International Journal of Innovative Research in Engineering
Volume 6, Issue 2 (March - April 2025), PP: 142-145.
https://www.doi.org/10.59256/ijire.20250602018
www.theijire.com
ISSN No: 2582-8746

An Overview on Computer Networking

Divyanshu Sharma[1], Harshita Rai[2], Mansi[3], Suhani Dubey[4], Harendra Yadav[5]
[1,2,3,4,5] *Computer Science & Engineering, Institute of Technology & Management, Gida Gorakhpur, Uttar Pradesh, India.*

How to cite this paper:
Divyanshu Sharma[1], Harshita Rai[2], Mansi[3], Suhani Dubey[4], Harendra Yadav[5], "An Overview on Computer Networking", IJIRE-V6I2-142-145.

Abstract: *Computer networks are set of connected devices that is use to sharing digital data from one device to another device. Computer networks vary in their size, topology, and organizational purpose, as well as in the physical media they employ to send signals and the communications protocols they use to manage network traffic. In this paper we discuss about introduction of computer network, network configuration, types of network, and real time challenges in computer network and computer security. There are so many protocols that are used for transmitting data from one device to another.*

Key Words: *Introduction to network, Types of network, Communication link, Application of computer network, Challenges of computer network application and security.*

I.INTRODUCTION

A computer network, sometimes known as a data network, is a communications network that facilitates data transmission between one device to another device. Applications like email and instant messaging, shared use of printers, machines, and application and storage servers, as well as access to the World Wide Web, are all supported by computer networks. Computer networks vary in their size, topology, and organizational purpose, as well as in the physical media they employ to send signals and the communications protocols they use to manage network traffic. Distributed processing is used by networks. Protocols in the communication medium are a set of rules that a group of computers follow when transferring information. A computer network is made up of computers that are wired up so they may share files or hardware, such as CD-ROMs, hard drives, and fax modems. The idea of interaction lies at the core of computer networks, allowing devices to communicate, share resources, and exchange data. Computer networks are essential to modern communication and information technologies, whether they are local networks that allow file sharing between workplace computers or the global Internet that links people worldwide.

II.TYPES OF NETWORK CONFIGURATION

There are basically two types of network configuration:

1. Peer-to-peer network
2. Client/Server network

1. Peer-to-peer network

Peer-to-peer networks are more frequently used in situations where rigorous security is not required and fewer than ten computers are involved. The term "peer" refers to the fact that all computers are on an equal footing and have the same status. It is possible for all computers on the network to share files and devices like printers and scanners that are attached to a single computer.

2. Client/Server network

Larger networks are more suited for client/server networks. Files and apps shared across a network are stored on a central computer, sometimes known as a "server". The server often performs better than a machine with ordinary performance. The other computers, known as "client" PCs, have their network access managed by the server as well. Nobody else will be able to access the server except the network administrator. Only the client PCs are accessible to others.

III.TYPES OF NETWORK

The network fits into five main groups and can be separated into geographical regions.

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)
- Wireless Network

1. **Local Area Network:** Typically, a LAN is used to a single location, like a floor, building, or other small space. In most situations, being limited allows for the use of just one transmission medium (cabling). Since all of your costs are contained inside a limited area, this technology is less expensive to deploy than WAN, and you can typically achieve faster speeds.

1.1. Some Common Physical Topologies

- **Bus Topology:** It has a backbone (means single cable) through which all the devices in the network are connected. It has plain design and requires fewer cable. But if any of cable is stumble the whole network should be collapse.

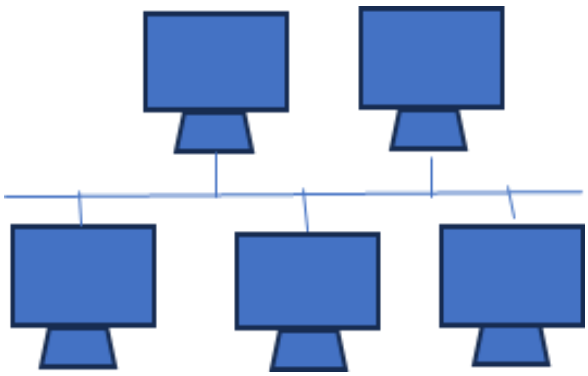

Fig: Bus Topology

- **Ring Topology:** This topology was named as ring topology because the device of network are connected in a loop or form a loop. In this the data flow is unidirectional and network control is straight forward. If any of the device connection is break, the device network may fail.

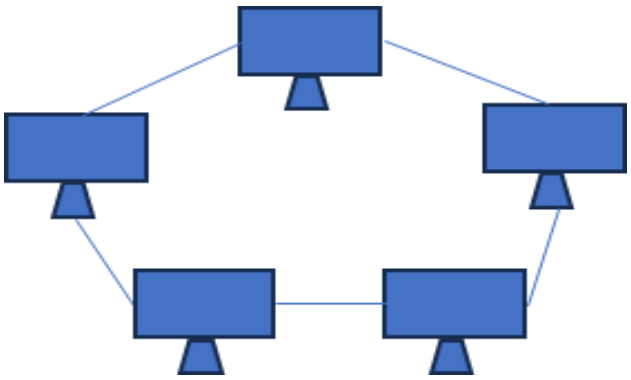

Fig: Ring Topology

- **Star Topology:** It has a core device known as switch or hub to which all other devices are connected. It has a benefit that if any of the devices in the network is fizzle the network system does not stop working. But if the primary switch is failed the whole network will go down.

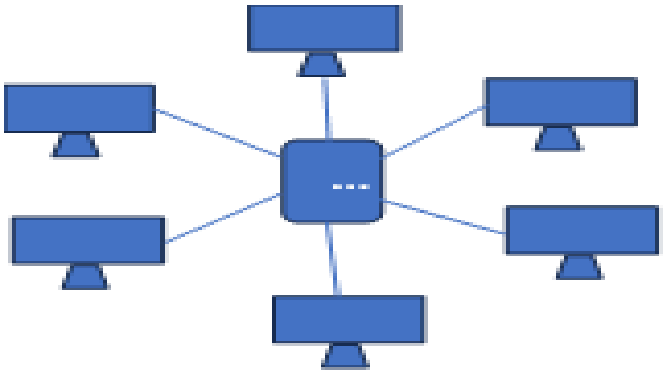

Fig: Star Topology

- **Mesh Topology:** Each device is coupled with every other device. This topology has high reliability. It means that if one of the connection is fail, then it has alternate path. It requires a larger number of cables that's why it is high priced. The number of physical link in a fully connected mesh network with n node is $\frac{n(n-1)}{2}$.

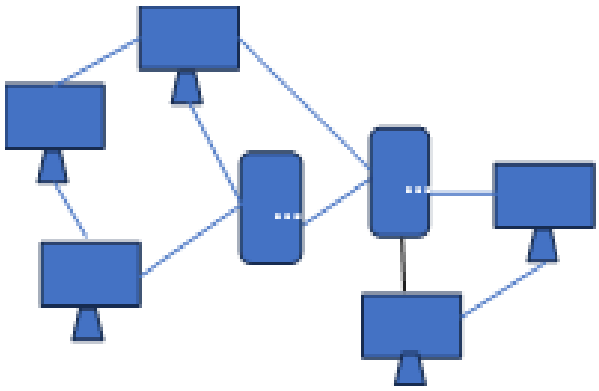

Fig: Mesh Topology

- **Tree Topology:** This is the fusion of star topology, in which there is root or chief node and all other devices are integrated like branches. It is mainly used for bigger network's and easily expandable.

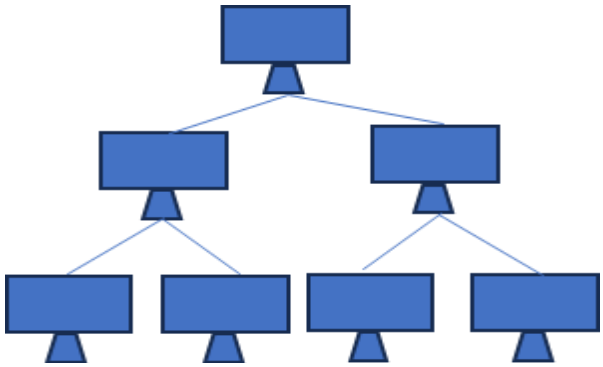

Fig: Tree Topology

2. **Wide Area Network:** An extensive geographic area, frequently a nation or continent, is covered by a wide area network. It increases a number of linked local area networks (LANs) that are geographically distant. The majority of wide area networks (WANs) have multiple telephone lines or cables connecting to a pair of routers. Two routers must interact indirectly if they want to talk to each other despite not sharing a cable. In order to indirectly interact with other computers on personal computers, we use modems.
3. **Metropolitan Area Network:** A metropolitan area network is essentially a larger LAN that often employs the same technologies. It may cover a metropolis or a collection of adjacent business headquarters, and it could be either public or private. A MAN, on the other hand, is a network that spans a city, like the backbone of a phone service provider. There are only one or two cables and no switching components in a MAN. A metropolitan area network, which frequently uses the same technology, is essentially a larger local area network (LAN). It could span a city or a group of adjacent businesses under the administration, and it could be either private or public. MANs, on the other hand, are networks that span an entire city, like the backbone of a phone service provider. A MAN lacks switching components and only has one or two cords.
4. **Personal Area Network:** PANs are small-scale computer networks that connect electronic devices, typically within a few meters of an individual. It enables communication and data sharing among gadgets such as smartphones, tablets, laptops, and wearables. Both wired and wireless PANs are possible, utilizing wires such as USB or FireWire or Bluetooth, Wi-Fi, or IrDA technologies. An information-sharing network centered on an individual is known as a personal area network. Typically wireless, these systems facilitate data transfer across various devices, including PCs, tablets, and cell phones. More recently, a specific type of network has been referred to as Personal Area Networks (PANs). PAN networks are frequently wireless and are configured on-demand or ad hoc when two or more devices need to join. Both devices belonging to the same person, such as a PDA and a laptop or cell phone, or two devices belonging to separate persons can rely on PAN networks. Since their range is often 10 meters or less, these networks are normally categorized as short-range.
5. **Wireless Network:** The market for mobile computers, such laptops and notebooks, is expanding at the highest rate. Due to the high cost of cable connections, wireless networks are required. People want to connect this computer to their office LANs so they can view the info while they're not there.

IV.COMMUNICATION LINK

Transmission media is a communication channel that carry the information from sender to receiver. Data is transmitted through electromagnetic signal. There are two types of transmission media:

1. Guided Media

- Twisted Pair Cable
- Coaxial Cable
- Optical Fiber Cable

2. Unguided Media

- Radio Wave
- Micro Wave
- Infrared Wave

Application of computer network

Computer networks serve as the backbone of modern communication and information exchange, facilitating seamless connectivity between various devices and systems across different fields. This interconnectedness enables organizations and industries to harness the full potential of computer networks, leading to significant improvements in work efficiency and quality across multiple sectors. In the realm of enterprise management, computer networks play a pivotal role in streamlining operations and enhancing decision-making processes. By integrating network technologies into organizational workflows, enterprises can achieve informatization and digitization, thereby optimizing resource allocation, enhancing communication channels, and fostering collaboration among employees. Real-time data exchange facilitated by computer networks empowers managers to make informed decisions promptly, thereby improving overall management levels and boosting business productivity.

Challenges of Network Applications

Large data transfers and a growth in multimedia content are driving up bandwidth consumption. However, performance deterioration and network congestion could result from scarce bandwidth resources. Furthermore, customers are demanding more and more real-time performance, particularly for applications where latency becomes a crucial factor, like online gaming and video conferencing. Additionally, network applications must have enough throughput to satisfy user demands in order to manage simultaneous requests and large-scale data transfers. Second, scalability presents difficulties. It is critical to maintain effective operation as user numbers and data quantities increase. Furthermore, network applications must meet basic standards for stability and high availability. Threats to them, though, include network attacks, software bugs, and hardware malfunctions. Consistent optimization and development are necessary to deliver a quick, seamless user experience and an easy to understand intuitive interface. Finally, compatibility between platforms is another important concern. Compatibility problems arise across platforms as a result of users using a range of devices, operating systems, and browser versions. It is a technological and testing challenge to guarantee a consistent user experience across all platforms.

Challenges of Computer Network Security

The first is our issue of data security. During transmission and storage, data is highly vulnerable to loss, alteration, and leakage. It can be difficult to protect data availability, confidentiality, and integrity using methods like access control and encryption. The problem of authorization and authentication comes in second. For network applications to be secure, user identities must be authenticated and secure, and user access rights must be efficiently managed. Another major problem is network assaults, such as SQL injection attacks, Distributed Denial of Service (DDoS) attacks, Cross-Site Scripting (XSS), and others. One of the most important challenges in the world of network security is quickly identifying and addressing different kinds of network threats. Furthermore, protecting privacy is difficult. Regulations and guidelines in many nations and areas must be complied with by network applications. One of the most significant obstacles is making sure network applications comply with rules and regulations while avoiding risks and penalties for breaking them.

References

1. *Russell Anthony Tantillo, Network Security through Open Source Intrusion Detection Systems, May 2012.*
2. *Bob Dickerson, Computer Networks, January 2005.*
3. *Peter L. Dordal, An Introduction to Computer Networks, Release 1.8.07, June 16, 2015.*
4. *Teodora Bakardjieva, Introduction to Computer Networking.*
5. *Antonio Carzaniga, Basic concepts in Computer Networking, September 19, 2014.*
6. *Pranab Kumar Chakravarty, Computer Networking Technologies and Application to IT Enabled Services.*
7. *Tanenbaum, Andrew S., and David Wetherall. "Computer networks." Prentice-Hall international editions (1996): I-XVII.*
8. *Carzaniga, Antonio. "Basic Concepts in Computer Networking." (2005).*
9. *Duchessi, Peter, and Indu Shobha Chengalur-Smith. "Client/server benefits, problems, best practices." Communications of the ACM 41.5 (1998): 87-94.*
10. *Kurose, James, and Keith Ross. "Computer networks: A top-down approach featuring the internet." Peorsoim Addison Wesley (2010).*
11. *White, Curt. Data communications and computer networks: A business user's approach. Cengage Learning, 2015.*
12. *Fowler, Henry J., and Will E. Leland. "Local area network characteristics, with implications for broadband network congestion management." IEEE Journal on Selected Areas in Communications 9.7 (1991): 1139-1149.*
13. *Meador, Brett. "A survey of computer network topology and analysis examples." Washington University (2008).*