An Internship Report on

Networking Virtual Internship

Submitted in partial fulfilment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

in

Computer Science and Engineering (Data Science)

by

S . SANDHYA

224G1A3284

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (DATA SCIENCE)

SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY (AUTONOMOUS)

(Affiliated to JNTUA, accredited by NAAC with 'A' Grade, Approved by AICTE, New Delhi & Accredited by NBA (EEE, ECE & CSE)) Rotarypuram village, B K Samudram Mandal, Ananthapuramu-515701.

2024 – 2025

SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY (AUTONOMOUS)

(Affiliated to JNTUA, accredited by NAAC with 'A' Grade, Approved by AICTE, New Delhi & Accredited by NBA (EEE, ECE & CSE))

Rotarypuram village, B K Samudram Mandal, Ananthapuramu-515701.

Department of Computer Science & Engineering (Data Science)

Certificate

This is to certify that the internship report entitled "Networking Virtual Internship" is the bonafide work carried out by **S. Sandhya** bearing Roll Number 224G1A3284 in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering (Data Science)** for 10 weeks from July 2024 to September 2024.

Internship Coordinator

Dr. G. Hemanth Kumar Yadav, M. Tech., Ph.D.,
Assistant Professor

Head of the Department

Dr. P. Chitralingappa, M. Tech., Ph.D.,
Associate Professor & HOD of CSD

Date:

Place: Ananthapuramu

EXTERNAL EXAMINER

PREFACE

I did this Internship from technology, June 2023 to September 2023 with the help of this are compared with real workflows theory, which leads to better transparency as well as insight into the processes. This is necessary because the reality of the processes usually does not correspond to the ideas of the process participants and the work steps in the reality are usually much more complex. This internship project is a part of III - Year B. Tech program which is conducted at Srinivasa Ramanujan Institute of Technology - Ananthapuramu.

AICTE has prepared a model curriculum with the help of prominent Academicians of the country so the country may produce competent employable graduates as per the needs of the industries. One of the best academicians in the India is Eduskills as for the AICTE curriculum they provided. The process mining was done in the platform of Celonis website, it helps companies achieve process excellence through its platform by eliminating operational friction with their Intelligent Business Cloud platform.

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, whose constant guidance and encouragement crowned our efforts with success. It is a pleasant aspect that I have now the opportunity to express my gratitude for all of them.

It is with immense pleasure that I would like to express my indebted gratitude to my internship coordinator **Dr. G. Hemanth Kumar Yadav, Assistant Professor**, who has supported me a lot and encouraged me in every step of the internship work. I thank him for the stimulating support, constant encouragement and constructive criticism which have made possible to bring out this internship work.

I am very much thankful **to Dr. P. Chitralingappa, Associate Professor & HOD, Computer Science and Engineering (Data Science),** for his kind support and for providing necessary facilities to carry out the work.

I wish to convey my special thanks to **Dr. G. Balakrishna, Principal of Srinivasa Ramanujan Institute of Technology** for giving the required information in doing my internship. Not to forget, I thank all other faculty and non-teaching staff, and my friends who had directly or indirectly helped and supported me in completing my internship in time.

I also express our sincere thanks to the Management for providing excellent facilities and support.

Finally, I wish to convey my gratitude to my family who fostered all the requirements and facilities that I need.

S. SANDHYA

(224G1A3284)

INDEX

Contents	Page No.
List of Figures	vi
List of Abbreviations	vii
Chapter 1 Introduction to Zscaler Networking	1-4
Chapter 2 Technology	5-7
Chapter 3 Applications	8-12
Chapter 4 Modules Explanation	13-24
Chapter 5 Real-time Examples	25-27
Chapter 6 Learning outcomes of the Internship:	28
Conclusion	29
Internship certificate	30
References	31

LIST OF FIGURES

Fig. No.	Description	Page No.
1.2	Networking Architecture	1
1.2.1	Networking Cables	4
4.1	Networking Protocol	13
4.2	The Seven Layers	15
4.3	IP Addressing & Subnetting	21
4.4	Tunneling	35

LIST OF ABBREVIATIONS

ACK – Acknowledgment

ARPANET – Advanced Research Project Agency Network

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DSAP – Destination Service Access Point

FIN – Finish

FTP – File Transfer Protocol

GRE – Generic Routing Encapsulation

HDLC – High-level Data Link Control

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

ICMP – Internet Control Message Protocol

IETF – Internet Engineering Task Force

CHAPTER - 1

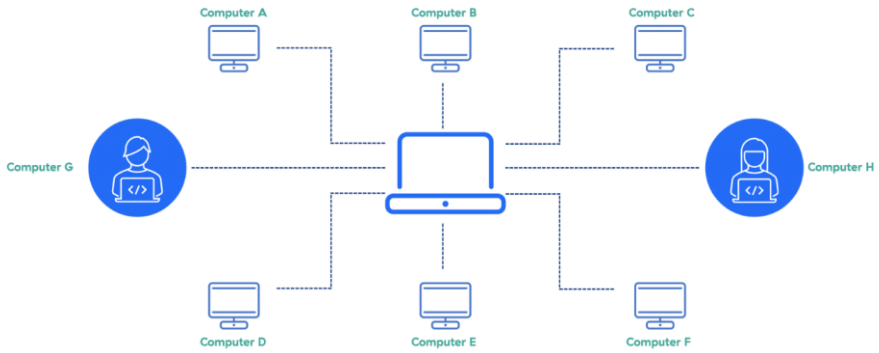
INTRODUCTION TO NETWORKING

In this course, you will learn the concepts and general principles of computer networking, including architecture, components, cables, and types of computer networks. You will learn about network protocols, data communications, and the OSI model. You will also discover the concept of IP addressing, subnetting, and tunnelling.

1.1 What is Computer Networking?

Computer networks refer to interconnected computing nodes that can exchange data and share resources.

Networks enhance the computer's ability to exchange, preserve, and protect information. Computers connected over a network can make the information exchange easier and faster.



1.2Network Architecture

Network architecture is a framework that defines structural and logical grouping of hardware, software, and applications.

The two common types of network architecture are**:**

- Peer-to-peer
- Client and Server

Peer-to-peer:

A peer-to-peer network is a type of network in which a group of computers are interconnected, with each node having equal permissions and responsibilities for processing data.

Client and Server:

In a client and server network, server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services.

Types of Networks:

Network types can be defined based on the network size, capabilities, and geographical regions they cover.

A computer network is mainly of five types:

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

Based on organizational intent, networks can be classified as:

- **Extranet**
- **Intranet**
- **Internet**
- **Ethernet**.

Network Components:

A network component is a hardware or software that plays a specific role in connecting devices and ensuring packet flow within a network.

Some of the network components are:

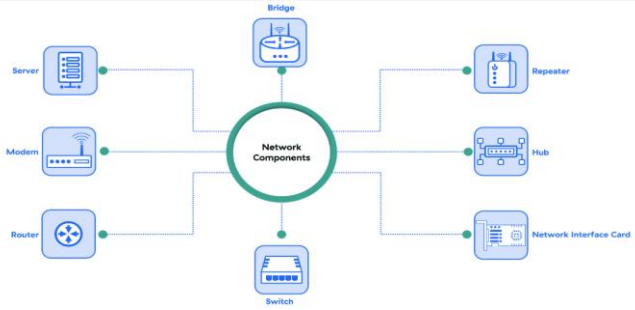


Fig: Network Components

Network Cabling:

A network cable is used to connect various devices (such as computers, mobile phones, and routers) to a network that allows a user to have internet access. Cables are the medium through which information moves from one network device to another.

Types of Network Cable

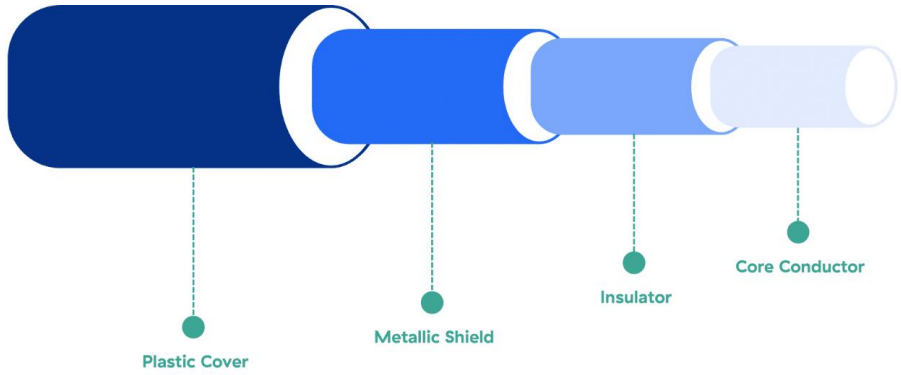
1.Coaxial cables:

The Coaxial cable got its name by the word “coax”. It is a type of network cable that has an inner conductor surrounded by a tubular insulating layer that is covered by a tubular conducting shield. The inner conductor and the outer shield share a geometric axis. Many Coaxial cables have an insulating outer sheath or jacket.

Coaxial cables are very difficult to install and maintain because these cables are too big to carry and replace.

These cables are used as a transmission line for Radio Frequency (RF) signals.

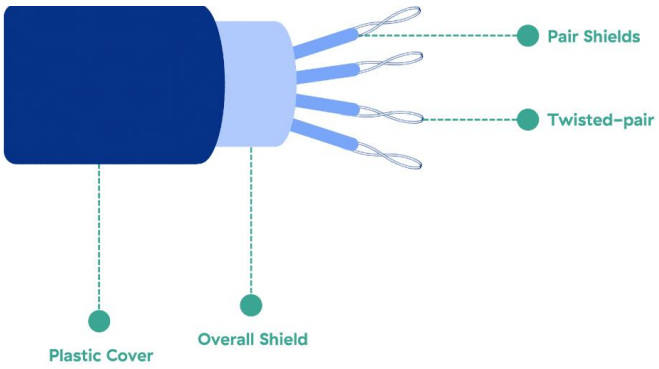
Coaxial cables are also used for dish TV where the setup box and the television are connected using the Coaxial cable only.



Twisted Pair cables:

A Twisted Pair cable is a type of wiring in which two conductors (usually copper) of a single circuit are twisted together. These cables are suitable for transferring balanced differential signals. Twisting two insulated copper wires together at a certain density helps to reduce crosstalk or electromagnetic induction between pairs of wires.

Twisted Pair cabling is often used in data networks for short and medium-length connections because of its relatively lower costs compared to optical fiber and Coaxial cable.



Fiber Optic cables:

A fiber optic cable consists of a central glass core surrounded by several layers of protective materials usually made of PVC or Teflon. It transmits light rather than electronic signals which helps to eliminate the problem of electrical interference.

Fiber optics can transmit signals over a very long distance as compared to Twisted Pairs or Coaxial cables. These cables can carry information at a great speed from 10 Mbps up to 100 Gbps or higher.

There are two types of fiberoptic cables – **multimode** and **single-mode**.

- Multimode optical fiber can carry multiple light rays (modes) at the same time as it has varying optical properties at the core.
- Single-mode fiber has a much smaller core size (9 microns). It has a single light path and can travel much longer distances, but it is more expensive.

CHAPTER - 2

TECHNOLOGY

Zscaler is a cloud-based security company that provides a variety of networking and security solutions to protect users and data in a zero-trust environment. The technology used in Zscaler's networking primarily focuses on secure access to applications, data, and the internet while eliminating the need for traditional hardware-based network security appliances. Below are the key technologies and components used by Zscaler:

1. Zscaler Zero Trust Exchange

This is Zscaler's core platform, which uses the following technologies to deliver secure access:

- Zero Trust Network Access (ZTNA): Zscaler provides secure access to internal applications without exposing them to the internet, ensuring users are authenticated and authorized before access.
- Application Segmentation: By segmenting applications at the user level, Zscaler reduces the attack surface by preventing lateral movement across the network.

2. Zscaler Cloud Security

Zscaler delivers security through a cloud-native architecture. The technologies include:

- Secure Web Gateway (SWG): Protects users by enforcing security policies and filtering web traffic, ensuring that malicious content, such as malware, is blocked.
- Cloud Firewall: Functions as a cloud-based firewall, offering next-generation firewall (NGFW) capabilities like URL filtering, bandwidth control, and threat detection.
- Cloud Sandbox: A cloud-based threat protection service that inspects suspicious content in a sandbox environment to detect and prevent malware.
- Data Loss Prevention (DLP): Prevents unauthorized sharing or leakage of sensitive data through monitoring and blocking such activities across the network.

3. Zscaler Private Access (ZPA)

ZPA is Zscaler's ZTNA solution that provides secure access to private applications, regardless of the user’s location. Technologies within ZPA include:

- Micro-segmentation: Limits user access to only the applications they are authorized for, reducing risks.
- App Connector: Installed in a company's environment, this component connects users to private applications without exposing the applications directly to the internet.

4. Zscaler Internet Access (ZIA)

ZIA acts as a secure gateway to the internet, routing traffic through Zscaler's cloud infrastructure where it can be inspected and filtered. It includes:

- SSL Inspection: Scans encrypted traffic (SSL/TLS) to ensure threats aren't hidden in secure connections.
- DNS Security: Prevents malicious DNS requests and protects against DNS-based attacks like phishing and command-and-control traffic.
- Advanced Threat Protection: Detects and blocks advanced persistent threats (APTs) and zero-day exploits.

5. Artificial Intelligence and Machine Learning

Zscaler leverages AI and ML to enhance its security capabilities, including:

- Threat Intelligence: Continuously monitors the internet for emerging threats using AI-driven threat detection.
- Behavioral Analysis: Uses machine learning algorithms to detect anomalies in user behavior and application traffic.

6. Cloud-Native Platform

Zscaler operates entirely on a cloud-native platform that offers global scalability. It doesn't require customers to maintain hardware appliances, which simplifies the network architecture.

- Edge Cloud Infrastructure: Zscaler has over 150 data centers worldwide to ensure low latency and reliable connectivity.
- Elastic Scalability: The cloud-based nature allows Zscaler to scale up or down based on traffic demands without any additional on-premise hardware.

7. Identity and Access Management (IAM) Integration

Zscaler integrates with identity providers (IdPs) like Okta, Azure AD, or Ping Identity, to enforce user authentication and enable Single Sign-On (SSO) for seamless user experience.

- Multi-Factor Authentication (MFA): Enforces strong authentication measures to ensure users are who they claim to be.

8. Software-Defined Perimeter (SDP)

Zscaler uses SDP technology to hide internal applications from public view while ensuring that authenticated users can securely connect to these apps. It reduces the risk of attack on exposed public IP addresses.

9. API Integration and Automation

Zscaler provides APIs for automation and integration with other security and networking tools like Security Information and Event Management (SIEM) systems, and orchestration platforms like ServiceNow.

10. VPN Replacement

Zscaler enables remote users to securely connect to private applications and cloud services without using a VPN. Instead of a traditional VPN, Zscaler uses:

- Policy-based Access Control: Dynamically routes user traffic based on predefined policies, ensuring users connect only to the applications they need access to.

These technologies together create a comprehensive, cloud-based security model that focuses on a zero-trust approach, minimizing reliance on physical infrastructure and securing the modern digital enterprise**.**

CHAPTER - 3

APPLICATIONS

Zscaler's networking solutions are widely used across industries to enhance security, enable secure remote access, and simplify the IT infrastructure of organizations. Its cloud-native approach, based on Zero Trust security principles, provides several key applications that support modern digital businesses. Here are some of the primary applications of Zscaler networking:

1. Secure Remote Work (Work-from-Anywhere)

Zscaler enables secure access for remote and distributed workforces, offering an efficient alternative to traditional VPNs. Its Zero Trust Network Access (ZTNA) model ensures that employees can securely access internal and cloud-based applications from any location without compromising security.

- **Zscaler Private Access (ZPA)**: Securely connects remote users to internal applications without exposing them to the public internet.
- **Zscaler Internet Access (ZIA)**: Protects users from threats on the public internet, offering security services like web filtering, malware detection, and SSL inspection for encrypted traffic.
- **Application Segmentation**: Reduces lateral movement threats by limiting user access to only the applications they are authorized to use.

2. Secure Internet Access for Branch Offices

Zscaler's cloud-based platform allows companies to provide secure internet access to their branch offices and retail locations without relying on traditional on-premise security appliances like firewalls and proxy servers.

- **Cloud Firewall and Secure Web Gateway**: These services filter and inspect traffic for malicious content, applying consistent security policies across distributed offices and users.
- **DNS Security**: Protects branch offices from DNS-based threats such as malware, phishing, and command-and-control communication.
- **SD-WAN Integration**: Zscaler integrates with SD-WAN solutions to route traffic intelligently, providing secure and optimized access to the internet and cloud applications.

3. Cloud Application Security

Zscaler supports secure access to cloud applications like Office 365, Salesforce, and other SaaS platforms, ensuring that data remains protected while enabling high-performance connectivity.

- **Cloud Security Posture Management (CSPM)**: Helps monitor and enforce security configurations of cloud infrastructure services like AWS, Azure, and Google Cloud Platform.
- **Data Loss Prevention (DLP)**: Inspects data traffic to and from cloud applications to prevent sensitive data from being leaked or compromised.
- **Advanced Threat Protection**: Protects users from malicious files and links in cloud apps by scanning traffic and detecting malware.

4. Zero Trust Network Access (ZTNA)

Zscaler's Zero Trust approach ensures that access to internal applications is granted only after user authentication and policy enforcement, making it ideal for organizations that want to replace traditional perimeter-based security models.

- **Micro-segmentation**: Users are granted access only to the applications they need, rather than the entire network, reducing the attack surface.
- **ZPA for Hybrid Cloud Environments**: Zscaler allows secure access to applications hosted in private data centers, public clouds, or hybrid environments without needing network-wide VPN access.
- **No VPN Requirement**: Users can securely access applications without using cumbersome VPNs, reducing latency and improving user experience.

5. Secure Digital Transformation

As organizations migrate from on-premise data centers to cloud environments, Zscaler helps them maintain secure, scalable, and flexible networking:

- **Elimination of MPLS**: By routing traffic directly through Zscaler's cloud platform instead of using MPLS networks, businesses can reduce costs while improving performance.

- **Application Access without Exposing IPs**: Zscaler ensures that internal applications are never exposed to the public internet, protecting them from potential attacks.

6. Protection Against Advanced Threats

Zscaler leverages AI, machine learning, and real-time threat intelligence to protect against sophisticated cyber threats, including zero-day exploits, ransomware, and other malicious activities.

- **SSL Traffic Inspection**: Zscaler inspects encrypted (SSL/TLS) traffic, ensuring that malware or hidden threats are not bypassing traditional security mechanisms.

- **Advanced Persistent Threat (APT) Protection**: Zscaler's cloud sandbox technology analyzes suspicious files and traffic in real time to detect and block advanced malware and threats.

7. IoT and OT Security

With the increasing use of IoT and Operational Technology (OT) devices, Zscaler offers enhanced protection for IoT environments by securing device-to-cloud communication:

- **Micro-segmentation for IoT Devices**: Zscaler's ZTNA ensures that IoT devices have restricted access, minimizing the risk of lateral movement or cyberattacks on critical systems.

- **Threat Detection for IoT Traffic**: Zscaler's platform monitors and inspects IoT traffic to detect and block potential threats in real-time.

8. Compliance and Data Governance

Zscaler helps businesses comply with various data protection regulations like GDPR, HIPAA, and CCPA by providing security tools that help protect sensitive information and enforce access control policies.

- **Data Loss Prevention (DLP)**: Monitors and controls the flow of sensitive data across the network, ensuring compliance with data protection laws.

- **Policy Enforcement**: Ensures that users and traffic comply with regulatory requirements, applying policies consistently across all network traffic.

9. Reduced Infrastructure Complexity and Costs

By adopting a cloud-first networking model, Zscaler eliminates the need for costly on-premises security appliances (like firewalls and VPNs), reducing IT complexity and operational costs.

- **Cloud-based Architecture**: Centralized management and a globally distributed cloud infrastructure mean that enterprises don't need to invest in physical hardware.

- **Simplified Management**: Centralized policies, automated updates, and the ability to quickly scale resources up or down simplify the management of security and networking infrastructure.

10. Business Continuity and Disaster Recovery

Zscaler's cloud-based model supports business continuity by allowing employees to securely access corporate resources from any location during unforeseen events, such as natural disasters or pandemics.

- **Remote Access for Critical Applications**: Zscaler ensures that users can always connect to critical applications securely, no matter their location.

- **Global Cloud Presence**: With data centers worldwide, Zscaler provides reliable and low-latency access for users, even if certain locations or resources are affected by outages.

11. Security for Mergers and Acquisitions

Zscaler facilitates secure networking and integration of IT infrastructure during mergers and acquisitions by providing consistent security across different environments.

- **Quick Integration of Networks**: Zscaler's platform allows newly acquired companies to quickly integrate into the existing IT infrastructure without complex network reconfiguration.

- **Unified Security Policies**: Centralized management of security policies ensures that new entities or users are subject to the same security standards as the rest of the organization.

12. Securing DevOps and CI/CD Pipelines

For organizations leveraging cloud-based development environments and continuous integration/continuous delivery (CI/CD) pipelines, Zscaler offers protection for the development lifecycle:

- **Secure Access to DevOps Tools**: Zscaler ensures that only authorized users can access development tools, code repositories, and cloud environments.

- **Protection Against Supply Chain Attacks**: Zscaler helps secure development environments and mitigate risks associated with compromised third-party software.

These applications demonstrate how Zscaler's solutions fit into a variety of use cases, providing security, efficiency, and scalability for modern digital enterprises. By focusing on a zero-trust architecture and cloud-based services, Zscaler offers organizations the ability to secure their networks, users, and data in a flexible and cost-effective manner.

CHAPTER - 4

MODULES

4.1 Network Protocol and Communications

4.1.1 Network Protocol

A Network Protocol is a set of rules that governs the formatting and processing of data communication between different devices in the network.

There are three types of network protocols:

- Network Communication Protocol
- Network Management protocol
- Network Security Protocol

1.Network Communication Protocol

Network Communication Protocol governs data transfer across networks, handling syntax, authentication, semantics, and error detection for analog and digital communications.

Some key network communication protocols include:

- Hypertext Transfer Protocol (HTTP)
- Transmission Control Protocol (TCP)
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- File Transfer Protocol (FTP)

2. Network Management Protocol

Network Management Protocol describes the procedures and policies used in monitoring, maintaining, and managing the computer network.

The most widely used network management protocols are:

- Internet Control Message Protocol (ICMP)
- Simple Network Management Protocol (SNMP
- Teletype Network (TELNET)

3. Network Security Protocol

Network Security Protocol ensures the security and integrity of data in transit over a network connection. These protocols make sure that no unauthorized devices, users, or services can access the network data.

Primarily, these protocols depend on encryption to secure data.

Some common network security protocols are:

- Secure File Transfer Protocol (SFTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Secure Socket Layer (SSL)

4.1.2 Data Communications

Data Communication is the process of transmitting and receiving data between two or more devices over a network. It converts the data into signals that can be transmitted and then decodes those signals at the receiving end.

You have learned what data communication is. Now, you will cover other topics related to the data communication including Communication Model, Encoding and Decoding Communication, and Network Packet. Let us begin with Communication Model.

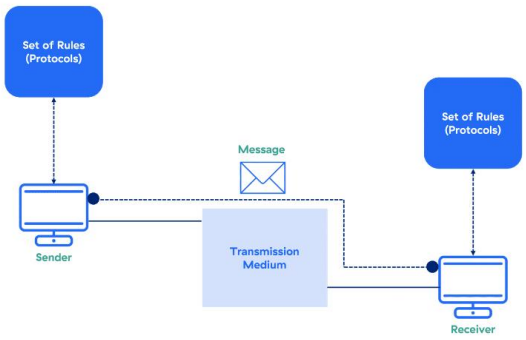
Communication Model

The basic communication model in computer networking is where the sender (encodes the message) channel sends a message over a channel or medium and receiver (decodes the message) gives feedback.

The components involved in a basic communication model are as follows:

- **Sender:** A sender is a device that is capable of sending the data (message) over the network.
- **Receiver:** A receiver is a device that is capable of receiving data (message) from the network.
- **Message:** A message is the information or data that needs to be exchanged between the sender and the receiver. It can be in the form of text, number, image, audio, video, etc.
- **Transmission Medium:** Transmission medium is the path by which the message travels from the sender to the receiver. It can be wired or wireless, television, newspapers, radio, etc. A television cable, telephone cable, ethernet cable, and satellite link are examples of transmission medium.
- **Protocol:** A protocol is a set or rules used by the sender and receiver in order to have reliable and successful data communication. Without

protocols, the communicating entities are like two persons trying to talk to each other in a different languages without knowing the other language.



Encoding and Decoding Communication

Encoding is implemented by applying an algorithm or computation in which the original data form is modified to a different form.

Decoding is the process of decrypting the encoded data to its original form by applying the decoding computation or the algorithm.

Network Packet

Network packets are the basic units of information that travel through a network. Each information sent off by a sender through a network is broken down into small units to enable easy and quick transmission over the network links.

For example, when a user requests a web page, the user's device sends packets to the server. The server then responds by sending its packets back to the user's device. This process continues until the transfer is complete. Then, the device's browser reassembles all packets into a single web page.

A network packet consists of three main parts:

- **Header:** Initial information of the packet.
- **Payload:** Actual data that is being transmitted to the destination.
- **Trailer:** A set of information added to the end of a packet. This information includes error-checking data and the timestamp.

4.3 OSI Model and The Seven Layers

The OSI model is a conceptual framework that is used to describe the functions of a networking system.

The OSI model characterizes computing functions into a universal set of rules and requirements to support interoperability between different products and software.

In the OSI reference model, the communications between a computing system are split into seven different abstraction layers:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session layer
- Presentation layer
- Application Layer

1.Physical Layer

The Physical layer is the first layer of the OSI model. This layer interacts with actual hardware and signaling mechanism, and plays a fundamental role in the OSI Model.

Some of the key functions of the Physical layer are as follows:

- Physical layer is the only layer of the OSI model which deals with the physical connectivity of two different stations.
- This layer is responsible for the transmission of data over the network by converting digital bits into electrical, optical, or radio signals that can be transmitted through the network medium.
- At the Physical layer, one might find “physical” resources, such as hubs, cabling, repeaters, network adapters, or modems.
- Physical layer avoids collisions between data flowing in the network due to the irretrievability of data packets.

2.Data Link Layer

The Data Link layer is the second layer from the bottom in the OSI network model. This is considered the most complicated layer of the OSI model as it hides all the complexities of the hardware from the other layers.

Some of the key functions of Data Link Layer are as follows:

- Data link layer is responsible for the node-to-node delivery of data.
- This layer is responsible for framing, detecting error, and ensuring reliable communication between nodes in any network.

- Data Link layer is also responsible for encoding, decoding, and organizing the incoming and outgoing data.

Sub-layers of the Data Link Layer

The Data Link layer encompasses two sub-layers of its own - Logical Link Control (LLC) and Media Access Control (MAC).

LLC Protocol

LLC protocols are a set of functions that enable communication between the Network layer and the Data Link layer, providing error control, flow control, and framing services to ensure reliable transmission of data.

LLC Format

The basic format of LLC protocols is modeled after the High-level Data Link Control (HDLC). These protocols are unacknowledged connectionless service, connection-oriented service, and acknowledged connectionless service. All of these protocols use the same Protocol Data Unit (PDU) format as shown in the image.

MAC Protocol

MAC protocol enables communication between devices on a network. This protocol is responsible for defining how devices on a network can access and use the network's resources. It also manages the flow of data between devices.

MAC Addresses are unique 48-bit hardware numbers of a computer that are embedded into a network card (also known as a Network Interface Card) during manufacturing. The MAC Address is also known as the Physical Address of a network device.

3.Network Layer

The Network Layer is the third layer in the OSI model of computer networks.

Some of the key features of Network layer are as follows:

- The main responsibility of the Network layer is to carry the data packets from the source to the destination without changing the content in them.
- If the packets are too large for delivery, they are fragmented i.e., broken down into smaller packets.
- It involves both the source host and the destination host.

- At the source, it accepts a packet from the Transport layer, encapsulates it in a datagram, and then delivers the packet to the Data Link layer so that it can further be sent to the receiver.

- At the destination, it decapsulates the datagram, extracts and delivers the packet to the corresponding Transport layer.

- The Network Layer is responsible for routing and addressing, allowing for the efficient transfer of data between different networks available in the network protocol stack.
- This layer is responsible for routing data packets to their destination and assigning unique addresses to each device on the network, ensuring efficient and reliable communication.
- At this layer, routers are a crucial component which is used to route information where it needs to go between networks.

Routed and Routing Protocols

When we discuss protocols, we commonly use two terms: **Routed Protocols** and **Routing Protocols**. These protocols are defined at the Network layer of the OSI model.

Routed protocols, such as IP, manage packets with routing information that enables those packets to be transported across networks using routing protocols.

Routing protocols specify how routers communicate with one another on a network. Routing protocols can either be **Static** or **Dynamic**.

4.Transport Layer

The Transport layer is the fourth layer in the OSI model. The main role of this layer is to provides communication services to the application processes that are running on different hosts.

The Transport layer is an end-to-end layer which ensures reliable communication by providing mechanisms such as segmentation, flow control, and error control. It is called an end-to-end layer because it provides a point-to-point connection instead of hop-to-hop, between the source host and destination host to deliver the services reliably.

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the most common protocols of the Transport layer.

Working of Transport Layer

The Transport Layer takes services from the Application layer and provides the services to the Network layer.

- At the sender's side: The Transport layer receives data (message) from the Application layer and then performs segmentation. It divides the actual message into segments, adds the source and destination's port numbers into the header of the segment, and transfers the message to the Network layer.
- At the receiver's side: The Transport layer receives data from the Network layer, reassembles the segmented data, reads its header, identifies the port number, and forwards the message to the appropriate port in the Application layer.

5.Session Layer

The Session layer is the fifth layer in the OSI model. This layer controls the conversations between different computers.

At the Session layer, a session or connection between machines is set up, managed, and is terminated.

Session layer services also include authentication and reconnections. In case of network error, the Session layer checks the authenticity and provides recovery options to the active sessions.

Some of the functions performed by the Session layer are as follows:

- The Session layer provides a mechanism of opening sessions, ensuring they remain open while data is being transferred, and closing them when communication ends.
- The Session layer establishes connections between devices known as sessions. Session allows users to share data, file management, and remote access.
- The Session layer is responsible for token management which prevents two users to simultaneously accessing or attempting the same critical operation.
- This layer allows synchronization by adding checkpoints, which are considered as synchronization points to the streams of data.

6.Presentation Layer

The Presentation layer is the sixth layer in the OSI model. The Presentation layer formats or translates data for the Application layer based on the syntax or

semantics that the application accepts. Because of this, it is also called the **Syntax** or **Translation** layer.

This layer can also handle the encryption and decryption required by the Application layer.

Some important functions of the Presentation layer are as follows:

- The Presentation layer translates data for the Application layer.
- The Presentation layer helps the receiver to understand the data and use it effectively and efficiently.
- This layer is responsible for encryption and decryption of data to avoid data leakage and data medication.
- This layer is responsible for data compression which helps to reduce the bandwidth of the data to be transmitted.

7. Application Layer

The Application layer is topmost layer in the OSI model. This layer offers different methods of data manipulation which enables all types of users to access network with ease.

The Application Layer makes a request to the presentation layer for receiving various types of information from it.

Some important functions of the Application layer are as follows:

- The Application layer is responsible for providing network services to user applications, including user interface and data representation, marking it a crucial layer in the network protocol stack.
- The Application layer is responsible for providing a user interface and representing data formats, allowing users to interact with the network and interpret data in a meaningful way.
- This layer sees network services provided to end-user applications, such as a web browser or Office 365.

4.4 IP Addressing and Subnetting

4.4.1 IP Addressing

An IP address is a unique address that identifies a device on a local network or on the internet. IP addresses are made up of binary values and drive the routing of all data over the Internet.

There are two versions of IP:

IP version 4 (IPv4) and IP version 6 (IPv6).

Because of the 32-bit length and the limited amount of unique IPv4 addresses, subnets and various methods for storing IP addresses have been developed. There are many unique addresses available for IPv6 addresses that are 128-bit.

4.4.2 Types of IP Addressing

1.Public IP Addressing

A public IP address is an external-facing IP address that is used to communicate outside the network. In most cases, this will be the router. All devices connected to a router communicate with other IP addresses using the router's IP address.

A public IP address is basically assigned by the Internet Service Provider (ISP).

2.Private IP Addressing

A private IP address is an internal-facing IP address that is not routed on the Internet, and no traffic can be sent to them from the Internet. Private IP addresses are used to establish a network connection in corporations, offices, or residents.

A private IP address boosts security within a network and prevents external users from establishing a connection.

3.Static IP Addressing

A static or dedicated IP address is a fixed address assigned to a device that remains constant. They are typically used for businesses that operate servers that require a constant presence on the internet, such as web servers.

Static addresses are manually configured either by the device itself or by the network administrator.

4.Dynamic IP Addressing

A dynamic IP address is an address assigned to a device temporarily by an ISP. Dynamic IP addresses are part of a typical home internet plan such as computers, smartphones, or routers. Unlike a static IP address, these addresses can change over time.

A dynamic IP address is pulled from a pool of addresses and then assigned to the home network by the ISP. After a few days, that IP address is put back into the pool and a new IP address is assigned.

4.4.3 Subnetting

Subnetting is the process of partitioning a complex network into multiple smaller subnetworks, or subnets.

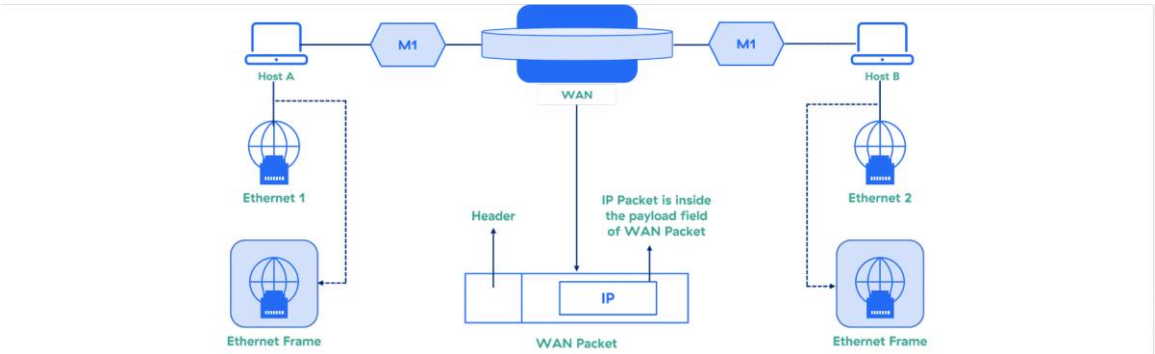
Advantages of subnetting are listed below:

- Subnetting enables network managers to create more controllable and segmented networks for performance or security needs.
- For example, a large enterprise could segment its network into subnetworks for multiple divisions or locations.
- In a complex network, traffic requires fast and efficient routes. Subnetting uses the route aggregation mechanism to limit the size of the routing table that each router has to maintain. This not only helps maintain efficient network speed, but also enhances performance.
- Subnetting reduces congestion and bottleneck problems.
- Subnetting enhances network security, as devices don't access the whole network.

4.5 Tunneling

Tunneling, an inter-networking technique, is a method of transporting data across a network using protocols that are not supported by that network. It is used when the same type of source and destination networks are connected through a network of different types.

Tunneling uses a layered protocol model such as OSI or TCP/IP.



For example, let us consider an Ethernet is connected to another Ethernet through a WAN as shown in the image.

4.5.1 Types of Tunneling

1.Generic Routing Encapsulation (GRE)

GRE is a method of encapsulating data packets that use one routing protocol inside the packets of another protocol. In other words, GRE tunnels establish a secure channel through which data can be sent between two locations.

2.Internet Protocol Security (IPsec)

IPsec is an **Internet Engineering Task Force (IETF)** standard suite of protocols between two communication points across the IP network. IPsec provides security services for IP network traffic, such as data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets.

3.IP-in-IP

It is a tunneling protocol for encapsulating IP packets inside another IP packet.

4.Secure Shell (SSH)

It is a cryptographic network protocol that is used for transferring encrypted data over the network. SSH is used to login and perform operations on remote computers and also be used for transferring data from one machine to another.

5.Point-to-Point Tunneling Protocol (PPTP)

PPTP generates a tunnel and confines the data packet. It is used to encrypt the data between the connections. PPTP is one of the most widely used VPN protocols and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

6.Secure Socket Tunneling Protocol (SSTP)

SSTP is a VPN protocol developed by Microsoft that uses SSL to secure the connection. This protocol is only available for Windows.

7.Layer 2 Tunneling Protocol (L2TP)

L2TP is a computer networking protocol that was designed to support VPN connections. It is used to transfer information securely and rapidly across public networks.

L2TP was created by Microsoft and Cisco in the year 2000 as a replacement for the older Point-to-Point Tunneling Protocol (PPTP). It combines the best features of PPTP and Layer 2 Forwarding (L2F) from Cisco Systems. The two protocols work together to create stable point-to-point connections at the OSI model Layer 2.

8.Virtual Extensible Local Area Network (VXLAN)

VXLAN is a network virtualization technology that stretches layer 2 connections over layer 3 networks. It encapsulates Ethernet frames in a VXLA packet which includes IP addresses to address the scalability problem in a more extensible manner.

CHAPTER 5

REAL-TIME EXAMPLES

1. Pfizer: Securing Research Data in Pharmaceuticals

Pfizer, a global pharmaceutical company, faced the challenge of securing sensitive research data while enabling its researchers to collaborate across the globe. With the rise of targeted cyberattacks and industrial espionage, Pfizer needed to ensure its network was both secure and scalable. Cisco's Secure Access Service Edge (SASE) model, combining SD-WAN and Cloud Security, was deployed to protect sensitive data. Pfizer also integrated Zscaler Internet Access (ZIA) to provide web and application security for all internet-bound traffic, including SSL inspection and threat intelligence.

Outcome:

- Protected research data from cyber threats like phishing and ransomware.
- Seamless collaboration across global research centers with secure access to critical resources.
- Improved compliance with industry regulations, ensuring data privacy.

2. Uber: Network Security for Global Operations

Uber operates in over 60 countries, and ensuring consistent security policies across its global workforce was a significant challenge. With employees accessing internal systems from remote locations, Uber implemented Zscaler Private Access (ZPA) to eliminate the need for traditional VPNs. The ZPA solution allowed Uber to secure application access based on user identity and device health, providing a zero-trust architecture that ensures only authenticated users can connect to specific apps.

Outcome:

- Improved remote access security with faster, direct access to applications.
- Reduced attack surface by segmenting applications and limiting user access based on zero-trust principles.
- Faster global deployment and network scalability with reduced IT complexity.

3. Facebook: Protecting Employee Devices

Facebook, a leading social media platform, has millions of daily active users and vast amounts of sensitive data to protect. With remote work becoming more prevalent, Facebook adopted BeyondCorp, a Google-originated zero-trust model, to provide secure access to internal applications without VPNs. This allowed employees to access Facebook’s systems securely from any device or network, using context-based access policies.

Outcome:

- Secure access for employees working remotely or on-site, minimizing the risk of unauthorized access.
- No reliance on VPNs, improving the user experience and reducing overhead.

- Enhanced endpoint security with device posture checks and multi-factor authentication (MFA).

4. Netflix: Scaling Network Security for Streaming Services

As a global leader in streaming, Netflix needed to ensure both internal and external security at scale. With millions of users accessing content, Netflix adopted AWS Security Services for scalable, cloud-native security, combined with Cloudflare's DDoS protection to guard against traffic spikes and cyberattacks. Zscaler Internet Access (ZIA) was also integrated to ensure secure internet access for internal users, providing threat detection and SSL traffic inspection to protect sensitive data and intellectual property.

Outcome:

- Protected global network from Distributed Denial of Service (DDoS) attacks, maintaining service uptime.
- Enhanced cloud security for internal systems and applications, safeguarding intellectual property.
- Scalable security infrastructure supporting millions of users globally.

5. Capital One: Securing Financial Data in the Cloud

Capital One, a financial services company, adopted a cloud-first strategy and moved critical workloads to Amazon Web Services (AWS). To secure sensitive financial data, Capital One implemented AWS Identity and Access Management (IAM) alongside Zscaler Internet Access (ZIA) for secure, policy-based access to cloud services. AWS security features, including encryption and real-time threat detection, helped Capital One meet compliance requirements and protect its users' data.

Outcome:

- Enhanced cloud security with encryption and access management for sensitive data.
- Improved compliance with financial regulations such as PCI DSS.
- Fast, secure cloud access for employees, improving productivity while safeguarding data.

6. Zoom: Securing Video Conferencing Platforms

As video conferencing usage surged during the COVID-19 pandemic, Zoom became a target for cyber threats, including data breaches and Zoombombing. Zoom implemented Okta's Identity and Access Management (IAM) and Cloudflare's DDoS protection to secure its infrastructure and ensure only authenticated users could access its services. In addition, Zoom adopted Zscaler Digital Experience (ZDX) to monitor network performance, ensuring high-quality video connections while maintaining security.

Outcome:

- Protected user data through secure authentication and identity management.
- Improved video quality by optimizing network performance and security simultaneously.
- Reduced security incidents by preventing unauthorized access and cyberattacks.

7. Adobe: Cloud Security for Creative Platforms

Adobe transitioned its Creative Cloud services to the cloud, enabling millions of users to access design and creative tools remotely. To secure user access and protect intellectual property, Adobe adopted Microsoft Azure Security features, along with Zscaler Internet Access (ZIA) for threat prevention and secure internet access. This ensured that users, whether individuals or enterprises, could access Adobe's services securely from anywhere.

Outcome:

- Secure access to cloud services for users globally, with SSL inspection and threat prevention.
- Scalable infrastructure to handle millions of users accessing Adobe's Creative Cloud.
- Intellectual property protection with data encryption and real-time threat monitoring.

8. British Airways: Protecting Customer Data

British Airways faced a significant cyberattack in 2018, resulting in a data breach that compromised customer payment details. Following the incident, the airline implemented Palo Alto Networks' Next-Generation Firewalls (NGFW) to secure its perimeter and adopted Zscaler Internet Access (ZIA) to protect internet-bound traffic, providing advanced threat detection, malware prevention, and SSL inspection.

Outcome:

- Improved perimeter defense and internal traffic security.
- Reduced risk of data breaches with advanced threat detection and real-time monitoring.
- Enhanced compliance with data protection regulations like GDPR.

CHAPTER 6

LEARNING OUTCOMES

After completing this Training Track, you will be able to:

- **Describe** computer network and its components
- **Discuss** various types of computer networks and network cables
- **Define** different types of network protocols
- **Explain** the fundamentals of data communication
- **Explain** the OSI model and its layers
- **Describe** the concept of IP addressing, subnetting, and tunneling

CONCLUSION

In conclusion, Zscaler's cloud-native networking solutions provide a transformative approach to securing modern, distributed environments. By leveraging a zero-trust architecture, Zscaler enables organizations to secure access to the internet, cloud applications, and internal resources without the need for traditional hardware like VPNs or firewalls. The platform ensures enhanced security through features like SSL inspection, advanced threat protection, and data loss prevention, all while delivering seamless and scalable access for users.

Zscaler's ability to streamline IT operations, reduce complexity, and enhance user experiences makes it a vital component for businesses undergoing digital transformation. Whether securing remote workforces, enabling cloud adoption, or integrating newly acquired entities, Zscaler helps organizations stay secure, agile, and compliant in today's fast-evolving technological landscape.

Internship Certificate:

REFERENCES

[1] https://www.zscaler.com

[2] https://studentacademy.zscaler.com