Chapter 13: Ethernet and TCP/IP Networking

1) The TCP/IP and OSI models are conceived and implemented as a hierarchical \_\_\_\_\_\_\_\_\_\_, in which each layer at the sending node contributes information that will be used by the corresponding peer layer at the receiving node.

a) rank structure

b) protocol stack

c) proprietary stack

d) communication levels

2) Which of the following is not part of the TCP/IP protocol suite?

a) http

b) ftp

c) SMS

d) ssh

3) A data packet in an Ethernet network is called a(n)

a) pack.

b) frame.

c) envelope.

d) container.

4) The data link layer is divided into \_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_ sublayers.

a) medium access control; logical link control

b) physical access control; logical link control

c) medium access control; virtual link control

d) physical access control; virtual link control

5) A \_\_\_\_\_\_\_\_\_\_\_\_\_ occurs when multiple nodes access and send data simultaneously in such a way that their messages become mixed together and garbled.

a) conflict

b) collision

c) confrontation

d) commingling

6) Switched Ethernet does not actually implement the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ protocol, because connections are point-to-point and messages can’t become mixed together and garbled.

a) ARP

b) L2TP

c) HDLC

d) CSMA/CD

7) What protocol is used to discover the relation between an IP address and a corresponding MAC address?

a) ARP

b) L2TP

c) HDLC

d) CSMA/CD

8) The amount of time that it takes for a packet to get from one end of the network to the other is called the

a) furthest node travel time.

b) network broadcast delay.

c) network propagation delay.

d) network diameter delay time.

9) The \_\_\_\_\_\_\_\_\_\_\_ is responsible for the addressing and routing of packets from the source end node through intermediate nodes, step by step, to their proper final destination.

a) transport

b) network layer

c) physical layer

d) Data Link Layer

10) Remember that the IP datagram may pass through different types of links. For certain types of physical layer connections, it is necessary to further divide the IP datagrams into smaller packets before they are delivered as frames to the data link layer. What are these smaller packets called?

a) pages

b) parcels

c) fragments

d) scatter grams

11) Although IP attempts to route every datagram to its final destination, it is a connectionless, packet switching service. IP is a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_ delivery service.

a) reliable best-effort

b) unreliable best-effort

c) reliable and guaranteed

d) unreliable but guaranteed

12) Such network tools as ping and traceroute use the query services of \_\_\_\_\_\_\_\_ to provide the information that they report.

a) ARP

b) FTP

c) ICMP

d) HTTP

13) The purpose of the \_\_\_\_\_\_\_\_\_\_\_ layer is to take messages from network applications and provide services that support reliable end-to-end communications.

a) network

b) physical

c) transport

d) Data Link

14) To identify the network application requesting service, the transport protocol identifies the application that created the message and the application that is to receive the message with

a) port numbers.

b) application numbers.

c) network node numbers.

d) application address numbers.

15) For communication between an application and the transport layer, operating systems provide an interface called a(n) \_\_\_\_\_\_\_\_\_\_\_, which makes it easy to add a request to the communication services provided by the TCP/IP suite.

a) socket

b) named interface

c) TCP/IP association

d) service association

16) TCP establishes a connection at the request of a network application. To initiate a connection, TCP sends a control packet to TCP at the Web site, requesting a connection; this results in a brief back-and-forth series of requests and acknowledgments known as

a) binding.

b) collaborating

c) handshaking.

d) service handling.

17) A connectionless protocol used instead of TCP for some applications is
a) user packet protocol.
b) user segment protocol.
c) user fragment protocol.
d) user datagram protocol.

18) An alternative to configuring individual workstations is to establish configurations dynamically when the computers connect to the network. What is this approach called?

a) NAT

b) DHCP

c) Masking

d) Dynamic NAT (DNAT)

19) What is the abbreviation for the protocol that translates domain names into IP addresses?

a) NAT

b) UDP

c) DNS

d) DHCP

20) Since DNS request packets are simple and small, \_\_\_\_\_\_\_\_\_\_\_\_\_\_ are used for packet transport.

a) IP packets

b) TCP packets

c) UDP datagrams

d) Ethernet frames

21) Two additional benefits of DNS services are: 1) permits the use of alias names that share the same IP address and 2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

a) perform load balancing for replicated servers

b) perform authentication on requesting computers

c) lower cost associated with managing IP addresses

d) enhance performance by caching multiple requests

22) In part, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ focuses on methods to reserve and prioritize channel capacity to favor packets that require special treatment.

a) DNS

b) QoS

c) TCP/IP

d) Ethernet

23) The variation in delay from packet to packet is known as \_\_\_\_\_\_\_\_\_. It is a particularly important parameter in the transmission of video and audio.

a) QoS

b) jitter

c) packet delay

d) network delay propagation

24) Modern routers, sometimes called \_\_\_\_\_\_\_\_\_\_\_\_, can prioritize and route packets based on the packet class.

a) QoS routers

b) Edge routers

c) Gateway routers

d) DiffServ capable nodes

25) Which of the following is a primary measure to keep the network and system resources intact and free from the results of intrusion?

a) CAPTCHAs

b) confidentiality

c) electronic signatures

d) limiting physical access to network wiring and network equipment.

26) Keeping the content of data traversing the network and information about the communication taking place private is known as

a) encryption.

b) authentication.

c) confidentiality.

d) nonrepudiation.

27) Protecting the content of data communication against changes is known as

a) integrity.

b) encryption.

c) confidentiality.

d) authentication.

28) Using encryption can be helpful in mitigating network security issues except

a) intrusion.

b) availability.

c) authentication.

d) nonrepudiation.

29) Reading data in all the packets as they pass through the network is known as

a) packet sniffing.

b) switch tapping.

c) packet spoofing.

d) packet cracking.

30) Symmetric key cryptography requires

a) two different keys, both private.

b) the same key be used for both encryption and decryption.

c) two different keys, one publicly available, and the other private.

d) the same key be used, one publicly available, and the other private.

31) The upper \_\_\_\_\_\_\_\_\_ layers of the OSI model assume that a successful end-to-end connection is established and maintained at the transport layer. These layers are concerned with the flow of data and control between applications on the communicating nodes.

a) two

b) three

c) four

d) five

32) The dialogue between two cooperating applications or processes at the ends of the communication link on the OSI model is known as a

a) session.

b) connection.

c) communications link.

d) time-sensitive service.

33) What is the name of the standard that includes the conversion of voice, as well as data, into IP data packets for transmission, as part of the specification?

a) VOIP

b) OSI LTE

c) Long Term Evolution (LTE)

d) Third generation mobile network

34) In cellular technology, the movement of the users from cell to cell is called a

a) handoff.

b) handover.

c) cell transfer.

d) next cell transfer.

35) MPLS operates at the \_\_\_\_\_\_\_\_\_\_\_\_ layer.

a) network

b) data link

c) transport

d) application

Discussion questions

1) What is the difference between "network application" and regular applications available to a user? Give three examples of each.

Sol: From the text: "The network applications represent standard protocols that are part of the TCP/IP protocol suite; they interface directly with other protocols that will break the message into packets and transport the message through the channel for retrieval by a corresponding network application at the receiving end."

Regular applications available to the user are email (Outlook), Word, Excel, PowerPoint, software development, and the like.

HTTP, FTP, and SSH are examples of network applications

Internet Explorer, Skype, and Dreamweaver are examples of regular applications available to a user.

2) In the Ethernet frame described in the text (figure 13.5), what is the minimum and maximum number of bytes?

Sol: (using Figure 13.5)

Preamble and start frame delimiter = 8

Destination and Source MAC addresses = 12

Number of data bytes = 2

Payload minimum = 46

CRC = 4

The minimum is 8 + 12 + 2 + 46 + 4= 72 bytes

Preamble and start frame delimiter = 8

Destination and Source MAC addresses = 12

Number of data bytes = 2

Payload maximum = 1500

CRC = 4

The maximum is 8 + 12 + 2 + 1500 + 4= 1526 bytes

3) Suppose a higher layer application wants to send a file 12MB in size across an Ethernet LAN. How many Ethernet frames are needed? Assume the largest Ethernet payload is 1500 bytes.

Sol: The goal is to send 12MB which must be broken down into Ethernet frames holding 1500 bytes of content each.

The file is 12 x 1,048,576 bytes = 12,582,912 bytes. So, 12582912 / 1500 = 8389 (rounded up) Ethernet frames are needed.

4) What two advantages does switched Ethernet have over hub-based Ethernet?

Sol:

Hub-based Ethernet is unsuitable for networks with widely separated nodes, due to the increase in the probability of collisions. Also because of collisions, networks covering longer ranges and higher speeds make hub-based Ethernet unsuitable.

Switched Ethernet has two additional advantages: (1) it is possible to connect nodes together in full-duplex mode, which is not possible with a single bus connection, and (2) each pair of connections can operate at the maximum bit rate of the network, since the media are unshared.

5) What is the network layer responsible for? What happens at each intermediate node in the packet's path?

Sol: From the text: "…the network layer is responsible for moving the message from sender to receiver, packet by packet, from one intermediate node to another through router packet switches. At each intermediate node, the network layer removes the current node's physical address and establishes an address for the next node, using various tables and algorithms. The new physical address is added to the packet and the packet is passed to the data link layer, which handles the actual connection between nodes."

6) The IP protocol attempts to route every datagram to its final destination, it is a connectionless, packet switching service. What is meant by "connectionless"?

Sol: From the text: "Connectionless means that every IP datagram is treated as an independent entity. Packet switching means that every datagram is routed independently. IP is an unreliable, best-effort delivery service: it does not guarantee delivery nor check for errors. Those tasks are the responsibility of the layer above, the transport layer, which takes responsibility for transmission of the entire message."

7) What happens when the ARP protocol is asked about an address it does not have cached?

Sol: From the text: "When ARP sees an IP address that it doesn't recognize, it sends a broadcast packet with the IP address to every node on the local network. The matching node responds with its physical address; in the case of Ethernet, the physical address is the MAC address of the destination node."

8) When initiating a connection, how does TCP establish a connection?

Sol: From the text: "To initiate a connection, TCP sends a control packet (through the usual network layers) to TCP at the Web site, requesting a connection; this results in a brief back-and-forth series of requests and acknowledgments known as handshaking."

9) Computers isolated on a local network access the Internet using a technique called network address translation (NAT). How does NAT work?

Sol: From the text: "A NAT-enabled router passes messages from the isolated network to the Internet, replacing the private address with the router's IP address. (Or addresses, since there might be multiple addresses available for this purpose.) Traffic passing through the NAT-enabled router to the outside, for example Web requests, must be carefully tracked by the router, so that responses from the outside are routed to the correct private address on the inside."

10) What types of network service qualities are particularly important for streaming audio and video applications, such as IPTV and VoIP?

Sol: From the text: "Certain types of data are dependent on reliable end-to-end transport where packets arrive at the receiving host in order, with sufficient throughput, with minimum, or at least, consistent, delay, at precise, even time intervals, and with a low probability of errors and missing packet failures."

11) An important quantity with regard to Quality of Service (QoS) is jitter. What is "jitter"?

Sol: From the text: "Jitter is defined as the variation in delay from packet to packet. It is a particularly important parameter in the transmission of video and audio because jitter causes large fluctuations in the image and sound."

12) What is a key requirement for a network to handle differentiated services needed for multimedia applications?

Sol: There must be nodes that can prioritize and route packets based on the differentiated services (DS) field.

From the text: "The DS field serves as an index into a table that defines various classes of service. For a particular set of packets, the DS field is set by the application at the sender or by the first node. Modern routers, sometimes called DiffServ capable nodes, can then prioritize and route packets based on the packet class.

13) What aspects of security does encryption *not* play an important role?

Sol: From the text: "Encryption in various forms is used to prevent intrusion, to protect privacy, for authentication, and to assure data integrity and nonrepudiation."

Encryption does not play a central role in availability.

14) What are the two fundamentally different kinds of algorithms used for encryption?

Sol: From the text: "Symmetric key cryptography requires that the same key be used for both encryption and decryption. This means that both users must have access to the same key, which is often difficult to achieve securely. The second category is called public key–private key cryptography, in which two different keys, one publicly available, the other private…."

15) Nearly all modern smartphones, some automobile dashboard systems, and some tablet computers provide data communication services, using cellular technology as the first link in a connection to the Internet. What global mobile communication standard is leading this convergence?

Sol: From the text: "..it appears that many of these systems are converging to a global mobile communication standard called Long Term Evolution (LTE), sometimes known as 4G LTE. Interestingly, LTE includes the conversion of voice, as well as data, into IP data packets for transmission, as part of the specification."

|  |  |  |
| --- | --- | --- |
| Problem | Answer | Section in text / comments |
| 1 | b | Section 13.1 TCP/IP, OSI, and Other Communication Protocol Models |
| 2 | c | 13.2 Program Applications vs. Network Applications |
| 3 | b | Section 13.3 The Physical and Data Link Layers |
| 4 | a | Section 13.3 The Physical and Data Link Layers |
| 5 | b | Section 13.3 The Physical and Data Link Layers |
| 6 | d | Section 13.3 The Physical and Data Link Layers |
| 7 | a | Section 13.3 The Physical and Data Link Layers |
| 8 | c | Section 13.3 The Physical and Data Link Layers |
| 9 | b | Section 13.3 The Physical and Data Link Layers |
| 10 | c | Section 13.4 The Network Layer |
| 11 | b | Section 13.4 The Network Layer |
| 12 | c | Section 13.4 The Network Layer |
| 13 | c | Section 13.5 The Transport Layer |
| 14 | a | Section 13.5 The Transport Layer |
| 15 | a | Section 13.5 The Transport Layer |
| 16 | c | Section 13.5 The Transport Layer |
| 17 | d | Section 13.5 The Transport Layer |
| 18 | b | Section 13.6 IP Addresses |
| 19 | c | Section 13.7 Domain Names and DNS Services |
| 20 | c | Section 13.7 Domain Names and DNS Services |
| 21 | a | Section 13.7 Domain Names and DNS Services |
| 22 | b | Section 13.8 Quality of Service |
| 23 | b | Section 13.8 Quality of Service |
| 24 | d | Section 13.8 Quality of Service |
| 25 | d | Section 13.9 Network Security |
| 26 | d | Section 13.9 Network Security |
| 27 | c | Section 13.9 Network Security |
| 28 | b | Section 13.9 Network Security |
| 29 | a | Section 13.9 Network Security |
| 30 | b | Section 13.9 Network Security |
| 31 | b | Section 13.10 Alternative Protocols |
| 32 | a | Section 13.10 Alternative Protocols |
| 33 | c | Section 13.10 Alternative Protocols |
| 34 | a | Section 13.10 Alternative Protocols |
| 35 | b | Section 13.10 Alternative Protocols |