Unit 4

1. Both HDLC and PPP both are Data link layer protocols.  
   a) True  
   b) False  
   Answer: a  
   Explanation: Both HDLC and PPP both are Data link layer protocol.
2. Which protocol does the PPP protocol provide for handling the capabilities of the connection/link on the network?  
   a) LCP  
   b) NCP  
   c) Both LCP and NCP  
   d) TCP  
   Answer: c  
   Explanation: LCP and NCP are the PPP protocol provide for handling the capabilities of the connection/link on the network.
3. The PPP protocol  
   a) Is designed for simple links which transport packets between two peers  
   b) Is one of the protocols for making an Internet connection over a phone line  
   c) Both Is designed for simple links which transport packets between two peers & Is one of the protocols for making an Internet connection over a phone line  
   d) None of the mentioned  
   Answer: c  
   Explanation: The PPP protocolis designed for simple links which transport packets between two peers and one of the protocols for making an Internet connection over a phone line.
4. PPP provides the \_\_\_\_\_\_\_ layer in the TCP/IP suite.  
   a) Link  
   b) Network  
   c) Transport  
   d) Application  
   Answer: a  
   Explanation: PPP provides thelinklayer in the TCP/IP suite.
5. PPP consists of \_\_\_\_\_\_\_\_components  
   a) Three (encapsulating, the Domain Name system)  
   b) Three ( encapsulating, a link control protocol, NCP )  
   c) Two ( a link control protocol, Simple Network Control protocol)  
   d) None of the mentioned  
   Answer: b  
   Explanation: PPP consists of three (encapsulating, a link control protocol, NCP)  
   Components.
6. The PPP encapsulation  
   a) Provides for multiplexing of different network-layer protocols  
   b) Requires framing to indicate the beginning and end of the encapsulation  
   c) Establishing, configuring and testing the data-link connection  
   d) None of the mentioned  
   Answer: a  
   Explanation: The PPP encapsulationprovides for multiplexing of different network-layer protocols.
7. A Link Control Protocol (LCP) is used for  
   a) Establishing, configuring and testing the data-link connection  
   b) Establishing and configuring different network-layer protocols  
   c) Testing the different network-layer protocols  
   d) None of the mentioned  
   Answer: a  
   Explanation: A Link Control Protocol (LCP) is used for establishing, configuring and testing the data-link connection.
8. A family of network control protocols (NCPs)  
   a) Are a series of independently defined protocols that provide a dynamic  
   b) Are a series of independently-defined protocols that encapsulate  
   c) Are a series of independently defined protocols that provide transparent  
   d) The same as NFS  
   Answer: b  
   Explanation: A family of network control protocols (NCPs)are a series of independently-defined protocols that encapsulate.
9. Choose one from the following  
   a) PPP can terminate the link at any time  
   b) PPP can terminate the link only during the link establishment phase  
   c) PPP can terminate the link during the authentication phase  
   d) None of the mentioned  
   Answer: a  
   Explanation: PPP can terminate the link at any time because it works on the data link layer protocol.
10. The link necessarily begins and ends with this phase. During this phase, the LCP automata will be in INITIAL or STARTING states  
    a) Link-termination phase  
    b) Link establishment phase  
    c) Authentication phase  
    d) Link dead phase  
    Answer: d  
    Explanation: The link necessarily begins and ends with this phase. During this phase, the LCP automata will be in INITIAL or STARTING states link dead phase.
11. A \_\_\_\_\_\_\_\_\_\_\_ is an extension of an enterprise’s private intranet across a public network such as the internet, creating a secure private connection.  
    a) VNP  
    b) VPN  
    c) VSN  
    d) VSPN  
    Answer: b  
    Explanation: VIRTUAL PRIVATE NETWORK.
12. When were VPNs introduced into the commercial world?  
    a) Early 80’s  
    b) Late 80’s  
    c) Early 90’s  
    d) Late 90’s  
    Answer: d  
    Explanation: LATE 90’S.
13. What protocol is NOT used in the operation of a VPN?  
    a) PPTP  
    b) IPsec  
    c) YMUM  
    d) L2TP  
    Answer: c  
    Explanation: YNUM.
14. Which of the following statements is NOT true concerning VPNs?  
    a) Financially rewarding compared to leased lines  
    b) Allows remote workers to access corporate data  
    c) Allows LAN-to-LAN connectivity over public networks  
    d) Is the backbone of the Internet  
    Answer: d  
    Explanation: virtual packet network is not a backbone of the internet.
15. Traffic in a VPN is NOT \_\_\_\_\_\_\_\_\_\_\_\_  
    a) Invisible from public networks  
    b) Logically separated from other traffic  
    c) Accessible from unauthorized public networks  
    d) Restricted to a single protocol in IPsec  
    Answer: c  
    Explanation: Because it is secured with the IP address.
16. VPNs are financially speaking \_\_\_\_\_\_\_\_\_\_  
    a) Always more expensive than leased lines  
    b) Always cheaper than leased lines  
    c) Usually cheaper than leased lines  
    d) Usually more expensive than leased lines  
    Answer: c  
    Explanation: It is very cheap.
17. Which layer 3 protocols can be transmitted over a L2TP VPN?  
    a) IP  
    b) IPX  
    c) Neither IP or IPX  
    d) Both IP or IPX  
    Answer: d  
    Explanation: Data roming layer.
18. ESP (Encapsulating Security Protocol) is defined in which of the following standards?  
    a) IPsec  
    b) PPTP  
    c) PPP  
    d) L2TP  
    Answer: a  
    Explanation: It is the security type of the IPsec.
19. L2F was developed by which company?  
    a) Microsoft  
    b) Cisco  
    c) Blizzard Entertainment  
    d) IETF  
    Answer: b  
    Explanation: Cisco is the second best company to design and make the computer networks.
20. Which layer of the OSI reference model does PPTP work at?  
    a) Layer 1  
    b) Layer 2  
    c) Layer 3  
    d) Layer 4  
    Answer: b  
    Explanation: Presentation layer.
21. Which layer of the OSI reference model does IPsec work at?  
    a) Layer 1  
    b) Layer 2  
    c) Layer 3  
    d) Layer 4  
    Answer: c  
    Explanation: Session layer.
22. Which of the following delay is faced by the packet in travelling from one end system to another ?  
    a) Propagation delay  
    b) Queuing delay  
    c) Transmission delay  
    d) All of the mentioned  
    Answer: d
23. For a 10Mbps Ethernet link, if the length of the packet is 32bits, the transmission delay is(in microseconds)  
    a) 3.2  
    b) 32  
    c) 0.32  
    d) 320  
    Answer: a  
    Explanation: Transmission rate = length / transmission rate = 32/10 = 3.2 microseconds.
24. The time required to examine the packet’s header and determine where to direct the packet is part of  
    a) Processing delay  
    b) Queuing delay  
    c) Transmission delay  
    d) All of the mentioned  
    Answer: a
25. Traffic intensity is given by, where L = number of bits in the packet a = average rate R = transmission rate  
    a) La/R  
    b) LR/a  
    c) R/La  
    d) None of the mentioned  
    Answer: a
26. In the transfer of file between server and client, if the transmission rates along the path is 10Mbps, 20Mbps, 30Mbps, 40Mbps. The throughput is usually  
    a) 20Mbps  
    b) 10Mbps  
    c) 40Mbps  
    d) 50Mbps  
    Answer: b  
    Explanation: The throughput is generally the transmission rate of bottleneck link.
27. If end to end delay is given by dend-end = N(dproc + dtrans + dprop) is a non congested network. The number of routers between source and destination is  
    a) N/2  
    b) N  
    c) N-1  
    d) 2N  
    Answer: c
28. The total nodal delay is given by  
    a) dnodal = dproc – dqueue + dtrans + dprop  
    b) dnodal = dproc + dtrans – dqueue  
    c) dnodal = dproc + dqueue + dtrans + dprop  
    d) dnodal = dproc + dqueue – dtrans – dprop  
    Answer: c
29. In a network, If P is the only packet being transmitted and there was no earlier transmission, which of the following delays could be zero  
    a) Propogation delay  
    b) Queuing delay  
    c) Transmission delay  
    d) Processing delay  
    Answer: b
30. Transmission delay does not depend on  
    a) Packet length  
    b) Distance between the routers  
    c) Transmission rate  
    d) None of the mentioned  
    Answer: b  
    Explanation: Transmission delay = packet length / transmission rate
31. Propagation delay depends on  
    a) Packet length  
    b) Transmission rate  
    c) Distance between the routers  
    d) None of the mentioned  
    Answer: c  
    Explanation: Propagation delay is the time it takes a bit to propagate from one router to the next.
32. The attackers a network of compromised devices known as  
    a) Internet  
    b) Botnet  
    c) Telnet  
    d) D-net  
    Answer: b
33. Which of the following is a form of DoS attack ?  
    a) Vulnerability attack  
    b) Bandwidth flooding  
    c) Connection flooding  
    d) All of the mentioned  
    Answer: d
34. The DoS attack is which the attacker establishes a large number of half-open or fully open TCP connections at the target host  
    a) Vulnerability attack  
    b) Bandwidth flooding  
    c) Connection flooding  
    d) All of the mentioned  
    Answer: c
35. The DoS attack is which the attacker sends deluge of packets to the targeted host  
    a) Vulnerability attack  
    b) Bandwidth flooding  
    c) Connection flooding  
    d) All of the mentioned  
    Answer: b
36. Packet sniffers involve  
    a) Active receiver  
    b) Passive receiver  
    c) Both Active receiver and Passive receiver  
    d) None of the mentioned  
    Answer: b  
    Explanation: They donot inject packets into the channel.
37. Sniffers can be deployed in  
    a) Wired environment  
    b) WiFi  
    c) Ethernet LAN  
    d) All of the mentioned  
    Answer: d
38. Firewalls are often configured to block  
    a) UDP traffic  
    b) TCP traffic  
    c) Both of the mentioned  
    d) None of the mentioned  
    Answer: a
39. In a network, If P is the only packet being transmitted and there was no earlier transmission, which of the following delays could be zero  
    a) Propogation delay  
    b) Queuing delay  
    c) Transmission delay  
    d) Processing delay  
    Answer: b
40. Network layer firewall works as a  
    a) Frame filter  
    b) Packet filter  
    c) Both Frame as well as Packet filter  
    d) None of the mentioned  
    Answer: b  
    Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.
41. Network layer firewall has two sub-categories as  
    a) State full firewall and stateless firewall  
    b) Bit oriented firewall and byte oriented firewall  
    c) Frame firewall and packet firewall  
    d) None of the mentioned  
    Answer: a  
    Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.
42. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as \_\_\_\_\_\_\_\_\_\_  
    a) Chock point  
    b) Meeting point  
    c) Firewall point  
    d) Secure point  
    Answer: a  
    Explanation: A firewall can be a PC, a router, a midrange, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Generally, a firewall is installed at the point where the secure internal network and untrusted external network meet, which is also known as a chokepoint.
43. Which of the following is / are the types of firewall?  
    a) Packet Filtering Firewall  
    b) Dual Homed Gateway Firewall  
    c) Screen Host Firewall  
    d) All of the mentioned  
    Answer: a  
    Explanation: A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router
44. . A proxy firewall filters at?  
    a) Physical layer  
    b) Data link layer  
    c) Network layer  
    d) Application layer  
    Answer: d  
    Explanation: The application firewall is typically built to control all network traffic on any layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is – without additional software – unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.
45. A packet filter firewall filters at?  
    a) Physical layer  
    b) Data link layer  
    c) Network layer or Transport layer  
    d) Application layer  
    Answer: c  
    Explanation: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.
46. What is one advantage of setting up a DMZ with two firewalls?  
    a) You can control where traffic goes in three networks  
    b) You can do stateful packet filtering  
    c) You can do load balancing  
    d) Improved network performance  
    Answer: c  
    Explanation: In a topology with a single firewall serving both internal and external users (LAN and WAN), it acts as a shared resource for these two zones.
47. What tells a firewall how to reassemble a data stream that has been divided into packets?  
    a) The source routing future  
    b) The number in the header’s identification field  
    c) The destination IP address  
    d) The header checksum field in the packet header  
    Answer: a  
    Explanation: source routing future.
48. A stateful firewall maintains a \_\_\_\_\_\_\_\_\_\_\_ which is a list of active connections?  
    a) Routing table  
    b) Bridging table  
    c) State table  
    d) Connection table  
    Answer: a  
    Explanation: Routing table with best performance
49. . A firewall needs to be \_\_\_\_\_\_\_\_\_\_ so that it can grow with the network it protects  
    a) Robust  
    b) Expansive  
    c) Fast  
    d) Scalable  
    Answer: b  
    Explanation: Expansive to block the fake subscribers
50. Which of the following is false with respect to UDP  
    a) Connection-oriented  
    b) Unreliable  
    c) Transport layer protocol  
    d) All of the mentioned  
    Answer: a  
    Explanation: UDP is an unreliable, connectionless transport layer protocol.
51. value of the UDP port “Chargen” is  
    a) String of characters  
    b) String of integers  
    c) Array of characters with integers  
    d) Array of zero’s and one’s  
    Answer: a  
    Explanation: Chargen with port number 19 returns string of characters.
52. Beyond IP, UDP provides additional services such as  
    a) Routing and switching  
    b) Sending and receiving of packets  
    c) Multiplexing and demultiplexing  
    d) Demultiplexing and error checking  
    Answer: d  
    Explanation: UDP is a simple protocol which provides demultiplexing and error checking.
53. The main advantage of UDP is  
    a) More overload  
    b) Reliable  
    c) Less overload  
    d) Fast  
    Answer: c  
    Explanation: UDP is an unreliable, connectionless transport layer protocol and uses minimum overload.
54. number used by Network Time Protocol(NTP) with UDP is  
    a) 161  
    b) 123  
    c) 162  
    d) 124
55. what is the header size of UDP packet?  
    a) 8 bytes  
    b) 8 bits  
    c) 16 bytes  
    d) 124 bytes  
    Answer: a  
    Explanation: The fixed size of the UDP packet header is 8 bytes.
56. port number is “ephemeral port number”, if the source host is ……  
    a) NTP  
    b) Echo  
    c) Server  
    d) Client  
    Answer: d  
    Explanation: If the source host is the client, the port number in most cases will be ephemeral port number.
57. “Total length” field in UDP packet header is the length of  
    a) Only UDP header  
    b) Only data  
    c) Only checksum  
    d) UDP header plus data  
    Answer: d  
    Explanation: Total length is the 16 bit field which contains the length of UDP header and the data.
58. Correct expression for UDP user datagram length is  
    a) UDP length = IP length – IP header’s length  
    b) UDP length = UDP length – UDP header’s length  
    c) UDP length = IP length + IP header’s length  
    d) UDP length = UDP length + UDP header’s length  
    Answer: a  
    Explanation: A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram the defines the total length. There is another field in the IP datagram that defines the length of the header. So if we subtract the length of a UDP datagram that is encapsulated in an IP datagram, we get the length of UDP user datagram.
59. field used to detect errors over the entire user datagram is  
    a) UDP header  
    b) Checksum  
    c) Source port  
    d) Destination port  
    Answer: b  
    Explanation: Checksum field is used to detect errors over the entire user datagram.
60. broad categories of congestion control are  
    a) Open-loop and Closed-loop  
    b) Open-control and Closed-control  
    c) Active control and Passive control  
    d) None of the mentioned  
    Answer: a  
    Explanation: These are two types of congestion control.
61. In open-loop control, policies are applied to \_\_\_\_\_\_\_\_\_\_  
    a) Remove after congestion occurs  
    b) Remove after sometime  
    c) Prevent before congestion occurs  
    d) Prevent before sending packets  
    Answer: c  
    Explanation: Policies are applied to prevent congestion before it occurs.
62. Retransmission of packets must be done when  
    a) Packet is lost  
    b) Packet is corrupted  
    c) Packet is needed  
    d) All of the mentioned  
    Answer: d  
    Explanation: Retransmission should be done on account of any of the above cases.
63. In Go-Back-N window, when the timer of the packet times out, several packets have to be resent even some may have arrived safe. whereas in Selective Repeat window, tries to send \_\_\_\_\_\_\_\_\_\_\_  
    a) Packet that have not lost  
    b) Packet that have lost or corrupted  
    c) Packet from starting  
    d) All the packets  
    Answer: b  
    Explanation: In selective repeat window, packet that have lost or corrupted must be sent.
64. Discarding policy is mainly done by  
    a) Sender  
    b) Receiver  
    c) Router  
    d) Switch  
    Answer: c  
    Explanation: This is done by the routers to prevent congestion.
65. . Closed-Loop control mechanism try to  
    a) Remove after congestion occurs  
    b) Remove after sometime  
    c) Prevent before congestion occurs  
    d) Prevent before sending packets  
    Answer: a  
    Explanation: Policies are applied to remove congestion after it occurs.
66. technique in which a congested node stops receiving data from the immediate upstream node or nodes is called as  
    a) Admission policy  
    b) Backpressure  
    c) Forward signalling  
    d) Backward signalling  
    Answer: b  
    Explanation: This is a node-to-node congestion control that starts with a node and propagates in opposite direction of data flow to the source.
67. Backpressure technique can be applied only to  
    a) Congestion networks  
    b) Closed circuit networks  
    c) Open circuit networks  
    d) Virtual circuit networks  
    Answer: d  
    Explanation: In Virtual circuit networks, each node knows the upstream node from which a flow data is coming.
68. The packet sent by a node to the source to inform it of congestion is called  
    a) Explicit  
    b) Discard  
    c) Choke  
    d) Backpressure  
    Answer: c  
    Explanation: Choke packet is sent by a node to the source to inform it of congestion.
69. . In the slow-start algorithm, the size of the congestion window increases \_\_\_\_\_\_\_\_\_\_ until it reaches a threshold.  
    a) Exponentially  
    b) Additively  
    c) Multiplicatively  
    d) None of the mentioned  
    Answer: a  
    Explanation: In the slow-start algorithm, the size of the congestion window increases exponentially until it reaches a threshold.
70. Internet Control Message Protocol(ICMP) has designed to compensate  
    a) Error-reporting  
    b) Error-correction  
    c) Host and management queries  
    d) All of the mentioned  
    Answer: d  
    Explanation: ICMP has been designed to address these issues.
71. Header size of the ICMP message is  
    a) 8-bytes  
    b) 8-bits  
    c) 16-bytes  
    d) 16-bits  
    Answer: a  
    Explanation: ICMP message has 8-bytes header and variable size data section.
72. During error reporting, ICMP always reports error messages to  
    a) Destination  
    b) Source  
    c) Next router  
    d) Previous router  
    Answer: b  
    Explanation: ICMP sends error message to the source because the datagram knows information about source and destination IP address.
73. Which of these is not a type of error-reporting messages  
    a) Destination unreachable  
    b) Source quench  
    c) Router error  
    d) Time exceeded  
    Answer: c  
    Explanation: Router error is not a type of error-reporting messages in ICMP.
74. ICMP error message will not be generated for a datagram having a special address such as  
    a) 127.0.0.0  
    b) 12.1.2  
    c) 11.1  
    d) 127  
    Answer: a  
    Explanation: No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.
75. When a router cannot route a datagram or host cannot deliver a datagram, the datagram is discarded and the router or the host sends a \_\_\_\_\_\_\_\_\_\_\_\_ message back to the source host that initiated the datagram.  
    a) Destination unreachable  
    b) Source quench  
    c) Router error  
    d) Time exceeded  
    Answer: a  
    Explanation: Router sends destination unreachable message if the destination is not found.
76. The source-quench message in ICMP was designed to add a kind of \_\_\_\_\_\_\_\_\_\_\_\_ to the IP.  
    a) Error control  
    b) Flow control  
    c) Router control  
    d) None of the mentioned  
    Answer: b  
    Explanation: Firstly, it informs the source that the datagram has been discarded. secondly, it warns the source that there is congestion in the network.
77. In case of time exceeded error, when the datagram visits a router, the value of time to live field is  
    a) Remains constant  
    b) Decremented by 2  
    c) Incremented by 1  
    d) Decremented by 1  
    Answer: d  
    Explanation: This field will be decremented by 1 at every router, and will be zero by the time it reaches source.
78. Two machines can use the timestamp request and timestamp replay messages to determine the \_\_\_\_\_\_\_\_\_\_\_ needed for an IP datagram to travel between them.  
    a) Half-trip time  
    b) Round-trip time  
    c) Travel time for the next router  
    d) Time to reach the destination/source  
    Answer: b  
    Explanation: Router sends destination unreachable message if the destination is not found.
79. During debugging, we can use the \_\_\_\_\_\_\_\_\_\_\_\_ program to find if a host is alive and responding  
    a) Traceroute  
    b) Shell  
    c) Ping  
    d) Java  
    Answer: c  
    Explanation: Ping program is used to find if a host is alive and responding.