Computer Networking and Its Importance in Cyber Security

This project delves into the intricate relationship between computer networking and cyber security, exploring how networking protocols, architectures, and technologies are designed, implemented, and managed to protect against cyber threats.

Securing the Digital Highway: The Vital Role of Computer Networking in Cyber Security

# Introduction

Welcome to the world of modern connectivity, where computers are not just standalone machines, but interconnected entities that drive the global digital revolution. Computer networking, the backbone of our digital infrastructure, has transformed the way we communicate, collaborate, and share information. From the internet that connects continents to local area networks (LANs) in our homes and offices, networking has become an integral part of our daily lives.

In this era of unprecedented technological advancements, the importance of computer networking in cyber security cannot be overstated. Cyber threats loom large, posing a constant challenge to the security and integrity of our digital systems. As we become increasingly reliant on technology, the need to protect our networks from malicious actors and potential vulnerabilities becomes paramount.

In this college project, we will delve into the intricacies of computer networking and explore its crucial role in safeguarding against cyber threats. We will examine the fundamental concepts of networking, including protocols, architectures, and technologies, that enable seamless communication between devices. We will also analyze the various types of cyber threats, such as malware, ransomware, and phishing attacks, that can compromise network security.

Furthermore, we will explore the key principles of cyber security, including confidentiality, integrity, availability, and authentication, and how they are applied in the context of computer networking. We will also delve into the best practices for securing networks, including firewalls, virtual private networks (VPNs), intrusion detection systems (IDS), and encryption techniques.

As we uncover the interplay between computer networking and cyber security, we will highlight real-world examples of cyber-attacks that have made headlines and the devastating consequences they can inflict on individuals, organizations, and even nations. We will also analyze the evolving landscape of cyber threats and the emerging technologies that are shaping the future of computer networking and cyber security.

In conclusion, computer networking is not just about connecting devices, but also about protecting them from potential cyber threats. Understanding the principles of networking and cyber security is critical in today's digital age, where data breaches and cyber-attacks are rampant. Join us on this fascinating journey as we unravel the intricate world of computer networking and its significance in safeguarding our digital world.

## 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.

Modern-day networks deliver more than connectivity. The organizations using them are digitally transforming them, with the networks themselves being critical to this transformation and to their success.

The types of network architectures most prominent in the modern world are:

*Software-defined* (SDN): In response to new requirements in the "digital" age, network architecture is becoming more programmable, automated, and open. In software-defined networks, routing of traffic is controlled centrally through software-based mechanisms. This helps the network to react quickly to changing conditions.

*Intent-based*: Building on SDN principles, intent-based networking (IBN) not only introduces agility but also sets up a network to achieve desired objectives by automating operations extensively, analyzing its performance, pinpointing problematic areas, providing all-around security, and integrating with business processes.

*Virtualized*: The underlying physical network infrastructure can be partitioned logically, to create multiple "overlay" networks. Each of these logical networks can be tuned to meet specific security, quality-of-service (QoS), and other requirements.

*Controller-based:* Network controllers are crucial to scaling and securing networks. Controllers automate networking functions by translating business intent to device configurations, and they monitor devices continuously to help ensure performance and security. Controllers simplify operations and help organizations respond to changing business requirements.

*Multidomain integrations*: Larger enterprises may construct separate networks, also called networking domains, for their offices, WANs, and data centers. These networks communicate with one another through their controllers. Such cross-network, or multidomain, integrations generally involve exchanging relevant operating parameters to help ensure that desired business outcomes that span network domains are achieved.

## Types of Networks

1. **Personal area network**

A *personal area network* (PAN) is the smallest and simplest type of network. PANs connect devices within the range of an individual, being no larger than about 10 meters (m). Because of their operation in such limited areas of space, most are wireless and provide short-range connectivity with infrared technology.

An example of a wireless PAN is when users connect Bluetooth devices, like wireless headsets, to a smartphone or laptop. Although most PANs are wireless, wired PAN options exist, including USB.

***PAN benefits***

*Portability* - Most devices that are connected by a PAN, are small and can be easily transported.

*Affordability* - The ability to form a connection between two devices in a PAN without additional wiring is more cost efficient, compared to wired equivalents.

*Reliability* - PANs guarantee stable connectivity between devices, provided that the devices remain within the 10 m range.

Security. PANs don't directly connect to larger networks, but rather to other devices connected to larger networks. The security of a device in a PAN is contingent upon how secure the intermediary device is within the larger overall network.

*PAN use cases*

PANs are configured so individual users can connect their devices within their personal vicinity. A literal example of this is a body area network, in which a user physically wears connected devices. Small home networks with computers, printers and other wireless devices are also considered PANs.

1. **Local Area Network (LAN)**

LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

LANs use both wired and wireless connectivity options. *Wireless LAN* (WLAN) has surpassed traditional wired LAN in terms of popularity, but wired LAN remains the more secure and reliable option. Wired LANs use physical cables, like Ethernet, and switches; WLANs use wireless routers and access points, to interconnect network devices via radio frequency.

Network administrators can implement security protocols and encryption standards to secure wireless networks. Wired LANs are usually more secure because they are connected via physical cables and are harder to compromise.

1. **Metropolitan Area Network** (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

A metropolitan area network (MAN) is an interconnection of several LANs throughout a city, town or municipality. Like LANs, a MAN can use various wired or wireless connectivity options, including fiber optics, Ethernet cables, Wi-Fi or cellular.

***MAN benefits***

*Municipal coverage* - A MAN can span an entire city or town, stretching network connectivity by dozens of miles.

*Efficient networking standards* - MAN configurations typically use IEEE 802.11 networking standards to increase bandwidth capacity and frequency levels, helping to boost network performance.

*High-speed connectivity* - Fiber optic cables are the most popular form of MAN connectivity because they provide safe and fast connection data rates.

*MAN use cases*

The main purpose of a MAN is to have the same network available in several locations. In a LAN, the network is accessible in one location. In a MAN, organizations with LANs in the same municipality -- such as different office buildings -- can extend their network connectivity to those different locations.

Government entities may also configure a MAN to provide public network connectivity to users. An example of this is when municipalities offer free, public Wi-Fi to city residents using wireless MAN technology.

1. **Wide Area Network [WAN]**

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they’re miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN’s vast reach, it is typically owned and maintained by multiple administrators or the public.

A wide area network (WAN) is the most expansive type of computer network configuration. Like a MAN, a WAN is a connection of multiple LANs belonging to the same network. WANs aren't limited to city limits, and can extend to any area of the globe. For example, an organization with a corporate office in New York can connect a branch location in London in the same WAN. Users in both locations obtain access to the same data, files and applications, and can communicate with each other.

***WAN benefits***

Large area coverage. WANs provide more expansive connectivity because networks can connect from anywhere in the world.

*Improved performance.* WANs use links with dedicated bandwidth to connect LANs together. These links enhance network speeds and provide faster data transfer rates than LANs.

*Increased security*. Dedicated links also increase safety across the network because the network only connects to itself, lowering the chances for hackers to hijack a system.

*WAN use cases*

The main draw of a WAN is its facilitation of long-distance network connectivity. Organizations use WANs to connect branch offices located away from headquarters. But businesses aren't the only ones that can use WANs; an estimated two-thirds of the global population uses the internet -- the world's most popular and largest WAN -- today.

1. ***Content Delivery Network [CDN]***

A *content delivery network* (CDN) is a geographically distributed group of servers that caches content close to end users, also allowing for the quick transfer of assets needed for loading Internet content, including HTML pages, JavaScript files, stylesheets, images, and videos. The majority of modern web traffic is served through CDNs, including traffic from major sites like Facebook, Netflix, and Amazon.

Basically, CDNs are networks of globally distributed servers that deliver dynamic multimedia content -- such as interactive ads or video content -- to web-based internet users. CDNs use specialized servers that deliver bandwidth-heavy rich media content by caching it and speeding up delivery time. CDN providers deploy these digitized servers globally at a network edge, creating geographically distributed points of presence.

When a user requests data in a network, a proxy server forwards the data to the nearest CDN server, which encrypts it into a smaller, more manageable file for the network to handle, before delivering it to the origin server. An origin server provides the content to the user.

CDNs are fairly simple to configure, and organizations have many CDN vendor options from which to purchase services.

***CDN benefits***

*Fast content delivery* - The main goal of a CDN is to load rich media content on websites quickly and reduce latency between requests.

*Increased security* - When traffic travels through a CDN server, potential viruses attached to data reroute to the server, too. A CDN service mitigates these threats so it can send uncompromised data through the network.

Improved site performance. Websites managed by CDNs experience less latency and bandwidth limitation issues. Network downtime caused by traffic spikes is also a rare occurrence in websites with CDNs.

*CDN use cases*

CDNs enable the delivery of rich -- i.e., dynamic -- media. Most websites and applications incorporate some form of dynamic content, from embedded social media posts to video-streaming players. CDNs are more important than ever for accommodating the vast amount of complex data shared among millions of internet users each day.

1. ***Virtual Private Network [VPN]***

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they’re not. Through a virtual point-to-point connection, users can access a private network remotely.

A virtual private network (VPN) creates a private network overlay across an existing public network. VPNs use tunneling protocols that create encrypted connections between the network and client devices. Network traffic travels over the VPN service's secure, encrypted tunnels instead of a public network, effectively hiding a user's IP address and data from ISPs and cybersecurity hackers. The user's location appears to be wherever the VPN server exists.

***VPN benefits***

*Privacy and anonymity* - Users can browse a network without having their activity monitored by an ISP.

*Increased security* - Users must receive authentication before gaining access to a VPN. Organizations can secure company data this way by preventing unauthenticated users from accessing sensitive information.

*Geo-spoofing* - Users connected to VPNs appear to be in the same location as the server, whether in an office building or another country entirely. Users can retrieve company data or gain access to geo-blocked content outside of their country's borders.

*VPN use cases*

Studies show that VPNs have risen in popularity in recent years as internet users seek to browse the web without surveillance from their ISPs. An ISP can monitor a user's web activity, including sites visited and the types of content downloaded. VPNs hide this information from an ISP, while still providing the user with access to the network service.

VPNs also facilitate remote work for individuals working outside of office locations. User devices with VPN client software can connect to their organization's VPN server and receive access to their office's data center. Using that connection, they can access the same files and resources as employees who are physically located in the building. This functionality made VPN a vital tool during the COVID-19 pandemic, when more than a third of the U.S. labor force worked from home, per Pew Research Center.

## What are network devices, and how exactly do they function and operate?

*Network devices* are hardware components used to facilitate communication and data transfer across computer networks. They perform various functions to ensure efficient and secure network operations, facilitating the flow of data packets across the network and provide connectivity, control, and security to ensure efficient and reliable communication.

Overall, networking devices play a crucial role in creating and managing computer networks, enabling communication and data transfer between devices, and ensuring the smooth operation of modern networks.

In summary, network devices are essential components that enable communication and data transfer within and between networks.

They perform functions such as routing, switching, security, wireless connectivity, signal amplification, and network segmentation, among others, to ensure efficient and secure network operations.

## Types of Networking Devices

*Repeater -* A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors to help regain its original strength.

*Hub* – a multi-port repeater that connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through a hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

***Hub types***

*Active Hub*:- These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

*Passive Hub*:- These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

*Intelligent Hub*:- It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

***Types of Bridges***

*Transparent Bridges*:- These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes: bridge forwarding and bridge learning.

*Source Routing Bridges*:- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

***Types of Switch***

*Unmanaged switches*: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.

*Managed switches*: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.

*Smart switches*: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

*Layer 2 switches*: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.

*Layer 3 switches*: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.

*PoE switches*: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.

*Gigabit switches*: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.

*Rack-mounted switches*: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.

*Desktop switches*: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.

*Modular switches*: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

***Routers*** – A Network Layer device that routes data packets based on their IP addresses. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

## References

Ankit87, (unknown date), *Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and router)*, Geeks for Geeks, <https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/>

Stéphane Bourgeois, (2016), *11 Types of Networks Explained: VPN, LAN & More*, <https://www.belden.com/blogs/network-types>  
Deanna Darah (2022), *7 types of networks and their use cases*, <https://www.techtarget.com/searchnetworking/feature/7-types-of-networks-and-their-use-cases>

Unknown author (unknown date), *What is a Content Delivery Network (CDN)? | How do CDNs work?*, <https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>