IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

Computer Networking: Fundamentals, Models, and Security Considerations

Renu Narwal[1], Nitish Panwar[2], Pankaj Yadav[3]
Assistant Professor, Department of Computer Science Engineering[1]
UG students, Department of Computer Science and Information Technology[2,3]
Dronacharya College of Engineering, Gurgaon, India

Abstract: *Computer networking is an emerging and fascinating field of study. A computer network allows communication and exchange of information between two or more independent computers and other devices. Computer networking is based on the related discipline of electrical engineering, computer engineering, and computer science. Nodes and Links constitute the basic building blocks of the computer network. An equipment for data communication or equipment of data terminal that connects two or more computers such as modem, router etc. can be exemplified as a network node. Links include wires, cables or free spaces of wireless networks. Working of computer networks relies on a set of defined rules or protocols. The network structure can be composed of various patterns known as network topology. Various networking models are developed that relies on various networking layers made of different protocols. In modern times, the importance of computer networks is remarkable in almost every areas including education, entertainment, business, military, healthcare, insurance, transportation and others. With so much reliance on computer networking, it becomes important to ensure a safe and secure networking system and thus network security system was developed such includes firewall, VPNs, IDS and IPS, etc*

Keywords: Computer networking

I. INTRODUCTION

Computer networking enables communication between two or more programs running on physically distant machines. A computer network consists of a collection of computers, which are in some way connected such that they can exchange data between themselves and other computers on the network.A computer network is composed of various hardware devices that allows it to feasibly communicate, like, network interface card (NIC), routers, hubs, switch and firewall. Network protocols allows the computer communication. A communication protocol is a defined set of conventions that governs the exchange of data between a transmitter and a receiver over a communication network. In simpler words, a protocol is the standard method to transfer data and to enable communication between different devices. These variety of functions are covered by these conventions including synchronization of communication, semantics and syntax, packaging of data into messages that has to be transmitted and received at the other ends. It also includes methods that helps in identifying, controlling and constructing connections and transfer of data from one end of network to another. To ensure that the data is flexible, can be scaled to any level in the architecture and is maintained well a layered architecture is required. Various layers provides different functions and their inter operations allows flexible implementation. Each layer provides services to the higher layers. The advantages of layered protocols is passing the information from one layer to another and changes in a protocols layers prevents from affecting the other layer. A set of different layers and protocols is called as network architecture. To avoid compatibility issues all devices use standardised network model is used for data communication. The TCP/IP and OSI are such network reference models. In 1978, the International Standards Organisation (ISO) developed an Open Systems of Interconnection (OSI) model to allow the communication equipment from any source or vendor to communicate with any other in a computer network. After the development of the OSI model the communication equipment became broadly available at reasonable prices. The OSI model is made of seven different layers. In early 1970s, transmission control protocol / internet protocol (TCP/IP) was developed by a research funded by U.S.A Defence Advanced Research Projects Agency (DARPA). This model defines how automatic devices should be secured on top of the internet, and how the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

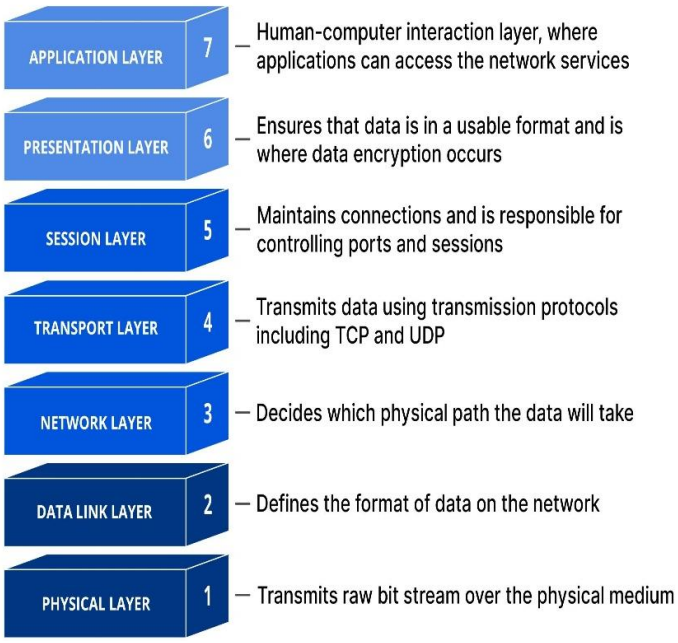
transmission of data should be carried out between them. With the increasing usage of networking in various organisations, security threats have also come into action. To provide a secure network and to ensure an authenticated access is very essential. Network security aims to provide protection to network and the various services of network from unauthorized alteration, damage or disclosure. In this review various aspects of computer networking will be discussed.

II. THE OSI (OPEN SYSTEM INTERCONNECTION) MODEL

The OSI network stands for Open System Interconnection. It is a reference model. OSI model consists of 7 layers and each layer performs a different network function. The OSI model was developed by International Organization for Standardization in the year 1984. OSI model breaks the tasks into smaller and manageable units. The OSI model is mainly divided into two layers: Upper layer and lower layer.

The top/upper layer of the OSI model handles the application related issues that are implemented in the software only. The bottom/lower layer of the OSI model handles the issues related with data transportation.

The OSI Model consists of 7 layers which are discussed below.



2.1. Application layer

- The application layer is the 7th layer of the OSI Model.
- For the sender the application layer acts as 1st layer and for receiver it acts as 7th layer of the model.
- It is responsible for providing interfaces for users to interact with application services and network services.
- This layer includes protocols that are used in emails, communication, file transfer etc.
- The application layer is used to transfer data to the presentation layer.
- The protocol data unit (PDU) for the application layer is USER DATA.

Protocols of application layer

There are many protocols of application layer, some of them are given below.

- DNS-: It stands for Domain Name Server. It uses port number 53.
- DHCP-: It stands for Dynamic Host Configuration Protocol.It uses port number 67 for servers and 68 for clients.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

- HTTP-: It stands for Hypertext Transfer Protocol. It uses port number 80.
- TELNET-: It stands for telecommunication Network.It uses port number 23.
- SSH-: It stands for Secure Shell. It uses port number 22.
- SMTP-: It stands for Simple Mail Transfer Protocol. It uses port number 25.

2.2. Presentation layer

- Presentation layer constitutes the sixth layer of OSI model.
- It is responsible for defining a standard format for data.
- The protocol data unit (PDU) for the presentation layer is formatted data.
- The presentation layer may include encryption, compression, decryption etc.

Protocols of presentation layer

- ICS(Independent Computing Architecture)
- NDR(Network Data Representation)
- AFP(Apple Filing Protocol)
- XDR(external Data Representation)

2.3. Session layer

- The 5th layer of the OSI Model is the session layer.
- It deals with the establishment, managing and termination of the session.
- The session id is used to identify the session or interaction.
- The protocol data unit for the session layer is formatted data.

Duplex-: It is a way of communication.

- There are three types of duplex
- Simple duplex-: In simple duplex the data is transmitted in only one direction.
- Half duplex-: In half duplex the data flows in both directions but not simultaneously.
- Full duplex-: In full duplex the data flows in both directions simultaneously.

2.4. Transport layer

The transport layer constitutes the 4th layer of the OSI Model.
This layer is used to insure reliable data transport across network
The protocol data unit for the transport layer is segment.
The transport layer gives two types of services.
TCP(Transmission Control Protocol)
UDP(User Datagram Protocol)

TCP	UDP
1.Transmission control protocol	1. User datagram protocol
2.Flow Control	2. No flow control
3.Secure	3. Not secure
4.Connection oriented	4. Connectionless
5.Three way handshake	5.No three way handshake
6. 20 Bytes header	6. 8 Bytes header

2.5. Network layer

- It is the 3th layer of the OSI model
- Makes best path determination

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

- This layer manages device addressing
- The protocol data unit of the network layer is packets.

Protocols of network layer are

- Internet protocol-: Its protocol number is 0.
- Internet control message protocol-: Its protocol number is 1.
- Enhance interior gateway routing protocol-: It's protocol number is 88
- Open shortest path first-: Its protocol number is 89.

2.6 Data link layer

- The data link layer is the 3rd layer of the OSI model.
- The data link layer ensures error free transfer of data frames.
- This layer provides reliable communication between two or more devices.
- The data link layer have two sub layers:
  1. Logical link control layer.
  2. Media Access control layer.

2.7. Physical layer

- It constitutes the last layer of the OSI model.
- For the sender the physical layer is the last layer of the OSI model and for the receiver it is the first layer of the OSI model.
- It is mainly used for establishing, maintaining and deactivating the physical connection.
- The main responsibility of this layer is to ensure transmission of the individual bits from one node to another node.

III. THE TCP/IP (TRANSMISSION CONTROL PROTOCOL AND THE INTERNET PROTOCOL) NETWORK MODEL

The TCP/IP network model stands for Transmission Control Protocol (TCP) and the Internet Protocol (IP). The TCP/IP is composed of conventions that allows it to act as the basic unit or language for communication on the internet. It is the most widely used and most widely available protocol suite for communication between computers on a network. All modern day computers support the TCP/IP model. Although TCP and IP are used interchangeably but there is a slight difference in the work they perform. The IP is responsible for primarily obtaining the internet address and helps in the communication joining the computers whereas the TCP delivers the data obtained to the address obtained by IP by breaking the data into smaller packets before sending them and then assembling the packets when they arrive. The TCP/IP suite consists of 4 layers: the network interface layer, the internet layer, the transport layer and the application layer. Each layer serves a specific function which has been discussed below:

3.1. The network interface layer

The network interface layer or the network access layer is responsible for incorporating the TCP/IP packets on the system medium and it also assists toaccept the TCP/IP packets off the system medium. It is in-charge of transmission of information across networks. It also directs the information between systems.

3.2. The internet layer

The Internet layer performs the task of exchanging data across networks and therefore it also provides a uniform networking interface. The main conventions of the Internet layer are internet protocol (IP), address resolution protocol (ARP), internet control message protocol (ICMP), and internet group management protocol (IGMP).

The IP is responsible for IP addressing and routing. The IP also regulates the fragmentation and the reassembly of the packets. The ARP aids in determining the location of the internet layer to the network layer. The ICMP plays role in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

giving symptomatic capacities. It also reports any mistakes committed due to unsuccessful conveyance of IP parcels. The IGMP administers the IP multicast bunches.

3.3. The transport layer

The transport layer also known as the host to host communication layer provides a channel for the communication needs of the applications. It ensures that the message are transferred error free and in the correct sequence. It consists of primarily two protocols, the UDP and the TCP. The UDP protocol offers an unreliable datagram service between one-to-one or one-to-many connections. The TCP offers a reliable datagram service between one-to-one or one-to-many connections.

3.4. The application layer

The Application layer gives the scope to applications to create data and communicate it to other applications of the same or different host thus it helps the applications to trade data between them. These applications use the services provided by the underlying layers. Various high level protocols are used in this layer including SMTP (for exchange of messages and connections), FTP (for intelligent record exchange), SSH, HTTP (to make web pages of the World Wide Web), telnet and operate.

IV. NETWORK TOPOLOGY

Network topologies define the structure of the network. Network topology designs the data flow in the network.One part of topology's definition is the physical topology which is the actual layout of the wire or media.The other part is the logical topology which defines how the media is accessed by the hosts for sending data.

Types of topology

1. Bus topology: In bus topology all the devices are connected with each other using a single backbone cable that is terminated at both ends. In this topology all the hosts are connected directly to this backbone.In bus topology coaxial cables are used. It is easy to use and inexpensive.

Advantages-

1. Bus topology are easy to use
2.Bus topology uses less cabling than mesh and star topology

2.Ring topology: A ring topology first host is connected with the last.This creates a physical ring of cable. Ring topology also uses coaxial cables. In ring topology data flow can get affected if a single device or connection fails.

Advantages

1 easy to install and reconfigure

3. Star topology: A star topology connects all cables directly to a central hub or switch. In star topology UTP straight cable is used. It is the most commonly used topology. In star topology if hub goes down then the whole system is down.

Advantages

1. Less expensive than mesh topology.

4. Mesh topology: A mesh topology is implemented to provide as much protection as possible from interruption of service. Each router has its own connection to all other routers. Although the internet has multiple path to any one location it does not adopt the full mesh topology

Advantages

1.Eliminating the traffic problem
2. Mesh topology is strong.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

5. Network Devices

Network devices are also known hardware devices. Network devices are essential parts of network and these physical devices allow the interaction and communication of hardware. Some of network devices are explain below-:

1. Network interface card (NIC)

NIC are hardware components installed in computers. Every NIC has its own MAC address that identifies the pc on the address. This is a peripheral cards that are used to attach to a pc in order to connect to a network.

2. Hubs

Hubs are those devices which connect multiple devices in a network. Hubs are brainless devices. Hubs are non-manageable devices. Hubs operate on the physical layer of the osi model.Hubs works on the same network.

3. Switch

Switches are those devices that connect devices within a single network. Switches are intelligent devices. Switch learns the media access control address. Switch also works on the same network. Switches are manageable devices. The switches operate on the data link layer of the OSI model.

4. Router

Routers are those devices that are used for connecting two different devices. Routers use a routing table to find the best path for data packets. It is used for long distance connectivity. Routers are manageable devices. Routers are operated on the network layer of the osi model.

5. Firewall

Firewall are devices that are used to monitor and control incoming and outgoing network traffic. They help to protect networks from unauthorized access, malware and other cyber threads.

VI. COMPUTER NETWORK SECURITY

Computer network security is the most important thing in today's digital environment. As cyber threats continue to grow, from malware and phishing attacks to data breaches and ransomware, organizations need to take effective security measures to protect their sensitive data and control the integrity of their networks. Cybersecurity includes a variety of technologies, processes, and practices designed to protect the confidentiality, integrity, and availability of information transmitted over computer networks. All organizations that rely on cyber systems, from small businesses to large enterprises, need to adopt a security approach that reduces risk and strengthens cyber defences.

Encryption plays an important role in protecting data transfers between data transfers. It ensures that messages remain anonymous and protected from unauthorized access, even if intercepted by criminals. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are widely used encryption methods that create secure connections between clients and servers, encrypting data in transit against eavesdropping and tampering. Encryption can also be used to store data on the server, database, or endpoint to prevent unauthorized access in the event of a security breach.

A firewall is an important line of network security protection that acts as a barrier between the organization's network and external threats from the Internet. Security devices in this environment control traffic in and out of the network and enforce security policies to block malicious traffic while allowing traffic to flow. Firewalls can be implemented as hardware, software programs or cloud services, allowing easy deployment to meet the specific needs of different environments.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential components of a network security infrastructure that monitors network traffic for signs of malicious activity or activity. IDS analyses network packets and logs to identify potential security threats, while IPS applies instant defence to block or mitigate threats by filtering or blocking bad traffic. By continuously monitoring network activity and detecting suspicious signs of unauthorized access or malicious behaviour, IDS and IPS can reduce the impact of cyberattacks by helping organizations in investigating and responding to such attacks in minimal time.

Virtual Private Networks (VPNs) provide secure security for users connecting to your organization's network from other locations, such as home offices or a public Wi-Fi hotspot. By encrypting communications and creating secure tunnels between untrusted parties, VPNs allow users to securely access corporate services while protecting confidential information, knowledge, and integrity. VPNs are widely used by remote workers, remote workers, and mobile workers

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

to access corporate intranets, data servers, and applications from anywhere; thus reducing security risks associated with remote connections.

VII. NETWORK PERFORMANCE AND MANAGEMENT

Network performance and management are crucial aspects of maintaining an efficient and reliable computer network. Effective management ensures that the network operates smoothly, meets performance requirements, and remains secure. Some key components of network performance and management are -:

1. **Monitoring-:** Network monitoring is used for continuously observing network traffic, performance metrics and device status. Monitoring tools track bandwidth usage, latency, packet loss etc.
2. **Performance Optimization-:** The aim of optimizing techniques is to improve network performance and efficiency. This may involve optimizing router algorithm, Quality of services or implementing a caching mechanism to reduce latency.
3. **Bandwidth Management-:** Bandwidth management involves allocating network resources effectively to ensure that critical applications get sufficient bandwidth. Traffic shaping, prioritization and traffic policing are used to manage bandwidth usage and prevent network congestion.Bandwidth monitoring helps identify bandwidth intensive applications and users.
4. **Fault Management-:**The aim of Fault management is to detect, isolate, and resolve network faults and failures in a timely manner. Fault tolerance, redundancy, and rapid fault recovery help minimize downtime and service disruptions; these are the techniques used in fault management .Network monitoring tools generate alerts and notifications when anomalies or failures occur, allowing administrators to take corrective action promptly.

VIII. CONCLUSION

computer networking is a complex and dynamic field that plays a pivotal role in enabling communication and data exchange across various sectors. From the foundational structure of nodes and links to the sophisticated models of OSI and TCP/IP, computer networks provide the framework for seamless data transmission and connectivity. The diverse network topologies and devices such as switches, routers, and firewalls contribute to the robust functionality and efficiency of modern networks. However, as reliance on computer networking continues to grow, so do the risks and challenges associated with network security. It is imperative for organizations and individuals to implement effective security measures, such as firewalls, VPNs, and encryption protocols, to safeguard networks from potential threats and unauthorized access.

The evolution of computer networking has undoubtedly transformed the way we communicate and access information, making it an indispensable part of contemporary life. As technology advances, the continuous development of networking systems and security solutions will be crucial to ensuring reliable and secure connectivity for all users. Through ongoing research and innovation, the field of computer networking will continue to shape and enhance the digital landscape for future generations.

REFERENCES

[1]. "A Review Paper on Networking Topologies", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 9, page no.324-330, September 2018, Available :http://www.jetir.org/papers/JETIRFH06055.pdf

[2]. A Comparison of OSI Model vs. TCP/IP Model http://www.inetdaemon.com/tutorials/basic_concepts/network_models/comparison.shtml Last Updated: Saturday, 15-Feb-2014 12:46:31 MST | By InetDaemon.

[3]. Alade A. A Survey of Computer Network Communication Protocols and Reference Models." American Journal of Engineering Research (AJER), vol. 6, no. 11, 2017, pp. 174- 180.

[4]. Antonio Carzaniga, Basic concepts in Computer Networking, September 19, 2014.

[5]. Balasubramaniam, Deepa. (2015). Computer Networking: A Survey. International Journal of Trend in Research and Development,. 2.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

[6]. H. Zimmermann, OSI reference model – the ISO model of architecture for open systems interconnection, IEEE Transactions on Communications, 28(4), 1980.

[7]. Kirandeep Kaur, Manmeet Kaur, Komalpreet Kaur, & Aanchal Madaan. (2023). A Comparative Study of OSI and TCP/ IP Models. *International Journal of Engineering and Management Research*, *13*(2), 127–135. https://doi.org/10.31033/ijemr.13.2.20.

[8]. Onyia, Cyprain & Nnamani, Kelvin & Alagbu, Ekene & Ezeagwu, Christopher. (2021). Comparative Analysis of OSI and TCP/IP Models in Network Communication. Quest. 7. 08-14. 10.35629/9795-07060814.

[9]. P. Ravali, A Comparative Evaluation of OSI and TCP/IP Models. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 4 (7), 2015.p:514-521.

[10]. P.E. Green, An introduction to network architectures and protocols, IBM Syst J. 18(2), 1979, 202-222.

[11]. Pandey, Shailja. (2011). MODERN NETWORK SECURITY: ISSUES AND CHALLENGES. International Journal of Engineering Science and Technology. 3.

[12]. Stewart, K., Adams, A. & Reid, A. (2008). Designing and supporting computer networks. CCNA Discovery Learning Guide, Cisco Press, USA.