Final Examination for the Course Software Defined Systems

Maximum score: 50%

Time Allowed: 2hrs

Item	True/ False	MSQ	Short Answer	Scenario based	Total
Value	5%	25%	12%	8%	50%

Part I: True or False Items

Instruction*: Indicate whether each of the following statements is true or false. Circle "True" if the statement is correct, or "False" if the statement is incorrect.** ***(total 5pts – 1pt each)

1. Routers and switches in an SDN network have their own control plane.
2. In an SDN network, network devices are responsible for making forwarding decisions.
3. SDN can only be implemented using OpenFlow as the communication protocol between the controller and network devices.
4. Virtualization allows for the migration of virtual machines between physical hosts with no downtime.
5. Multi-tenancy, where multiple customers share the same physical infrastructure, is a fundamental characteristic of private cloud deployments.

Part II: Multiple Choice Items

Instruction*: For each of the following questions, select the one answer choice that best completes the statement or answers the question. Circle the letter of your chosen answer.** ***(total 25pts – 1pt each)

1. Which of the following is a key component of an SDN architecture?
   A. Firewall
   B. SDN controller
   C. Router
   D. Switch
2. Which of the following is a potential challenge in SDN implementation?
   A. Vendor lock-in
   B. Increased network flexibility
   C. Improved network visibility
   D. Simplified network management
3. Which of the following is not a key characteristic of SDN?
   A. Centralized control
   B. Network programmability
   C. Static network topology
   D. Logically centralized control plane

4. The protocol used for communication between the SDN controller and network applications is the:
    A. OpenFlow protocol
    B. Northbound API
    C. Southbound API
    D. OVSDB protocol
5. Which of the following is ***not*** a common use case for SDN?
    A. Network virtualization
    B. Compute virtualization
    C. Traffic engineering
    D. Network slicing
6. In an SDN architecture, the network devices are responsible for:
    A. Making forwarding decisions
    B. Real-time traffic steering
    C. Implementing network policies
    D. None of the above
7. SDN can be used to implement which of the following network functions?
    A. Load balancing
    B. Network security
    C. Quality of Service (QoS)
    D. All of the above
8. Which of the following best describes the relationship between the SDN controller and the network devices in an SDN architecture?
    A. The SDN controller makes all the forwarding decisions and instructs the network devices on how to handle network traffic.
    B. The network devices make all the forwarding decisions independently, while the SDN controller only provides high-level policies and configurations.
    C. The SDN controller and the network devices work collaboratively, with the controller providing the overall network intelligence and the devices handling the actual packet forwarding.
    D. The SDN controller and the network devices operate completely independently, with no direct communication between them.
9. An organization is considering implementing SDN to improve the flexibility and agility of their network. Which of the following potential benefits of SDN would be the most relevant to this goal?
    A. Increased network visibility and monitoring capabilities
    B. Simplified network management and reduced operational costs
    C. The ability to quickly and dynamically modify network policies and configurations
    D. Improved network security through centralized access control and traffic monitoring

10. An SDN network administrator wants to integrate a new network application that requires access to real-time network statistics and the ability to influence traffic routing decisions. Which of the following SDN architectural components would be the most appropriate for this use case?
    A. The southbound API, which allows the network application to communicate directly with the network devices
    B. The northbound API, which provides the network application with a programmatic interface to interact with the SDN controller
    C. The OpenFlow protocol, which defines the communication between the SDN controller and the network devices
    D. The forwarding plane, which is responsible for the actual packet processing and forwarding within the network devices
11. A network engineer is evaluating different SDN solutions and is concerned about potential vendor lock-in issues. Which of the following approaches would be the most effective in mitigating this concern?
    A. Deploying an SDN solution that uses proprietary protocols and interfaces for communication between the controller and network devices
    B. Choosing an SDN solution that supports multiple, standard-based southbound protocols to enable interoperability with a variety of network hardware
    C. Implementing a custom SDN controller developed in-house, which can be easily integrated with the organization's existing network infrastructure
    D. Adopting an SDN solution that requires the use of specialized, SDN-enabled network hardware from a single vendor
12. What type of virtualization allows a single physical desktop to be shared by multiple users?
    A. OS virtualization
    B. Server virtualization
    C. Network virtualization
    D. Desktop virtualization
13. What is the main function of a hypervisor in a virtualized environment?
    A. Manage virtual machine lifecycles
    B. Allocate physical hardware resources
    C. Host the guest operating systems
    D. All of the above

14. What is the primary difference between Type 1 and Type 2 hypervisors?
    A. Type 1 runs on bare metal, while Type 2 runs on top of a host OS
    B. Type 1 supports more virtual machines than Type 2
    C. Type 1 has lower performance overhead than Type 2
    D. Type 1 provides better security isolation than Type 2
15. Which virtualization technique allows multiple applications to be virtualized and run in isolation from each other?
    A. Server virtualization
    B. Desktop virtualization
    C. Container virtualization
    D. Network function virtualization
16. Which virtualization technology enables the dynamic allocation of network as software components?
    A. Application virtualization
    B. Storage virtualization
    C. Network function virtualization
    D. GPU virtualization
17. What is the primary benefit of using virtual machines instead of physical machines for development and testing?
    A. Faster provisioning of new environments
    B. Reduced hardware costs
    C. Increased security
    D. Improved application performance
18. What is the primary purpose of micro-segmentation?
    A. To create larger network segments
    B. To increase network complexity
    C. To enhance security through granular access control
    D. To reduce network bandwidth utilization
19. Which of the following is a key characteristic of an Intent-Based Networking system?
    A. It relies on manual configuration of network devices
    B. It requires a highly skilled network engineering team
    C. It provides a high-level abstraction of desired network behavior
    D. It is limited to static network environments
20. A cloud provider's responsibility in the shared responsibility model typically includes:
    A. Securing the physical data centers
    B. Implementing access control for user accounts
    C. Maintaining the guest operating system
    D. All of the above

21. Which one of the following is true about the difference between a public cloud and a private cloud?
    A. Public cloud is free, while private cloud requires investment.
    B. Public cloud offers shared resources, while a private cloud is dedicated to a single organization.
    C. Public cloud is more secure than a private cloud.
    D. Public cloud offers better performance than a private cloud.
22. In a multi-tenant cloud environment, which security isolation technique leverages virtual LANs (VLANs) to slice traffic for different tenants?
    A. Resource virtualization
    B. Network segmentation
    C. Data encryption
    D. Identity and Access Management (IAM)
23. Which of the following best describes the concept of Infrastructure as a Service (IaaS) from a user control perspective?
    A. Users manage the underlying hardware but not the operating system.
    B. Users have full control over the virtualized infrastructure, including operating system and applications.
    C. Users manage the application code but not the platform or infrastructure.
    D. Users access software applications over the internet without managing any underlying resources.
24. Emerging trends in cloud computing include serverless computing. What is the PRIMARY advantage of serverless architecture for application development?
    A. Improved security posture through centralized server management by the cloud provider.
    B. Increased development time due to the need to manage server infrastructure.
    C. Reduced development and operational costs by paying only for the resources actually used.
    D. Granular control over server configuration and resource allocation for optimal performance.
25. Identity and Access Management (IAM) in cloud security is primarily concerned with:
    A. Encrypting data at rest and in transit
    B. Controlling user access to cloud resources
    C. Isolating network traffic for different tenants
    D. Monitoring and auditing cloud activity for security threats

Part III: Short Answer Items *(total 12pts)*

***Instruction*: Provide a short answer to each of the following questions. Write your answers in the space provided.**

1. Briefly explain the difference between traditional network management and SDN. ***(2pts)***
2. List and discuss at least ***four*** common network functions ***(4pts)***
3. Explain the concept of elasticity in cloud computing and how it differs from scalability. ***(1pt)***
4. What is a Secure Channel in an SDN Controller, and What protocols are used in SDN? ***(2pts)***
5. Describe three common cloud deployment models and the trade-offs between them in terms of control, security, and cost. ***(3pts)***

Part IV – Scenario based Items *(total 8pts)*

***Instruction*: Read the scenario carefully and then answer the related question(s) that follow. Provide thorough, well-reasoned responses based on the information given in the scenario.**

Scenario:

Your company has a server with limited physical resources that is struggling to keep up with the growing demands of your business. You want to explore virtualization as a way to better utilize the server's hardware and run multiple virtual machines (VMs) on it.

As the IT manager, answer the following questions.

a) Explain what virtualization is and how it works. ***(2pts)***
b) Discuss the key advantages of virtualization, such as improved resource utilization, increased flexibility, and cost savings. ***(2pts)***
c) Recommend the steps you would take to set up a virtualized infrastructure, including selecting a hypervisor, planning VM configurations, and migrating existing workloads. ***(2pts)***
d) Outline any potential challenges or risks to consider, and how you would mitigate them. ***(2pts)***