



Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India
(Autonomous College Affiliated to University of Mumbai)

End Semester Examination 06/01/2020- Synoptic

Duration: 3 Hr.

Semester: VI

Max. Marks: 60

Class: T.E.

Course Code: ET62

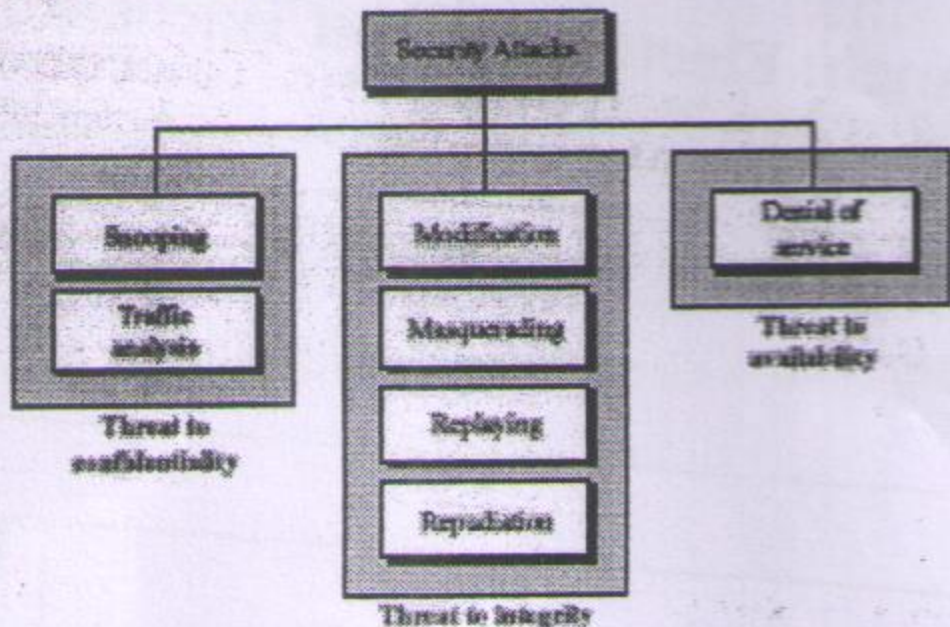
Name of the Course: Computer Communication Networks

Branch: Electronics and Telecommunication

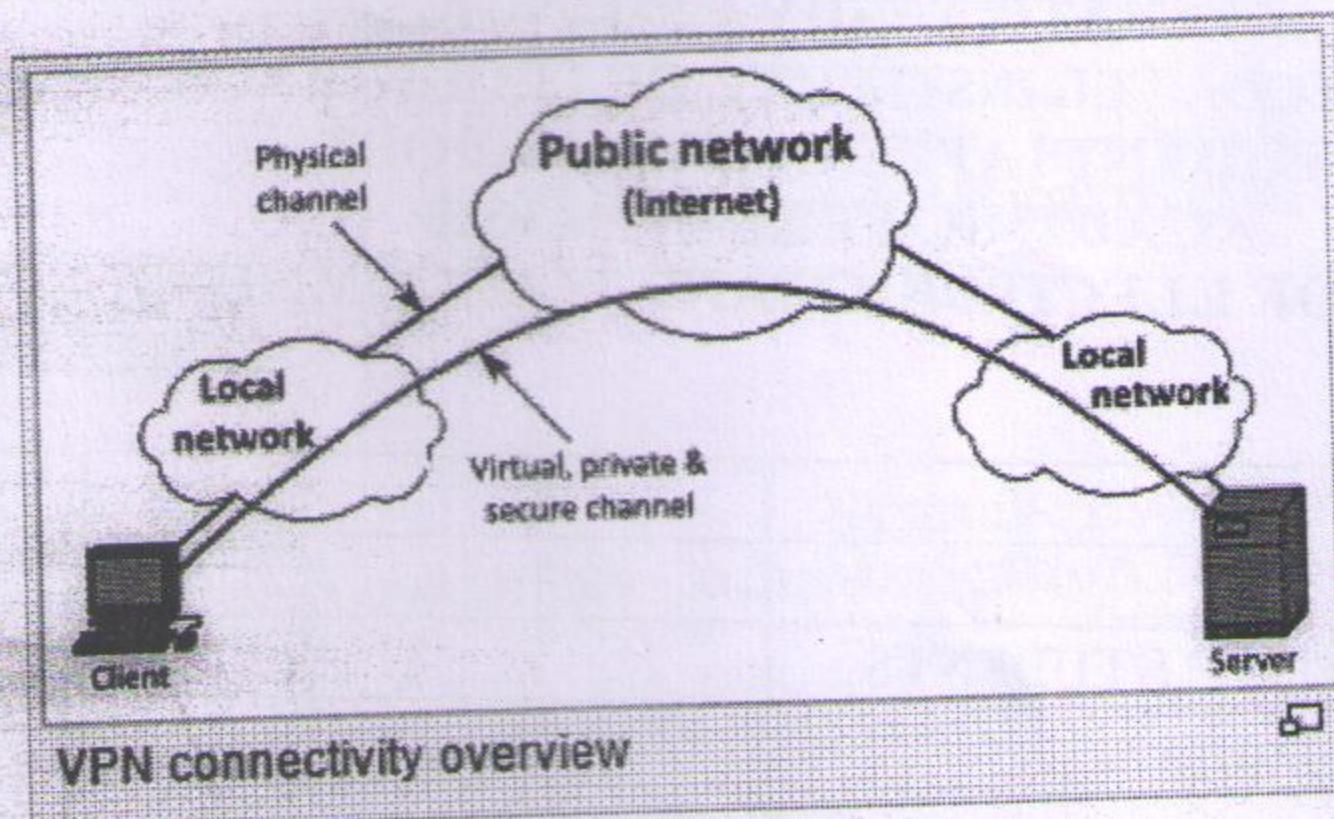
Instruction:

- (1) All questions Q1-Q4 are compulsory
- (2) Assume suitable data if necessary
- (3) Draw neat diagrams

Q No.		Max. Marks	CO
Q.1 (a)	Define the role of layer of OSI model. ii) Session Layer ii) Transport layer	5	CO1
Q.1 (b)	Key function of each layer is 2.5 M What is socket programming? Explain the working principle of client server model. Example of socket add is 2 M and client server model with explanation =8M	10	CO1
Q.1 (b)	OR State the hierarchical name space. Give the role of any two DNS resolver Hierarchical dia=2M Resolution with diagram =8M	10	CO1
Q.2 (a)	Justify the following services provided by TCP ii) Process to process Communication ii) Stream delivery service iii) segment iv) Connection oriented service. Process to process Communication= 3M rest each is =2M	10	CO3
Q.2 (b)	Justify the merits of Go Back N over Stop and Wait reliable data transfer Dia=1M, explanation=3M merits =1M	5	CO3
Q.2 (b)	OR The following is a dump of a TCP header in hexadecimal format. (05320017 00000001 00000000 500207FF 00000000)16 The source port number is 0532 in hex and 1330 in decimal. b. The destination port number is 0017 in hex and 23 in decimal. c. The sequence number is 00000001 in hex and 1 in decimal. d. The acknowledgment number is 00000000 in hex and 0 in decimal. e. The HLEN = 5. The header is $5 \times 4 = 20$ bytes long.	5	CO3
Q.3 (a)	What are the fragmentation field in IP datagram. Give the importance of these fields. Identification, Flags, fragmentation offset=1M	10	CO2
Q.3 (a)	Role of each =3M OR Draw packet format of IPv6. Give the importance of each field and highlight the merits of IPv6 over IPv4.	10	CO2

	Packet format=2M, Explanation =7M , Merits=1M		
Q.3 (b)	BGP is exterior protocol, justify Dia of autonomous system=1m Exterior principle=4M	5	CO2
Q.4(a)	<i>State three security goals. Justify Taxonomy of attacks with relation to security goals can be threatened by security attacks</i>	10	CO1
Q.4(a)	<p>security goals: confidentiality, integrity, and availability=1M, Dia= 2M, Explanation=7M</p>  <p style="text-align: center;">OR</p> <p>What do you mean by Firewall? How it control access to a system</p> <p>A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others with dia= 2M</p> <p>Packet-Filter Firewall= 7M</p> <p>A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded).</p> <p>According to the figure, the following packets are filtered:1. Incoming packets from network 131.34.0.0. are blocked (security precaution). Note that the * (asterisk) means "any."2. Incoming packets destined for any internal TELNET server (port 23) are blocked. 3. Incoming packets destined for internal host 194.78.20.8. are blocked. The organization wants this host for internal use only. 4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.</p> <p>Dia=1M</p>		
Q.4(b)	<p>Give the concept of VPN with neat diagram. Dia-1M, peinciple=4M</p> <p>A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, though not an inherent, part of a VPN connection. VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunneling protocol, and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN. In other applications, Internet users may secure their connections with a VPN to circumvent geo-restrictions and censorship or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. Some websites, however, block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.A VPN is created by establishing a virtual point-to-point connection through the use of</p>	5	CO1

dedicated circuits or with tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.



OR

What is the issue with Symmetric-Key Distribution? How it is overcome by *Key-Distribution Center* (KDC)

Symmetric-Key Distribution

Symmetric-key cryptography is more efficient than asymmetric-key cryptography for enciphering large messages. Symmetric-key cryptography, however, needs a shared secret key between two parties. If Alice needs to exchange confidential messages with N people, she needs N different keys. What if N people need to communicate with each other? A total of $N(N-1)$ keys is needed if we require that Alice and Bob use two keys for bidirectional communication; only $N(N-1)/2$ keys are needed if we allow a key to be used for both directions. This means that if one million people need to communicate with each other, each person has almost one million different keys; in total, almost one billion keys are needed. This is normally referred to as the N^2 problem because the number of required keys for N entities is close to N^2 . The number of keys is not the only problem; the distribution of keys is another. If Alice and Bob want to communicate, they need a way to exchange a secret key; if Alice wants to communicate with one million people, how can she exchange one million keys with one million people? Using the Internet is definitely not a secure method. It is obvious that we need an efficient way to maintain and distribute secret keys.

Key-Distribution Center: KDC

A practical solution is the use of a trusted third party, referred to as a **key-distribution center (KDC)**.

To reduce the number of keys, each person establishes a shared secret key with the KDC. A secret key is established between the KDC and each member. Now the question is how Alice can send a confidential message to Bob. The process is as follows:

1. Alice sends a request to the KDC stating that she needs a session (temporary) secret key between herself and Bob.
 2. The KDC informs Bob about Alice's request.
 3. If Bob agrees, a session key is created between the two.
- The secret key between Alice and Bob that is established with the KDC is used to authenticate Alice and Bob to the KDC and to prevent Eve from impersonating either of them.