Computer Networking

What is Computer Networking? Computer networking refers to interconnected computing devices that can exchange data and share resources with each other. These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies.

The Importance of Computer Networking in Cybersecurity

The reason why it is so important to provide computer and network security is that if the computer or network is compromised, the information contained within it could be lost or stolen. The consequences of losing data can be devastating to an organization's ability to operate efficiently. When your computers are connected they could be open to more cyber threats. When you have one computer that has an issue it can spread to the rest. Corrupt files are not isolated when you have computer networking.

This is not a problem when you have IT support to keep your system as a whole safe. IT consulting will give you all of the information you and your employees need to keep your company data safe. Employees may exchange corrupt files when they don’t know how to recognize and avoid these incidents.

Proper training of employees will keep your company data safe while remaining accessible to promote employee productivity. Company security policies are crucial for a company of any size.  Also there are a number of ways that computer network in cybersecurity includes:

Large Storage Capacity

Improved Business Communication

Flexibility and Convenience

Improved Customer Service

Different of Networks

LAN

What is LAN? A local area network is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

WAN

What is Wan? A wide area network (also known as WAN), is a large network of information that is not tied to a single location. WANs can facilitate communication, the sharing of information and much more between devices from around the world through a WAN provider.

WANs can be vital for international businesses, but they are also essential for everyday use, as the internet is considered the largest WAN in the world. Keep reading for more information on WANs, their use, how they differ from other networks and their overall purpose for businesses and people, alike.

MAN

What is Man? A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a [local area network (LAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) but smaller than a [wide area network (WAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). MANs do not have to be in urban areas; the term "metropolitan" implies the size of the network, not the demographics of the area that it serves. Like WANs, a MAN is made up of interconnected LANs. Because MANs are smaller, they are usually more efficient than WANs, since data does not have to travel over large distances. MANs typically combine the networks of multiple organizations, instead of being managed by a single organization.

Most MANs use fiber optic cables to form connections between LANs. Often a MAN will run on "dark fiber" — formerly unused fiber optic cables that are able to carry traffic. These fiber optic cables may be leased from private-sector Internet service providers (ISP).

In some cases, this model is reversed: a city government builds and maintains a metropolitan fiber optic network, then leases dark fiber to private companies.

WLAN

What is Wlan? A wireless local-area network (WLAN) is a group of collocated computers or other devices that form a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi while reading this webpage is using a WLAN. They are used for home and small office networks that link together [laptop computers](https://en.wikipedia.org/wiki/Laptop_computer), [printers](https://en.wikipedia.org/wiki/Printer_(computing)), [smartphones](https://en.wikipedia.org/wiki/Smartphone), [Web TVs](https://en.wikipedia.org/wiki/Web_TV) and gaming devices with a [wireless router](https://en.wikipedia.org/wiki/Wireless_router), which links them to the internet. [Hotspots](https://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)) provided by routers at restaurants, coffee shops, hotels, libraries, and airports allow consumers to access the internet with portable wireless devices.

PAN

What is Pan? A personal area network (PAN) connects electronic devices within a user's immediate area. The size of a PAN ranges from a few centimeters to a few meters. One of the most common real-world examples of a PAN is the connection between a Bluetooth earpiece and a smartphone. PANs can also connect laptops, tablets, printers, keyboards, and other computerized devices. PAN network connections can either be wired or wireless. Wired connection methods include USB and FireWire; wireless connection methods include Bluetooth (the most common), Wi-Fi, IrDA, and ZigBee.

While devices within a PAN can exchange data with each other, PANs typically do not include a router and thus do not connect to the [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/) directly. A device within a PAN, however, can be connected to a [local area network (LAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) that then connects to the Internet. For instance, a desktop computer, a wireless mouse, and wireless headphones can all be connected to each other, but only the computer can connect directly to the Internet.

Different types of Network Topologies

Star Topology

What is Star Topology? Star topology is a [network topology](https://www.techopedia.com/definition/5538/network-topology) in which each network component is physically connected to a central node such as a router, hub or switch. In a star topology, the central hub acts like a server and the connecting nodes act like clients. When the central node receives a [packet](https://www.techopedia.com/definition/5380/packet) from a connecting node, it can pass the packet on to other nodes in the network. A star topology is also known as a star network. Star networks require a [point-to-point connection](https://computernetworktopology.com/point-to-point-topology/) between the central node and connecting devices. To improve communication between the devices on the network, the central node can provide signal reconditioning and amplification services.

Star topologies are often used in home networks. The benefits of a star network topology include the following:

* Limits the impact of a single point of failure. In star networks, each connecting node is isolated from other connecting nodes. If one connecting node goes down, it will not impact the performance of other connecting nodes in the network.
* Facilitates adding or removing individual components to and from a network. Star networks are usually kept small because network performance can suffer when too many devices compete for access to the central node.

Bus Topology

What is bus Topology? Bus topology is a specific kind of network topology in which all of the various devices in the network are connected to a single cable or line. In general, the term refers to how various devices are set up in a network. In bus topology, all devices are connected to a single cable (backbone), which acts as the main communication channel for the entire network. The bus is usually a coaxial cable, but it can also be made of twisted pair or fiber optic cable. Data is transmitted along the bus in both directions and all devices on the network can receive the data. However, only the device for which the data is intended can process it. This is achieved through the use of unique addresses, or MAC addresses, assigned to each device on the network.

A bus topology is relatively simple and inexpensive to implement as it requires only one cable to connect all devices. It is also easy to expand by adding more devices to the network. However, it has some disadvantages as well. For example, if the central cable (bus) fails, the entire network goes down. Additionally, as the number of devices on the network increases, the bus can become a bottleneck and slow down the network's performance.

It's also worth noting that bus topology is not suitable for large networks and it's primarily used for small networks such as home networks or small office networks.

Ring Topology

What is Ring Topology? A **ring topology** is a [network](https://www.computerhope.com/jargon/n/network.htm) configuration where device connections create a circular [data](https://www.computerhope.com/jargon/d/data.htm) path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are called a **ring network**.

In a ring network, [packets](https://www.computerhope.com/jargon/p/packet.htm) of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected.

Ring topologies may be used in either [LANs](https://www.computerhope.com/jargon/l/lan.htm) (local area networks) or [WANs](https://www.computerhope.com/jargon/w/wan.htm) (wide area networks). Depending on the [network card](https://www.computerhope.com/jargon/n/nic.htm) used in each computer of the ring topology, a [coaxial cable](https://www.computerhope.com/jargon/c/coaxialc.htm) or an [RJ-45](https://www.computerhope.com/jargon/r/rj45.htm) network cable is used to connect computers together.

Mesh Topology

What is Mesh Topology? Mesh topology is a type of network topology in which all devices in the network are interconnected. In a mesh topology, data can be transmitted by routing (sent the shortest distance) and flooding (sent to all devices). Mesh networks operate in two ways: by either *routing* the data or *flooding* the data. When you’re *routing* a message in a mesh network, it propagates along a predefined path, hopping from node to node until it reaches its destination. In order to establish these routes and ensure that the paths are available, the network needs to be continuously connected and configuring itself. In other words, it has to constantly work to find broken paths and create self-healing algorithms to build route tables. Because there’s a lot of layer two (MAC) traffic flowing on the network to establish this route, mesh networks can be less efficient than star networks (which we’ll cover in a moment).

A simpler mesh network takes a *flood* approach, where the data flows continuously throughout the network. If a module sees data with its address, it simply grabs it. This works because of the time to live, or TTL, value where messages are allowed to propagate through the mesh for only a fixed number of hops before they are removed.

Hybrid Topology

What is Hybrid Topology? A **hybrid topology** is a type of network topology that uses two or more differing network [topologies](https://www.computerhope.com/jargon/t/topology.htm). These topologies can include a mix of [bus topology](https://www.computerhope.com/jargon/b/bustopol.htm), [mesh topology](https://www.computerhope.com/jargon/m/mesh.htm), [ring topology](https://www.computerhope.com/jargon/r/ringtopo.htm), [star topology](https://www.computerhope.com/jargon/s/startopo.htm), and [tree topology](https://www.computerhope.com/jargon/t/treetopo.htm).

There are various applications using hybrid topology because of effective cost. The mechanism of hybrid topology is efficient from other fundamental mechanisms and it can also be deployed in multiple environments. So the adaptability and flexibility of the network offer the user to create, run and manage the organization. Some of the major applications of the hybrid topology are the financial and banking sector, automated industries, multi-national companies, research organizations, and many educational institutions. The combination of any two topologies such as a partial star, extended star, point-to-point networks and full mesh topology is done to develop a new hybrid topology.

The application and examples of hybrid topologies are widely spread. It is the people choose to deploy it in-home or office and it is declared as a smart option as it has a super-power set up and flexible option. It offers a compact to the small-scale industries and even to their subunits. So it is a good choice in the office or home which has multi-floor buildings and departments. There are plenty of benefits in the implementation of hybrid topology. So according to the requirements it is placed to give its maximum efficiency. But the combination of basic topology creates a complex network that impacts your budget.

Different types of Networking Devices

What is a router? A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to their intended [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and allowing multiple devices to use the same Internet connection. In order to direct packets effectively, a router uses an internal routing table — a list of paths to various network destinations. The router reads a packet's header to determine where it is going, then consults the routing table to figure out the most efficient path to that destination. It then forwards the packet to the next network in the path.

Switches

What is Switch? A switch, in the context of networking, is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). Switches keep traffic between two devices from getting in the way of your other devices on the same network. Switches allow you to control who has access to various parts of the network. Switches allow you to monitor usage.

Hubs

What is a hub? a **hub** is a basic networking [device](https://www.computerhope.com/jargon/d/device.htm) that connects multiple computers or other network devices. Unlike a network [switch](https://www.computerhope.com/jargon/s/switch.htm) or [router](https://www.computerhope.com/jargon/r/router.htm), a network hub has no [routing tables](https://www.computerhope.com/jargon/r/routing_table.htm) or intelligence on where to send information and [broadcasts](https://www.computerhope.com/jargon/b/broadcas.htm) all network data across each connection. Most hubs can detect basic network errors, such as [collisions](https://www.computerhope.com/jargon/c/collisio.htm), but having all information broadcast to multiple ports is a [security risk](https://www.computerhope.com/jargon/c/computer-security.htm) and causes [bottlenecks](https://www.computerhope.com/jargon/b/bottlene.htm). In the past, network hubs were popular because they were cheaper than a switch or router. Today, switches do not cost more than a hub and are a better solution for any network.

FireWalls

What is a Firewall? A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls are used to secure a computer network. Firewalls are [network security](https://www.simplilearn.com/network-security-interview-questions-and-answers-article) systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent [cyberattacks.](https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks)

Firewalls are used in enterprise and personal settings. They are a vital component of network security. Most operating systems have a basic built-in firewall. However, using a third-party firewall application provides better protection.

I was employed at a company named Advanced Optimistic Technologies Limited and I was given a task to performed a security audit on their network upon my findings on their network, there were a lot of problems within the network being left vulnerable these are:

Missing Patches

Known Malware

Open Ports

Weak Password

There are also other potential security vulnerability, these include:

Security Misconfiguration

Broken Authentication

Cross Site Scripting

Missing Data Encryption

Social Engineering

Unmanaged Software

Weak Passwords

Missing Authorization

Software Bugs

Unpatched Security Vulnerabilities

Data Leakage

Holder Breakdown Programs

Insider Threat

Misconfigured Firewalls

SQL Injection

Security Testing before Database Deployment

Supervisor Admin Account Privileges Bugs

Human Vulnerabilities

Unauthorized Devices

Invalidated Redirect and Forwards

These are the potential security vulnerabilities that I find that could pose a serious security risk to the company, If they are not tackle immediately it could ended up making loses millions of dollars in loss and damages. In order to tackle these security threats I put in place a plan to prevent any future cybercrime attacks. These are the things I put in place for the security network system, these are the list of measures to use to prevent these issues from recurring too often and these includes:

Use Strong Passwords

Update Regularly

Securing the Router

Proper Backing up of Data

Educating Employees

Breach Response

Installing Centralized Firewalls

Encrypted Transmission

Antivirus Software

Proactive and Continuous Auditing

And also I want to another plan in order for the proper maintenance of the security network. These are the plans that I would like the company to use for a safe and better security network these includes:

Be Organized

Develop and Enforce a Strong Password Policy

Build a Vulnerability Management

Install Endpoint and Antivirus Protection

Ensure Firewalls are Properly Configured

Set User Access Permission

Develop Data backup Solutions

These are the steps that a company must have in order to minimize any potential and future threats and any damages and losses, so once the company implement these steps into the company then the will no longer have to face issues too often.

