JYOTI NIVAS COLLEGE
POST GRADUATE CENTRE

DEPARTMENT OF MCA

1 YEAR

TECH - ON - TAP

E -JOURNAL

ON

COMPUTER NETWORKS

ISSUE: 5

JANUARY 2021

CRYPTOCURRENCY

JOICE RANI J (20MCA16)
S V TEJASHREE (20MCA31)

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology a distributed ledger enforced by a disparate network of computers.

CRYPTO TOKEN

A blockchain account can provide functions other than making payments, for example in decentralized applications or smart contracts. In this case, the units or coins are sometimes referred to as crypto tokens (or cryptotokens). Cryptocurrencies are generally generated by their own blockchain like Bitcoin and Litecoin whereas tokens are usually issued within a smart contract running on top of a blockchain such as Ethereum.

BITCOIN SYSTEM

Bitcoin is a cryptocurrency based on accounting entries. Therefore, bitcoins should not be seen as digital tokens but as the balance of a Bitcoin account. A Bitcoin account is defined by an elliptic curve cryptography key pair. The Bitcoin account is publicly identified by its Bitcoin address, obtained from its public key. Using this public information, users can send bitcoins to that address.

REFERENCES:

https://www.hindawi.com/journals/misy/2018/2159082/
https://en.wikipedia.org/wiki/Cryptocurrency

NAMED DATA NETWORKING (NDN)

AMRUTHA MB (20MCA02)
VIJAYALAKSHMI Y (20MCA43)

Named Data Networking (related to content-centric networking (CCN), content-based networking, data-oriented networking or information-centric networking (ICN)) is a proposed Future Internet architecture inspired by research into network usage and a growing awareness of unsolved problems in contemporary internet architectures like IP.

NDN has three core concepts that distinguish NDN from other network architectures. First, applications name data and data names will directly be used in network packet forwarding; consumer applications request desired data by its name, so communications in NDN are consumer-driven. Second, NDN communications are secured in a data-centric manner, i.e. each piece of data (called a Data packet) will be cryptographically signed by its producer and sensitive payload or name components can also be encrypted for the purpose of privacy. Third, NDN adopts a stateful forwarding plane where forwarders will keep a state for each data request (called an Interest packet) and erase the state when a corresponding Data packet comes back; this forwarding allows intelligent forwarding strategies and eliminates loop.

REFERENCES:

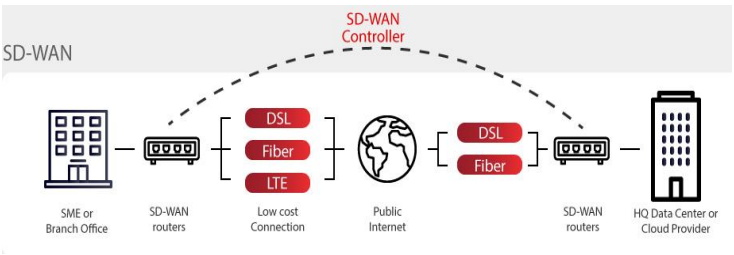
https://en.wikipedia.org> wiki> named_data_networking
https://www.networkworld.com/article/3313338/introducing-named-data-networking.html

SD-WAN: THE NEW WAN NORM

M KOMAL SINGH (20MCA20)
SUSHEELA R (20MCA36)

A software-defined wide-area network (SD-WAN) is networking technology that offers greater flexibility for companies than previous WAN systems. SD-WAN simplify the management and operation of a WAN by decoupling the networking hardware from its control mechanism. SD-WAN add cloud-based applications to the mix, allowing employees to remotely gain entry to enterprise-wide programs like Salesforce, Amazon Web Services, and Microsoft 365.

WHY SWITCH TO SD-WAN?



The traditional WAN's (wide-area network) function was to connect users at the branch or campus to applications hosted on servers in the data centre. Typically, dedicated MPLS circuits were used to help ensure security and reliable connectivity. This doesn't work in a cloud-centric world.

While businesses adopt to the use of SaaS and infrastructure-as-a-service (IaaS) applications in multiple clouds, IT is realizing that the user application experience is poor. That is because WANs designed for a different era are not ready for the unprecedented explosion of WAN traffic that cloud adoption brings. That traffic causes management complexity, application-performance unpredictability, and data vulnerability.

THE NEW WAN & IT'S BENEFITS

SD-WAN address the current IT challenges. This new approach to network connectivity can lower operational costs and improve resource usage for multisite deployments. Network administrators can use bandwidth more efficiently and can help ensure high levels of performance for critical applications without sacrificing security or data privacy. SD-WAN takes the process of a WAN a step further, using Long Term Evolution (LTE) and broadband internet services to provide access.

With SD-WAN, IT can deliver routing, threat protection, efficient offloading of expensive circuits and simplification of WAN network management. Business benefits include: Better application experience, more security, Optimized cloud connectivity and Simplified management.

Considering all the above mentioned facts, it absolutely makes a lot of sense for business and enterprises to adapt to SD-WAN. SD-WAN will likely become the new norm. SD-WAN is here and it's here to stay.

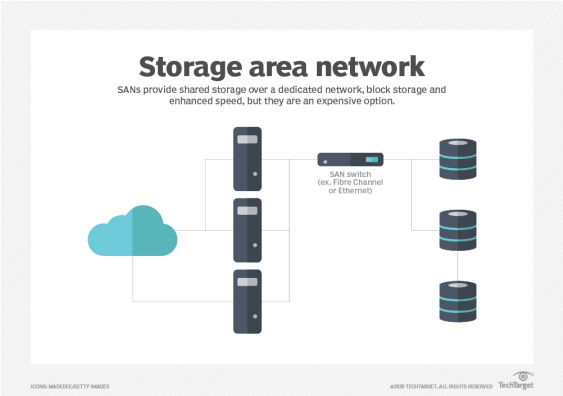
REFERENCES:

https://www.silver-peak.com/sd-wan/sd-wan-explained
https://www.riverbed.com/in/solutions/sd-wan.html
https://youtu.be/u2N7q1w26Mg

SAN: STORAGE AREA NETWORK

GUDIYA KUMARI (20MCA12)
VIDYA RATHOD (20MCA42)

A storage area network (SAN) is a dedicated high-speed network or sub network that interconnects and presents shared pools of storage devices to multiple servers.
SAN technology addresses advanced enterprise storage demands by providing a separate, dedicated, highly scalable high-performance network designed to interconnect a multitude of servers to an array of storage devices. The storage can then be organized and managed as cohesive pools or tiers. A SAN enables an organization to treat storage as a single collective resource that can also be centrally replicated and protected, while additional technologies, such as data de-duplication and RAID, can optimize storage capacity and vastly improve storage resilience -- compared to traditional direct-attached storage (DAS).



WHAT STORAGE AREA NETWORKS ARE USED FOR?

A SAN can improve storage availability. Because a SAN is essentially a network fabric of interconnected computers and storage devices, a disruption in one network path can usually be overcome by enabling an alternative path through the SAN fabric.
A SAN can support a huge number of storage devices, and storage arrays -- specially designed storage subsystems -- that support a SAN can scale to hold hundreds or even thousands of disks.
There are two principal types of networking technologies and interfaces employed for SANs: Fibre Channel and iSCSI.

REFERENCES:

https://searchstorage.techtarget.com/definition/storage-area-network-SAN
https://www.netapp.com/data-storage/what-is-san-storage-area-network/

NETWORK FABRIC

ASWATHI MOHAN (20MCA04)
SUPRIYA R (20MCA35)

A network fabric is a type of network topology where all nodes, in this case switches and endpoints are interconnected to all other nodes. This is commonly depicted as a matrix that resembles a woven square, thus the term “fabric”. Network fabrics are traditionally associated with data centers, though they have become part of WANs as well. Ethernet network fabrics are one of the two modern network fabrics. They use industry-standard protocols and Ethernet switches. There are two major types of Ethernet network fabrics, the shortest path bridging (SPB) and the transparent Interconnection of lots of links (TRILL).The other kind of modern network fabric is an IP fabric, which uses border gateway protocol (BGP) and Ethernet virtual private networks (EVPNs). The benefits of having a modern network fabric are based on network functions virtualization (NFV).

BENEFITS OF USING A VIRTUALIZED NETWORK FABRIC

Virtualizing a network fabric means manual configuration can become a thing of the past, for the most part. In traditional non-virtualized networks, administrators would have to manually configure every switch in the network through a command-line interface (CLI). Virtualized network fabrics allow administrators to use automation to make changes and reconfigure nodes in modern networks. The virtualization of network fabrics brings benefits that include making a network easier to configure, use, secure, and keep running. Large-scale configurations can be done through a network configuration tool like Puppet, which can be part of an SD-WAN vendor’s management system. Shifting traditional network architecture to a network fabric topology means there is improved resiliency, because if part of the network goes down for any reason, then there are still paths to get to endpoints. Additionally, when a rolling update is released, individual nodes are not taken out of service because one switch can remain functioning while the other is updated. A major aspect of network security possible with modern virtualized network fabrics is network segmentation. A network with a modern fabric topology uses algorithms in its software to determine the shortest path for traffic to cross while heading to its destination.

REFERENCES:

https://www.commscope.com/blog/2018/what-is-a-network-fabric-and-is-it-the-same-as-a-campus-fabric/
https://www.sdxcentral.com/networking/virtualization/definitions/what-is-network-fabric-definition/

MEDIA GATEWAY CONTROL PROTOCOL (MGCP)

PRANATHI R (20MCA27)
SWATHI N (20MCA37)

Media Gateway control protocol (MGCP), commonly known as H.248 is a standard protocol for handling the signalling and session management needed during a multimedia conference. MGCP is used in voice over IP telecommunication systems. This happens when call-control devices use a plain-text protocol, MGCP to manage IP Telephony gateways. The advantage of this is that it creates a centralized gateway administration and provides for largely scale-able IP Telephony solutions. The state of each individual port on the gateway is known as controller. This allows complete control of the dial plan and gives per-port control of connections to the public switched telephone network (PSTN), legacy PBX, voice mail systems, plain old telephone services (POTS) phones, and so forth.

MGCP

MGCP Media Gateway Control Protocol provides the reformation of normal electronic voice communication to IP based voice communication. MGCP presents call control architecture with limited intelligence at edge (endpoints, media gateways) and intelligence at the core controllers. The call agent uses MGCP to request event notifications, reports, status, and configuration data from the media gateways, as well as to specify connection parameters and activation of signals towards the PSTN telephony interface.

VOIP terminology involves some common terms related to VOIP communication over the TCP/IP network or internet. The first term related to VOIP is Session initiation protocol SIP. SIP initiated the sessions between different clients to provide connectivity so the clients can make VOIP call with each other. The connection can be initiated, modified or terminated by SIP protocol. CODEC are uses to compress the VOIP data on the network to save the bandwidth.

MGCP protocol used nine standard commands. These commands are the combination of four letters. AUEP, AUCX, CECX, DLCX, EPCF, MDCX, NTFY, RQNT, and RSIP are nine commands. Response code tells about the results of event.

REFERENCES:

https://ccnatutorials.in/application-layer-of-tcp-ip/mgcp-media-gateway-control-protocol/
https://en.m.wikipedia.org/wiki/Media_Gateway_Control_Protocol
https://ccnatutorials.in/application-layer-of-tcp-ip/mgcp-media-gateway-control-protocol/

ADVANCED ENCRYTION STANDARD (AES)

BHOOMIKA.S (20MCA06)
HERMAIN.K. S (20MCA15)

ADVANTAGES OF AES

As it is implemented in both hardware and software, it is most robust security protocol.
➨It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.
➨It is most common security protocol used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.
➨It is one of the most spread commercial and open-source solutions used all over the world.
➨No one can hack your personal information.
➨For 128 bits, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol. at each stage of a round. All stages of each round are reversible.

DISADVANTAGES OF AES

It uses too simple algebraic structure.
➨Every block is always encrypted in the same way.
➨Hard to implement with software.
➨AES in counter mode is complex to implement in software taking both performance and security into considerations.

ANALYSIS OF AES:

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

REFERENCES:

https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

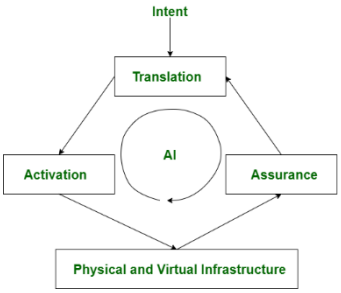
INTENT BASED NETWORKING (IBN)

DAINY JOSE (20MCA09)
MEERA RAMDAS. E (20MCA22)

Intent-based networking (IBN) is a systematic approach to bind infrastructure management and business intent. It is a network management approach in which artificial intelligence (AI) and machine learning (ML). In the IBN approach, the network can translate the intents into network polices. The input to input to IBN is provided either with the help of API (Application Program Interface) or through the Graphical User Interface (GUI).

WORKING:

IBN is an extension of software-defined networking (SDN). It consists of a network controller that acts as a central control point for the network by managing the distributed devices present across the network. The central abstraction along with the integration.



There are tree functional blocks of IBN namely-

Translation: The translation block can capture and translate business intents into polices across the system.
Assurance: The activation block is responsible for the end-to-end verification of the wide network. It predicts the changes which have taken place concerning the original intent and then provides recommendations to fix it. This recommendation process is solely carried out by the AI and ML which is incorporated in this network. Here the security and performance factors of the network are studied constantly and necessary re-configuration are made if required.
Activation: After specifying the intent and the development of policies, the activation block makes use of network-wide automation to verify the configuration of the devices before their deployment.

APPLICATIONS:

IBN system can help in performance testing of an application. It can provide high security to the application by the support of AI and ML algorithms. IBN system also provides a firewall to web application which can help in Internet traffic and also enhance security measures.

EXAMPLE:

Cisco Digital Network Architecture (Cisco DNA) is an example of an IBN network.

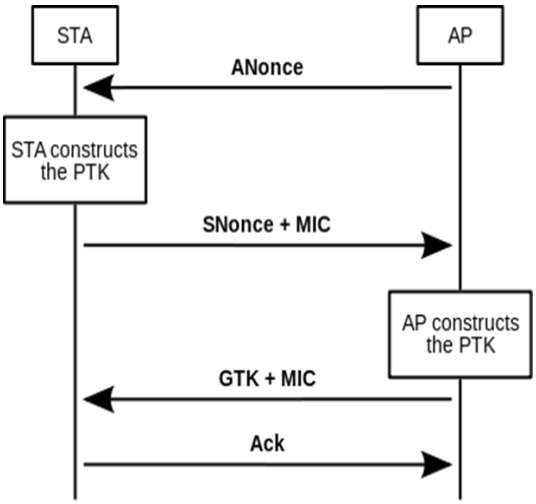
REFERENCES:

https://www.geeksforgeeks.org/intent-based-networking-ibn/?ref=rp
https://whatis.techtarget.com/definition/intent-based-networking-IBN

WIRELESS 4-WAY HANDSHAKE

RAMYA KP (20MCA29)
RAMYA S (20MCA30)

A 4-way handshake is a type of network authentication protocol established by IEEE-802.11i that involves standard set up for the construction and use of wireless local area networks (WLANs). The four-way handshake provides a secure authentication strategy for data delivered through network architectures.



The 4-way handshake is the process of exchanging 4 messages between an access point(authentication) and the client device (supplicant) to generate some encryption keys which can be used to encrypt actual data sent over wireless medium. The four-way handshake is designed so that the access point (or authentication) and wireless client (or supplicant) can independently prove to each other that they know the PSK/PMK, without ever disclosing the key, the Access Point (AP) and client encrypt messages to each other-that can only be decrypted by using the PMK that they already share-and if decryption of the messages was successful, this proves knowledge of the PMK. The four-way handshake is critical for protection of the PMK from malicious access points-for example, an attacker's SSID impersonating a real access point-so that the client never has to tell the access point its PMK.

The PMK is designed to last the entire session and should be exposed as little as possible, therefore, keys to encrypt the traffic need to be derived. A four-way handshake is used to establish another key called the Pairwise Transient Key (PTK). The PTK is generated by concatenating the following attributes. PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, address, and STA MAC address. The product is then put through a pseudo-random function. The handshake also yields the GTK(Group Temporal Key),used to decrypt multicast and broadcast traffic.

REFERENCES:

https://en.wikipedia.org/wiki/IEEE_802.11i-2004
https://www.techopedia.com/definition/27188/four-way-handshake#:~:text=A%20four%2Dway%20handshake%20is,data%20delivered%20through%20network%20architectures

HONEYPOT- THE SWEET SPOT IN NETWORK SECURITY

SANDHYA M-20MCA32
SUDAGANI SAI SARIKA-20MCA34

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers.

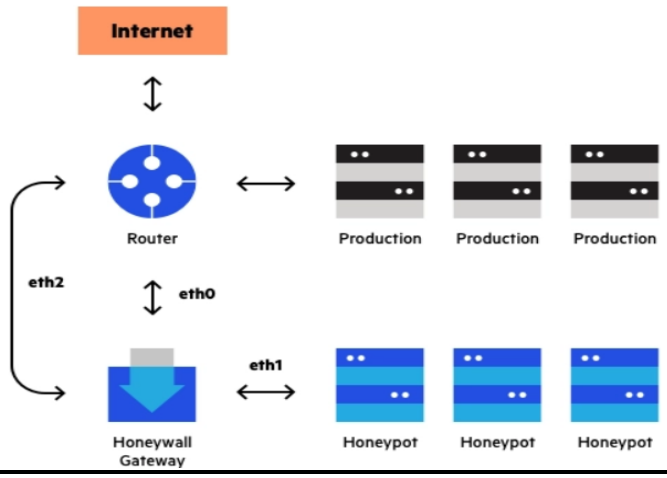
Honeypots are a type of deception technology that allows you to understand attacker behavior patterns. Security teams can use Honeypots to investigate cyber security breaches to collect intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cyber security measures, because they are unlikely to attract legitimate activity.

Honeypots vary based on design and deployment models, but they are all decoys intended to look like legitimate, vulnerable systems to attract cybercriminals.

Types of Honeypot Deployments are Pure Honeypots, Low-interaction Honeypots and High-interaction Honeypots.

HONEYNET: A NETWORK OF HONEYPOTS

A honeynet is a combination of two or more honey pots on a network.



REFERENCES:

https://www.imperva.com/learn/application-security/honeypot-honeynet/
https://searchsecurity.techtarget.com/definition/honey-pot/

FRAME RELAY

SHARMILA S (20MCA33)
THANUJA C (20MCA40)

Frame relay is standardized wide area network technology that specifies the physical and data link layer of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Service Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces. Network providers commonly implement Frame Relay for voice and data as an encapsulation technique used between local area network (LANs) over a wide area network (WAN). Each end-user gets a private line (or leased line) to a Frame Relay node. The Frame Relay network handles the transmission over a frequently changing path transparent to all end-user extensively used WAN protocols. It is less expensive than leased lines and that is one reason for its popularity.

Frame Relay often serves to connect local area network (LANs) with major backbones, as well as on public wide-area networks (WANs) and also in private network environments with leased lines over T-1 lines. It requires a dedicated connection during the transmission period. Frame Relay does not provide an ideal path for voice or video transmission, both of which require a steady flow of transmissions. However, under certain circumstances, voice and video transmission do use Frame Relay. Frame Relay originated as an extension of integrated services digital network (ISDN). Its designers aimed to enable a packet-switched network to transport over circuit-switched technology. The technology has become a stand-alone and cost-effective means of creating a WAN. Frame Relay switches create virtual circuits to connect remote LANs to a WAN. The Frame Relay network exists between a LAN border device, usually a router, and the carrier switch. The technology used by the carrier to transport data between the switches is variable and may differ among carriers.

Frame Relay began as a stripped-down version of the X.25 protocol, releasing itself from the error-correcting burden most commonly associated with X.25. When Frame Relay detects an error, it simply drops the offending packet. Frame Relay uses the concept of shared access and relies on a technique referred to as "best-effort", whereby error-correction practically does not exist and practically no guarantee of reliable data delivery occurs. Frame Relay provides an industry-standard encapsulation, utilizing the strengths of high-speed, packet-switched technology able to service multiple virtual circuits and protocols between connected devices, such as two routers. Although Frame Relay became very popular in North America, it was never very popular in Europe. X.25 remained the primary standard until the wide availability of IP made packet switching almost obsolete. It was used sometimes as backbone for other services, such as X.25 or IP traffic. X.25 prepares and sends packets, while Frame Relay prepares and sends frames. X.25 packets contain several fields used for error checking and flow control, most of which are not used by Frame Relay.

REFRENCES:

https://en.wikipedia.org/wiki/Frame_Relay
https://ecomputernotes.com/computernetworkingnotes/network-technologies/frame-relay

IMAGESNET

MAHIMA I (20MCA21)
HARSHITHA M (20MCA14)

ImageNet is a large database or dataset of over 14 million images. It was designed by academics intended for computer vision research. These images have been hand-annotated by the project to indicate what objects are pictured and in at least one million of the images, bounding boxes are also provided. ImageNet uses the hierarchical structure of WordNet. Each meaningful concept in WordNet, possibly described by multiple words or word phrases, is called a "synonym set" or "synset". There are around 80, 000 noun synsets in WordNet.
This ImageNet is useful for many computer vision applications such as object recognition, image classification and object localization. The images for ImageNet were collected from various online sources. ImageNet doesn't own the copyright for any of the images. This has implication on how ImageNet shares the images to researchers.ImageNet consists of 14,197,122 images organized into 21,841 subcategories. These subcategories can be considered as sub-trees of 27 high-level categories. Thus, ImageNet is a well-organized hierarchy that makes it useful for supervised machine learning tasks.

REFERENCES:

http://www.image-net.org/papers/imagenet_cvpr09.pdf
https://devopedia.org/imagenet

NETWORK SECURITY

CHINMAYI K P (20MCA08)
LAVANYA ACHARYA (20MCA18)

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.

VULNERABILITIES & ATTACKS

The common vulnerability that exists in both wired and wireless networks is an "unauthorized access" to a network. An attacker can connect his device to a network however unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection.

TYPES OF NETWORK SECURITY

- Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components.
- Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network.
- Administrative security controls consist of security policies and processes that control user behavior.

REFERENCES:

https://www.tutorialspoint.com/network_security/network_security_overview.htm
https://www.cisco.com/c/en_in/products/security/what-is-network-security.html

WIFI-6

RACHANA K Y (20MCA28)
ANJU S M (20MCA03)

Wi-Fi-6 is the newest version of Wi-Fi and is based on the IEEE 802.11ax standard. it provides a number of advantages over older Wi-Fi technology which we will discuss shortly. It is accompanied by a new naming convention that is designed to enable users easily understand the type of devices they are using. The Wi-Fi generation name is linked to the IEEE standard that they support.

WIFI-6

Wi-Fi is more than just a new named and a set labelling conventions. Each generation of wifi has provided greater data transfer speed and wifi-6 is no exception. The theoretical speed of WiFi-6 is 10Gbps.It achieves this speed increase by combining the 2.4GHx and 5GHx spectrum bands and employing MU-MIMO technology for both uplink and downlink data transfers. A single device can achieve up to 40% faster data transfer when using WiFi-5.Even 2.4GHx networks will experience increased speeds when using WiFi-6 router. Battery life is extended through a feature known as target wake time (TWT).TWT enables the Wi-Fi access point to communicate with your device to tell it when exactly to turn its Wi-Fi radio to wake up and go to sleep. Wi-Fi performance can be negatively affected is when it is used in crowded areas where there is competition for the signal. One way this is accomplished is with a technology known as Orthogonal Frequency Division Multiple (OFDMA).this allows wireless channel to be divided into a number of sub-channels that can be used to carry data for a different device. This allows a single access point to communicate with more devices simultaneously. Improvements in Multiple In/Multiple out (MIMO) capabilities now allow a router with multiple antennas to both send and receive data transmission from multiple devices at the same time.WiFi-5 could only send, but not receive multiple signals at once.

WiFi6 Router Rax80 Ax6000 8 stream
fig.1

ex.TP-Link Archer AX6000.fig.2

REFERENCES:

https://www.netspotapp.com/what-is-wifi-6.html
https://www.mobilesportsreport.com/2019/11/wi-fi-6-research-report-download-it-now/

HOW LEADERS ACROSS INDUSTRIES SEE 5G HELPING THEIR BUSINESSES

MISBA RAFIA KHANUM (20MCA23)
NEHA KOUSER (20MCA24)

A report from Verizon on business leaders opinion of 5G finds that 5G adoption is well underway across industries, but the reasons for excitement and the ways in which business plan to deploy 5G tech vary greatly. The report surveyed 700 business tech decision-makers, and found that 55% had heard, read, or seen a lot about 5G, and 80% believe it will create new opportunities for their companies. The belief in 5G benefits for business extends to believing that 5G will benefit their individual industries and roles, with 79% saying they agreed with both statements.

There was some split between IT leaders and C-level executives on whether 5G is a top priority: 54% of IT leaders said it was, while only 39% of the C-suite agreed.

Another large difference appeared between business leaders and general public: As mentioned above, 55% of business tech decision-makers said they had heard a lot about 5G, while only 23% of the US adults said the same. This cloud indicates the knowledge gap that drags 5G progress down, or otherwise slows customer adoption of the new technology. Regardless business leaders seem eager to incorporate 5G into their organizations, both internally and externally.

In the entertainment, sports and media industries, most of the excitement comes from the sheer amount of bandwidth that 5G will be able to deliver. Eighty four percent of respondents said they believe 5G would eliminate “miles of cables and wiring”, and the same amount said they were excited by high bandwidth connections allowing for multiple broadcast and video streams. The public sector sees 5G value in real-time video surveillance and public safety programs.

In the healthcare world, remote health monitoring technology leads as the most valuable tech, with 80% saying they find its potential valuable.

In summing up the report said the data points to 5G has become top-of-mind foe business as they manage through condensed digital transformation timelines. These findings underscore the critical role 5G will play in economic recovery and growth.

REFERENCES:

Techrepublic.com/article/how-leaders-across-industries-see-5g-helping-their-businesses/

FIREWALL

HARSHA P C (20MCA13)
SWETHA M (20MCA39)

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and entrusted outside networks, such as the Internet.
A firewall can be hardware, software, or both.

FIREWALL

The purpose of firewall is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

HOW FIREWALL WORKS:

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers.

REFERENCES:

https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network
https://www.forcepoint.com/cyber-edu/firewall
https://www.cisco.com/c/en_in/products/security/firewall

DIGITAL TWIN

EMILIN MERIA JAMES (20MCA10)
NEHA SREESHKUMAR (20MCA25)

A digital twin is the generation or collection of digital data representing a physical object. The concept of digital twin has its roots in engineering and the creation of engineering drawings/graphics. Digital Twins are the outcome of continuous improvement in the creation of product design and engineering activities. Product drawings and engineering specifications progressed from handmade drafting to computer aided drafting/computer aided design (CAD) to model-based systems engineering (MBSE).
The digital twin of a physical object is dependent on the digital thread**.** A digital thread is the lowest level component of a digital twin and the "twin" is dependent on the digital thread to maintain accuracy. Changes to product design are implemented using Engineering Change Orders (ECO). An ECO made to a component item will result in a new version of the item's digital thread, and correspondingly to the digital twin.

TYPES OF DIGITAL TWIN

- Digital Twin Prototype (DTP)**:** It consists of the designs, analyses, and processes to realize a physical product and it exists before there is a physical product.
- Digital Twin Instance (DTI)**:** It is the digital twin of each individual instance of the product once it is manufactured.
- Digital Twin Aggregate (DTA)**:** It is the aggregation of DTIs whose data and information can be used for interrogation about the physical product, prognostics, and learning.

EXAMPLE

1. Digital twins are used to optimize machines is with the maintenance of power generation equipment such as power generation turbines, jet engines and locomotives.
2. Digital twins are the use of 3D modelling to create digital companions for the physical objects.
3. Digital twin also can be used for monitoring, diagnostics and prognostics to optimize asset performance and utilization.

REFERENCES:

https://www.google.com/url?sa=t&source=web&rct=j&url=https://en.m.wikipedia.org/wiki/Digital_twin
https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.ge.com/digital/applications/digitaltwin

NETWORK ARCHITECTURE METHODOLOGY

POOJA M (20MCA26)
GOPIKA S (20MCA11)

Network Architecture focuses specific design patterns to implement modularity and specifically hierarchical design to create a modular network design .Network design reaches beyond hub and topologies at the module level and provides general methods of design that provide for the best overall network design. This section discusses each of these methods or rules. The first general rule in hierarchical network design is to assign each module a single function. In networking terms a function is a user connection a form of traffic admission control, this is most often an edge function in the network. Here, traffic offered to the network by connected devices is checked for policy errors, marked for quality of service processing, managed in terms of flow rate and prodded to ensure the traffic is handled properly throughout the network.

Here the edge function can be double sided; however, not only must the network decide what traffic should be accepted from connected devices, it must also decide what traffic should be forwarded towards the services. Stateful packet filters, policy implementations and other security functions are common along service connection edges. Traffic aggregation usually occurs at the edge of a module or a sub topology within a network module. Traffic aggregation is where smaller links are combined into bigger ones, such as the point where a higher-speed local area network meets a lower-speed wide area link.

Traffic can be shaped and processed based on the QoS markings given to packets at the network edge to provide effective aggregation services. Traffic forwarding specifically between modules or over longer geographic distances, this is a function that's important enough to split off into a separate module; generally this function is assigned to core modules whether local, regional or global. Control plane aggregation should happen only at module edges. Aggregating control plane information separates failure domains and provides an implementation point for control plane policy.

REFERENCES:

https://www.informit.com/

3D-DOCTOR

BABY (20MCA05)
K M POOJA MAURYA (20MCA17)

ABSTRACT

- 3D-DOCTOR Software is used to extract information from image files to create 3D model.
- It was developed using object-oriented technology and provides efficient tools to process and analyse 3D images, object boundaries, 3D models.
- INTRODUCTION:
- 3D-DOCTOR is an advanced, 3D imaging software developed by Able Software Corp. It is advanced 3D modelling, image processing and measurement software for MRI, CT, PET, microscopy, scientific, and industrial imaging applications.
- 3D-Doctor supports both greyscale and colour images stored in DICOM, TIFF, Interfile, GIF, JPEG, PNG, BMP, PGM, RAW and other image file formats.

3D-DOCTOR BASIC

- 3D- images such as CT, MRI and microscopy images.
- DOCTOR uses its unique vector-based technologies to create better 3D models from volumetric Unique vector-based technologies for better 3D model creation and easy editing.

TECHNOLOGY

- object oriented technologies
- advance 3d image processing

3D MEASUREMENTS

- Object volume and Object surface area
- Object surface area
- Length on 3D object and Digitize 3D points
- Crop 3D object and Cut 3D object

CONCLUSION

- 3D-DOCTOR Software has been one of the tremendous analysis software that is use to extract information from image files to create 3D model. It provides engineering team.
- More accurate analysis for internal human parts and also create visual models for complex blood vessel.

REFERENCES:

www.seminarsonly.com
https://www.3d-doctor.com

STEGANOGRAPHY

S SWATHI (20MCA38)
V UVARANI (20MCA41)

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of Steganography can be combined with encryption as an extra step for hiding or protecting data.

The word *Steganography* is derived from the Greek words *steganos* (hidden) and the Greek root *graph* (*write*). Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through Steganography -- called *hidden text* -- is often encrypted before being incorporated into the innocuous-seeming *cover text* file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content. Steganography is practiced by those wishing to convey a secret message or code.

While there are many legitimate uses for Steganography, malware developers have also been found to use Steganography to obscure the transmission of malicious code. Forms of Steganography have been used for centuries and include almost any technique for hiding a secret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoffensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information. In modern digital Steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as a JPEG image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data.

The practice of adding a watermark -- a trademark or other identifying data hidden in multimedia or other content files -- is one common use of Steganography. Watermarking is a technique often used by online publishers to identify the source of media files that have been found being shared without permission. While there are many different uses of Steganography, including embedding sensitive information into file types, one of the most common techniques is to embed a text file into an image file. When this is done, anyone viewing the image file should not be able to see a difference between the original image file and the encrypted file; this is accomplished by storing the message with less significant bites in the data file. This process can be completed manually or with the use of a Steganography tool.

REFERENCES:

https://arxiv.org
https://www.uKessyays.com