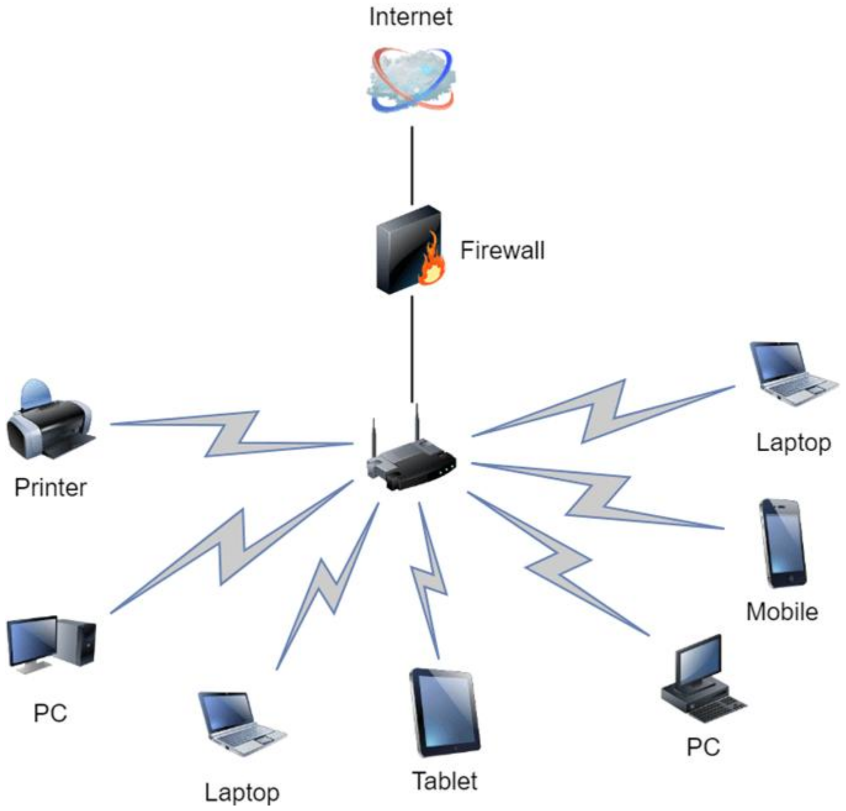
Security and Networking

What is a network?

When you buy a new computer, the first thing you'll probably try to do is connect to the Internet. To do this, you establish a connection to your **router**, which receives the data from the Internet and then forwards it to the computer. Of course that's not all: Next, you could also connect your printer, smartphone or TV to the router so that these devices are also connected to the Internet. Now you have connected **different devices to each other** via a central access point and created your own network.



In information technology, a network is defined as the connection of at least two computer systems, either by a cable or a wireless connection. The simplest network is a combination of two computers connected by a cable. This type of network is called a peer-to-peer network. There is no hierarchy in this network; both participants have equal privileges. Each computer has access to the data of the other device and can share resources such as disk space, applications or peripheral devices (printers, etc.).

Today’s networks tend to be a bit more complex and don’t just consist of two computers. Systems with more than ten participants usually use client-server networks. In these networks, a central computer (server) provides resources to the other participants in the network (clients).

A network is a **group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data and sharing resources**. These devices can be connected by physical or wireless connections

Types of networks.

Network example: your home Wi-Fi

The Wireless LAN (Wireless Local Area Network, i.e. the Wi-Fi network) in your home is a good example of a small **client-server network**. The various devices in your home are wirelessly connected to the router, which acts as a central node (server) for the household. The router itself is connected to a much larger network: the Internet.

Since the devices are connected to the router as clients, they are part of the network and can use the same resource as the server, namely the Internet. The devices can also **communicate with each other** without having to establish a direct connection to each device. For example, you can send a print job to a Wi-Fi-enabled printer without first connecting the printer to the computer using a cable.

Before the advent of modern networks, communication between different computers and devices was very complicated. Computers were connected using a LAN cable. Mechanical **switches** were used so that peripheral devices could also be shared. Due to physical limitations (cable length), the devices and computers always had to be very close to each other.

What are the tasks and advantages of a network?

The main task of a network is to provide participants with a single **platform** for **exchanging data** and sharing **resources**. This task is so important that many aspects of everyday life and the modern world would be unimaginable without networks.

Here’s a real-life example: In a typical office, every workstation has its own computer. Without a network of computers, it would be very difficult for a team to work on a project since there would be no **common place to share** or store digital documents and information, and team members would not be able to share certain applications.
In addition, many offices only have one printer or a few printers that are shared by everyone. Without a network, the IT department would have to connect every single computer to the printer, which is difficult to implement from a technical standpoint. A network elegantly solves this problem because all computers are connected to the printer via one **central node**.

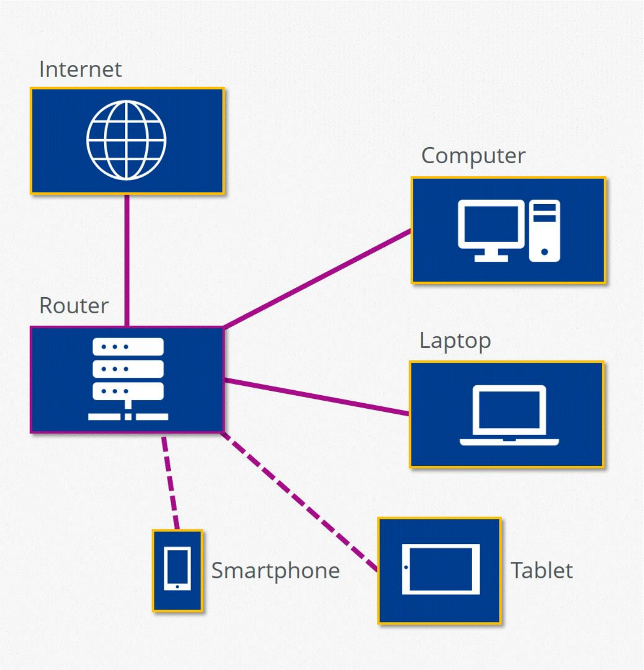
The main advantages of networks are:

- Shared use of data
- Shared use of resources
- Central control of programs and data
- Central storage and backup of data
- Shared processing power and storage capacity
- Easy management of authorizations and responsibilities

How does a network work?

In a typical client-server network there is a central node called the **server**. The server is connected to the other devices, which are called **clients**. This connection is either wireless (**Wireless LAN**) or wired (**LAN**).
In a typical home network, the router assumes the role of the server. It is connected to the Internet and provides the “Internet” resource for the other devices (computers, smartphones, etc.).

The router combines all wired and wireless devices in a local network.



Advantages of Computer Networking

Here are the fundamental benefits/pros of using Computer Networking:

- Helps you to connect with multiple computers together to send and receive information when accessing the network.
- Helps you to share printers, scanners, and email.
- Helps you to share information at very fast speed
- Electronic communication is more efficient and less expensive than without the network.

Disadvantages of Computer Networking

Here are drawbacks/ cons of using computer networks:

- Investment for hardware and software can be costly for initial set-up
- If you don't take proper security precautions like file encryption, firewalls then your data will be at risk.
- Some components of the network design may not last for many years, and it will become useless or malfunction and need to be replaced.
- Requires time for constant administration
- Frequent server failure and issues of regular cable faults

Basic network components.

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), local operating system(LOS), and the network operating system (NOS).

Switches

Switches work as a controller which connects computers, printers, and other hardware devices to a network in a campus or a building.

It allows devices on your network to communicate with each other, as well as with other networks. It helps you to share resources and reduce the costing of any organization.

Routers

Routers help you to connect with multiple networks. It enables you to share a single internet connection with multiple devices and saves money. This networking component acts as a dispatcher, which allows you to analyze data sent across a network. It automatically selects the best route for data to travel and send it on its way.

Servers

Servers are computers that hold shared programs, files, and the network operating system. Servers allow access to network resources to all the users of the network.

Clients

Clients are computer devices which access and uses the network as well as shares network resources. They are also users of the network, as they can send and receive requests from the server.

Transmission Media

Transmission media is a carrier used to interconnect computers in a network, such as coaxial cable, twisted-pair wire, and optical fiber cable. It is also known as links, channels, or lines.

Access points

Access points allow devices to connect to the wireless network without cables. A wireless network allows you to bring new devices and provides flexible support to mobile users.

Shared Data

Shared data are data which is shared between the clients such as data files, printer access programs, and email.

Network Interface Card

Network Interface card sends, receives data, and controls data flow between the computer and the network.

Local Operating System

A local OS which helps personal computers to access files, print to a local printer and uses one or more disk and CD drives which are located on the computer.

Network Operating System

The network operating system is a program which runs on computers and servers. It allows the computers to communicate via network.

Protocol

A protocol is the set of defined rules that allows two entities to communicate across the network. Some standard protocols used for this purpose are IP, TCP, UDP, FTP, etc.

Hub

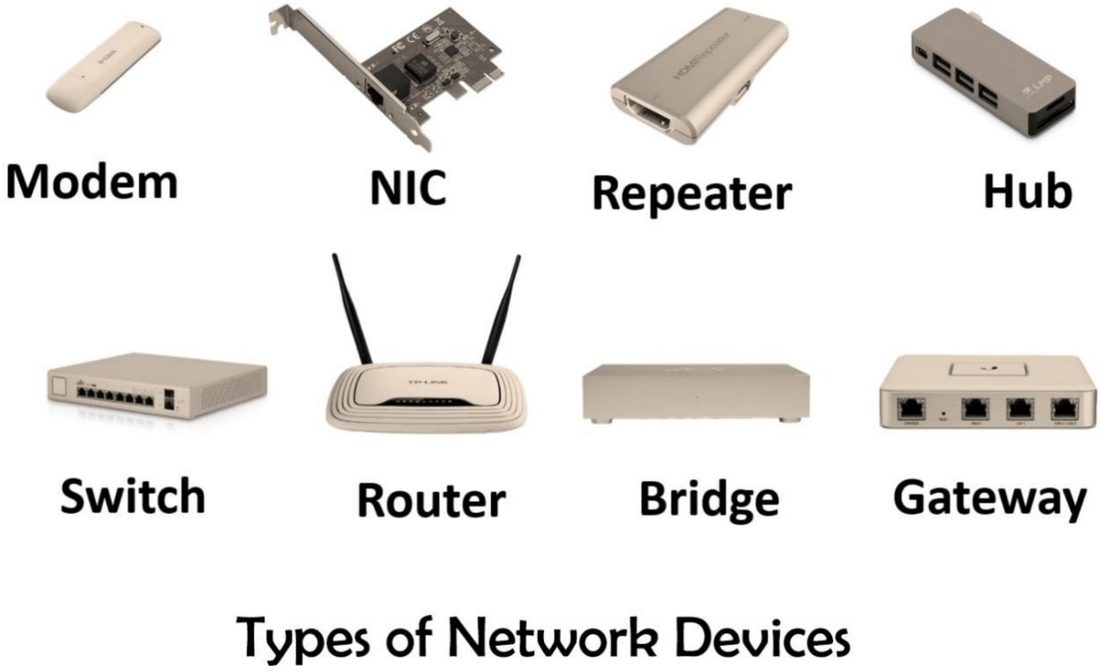
Hub is a device that splits network connection into multiple computers. It acts a distribution center so whenever a computer requests any information from a computer or from the network it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network.

LAN Cable

Local Area Network(LAN) cable is also called as Ethernet or data cable. It is used for connecting a device to the internet.

OSI

OSI stands for Open Systems Interconnection. It is a reference model which allows you to specify standards for communications.



What Is Network Security?

Network security refers to the technologies, policies, people, and procedures that defend any communication infrastructure from cyberattacks, unauthorized access, and data loss. In addition to the network itself, they also secure traffic and network-accessible assets at both the **network edge** and inside the perimeter.
Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner. Network security technologies work within several layers to protect your network as a whole against any potential threats. Networking and security include three main areas: physical, technical, and administrative.

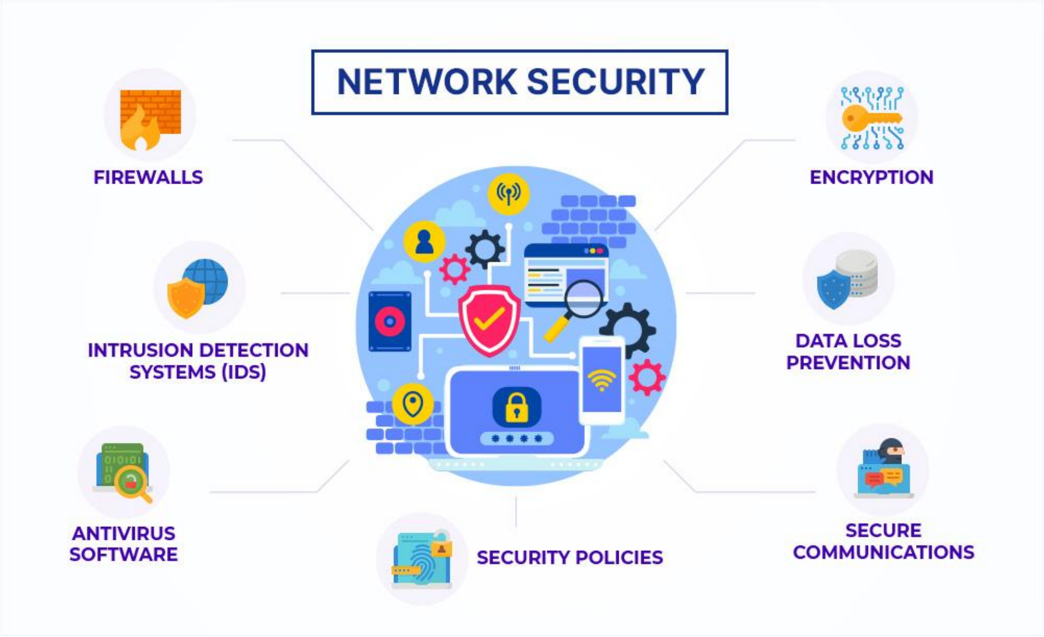
How does network security work?

Digital acceleration paved the way for business efficiencies, cost reductions, and productivity improvements. Yet, it has also led to an expanded attack surface across the growing network edge. From local area networks (LAN) and wide area networks (WAN) to the Internet of Things (IoT) and cloud computing, each new deployment results in another potential vulnerability.

Network Security Basics.

Network security basics include:

- Creating strong passwords
- Fully logging out of community computers
- Access control
- Encryption to keep sensitive data and communications secure
- Safeguarding networks and programs



Understanding network threats.

Understanding networking threats involves recognizing different types of attacks that can compromise network security. These threats can lead to data breaches, system downtime, and other serious consequences. Here are some key points:

- A network threat targets a computer network or its connected devices.
- Network threats can harm or interrupt systems, applications, and services.

- Different types of network threats have varying goals.
- Network security policies should address vulnerabilities and protect against attacks.
- The end-goal of a network attack is often to steal, modify, or remove access to valuable data

Network Troubleshooting Basics

What is Network Troubleshooting?

Network troubleshooting is a process that helps network administrators look into the network issues, run diagnosis, and resolve them before they impact the overall network performance. In this process, administrators gain better visibility into each network component and analyze connectivity issues, network security-related problems, and other key performance metrics.

Be it a simple network issue or a complex problem, it helps users diagnose the root cause of the problem, troubleshoot issues, and ensure seamless connectivity across the networks.

Why is Network Troubleshooting important?

Even a minor fault in a network component can impact the overall efficiency of a network and increase downtime. Hence, network troubleshooting is important as it helps IT managers and network administrators better understand the network performance issues in real time and improve the network's Quality of Service (QoS) for users. By timely identifying network troubleshooting problems and solutions, businesses can prevent downtime and ensure that important systems and services continue to operate. Further, quick troubleshooting reduces the cost effect of network outages and potential data loss.

In addition to trouble eshooting, network monitoring systems aid in the management of network setups and the monitoring of vital metrics such as packet data and capacity to maintain smooth company operations.

Examples of troubleshooting network include:

- Using basic network troubleshooting tools such as ping, tracert, ipconfig, netstat, nslookup, pathping, route, and PuTTY to diagnose and resolve network problems.
- Identifying and fixing network problem symptoms such as laggy video calls, slow application or network speed, buffering downloads, choppy VoIP quality, and no Internet connection.

- Addressing the four major groups of issues that can affect a network, namely network connectivity issues, bandwidth issues, connectivity device configuration issues, and IP and addressing issues.

Basic Network Troubleshooting Steps?

Network problems can impede corporate operations and impact performance which is why it is essential to find and fix network problems at an initial stage. Here are a few basic network troubleshooting steps that will help you identify and resolve network issues in real time.

Step 1: Define the Problem and Check the Physical Connections

First and foremost, collect all the information related to the network and its components from different sources at a central place.

Now, check all the network devices, cables, and routers and diagnose network issues.

Track the issue, i.e., slow internet, LAN connectivity issues, or any other issue in the configuration settings.

Define the issue and how it affects the network and users.

Teams can also try rebooting equipment like the modem, PC, and router to troubleshoot simple network problems.

Step 2: Track and Fix Duplicate IP Address Entry

To track if your device or computer is receiving a valid IP address, run “ipconfig” into the command prompt. If the IP address begins with 169, it is assigned an invalid IP address.

Step 3: Run a DNS Check

Use the “nslookup” command to find server problems. Responses such as rejected, timed out, or server failure suggest that the destination URL’s DNS server is the source of the issue. Double check the outcome of the NSlookup command by using an NS lookup tool. If the result corroborate each other, it means there is an issue with the target website.

Step 4: Check Your Malware Protection

Make that the drivers and software on your devices are the most recent versions and that the firmware on your router is up to date.

Also, no programs, applications, or settings are impacting your network performance by checking if your malware protection software has identified anything.

Step 5: Examine Logs

Analyzing logs is a highly effective method for detecting and resolving network performance disruptions and problems.

To assist in determining the underlying source of the problems, logs offer detailed information on every program, device, and application.