JYOTI NIVAS COLLEGE

Bengaluru, India

Post Graduated Centre

DEPARTMENT OF MCA

TECH-ON-TAP

E-JOURNAL

ON

COMPUTER NETWORKS

ISSUE-4 **SEPTEMBER 2023**

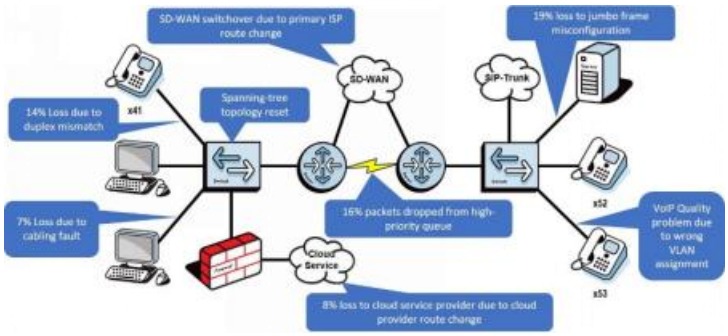
INDEX

NETWORK TROUBLE SHOOTING

KONDA KAVYA
(22MCA20)

INTRODUCTION:

Network troubleshooting refers to the combined measures and processes used to identify, locate, and resolve network problems located anywhere along a network, from WAN to LAN. Network troubleshooting is used to identify and resolve issues that can occur in a computer network. Computer networks are complex systems that are made up of various components, such as routers, switches, servers, and cables, that work together to transmit data and enable communication between devices. Network troubleshooting involves a range of techniques, including analyzing network traffic, checking hardware and software configurations, and testing network connections.



Essential steps to diagnose and resolve network troubles effectively.

1.Identifying the Problem

The first step in network troubleshooting is to identify the problem accurately. This requires active listening and communication with users or colleagues experiencing the issue. Ask specific questions to gather relevant information, such as the type of problem (e.g., slow internet, connectivity loss), the affected devices, and the time the issue started. Understanding the symptoms is crucial in narrowing down the possible causes.

2.Verify Physical Connections

Physical connectivity issues are among the most common culprits for network troubles. Ensure all cables, switches, routers, and other networking equipment are securely connected. Examine for loose connections, damaged cables, or faulty hardware. Replace any damaged components as necessary and retest the network.

3.Check Network Devices

Network devices such as routers, switches, and access points can also be potential sources of trouble. Verify their power status and indicator lights to ensure they are functioning correctly. If possible, access the device's web interface or command-line interface to review configurations and logs for any errors or abnormal activities.

4.Test Connectivity

To determine the extent of the network problem, perform connectivity tests. Use tools like the "ping" command to check if devices can communicate with each other. If pings fail, it can indicate issues with the network configuration, firewall settings, or hardware problems. Additionally, tools like "traceroute" can help identify the path a packet takes, highlighting potential points of failure

5.Analyze Network Traffic

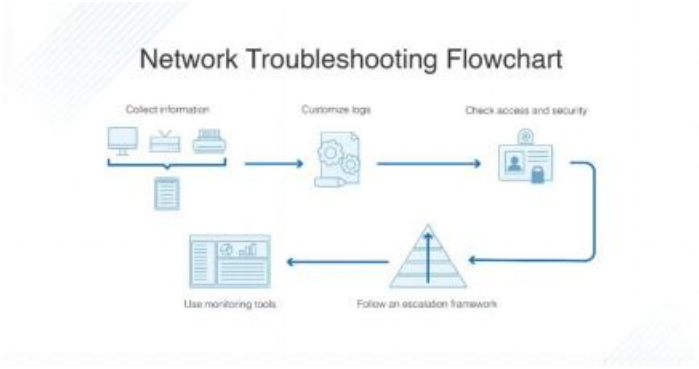
Network congestion and bandwidth issues can lead to slow or unreliable connections. Network monitoring tools can provide insights into data usage, packet loss, and network traffic patterns. Identify bandwidth hogs or unusual traffic spikes that may be causing the problem. This step is crucial for identifying and resolving performance-related issues.

6.Firewall and Security Checks

Firewalls are essential for network security, but they can also cause network issues if misconfigured. Review firewall rules and access control lists to ensure they permit necessary traffic and block unauthorized access. Be cautious about making changes to firewall settings, as they directly impact network security.

7.Update Firmware and Software

Outdated firmware and software can lead to compatibility issues and vulnerabilities. Regularly check for updates from the manufacturers and apply them to your networking equipment and devices. This step can often resolve known bugs and security weaknesses.



CONCLUSION:

Network troubleshooting is a crucial skill for IT professionals and anyone responsible for maintaining a reliable network. By following a structured approach and utilizing diagnostic tools, you can identify and resolve network issues efficiently. Remember to document your troubleshooting steps and solutions for future reference. With a well-maintained network, businesses and individuals can enjoy uninterrupted connectivity and improved productivity.

INTERNET OF THINGS

INAMDAR JAITASHREE SHRIRAMDAS
(22MCA14)

The Internet of Things (IoT) refers to the network of interconnected physical devices that communicate and exchange data with each other through the internet. These devices, often embedded with sensors and actuators, can collect, and share information, enabling them to make intelligent decisions and perform various tasks.

Here are some key aspects of the Internet of Things:

1. Connectivity: IoT devices use various communication technologies such as Wi-Fi, Bluetooth, Zigbee, cellular networks, and more to connect and share data.

2. Sensors and Actuators:

Sensors: Devices equipped with sensors can collect data from the environment. Examples include temperature sensors, motion sensors, and humidity sensors.

Actuators: These devices can perform actions based on the data received. For example, actuators might control the temperature of a room, turn on lights, or adjust the speed of a motor.

3. Data Processing:

- Data collected by IoT devices is often sent to the cloud or processed at the edge for analysis. Advanced analytics, machine learning, and artificial intelligence may be used to derive meaningful insights from the data.

4. IoT Platforms:

- IoT platforms provide the infrastructure to manage, monitor, and analyse IoT devices. They often include features for device management, data storage, and application development.

5. Security:

- Security is a critical concern in IoT due to the vast amount of data being exchanged. Measures such as encryption, secure device onboarding, and regular security updates are essential to protect against potential threats.

6. Applications:

- IoT has a wide range of applications across various industries, including:

Smart Homes: Connected devices for home automation (smart thermostats, lights, security systems).

Healthcare: Wearable devices for health monitoring, smart medical equipment.

Industrial IoT

(IIoT): Monitoring and optimizing industrial processes, predictive maintenance.

Smart Cities: Intelligent transportation systems, waste management, energy efficiency.

Agriculture: Precision farming, monitoring crop conditions.

7. Challenges:

- Implementing IoT comes with challenges, including privacy concerns, interoperability issues, standardization, and the need for robust cybersecurity.

8. Future Trends:

- Continued growth is expected in areas such as edge computing, 5G connectivity, and the integration of AI with IoT to enable more intelligent and autonomous systems.

IoT is a rapidly evolving field with significant implications for how we live and work. Its ability to create a network of interconnected devices and systems has the potential to drive efficiency, improve decision-making, and enhance various aspects of daily life and business operations.

5G NETWORKS IMPACT ON FIBER-OPTIC CABLING REQUIREMENTS

ASHMIKA SHANDILYA
(22MCA05)

5G networks promise to connect people and things through intelligent networks and applications, all generating an immense amount of data. It seeks to provide the best of all performance factors while simultaneously connecting more devices. These network advancements will enable and inspire a new wave of computing and technological innovation that will change the way we live and work. But before 5G becomes a reality, the network infrastructure has to be in place to support the billions of devices and the trillions of megabits of data that will flood the network. Let's take a look at how 5G will impact optical-fiber requirements.

Cellular capabilities started off rather simply, but as each generation expanded functionality, applications, and services the network infrastructure supporting them has grown increasingly complex. To achieve all that 5G offers, a denser, fiber-rich network infrastructure will be needed to deliver the key performance indicators: lower latency, longer battery life, higher data rates, ultra-high reliability and more connected devices

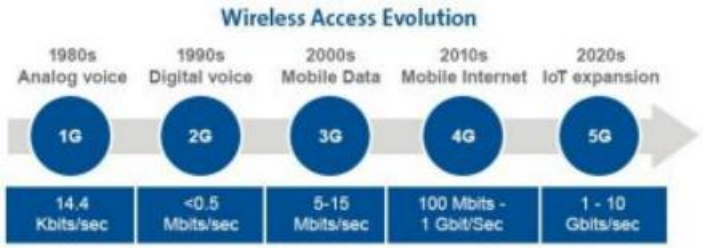
Why 5G is different

5G enables the vision of a truly connected society with its impact being felt across virtually every industry. The Internet of Things (IoT) will transform the economy and the way we live our lives. 5G will similarly change and create new economic opportunities.

- 5G Smart buildings/cities/communities will provide more effiicient services to citizens, increase collaboration among different economic sectors, and encourage innovative business models in both private and public sectors.

- In healthcare, 5G will enable virtual medicine to substantially increase the effectiveness of preventative care, as well as robotic surgery.

- Autonomous vehicles will help make transportation safer, parking easier, and improve traffic flow and congestion.



The opportunities above depend heavily on real-time data, and the need for lower latency and higher bandwidth becomes much more critical. This, in turn, drives the need for edge computing to enable critical data to be transferred quickly.

The early development of cellular networks leveraged macro towers using lower-wavelength spectr4um capable of covering wide physical areas, positioning some up to 25 miles apart (if topology allowed). Towers, however, couldn't be placed everywhere, and small cells and radio heads were increasingly deployed to get the radio closer to the user.

Small cells began to augment coverage and capacity in both 3G and 4G deployments, the term "densification" was introduced. With 5G, unlike its predecessors, a different set of frequencies will be used to implement new services. Sub-6-GHz will be used worldwide as the basis for city-wide mobile connectivity, while higher parts of the spectrum (millimeter wave frequencies of 24 GHz and above) will be used for high-bandwidth coverage. This new higher-band spectrum inherently has more significant distance coverage limitation. Thus, densification takes on an entirely new meaning.

Optical fiber is the preferred medium for existing wireless backhaul networks, and even in networks where this is not the case, the wireless backhaul eventually needs to connect into a fiber backhaul. Fiber will also be preferred for what is known as "fronthaul," connecting the dense mesh of 5G small cells. Why is this? Increased speeds with lower attenuation, immunity to electromagnetic interference, small size, and virtually unlimited bandwidth potential are among the many reasons why fiber is the right choice. The question becomes, "How many fibers are needed to support each cell?" And the answer will depend primarily on what technology protocols will be employed.

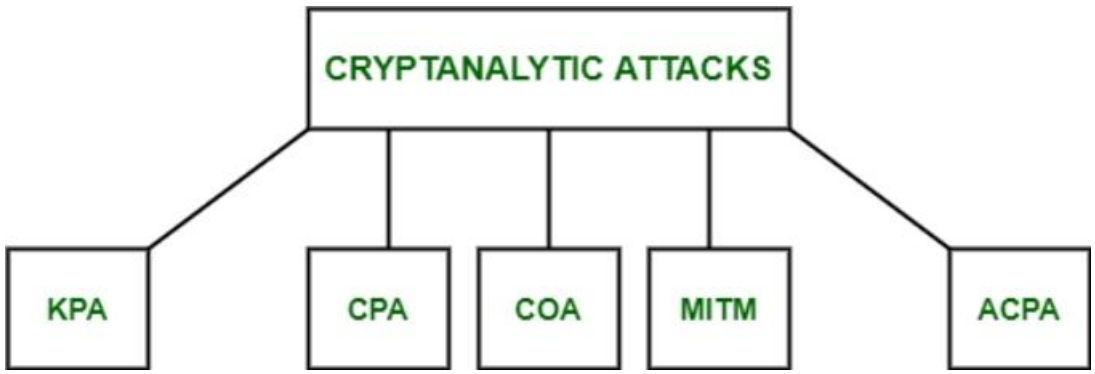
CRYPTANALYSIS AND TYPES OF ATTACKS

BHOOMIKA C R
(22MCA06)

Cryptology has two parts namely, Cryptography which focuses on creating secret codes and Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a Cryptanalyst. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. For example, a Cryptanalyst might try to decipher a ciphertext to derive the plaintext. It can help us to deduce the plaintext or the encryption key.

To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called Cryptanalytic attacks. The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java. Therefore, nature of the plaintext should be known before trying to use the attacks.

Types of Cryptanalytic attacks :



Known-Plaintext Analysis (KPA) : In this type of attack, some plaintext-ciphertext pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.

Chosen-Plaintext Analysis (CPA) : In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. Its very simple to implement like KPA but the success rate is quite low.

Ciphertext-Only Analysis (COA) : In this type of attack, only some cipher-text is known and the attacker tries to find the corresponding encryption key and plaintext. Its the hardest to implement but is the most probable attack as only ciphertext is required.

Man-In-The-Middle (MITM) attack : In this type of attack, attacker intercepts the message/key between two communicating parties through a secured channel.

Adaptive Chosen-Plaintext Analysis (ACPA) : This attack is similar CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have ciphertexts for some texts.

Birthday attack: This attack exploits the probability of two or more individuals sharing the same birthday in a group of people. In cryptography, this attack is used to find collisions in a hash function.

Side-channel attack: This type of attack is based on information obtained from the physical implementation of the cryptographic system, rather than on weaknesses in the algorithm itself. Side-channel attacks include timing attacks, power analysis attacks, electromagnetic attacks, and others.

Brute-force attack: This attack involves trying every possible key until the correct one is found. While this attack is simple to implement, it can be time-consuming and computationally expensive, especially for longer keys.

Differential cryptanalysis: This type of attack involves comparing pairs of plaintexts and their corresponding ciphertexts to find patterns in the encryption algorithm. It can be effective against block ciphers with certain properties.

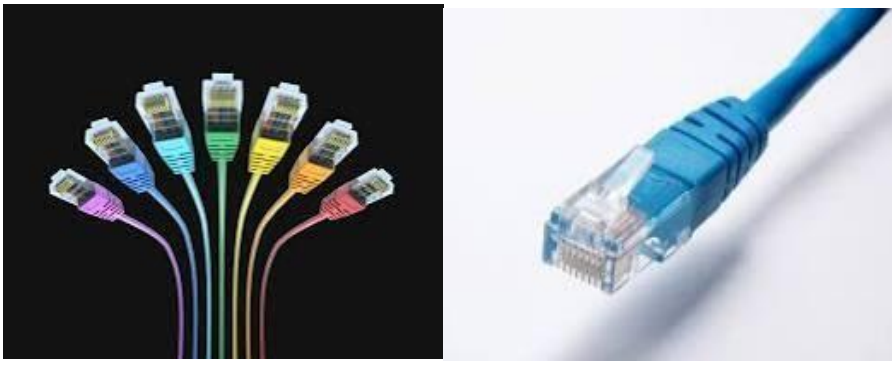
ETHERNET

GINITHA G
(22MCA11)

INTRODUCTION:

Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN). It enables devices to communicate with each other via a protocol, which is a set of rules or common network language.

Ethernet is a way of connecting computers and other network devices in a physical space. This is often referred to as a local area network or LAN. Ethernet describes how network devices format and transmit data so other devices on the same LAN or campus network can recognize, receive and process the information. An Ethernet cable is the physical, encased wiring over which the data travels. Connected devices that use cables to access a geographically localized network -- instead of a wireless connection -- likely use Ethernet. From businesses to gamers diverse end users rely on the benefits of Ethernet connectivity, which include reliability and security. Ethernet uses cables to transmit data in a network model, such as LAN and, in some cases, WAN. It is more reliable and secure, providing better network Connectivity.



.

Features:

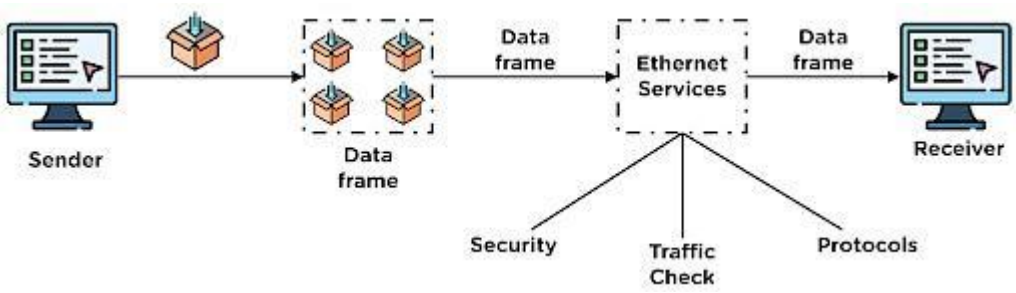
- Fast Ethernet provides 100 Mbps speed.
- Fast Ethernet is simple configured.
- Fast Ethernet generate more delay comparatively.
- The coverage limit of Fast Ethernet is up to 10 km.
- The round-trip delay in Fast Ethernet is 100 to 500 bit times.
- Fast Ethernet is the Successor of 10-Base-T Ethernet.

Working of Ethernet Network:

The Ethernet network is designed to work in the 1st layer (physical layer) and 2nd layer (Data Link Layer) of the OSI model.

Ethernet divides the transmission of data into two parts: packets and frames.

- Packet–Refers to a unit of data in the network.
- Frame–Refers to the collection of data packets being transmitted.



The data to be transmitted is converted into data packets in the network and then transferred to the channel. At a point, multiple data packets are collected to form a data frame, which is then transmitted further in the network channel.

During data transmission, Ethernet applies various services over the data being transmitted,such as security checks, traffic control services & other protocols.

Types of Ethernet:

Depending on the network requirements, the type of Ethernet networks applied in the communication also varies. The different types of Ethernet connections are mentioned below:

- **Fast Ethernet:** This Ethernet type is used for transferring data around the network at a speed of 100 Mbps through twisted-pair cables or optical cables. This type of data transmitted can be done without applying protocols.
- **Gigabit Ethernet:** This type of Ethernet also uses optical and twisted pair cables for data transmission at 1000 Mbps. This is also one of the most preferred Ethernet networks.
- **Switched Ethernet:** This Ethernet type installs network devices such as switches or hubs to improve the network transmission. The transmission range for this type ranges from 1000Mbps to 10Gbps.

Seven types of Ethernet cables

- **Cat 5:** Up to 350 MHz and 100 Mbps.
- **Cat 5e (enhanced):** Up to 350 MHz and 1Gbps
- **Cat 6:** Up to 550 MHz and 1Gbps.
- **Cat 6a (augmented):** Up to 550 MHz and 10Gbps.
- **Cat 7:** Up to 600 MHz and 10Gbps.
- **Cat 7a:** Up to 1 GHz and 40Gbps.
- **Cat 8:** Up to 2 GHz and 25 or 40Gbps.

Why Use Ethernet:



Ethernet technology is used for establishing connections and is preferred for network channels. It is used in industry networks, college campuses, and medical institutions because it provides services to the data being transmitted.

- Ethernet provides high-speed data transmission in the network.
- It establishes a secure connection for transferring data in the network.
- Ethernet is reliable, as the possibility of outside interference is very low as cable data is difficult to hack into.

Advantages of Ethernet

- Relatively low cost.
- Backward compatibility.
- Generally resistant to noise.
- Good data transfer quality.
- Speed.
- Reliability.
- Data security.

Disadvantages of Ethernet

- Intended for smaller,shorter distance network.
- Limitted mobility.
- Use of longer cables can create crosstalk.
- Doesn't work well with real-time or interractive application.
- Speeds decrease with increased traffic.
- Receivers don't acknowledge the reception of data packets.
- Troubeshooting is hard when trying to trace which specific cable or node is causing the issue.

Conclusion:

In this tutorial on 'What Is Ethernet?', you learned about the Ethernet connection and the working steps involved in establishing the connection. The Ethernet network is preferred for small area network connections and provides different types of Ethernet connections for data transmission, which can be selected depending on your requirements.

If you want to learn more about implementing an Ethernet network in the system for establishing a stable and secure connection, you can refer to Simplilearn's Cyber Security Expert course. By the end of this professional course, you will be able to perform Ethernet network-related tasks much more efficiently.

References:

- "Ethernet History".
- "The Ethernet: A Local Area Network".
- "Evolution of Ethernet".

IMPACT OF COVID 19 ON COMPUTER NETWORKS

ESTHER JELINAL J
22MCA10

The COVID-19 pandemic has brought about unprecedented changes in various facets of life, including the way computer networks are utilized and managed. As nations implemented lockdowns and people adapted to remote work and online learning, computer networks faced extraordinary challenges, reshaping their roles and emphasizing their critical importance. This summary explores the multifaceted impact of the pandemic on computer networks.

The COVID-19 pandemic has left an indelible mark on computer networks globally. With widespread lockdowns and the shift to remote work and education, there was a massive surge in internet traffic, straining network infrastructure. Organizations and individuals heavily relied on video conferencing, cloud services, and virtual private networks (VPNs), necessitating rapid adaptations and investments in network scalability and resilience. However, the increased online activity also attracted cyber threats, emphasizing the need for enhanced cybersecurity measures. Additionally, the pandemic accelerated the adoption of 5G technology in some regions and underscored the importance of network redundancy and business continuity planning, ultimately reshaping the way we perceive and utilize computer networks in our daily lives.

In conclusion, the COVID-19 pandemic accelerated digital transformation and underscored the critical role of computer networks in our interconnected world. It forced organizations and individuals to adapt to new work and learning environments, leading to a surge in internet traffic and reliance on remote access solutions. These challenges highlighted the significance of network scalability, cybersecurity, and redundancy. The pandemic served as a catalyst for innovations in network technology, reshaping our reliance on and expectations of computer networks as we move forward into a more digitally interconnected future.

COMMUNICATION NETWORK PROTOCOLS

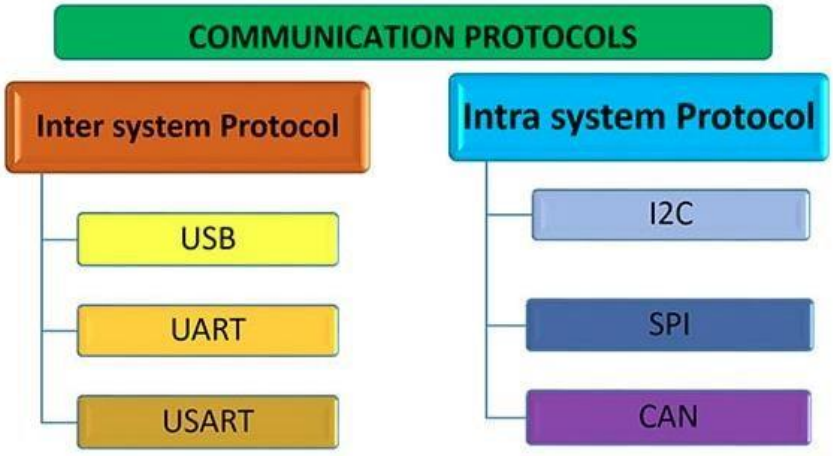
JAYA PRIYA R
(22MCA16)

In an embedded world, communication protocols are vital as they provide a gateway to exchange information among various devices with excellent reliability. Any secure and efficient communication must agree between sender and receiver on a specific set of rules called a protocol. So, a protocol is a collection of rules that governs data communications.

Communication protocol

Types of Communication protocols

The communication protocols have different categories.



Types of communication protocols

Intersystem Protocol

The intersystem protocol helps to establish communication between two devices. A good example is a computer and a development board via inter bus system.

Types of Inter System Protocol :

Intersystem protocols are of three categories:

1.USB Communication protocol

2.UART Communication protocol

3.USART Communication protocol

USB Communication protocol :

*Detecting attachment and removal of USB devices

*Managing data flow among host and devices

*Provide and control power to the attached devices

*Monitor activities on the bus

UART Communication Protocol :

Advantages of UART protocol

1.Simple, single-wire transmission and single wire reception of data with error checking

2.Easy interface for interconnecting embedded devices and desktop computers etc.

Disadvantages of UART protocol

1.The typical maximum data rate is low compared to SPI

2.Since it is asynchronous, the clock on both devices must be accurate, particularly at higher baud rates

USART Communication Protocol :

Advantages of USART protocol :

1.The speed of USART is more than the speed of UART

2.Data is transmitted in the form of blocks

Disadvantages of USART protocol :

1.Data is transmitted at a definite rate

2.USART is more complex than UART in terms of complexity

CAN communication protocol :

Robert Bosch developed the Controller Area Network (CAN) protocol in the 1980s. A CAN bus system in a vehicle makes it possible to network electronic modules such as control units or intelligent sensors. The CAN bus is independent of the vehicle's electronics systems and functions as a data line to swap information among control units.

Advantages of CAN protocol :

1.It is a low-cost solution as the number of wires used reduces compared to old communication models in automotive and thus reduces vehicle weight

2.It can auto retransmit the same message if any device does not receive a notification

Disadvantages of CAN protocol :

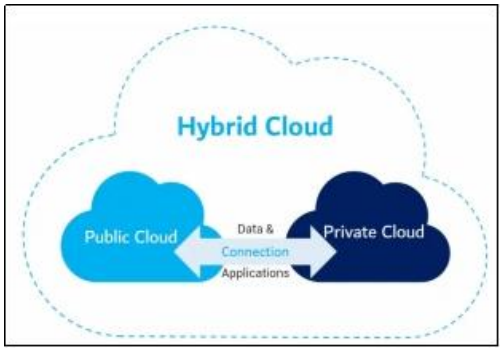
1.It lacks encryption and authentication mechanisms

2.It is limited to a maximum of 64 nodes or devices

THE FUTURE OF HYBRID CLOUD: INTEGRATING AI FOR OPTIMIZED NETWORKING

JOANNAH P
(22MCA18)

In today's dynamic tech landscape, Hybrid Cloud is not just a buzzword; it's a necessity. Offering the best of both private and public cloud environments, Hybrid Cloud has become a cornerstone for businesses seeking flexibility, scalability, and cost-efficiency. However, managing these complex infrastructures is no cakewalk. Enter Artificial Intelligence (AI). A game-changer in its own right, AI holds the promise of transforming Hybrid Cloud management. Intelligent systems can sift through vast datasets, automate resource allocation, and even enhance security measures. In essence, AI acts as the missing puzzle piece, seamlessly integrating with Hybrid Cloud to optimize its resources.



So, why is AI essential for the future of Hybrid Cloud?

1. **Role of AI in Hybrid Cloud:**

   Managing a Hybrid Cloud environment is fraught with challenges. From the labyrinthine intricacies of security and compliance to the ever-evolving maze of resource management and cost-efficiency, the difficulties are numerous and complex. However, Artificial Intelligence (AI) emerges as a beacon of hope in this landscape, offering innovative solutions to these challenges. Let's explore how AI fundamentally alters the equation, providing smarter approaches to resource allocation, predictive maintenance, and security.

   - **Automated Resource Allocation.**
     Utilizing machine learning algorithms, intelligent systems can continuously monitor workload requirements and performance metrics. These systems dynamically allocate or deallocate resources such as CPU, memory, and storage in real-time, ensuring optimal performance without unnecessary costs. It's a win-win—resources are efficiently used, and expenditures are kept in check.

- **Predictive Maintenance.**
  Traditional cloud maintenance often involves reactive measures, where problems are addressed after they manifest. This approach, while effective to some extent, is far from ideal. AI changes this by enabling proactive maintenance. **Machine learning models** can analyze historical data to predict potential failures or downtimes. This foresight allows for preventive measures to be taken before a problem escalates, thereby ensuring uninterrupted service and greater reliability.
- **Security**.
  Traditional security measures often rely on predefined rules or signatures to identify threats, a method that is increasingly becoming obsolete in the face of sophisticated cyber-attacks. AI, with its ability to analyze patterns and learn from them, offers a more dynamic solution. It continuously monitors network traffic and system behavior, flagging any abnormal activity in real-time. Such quick detection enables immediate action, thereby minimizing potential damage and enhancing overall security.

2. Technologies Powering AI in Hybrid Cloud:

The magic of AI in Hybrid Cloud management doesn't happen in a vacuum. It's powered by an array of advanced technologies that work in unison to bring intelligence and automation to your cloud infrastructure.

- **Machine Learning Models.**
  The backbone of AI's application in Hybrid Cloud is undeniably machine learning. Various types of models—including supervised, unsupervised, and reinforcement learning—are employed to make sense of complex data sets. For example, supervised learning models are often used in predictive maintenance, training on historical data to foresee future system failures.
- **Neural Networks.**
  Neural networks, particularly **deep learning architectures**, offer another layer of sophistication. These networks mimic the human brain's ability to learn from data, making them particularly effective for tasks like image recognition or natural language processing. In Hybrid Cloud settings, they can be utilized for advanced security protocols like identifying malicious activities based on intricate patterns.

- **Containers and Microservices**
  The modularity provided by containers and microservices plays a critical role in the effective deployment of AI in a Hybrid Cloud environment. These technologies allow machine learning models to be isolated and scaled independently, which is essential for handling diverse workloads efficiently.
- **APIs and SDKs**
  The interaction between AI algorithms and cloud resources is often facilitated through APIs (Application Programming Interfaces) and SDKs (Software Development Kits). These tools offer a seamless way to integrate machine learning capabilities into existing cloud management systems without the need for extensive code overhauls.

- **Data Lakes and Warehouses**

  Data is the fuel that powers AI, and Hybrid Clouds often incorporate data lakes or warehouses to store this valuable resource. Advanced analytics tools can sift through this data, ensuring that the machine learning models are fed high-quality, relevant data for training and inference.

- **Edge Computing**

  Last but not least, edge computing is becoming increasingly crucial in Hybrid Cloud environments equipped with AI. **Edge computing** allows for data processing to occur closer to where it is generated, which is essential for real-time analytics and low-latency responses—key attributes for successful AI applications.

3. The challenges of Hybrid Cloud Management:

As compelling as the advantages of Hybrid Cloud may be, its management isn't a straightforward affair. From balancing security protocols between different environments to ensuring compliance and cost-efficiency, there's a myriad of challenges to overcome.
Some of the challenges are:

- Security
- Compliance
- Resource Management
- Cost-Effectiveness

4. **Conclusion**:

As we've navigated through the intricate landscape of AI-integrated Hybrid Cloud systems, several key takeaways have emerged. The synergy between AI and Hybrid Cloud is not only revolutionary but also immensely practical, addressing real-world challenges from cost-efficiency and scalability to security and reliability. The future of Hybrid Cloud is unmistakably intertwined with advancements in AI, as machine learning models and other intelligent systems become increasingly crucial for optimizing cloud resources.

And as we look toward the future, it's clear that the boundary between AI and Hybrid Cloud will continue to blur, bringing forth new possibilities, solutions, and even challenges that we can't yet fully comprehend. To not only adapt but to thrive in this dynamic landscape, it's crucial to begin your journey into AI-integrated Hybrid Cloud today.

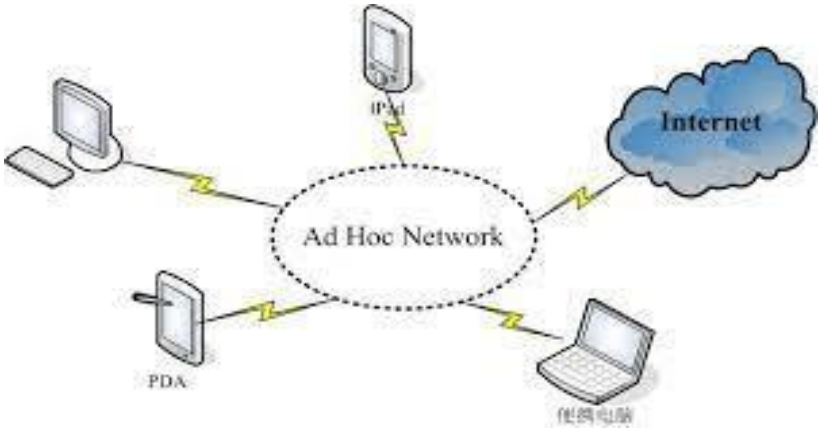
AD HOC NETWORKS

NIDHI DUBEY

(22MCA28)

Introduction:

In today's interconnected world, communication is at the heart of various aspects of our lives. However, in certain situations, establishing traditional communication infrastructures can be challenging or even impossible. Ad hoc networks come to the rescue in such scenarios by enabling devices to communicate directly with each other without relying on a fixed infrastructure. This article explores the concept of ad hoc networks, their key features, applications, and the challenges they present.



What is an Ad Hoc Network?

An ad hoc network is a decentralized wireless network that allows devices, such as laptops, smartphones, and IoT devices, to establish communication with each other on the fly. Unlike traditional networks that depend on centralized access points or routers, ad hoc networks form temporary connections between nearby devices, creating a dynamic and self-organizing network. Each device in the network acts as a node and forwards data to other devices, enabling multi-hop communication paths.

Key Features:

1. **Decentralization:** Ad hoc networks operate without any central control or fixed infrastructure. The absence of a central authority allows for flexible and adaptive networking, making them ideal for scenarios with no existing communication infrastructure.

2. **Dynamic Topology**: The network topology in an ad hoc network can change rapidly as devices join or leave the network. Devices must be capable of adjusting to these dynamic changes to maintain connectivity and efficient data transmission.

3. **Self-Organization**: Devices in an ad hoc network must self-organize to establish connections and maintain communication. This self-organization ensures that the network can be quickly set up and reconfigured without manual intervention.

4. **Limited Range**: Ad hoc networks typically have a limited communication range, as the direct communication between devices requires them to be within close proximity of each other. This range limitation impacts the overall coverage area of the network.

Applications of Ad Hoc Networks:

Ad hoc networks find applications in various domains, where traditional communication infrastructure is impractical or unavailable. Some prominent use cases include:

1. **Disaster Recovery**: During natural disasters or emergencies, when conventional communication channels may be disrupted, ad hoc networks enable emergency responders to establish communication and coordinate relief efforts.

2. **Military Operations**: Ad hoc networks play a crucial role in military operations, allowing soldiers to communicate and share information in remote or hostile environments where setting up fixed infrastructure is not feasible.

3. **Internet of Things (IoT)**: IoT devices often need to interact and exchange data with each other. Ad hoc networks facilitate seamless communication between IoT devices, especially in situations where connecting to a centralized server may not be possible.

4. **Collaborative Work and Conferences**: In meetings, conferences, or collaborative work environments, ad hoc networks enable participants to quickly share files and collaborate without relying on external Wi-Fi or wired connections.

Challenges and Considerations:

While ad hoc networks offer numerous advantages, they also present several challenges:

1. **Network Stability**: Frequent changes in the network topology can lead to instability and routing inefficiencies. Designing robust and adaptive routing protocols is essential to maintain network stability.

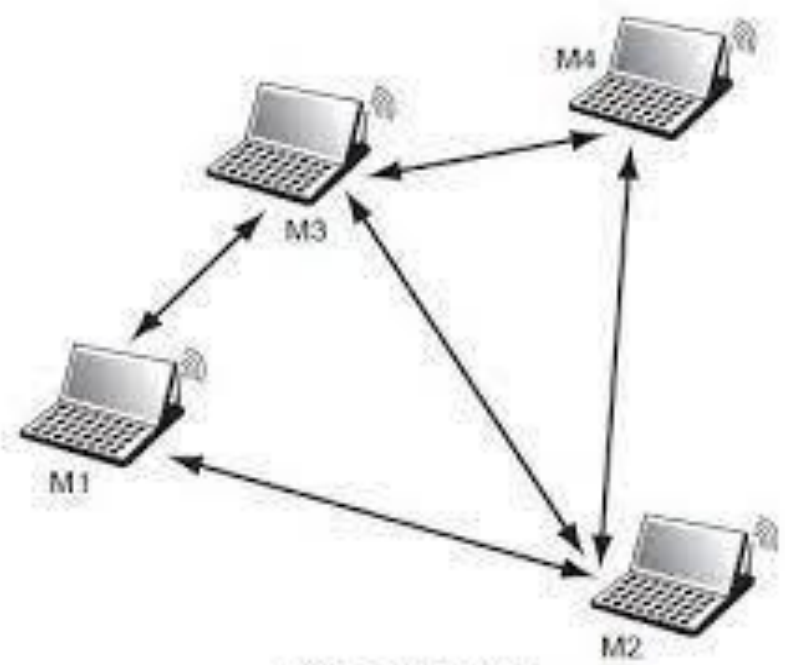
2. **Security**: Ad hoc networks are susceptible to security threats due to their decentralized and dynamic nature. Implementing encryption, authentication, and intrusion detection mechanisms is crucial to safeguard data and prevent unauthorized access.

3. **Scalability**: As the number of nodes in the ad hoc network increases, the complexity of network management and data routing grows exponentially. Ensuring scalability is vital for the network's long-term viability.

Conclusion:

Ad hoc networks are a remarkable solution for establishing communication in scenarios where traditional infrastructure is unavailable or impractical. Their decentralized nature, dynamic topology, and self-organizing capabilities make them invaluable in disaster recovery, military operations, IoT, and

collaborative work environments. However, addressing challenges related to network stability, security, and scalability remains crucial to unlock their full potential. As technology advances, ad hoc networks are likely to play an increasingly vital role in shaping the future of communication.



ad-hoc Network

ROUTER

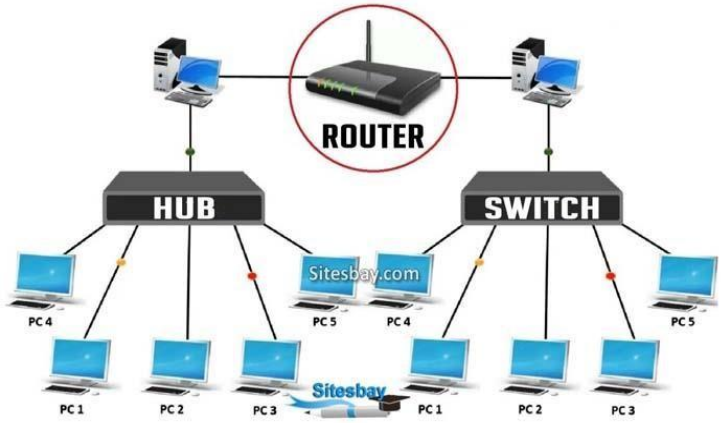
KAVYA L
(22MCA19)

What is Router?

A router is a device that connects two or more packet switched networks or subnetworks, connect computers and other devices to the Internet. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

A router acts as a dispatcher, choosing the best route for your information to travel. It connects your business to the world, protects information from security threats, and can even decide which computers get priority over others.

How router works?



When a computer sends a message, the message breaks into IP packets containing sender and receiver network information and the router has the capability to read this information, using this information, it calculates the best route for IP packets to travel on the network.

A router works by analysing the destination IP address of incoming data packets and forwarding them to the appropriate network. When a packet of data is sent from one network to another, the router determines the most efficient path for the packet to travel, based on a set of rules called routing protocols.
Routing protocols are a set of rules that determine how data packets are sent and received across a network. There are many different types of routing protocols, each with its own set of rules and algorithms for determining the best path for data to travel.

Types of Router
1. Wireless Router: Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard Ethernet routing for a small number of wired network systems.
2.Brouter : A brouter is a combination of the bridge and a router. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems.
3.Core router : A core router is a type of router that can route the data within a network, but it is not able to route the data between the networks.
4.Edge router: An edge router is a lower-capacity device that is placed at the boundary of a network. It allows an internal network to connect with the external networks. It is also called as an access router. It uses an External BGP (Border Gateway Protocol) to provides connectivity with remote networks over the internet.

Features of Router o A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
O A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
O It allows the users to configure the port as per their requirements in the network. o Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
O Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
O Routers filter out the unwanted interference, as well as carry out the data encapsulation and decapsulation process.
O Routers provide the redundancy as it always works in master and slave mode.
O It allows the users to connect several LAN and WAN. o Furthermore, a router creates various paths to forward the data.

Disadvantages of Routers

- Limited Bandwidth
- Vulnerability to Cyberattacks
- Limited Range
- Cost

CYBERNETICS AND SYSTEMS

LIKITHA M
(22MCA22)

Understanding the Control and Complexity of Interconnected Entities

Introduction:

The study of complex systems has been a topic of fascination for scientists and researchers across various disciplines. Two fundamental approaches that delve into the understanding of these intricate systems are cybernetics and systems theory. Cybernetics explores the principles of control and communication within systems, while systems theory provides a holistic framework to comprehend the interdependence and emergent behaviours of complex entities. This article aims to shed light on the significance of cybernetics and systems theory, their applications, and how they complement each other in understanding the dynamic world of interconnected systems.

Cybernetics:

Understanding Control and Communication: Cybernetics, a term coined by Norbert Wiener in the mid-20th century, derives from the Greek word "kybernetes," meaning "steersman." It encompasses the study of self-regulating systems, regardless of their nature be it mechanical, biological, social, or computational. The central theme of cybernetics lies in the concept of feedback loops, where a system receives information about its output and utilizes that information to modify its behaviour.

Cybernetic systems are pervasive in both natural and artificial environments. From the intricate neural networks governing human cognition to the autopilot systems in aircraft, cybernetics has proven invaluable in designing effective control mechanisms and artificial intelligence applications.

Systems Theory:

Embracing Complexity and Interdependence: Systems theory, as an interdisciplinary conceptual framework, studies complex systems as a whole, focusing on the relationships and interactions between their elements. Systems are viewed as interconnected and interdependent entities, where the whole is more than the sum of its parts. This approach emphasizes understanding emergent properties that arise from the interactions between the components. In systems theory, entities are analyzed in the context of their environments, recognizing that they are open systems continuously exchanging information and energy with their surroundings.

The approach encourages systems thinking, a method of problem-solving that examines the system's behavior as a whole, rather than focusing on isolated components. Systems theory finds applications in diverse domains, ranging from biology, where ecosystems exhibit complex interdependencies, to the social sciences, where organizations function as intricate systems with interconnected roles and responsibilities.

Interconnection Between Cybernetics and Systems: The relationship between cybernetics and systems theory is one of mutual benefit and complementarity. Cybernetics contributes theoretical tools and concepts to understand the control and communication aspects within systems. It provides a deeper insight into how systems self-regulate and adapt to changing conditions. Systems theory, on the other hand, offers a broader framework to study complex systems as unified wholes, allowing for a comprehensive understanding of the interactions and feedback mechanisms that influence the behavior of interconnected entities. By combining cybernetics and systems theory, researchers and practitioners gain a more comprehensive understanding of complex phenomena, enabling them to design effective control mechanisms, optimize system performance, and devise innovative solutions to intricate problems.

Practical Applications: The practical applications of cybernetics and systems theory are manifold. In engineering and technology, cybernetics plays a pivotal role in the design of autonomous systems, robotics, and advanced control algorithms. Additionally, systems thinking facilitates effective project management, organizational development, and strategic planning in various industries. In healthcare, cybernetics aids in the development of prosthetics and medical devices that interact seamlessly with the human body, adapting to physiological changes. Systems theory, on the other hand, helps in understanding disease patterns and designing efficient healthcare delivery systems.

Challenges and Future Directions: While cybernetics and systems theory have shown remarkable promise, they also face challenges in practical implementation. Dealing with highly complex systems requires robust computational resources, sophisticated modeling techniques, and vast amounts of data. Interdisciplinary collaboration is crucial to harness the full potential of these approaches. Looking ahead, the future of cybernetics and systems theory is promising. Advancements in artificial intelligence and machine learning will likely enhance the understanding and control of complex systems. Moreover, with increasing global challenges, these approaches hold immense potential in solving intricate problems, such as climate change, socio-economic inequalities, and healthcare disparities.

Conclusion:

In conclusion, cybernetics and systems theory offer valuable perspectives on understanding and managing complex systems. The synergy between these fields empowers us to navigate the intricacies of interconnected entities, allowing for better decision-making, problem-solving, and innovation across various domains. By embracing the principles of cybernetics and systems theory, we equip ourselves to tackle the challenges of a dynamically interconnected world.

IP ADDRESS

SHANTHA KUMARI J
(22MCA35)

What is an IP Address?

An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate. Computers that communicate over the internet or via local networks share information to a specific location using IP addresses.

IP addresses have two distinct versions or standards. The Internet Protocol version 4 (IPv4) address is the older of the two, which has space for up to 4 billion IP addresses and is assigned to all computers. The more recent Internet Protocol version 6 (IPv6) has space for trillions of IP addresses, which accounts for the new breed of devices in addition to computers. There are also several types of IP addresses, including public, private, static, and dynamic IP addresses.

Every device with an internet connection has an IP address, whether it's a computer, laptop, IoT device, or even toys. The IP addresses allow for the efficient transfer of data between two connected devices, allowing machines on different networks to talk to each other.

How does an IP Address work?

An IP address works in helping your device, whatever you are accessing the internet on, to find whatever data or content is located to allow for retrieval.

Common tasks for an IP address include both the identification of a host or a network, or identifying the location of a device. An IP address is not random. The creation of an IP address has the basis of math. The Internet Assigned Numbers Authority (IANA) allocates the IP address and its creation. The full range of IP addresses can go from 0.0.0.0 to 255.255.255.255.

With the mathematical assignment of an IP address, the unique identification to make a connection to a destination can be made.

IPv4 vs IPv6: What's the difference?

Both IPv4 and IPv6 identify connected devices on the network. However, there are slight differences in the way they operate. IPv6 is the newer IP version and was introduced to address the limitations IPv4 posed on the availability of IP addresses.

The following is a list of differences between IPv4 and IPv6:

- IPv4 is 32-bit, whereas IPv6 is 128-bit.
- In IPv4, binary bits are separated by a dot (.); IPv6 separates binary bits by a colon (:).
- IPv4 follows the numeric addressing method and IPv6 is alphanumeric.
- IPv4 offers 12 header fields and IPv6 offers eight header fields.
- IPv4 has checksum fields but IPv6 doesn't.
- IPv4 supports broadcast address, which is a type of special address that transmits data packets to every node on the network. IPv6 doesn't support broadcast, but instead uses a multicast address, which is a logical identifier for a collection of hosts on a network.
- IPv4 supports Variable Length Subnet Mask, but IPv6 doesn't.
- When mapping to media access control addresses, IPv4 uses the Address Resolution Protocol. IPv6 uses the Neighbor Discovery Protocol, which uses stateless auto-configuration and address resolution.

Types of IP Address:

Here is a list of the five most common types of IP addresses:

1. Private IP addresses

Each device connected to a home network or a private network carries a private IP address. Private IP addresses are non-internet facing and are only used on an internal network. Devices with private IP addresses might include computers, tablets, smartphones, Bluetooth devices, smart TVs and printers. With the increasing popularity of internet of things products, the use of private IP addressing is likely to keep growing.

2. Public IP addresses

An ISP assigns these addresses, which enable a router to communicate with the internet or an outside network. Public IP addresses cover the entire network, meaning multiple devices sharing the same internet connection will also share the same public IP address.

3. Dynamic IP addresses

These IP addresses are constantly changing and a new dynamic IP address is assigned to a device every time it connects to the internet. ISPs buy large pools of IP addresses to assign to their customers automatically. They revolve and reuse these addresses between different customers to generate cost savings and to provide easier network management. A dynamic IP address also offers security benefits, as it's harder for cybercriminals to hack into a network interface if its IP is constantly changing.

4. Static IP addresses

Unlike dynamic IP addresses, static IP addresses never change once they're assigned by the network. While most internet users and businesses don't require static IP addresses, they're a requirement for businesses that wish to host their own web servers. A static IP address ensures that all websites and email addresses associated with a certain web server will always have a consistent IP address so it can be reached on the internet.

5. Website IP addresses

These are IP addresses for website owners who don't host their websites on their own servers but rely on a hosting company to do so. Website IP addresses are composed of the following two types:

Shared. This IP address is shared among many different websites and is mostly used by small businesses that use a managed hosting service, such as WordPress.

Dedicated. This is a unique IP address assigned to an individual website. Dedicated IP addresses help website owners avoid getting blocked or blacklisted, something that owners of shared IP addresses might face when malicious behavior is exhibited by other websites sharing the same IP. Owners of dedicated IP addresses can access their websites while waiting for a domain transfer.

Conclusion:

IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. IP Address is used for communication between two or more different devices within/outside the network using TCP/IP protocol to locate and administrate devices using Internet Service Provider (ISP).

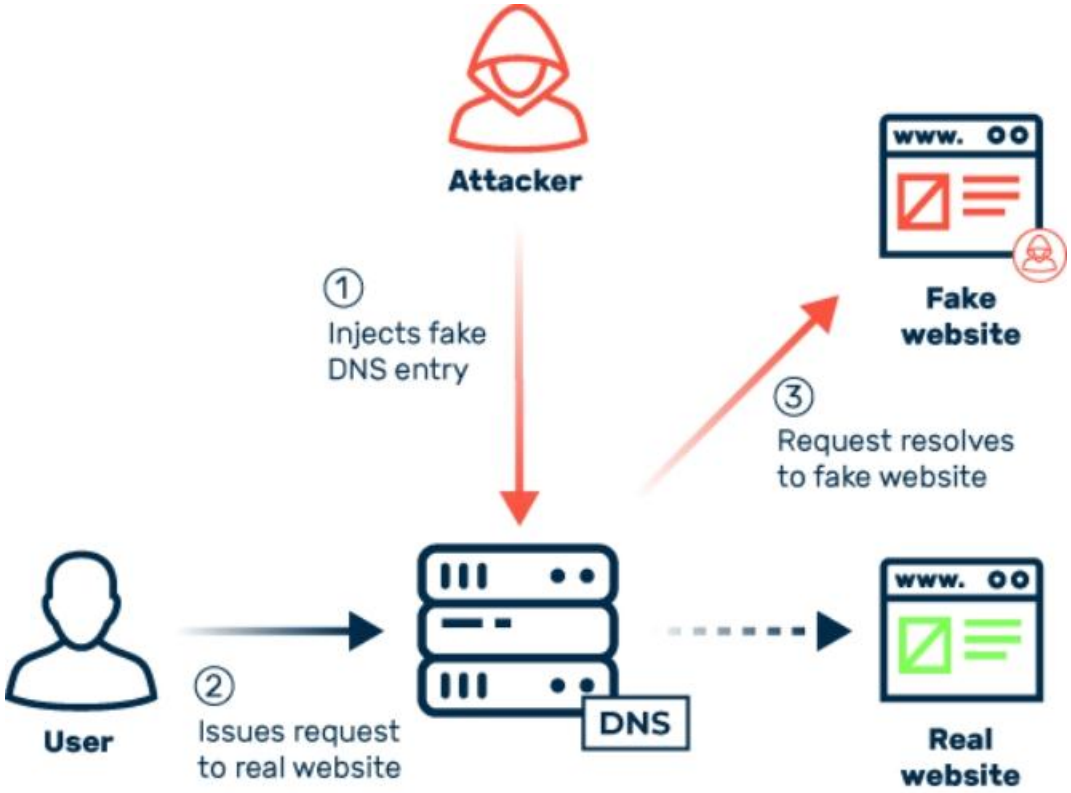
TYPES OF DNS ATTACKS AND TACTICS FOR SECURITY

POOJA SRI R
(22MCA30)

DNS (Domain Name Server) is a prominent building block of the Internet. It's developed as a system to convert alphabetical names into IP addresses, allowing users to access websites and exchange e-mails. DNS is organized into a tree-like infrastructure where the first level contains topmost domains, such as .com and .org. The second-level nodes contain general, traditional domain names. The 'leaf' nodes on this tree are known as hosts.

DNS works similarly to a database that is accessed by millions of computer systems in trying to identify which address is most likely to solve a user's query.

In DNS attacks, hackers will sometimes target the servers which contain the domain names. In other cases, these attackers will try to determine vulnerabilities within the system itself and exploit them for their own good.



Types of Attacks:

1. **Denial of service (DoS):** An attack where the attacker renders a computer useless (inaccessible) to the user by making a resource unavailable or by flooding the system with traffic.
2. **Distributed denial of service (DDoS):** The attacker controls an overwhelming amount of computers (hundreds or thousands) in order to spread malware and flood the victim's computer with unnecessary and overloading traffic. Eventually, unable to harness the power necessary to handle the intensive processing, the systems will overload and crash.
3. **DNS spoofing (also known as DNS cache poisoning):** An attacker will drive the traffic away from real DNS servers and redirect them to a "pirate" server, unbeknownst to the users. This may cause the corruption/theft of a user's personal data.
4. **Fast flux:** An attacker will typically spoof his IP address while performing an attack. Fast flux is a technique to constantly change location-based data in order to hide where exactly the attack is coming from. This will mask the attacker's real location, giving him the time needed to exploit the attack. Flux can be single or double or of any other variant. A single flux changes the address of the webserver while double flux changes both the address of the web server and the names of DNS serves.
5. **Reflected attacks:** Attackers will send thousands of queries while spoofing their own IP address and using the victim's source address. When these queries are answered, they will all be redirected to the victim himself.
6. **Reflective amplification DoS:** When the size of the answer is considerably larger than the query itself, a flux is triggered, causing an amplification effect. This generally uses the same method as a reflected attack, but this attack will overwhelm the user's system's infrastructure further.

sures against Attacks:

- Use digital signatures and certificates to authenticate sessions in order to protect private data.
- Update regularly and use the latest software versions, such as BIND. BIND is open-source software that resolves DNS queries for users. It is widely used by a good majority of the DNS servers on the Internet.
- Install appropriate patches and fix faulty bugs regularly.
- Replicate data in a few other servers, so that if data is corrupted/lost in one server, it can be recovered from the others. This could also prevent single-point failure.
- Block redundant queries in order to prevent spoofing.
- Limit the number of possible queries.