Chapter 5 Sample MCQ

Software-Defined Networking (SDN) *(1–20)*

1. SDN primarily separates which two planes?
   - a) Transport and Application
   - b) Control and Data
   - c) Network and Application
   - d) Session and Transport
2. The core component of SDN architecture is:
   - a) Switch
   - b) Controller
   - c) Firewall
   - d) Router
3. OpenFlow is used for:
   - a) Packet encryption
   - b) Packet forwarding rules
   - c) Routing protocols
   - d) Network security
4. SDN controllers communicate with switches using:
   - a) Southbound API
   - b) Northbound API
   - c) REST API
   - d) BGP
5. An example of an SDN controller is:
   - a) TensorFlow
   - b) ONOS
   - c) Hadoop
   - d) Docker
6. Which is a benefit of SDN?
   - a) Manual configuration
   - b) Centralized management
   - c) Static routing
   - d) Fixed hardware
7. The Northbound API in SDN is used by:
   - a) Switches
   - b) Applications
   - c) Users
   - d) Routers
8. OpenFlow tables store:
   - a) User data
   - b) Flow entries
   - c) Programs
   - d) Port numbers only
9. SDN improves:

- a) Hardware dependency
- b) Network programmability
- c) Manual routing
- d) Static topology

10. SDN virtualizes:
    - a) Network functions
    - b) Cloud instances
    - c) Software
    - d) User applications
11. SDN is highly suitable for:
    - a) Static networks
    - b) Dynamic data centers
    - c) Traditional LANs
    - d) Small home routers
12. OpenFlow operates at:
    - a) Application layer
    - b) Control layer
    - c) Data plane
    - d) Transport layer
13. The controller's global network view enables:
    - a) Distributed routing
    - b) Optimal decision making
    - c) Hardware-based forwarding
    - d) Manual updates
14. Network Function Virtualization (NFV) is used to:
    - a) Replace hardware with software functions
    - b) Increase router size
    - c) Enhance cabling
    - d) Improve wireless signals
15. SDN enhances security through:
    - a) Distributed decision-making
    - b) Central policy enforcement
    - c) Manual firewalls
    - d) None
16. Flow rule installation is done by:
    - a) Hosts
    - b) Clients
    - c) Controller
    - d) Switch
17. Which protocol supports SDN southbound communication?
    - a) HTTP
    - b) OpenFlow
    - c) SMTP
    - d) FTP
18. SDN switches are also known as:
    - a) Dumb switches
    - b) Smart switches
    - c) Learning switches
    - d) Autonomous switches
19. SDN improves network:

   - a) Complexity
   - b) Flexibility
   - c) Latency
   - d) Cable length

20. A key challenge of SDN is:
   - a) Lack of programmability
   - b) Controller scalability
   - c) Static routing
   - d) High hardware cost

---

2. Fog Computing *(21–35)*

21. Fog computing operates:

- a) In the cloud
- b) Near the network edge
- c) Inside data centers
- d) On mobile phones

22. Fog computing reduces:

- a) Local processing
- b) Latency
- c) Edge usage
- d) Storage

23. A fog node may be:

- a) Cloud server
- b) IoT gateway
- c) End-user mobile
- d) None

24. Fog is suitable for:

- a) High-latency apps
- b) Autonomous vehicles
- c) Offline storage
- d) Long-distance routing

25. Fog computing extends:

- a) Data centers
- b) Cloud services to edge
- c) Physical LAN
- d) Satellite links

26. Fog nodes handle:

- a) Central control
- b) Local analytics
- c) GPU training
- d) WAN routing

27. Fog computing enhances:

- a) Cloud workloads
- b) Real-time processing
- c) Server memory
- d) Database replication

28. Fog reduces:

- a) Cloud dependency
- b) Edge devices
- c) Transmission speed
- d) Local data storage

29. Fog network architecture is typically:

- a) Layered
- b) Single-tier
- c) Peer-to-peer
- d) Centralized only

30. Fog computing supports:

- a) Industrial IoT
- b) Gaming consoles
- c) Social media
- d) Email automation

31. Fog helps minimize:

- a) Energy efficiency
- b) Bandwidth usage
- c) Processing power
- d) Local computation

32. Fog is more suitable than cloud for:

- a) Delay-sensitive tasks
- b) Backup storage
- c) Long-term computation
- d) Data warehousing

33. Fog nodes often connect using:

- a) SDN
- b) NFC
- c) Bluetooth only
- d) SMTP

34. Fog data analytics occur:

- a) At cloud
- b) Near data source
- c) On user devices
- d) In satellites

35. Fog computing enhances:

- a) Latency
- b) Real-time responsiveness
- c) Packet loss
- d) Congestion

---

3. Edge Computing *(36–50)*

36. Edge computing is designed to process data:

- a) In cloud
- b) At core network
- c) On local devices
- d) In routers only

37. Edge provides:

- a) Centralized storage
- b) Ultra-low latency
- c) High-latency computing
- d) Large data centers

38. A key example of edge devices:

- a) Datacenter servers
- b) IoT sensors
- c) Cloud VMs
- d) CDNs

39. Edge helps reduce:

- a) Real-time performance
- b) Cloud bandwidth usage
- c) Device intelligence

- d) Connectivity

40. Edge computing is essential for:

- a) VR/AR
- b) Email
- c) File storage
- d) Batch processing

41. Edge reduces:

- a) Response speed
- b) Latency
- c) Local tasks
- d) Security

42. Edge enhances:

- a) Privacy
- b) Broadcast
- c) Non-real-time apps
- d) WAN complexity

43. Edge supports:

- a) Time-critical computing
- b) High-power cloud-only apps
- c) Long-term archiving
- d) Database backups

44. Edge devices may process:

- a) AI inference
- b) Cloud orchestration
- c) Virtual machines
- d) Data center routing

45. Edge computing is widely used in:

- a) Autonomous driving
- b) Book printing
- c) Banking storage
- d) Web hosting

46. Edge reduces:

- a) Local computation
- b) WAN traffic
- c) Device sensors
- d) Processing power

47. A major challenge of edge:

- a) Decreased speed
- b) Security complexity
- c) Cloud cost
- d) Bandwidth increase

48. Edge nodes are generally:

- a) Distributed
- b) Centralized
- c) Layered in cloud
- d) Single-instance

49. Edge assists IoT systems by:

- a) Adding cloud usage
- b) Performing local decisions
- c) Delaying results
- d) Increasing traffic

50. Edge computing often works with:

- a) Fog and cloud
- b) LAN only
- c) Mobile SMS
- d) DNS only

---

4. Green Networking *(51–65)*

51. Green networking aims to:

- a) Increase energy use
- b) Reduce environmental impact
- c) Reduce device speed
- d) Remove wireless networks

52. A green networking strategy:

- a) Increase hardware size
- b) Energy-efficient routing
- c) Increase redundancy
- d) Reduce node sleep cycles

53. Energy-aware routing selects:

- a) Longest path

- b) Most energy-efficient path
- c) Random path
- d) Highest delay link

54. Green networking reduces:

- a) Energy consumption
- b) Efficiency
- c) Speed
- d) Security

55. A major driver for green networks:

- a) Global warming
- b) High latency
- c) Software updates
- d) User requests

56. Green data centers use:

- a) Renewable energy
- b) Gas generators
- c) Coal power
- d) Manual cooling

57. Power-efficient hardware uses:

- a) Static voltage
- b) Dynamic voltage scaling
- c) Manual routing
- d) Increased clocks

58. Green networking reduces:

- a) Carbon footprint
- b) Routing tables
- c) SDN usage
- d) TCP packets

59. Virtualization helps green networking by:

- a) Increasing servers
- b) Reducing hardware usage
- c) Increasing cooling
- d) Expanding data centers

60. A benefit of green networking:

- a) More hardware
- b) Lower energy cost

- c) Higher load
- d) Lower bandwidth

61. Energy-efficient Ethernet reduces energy when:

- a) Idle
- b) In use
- c) Overloaded
- d) Disconnected

62. Green networks may use:

- a) Sleep modes
- b) Max power mode
- c) Full utilization
- d) Always-on links

63. Cloud consolidation helps by:

- a) Reducing VMs
- b) Lowering energy
- c) Wasting resources
- d) Increasing cooling

64. Green networking improves:

- a) Cost efficiency
- b) Heat generation
- c) Traffic load
- d) Packet errors

65. Energy-efficient protocols aim to:

- a) Reduce RF power
- b) Increase congestion
- c) Increase CPU load
- d) Reduce performance

---

5. Quantum Networking *(66–80)*

66. Quantum networking uses:

- a) Classical bits
- b) Qubits
- c) Modems
- d) IPv4

67. Qubits can be:

- a) 0 or 1
- b) Both 0 and 1
- c) 2 only
- d) Undefined

68. A key quantum property enabling networking:

- a) Fragmentation
- b) Entanglement
- c) Congestion control
- d) Packet switching

69. Quantum communication is highly:

- a) Hackable
- b) Secure
- c) Slow
- d) Unstable

70. Quantum key distribution (QKD) ensures:

- a) Faster routing
- b) Secure key exchange
- c) Data compression
- d) Multipath routing

71. Quantum repeaters help:

- a) Extend qubit distance
- b) Increase cloud storage
- c) Speed up routers
- d) Reduce frequency

72. Quantum teleportation transmits:

- a) Matter
- b) Quantum states
- c) Packets
- d) Encryption

73. Quantum networks rely heavily on:

- a) Classical routers
- b) Photons
- c) Electric pulses
- d) Copper wires

74. A challenge in quantum networking:

- a) High latency
- b) Qubit decoherence
- c) Low encryption
- d) Routing loops

75. Quantum communication uses:

- a) Fiber optics
- b) Ethernet
- c) Satellite only
- d) Coaxial cables

76. Main benefit of quantum networking:

- a) Energy savings
- b) Unbreakable security
- c) Higher CPU usage
- d) Stronger signals

77. Quantum Internet aims to connect:

- a) Cloud centers
- b) Quantum computers
- c) Routers
- d) Mobile devices

78. Quantum channels transmit:

- a) Classical bits
- b) Qubits
- c) Cache data
- d) Noise

79. Entanglement distribution enables:

- a) Classical routing
- b) Secure communication
- c) UDP acceleration
- d) Multipath routing

80. Quantum routing is:

- a) Similar to TCP
- b) Probabilistic
- c) Static
- d) Rule-based

6. AI in Networking *(81–90)*

81. AI helps optimize:

- a) Manual routing
- b) Network performance
- c) Physical cable length
- d) Static addresses

82. Machine learning detects:

- a) Hardware faults
- b) Traffic anomalies
- c) Network power usage
- d) Cable wear

83. AI enhances:

- a) Congestion
- b) Predictive maintenance
- c) Manual configuration
- d) Latency

84. AI improves:

- a) Traffic management
- b) Cloud cooling
- c) Wi-Fi channels
- d) Power cables

85. Neural networks help in:

- a) Packet sniffing
- b) Pattern recognition
- c) Encryption
- d) Address allocation

86. AI-driven routing is:

- a) Manual
- b) Adaptive
- c) Static
- d) Random

87. AI improves network security by:

- a) Static rules
- b) Attack prediction
- c) Manual firewalls

- d) Deep packet blocking

88. AI can automate:

- a) Configuration
- b) Manual wiring
- c) OS installation
- d) Hardware assembly

89. AI-based traffic classification helps:

- a) Reduce QoS
- b) Improve QoS
- c) Eliminate latency
- d) Increase noise

90. AI in SDN controllers enables:

- a) Autonomous decisions
- b) Manual routing
- c) Slow updates
- d) Hardware changes

---

7. Next-Generation Protocols (Segment Routing, MPTCP, QUIC) *(91–100)*

91. Segment Routing is based on:

- a) Source routing
- b) Distance vector
- c) Static routing
- d) Flooding

92. Segment Routing uses:

- a) MAC addresses
- b) Segment identifiers
- c) DNS records
- d) Port numbers

93. Segment Routing simplifies:

- a) MPLS labels
- b) Routing state
- c) Packet size
- d) Encryption

94. MPTCP allows:

- a) Multiple subflows
- b) Single path only
- c) UDP tunneling
- d) Local switching

95. MPTCP improves:

- a) Congestion
- b) Reliability
- c) Manual routing
- d) Latency always

96. MPTCP is useful for:

- a) Dual-band Wi-Fi/5G devices
- b) Single-cable networks
- c) SMS
- d) FTP only

97. QUIC runs on:

- a) UDP
- b) TCP
- c) ICMP
- d) HTTP

98. QUIC improves:

- a) Connection migration
- b) Cable length
- c) VLAN switching
- d) DNS lookup

99. QUIC reduces:

- a) Handshake latency
- b) Encryption strength
- c) Mobility
- d) Security

100. QUIC is widely used in:

- a) Browsers (Chrome/Firefox)
- b) Switches
- c) Routers
- d) LAN hubs