Exam

350-401

Implementing Cisco Enterprise Network Core Technologies

Free demo	40 sample questions
Full exam	271 questions with answers and explanations
Contents	Questions with answers and explanations

Exam domains

Domain	Exam weight	Questions
D1 Architecture		11
D2 Virtualization		3
D3 Infrastructure		6
D4 Network Assurance		1
D5 Security		9
D6 Automation and Artificial Intelligence		10

This is a free demo from Dumpsgate: 40 of the exam's 271 questions. **Get the full 350-401 exam** with every question, answer and explanation.

Case study

This section contains standalone questions (no scenario).

Implementing Cisco Enterprise Network Core Technologies Exam Syllabus & Objectives Exam Overview The Cisco 350-401 certification exam validates your ability to implement and maintain enterprise-grade network solutions using Cisco technologies. This exam assesses both foundational knowledge and hands-on configuration skills across multiple domains of modern networking, including traditional infrastructure, software-defined networking, virtualization, security, and automation capabilities.

Architecture and Design Principles (15%)

This domain focuses on understanding how enterprises structure their networks and the architectural patterns that enable scalability and reliability. You will explore classical tiered network designs, modern fabric-based approaches, and cloud-integrated architectures. High-availability techniques form a critical component, requiring you to understand redundancy strategies, First Hop Redundancy Protocols, and stateful switchover mechanisms that keep networks operational during failures. Additionally, you must comprehend Cisco's software-defined solutions that modernize network operations. The SD-WAN curriculum covers how control and data planes work together to optimize wide-area network performance and application delivery. Similarly, SD-Access principles teach you how campus networks evolve through software-defined methods while maintaining compatibility with traditional deployments.

Quality of Service configurations round out this section, ensuring you can interpret how traffic prioritization mechanisms operate.

Virtualization Technologies (10%)

Modern networks depend on virtualization to improve resource utilization and operational flexibility. You need to understand device-level virtualization through hypervisors—both bare-metal and hosted varieties—and virtual machine principles. Virtual switching extends network functionality into hypervisor environments, creating complex multi-tenant scenarios. Data path virtualization enables logical network segmentation and secure connectivity through technologies like Virtual Routing and Forwarding, Generic Routing Encapsulation, and IPsec tunneling. Network virtualization adds another abstraction layer, allowing physical infrastructure to support multiple logical networks simultaneously. You will encounter protocols such as Locator/ID Separation Protocol and Virtual Extensible Local Area Network that accomplish this abstraction at scale.

Infrastructure—Layer 2 and Layer 3 Technologies (30%)

This largest domain thoroughly covers the protocols and configurations that form network foundations.

At Layer 2, you must troubleshoot trunking protocols, Ethernet channel aggregation, and Spanning Tree variants including Rapid Spanning Tree and Multiple Spanning Tree. You should understand protective mechanisms like root guard and Bridge Protocol Data Unit guard that enhance network stability. Layer 3 content emphasizes dynamic routing protocols that form the backbone of enterprise networks. You will compare distance-vector and link-state paradigms through detailed examination of Enhanced Interior Gateway Routing Protocol and Open Shortest Path First, including their advanced features like load balancing and summarization. Border Gateway Protocol fundamentals teach you how autonomous systems interconnect globally and apply policy-based selection criteria. Basic policy-based routing concepts also appear in this section. IP Services subsection covers operational technologies that Operational excellence requires sophisticated diagnostic and monitoring capabilities. You must be proficient with tools that reveal network behavior, including packet inspection through debug commands, conditional filtering, route tracing, and echo requests. Network monitoring protocols like Simple Network Management Protocol and syslog provide visibility at scale. Advanced monitoring capabilities include Flexible NetFlow for traffic analysis, SPAN, RSPAN, and ERSPAN for traffic mirroring, and IP Service Level Agreement for performance measurement. Cisco Catalyst Center—the evolved DNA Center platform—provides orchestration, configuration management, and AI-assisted workflows that modernize network operations. Finally, NETCONF and RESTCONF represent the programmatic configuration interfaces you must understand for infrastructure management.

Network Security (20%)

Security permeates modern enterprise networks, and this domain requires you to implement protective mechanisms at multiple levels. Device access control begins with authentication at connection points,

Free demo · full exam: 271 questions

including local credential management and centralized AAA services. Infrastructure protection involves Access Control Lists for traffic filtering and Control Plane Policing to prevent denial-of-service attacks.

Security design spans multiple architectural layers, from threat defense appliances to endpoint protection mechanisms and next-generation firewalls that understand application-layer threats.

Advanced security frameworks like Cisco TrustSec and Media Access Control Security provide identity-based access and encrypted data plane protection. REST API security considerations round out the security topics, addressing how modern programmable networks maintain protection while enabling automation.

Automation and Artificial Intelligence (15%)

Contemporary network engineers must understand automation fundamentals and emerging AI capabilities. You will work with Python scripting basics, recognizing common programming constructs and interpreting existing code samples. JSON encoding skills enable you to work with modern APIs and configuration formats. Data modeling languages such as YANG provide structured approaches to describing network configuration and operational data. Cisco Catalyst Center and SD-WAN Manager APIs An enterprise architect is designing a new campus network for a 500-person office with plans to scale to 2,000 employees over the next three years. The network must support high availability, separate control and data planes, and policy-based segmentation using dynamic paths. Which design approach best aligns with these requirements while enabling zero-trust principles?

A. Traditional 3-tier hierarchical design with static access control lists

B. SD-Access architecture with Cisco Catalyst Center and policy-based segmentation via Cisco

TrustSec

C. Flat 2-tier design with all switches connected directly to core routers

D. Pure fabric design using only VXLAN without controller integration

Answer: B

SD-Access is the correct choice because it provides a controller-driven architecture (Cisco Catalyst Center) that separates control and data planes, enables dynamic policy-based segmentation through TrustSec (scalable beyond traditional ACLs), and inherently supports high availability and scalability. The architecture uses VXLAN for underlay encapsulation and allows the network to grow without redesigning the physical topology.

A traditional 3-tier design lacks dynamic policy capabilities and does not separate control/data planes. A 2-tier flat design creates scalability and performance bottlenecks. A fabric-only design without controller integration loses centralized policy management and visibility that the scenario requires.

Question 1

Single choice · Domain: D1 Architecture › Describe how the StackWise active switch synchronizes a newly added stack member

SINGLE CHOICE

An engineer adds a new switch to a Cisco StackWise stack. The switch that was active before the switch was added is elected as the active switch again. Which action does the active switch take?

A. It checks the IOS and running configuration of the new switch and updates them if necessary to match stack.

Answer: A. It checks the IOS and running configuration of the new switch and updates them if necessary to match stack.

Explanation

This question tests StackWise high-availability behavior when a switch joins an existing stack. The active

Free demo · full exam: 271 questions

switch verifies the new member's software and configuration and synchronizes them as necessary so the stack operates consistently.

✓ **A** It checks the IOS and running configuration of the new switch and updates them if necessary to match stack.
Correct. When a switch is added to a Cisco StackWise stack, the active switch provides the stack configuration and ensures that the new member uses a compatible software image and configuration. This maintains consistent operation across stack members.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/stck_mgr/b_179_stck_mgr_9300_cg.html

---

Question 2

Single choice · Domain: D1 Architecture › Identify modularity as the use of self-contained, repeatable network design components

SINGLE CHOICE

What is modularity in network design?

A. Ability to self-heal the network to prevent service outages
B. Ability to scale and accommodate future needs of the network
C. Ability to create self-contained, repeatable sections of the network
D. Ability to bundle several functions into a single layer of the network

Answer: C. Ability to create self-contained, repeatable sections of the network

Explanation

This question tests understanding of modular network architecture, in which functional and repeatable building blocks can be designed, deployed, and expanded independently. Modularity supports scalability and operational consistency but is distinct from self-healing, general scalability, or function consolidation.

✗ **A** Ability to self-heal the network to prevent service outages
Incorrect. Self-healing describes resiliency or fault recovery, not modularity. Modularity concerns organizing the network into repeatable, self-contained components.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise/campus-lan-wlan/design-guide-c07-743908.html

✗ **B** Ability to scale and accommodate future needs of the network
Incorrect. This describes scalability. A modular design can improve scalability, but modularity specifically means constructing the network from self-contained, repeatable modules.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise/campus-lan-wlan/design-guide-c07-743908.html

✓ **C** Ability to create self-contained, repeatable sections of the network
Correct. Modularity is the practice of designing a network as self-contained, repeatable functional sections or building blocks that can be deployed and expanded consistently.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise/campus-lan-wlan/design-guide-c07-743908.html

✗ **D** Ability to bundle several functions into a single layer of the network
Incorrect. Bundling multiple functions into one layer describes function consolidation or a collapsed-layer design, not modularity. Modularity separates repeatable functions into defined building blocks.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise/campus-lan-wlan/design-guide-c07-743908.html

Question 3

Single choice · Domain: D1 Architecture › Identify the management-plane role of Cisco Catalyst Center in an SD-Access fabric

SINGLE CHOICE

What is the function of Cisco Catalyst Center (formerly DNA Center) in a Cisco SD-Access deployment?

A. It is responsible for routing decisions inside the fabric.

B. It possesses information about all endpoints, nodes, and external networks related to the fabric.

C. It provides integration and automation for all nonfabric nodes and their fabric counterparts.

D. It is responsible for the design, management, deployment, provisioning, and assurance of the fabric network devices.

Answer: D. It is responsible for the design, management, deployment, provisioning, and assurance of the fabric network devices.

Dumpsgate

Explanation

This question tests recognition of the Cisco Catalyst Center functions that support SD-Access design, policy, provisioning, deployment, management, and assurance. These are management-plane responsibilities rather than fabric routing or endpoint control-plane functions.

✗ **A** It is responsible for routing decisions inside the fabric.
Incorrect. Routing and endpoint-location decisions inside the fabric are performed by the SD-Access fabric control and data plane components, not by Cisco Catalyst Center. Catalyst Center manages and orchestrates the fabric.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **B** It possesses information about all endpoints, nodes, and external networks related to the fabric.
Incorrect. This description primarily matches the role of the SD-Access control-plane node, which maintains endpoint and network location mappings. Catalyst Center uses fabric information for management and assurance but is not the fabric control-plane mapping service.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **C** It provides integration and automation for all nonfabric nodes and their fabric counterparts.
Incorrect. Catalyst Center can integrate with and automate parts of the broader network, but this is not the complete defining function stated for its SD-Access role. Its primary responsibility is lifecycle management of the fabric, including design, deployment, provisioning, management, policy, and assurance.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✓ **D** It is responsible for the design, management, deployment, provisioning, and assurance of the fabric network devices.
Correct. Cisco Catalyst Center is the SD-Access management and orchestration platform. It provides fabric design, device onboarding and provisioning, policy and deployment workflows, ongoing management, and assurance visibility.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

Free demo · full exam: 271 questions

Question 4

Single choice · Domain: D1 Architecture › Identify the Cisco SD-Access components that provide centralized management and identity-based policy enforcement

SINGLE CHOICE

Which two components function together in a Cisco SD-Access solution?

A. Cisco campus fabric and Cisco vManage
B. Cisco vBond orchestrator and Cisco Catalyst Center (formerly DNA Center)
C. Cisco vSmart controller and Cisco Catalyst Center (formerly DNA Center)
D. Cisco ISE and Cisco Catalyst Center (formerly DNA Center)

Answer: D. Cisco ISE and Cisco Catalyst Center (formerly DNA Center)

Explanation

This question tests recognition of the Cisco Catalyst Center and Cisco ISE integration within an SD-Access architecture. Catalyst Center orchestrates the fabric, while ISE provides identity, authentication, and policy information used for segmentation and access control.

✗ **A** Cisco campus fabric and Cisco vManage
Incorrect. A campus fabric is part of SD-Access, but Cisco vManage is the management platform for Cisco SD-WAN rather than the SD-Access policy and orchestration component. Cisco SD-Access uses Cisco Catalyst Center for fabric automation and management.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **B** Cisco vBond orchestrator and Cisco Catalyst Center (formerly DNA Center)
Incorrect. Cisco vBond orchestrator is an SD-WAN control component that assists with orchestration and device onboarding. It does not function with Cisco Catalyst Center as an SD-Access component pair.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **C** Cisco vSmart controller and Cisco Catalyst Center (formerly DNA Center)
Incorrect. Cisco vSmart is the SD-WAN control-plane controller responsible for distributing routing and policy information in an SD-WAN overlay. It is not an SD-Access component.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✓ **D** Cisco ISE and Cisco Catalyst Center (formerly DNA Center)
Correct. Cisco Catalyst Center provides SD-Access design, provisioning, and fabric orchestration, while Cisco ISE supplies identity and policy services that enable group-based access control and segmentation. Together they support centralized policy and zero-trust-oriented access in SD-Access. and.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html
https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

Free demo · full exam: 271 questions

Question 5

Single choice · Domain: D1 Architecture › Interpret show policy-map interface output to identify QoS traffic rates, hierarchical shaping, and class bandwidth allocations

SINGLE CHOICE

Refer to the exhibit.

```
R3#show policy-map interface Multilink2
Multilink2
  Service-policy output: SHAPE_256K
    Class-map: class-default (match-any)
      63 packets, 2266 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 57/4874
      shape (average) cir 256000, bc 1536, be 1536
      target shape rate 256000
      Service-policy : CBWFQ
        queue stats for all priority classes:
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 5/510
        Class-map: VOICE (match-all)
          5 packets, 420 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip dscp ef (46)
          Priority: 64 kbps, burst bytes 1500, b/w exceed drops: 0
        Class-map: SIGNALING (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip dscp cs3 (24)
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 48 kbps
        Class-map: class-default (match-any)
          61 packets, 1576 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
          (pkts output/bytes output) 61/4234
          bandwidth 134 kbps
```

What can be determined about the QoS service policy applied to the interface?

A. No traffic was flowing out of the interface when the command was issued.

B. The class map class-default policy allows 256 kbps of traffic not assigned to other classes to flow through it.

Answer: A. No traffic was flowing out of the interface when the command was issued.

Explanation

This question tests interpretation of a hierarchical QoS service-policy, including five-minute offered rates, shaping rates, nested class policies, and bandwidth assignments. QoS behavior and policy structure are part of the ENCOR architecture objectives.

✓ **A** No traffic was flowing out of the interface when the command was issued.
Correct. The displayed five-minute offered rate and drop rate are 0 bps for the relevant classes, indicating that no traffic was actively being offered during the measurement interval when the command was issued. The nonzero packet counters reflect previously processed traffic and do not contradict the current offered-rate value.

Free demo · full exam: 271 questions

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/10100-policevsshape.html

✗ **B** The class map class-default policy allows 256 kbps of traffic not assigned to other classes to flow through it.
Incorrect. The 256000 bps value is the shaping rate shown for the VOICE class, not the bandwidth allocation of the nested class-default class. The nested class-default class is assigned 134 kbps, while the policy uses hierarchical shaping to limit the applicable parent class.
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/10100-policevsshape.html

Question 6

Single choice · Domain: D1 Architecture › Identify the operational and security benefits of centralized policy management in Cisco Catalyst SD-WAN

SINGLE CHOICE

Which benefit does Cisco Catalyst SD-WAN provide over a traditional WAN solution?

A. Centralized operation and security policies
B. Distributed data plane
C. Distributed control plane
D. Reduced training requirements

Answer: A. Centralized operation and security policies

Explanation

This question tests understanding of Cisco Catalyst SD-WAN architecture, particularly centralized control and policy orchestration compared with traditional WAN operations.

✓ **A** Centralized operation and security policies
Correct. Cisco Catalyst SD-WAN centralizes WAN orchestration and enables consistent application of security and routing policies across the environment, reducing the need to configure each WAN device independently.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html

✗ **B** Distributed data plane
Incorrect. A distributed data plane is an architectural characteristic of SD-WAN, but it is not the primary operational benefit identified over traditional WAN solutions. The key benefit is centralized management and policy control while forwarding remains distributed at branch devices.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html

✗ **C** Distributed control plane
Incorrect. Cisco Catalyst SD-WAN uses centralized control and management functions through its controller-based architecture rather than relying on a fully distributed control plane.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html

✗ **D** Reduced training requirements
Incorrect. Although centralized orchestration can simplify operations, Cisco Catalyst SD-WAN does not inherently guarantee reduced training requirements. This is not a defining technical benefit over traditional WAN solutions.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html

Free demo · full exam: 271 questions

Question 7

Single choice · Domain: D1 Architecture › Differentiate first-hop redundancy protocols from stateful switchover

SINGLE CHOICE

How do FHRPs differ from SSO?

```
from pythonping import ping
import paramiko
import sys

s= "%s %s" % (sys.argv[1],'')
s1=s.replace(' ','')
ip= s1
t= "%s %s" % (sys.argv[2],'')
r= ping(s1, count=7)
r1= r.success()
if r1 != True:
   exit()
client= paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(ip, port= 22, username= usr, password= pswd)
stdin, stdout, stderr = client.exec_command(t + '\n')
time.sleep(3)
print(t)
for u in stdout:
   print(u)
client.close()
```

A. FHRPs provide gateway redundancy, and SSO provides failover within a single device

B. FHRPs maintain state information within a single device, and SSO manages state information across multiple devices.

C. FHRPs use OTV for redundancy, and SSO uses VXLAN for state synchronization.

D. FHRPs influence bandwidth allocation, and SSO influences routing decisions. Refer to the exhibit. Which action results from executing the Python script?

A. display the unformatted output of a command that is entered on that device

B. display the output of a command that is entered on that device in a single line

C. SSH to the IP address that is manually entered on that device

D. display the output of a command that is entered on that device

Answer: A. display the unformatted output of a command that is entered on that device

Explanation

This question tests the ability to distinguish gateway availability mechanisms provided by FHRPs from

state synchronization and failover between redundant control-plane components provided by SSO.

✓ **A** display the unformatted output of a command that is entered on that device
Correct. FHRPs such as HSRP and VRRP provide a resilient default gateway by using multiple devices, while SSO synchronizes state between redundant supervisors or route processors within a single device to support stateful failover.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-16/ipapp-fhrp-xe-16-book/ip-fhrp-hsrp.html

✗ **B** display the output of a command that is entered on that device in a single line
Incorrect. The descriptions are reversed: SSO maintains synchronized state between redundant control-plane components within one device, whereas FHRPs provide gateway redundancy across multiple network devices.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ha/configuration/xe-3s/ha-xe-3s-book/ha-sso.html

✗ **C** SSH to the IP address that is manually entered on that device
Incorrect. FHRPs do not require OTV, and SSO does not use VXLAN to synchronize device state. FHRPs use protocols such as HSRP or VRRP, while SSO synchronizes control-plane state between redundant components.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-16/ipapp-fhrp-xe-16-book/ip-fhrp-hsrp.html

✗ **D** display the output of a command that is entered on that device
Incorrect. FHRPs determine which device presents the active default gateway and do not allocate bandwidth. SSO provides stateful failover and does not directly make routing-policy decisions.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ha/configuration/xe-3s/ha-xe-3s-book/ha-sso.html

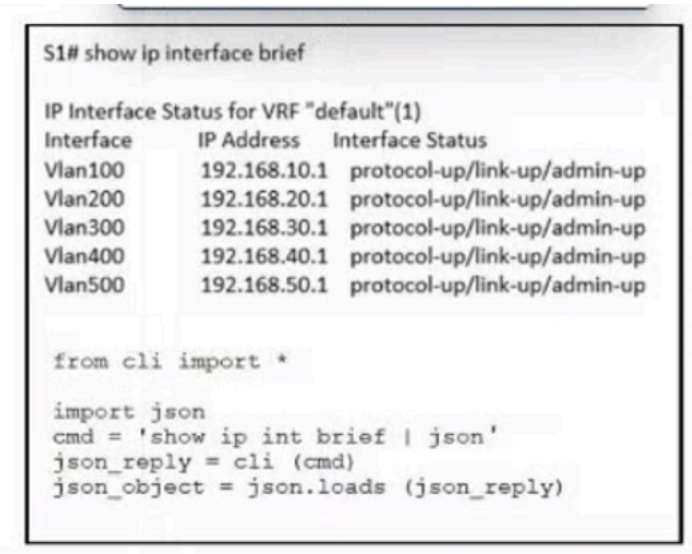
Dumpsgate

Question 8

Single choice · Domain: D1 Architecture › Differentiate traditional WAN characteristics from Cisco Catalyst SD-WAN architecture and operational capabilities

SINGLE CHOICE

Which characteristic applies to a traditional WAN solution but not to a Cisco Catalyst SD-WAN solution?



```
S1# show ip interface brief

IP Interface Status for VRF "default"(1)
Interface         IP Address      Interface Status
Vlan100           192.168.10.1    protocol-up/link-up/admin-up
Vlan200           192.168.20.1    protocol-up/link-up/admin-up
Vlan300           192.168.30.1    protocol-up/link-up/admin-up
Vlan400           192.168.40.1    protocol-up/link-up/admin-up
Vlan500           192.168.50.1    protocol-up/link-up/admin-up

from cli import *

import json
cmd = 'show ip int brief | json'
json_reply = cli (cmd)
json_object = json.loads (json_reply)
```

A. Centralized reachability, security, and application policies

B. Time-consuming configuration and maintenance

C. Low complexity and increased overall solution scale Increased operational overhead Slower deployment times Higher chances of configuration inconsistency Difficult scalability According to Cisco ENCOR (350-401) architecture principles, traditional WANs lack centralized orchestration, making configuration and maintenance time-consuming and complex. In contrast, Cisco Catalyst SD-WAN introduces: Centralized management and control (via vManage, vSmart, vBond) Policy-based automation Zero-touch provisioning (ZTP) Simplified operations and faster deployment Now, why the other options are incorrect:

A. Centralized reachability, security, and application policies This is a defining feature of Cisco SD-WAN, not traditional WAN.

C. Low complexity and increased overall solution scale SD-WAN is specifically designed to reduce complexity and improve scalability.

D. Operates over DTLS/TLS-authenticated and secured tunnels Cisco SD-WAN uses secure control connections (DTLS/TLS), which is not a characteristic of traditional WAN. Final Concept (ENCOR Exam Focus):

A. print(json.dumps['TABLE_intf']['ROW_intf']['prefix'])

B. print(json.dumps['TABLE_intf']['ROW_intf'][2]['prefix'])

C. print(json_object['TABLE_intf']['ROW_intf'][1]['prefix'])

D. print(json_object['TABLE_intf']['ROW_intf'][0]['prefix'])

Answer: B. print(json.dumps['TABLE_intf']['ROW_intf'][2]['prefix'])

Free demo · full exam: 271 questions

Dumpsgate

Question 9

Single choice · Domain: D1 Architecture › Identify the Cisco DNA Center User-Defined Network workflow capability for automated endpoint segmentation

SINGLE CHOICE

Which feature does the Cisco DNA Center User-Defined Network workflow provide?

A. automatic segmentation of IoT devices
B. replacement of malfunctioning devices
C. automatic provisioning of AP devices
D. interface for AP configuration

Answer: A. automatic segmentation of IoT devices

Explanation

This question tests knowledge of how User-Defined Network workflows provide policy-based segmentation for users and endpoint devices, including IoT devices, within a Cisco SD-Access environment.

✓ **A** automatic segmentation of IoT devices
Correct. The Cisco DNA Center User-Defined Network workflow enables policy-based segmentation by allowing users and their devices, including IoT devices, to be placed into isolated user-defined networks.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **B** replacement of malfunctioning devices
Incorrect. User-Defined Network is a segmentation and access-policy workflow; it does not replace failed network devices. Device replacement is associated with hardware lifecycle and support processes.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **C** automatic provisioning of AP devices
Incorrect. User-Defined Network does not primarily provision wireless access points. It provides user- and device-oriented segmentation and policy assignment.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **D** interface for AP configuration
Incorrect. An interface for configuring access points is a wireless-management function, whereas the User-Defined Network workflow is designed to implement user and device segmentation policies.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

Question 10

Multiple choice · Domain: D1 Architecture › Identify the roles of Cisco SD-Access fabric nodes, including control-plane mapping and border-node connectivity

What are two characteristics of Cisco SD-Access elements? (Choose two.)

A. The border node has the full RLOC-to-EID mapping database.
B. The border node is required for communication between fabric and nonfabric devices
C. The control-plane node maintains the endpoint EID-to-RLOC mapping database for the fabric

Answer

- B. **The border node is required for communication between fabric and nonfabric devices**
- C. **The control-plane node maintains the endpoint EID-to-RLOC mapping database for the fabric**

Explanation

This question tests recognition of SD-Access fabric-node responsibilities. Specifically, it assesses which node maintains endpoint-to-routing-locator mappings and which node provides connectivity between the fabric and external, nonfabric networks.

✗ **A** The border node has the full RLOC-to-EID mapping database.
Incorrect. The SD-Access control-plane node performs the LISP control-plane function and maintains the endpoint identifier (EID) to routing locator (RLOC) mapping database. The border node connects the fabric to external networks and does not own the complete mapping database.
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✓ **B** The border node is required for communication between fabric and nonfabric devices
Correct. The fabric border node provides connectivity between the SD-Access fabric and external networks or nonfabric devices, such as WAN, data-center, Internet-edge, and shared-services networks.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✓ **C** The control-plane node maintains the endpoint EID-to-RLOC mapping database for the fabric
The SD-Access control-plane node implements the LISP Map-Server/Map-Resolver function and maintains the database associating endpoints with their network locations.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center/cisco-validated-solution-profiles/validated_profile_financial_vertical_sda_sdwan.html

Question 11

Single choice · Domain: D1 Architecture › Identify the control, data, and policy planes and their protocols in Cisco SD-Access

SINGLE CHOICE

Which characteristic applies to the Cisco SD-Access solution?

A. Dynamic routing is used to discover and provision border and edge switches.
B. The control plane is based on VXLAN.
C. The data plane is based on VXLAN.
D. GRE is used as the policy plane.

Answer: C. The data plane is based on VXLAN.

Explanation

This question tests knowledge of the protocol roles within the Cisco SD-Access fabric. Specifically, it requires distinguishing VXLAN as the data-plane encapsulation from LISP control-plane functions and TrustSec-based policy enforcement.

✗ **A** Dynamic routing is used to discover and provision border and edge switches.
Incorrect. SD-Access uses a routed underlay for IP reachability, but fabric device roles and endpoint information are managed through Cisco Catalyst Center and the LISP-based control plane, not discovered and provisioned solely through dynamic routing.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **B** The control plane is based on VXLAN.
Incorrect. VXLAN is used for SD-Access data-plane encapsulation. The control plane uses LISP to exchange endpoint and host-location information.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✓ **C** The data plane is based on VXLAN.
Correct. Cisco SD-Access uses VXLAN to provide data-plane encapsulation across the fabric, including support for virtual network and endpoint-group segmentation.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

✗ **D** GRE is used as the policy plane.
Incorrect. GRE is not the SD-Access policy-plane technology. Policy enforcement is based on Cisco TrustSec concepts such as security-group tags, while VXLAN provides data-plane encapsulation.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access.html

Free demo · full exam: 271 questions

Question 12

Single choice · Domain: D2 Virtualization › Identify the LISP component that receives an ITR Map-Request when the EID-to-RLOC mapping is unknown

SINGLE CHOICE

In a LISP topology, which component does the ITR send a resolution request to when it does not know the path to a specific EID?

A. Map resolver
B. Routing locator
C. Proxy ingress tunnel router
D. Proxy egress tunnel router

Answer: A. Map resolver

Explanation

This question tests LISP control-plane operation and the role of the Map Resolver in locating mappings for destination endpoint identifiers. LISP uses the Map Resolver to receive Map-Requests from an ITR and obtain the appropriate EID-to-RLOC resolution.

✓ **A** Map resolver
Correct. When an ITR does not have a mapping for a destination EID, it sends a Map-Request to the Map Resolver. The Map Resolver processes the request and forwards it toward the authoritative Map Server for resolution.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_lisp/configuration/xe-17/lisp-xe-17-book.html

✗ **B** Routing locator
Incorrect. A routing locator (RLOC) is an address used to identify the location of a LISP tunnel endpoint; it is not a LISP component that receives Map-Requests for EID resolution.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_lisp/configuration/xe-17/lisp-xe-17-book.html

✗ **C** Proxy ingress tunnel router
Incorrect. A Proxy-ITR provides LISP ingress tunneling for traffic sourced from non-LISP sites. It does not serve as the normal Map-Request resolution component for an ITR that lacks an EID mapping.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_lisp/configuration/xe-17/lisp-xe-17-book.html

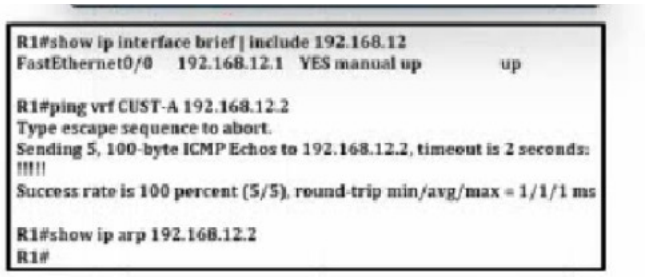
✗ **D** Proxy egress tunnel router
Incorrect. A Proxy-ETR provides LISP egress tunneling toward non-LISP destinations. It is not the component to which an ITR sends a Map-Request when it needs an EID-to-RLOC mapping.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_lisp/configuration/xe-17/lisp-xe-17-book.html

Question 13

Single choice · Domain: D2 Virtualization › Interpret VRF-specific ARP behavior and verify ARP entries within the correct VRF

SINGLE CHOICE

Refer to the exhibit.



A. Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.
B. When VRFs are used, ARP protocol is disabled in the global routing table.
C. When VRFs are used, ARP protocol must be enabled in each VRF.
D. The ping command must be executed in the global routing table.

Answer: A. Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.

Explanation

This question tests how Virtual Routing and Forwarding separates routing and ARP information into independent tables. The candidate must recognize that a VRF-aware ping can succeed even when a standard global-table ARP lookup does not display the entry.

✓ **A** Interface FastEthernet0/0 is configured in VRF CUST-A, so the ARP entry is also in that VRF.
Correct. ARP entries are associated with the routing table or VRF in which the interface operates. Because the ping is executed with 'vrf CUST-A', the relevant ARP entry is in the CUST-A ARP table and should be viewed with a VRF-specific command such as 'show ip arp vrf CUST-A'.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xe-3s/arp-xe-3s-book.html

✗ **B** When VRFs are used, ARP protocol is disabled in the global routing table.
Incorrect. Configuring a VRF does not disable ARP in the global routing table. ARP remains operational in the global table and in individual VRFs; each table maintains its own ARP information.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xe-3s/arp-xe-3s-book.html

✗ **C** When VRFs are used, ARP protocol must be enabled in each VRF.
Incorrect. ARP is automatically used for connected IPv4 interfaces in a VRF; there is no separate ARP enablement requirement for each VRF. The ARP cache is maintained in the context of the applicable VRF.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xe-3s/arp-xe-3s-book.html

✗ **D** The ping command must be executed in the global routing table.
Incorrect. The ping can be executed in a specific VRF, as demonstrated by 'ping vrf CUST-A'. In fact, testing from the correct VRF is necessary to validate reachability through that VRF's routing and ARP tables.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xe-3s/arp-xe-3s-book.html

Question 14

Single choice · Domain: D2 Virtualization › Identify the VTEP function of encapsulating and decapsulating VXLAN Ethernet frames

SINGLE CHOICE

Which action is a function of VTEP in VXLAN?

A. tunneling traffic from IPv6 to IPv4 VXLANs
B. allowing encrypted communication on the local VXLAN Ethernet segment
C. encapsulating and de-encapsulating VXLAN Ethernet frames
D. tunneling traffic from IPv4 to IPv6 VXLANs

Answer: C. encapsulating and de-encapsulating VXLAN Ethernet frames

Explanation

This question tests understanding of VXLAN data-plane operation and the role of a Virtual Tunnel Endpoint. A VTEP encapsulates Ethernet frames into VXLAN packets for transport across an IP underlay and decapsulates received VXLAN packets back into Ethernet frames.

✗ **A** tunneling traffic from IPv6 to IPv4 VXLANs
Incorrect. A VTEP does not perform IPv6-to-IPv4 protocol translation. Its VXLAN function is to encapsulate and decapsulate Ethernet frames over an IP transport network.

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/data-center-vxlan-network/white-paper-c11-729383.html

✗ **B** allowing encrypted communication on the local VXLAN Ethernet segment
Incorrect. VXLAN provides overlay encapsulation and segmentation, but encryption is not an inherent VTEP function. A VTEP handles VXLAN encapsulation and decapsulation rather than encrypting local Ethernet traffic.

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/data-center-vxlan-network/white-paper-c11-729383.html

✓ **C** encapsulating and de-encapsulating VXLAN Ethernet frames
Correct. A VTEP encapsulates Ethernet frames with a VXLAN header and outer IP/UDP headers when sending traffic into the VXLAN overlay, and decapsulates received VXLAN packets to deliver the original Ethernet frames.

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/data-center-vxlan-network/white-paper-c11-729383.html

✗ **D** tunneling traffic from IPv4 to IPv6 VXLANs
Incorrect. A VTEP does not provide IPv4-to-IPv6 tunneling or protocol translation as its VXLAN role. It encapsulates and decapsulates Ethernet frames across the VXLAN overlay.

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/data-center-vxlan-network/white-paper-c11-729383.html

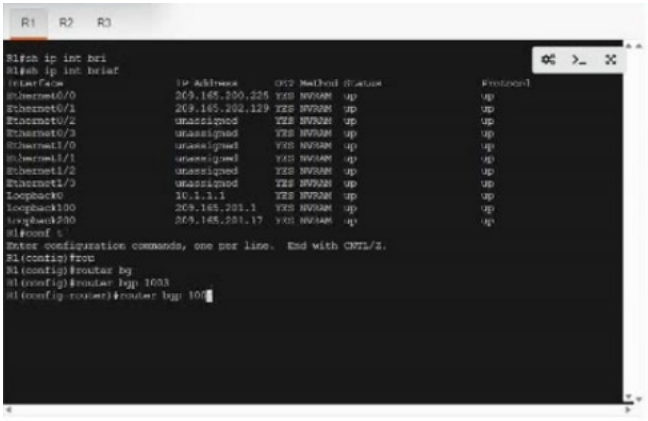
Question 15

Single choice · Domain: D3 Infrastructure › Interpret Cisco IOS interface status and configuration output

SINGLE CHOICE

Refer to the Cisco IOS terminal exhibit.

Which command displays a concise summary of the router's interfaces, including their IP addresses, configuration method, interface status, and line-protocol status?



A. show ip interface brief
B. show ip route
C. show running-config
D. show interfaces status

Answer: A. show ip interface brief

Explanation

Cisco's show ip interface brief command provides the following information: - Interface name - IP address - Address assignment method - Interface status - Line-protocol status The page 10 screenshot visibly displays these columns, including interfaces with up/up operational states. Cisco documents this command specifically for displaying a concise summary of interface status and IP information.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s4.html
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-1/command_reference/b_171_9600_cr/interface_and_hardware_commands.html

✗ **A** See the solution below in Explanation
Incorrect or unverifiable as presented. This is a placeholder rather than a substantive answer choice, and the supplied question does not include the referenced solution or enough readable command context to determine a correct response. Cisco's IOS interface command documentation provides the relevant reference for interpreting and configuring interface status and addressing.

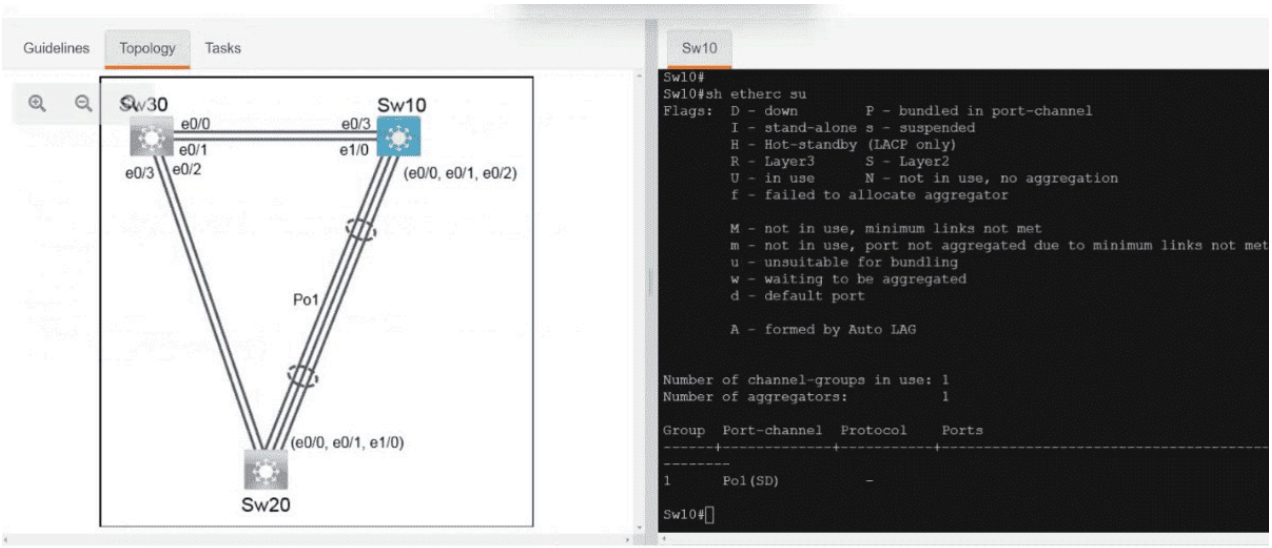
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/iap-15-s.html

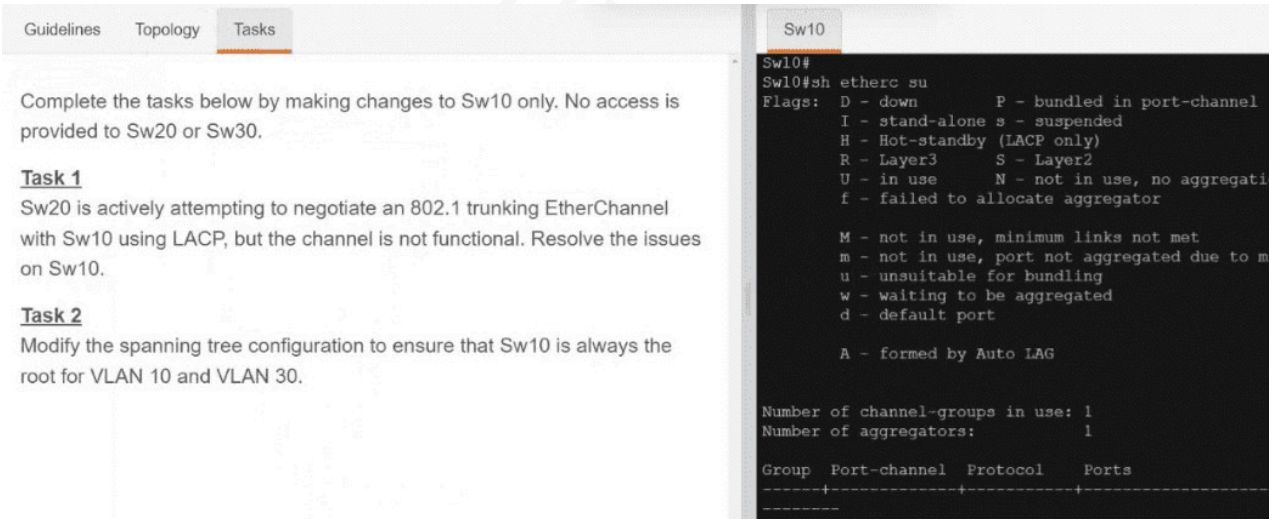
Question 16

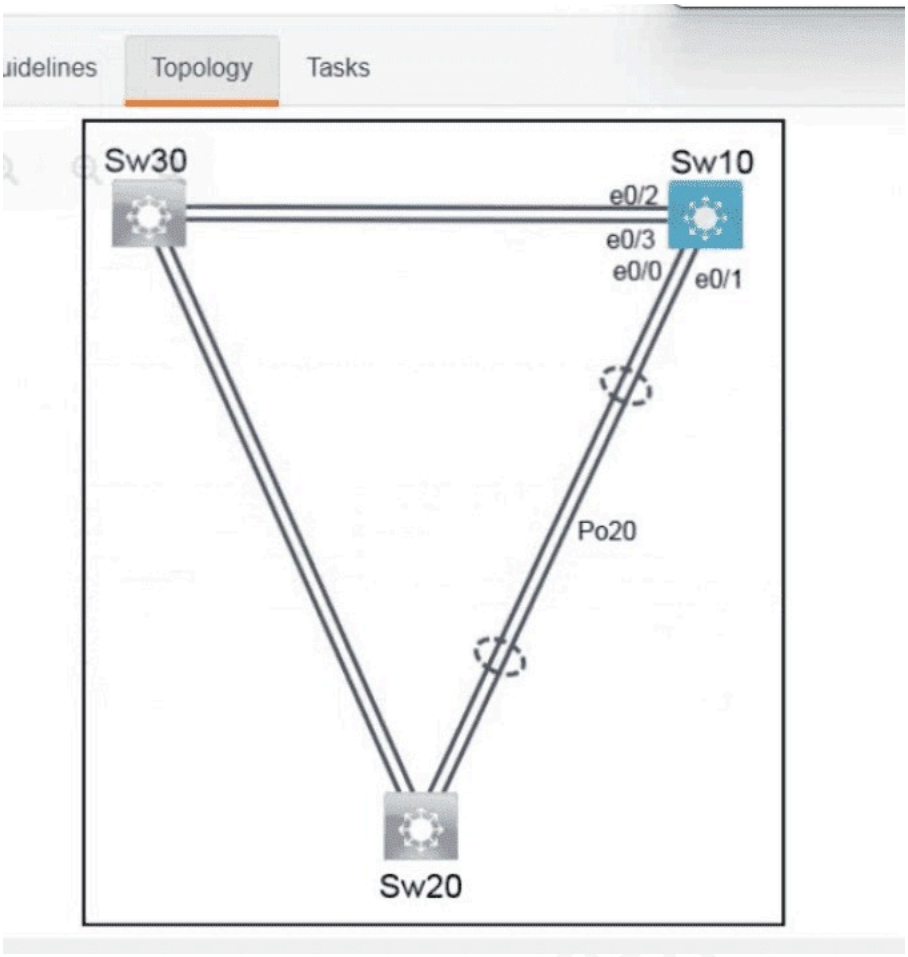
Single choice · Domain: D3 Infrastructure › Troubleshoot and configure an LACP Layer 2 EtherChannel and make a switch the spanning-tree root for a VLAN

SINGLE CHOICE

SIMULATION







Complete the tasks below by making changes to Sw10 only. No access is provided to Sw20 or Sw30.

Task 1

Sw20 is actively attempting to negotiate an 802.1 trunking EtherChannel with Sw10 using LACP, but the channel is not functional. Resolve the issues on Sw10.

Task 2

Modify the spanning tree configuration to ensure that Sw10 is always the root for VLAN 20.

Sw10

Config t no int po1 default int ran et0/0-2 int ran e0/0-2 switchport trunk encap dot1q switchport mode trunk channel-group 1 mode active

Free demo · full exam: 271 questions

A. See the solution below in Explanation

Answer: A. See the solution below in Explanation

Explanation

This simulation tests configuration of trunk interfaces and LACP channel-group negotiation on Sw10, followed by spanning-tree root election for VLAN 20. These are core Layer 2 infrastructure implementation skills in the ENCOR blueprint.

✓ **A** See the solution below in Explanation

The required Sw10 configuration should remove the nonfunctional port-channel, reset the relevant member interfaces, configure them as 802.1Q trunks, enable LACP active mode, and make Sw10 the VLAN 20 root. A suitable configuration is: `no interface port-channel 1`, `default interface range ethernet0/0-2`, `interface range ethernet0/0-2`, `switchport trunk encapsulation dot1q`, `switchport mode trunk`, `channel-group 1 mode active`, and `spanning-tree vlan 20 root primary`. LACP requires compatible member interfaces and active/passive negotiation, while `root primary` adjusts spanning-tree priority so Sw10 becomes the preferred root for VLAN 20. and.

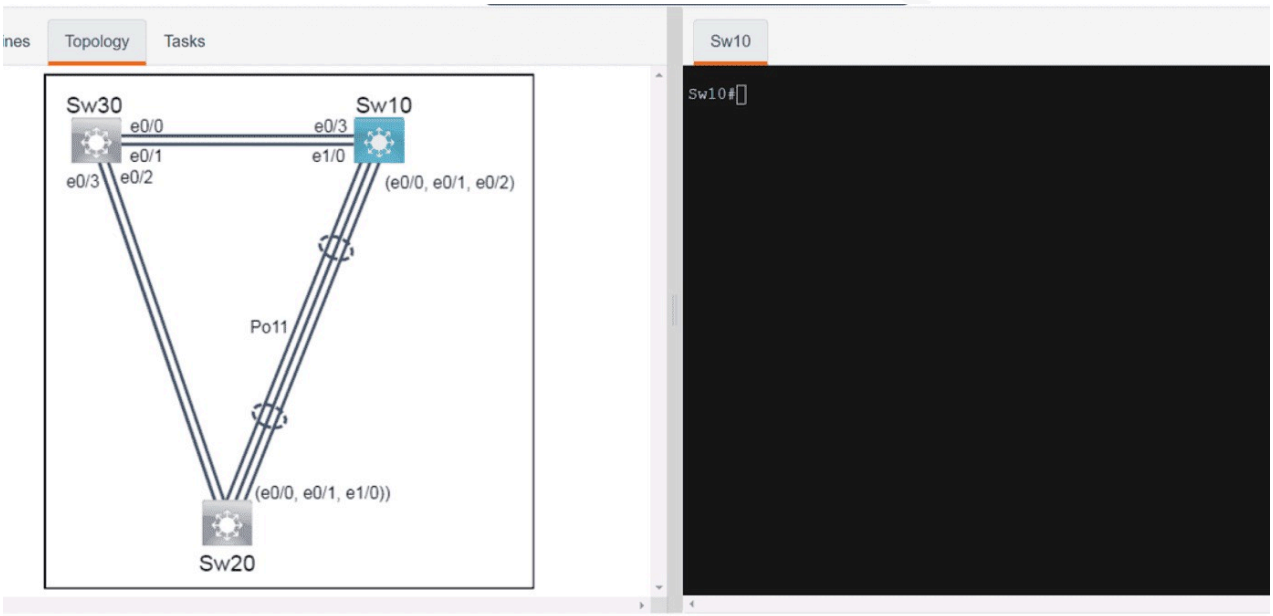
https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/116644-technote-etherchannel-00.html
https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10553-14.html

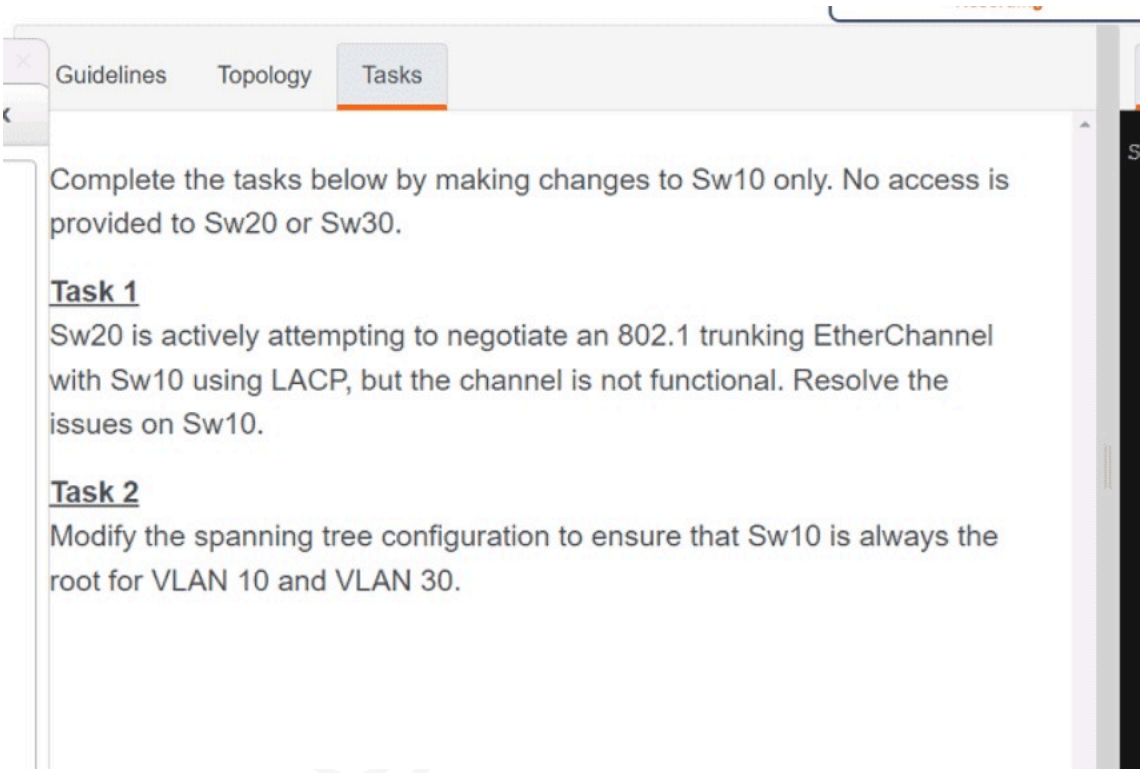
Question 17

Single choice · Domain: D3 Infrastructure › Configure an LACP EtherChannel trunk and establish the spanning-tree root bridge for specified VLANs

SINGLE CHOICE

SIMULATION





Solution:-
Default int range et0/0-1
Int range e0/0 -- 1
Sw trunk encap dot1
Switch mode trunk
Channel-group 2 mode passive
No shut
Spanning-tree vlan 10 priority 0
Spanning-tree vlan 30 priority 0

A. Default interfaces Ethernet0/0 through Ethernet0/1; configure Ethernet0/0 through Ethernet0/1 as 802.1Q trunks; configure the interfaces with channel-group 2 mode passive; enable the interfaces; set spanning-tree VLAN 10 and VLAN 30 priority to 0

Answer: A. Default interfaces Ethernet0/0 through Ethernet0/1; configure Ethernet0/0 through Ethernet0/1 as 802.1Q trunks; configure the interfaces with channel-group 2 mode passive; enable the interfaces; set spanning-tree VLAN 10 and VLAN 30 priority to 0

Explanation

This simulation tests Layer 2 infrastructure skills: configuring trunking and LACP on the local switch, enabling the interfaces, and assigning spanning-tree priorities so Sw10 becomes root for VLANs 10 and 30.

✓ **A** Default interfaces Ethernet0/0 through Ethernet0/1; configure Ethernet0/0 through Ethernet0/1 as 802.1Q trunks; configure the interfaces with channel-group 2 mode passive; enable the interfaces; set

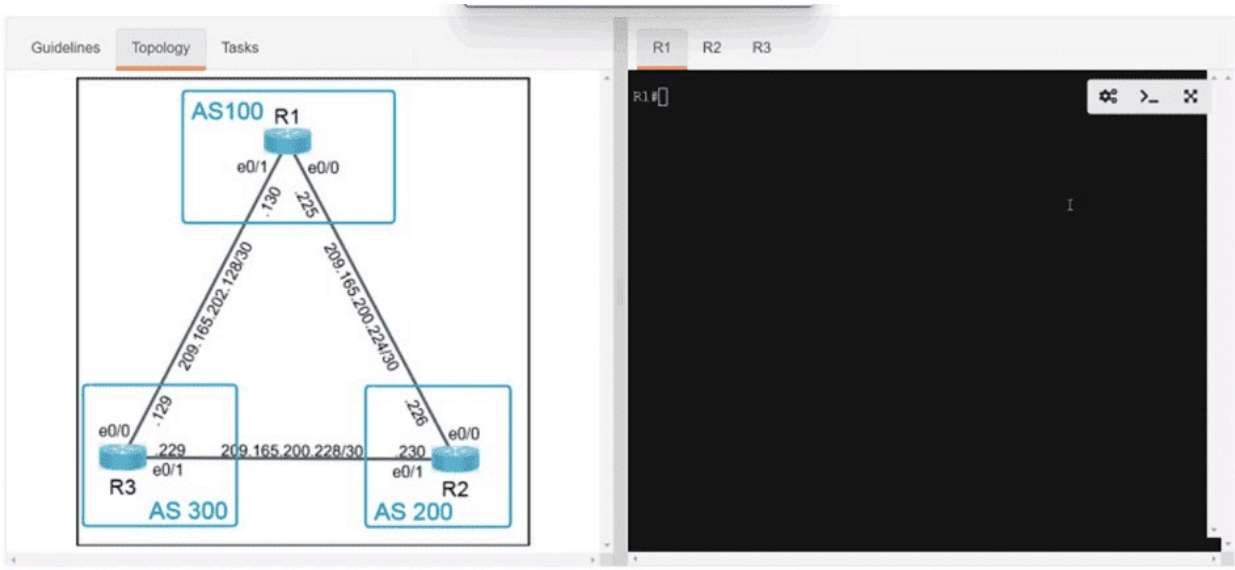
spanning-tree VLAN 10 and VLAN 30 priority to 0
Correct. Because Sw20 is actively attempting LACP negotiation, configuring Sw10 with channel-group 2 mode passive allows the EtherChannel to form. Both member interfaces must use compatible 802.1Q trunking and be enabled. Setting the spanning-tree priority to 0 makes Sw10 the preferred root bridge for VLANs 10 and 30. and.
https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/10680-64.html
https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html

Question 18

Single choice · Domain: D3 Infrastructure › Configure classic IPv4 eBGP using a Loopback 0 router ID and advertise loopback networks with network statements

SINGLE CHOICE

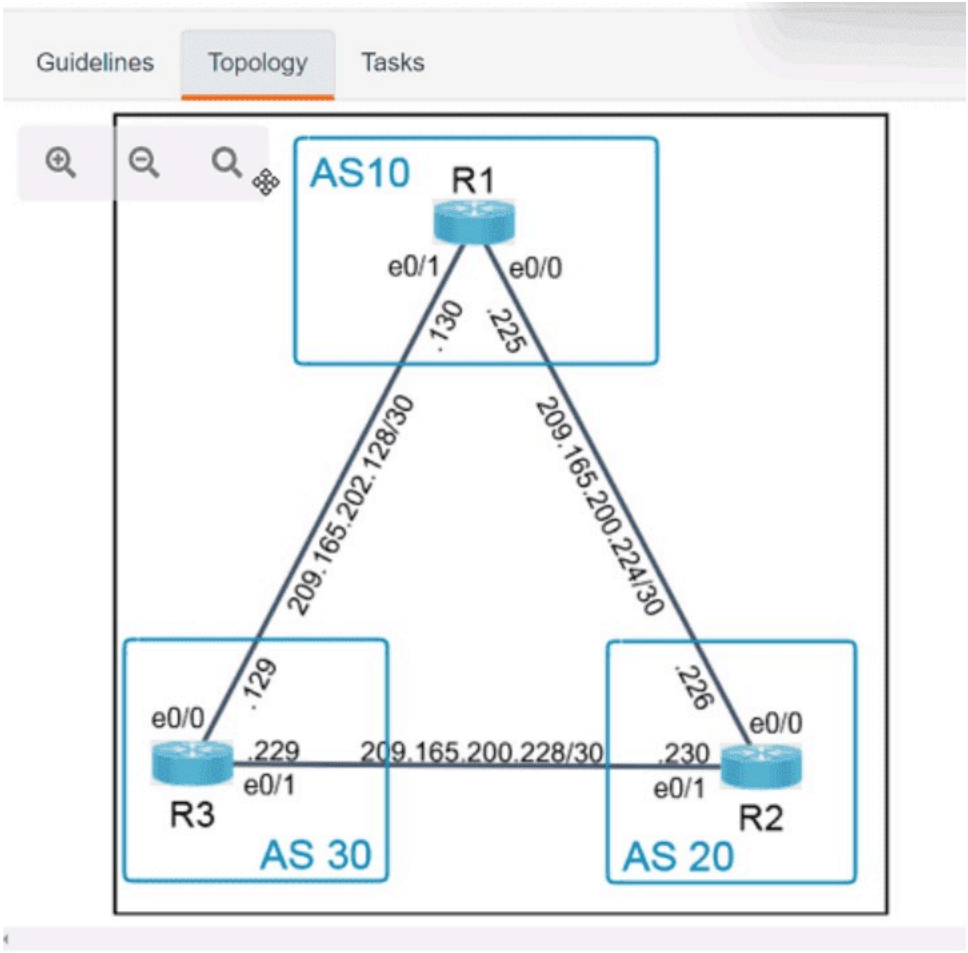
SIMULATION

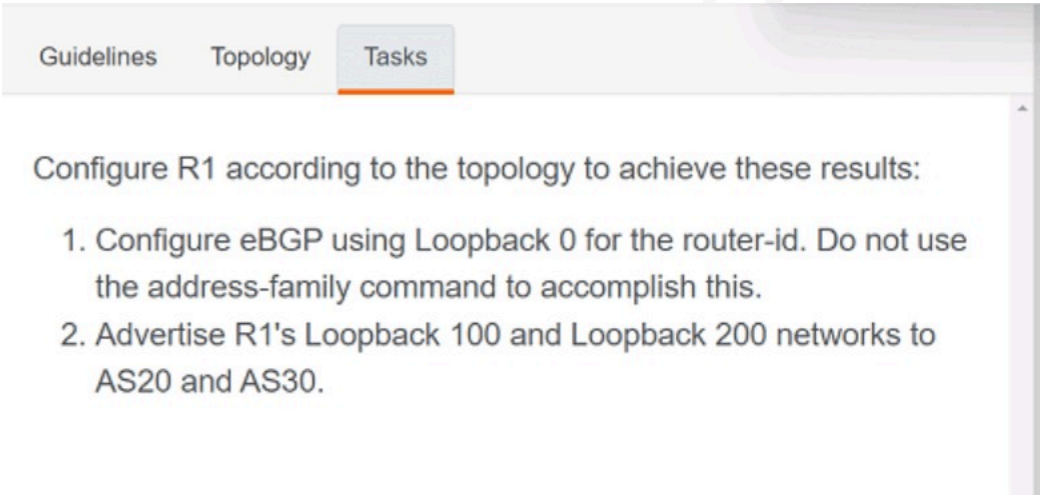


Guidelines Topology Tasks

Configure R1 according to the topology to achieve these results:

1. Configure eBGP using Loopback 0 for the router-id. Do not use the address-family command to accomplish this.
2. Advertise R1's Loopback 100 and Loopback 200 networks to AS200 and AS300.





A. See the solution below in Explanation
A. See the solution below in Explanation

Answer: A. See the solution below in Explanation

Dumpsgate

Question 19

Single choice · Domain: D3 Infrastructure › Interpret traceroute behavior and identify filtering of UDP probe traffic by a firewall

SINGLE CHOICE

A firewall address of 192.168.1.101 can be pinged from a router but, when running a traceroute to it, the following output is received:

1 * * * 2 * * * 3 * * * 4 * * * 5 * * * 6 * * * 7 * * * 8 * * * 9 * * * 10 * * * What is the cause of this issue?

A. The firewall blocks UDP traffic.
B. The firewall rule that allows ICMP traffic does not function correctly.
C. The firewall blocks ICMP traceroute traffic.
D. The firewall blocks ICMP traffic.

Answer: A. The firewall blocks UDP traffic.

Explanation

This question tests troubleshooting of IP services by distinguishing successful ICMP echo traffic from unanswered UDP probes used by Cisco traceroute. The candidate must identify that a firewall can permit ping while blocking the UDP traffic required for standard traceroute.

✓ **A** The firewall blocks UDP traffic.
Correct. Cisco traceroute uses UDP probe packets by default, while ping uses ICMP Echo messages. Because the firewall address responds to ping but every traceroute hop times out, the firewall is likely

Free demo · full exam: 271 questions

blocking the UDP probes or the resulting traceroute responses.

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/13730-traceroute.html

✗ **B** The firewall rule that allows ICMP traffic does not function correctly.
Incorrect. A successful ping demonstrates that the relevant ICMP Echo traffic is being permitted and processed. The failure is specific to the traffic used by standard traceroute, not evidence that the ICMP rule is malfunctioning.

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/13730-traceroute.html

✗ **C** The firewall blocks ICMP traceroute traffic.
Incorrect. Standard Cisco traceroute sends UDP probes; intermediate devices normally return ICMP Time Exceeded messages, and the destination returns an ICMP Port Unreachable message. The described behavior is therefore most consistent with UDP filtering rather than blocking a distinct ICMP traceroute protocol.

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/13730-traceroute.html

✗ **D** The firewall blocks ICMP traffic.
Incorrect. The firewall can be pinged successfully, so ICMP Echo traffic is not generally blocked. The traceroute failure points instead to filtering of the UDP probes or associated response traffic.

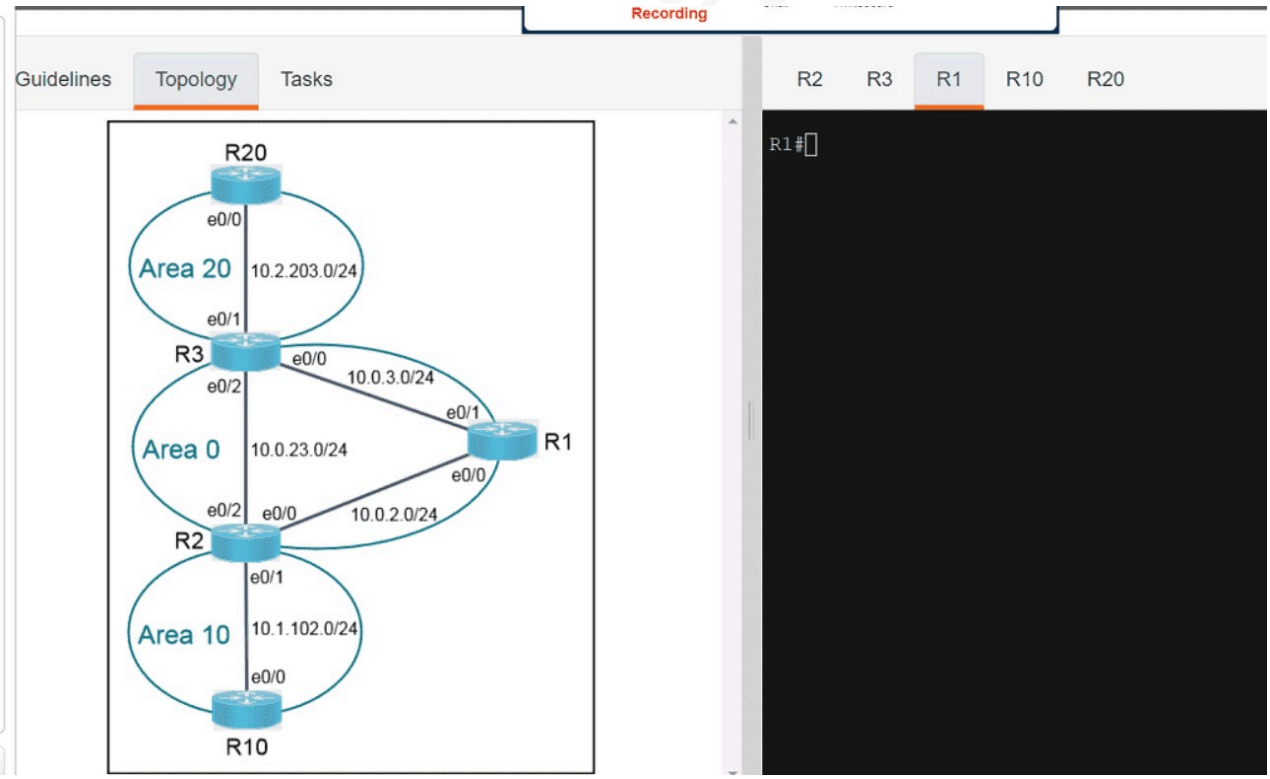
https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/13730-traceroute.html

Question 20

Multiple choice · Domain: D3 Infrastructure › Configure OSPF interface activation, ABR route summarization, and area filtering with prefix lists

SINGLE CHOICE

SIMULATION



Guidelines Topology Tasks

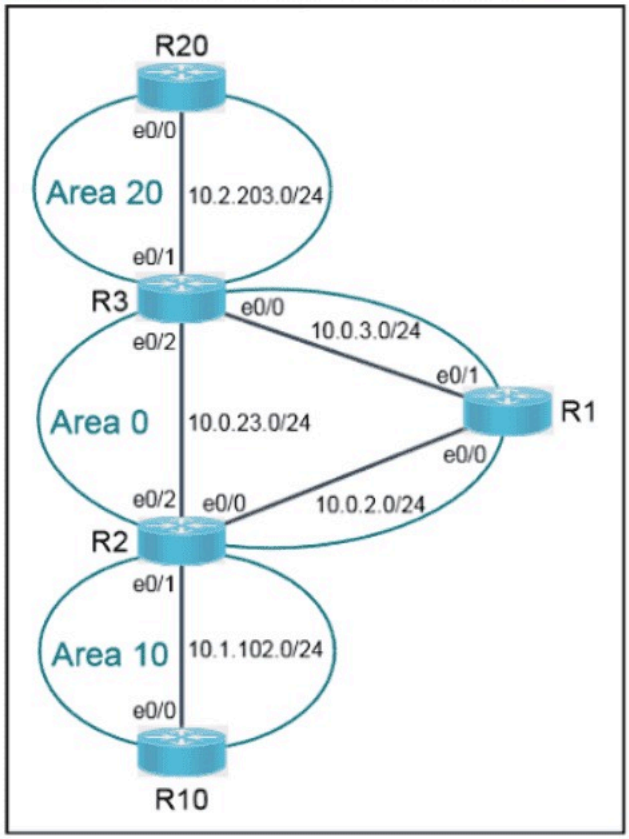
R2 R3

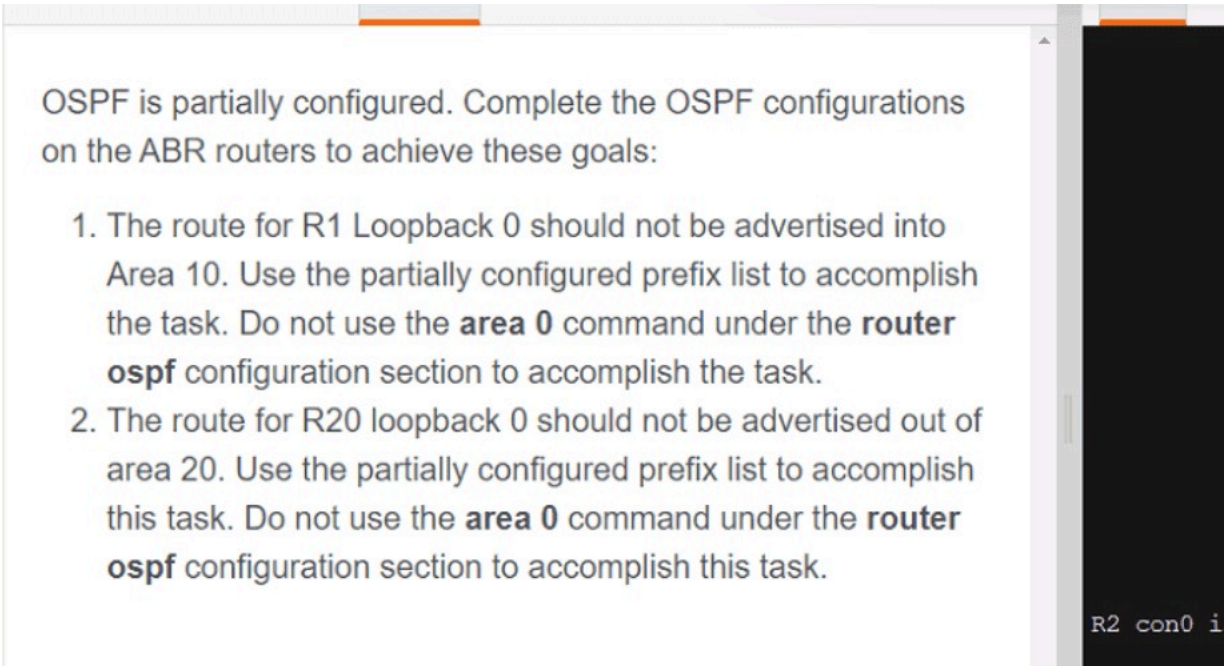
R1#

OSPF is partially configured. Complete the OSPF configurations to achieve these goals:

1. Configure OSPF on router R1 according to the topology so that all networks are advertised. Do not use the network statement under the "router ospf" configuration section to accomplish this task.
2. Configure a single command on the ABR routers to ensure only one summary route is advertised to area 0.

Guidelines Topology Tasks





Solution:
R1 en
Conf t
Router ospf 10
Router-id 10.x.x.x -- lo0 address
Int range lo0, e0/0-1
Ip ospf 10 area 0
Exit wr
R2
Router ospf 10
Area 10 range 10.1.0.0 255.255.0.0 exit wr
R3
Router ospf 10
Area 10 range 10.2.0.0 255.255.0.0

A. On R1, configure router ospf 10, set the router ID to the Loopback 0 address, and apply ip ospf 10 area 0 under Loopback 0 and Ethernet 0/0 through Ethernet 0/1
B. On R2, under router ospf 10, configure area 10 range 10.1.0.0 255.255.0.0; on R3, configure area 20 range 10.2.0.0 255.255.0.0
C. On R2, under router ospf 10, apply area 10 filter-list prefix <R1-Loopback-prefix-list> in
D. On R3, under router ospf 10, apply area 20 filter-list prefix <R20-Loopback-prefix-list> out

Dumpsgate

Answer

- A. **On R1, configure router ospf 10, set the router ID to the Loopback 0 address, and apply ip ospf 10 area 0 under Loopback 0 and Ethernet 0/0 through Ethernet 0/1**
- B. **On R2, under router ospf 10, configure area 10 range 10.1.0.0 255.255.0.0; on R3, configure area 20 range 10.2.0.0 255.255.0.0**
- C. **On R2, under router ospf 10, apply area 10 filter-list prefix <R1-Loopback-prefix-list> in**
- D. **On R3, under router ospf 10, apply area 20 filter-list prefix <R20-Loopback-prefix-list> out**

Explanation

This simulation tests OSPF configuration across multiple areas, including enabling OSPF directly on interfaces without network statements, summarizing area routes at ABRs, and filtering interarea prefixes with OSPF prefix-list policies.

✓ **A** On R1, configure router ospf 10, set the router ID to the Loopback 0 address, and apply ip ospf 10 area 0 under Loopback 0 and Ethernet 0/0 through Ethernet 0/1
Correct. Applying OSPF directly under the interfaces advertises the connected networks without using a network statement. The Loopback 0 address can also be used as the stable OSPF router ID.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-17/iro-xe-17-book.html

✓ **B** On R2, under router ospf 10, configure area 10 range 10.1.0.0 255.255.0.0; on R3, configure area 20 range 10.2.0.0 255.255.0.0
Correct. The area range command summarizes the specified internal area prefixes when they are advertised by the ABR into Area 0. R2 summarizes the Area 10 10.1.x.x routes, while R3 summarizes the Area 20 10.2.x.x routes.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-17/iro-xe-17-book.html

✓ **C** On R2, under router ospf 10, apply area 10 filter-list prefix <R1-Loopback-prefix-list> in
Correct. The in direction on the Area 10 ABR filters interarea routes before they are installed or advertised into Area 10. The partially configured prefix list must deny the R1 Loopback 0 prefix and permit the other required prefixes.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-17/iro-xe-17-book.html

✓ **D** On R3, under router ospf 10, apply area 20 filter-list prefix <R20-Loopback-prefix-list> out
Correct. The out direction on the Area 20 ABR filters routes originating in Area 20 before they are advertised toward Area 0. The configured prefix list must deny the R20 Loopback 0 prefix and permit the other required routes.

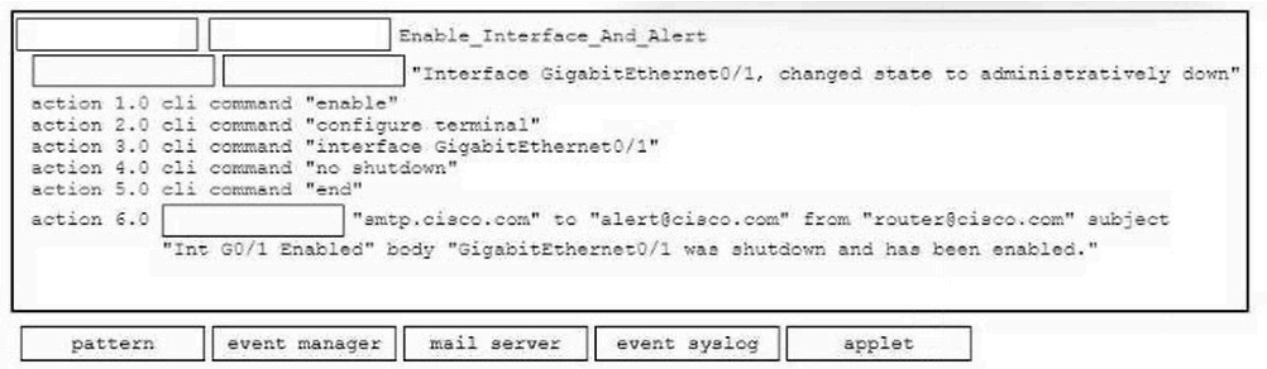
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-17/iro-xe-17-book.html

Question 21

Multiple choice · Domain: D4 Network Assurance › Configure a Cisco Embedded Event Manager applet to detect a syslog event, perform CLI-based interface recovery, and send an email notification

Drag and drop the command snippets from the bottom onto the boxes to configure an EEM applet to enable a previously shutdown interface and send an alert to alert@cisco.com.

QUESTION IMAGE:



A. event manager applet Enable_Interface_And_Alert

B. event syslog pattern "Interface GigabitEthernet0/1, changed state to administratively down"

C. action 1.0 cli command "enable"

D. action 2.0 cli command "configure terminal"

E. action 3.0 cli command "interface GigabitEthernet0/1"

F. action 4.0 cli command "no shutdown"

G. action 5.0 cli command "end"

H. action 6.0 mail server "smtp.cisco.com" to "alert@cisco.com" from "router@cisco.com" subject "Int G0/1 Enabled" body "GigabitEthernet0/1 was shutdown and has been enabled."

Answer

- A. **event manager applet Enable_Interface_And_Alert**
- B. **event syslog pattern "Interface GigabitEthernet0/1, changed state to administratively down"**
- C. **action 1.0 cli command "enable"**
- D. **action 2.0 cli command "configure terminal"**
- E. **action 3.0 cli command "interface GigabitEthernet0/1"**
- F. **action 4.0 cli command "no shutdown"**
- G. **action 5.0 cli command "end"**
- H. **action 6.0 mail server "smtp.cisco.com" to "alert@cisco.com" from "router@cisco.com" subject "Int G0/1 Enabled" body "GigabitEthernet0/1 was shutdown and has been enabled."**

Explanation

This task tests automated operational remediation using EEM. The applet must match the administratively down syslog message, enter configuration mode to issue no shutdown, and send an SMTP alert after recovery.

✓ **A** event manager applet Enable_Interface_And_Alert
Correct. This creates and names the EEM applet that contains the syslog trigger and remediation actions.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **B** event syslog pattern "Interface GigabitEthernet0/1, changed state to administratively down"
Correct. The syslog event detector starts the applet when the specified interface-down message is generated.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **C** action 1.0 cli command "enable"
Correct. This action enters privileged EXEC mode before configuration commands are executed.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **D** action 2.0 cli command "configure terminal"
Correct. The action enters global configuration mode so the interface can be modified.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **E** action 3.0 cli command "interface GigabitEthernet0/1"
Correct. This selects the interface that generated the administrative-down event.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **F** action 4.0 cli command "no shutdown"
Correct. The no shutdown command administratively enables GigabitEthernet0/1.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **G** action 5.0 cli command "end"
Correct. This exits configuration mode after the interface has been enabled.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

✓ **H** action 6.0 mail server "smtp.cisco.com" to "alert@cisco.com" from "router@cisco.com" subject "Int G0/1 Enabled" body "GigabitEthernet0/1 was shutdown and has been enabled."
Correct. The EEM mail action sends an SMTP notification to alert@cisco.com after the interface recovery commands complete.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book.html

Question 22

Single choice · Domain: D5 Security › Identify the purpose and function of Cisco TrustSec

SINGLE CHOICE

What is Cisco TrustSec?

A. Technology that provides abstraction between the network topology and network security
B. Zero-trust security framework
C. Technology that provides data encryption for data at rest
D. Technology that provides link encryption for wired networks

Answer: A. Technology that provides abstraction between the network topology and network security

Explanation

This question tests recognition of Cisco TrustSec as an identity-based security technology that separates

security policy from physical network topology and uses Security Group Tags to enforce access policies.

✓ **A** Technology that provides abstraction between the network topology and network security
Correct. Cisco TrustSec abstracts security policy from network topology by using identity-based classification and Security Group Tags, allowing policy enforcement without depending solely on IP addresses or physical location.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-17/sec-usr-cts-xe-17-book.html

✗ **B** Zero-trust security framework
Incorrect. TrustSec supports zero-trust principles through identity-based policy enforcement, but it is not itself a complete zero-trust security framework.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-17/sec-usr-cts-xe-17-book.html

✗ **C** Technology that provides data encryption for data at rest
Incorrect. TrustSec focuses on identity-based access control and policy enforcement in the network; it does not provide encryption for stored data.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-17/sec-usr-cts-xe-17-book.html

✗ **D** Technology that provides link encryption for wired networks
Incorrect. Link-layer encryption for wired networks is provided by MACsec, whereas TrustSec provides identity-based segmentation and access policy enforcement.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-17/sec-usr-cts-xe-17-book.html

Dumpsgate

Question 23

Single choice · Domain: D5 Security › Configure AAA login authentication using a RADIUS server for console access

SINGLE CHOICE

An engineer must implement a configuration to allow a network administrator to connect to the console port of a router and authenticate over the network. Which command set should the engineer use?

A. aaa new-model aaa authentication login console local
B. aaa new-model aaa authentication login default enable
C. aaa new-model aaa authentication login console group radius
D. aaa new-model aaa authentication enable default

Answer: C. aaa new-model aaa authentication login console group radius

Explanation

This question tests the ability to create a named AAA login method list that uses a centralized RADIUS server. The method list can then be applied to the console line to authenticate administrators through the network-based AAA service.

✗ **A** aaa new-model aaa authentication login console local
Incorrect. This creates a named login method list that uses the router's local username database, not a network-based authentication service such as RADIUS.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-s/12-4/sec-usr-aaa-12-4-book.html

✗ **B** aaa new-model aaa authentication login default enable
Incorrect. This uses the privileged EXEC enable password for login authentication and does not authenticate through a centralized network AAA server.

Free demo · full exam: 271 questions

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-s/12-4/sec-usr-aaa-12-4-book.html

✓ **C** aaa new-model aaa authentication login console group radius
Correct. This enables AAA and creates the named console login method list, directing authentication requests to the configured RADIUS server group. The list must be applied under the console line with the appropriate login authentication command.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-s/12-4/sec-usr-aaa-12-4-book.html

✗ **D** aaa new-model aaa authentication enable default
Incorrect. The aaa authentication enable command controls authentication for entering privileged EXEC mode; it does not define login authentication for the console connection.

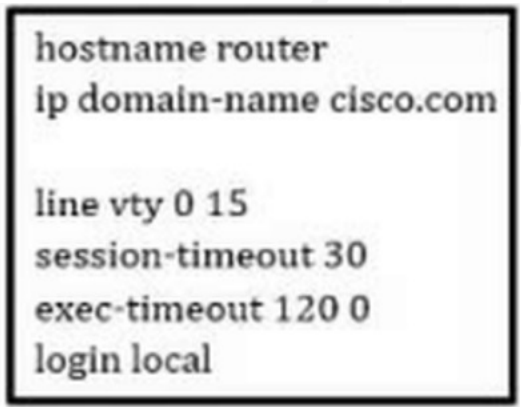
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-s/12-4/sec-usr-aaa-12-4-book.html

Question 24

Single choice · Domain: D5 Security › Configure secure remote CLI access using RSA keys and VTY transport restrictions

SINGLE CHOICE

Refer to the exhibit.



Which configuration must be added to enable remote access only using SSHv1 or SSHv2 to this router?

A. R1(config)# crypto key generate rsa modulus 2048 R1(config)# ip ssh version 2 R1(config)# line vty 0 15 R1(config-line)# transport input all

B. R1(config)# crypto key generate rsa modulus 2048 R1(config)# line vty 0 15 R1(config-line)# transport input ssh

C. R1(config)# ip ssh version 2 R1(config)# line vty 0 15 R1(config-line)# transport input ssh R1(config-line)# transport output ssh

D. R1(config)# line vty 0 15 R1(config-line)# transport input ssh R1(config-line)# transport output ssh

Answer: B. R1(config)# crypto key generate rsa modulus 2048 R1(config)# line vty 0 15 R1(config-line)# transport input ssh

Explanation

This question tests the configuration required to enable SSH on a Cisco router and restrict incoming VTY connections to SSH rather than Telnet. It specifically assesses RSA key generation and the use of the transport input ssh command.

✗ **A** R1(config)# crypto key generate rsa modulus 2048 R1(config)# ip ssh version 2 R1(config)# line vty 0 15 R1(config-line)# transport input all
Incorrect. Although RSA keys are generated, transport input all permits all supported inbound protocols, including Telnet, so access is not restricted to SSH.

https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

✓ **B** R1(config)# crypto key generate rsa modulus 2048 R1(config)# line vty 0 15 R1(config-line)# transport input ssh
Correct. Generating RSA keys enables the router to operate as an SSH server, while transport input ssh restricts inbound VTY access to SSH. Because no SSH version is explicitly forced, the router can negotiate the supported SSH version, including SSHv1 or SSHv2 where supported.

https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

✗ **C** R1(config)# ip ssh version 2 R1(config)# line vty 0 15 R1(config-line)# transport input ssh R1(config-line)# transport output ssh
Incorrect. The VTY restrictions are appropriate for SSH, but the configuration does not generate the RSA key pair required for the router to provide SSH server access. The transport output command controls outbound sessions and is not required for inbound SSH access.

https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

✗ **D** R1(config)# line vty 0 15 R1(config-line)# transport input ssh R1(config-line)# transport output ssh
Incorrect. Restricting VTY input to SSH is necessary, but this configuration does not generate RSA keys, so the router is not fully configured to operate as an SSH server. The outbound transport setting is unnecessary for the requested inbound access.

https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

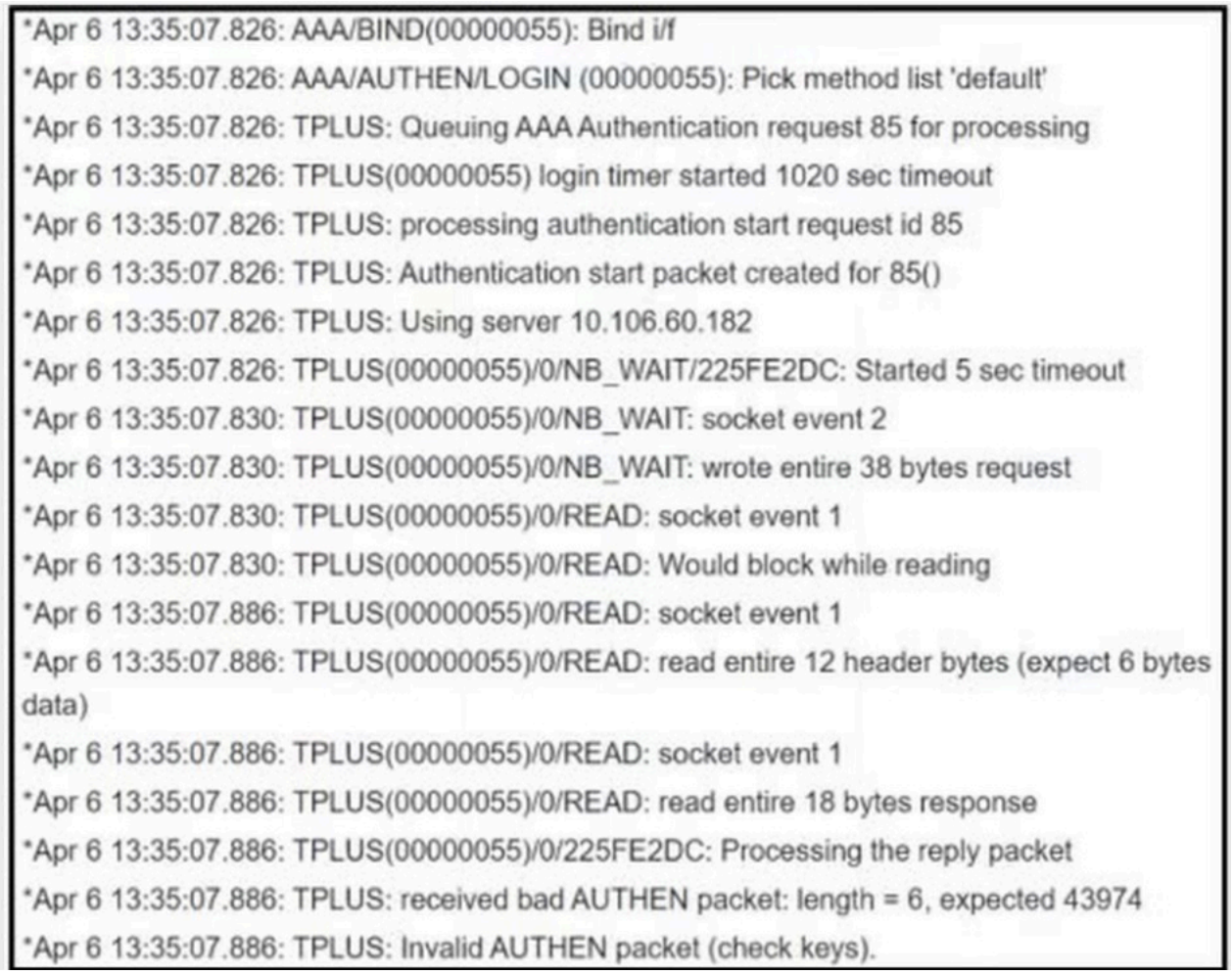
Dumpsgate

Question 25

Single choice · Domain: D5 Security › Troubleshoot TACACS+ authentication failures by interpreting AAA debug output and identifying shared-secret mismatches

SINGLE CHOICE

Refer to the exhibit.



B. R1(config)# ip tacacs source-interface Gig 0/0
C. R1(config)# tacacs server prod R1(config-server-tacacs)# port 1020
D. R1(config)# aaa authorization exec default group tacacs+ local

Answer: C. R1(config)# tacacs server prod R1(config-server-tacacs)# port 1020

Explanation

Option C is correct because it configures the TACACS+ server named `prod` to use port 1020, directly setting the server port. The other commands configure the source interface or an authorization method list, rather than changing the TACACS+ server port.

https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_i3.pdf
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srftacs.pdf

✗ **B** R1(config)# ip tacacs source-interface Gig 0/0
This command specifies the interface whose address is used as the source for TACACS+ packets. It does not configure the TCP port used to communicate with the TACACS+ server.

https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_i3.pdf
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srftacs.pdf

✓ **C** R1(config)# tacacs server prod R1(config-server-tacacs)# port 1020
This enters the configuration for the named TACACS+ server `prod` and sets its port to 1020. It therefore directly makes the requested server-port change.

https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_i3.pdf
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srftacs.pdf

✗ **D** R1(config)# aaa authorization exec default group tacacs+ local
This defines the default method list for EXEC authorization, using TACACS+ and then local authorization as a fallback. It does not set the TACACS+ server's port.

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-0sy/sec-config-auth.html
https://www.cisco.com/c/en/us/td/docs/ios/sec_user_services/configuration/guide/convert/aaa/sec_cfg_authorizatn.html

---

Question 26

Single choice · Domain: D5 Security › Configure console-line privilege levels for direct privileged EXEC access

SINGLE CHOICE

A network engineer wants to configure console access to a router without using AAA so that privileged EXEC mode is entered directly after a user provides the correct login credentials. Which action achieves this goal?

A. Configure a RADIUS or TACACS+ server and use it to send the privilege level.
B. Configure login authentication privileged on line con 0.
C. Configure privilege level 15 on line con 0.
D. Configure a local username with privilege level 15.

Answer: C. Configure privilege level 15 on line con 0.

Explanation

This question tests device access control by requiring a console line to assign privilege level 15 after successful password authentication without relying on AAA services.

✗ **A** Configure a RADIUS or TACACS+ server and use it to send the privilege level.
Incorrect. This explicitly uses external AAA, which violates the requirement to configure console access without AAA. Cisco describes privilege assignment through AAA as a centralized authentication function.

https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/23283-privilege-levels.html

✗ **B** Configure login authentication privileged on line con 0.
Incorrect. The login authentication command applies an AAA login authentication method list named privileged; it does not directly assign privilege level 15 and would not satisfy the no-AAA requirement.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_user/configuration/xe-17/sec-user-xe-17-book.html

✓ **C** Configure privilege level 15 on line con 0.
Correct. The line configuration command privilege level 15 assigns users accessing the console line

privilege level 15 after successful line authentication, causing privileged EXEC mode to be entered directly without AAA.

https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/23283-privilege-levels.html

✗ **D** Configure a local username with privilege level 15.
Incorrect. A local username with privilege level 15 affects authentication only when the console is configured to use the local username database, such as with login local. The option alone does not configure console authentication or ensure direct privileged EXEC access.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_user/configuration/xe-17/sec-user-xe-17-book.html

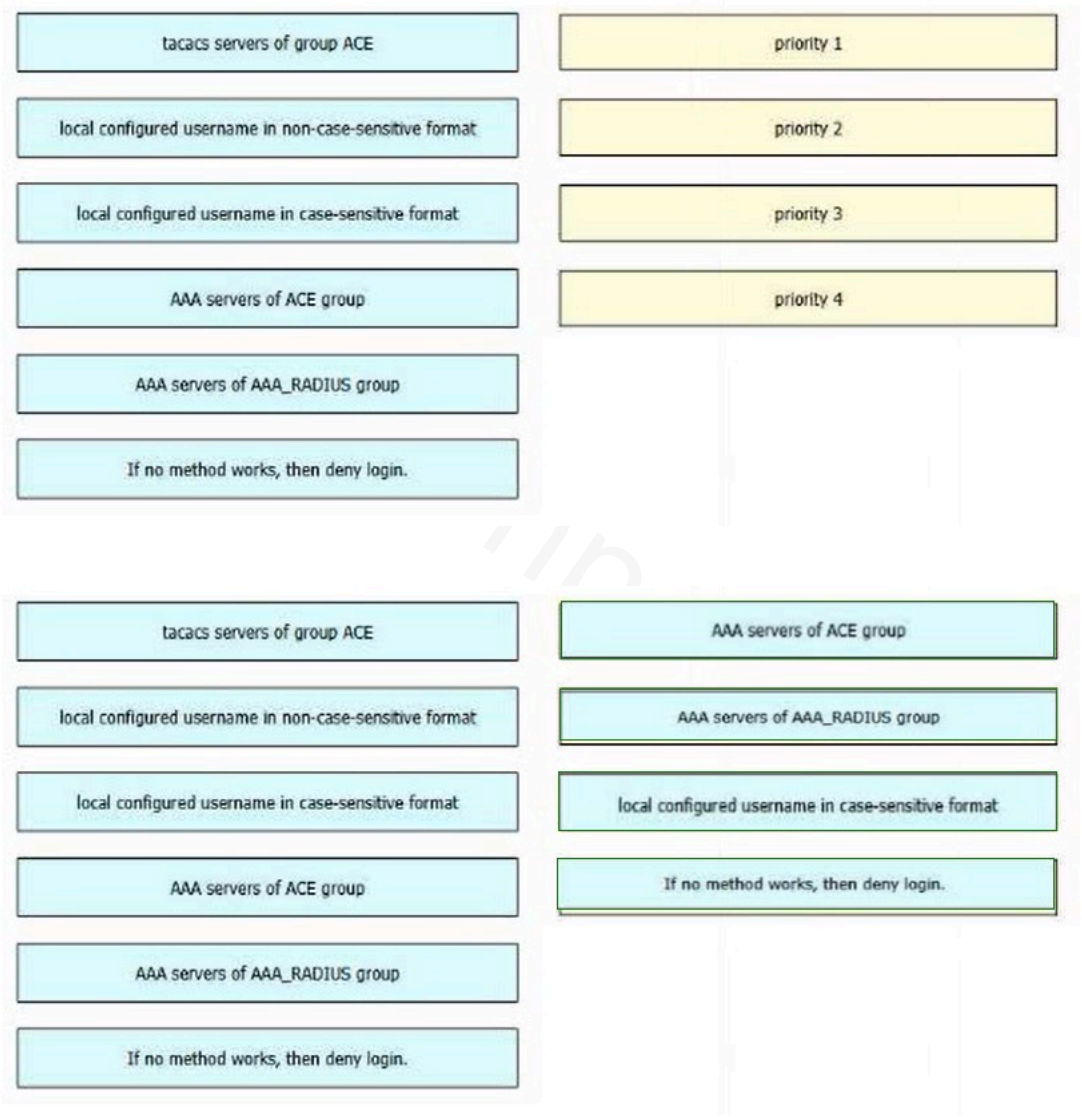
Dumpsgate

Question 27

Multiple choice · Domain: D5 Security › Determine the processing order of AAA authentication methods in a Cisco IOS login method list

An engineer creates the configuration below. Drag and drop the authentication methods from the left into the order of priority on the right. Not all options are used.

R1#show run | include aaa aaa new-model aaa authentication login default group ACE group AAA_RADIUS local-case aaa session-id common QUESTION IMAGE:



A. group ACE
B. group AAA_RADIUS
C. local-case

Answer

- A. **group ACE**
- B. **group AAA_RADIUS**
- C. **local-case**

Dumpsgate

Question 28

Single choice · Domain: D5 Security › Differentiate next-generation firewall capabilities from traditional firewall functions

SINGLE CHOICE

Which security mechanism is offered on a next-generation firewall but not on a traditional firewall?

A. integrated IPS
B. stateful firewall policies
C. SSL VPN
D. NAT

Answer: A. integrated IPS

Explanation

This question tests recognition of integrated intrusion prevention as a next-generation firewall capability. Stateful policy enforcement, SSL VPN, and NAT are established functions that can also be provided by traditional firewalls.

✓ **A** integrated IPS
Correct. A next-generation firewall integrates intrusion prevention capabilities with traditional firewall inspection, allowing it to detect and block threats beyond basic stateful traffic filtering.
https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

✗ **B** stateful firewall policies
Incorrect. Stateful policy enforcement is a fundamental traditional firewall capability and is also included in next-generation firewalls.

Free demo · full exam: 271 questions

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

✗ **C** SSL VPN
Incorrect. SSL VPN can be provided by traditional Cisco firewalls such as the ASA; it is not exclusive to next-generation firewalls.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/vpn/asa-916-vpn-config.html

✗ **D** NAT
Incorrect. Network Address Translation is a conventional firewall and routing function that predates next-generation firewalls.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/general/asa-916-general-config.html

Question 29

Single choice · Domain: D5 Security › Identify the threat category that a data center next-generation firewall is designed to protect against

SINGLE CHOICE

Which common type of attack does a data center next-generation firewall protect against?

A. DDoS protection
B. Unauthorized analyzers
C. Rogue APs
D. Malicious or risky applications

Answer: D. Malicious or risky applications

Explanation

This question tests recognition of next-generation firewall capabilities, particularly application-aware inspection and protection against malicious or risky applications in enterprise and data center environments.

✗ **A** DDoS protection
Incorrect. Although firewalls can contribute to traffic filtering and mitigation strategies, DDoS protection is not the best match for the common data center next-generation firewall capability described here. Cisco identifies application visibility and control, including protection against threats and risky applications, as core NGFW functions.

https://www.cisco.com/c/en/us/products/security/firepower-ngfw/index.html

✗ **B** Unauthorized analyzers
Incorrect. Unauthorized analyzers are not a standard threat category directly associated with the primary protection capabilities of a data center next-generation firewall. NGFWs focus on inspecting and controlling network traffic, users, applications, and threats.

https://www.cisco.com/c/en/us/products/security/firepower-ngfw/index.html

✗ **C** Rogue APs
Incorrect. Rogue access-point detection and containment are primarily wireless LAN security functions, rather than the common protection role of a data center next-generation firewall.

https://www.cisco.com/c/en/us/products/security/firepower-ngfw/index.html

✓ **D** Malicious or risky applications
Correct. A next-generation firewall provides application visibility and control and can identify, block, and

protect against malicious or risky applications using application-aware and threat-aware inspection.
https://www.cisco.com/c/en/us/products/security/firepower-ngfw/index.html

Question 30

Single choice · Domain: D5 Security › Identify the HTTP response behavior for a REST API request that lacks required authentication data

SINGLE CHOICE

What is the result of sending a GET REST API call that does not contain the necessary authentication data to a server?

A. The server authenticates the client using its IP address and executes the call accordingly.
B. The server keeps the session open and waits for the client to supply the authentication data, then executes the call accordingly.
C. The server executes the call with guest privileges.
D. The server responds with a 4xx response code without executing the call.

Answer: D. The server responds with a 4xx response code without executing the call.

Explanation

This question tests REST API security fundamentals, specifically how a server rejects an unauthenticated request. A server normally returns a 4xx client-error response, such as HTTP 401 Unauthorized, and does not execute the requested operation.

✗ **A** The server authenticates the client using its IP address and executes the call accordingly.
Incorrect. A server does not normally authenticate a REST API client solely by its source IP address when required authentication data is missing. The request should be rejected with a client-error response.
https://developer.cisco.com/docs/ios-xe/#!restconf/overview

✗ **B** The server keeps the session open and waits for the client to supply the authentication data, then executes the call accordingly.
Incorrect. REST API servers generally respond to the unauthenticated request immediately rather than keeping the session open while waiting for credentials. The client must send a new request containing valid authentication data.
https://developer.cisco.com/docs/ios-xe/#!restconf/overview

✗ **C** The server executes the call with guest privileges.
Incorrect. The server executes a request with guest or anonymous privileges only when that access model is explicitly configured. Missing required authentication data results in rejection rather than automatic guest access.
https://developer.cisco.com/docs/ios-xe/#!restconf/overview

✓ **D** The server responds with a 4xx response code without executing the call.
Correct. When required authentication data is absent, the server rejects the request with a 4xx client-error response, commonly HTTP 401 Unauthorized, and does not execute the GET operation.
https://developer.cisco.com/docs/ios-xe/#!restconf/overview

Question 31

Single choice · Domain: D6 Automation and Artificial Intelligence › Interpret basic Python components and scripts

SINGLE CHOICE

Refer to the exhibit.

```
count = -4
while count > -8:
    print(count)
    count -= 1
```

What is output by this code?

A. -4 -5 -6 -7

B. -1 -2 -3 -4

C. 8 7 6 5

D. 4 5 6 7 next condition check, -8 > -8 is false because the comparison uses the strict greater-than operator rather than greater-than-or-equal-to. The loop therefore terminates without printing -8. Python's language reference specifies that a while statement repeatedly executes its suite while its controlling expression evaluates as true and terminates when that expression becomes false. Consequently, the output sequence is -4, -5, -6, -7, making option A correct. This type of code interpretation is explicitly covered by the current ENCOR blueprint. Study Guide Reference: ENCOR v1.2 --- 6.0 Automation and Artificial Intelligence 6.1 Interpret basic Python components and scripts.

Answer: A. -4 -5 -6 -7

Explanation

This question tests interpretation of a Python while loop, including variable initialization, decrementing a counter, output sequencing, and strict greater-than evaluation. These skills align with the ENCOR automation and artificial intelligence objectives.

✓ **A** -4 -5 -6 -7
Correct. Starting at -4, the loop prints the current value and decrements it by 1 while the value is greater than -8. It prints -4, -5, -6, and -7; when the value becomes -8, the condition -8 > -8 is false, so -8 is not printed.

https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/350-401-encor.html

✗ **B** -1 -2 -3 -4
Incorrect. The sequence begins with the initialized value -4, not -1, and the loop continues downward while the value remains greater than -8.

https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/350-401-encor.html

✗ **C** 8 7 6 5
Incorrect. The counter starts at -4 and is decremented, so the output consists of negative values rather than positive values.

https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/350-401-encor.html

✗ **D** 4 5 6 7 next condition check, -8 > -8 is false because the comparison uses the strict greater-than operator rather than greater-than-or-equal-to. The loop therefore terminates without printing -8. Python's language reference specifies that a while statement repeatedly executes its suite while its controlling expression evaluates as true and terminates when that expression becomes false.

Consequently, the output sequence is -4, -5, -6, -7, making option A correct. This type of code interpretation is explicitly covered by the current ENCOR blueprint. Study Guide Reference: ENCOR v1.2 --- 6.0 Automation and Artificial Intelligence 6.1 Interpret basic Python components and scripts.
Incorrect. The counter starts at -4 and decreases on each iteration; it does not start at 4 or increase.
https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/350-401-encor.html

Question 32

Single choice · Domain: D6 Automation and Artificial Intelligence › Interpret HTTP status codes and JSON responses from Cisco Catalyst Center APIs

SINGLE CHOICE

Refer to the exhibit.

What can be concluded from the Cisco Catalyst Center (formerly DNA Center) Developer Toolkit API output?

A. The content-type of the response is YAML.
B. The status code ''200'' indicates that the client request was accepted successfully.
C. The status code ''200'' indicates that the client must take some additional action to complete the request.
D. The content-type of the response is XML.

Answer: B. The status code ''200'' indicates that the client request was accepted successfully.

Explanation

This question tests the ability to interpret a Cisco Catalyst Center Developer Toolkit API response, including recognizing JSON formatting and understanding the meaning of an HTTP 200 status code.

✗ **A** The content-type of the response is YAML.
Incorrect. The response is represented in JSON format, as shown by the structured objects, quoted

property names, arrays, and key-value pairs. Cisco Catalyst Center API documentation is available at.
https://developer.cisco.com/docs/dna-center/

✓ **B** The status code "200" indicates that the client request was accepted successfully.
Correct. HTTP status code 200 means the request was successfully processed and the response contains the requested result, which here is the device role of Edge Node. Cisco Catalyst Center API documentation is available at.
https://developer.cisco.com/docs/dna-center/

✗ **C** The status code "200" indicates that the client must take some additional action to complete the request.
Incorrect. HTTP 200 indicates successful completion of the request. A status such as 202 Accepted is generally used when processing has been accepted but is not yet complete. Cisco Catalyst Center API documentation is available at.
https://developer.cisco.com/docs/dna-center/

✗ **D** The content-type of the response is XML.
Incorrect. The response uses JSON syntax rather than XML syntax; it contains JSON objects and an array for the roles field. Cisco Catalyst Center API documentation is available at.
https://developer.cisco.com/docs/dna-center/

Question 33

Single choice · Domain: D6 Automation and Artificial Intelligence › Identify the purpose and direction of northbound APIs in controller-based networks

SINGLE CHOICE

What does a northbound API accomplish?

A. Programmatic control of abstracted network resources through a centralized controller
B. Access to controlled network resources from a centralized node
C. Controlled access to switches from automated security applications
D. Communication between SDN controllers and physical switches

Answer: A. Programmatic control of abstracted network resources through a centralized controller

Explanation

This question tests whether the candidate can distinguish northbound APIs, which expose abstracted controller-managed network capabilities to applications and automation systems, from southbound interfaces used between controllers and network devices.

✓ **A** Programmatic control of abstracted network resources through a centralized controller
Correct. A northbound API allows applications and automation systems to programmatically interact with abstracted network resources exposed by a centralized controller. Cisco describes controller-based networking and programmability in its software-defined networking overview.
https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

✗ **B** Access to controlled network resources from a centralized node
Incorrect. This wording does not identify the northbound direction or the application-facing nature of the interface. Northbound APIs provide access from applications or orchestration systems to controller

Free demo · full exam: 271 questions

abstractions, rather than simply describing access from a centralized node.

https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

✗ **C** Controlled access to switches from automated security applications
Incorrect. Northbound APIs are not specifically security-application interfaces or switch-access mechanisms. They expose controller services and abstractions to applications; direct controller-to-device communication is generally associated with southbound interfaces.

https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

✗ **D** Communication between SDN controllers and physical switches
Incorrect. Communication between an SDN controller and physical network devices is the role of a southbound interface or API, not a northbound API. Northbound interfaces connect the controller to applications and higher-level orchestration systems.

https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

Dumpsgate

Question 34

Single choice · Domain: D6 Automation and Artificial Intelligence › Use Python JSON serialization to write a data structure to a file with json.dump()

SINGLE CHOICE

Refer to the exhibit.

```
import json

Devices={'Switches':
  [
   {'name': 'AccSw1', 'ip': '2001:db8:1:fffe::1'},
   {'name': 'AccSw2', 'ip': '2001:db8:1:fffe::2'}
  ],
  'Routers':
    {'CE1': {'ip': '2001:db8:1:ffff::1'},
     'CE2': {'ip': '2001:db8:1:ffff::2'}
    }
}
```

Which Python snippet stores the data structure of the device in JSON format?

A. with open('devices.json', 'w') as OutFile: Devices = json.load(OutFile)

B. OutFile = open('devices.json', 'w') json.dump(Devices, OutFile) OutFile.close()

C. OutFile = open('devices.json', 'w') The correct snippet is option B because json.dump(Devices, OutFile) serializes the Python data structure and writes the resulting JSON directly to the open file object. The file is opened in write mode with open('devices.json', 'w'), and OutFile.close() closes the file after writing. Option A is wrong because json.load() reads JSON from a file and converts it into a Python object; it does not write a Python object to disk. It is also being used on a file opened in write mode, which is logically incorrect. Option C writes str(Devices), which produces a Python string representation of the dictionary, not standards-compliant JSON. That output may use single quotes and Python-specific formatting, which is not proper JSON. Option D uses json.dumps(Devices), which returns a JSON-formatted string, but it does not write that string to the file because the return value is ignored. ENCOR automation questions often test the difference between dump, dumps, load, and loads. Reference/topics: ENCOR Automation, Python, JSON, json.dump(), json.dumps(), file output, API data formatting.

Answer: B. OutFile = open('devices.json', 'w') json.dump(Devices, OutFile) OutFile.close()

Explanation

This question tests the ability to distinguish Python JSON serialization and deserialization functions and select the method that writes a Python data structure directly to a JSON file.

✗ **A** with open('devices.json', 'w') as OutFile: Devices = json.load(OutFile)
Incorrect. json.load() reads JSON from a file and converts it into a Python object. It does not serialize and write the Devices structure, and the file is opened in write mode.

Free demo · full exam: 271 questions

https://developer.cisco.com/learning/tracks/programmability/

✓ **B** OutFile = open('devices.json', 'w') json.dump(Devices, OutFile) OutFile.close()
Correct. json.dump() serializes the Python object and writes the resulting JSON directly to the open file object. The file is opened in write mode and then closed after the data is written.

https://developer.cisco.com/learning/tracks/programmability/

✗ **C** OutFile = open('devices.json', 'w') The correct snippet is option B because json.dump(Devices, OutFile) serializes the Python data structure and writes the resulting JSON directly to the open file object. The file is opened in write mode with open('devices.json', 'w'), and OutFile.close() closes the file after writing. Option A is wrong because json.load() reads JSON from a file and converts it into a Python object; it does not write a Python object to disk. It is also being used on a file opened in write mode, which is logically incorrect. Option C writes str(Devices), which produces a Python string representation of the dictionary, not standards-compliant JSON. That output may use single quotes and Python-specific formatting, which is not proper JSON. Option D uses json.dumps(Devices), which returns a JSON-formatted string, but it does not write that string to the file because the return value is ignored. ENCOR automation questions often test the difference between dump, dumps, load, and loads. Reference/topics: ENCOR Automation, Python, JSON, json.dump(), json.dumps(), file output, API data formatting.
Incorrect. Converting the object with str() produces Python's string representation, which may use single quotes and other Python-specific formatting rather than standards-compliant JSON.

https://developer.cisco.com/learning/tracks/programmability/

✗ **D** OutFile = open('devices.json', 'w') json.dumps(Devices) OutFile.close()
Incorrect. json.dumps() returns a JSON-formatted string, but this snippet ignores the returned value and does not write it to OutFile. json.dump() is the appropriate function when writing directly to a file.

https://developer.cisco.com/learning/tracks/programmability/

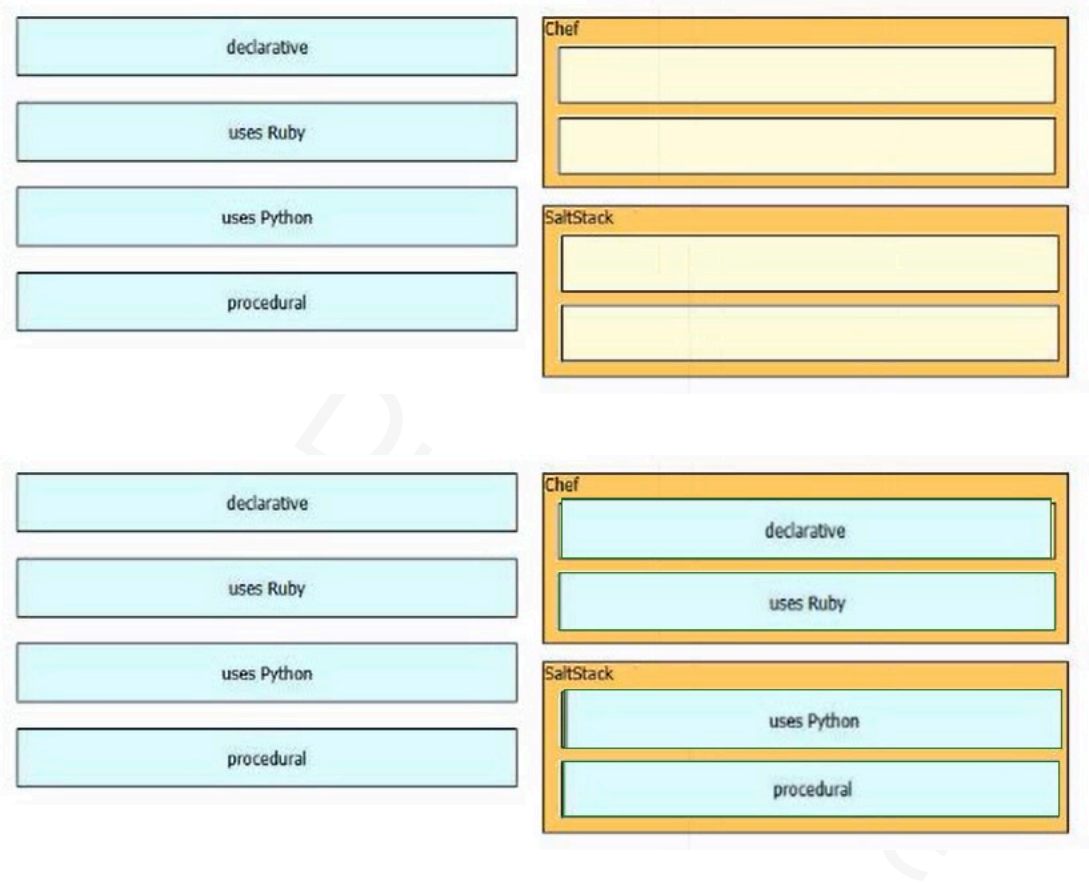
Dumpsgate

Question 35

Multiple choice · Domain: D6 Automation and Artificial Intelligence › Match configuration-management tools with their implementation language and configuration approach

Drag and drop the characteristics from the left into the orchestration tools that they describe on the right.

QUESTION IMAGE:



A. Declarative — SaltStack
B. Uses Ruby — Chef
C. Uses Python — SaltStack
D. Procedural — Chef

Answer

- A. **Declarative — SaltStack**
- B. **Uses Ruby — Chef**
- C. **Uses Python — SaltStack**
- D. **Procedural — Chef**

Explanation

This drag-and-drop question tests recognition of common automation and configuration-management tools, including the languages they use and whether their typical model is declarative or procedural.

Free demo · full exam: 271 questions

✓ **A** Declarative — SaltStack
Correct. SaltStack state files commonly describe the desired end state of systems, which is a declarative configuration approach. Cisco includes automation and configuration-management concepts in the ENCOR objectives.
https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/encor.html

✓ **B** Uses Ruby — Chef
Correct. Chef recipes use a Ruby-based domain-specific language and are authored using Ruby syntax. Cisco identifies automation technologies and tools as part of the ENCOR exam scope.
https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/encor.html

✓ **C** Uses Python — SaltStack
Correct. SaltStack is primarily implemented in Python, and its modules and extensions use Python extensively. This aligns with the ENCOR automation and programmability focus.
https://developer.cisco.com/automation/

✓ **D** Procedural — Chef
Correct for this comparison. Chef recipes are commonly treated as procedural because resources and actions are processed in recipe order, although Chef also provides desired-state behavior. Cisco lists automation technologies among the ENCOR exam topics.
https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/encor.html

Question 36

Single choice · Domain: D6 Automation and Artificial Intelligence › Differentiate Cisco DNA Center southbound APIs from northbound integrations

SINGLE CHOICE

What is a capability of the Cisco DNA Center southbound API?

```
list = [1, 2, 3, 4]
list[3] = 10
print(list)
```

Refer to the exhibit. What is the value of the variable list after the code is run?

A. [1, 2, 10]
B. It communicates with managed network devices through southbound device-management interfaces to discover devices, collect network state, and apply configuration
C. [1, 2, 10, 4]
D. [1, 10, 10, 10]

Answer: B. It communicates with managed network devices through southbound device-management interfaces to discover devices, collect network state, and apply configuration

Explanation
This question tests whether the candidate can identify the function of Cisco DNA Center southbound

APIs. Southbound interfaces communicate with and configure network infrastructure, whereas ITSM integrations such as ServiceNow are northbound capabilities.

✗ **A** [1, 2, 10]
Incorrect. Connecting Cisco DNA Center to ITSM platforms such as ServiceNow is a northbound integration capability. Southbound APIs communicate with network devices and infrastructure controllers.

https://developer.cisco.com/docs/dna-center/

✓ **B** It communicates with managed network devices through southbound device-management interfaces to discover devices, collect network state, and apply configuration
The controller architecture definition is that northbound APIs serve applications, whereas southbound interfaces communicate with managed devices. Catalyst Center's documented device-facing communications include SSH, Telnet, SNMP, ICMP, and NETCONF where applicable.

https://developer.cisco.com/docs/nx-os/controller-layer/

✗ **C** [1, 2, 10, 4]
Incorrect. This is an answer choice from the unrelated Python exhibit question, not a capability of the Cisco DNA Center southbound API.

https://developer.cisco.com/docs/dna-center/

✗ **D** [1, 10, 10, 10]
Incorrect. This is an answer choice from the unrelated Python exhibit question, not a capability of the Cisco DNA Center southbound API.

https://developer.cisco.com/docs/dna-center/

Dumpsgate

Question 37

Multiple choice · Domain: D6 Automation and Artificial Intelligence › Identify NETCONF and RESTCONF as protocols that use YANG data models

Which two protocols are used with YANG data models? (Choose two.)

A. NETCONF
B. RESTCONF
C. SSH
D. TLS
E. HTTPS

Answer

- A. **NETCONF**
- B. **RESTCONF**

Explanation

This question tests knowledge of model-driven programmability in which YANG defines structured data models and NETCONF or RESTCONF provides the protocol used to retrieve or configure that data.

✓ **A** NETCONF
Correct. NETCONF is a model-driven network management protocol that uses YANG data models for structured configuration and operational data. Cisco.

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/programmability/b-programmability.html

✓ **B** RESTCONF
Correct. RESTCONF exposes YANG-modeled data through a REST-like HTTPS interface for programmatic configuration and retrieval. Cisco.
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/programmability/b-programmability.html

✗ **C** SSH
Incorrect. SSH is a secure transport commonly used by NETCONF, but it is not the protocol that defines or directly provides YANG model-based management. Cisco.
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/programmability/b-programmability.html

✗ **D** TLS
Incorrect. TLS provides transport security and may protect management sessions, but it is not a YANG-based network management protocol. Cisco.
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/programmability/b-programmability.html

✗ **E** HTTPS
Incorrect. HTTPS is the secure transport used by RESTCONF; RESTCONF itself is the protocol that operates on YANG-modeled resources. Cisco.
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/programmability/b-programmability.html

Question 38

Single choice · Domain: D6 Automation and Artificial Intelligence › Interpret Python for loops using the range() function and its exclusive stop value

SINGLE CHOICE

Refer to the exhibit.

```
for x in range(0, 5):
    print(x)
```

Refer to the exhibit. What is output by this code?

A. 012345
B. (0.5)
C. 05
D. 01234

Answer: D. 01234

Explanation

This question tests the ability to determine the output of a basic Python iteration construct. Specifically, it requires understanding that range(0, 5) produces the values 0 through 4, excluding 5.

✗ **A** 012345
Incorrect. Python's range(0, 5) stops before 5, so the loop prints only 0, 1, 2, 3, and 4. Cisco includes Python and automation fundamentals among its network programmability topics.

Dumpsgate

https://developer.cisco.com/learning/tracks/devnet-associate/programmability-basics/

✗ **B** (0.5)
Incorrect. The code does not perform decimal arithmetic or print parentheses. It iterates through integer values generated by range(0, 5). Cisco includes Python and automation fundamentals among its network programmability topics.

https://developer.cisco.com/learning/tracks/devnet-associate/programmability-basics/

✗ **C** 05
Incorrect. The loop prints every value in the sequence, not only the first and last values. The resulting values are 0, 1, 2, 3, and 4. Cisco includes Python and automation fundamentals among its network programmability topics.

https://developer.cisco.com/learning/tracks/devnet-associate/programmability-basics/

✓ **D** 01234
Correct. range(0, 5) generates 0, 1, 2, 3, and 4 because the stop value 5 is exclusive, and print(x) outputs each value in sequence. Cisco includes Python and automation fundamentals among its network programmability topics.

https://developer.cisco.com/learning/tracks/devnet-associate/programmability-basics/

Dumpsgate

Question 39

Single choice · Domain: D6 Automation and Artificial Intelligence › Use Python ncclient NETCONF get_config with an XML subtree filter to retrieve selected running configuration data

SINGLE CHOICE

Refer to the exhibit.

```
interface_filter = '''
 <filter>
   <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
     <interface>
       <GigabitEthernet>
         <name>1</name>
       </GigabitEthernet>
     </interface>
   </native>
 </filter>
'''


result = m.get_config('running', interface_filter)
print(result)
```

What is the result of running the Python NETCONF script?

A. It prints the XML output of show running interface GigabitEthernet 1 on the device with IP address

B. 192.168.1.10.

B. It configures the IP address 192.168.1.10 on the GigabitEthernet 1 interface and prints the new XML configuration.

C. It opens interface configuration mode on the router and prompts for further XML commands from the user.

D. It prints the XML output of show running on the device with IP address 192.168.1.0.

Answer: A. It prints the XML output of show running interface GigabitEthernet 1 on the device with IP address

Explanation

This question tests understanding of NETCONF operational behavior and XML filtering. The get_config operation reads the running configuration and returns only the interface subtree requested by the filter; it does not modify the device or open CLI configuration mode.

✓ **A** It prints the XML output of show running interface GigabitEthernet 1 on the device with IP address Correct. m.get_config("running", interface_filter) retrieves configuration from the running datastore and applies the XML subtree filter for GigabitEthernet 1. The returned result is XML and is printed; the operation does not configure the interface.

https://developer.cisco.com/docs/ios-xe/netconf/

✗ **B** It configures the IP address 192.168.1.10 on the GigabitEthernet 1 interface and prints the new XML configuration.
Incorrect. get_config is a read operation that retrieves configuration. It does not change interface addressing; configuration changes require an operation such as edit_config.

https://developer.cisco.com/docs/ios-xe/netconf/

✗ **C** It opens interface configuration mode on the router and prompts for further XML commands from the user.
Incorrect. NETCONF does not open an interactive IOS CLI configuration mode. The script sends a NETCONF RPC and receives an XML response from the running datastore.

https://developer.cisco.com/docs/ios-xe/netconf/

✗ **D** It prints the XML output of show running on the device with IP address 192.168.1.0.
Incorrect. The request uses the running datastore with a filter selecting only GigabitEthernet 1, rather than retrieving the complete running configuration. It also does not identify or change the device address to 192.168.1.0.

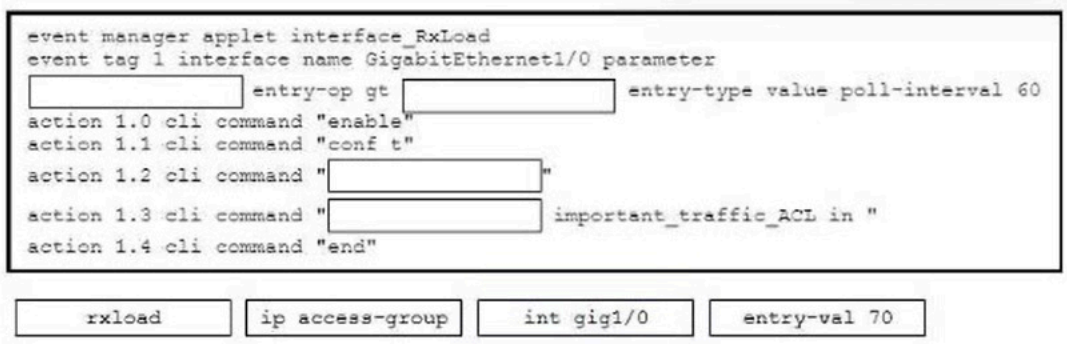
https://developer.cisco.com/docs/ios-xe/netconf/

Question 40

Multiple choice · Domain: D6 Automation and Artificial Intelligence › Configure an Embedded Event Manager applet to monitor interface receive load and apply an ACL when a threshold is exceeded

Refer to the exhibit. Drag and drop the command snippets from the bottom onto the boxes to configure an EEM applet to only allow important traffic on interface GigabitEthernet1/0 when rxload exceeds 70%.

QUESTION IMAGE:



A. event manager applet interface RxLoad

B. event tag 1 interface name GigabitEthernet1/0 parameter rxload entry-op gt entry-type value entry-val 70 poll-interval 60

C. action 1.0 cli command "enable"

D. action 1.1 cli command "conf t"

E. action 1.2 cli command "interface GigabitEthernet1/0"

F. action 1.3 cli command "ip access-group important_traffic_ACL in"

G. action 1.4 cli command "end"

Answer

- A. **event manager applet interface RxLoad**
- B. **event tag 1 interface name GigabitEthernet1/0 parameter rxload entry-op gt entry-type value entry-val 70 poll-interval 60**
- C. **action 1.0 cli command "enable"**
- D. **action 1.1 cli command "conf t"**
- E. **action 1.2 cli command "interface GigabitEthernet1/0"**
- F. **action 1.3 cli command "ip access-group important_traffic_ACL in"**
- G. **action 1.4 cli command "end"**

Explanation

This question tests the use of Cisco EEM event detectors and CLI actions to automate interface policy changes based on an operational threshold. The applet monitors GigabitEthernet1/0 receive load and applies an inbound ACL when the value exceeds 70 percent.

✓ **A** event manager applet interface RxLoad
Correct. This command creates the EEM applet named interface RxLoad, which is the container for the event detector and actions.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-s/eem-15-s-book.html

✓ **B** event tag 1 interface name GigabitEthernet1/0 parameter rxload entry-op gt entry-type value entry-val 70 poll-interval 60
Correct. This event detector monitors the rxload parameter on GigabitEthernet1/0 and triggers when its value is greater than 70, checking every 60 seconds.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-s/eem-15-s-book.html

✓ **C** action 1.0 cli command "enable"
Correct. The first EEM action enters privileged EXEC mode so subsequent configuration commands can be executed.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-s/eem-15-s-book.html

✓ **D** action 1.1 cli command "conf t"
Correct. This action enters global configuration mode, which is required before changing the interface ACL configuration.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-s/eem-15-s-book.html

✓ **E** action 1.2 cli command "interface GigabitEthernet1/0"
Correct. This action selects the monitored interface so the following ACL command is applied to the correct interface.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-s/eem-15-s-book.html

✓ **F** action 1.3 cli command "ip access-group important_traffic_ACL in"
Correct. This action applies the important_traffic_ACL access list in the inbound direction on GigabitEthernet1/0, allowing the intended traffic policy to be enforced when rxload exceeds the threshold.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaccess/configuration/15-s/iap-15-s-book.html

✓ **G** action 1.4 cli command "end"
Correct. The final action exits configuration mode after the ACL has been applied.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-s/eem-15-s-book.html

Free demo · full exam: 271 questions