DUMPSARENA

# AI+ NetworkExamination

## AI CERTs AT-510

**Version Demo**

**Total Demo Questions: 6**

**Total Premium Questions: 61**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Introduction to AI in Networking | 12 |
| Topic 2, AI-Driven Network Automation | 16 |
| Topic 3, AI for Network Security | 15 |
| Topic 4, AI in Network Optimization | 9 |
| Topic 5, Predictive Network Analytics | 3 |
| Topic 6, AI-Enabled Network Management | 1 |
| Topic 7, Emerging Trends and Future Directions | 5 |
| Total | 61 |

QUESTION NO: 1

(How can SDN controllers enhance VNET management?)

**A.** Decentralized control

**B.** Limited visibility into the network

**C.** Simplified local configuration

**D.** Automated task provisioning

**ANSWER: D**

**Explanation:**

Automated task provisioning is correct because an SDN controller provides a centralized, programmable control plane that can translate high-level network policies into consistent configurations across the virtual network infrastructure. Rather than requiring administrators to configure individual virtual switches, routes, segmentation rules, and service policies separately, the controller can use APIs and automation workflows to deploy these settings at scale. This makes VNET management faster, more repeatable, and less prone to configuration drift or manual error. For example, when a new virtual network or workload is created, the controller can automatically apply the required connectivity, access-control, quality-of-service, and isolation policies. Centralized automation also lets operations teams update policies rapidly as application requirements or security needs change, while maintaining a unified view of the intended network state. The Open Networking Foundation describes SDN as separating the control plane from forwarding functions and enabling network control to be directly programmable, which is the architectural basis for automated provisioning. The NIST SDN definition similarly identifies centralized control and programmability as core characteristics that support efficient network management. See the Open Networking Foundation SDN definition and NIST cloud computing reference architecture.

**QUESTION NO: 2**

Scenario: A 5G operator supports an autonomous-vehicle service requiring low latency and a consumer video service requiring high throughput. Both services share physical infrastructure, but peak video demand begins affecting vehicle-message delivery.

Question: Which network-slicing strategy best addresses the problem?

**A.** Place both services in one undifferentiated slice to maximize shared capacity.

**B.** Assign fixed equal bandwidth to each service regardless of current conditions.

**C.** Prioritize video traffic because it consumes the greatest volume of bandwidth.

**D.** Allocate and continuously adjust slice resources according to each service's latency and throughput requirements.

**ANSWER: D**

**Explanation:**

**Allocate and continuously adjust slice resources according to each service's latency and throughput requirements.** is correct because network slicing creates logical service environments with distinct performance objectives on shared infrastructure. AI-assisted monitoring and automation can adjust resources as demand changes while preserving the low-latency requirements of the autonomous-vehicle slice.

Placing both services in one undifferentiated slice prevents service-specific treatment. Assigning fixed equal bandwidth ignores changing demand and differing service objectives. Prioritizing video would directly conflict with the requirement to protect time-sensitive vehicle communications.

**QUESTION NO: 3**

Scenario: A 5G operator uses network slices for a remote-surgery application and for consumer video streaming. A sudden video-demand increase begins consuming shared resources and risks increasing delay for the remote-surgery service.

Question: Which action best preserves the remote-surgery service objective?

**A.** Apply slice-specific resource and quality-of-service policies that protect the low-latency service.

**B.** Assign identical bandwidth and latency treatment to both slices.

**C.** Merge the two services into a single shared network slice.

**D.** Reduce performance telemetry so that video demand does not trigger policy changes.

**ANSWER: A**

**Explanation:**

Applying slice-specific resource and quality-of-service policies that protect the low-latency service is correct. Network slicing allows logically distinct services to operate on shared infrastructure with different performance requirements. The remote-surgery slice should receive policies and resource treatment aligned with its stringent latency and reliability needs, while video traffic can use the remaining or separately controlled capacity.

Assigning identical treatment to both services ignores their different service requirements. Sending all traffic through one slice removes the isolation benefit, and reducing telemetry would make it harder to identify and manage resource contention.

## QUESTION NO: 4

(Which system is best for detecting unauthorized logins and adapting to new threats?)

**A.** Static firewalls

**B.** Load balancers

**C.** Reactive AI

**D.** Machine learning-driven intrusion detection

**ANSWER: D**

**Explanation:**

Machine learning-driven intrusion detection is the best choice because an intrusion detection system monitors network and system activity for indicators of compromise, including anomalous authentication behavior such as repeated failed logins, logins from unusual locations, impossible travel patterns, or access attempts outside a user's normal schedule. Machine-learning models strengthen this capability by establishing a baseline of expected behavior from historical and real-time telemetry, then identifying deviations that may indicate compromised credentials, brute-force attacks, or unauthorized access. This behavioral approach is especially valuable for new threats because it is not limited solely to previously defined signatures or manually written rules. As environments, users, and attack techniques change, models can be retrained and tuned using fresh data to improve detection quality and reduce alert fatigue. Effective deployment also combines the detection system with centralized logging, incident-response workflows, and human review, so that high-risk findings can be investigated and contained promptly. The National Institute of Standards and Technology describes intrusion detection and prevention technologies and their monitoring role in NIST SP 800-94. Guidance on detecting anomalous account behavior and responding to identity-related threats is also available from CISA Cyber Threats and Advisories.

## QUESTION NO: 5

Scenario: A network-operations team trains a model to predict WAN congestion using interface utilization collected every five minutes. Several branch routers have intermittent telemetry gaps, and the model begins recommending capacity upgrades for links that operators know are lightly used.

Question: Which action should the team take before relying on the model's recommendations?

**A.** Increase the model's complexity so it can infer all missing telemetry values.

**B.** Validate and clean the telemetry data, including missing-value handling and timestamp consistency.

**C.** Automatically add bandwidth to every link identified as congested.

**D.** Remove all low-utilization links from the training data.

**ANSWER: B**

**Explanation:**

**Validate and clean the telemetry data, including missing-value handling and timestamp consistency.** is correct because predictive models treat their input observations as evidence of network behavior. Missing samples, inconsistent collection intervals, duplicated records, or incorrectly aligned timestamps can distort utilization trends and produce false congestion forecasts.

Increasing model complexity or automating recommendations does not correct unreliable inputs. Adding bandwidth may address a genuine capacity constraint, but it would be premature when the observed issue may be caused by data quality. A validated telemetry pipeline provides the dependable historical data required for meaningful forecasting.

**QUESTION NO: 6**

(What is a key advantage of using Ansible for network automation?)

**A.** It utilizes an agentless architecture for managing devices.

**B.** It relies on Ruby scripts for configuration tasks.

**C.** It mandates pre-installation of agents on managed devices.

**D.** It limits network management to Linux-based devices only.

**ANSWER: A**

**Explanation:**

It utilizes an agentless architecture for managing devices. This is a central advantage of Ansible in network automation because managed network devices generally do not need an Ansible agent installed locally. Instead, Ansible runs from a control node and communicates with devices through supported connection methods, commonly SSH, HTTPS-based APIs, or vendor-specific network APIs. This reduces deployment effort because teams do not have to install, update, monitor, and secure an additional software component across every router, switch, firewall, or controller.

Agentless operation is particularly valuable in heterogeneous network environments, where devices may use different network operating systems and have constrained storage or processing capabilities. Ansible network collections provide platform-specific modules that let playbooks express intended configuration and operational tasks in YAML while using the appropriate connection mechanism underneath. This makes automation easier to adopt, supports repeatable changes at scale, and helps teams standardize workflows across multi-vendor infrastructure. Ansible documentation describes network automation as executing playbooks from a control node without requiring an agent on the managed node, and its network connection documentation details the available network connection methods. See Ansible Network Getting Started: Differences from Linux and Ansible Network Connection Options.