Q:1:~

Sol

The internet is a global network of devices & computers connecting to one another using established protocols. It makes it easier for people to share resources, services, & information across regional borders. its importance system from its ability to facilitate instantaneous communication, access to a wealth of information, online collaboration, e-commerce, social networking, & a plethora of other applications that have revolutionized nearly every facet of contemporary life, including business, government, education, healthcare, & entertainment. it is now a vital instrument for global economic progress, innovation, & connectedness.

Q:2:~

Sol

The network edge includes various components that facilitate communication between & end-users & the internet. These components includes:

- End-Systems: Devices that generate & utilize data on a network, such as computers, smartphones, tablets, & servers, are known as end-systems, or hosts. These gadgets make use of programs & services that let users interacts with & connect to material on the internet, such social networking platforms, email clients, & web browsers.
- Access networks: End systems connect to their internet service provider using access networks. To give consumers connections, they make use of a variety of technologies, including as cellular networks, DSL, cable modem, fiber-optic, wifi, & wireless. End-systems can access the larger internet infrastructure using these networks.

• Links: links are connection that link different parts of a network. Depending on the technology & distance, they can have varying speeds, capacities, latencies, & reliability while transmitting data between devices.

↳ Together, these components form the network edge, enabling end-users to connect to the internet & access the vast array of resources & services available online.

Q: 3: ~

Sol

↳ The network core is the central part of the internet infrastructure, known as the network core, is in charge of forwarding & routing data packets over large distances & between other networks. it consists of fiber-optic cables & other transmission media connecting high-capacity, high speed routers & switches.

1) Packet switching:

- Before being sent, data is split up into smaller packets via packet switches.
- Each packet includes routing information & a piece of the original contents.
- Each packet is sent separately, & it may take several routes to get to its destination.
- Each packets destination address is checked by routers located in the network core, which then send it via the most direct route.
- It serves as the foundation for contemporary internet protocols, such as TCP/IP.
- Packet switches offers improved resources efficiency and is more effective at transferring variables-rate, bursty data traffic.

2) Circuit Switches:

- Before data transmission starts, circuit switching creates a specialized communication channel, or circuit, between the sender & recipient.
- Data is constantly transferred across the designated path when the circuit is formed until the communication session is over.
- whether or not data is being transferred, the route is reserved for the length of the conversation.
- Circuit switching works effectively for applications requiring a consistent data rate & occurring in real time, such as video & audio communication.
- However, it may result in the underutilization of network resources & is less effective for bursty data flow.
- Circuit switching is used in certain older communication systems including conventional phone networks.

Q. 4 :-

Sol

↳ The Quality of communication in computer networks is determined by many important performance criteria.

1) Delay:

- The term delay describes the amount of time data packets take to go from their sources to their destination.
- There are several kinds of delays.
  - Transmission delay: The amount of time needed to push every bit of a packet onto the connection.
  - Propagation delay: The amount of time it takes for a signal to go from its source to its destination.
  - Processing delay: The amount of time switches or routers need to process a packet.
  - Delay in Queuing: The amount of time a packet spends in buffers before being sent.

- for real-time applications such as online gaming & video conferencing, where delays can cause a bad user experience or even make the program unplayable, low latency is essential.

2) Loss:

- Packets that are lost can be attributed to a number of factors, including network malfunctions, congestion & mistakes.
- Communication quality can be negatively impacted by Packet loss, particularly in applications where data integrity is important, including voice & video transmission.
- Network congestion might result in loss because routers reject packets when their buffers overflow.

3) Throughput:

- The speed at which data is successfully sent via a network from the source to the destination is known as throughput.
- Bits Per Second (BPS) or Packets Per second (PPS) are the common units of measurement.
- Good performance & effective use of network resources are indicated by high throughput.
- Many factors, including network congestion, connection capacity, Packet loss, & Protocol overhead, can have an impact on throughput.
- For applications like file downloads, streaming videos & huge data transfers that demand high data transfer speeds, it is essential.

Understanding & evaluating network Performance requires grasping these core concepts. To ensure reliable & efficient communication in computer networks, particularly when catering to different applications with diverse requirements & constraints, it is essential to strike a balance between delay, loss & throughput.

Q: 5 :~

Sol

1) Protocol layers:

↳ Different levels of rules & guidelines for how things communicate with eachother. There's this thing called Protocol layers that represent the hierarchy of services & protocols used in network communication. Two well-known reference models that explain these layers are TCP/IP & OSI. Each layer has specific tasks & communicate with other layers through clear interfaces. The OSI model has seven levels: Physical, Data link, Network, Transport, Session, Presentation & application. On the other hand the TCP/IP Paradigm consist of four levels: Internet, Transport, applications, & Network interface. Before passing data to the lower layer, each layer wraps up information from the layer above & adds its own header.

2) Service models:

↳ There are different types of services that exist. Service models specify the services provided by a network to users & applications. These models cater to various communication needs such as security, timeliness, & dependability.

* How layers & service models works together:

↳ The collaboration between layers & service models. Protocol layers & service models play a crucial role in facilitating communication & data sharing. Each layer performs specific functions such as data encapsulation, addressing, routing, error detection, & flow management. lower-layer Protocol Provide necessary functions for data transfer & feedback, which higher-layer Protocols depend on. The layered approach enables interperability between systems & devices that adhere to the same Protocol standards. Dividing issues into distinct layers & servic models enhances control, scalability, & modularity in network communication.

Q. 6 :-

Sol

Security threat:

- Malware: Viruses, worms, ransomware, & spyware are examples of programs intended to interface with, harm or get illegal access to systems & data.
- Phishing: Attacks attempt to trick users into revealing sensitive information such as passwords, financial details or personal information.
- Attacks known as denial of service (DOS) & distributed denial of service (DDOS) overload servers, network, or systems with excessive traffic them unavailable to authorized users.
- man in the middle (MitM) Attacks: unbeknownst to the parties involves, hackers intercept & may modify communication to allow for eavesdropping, data manipulation, or session ~~hard~~ hijacking.
- Insider threats are when authorized users abuse their access rights or unintentionally violate security due to carelessness, which can result in system compromise or data breaches.

Network security:

- Firewalls: they monitor & manage outgoing & incoming traffic, Prevent malicious activity, & enforce controls restrictions.
- Systems for detecting & stopping intrusions into networks known as intrusion Prevention & detection (IDS & IPS), are designed to identify & address suspicious activity or possible threats.
- Data encryption protects information both in transit & at rest by thwarting illegal access or interception.
- Access controls: least privilege guidelines, strict authentication ~~Protocols~~ Procedures & permission processes restrict access to critical resources.

- Frequent Patching: Applying security updates & patches on times lowers the chances that a known vulnerable will be exploited
- Security Awareness Training: Users capacity to recognize & react to possible hazards is improved by teaching them about common threats, phishing techniques, & cyber-security best practices.
- Network segmentation: Reducing the spread of risks by breaking up networks into smaller, isolated sections with restricted access.

Q: 7 :~

Sol

The growth of computer networks & the internet has seen significant advancement & important milestones. The US Department of Defense funded the creation of ARPANET, the first Packet-Switching network, during the 1960s. This network connected four research institutes in the US & laid the groundwork for the internet. In the 1970s, the TCP/IP Suite was created to establish consistent communication protocols for various networks & it later became the basis for the internet's architecture. In the 1980s, networks such as LANs & WANs grew rapidly in the business, government, & academic sectors. LANs heavily relied on ethernet technology. In the 2020s, 5G networks & the internet of things becomes Popular, allowing for more devices to connect to the internet & improving various industries like healthcare & home ~~auto~~ automation. The introduction of 5G also Promised better connectivity, faster speeds & reduced delays for advanced application.

Q: 8:~

Sol:

• functions:

- Access Provision: Internet servic providers (ISPs) provide consumers with a range of options for connecting to the internet, including fiber-optic, DSL, wireless, satellite & cable modem technologies.
- IP address assignment: ISPs provide their clients with IP addresses so that their devices may connect & use the internet.
- ISPs oversee the routing of data packets between networks maximizing traffic flow & guaranteeing effective delivery.

• Types:

⇒ The information is divided into different groups or categories. ISPs are ranked based on their level of connectivity & influence in the global internet network. Tier 1 ISPs are at the top, operating international network & exchanging traffic with other top-tier ISPs. They have a significant share of internet traffic & an complex network structure. Tier 2 ISPs connect to Tier 1 ISPs & other networks to access the internet, often purchasing services from Tier 1 ISPs.

• Influence on network connectivity:

⇒ The effect on the connection & communication between networks. ISPs determine if internet services are accessible in a certain location based on their network coverage & infrastructure. The speed, reliability & quality of internet connections are influenced by the network infrastructure & services provided by ISPs. ISPs engage in network interconnection & peering arrangements to facilitate traffic exchange & ensure worldwide connectivity, which can impact the overall performance of the network & internet traffic routing.

Q: 9: ~

Sol

• Virtual Private networks (VPN):

↳ VPNs are networks that Provided a secure & Private connection over the internet. Virtual Private networks (VPNs) Provide secure & Private communication by encrypting data & concealing users IP addresses. Additionaly, it is critical to have robust authentication & encryption measure to ensure VPN security, as ~~not~~ any misconfigurations or vulnerabilities could compromise user Privacy.

• Internet of Things (IoT):

↳ The internet of things (IoT) refers to a network of interconnected devices that can communicate & share data with each other over the internet. The IoT allows for remote automation & monitoring by connecting everyday objects to the internet, This has advantages such as increased efficiency, cost savings, & new revenue streams in various industries. However, IoT devices face challenges in terms security, Privacy, scalability, interoperability, & reliability, which limit their widespread adoption.

• cloud computing:

↳ Benefits: Through the internet, cloud computing Provides on-demand access to computer resources including storage, Processing Power, & APP.

↳ Difficulties: cloud computing Presents a number of security & Privacy issues, Particularly with relation to data security, compliance & legal obligations. in multi-cloud setups, mobility & flexibility may be restricted by vendor lock-in & interoperability Problem.

Q. 10 :-

Sol

1) Transmission Delay :

∵ formula $T_{transmission}$ = size of file / Bandwidth

Give data.

File size = 5MB = $5 * 8 * 10^6$ bits

Bandwidth = 10 Mbps

$T_{transmission}$ = ?

Put the values in above formula:

$$T_{transmission} = \frac{40 * 10^6 \text{ bits}}{10 * 10^6 \text{ bits/sec}} = 4 \text{ seconds.}$$

2) Propagation Delay :

∵ formula $T_{Propagation}$ = Distance / Speed of light.

Give data.

Distance = 10000Km = 10000×10^3 meters.

Speed of light = 3×10^8 meter/sec.

$T_{Propagation}$ = ?

Put the value in formula:

$$T_{Propagation} = \frac{10000 \times 10^3 \text{ meter}}{3 \times 10^8 \text{ meter/sec}} = 3.3 \text{ milisec.}$$

Now, add both answers to get total.

T_{total} = 4 sec 3.3 milisec.

= 4.00333 Sec

Q.11:-

Sol:

A). Given Data.

R_1 = 500 Kbps

R_2 = 2 mbps = 2000 Kbps

R_3 = 1 mbps = 1000 kbps

↳ The bottleneck link is link (R_1) with a bandwidth of 500 Kbps.

B)

Given Data

file size = 4 million bytes = 4 * 8 = 32 million bits.

Throughput = 500 Kbps

- Time to transfer file:

Time = file size / Throughput

$$= \frac{32,000,000 \text{ bits}}{500,000 \text{ bits/sec}} = 64 \text{ seconds.}$$

↳ file will take 64 sec to transfer Host B.

c) Given Data.

R_1 = 500 Kbps

R_2 = 100 Kbps

R_3 = 1 mbps = 1000 Kbps.

- The bottleneck link is now link (R_2) with bandwidth 100 Kbps.
- Throughput for the file transfer is 100 Kbps.
- for time to transfer the file:

Time = file size / Throughput.

$$= \frac{32,000,000 \text{ bits}}{100,000 \text{ bits/sec}} = 320 \text{ sec}$$

Q:12 :-

Sol:

A)

Given Data:

Bandwidth = 3 Gbps = 3×10^9 bits/sec

Propagation delay = 50 milisec = 50×10^{-3} sec

∵ BDP = Bandwidth × Propagation delay.

$= 3 \times 10^9$ bits/sec $\times$ 50×10^{-3} sec $= 150,000,000$ bits

$= 3 \times 10^9$ bits/sec $\times$ 50×10^{-3} sec

$= 150,000,000$ bits.

Hence, Bandwidth-delay.

B)

Given Data:

Packet transmission time = 0.003 sec

Packet propagation time = 0.001 sec

∵ Total end-to-end delay = transmission time + Propagation time

= 0.003 sec + 0.001 sec

= 0.004 sec

Hence, end-to-end delay is 0.004 sec

c)

Given Data:

transmission time = 0.01 sec

Propagation time = 0.005 sec.

∵ end-to-end delay = transmission time + Propagation time.

= 0.01 sec + 0.005 sec

= 0.015 sec

Hence, end-to-end delay 0.015 sec

D) Given data.

file size = 10,000,000 bits.

bandwidth = 10 mbps = 10×10^6 bits/sec

efficiency is typically assumed to be 1.

∴ Time = 10,000,000 bits / 10×10^6 bits/sec

= 1 sec

Hence, take one sec to transmit entire file.

E) Given data.

file size = 4,000,00 bits.

bandwidth = 2 Mbps

∴ Time = file size / bandwidth.

= $\frac{4,000,000 \text{ bits}}{2 \times 10^6 \text{ bits/sec}}$ = 2 sec

Hence, it will take 2 sec to transmit entire file.

Q.13 :~

Sol

1) Hackers:

- Motivations: Hackers may be driven by a variety of things, such as monetary gain, intellectual curiosity, personal challenge, or ideological convictions.
- Capabilities: Hackers possesses advanced technical skills and in-depth knowledge of networks & computer systems. They can utilize various methods such as creating malware, exploiting security vulnerabilities, or execution complex attacks to achieve their objectives.

2) Cybercriminals:

- Motivations: The primary motivation for cybercriminals is financial gain. They aim to steal sensitive information, such as credit card details, personal identification data or intellectual property, with the intention of either using it for fraudulent activities or selling it on the black market.
- Capabilities: Cybercriminal employ various methods like ransomware, malware, phishing, & online scams to target individuals, companies, or organizations. They may work individually or as part of organized criminal group.

3) State-sponsored actors:

- Motivations: Governments or intelligence services support & enable state-sponsored actors to engage in cyberwarfare cyberespionage, or cybersabotage in order to advance their nation's interests, acquire information, or gain an advantage over other countries or organization
- Capabilities: Government-backed actors have access to significant resources & skilled personal. They can use advanced tactics like customized malware, unknown software vulnerabilities, or persistent threats to infiltrate to targeted networks.

4) Insiders:

- Motivations: Insiders are individuals who have authorized access to internal systems & networks; but use it for malicious purposes.
- Capabilities: Insiders pose a significant threat due to their knowledge of internal systems & protocols.

5) Hacktivists:

- Motivations: Hacktivists are individuals or groups that use hacking techniques to bring attention to issues, promote social or political causes, or express their disapproval of perceived unfairness.
- Capabilities: Hacktivists use various strategies, such as data leaks, DDoS attacks, data defacement, & cyber vandalism to achieve their goals.

Q. 14 :~

Sol

↳ The ethical & legal implications of hacking activities conducted by threat actors are significant & can have far-reaching consequences.

- Breach of Privacy: Hacking often involves gaining unauthorized access to personal data, leading to breaches of confidentiality agreements & the violation of Private rights.
- Intellectual Property theft: occurs when hackers steal trade secrets, confidential information, or intellectual Property, leading to financial losses & hindering a company's competitive edge.
- Service disruption: cyberattacks such as ransomware & DDoS attacks can disrupt services, jeopardize public safety, damage critical infrastructure, & interrupt essential operations.
- Financial fraud: Involves cybercriminals using hacking techniques to carry out crimes such as identity theft, credit card fraud, & internet scams, which result in financial losses for individuals & businesses.
- Legal repercussions: Engaging in hacking is against the law & can lead to severe consequences such as imprisonment, monetary penalties, & legal action.

↳ To combat cybercrime effectively, law enforcement agencies can takes several measure.

- cooperation & information sharing: law enforcement agencies collaborate with foreign counterparts, governmental bodies, businesses, & cybersecurity experts to share information, resources, & strategies in orders to Prevent cybercrime.

- Cybercrime units: law enforcement organizations establish dedicated units to investigate & prosecute cybercriminals utilizing specialized expertise, tools, & techniques to apprehend & charge offenders.
- legislative actions: we need to make rules to stop people from hacking into computers & stealing information.
- Building capacity & training: Providing resources & training to law enforcement can enhance their ability to detect & address cybercrime. Training programs should incorporate cyber ~~and~~ incident response & digital forensics.
- Public education & awareness: Educating the public about cybersecurity risks, preventive measures, & reporting protocols is essential in increasing resistances to cyberattacks & minimizing vulnerability.
- cybersecurity partnerships: Promote collaborations between law enforcement, industry, academia, & civil society to address cybersecurity challenges.

Q: 15 :~

Sol

* Service layering:

⇒ Service layering, also known as Protocols layering or network layering, is a concept in networking design that organizes communications protocols into seperate levels. The TCP/IP & OSI models are commonly used to define standarized layers of network communication.

* Encapsulation:

⇒ Encapsulation is the process of wrapping information within protocols headers at each level of the network stack. Decapsulation, on the other hand, occurs at the receiving end when each layer removes its header & passes the payload to the next higher layer. Encapsulation in network communication provides abstraction, modularity, & flexibility, allowing different protocols to interact smoothly & promoting interoperability among systems & devices.