packet contains the data being sent plus addressing information, which allows it to reach the correct destination even if packets travel different paths.

Packet switching works by breaking data into small packets and sending them independently through the network. If a network sent data as one large continuous stream, the channel would be occupied until the entire transmission finished, blocking others. With packet switching, packets from many users are interleaved on the same links. This allows the network to stay busy and avoids wasting bandwidth when one sender is slow or idle. Packets can also take different paths through the network. If a link or router fails, packets are automatically rerouted through alternative paths. If some packets are lost or corrupted, only those packets are retransmitted, not the entire message. This makes the system robust against failures and congestion.

Port in networking is a logical endpoint used by applications to separate different types of communication. For example, web traffic uses port 80 or 443. Ports allow multiple services to run on the same device without mixing their data.

Exercise. Determine IP and MAC addresses in your device.

Network Topologies

Network topology describes the *physical* or *logical* arrangement of devices and connections in a network. It defines how *nodes* (computers, switches, routers) are interconnected and how data flows between them.

Physical topology refers to the actual cables and hardware connections, when logical topology refers to how data moves regardless of the physical wiring. The choice of topology directly affects latency, bandwidth utilization, ease of expansion, and how failures propagate through the network.

Common network topologies include bus, star, ring, mesh, and hybrid forms. Each topology represents a different trade-off between simplicity, cost, performance, and resilience. Early networks favored simple topologies due to hardware limitations, while modern networks often use hierarchical or hybrid topologies to support large scale and high availability.

Bus Topology

In a bus topology, all devices are connected to a single main cable, often called the backbone. Every device sends data onto this shared cable, and all other devices listen, but only the intended device processes the data. Because all communication uses the same line, too many devices can cause collisions and slow performance. If the main cable fails, the entire network stops functioning.

Example. Early office networks used a single coaxial cable running along the floor or ceiling, and all computers tapped into it. If someone accidentally damaged that cable, no computer could communicate.

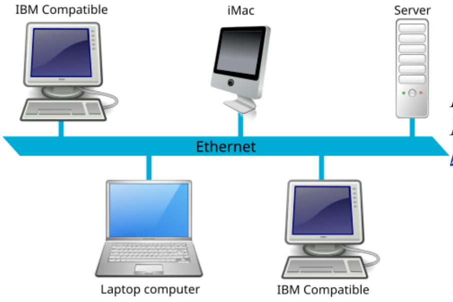

Figure 1. A conceptual diagram of a LAN using bus topology *Adapted from Network Topologies, Wikipedia, Wikimedia Commons, https://en.wikipedia.org/wiki/Bus_network. Licensed under CC BY 2.5*

Star Topology

In a *star topology*, all devices connect to a central device, typically a switch or hub. Each device has its own cable to the central point. The central device controls all data flow and decides where data should go. If one cable fails, only that one device is affected; the rest of the network continues working. However, if the central switch fails, the entire network stops.

Example. Modern home and office networks use star topology. Every computer, printer, or access point connects individually to a central switch or router.

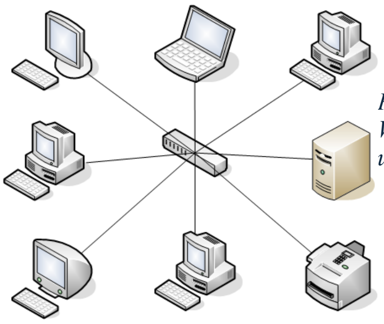

Figure 2. Star topology in use in a network Adapted from Network Topologies, Wikipedia,WikimediaCommons, https://en.wikipedia.org/wiki/Star_network. Licensed under By Umapathy - Own work, CC BY-SA 3.0,

Ring Topology

In a *ring topology*, each device connects to exactly two others, forming a closed loop. Data travels around the ring in one direction (or sometimes both directions), passing through each device until it reaches the destination. If one connection breaks, the entire loop can be disrupted, unless the network is designed with automatic rerouting.

Example. Some older MANs and early campus networks connected buildings in a circular loop. Data traveled from one building to the next until it reached the correct location.

Mesh Topology

In a mesh topology, every device connects directly to several other devices. There are multiple paths for data to travel. If one link fails, the network automatically uses another path. This provides very high reliability and performance but requires more cables and is more expensive to build.

Example. Internet backbone providers use mesh topology. Major routers in different cities and countries connect through multiple redundant links so that if one line fails, global communication continues without interruption.

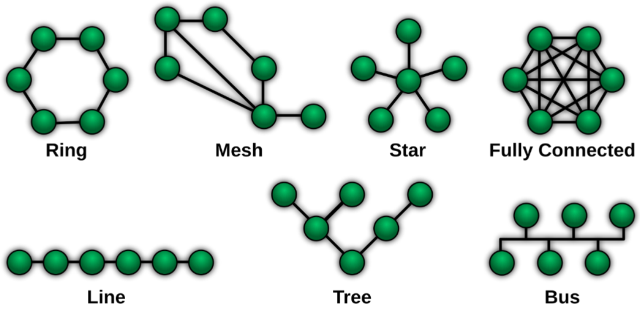

Figure 3. Diagram of different network topologies Adapted fromNetworkTopologies,Wikipedia, Wikimedia Commons,https://en.wikipedia.org/wiki/network_topologies. Licensed under CC BY 2.5

Topology	Advantages	Disadvantages
Bus	Simple to set up; requires less cable; cheap for small networks.	Entire network stops if the main cable fails; performance drops with more devices; difficult to troubleshoot.
Star	Easy to manage; failure of one device does not affect others; easy to add or remove devices; high performance.	If the central switch/hub fails, the whole network fails; requires more cables than bus or ring.
Ring	Data flows in an organized, predictable sequence; no collisions; equal access for all devices.	Failure of one device or link can break the entire loop; harder to reconfigure or add new devices.
Mesh	Very reliable because multiple paths exist; excellent fault tolerance; strong performance even with heavy traffic.	Expensive due to many cables; complex installation and maintenance.
Line	Simple linear structure; easy to extend by adding devices at the ends.	If any middle device fails, communication beyond that point stops; limited scalability.
Tree	Easy to expand; central control possible; commonly used for large networks like campuses.	Failure in the central backbone affects entire branches; more cable required; harder to configure than simple star.

Additional Material

- Computer Networks: Crash Course Computer Science #28
- Network Layers Model (Networking Basics) - Computerphile
- Hub, Switch, & Router Explained - What's the difference?
- Network Topologies (Star, Bus, Ring, Mesh, Ad hoc, Infrastructure, & Wireless Mesh Topology)
- What is Ethernet?