Reg.no: 20505015 Name: D.Smilin Jasper Sub.Code: 35242

PART-A

1. Define Topology.

Ans:-

*Topology is defined as the way a network is laid out physically. Two or more devices connect to a link; two or more links form a topology.

2. Define Simplex.

Ans:-

*In the simplex communication the direction of signal of data flow is in only one direction i.e unidirectional only. Eg. Radio station broadcasting the programs and the receiver receives the signal and listen to the program.

3. Define Protocol.

Ans:-

*It is a set of rules that governs the data communications. It represents an 4 agreement between the communicating devices. Without a protocol, two devices may be connected but cannot communicate.

Date: 22.05.2021

Signature: Smil

Reg.no: 20505015 Name: D.Smilin Jasper Sub.Code: 35242

4. What is OSI?

Ans:-

*It is an open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

5. What is IP Address?

Ans:-

*An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

6. Define Socket.

Ans:-

* The term socket address or simply socket is used to identify the IP address and the port number concatenated together.

7. Define Kerberos.

Ans:-

* Kerberos is a key distribution and user authentication service developed at MIT.

Date: 22.05.2021

Signature: Smil

8. Define Cryptography.

Ans:-

* Cryptography, a word with Greek origins, means "secret writing. The term to refer to the science and art of transforming messages to make them secure and immune to attacks.

9. What is Hacking?

Ans:-

* Hacking currently refers to the process of breaking into computers.

10. Define Spam.

Ans:-

* Email spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

PART-B

11. Discuss Bad Password.

Ans:-

* Weak passwords always play a major role in any hack. For the ease of user, sometime applications do not enforce password complexity and as a

Date: 22.05.2021

Signature: Smil

result of that users use simple passwords such as password, password123, Password@123, 12345, god, own mobile number etc.

*Weak password does not always mean length and the characters used, it also means the guessability. Name@12345, it looks quite complex password but can be guessable.

12. Explain SSL.

Ans:-

*SSL probably most widely used web security mechanism. Its implemented at the Transport layer. SSL is designed to make use of TCP to provide a reliable end-to-end secure service.

*Netscape originated SSL. Version 3 of the protocol was designed with public review and input from industry and was published as an Internet draft document. Subsequently, the IETF TLS working group was formed to develop a common standard.

*SSL is not a single protocol but rather two layers of protocols.

13. Explain Ring Topology.

Ans:-

*In a ring topology, each device has dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the

Date: 22.05.2021

Signature: Smil

ring in one direction, from device to device, until it reached its destination.

It could be point to point with 2 devices on both sides

Advantages:

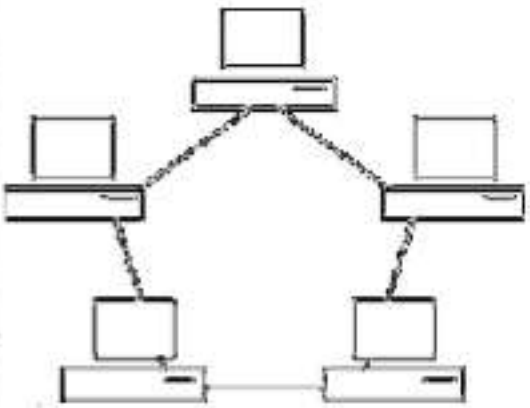
- Easy to install
- Maintain: add move delete
- Fault isolation

Disadvantages:

Unidirectional traffic

A break in the ring the entire network is disabled.

Example Diagram:-



Date: 22.05.2021

Signature: Smil

14. Give the advantages of FDDI.

Ans:-

* Token passing topology
* High speed fiber optic transmission
* Dual rings offer improved fault tolerance over other options
* Fiber optic cabling is less susceptible to EMI and noise
* Fiber optic cabling is more secure than copper wire
* It can send data for larger distances than Token Ring or Ethernet
* FDDI supports real-time allocation of network bandwidth.
* This allows you to use a wide array of different types of traffic.
* FDDI has a dual ring that is fault-tolerant. The benefit here is that if a station on the ring fails or if the cable becomes damaged, the dual ring is automatically doubled back onto itself into a single ring.
* The FDDI compensates for wiring failures. The stations wrap within themselves when the wiring fails.
* Optical bypass switches are used that can help prevent ring segmentation. The failed stations are eliminated from the ring.

Date: 22.05.2021

Signature: Smil

15. Discuss RARP.

Ans:-

* The Reverse Address Resolution Protocol (RARP) is an network layer protocol used by a client computer to request its Internet Protocol(IPV4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.

* RARP (replaced by DHCP): mapping a MAC address to an IP address.

PART-C

16. B) Discuss about

(a) Switch:-

Ans:-

*Switch is one of the devices used to group the nodes together to form a network.

*Instead of broadcasting the frames to all the ports, a switch actually checks for the destination MAC address (physical address) and forward it to the relevant port to reach that computer only.

*This way, switches reduce traffic and divide the collision domain into segments, this is very sufficient for busy LANs and it also protects

Date: 22.05.2021

Signature: Smil

frames from being sniffed by other computers sharing the same segment.

*They build a table of which MAC address belongs to which segment. If a destination MAC address is not in the table it forwards to all segments except the source segment.

*If the destination is same as the source, frame is discarded.

*Switches have built-in hardware chips solely designed to perform switching capabilities, therefore they are fast and come with many ports.

*Sometimes they are referred to as intelligent bridges or multiport bridges.

*Different speed levels are supported. They can be 10 Mb/s, 100 Mb/s, 1 Gb/s or more.

Most common switching methods are:

1. Cut-through: Directly forward what the switch gets.
2. Store and forward: receive the full frame before retransmitting it.

(b) Router

Ans:-

*Routers are used to connect different LANs or a LAN with a WAN (e.g. the internet).

Date: 22.05.2021

Signature: Smil

*If the packet's destination is on a different network, a router is used to pass it the right way, so without routers the internet could not functions.

*Routers use NAT (Network Address Translation) in conjunction with IP hidden to provide the internet to multiple nodes in the LAN under a single IP address.

*For a network router to know where to send packets of data it receives, it uses a routing table.

*A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination.

*When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination.

*The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

17. B) Explain ISDN and its services.

Ans:-

INTEGRATED SERVICES DIGITAL NETWORK (ISDN):-

*Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video,

Date: 22.05.2021

Signature: Smil

data, and other network services over the traditional circuits of the public switched telephone network.

*The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system.

*The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

*ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide.

*It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s.

*In some countries, ISDN found major market application for Internet access, in which ISDN typically provides a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically, the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

Date: 22.05.2021 Signature: Smil

*In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

ISDN INTERFACES:-

*Integrated services refers to ISDN's ability to deliver at minimum two simultaneous connections, in any combination of data, voice, video, and fax, over a single line.

*Multiple devices can be attached to the line, and used as needed.

*That means an ISDN line can take care of most people's complete communications needs (apart from broadband Internet access and entertainment television) at a much higher transmission rate, without forcing the purchase of multiple analog phone lines.

*It also refers to integrated switching and transmission in that telephone switching and carrier wave transmission are integrated rather than separate as in earlier technology.

BASIC RATE INTERFACE:-

*The entry level interface to ISDN is the Basic Rate Interface (BRI), a 128 Kbit/s

service delivered over a pair of standard telephone copper wires.

*The 144 Kbit/s payload rate is broken down into two 64 Kbit/s bearer channels ('B' channels) and one 16Kbit/s signaling channel ('D' channel or data channel).

PRIMARY RATE INTERFACE:-

*The other ISDN access available is the Primary Rate Interface (PRI), which is carried over an E1 (2048 Kbit/s) in most parts of the world.

*An E1 is 30 'B' channels of 64 Kbit/s, one 'D' channel of 64 Kbit/s and a timing and alarm channel of 64 Kbit/s.

BROADBAND INTEGRATED SERVICES DIGITAL NETWORK:-

*In the 1980s the telecommunications industry expected that digital services would follow much the same pattern as voice services did on the public switched telephone network, and conceived an end-to-end circuit switched services, known as Broadband Integrated Services Digital Network (B-ISDN).

*Before B-ISDN, the original ISDN attempted to substitute the analog telephone

Date: 22.05.2021 Signature: Smil

system with a digital system which was appropriate for both voice and non-voice traffic.

*Obtaining worldwide agreement on the basic rate interface standard was expected to lead to a large user demand for ISDN equipment, hence leading to mass production and inexpensive ISDN chips.

*However, the standardization process took years while computer network technology moved rapidly.

*Once the ISDN standard was finally agreed upon and products were available, it was already obsolete. For home use the largest demand for new services was video and voice transfer, but the ISDN basic rate lacks the necessary channel.

*This led to introduction of B-ISDN, by adding the word broadband. The designated technology for B-ISDN was Asynchronous Transfer Mode (ATM), which was intended to carry both synchronous voice and asynchronous data services on the same transport.

*The BISDN vision has been overtaken by other disruptive technologies used in the Internet.

PROTOCOL STRUCTURE OF B-ISDN:-

*Broadband ISDN protocol reference model is based on the ATM reference model.

Date: 22.05.2021 Signature: Smil

*ATM adaption layer is responsible for mapping the service offered by ATM to the service expected by higher layers.

*ATM layer is independent of the physical medium over which transmission is to take place.

*Physical layer consists of two sub layers Transport convergence and physical medium.

*The control plane is responsible for the supervision of connections including call set up, call release and maintenance.

*The user plane provides for the Transfer of user information. It also includes mechanisms to perform error recovery and flow control.

Diagram:-

B- ISDN protocol reference model

Date: 22.05.2021

Signature: Smil

Reg.no: 20505015 Name: D.Smilin Jasper Sub.Code: 35242

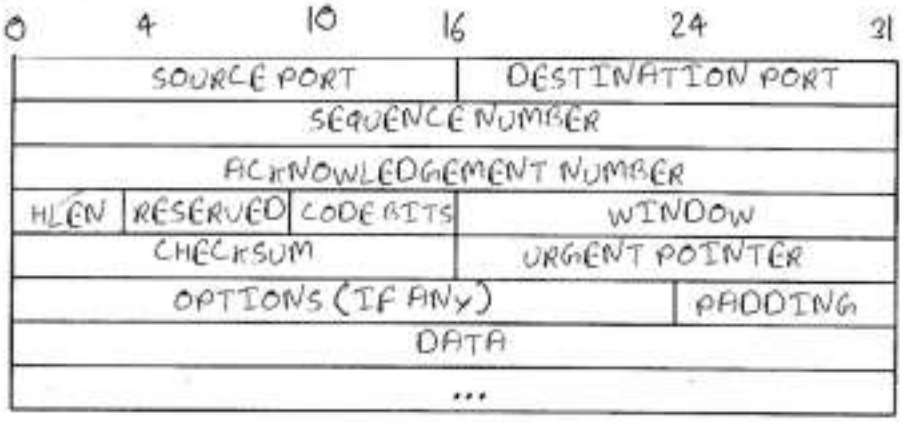
18. A) Explain TCP

Ans:-

Transmission Control Protocol (TCP) :-

- Basic Features
  - TCP provides connection-oriented communication (virtual circuit connection, like telephone communication). It manages a point-topoint and full-duplex connection for an application between two computers.
    - creates a connection before communication;
    - sends and receives data over this connection;
    - closes a connection after communication.
  - TCP guarantees reliable data delivery.
  - The TCP recipient will receive data in a correct order without data loss or error.

Format of a TCP segment:



Date: 22.05.2021

Signature: Smil

Reg.no: 20505015 Name: D.Smilin Jasper Sub.Code: 35242

19. A) Explain RSA Algorithm.

Ans:-

RSA ALGORITHM:-

*The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods.

*The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

Date: 22.05.2021

Signature: Smil

How to Determine Appropriate values for e, d, and n:-

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
2. Set n equal to p * q.
3. Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
4. Find e such that e * d = 1 (mod ((p-1) * (q-1)))

Rivest, Shamir, and Adleman provide efficient algorithms for each required operation[4].

How secure is a communication using RSA?

*Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key.

*The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers.

*If 100 digit numbers are used for p and q, the resulting n will be approximately 200 digits.

*The fastest known factoring algorithm would take far too long for an attacker to ever break the code.

*Other methods for determining d without factoring n are equally as difficult. Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

Date: 22.05.2021

Signature: Smil

20. B) Explain Honeypots.

Ans:-

Honeypots:-

*A relatively recent innovation in intrusion detection technology is the honeypot.

*Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

Honeypots are designed to:

- divert an attacker from accessing critical systems.
- collect information about the attacker's activity.
- encourage the attacker to stay on the system long enough for administrators to respond.

*These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect.

*The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities.

*Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems.

Date: 22.05.2021

Signature: Smil

*Initial efforts involved a single honeypot computer with IP addresses designed to attract hackers.

*More recent research has focused on building entire honeypot networks that emulate an enterprise, possibly with actual or simulated traffic and data.

*Once hackers are within the network, administrators can observe their behavior in detail and figure out defenses.

Date: 22.05.2021

Signature: Smil