TNE20003 internet and Cybersecurity for engineering

Revision question

1.How many networks are there in this topology?

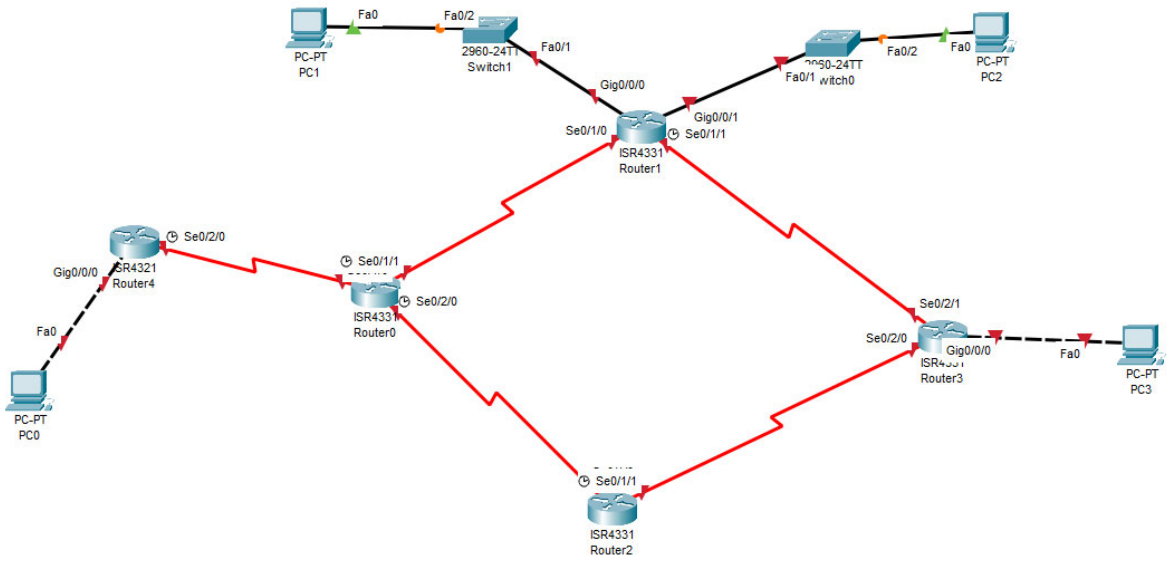


Figure 1.0
Answers: 9

2.How many bits do I need to borrow if I want to subnet 215.16.15.0/24?

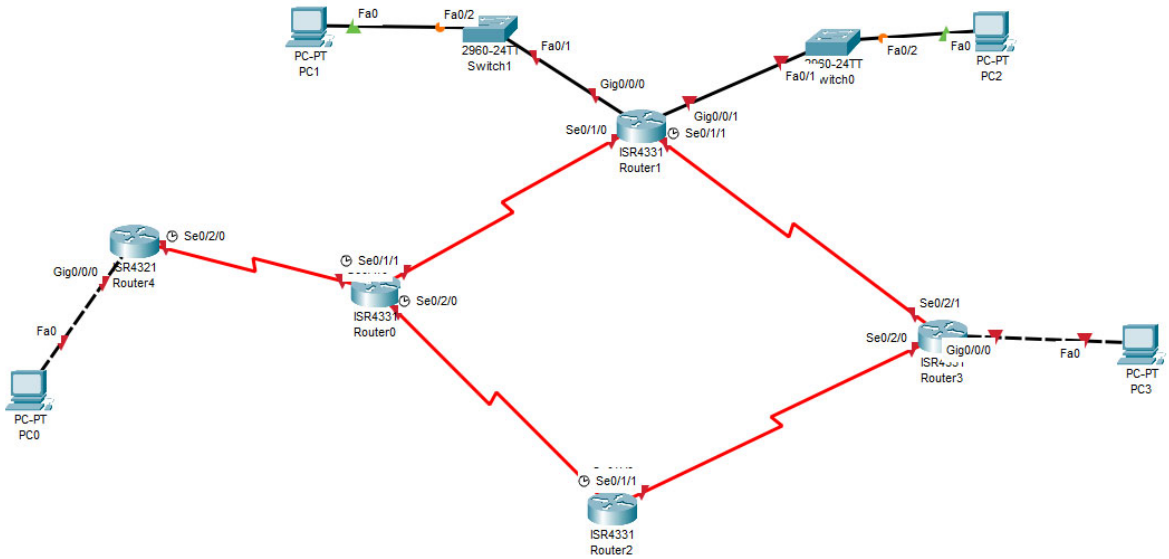
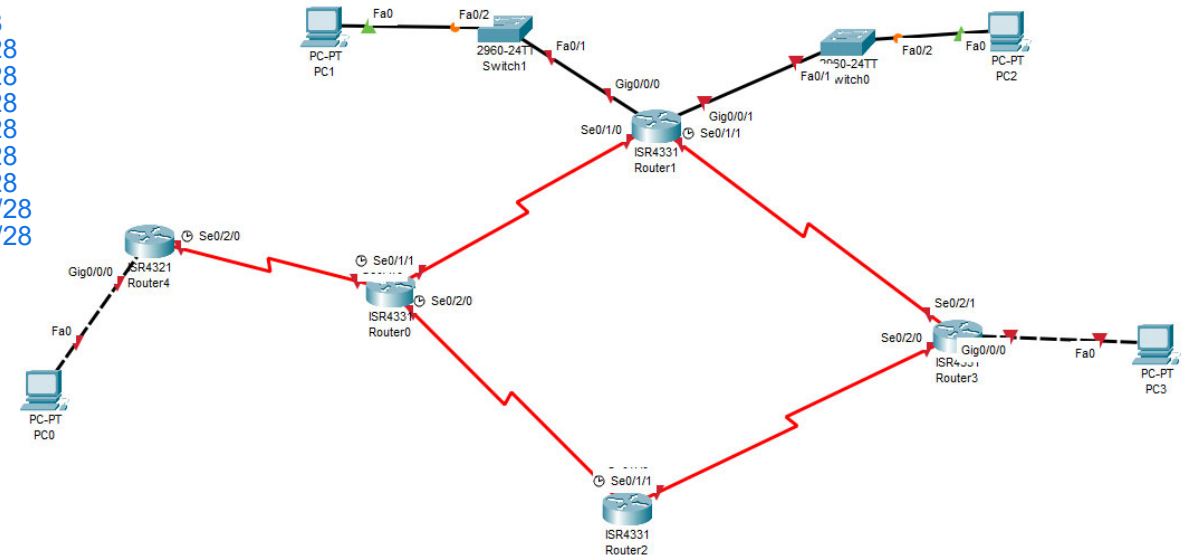


Figure 1.1

Answer 4

3.From this network work out the network address for 216.12.12.0/24

216.12.12.0 /28
216.12.12.16 /28
216.12.12.32 /28
216.12.12.48 /28
216.12.12.64 /28
216.12.12.80 /28
216.12.12.96 /28
216.12.12.112 /28
216.12.12.128 /28



Answer

4. Given the following address of 165.75.45.38/19 what is the network address?

Answer is 165.75.32.0 /19

5. If I have the following address of 199.32.34.0/21 what is the 8th subnet address?

Ans 199.32.88.0 /21

6. Choose the missing word from the list

sliding flow sequence threeway acknowledgement

- TCP ensures reliable data transmission by using a process called _____, which requires the receiving device to acknowledge the receipt of packets. acknowledgement
- The process in TCP where a connection is established between two devices by exchanging a series of packets is known as the threeway handshake.
- TCP uses flow control to prevent overwhelming the receiving device with too much data at once.

- In TCP, each segment is assigned a unique sequence number that helps in reordering the data packets in the correct sequence.
- The process of controlling the amount of data a TCP sender can transmit before receiving an acknowledgment is managed by the sliding window.

7.Choose the following words to fill out the questions:

acknowledgment
congestion
checksum
sequence
flow
retransmission
sliding
handshake

1. In TCP, after the threeway handshake, the sender starts transmitting data using sequence numbers to ensure proper sequencing and reordering.

2. TCP uses a combination of flow control and congestion avoidance to manage the transmission rate and prevent network overload.

3. To ensure data integrity, TCP calculates a checksum for each segment, and the receiver checks this value during retransmission of data to detect errors.

retransmission

4. When a packet is lost in transmission, TCP uses the _____ mechanism to resend the lost packet, and the sender waits for an _____ from the receiver before sending more data.

acknowledgement

8. Which of the following is a key characteristic of UDP?

a) Connectionoriented protocol
b) Provides reliable data transmission
c) No acknowledgment of received data
d) Utilizes flow control

9. UDP is primarily used for applications that require:

a) High reliability and error correction
b) Low latency and fast data transmission
c) Connection establishment before data transfer
d) Guaranteed packet delivery in order

10. Which of the following applications typically uses UDP?

a) Email
b) File Transfer Protocol (FTP)
c) Video streaming
d) Secure Shell (SSH)

11. Which of the following protocols operate primarily at the Transport Layer (Layer 4) of the OSI model, and what is the primary function of this layer?

a) HTTP and FTP; error detection and correction
b) TCP and UDP; segmentation and reliable data transfer
c) IP and ICMP; logical addressing and routing
d) ARP and DNS; hardware addressing and flow control

12. At which OSI layer does the process of encapsulation involve the addition of a frame header, and what does this header typically include?

a) Data Link layer; source and destination IP addresses
b) Transport layer; sequence and acknowledgment numbers
c) Data Link layer; MAC addresses and frame synchronization information
d) Network layer; source and destination MAC addresses

13. Which OSI layer is responsible for ensuring that data from a transmitting device is formatted correctly for the receiving device, and which of the following standards operate at this layer?

a) Application layer; HTTP and DNS
b) Presentation layer; JPEG and SSL/TLS
c) Session layer; NetBIOS and RTP
d) Network layer; IP and OSPF

14. Which OSI layers are involved in the process of establishing, managing, and terminating a communication session between two networked devices, and what protocols facilitate this?

a) Network and Data Link layers; ICMP and ARP
b) Presentation and Application layers; HTTPS and DNS
c) Session and Transport layers; NetBIOS and TCP
d) Physical and Transport layers; Ethernet and UDP

15. Which of the following is the primary purpose of DNS?
A) To translate domain names into IP addresses
B) To create network firewalls
C) To manage Internet traffic
D) To generate encryption keys

16. What is a DNS resolver?
A) A server that hosts domain names
B) A server that translates humanreadable domain names into IP addresses
C) A protocol used to secure DNS queries
D) A software used for configuring DNS records

17. Which DNS record type is responsible for linking a domain name to an IP address?
A) CNAME
B) MX
C) A (or AAAA for IPv6)
D) PTR

18. What is the function of a DNS root server?
A) It resolves IP addresses for all toplevel domains (TLDs).
B) It handles DNS queries for local networks.
C) It manages DNS records for specific domains.
D) It converts IP addresses into domain names.

19. What is the typical port used by DNS for resolving queries?
A) 80
B) 25
C) 53
D) 443

20. What does a CNAME record in DNS do?
A) It redirects email traffic to a mail server.
B) It maps a domain name to another domain name.
C) It links a domain to a subdomain.
D) It assigns an IP address to a domain name.

21. Which of the following is NOT a valid DNS record type?
A) A
B) MX
C) TTL
D) CNAME

22. What is the main purpose of HTTP in web communications?
A) Encrypting web traffic
B) Transmitting hypertext documents between a server and a client
C) Managing DNS queries
D) Securing network connections

23. Which of the following HTTP request methods is used to retrieve data from a server?
A) POST
B) DELETE
C) PUT
D) GET

24. Which HTTP method is typically used to submit data to be processed to a server?
A) GET
B) POST
C) HEAD
D) OPTIONS

25. What is the status code 404 in HTTP used for?
A) OK
B) Internal Server Error
C) Not Found
D) Moved Permanently

26. What does HTTPS add to the standard HTTP protocol?
A) Compression of data
B) Faster load times
C) Encryption and secure communication via SSL/TLS
D) Additional caching capabilities

27. Which of the following is a persistent connection in HTTP?
A) A connection that closes after each request
B) A connection that stays open for multiple requests/responses between the client and server
C) A connection used only for secure communications
D) A connection that supports only GET requests

28. What is the main purpose of DHCP in a network?
A) To assign dynamic IP addresses to devices
B) To encrypt network traffic
C) To resolve domain names to IP addresses
D) To monitor network traffic

29. Which of the following is a key advantage of using DHCP?
A) Increased network security
B) Automatic IP address assignment, reducing manual configuration
C) Faster DNS resolution
D) Improved data encryption

30. Which of the following is NOT a DHCP message type?
A) DHCPDISCOVER
B) DHCPOFFER
C) DHCPREQUEST
D) DHCPACKNOWLEDGE

31. Which protocol does DHCP use for communication?
A) TCP
B) UDP
C) ICMP
D) HTTP

32. What is the function of the DHCP lease time?
A) The amount of time DHCP servers wait before responding to requests
B) The duration for which an IP address is assigned to a client
C) The time a server takes to process a DHCP request
D) The time required for DNS resolution

33. Which of the following ports are used by DHCP?
A) 53 and 54
B) 67 and 68
C) 80 and 443
D) 110 and 143

34. What is the primary purpose of NAT?
A) To encrypt data packets during transmission
B) To map private IP addresses to a public IP address
C) To monitor network traffic
D) To resolve DNS queries

35. Which of the following is an advantage of NAT?
A) NAT increases data encryption across the network.
B) NAT helps conserve public IP addresses.
C) NAT provides faster DNS resolution.
D) NAT automatically assigns IP addresses like DHCP.

36. Which type of NAT maps multiple private IP addresses to a single public IP address?
A) Static NAT
B) Dynamic NAT
C) Port Address Translation (PAT)
D) Proxy NAT

37. Which of the following best describes static NAT?
A) It translates a private IP address to a different public IP address for each session.
B) It permanently maps a private IP address to a public IP address.
C) It randomly assigns IP addresses for network devices.
D) It converts IPv4 addresses to IPv6 addresses.
Answer: B) It permanently maps a private IP address to a public IP address.

38. What is one of the potential drawbacks of using NAT?
A) It requires the use of more public IP addresses.
B) It can slow down packet transmission by modifying IP headers.
C) It increases the number of available IP addresses.
D) It simplifies network configurations.

39. Which of the following types of NAT is most commonly used in home routers?
A) Static NAT
B) Dynamic NAT
C) Port Address Translation (PAT)
D) OnetoOne NAT

40. Which of the following features distinguishes TCP from UDP?
A) Connectionless communication
B) Connectionoriented communication with reliable delivery
C) Faster transmission due to lack of handshaking
D) Smaller packet size for lower overhead

41. What is the purpose of the threeway handshake in TCP?
A) To initiate a secure connection between client and server
B) To establish a connection, synchronize sequence numbers, and acknowledge the connection
C) To negotiate the window size and maximum segment size (MSS)
D) To encrypt the data stream before transmission

42. In TCP, what does flow control help achieve?
A) It prevents congestion in routers and switches.
B) It ensures that data is delivered to the correct application on the destination host.
C) It prevents the sender from overwhelming the receiver with too much data at once.
D) It compresses data to improve transmission speed.

43. Which of the following fields is unique to the TCP header but not present in the UDP header?
A) Source port
B) Destination port
C) Sequence number
D) Length

44. What is the purpose of the TCP window size?
A) It defines the maximum amount of unacknowledged data the sender can transmit.
B) It controls how much data can be stored in a buffer before transmission.
C) It limits the number of simultaneous connections allowed.
D) It sets the maximum number of retransmissions allowed.

45. Which of the following describes how TCP handles data loss?
A) TCP drops the connection and reestablishes it.
B) TCP relies on applicationlayer protocols to detect data loss.
C) TCP retran smits lost packets using sequence numbers and acknowledgements.
D) TCP ignores lost packets to maintain transmission speed.

46. Which of the following best describes UDP?
A) Connection oriented protocol with guaranteed delivery
B) Connectionless protocol with no guarantee of delivery
C) Protocol used for encrypted transmissions
D) Protocol that ensures flow control and error correction

47. Why is UDP preferred over TCP for realtime applications like video streaming or online gaming?
A) It provides reliable delivery and error correction.
B) It uses encryption to secure data.
C) It offers faster transmission by not waiting for acknowledgments or performing handshakes.
D) It has a more complex header for better traffic control.

48. Which of the following applications would most likely use UDP instead of TCP?
A) File Transfer Protocol (FTP)
B) Hypertext Transfer Protocol (HTTP)
C) Domain Name System (DNS) queries
D) Email (SMTP)

49. What is a key disadvantage of using UDP?
A) It consumes more bandwidth than TCP.
B) It does not guarantee that packets will arrive in the correct order or even arrive at all.
C) It introduces significant latency due to error checking.
D) It requires a connection to be established before sending data.

50. Which of the following is a typical use case for UDP?
A) Large file transfers that require reliable data delivery
B) Streaming media services where speed is more important than reliability
C) Email services that need encryption and confirmation of delivery
D) Database synchronization between servers

51. What is a key feature of the UDP header?
A) It contains a sequence number to track the order of packets.
B) It contains a checksum for optional error detection but no error correction.
C) It includes flow control to prevent network congestion.
D) It negotiates the packet size and flow rate with the receiving host.

52.A company is allocated the IP block 192.168.10.0/24. The company needs to create 6 subnets to accommodate departments with at least 30 hosts each. What subnet mask should be used for each subnet, and what are the network addresses for the subnets?

s/m: /27

1) 192.168.0.0 /27
2) 192.168.0.32 /27
3) 192.168.0.64 /27
4) 192.168.0.96 /27
5) 192.168.0.128 /27
6) 192.168.0.160 /27

53. Which of the following best describes the relationship between latency and throughput in a network?

a) High latency always results in higher throughput
b) Lower latency can improve throughput, but high throughput doesn't necessarily mean low latency
c) Low throughput causes lower latency
d) Latency and throughput are unrelated in network performance

54. What factors can contribute to high network latency?

a) Short transmission distance and a fast router
b) High congestion, physical distance, and packet queuing delays
c) High bandwidth and low data volume
d) Low error rate and large packet sizes

55.. Which metric measures the total amount of data successfully transmitted over a network in a given time, and how does it differ from latency?

a) Latency; measures the time it takes for a packet to travel from source to destination
b) Jitter; measures the variation in packet arrival times
c) Throughput; measures the data transmission rate, while latency measures delay
d) Bandwidth; measures the maximum capacity of a link, while latency measures reliability