CERT EMPIRE

CISCO ENCOR 350-401 Exam Questions

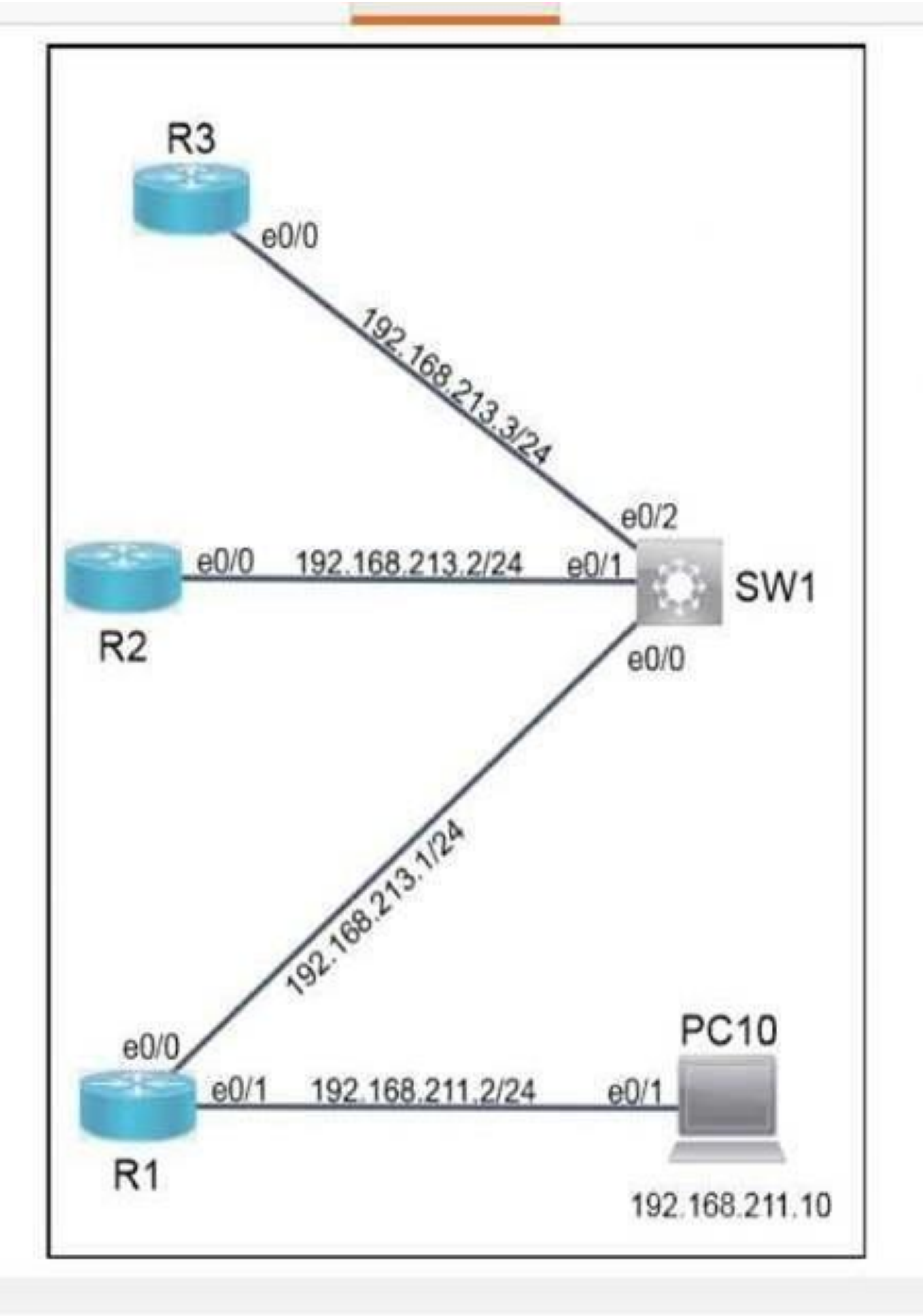
Total Questions: 230+
Demo Questions: 35
Version: Updated for 2025

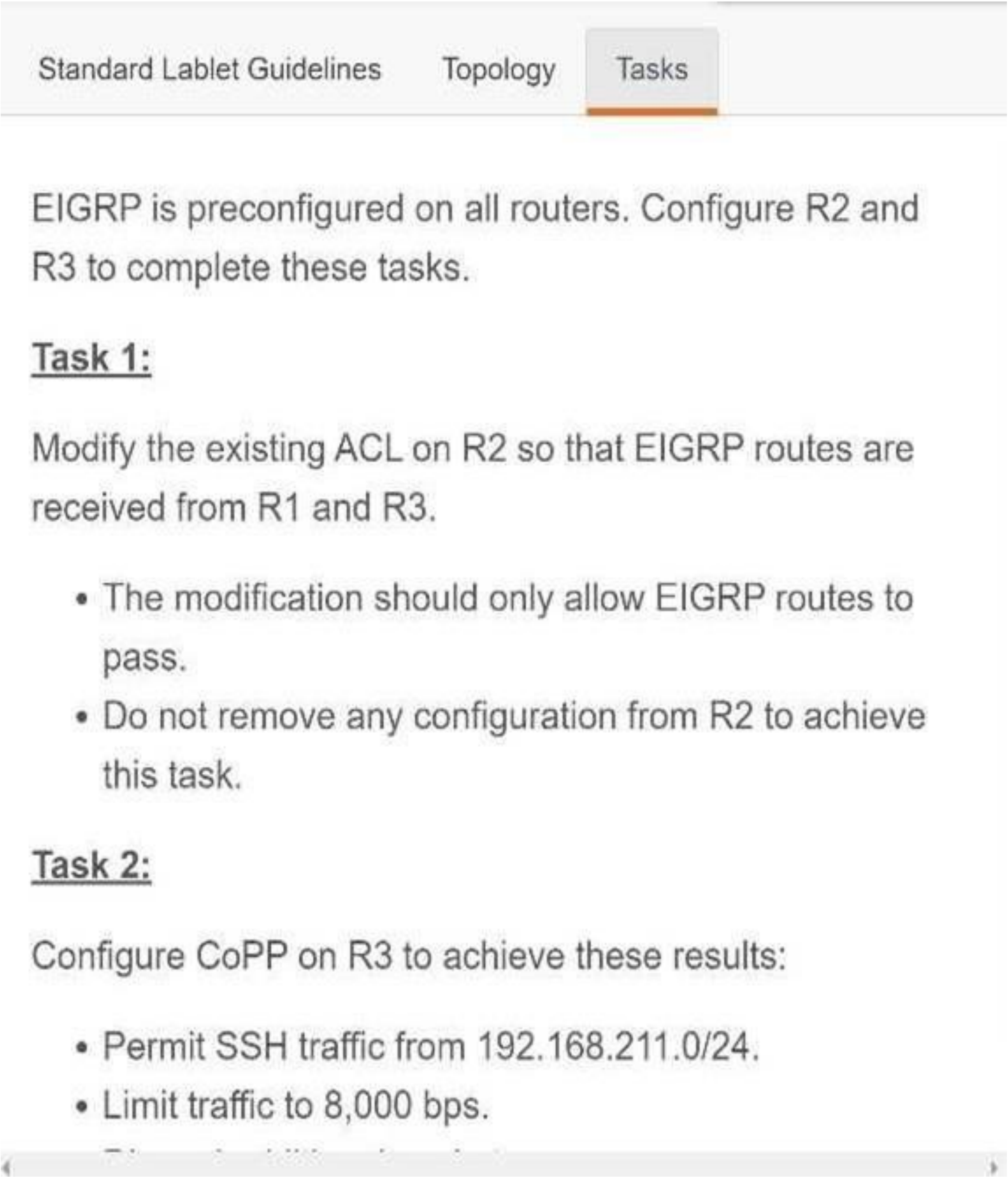
Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
350-401 Exam Dumps by Cert Empire

Question: 1

Simulation: -





EIGRP is preconfigured on all routers. Configure R2 and R3 to complete these tasks.

Task 1:

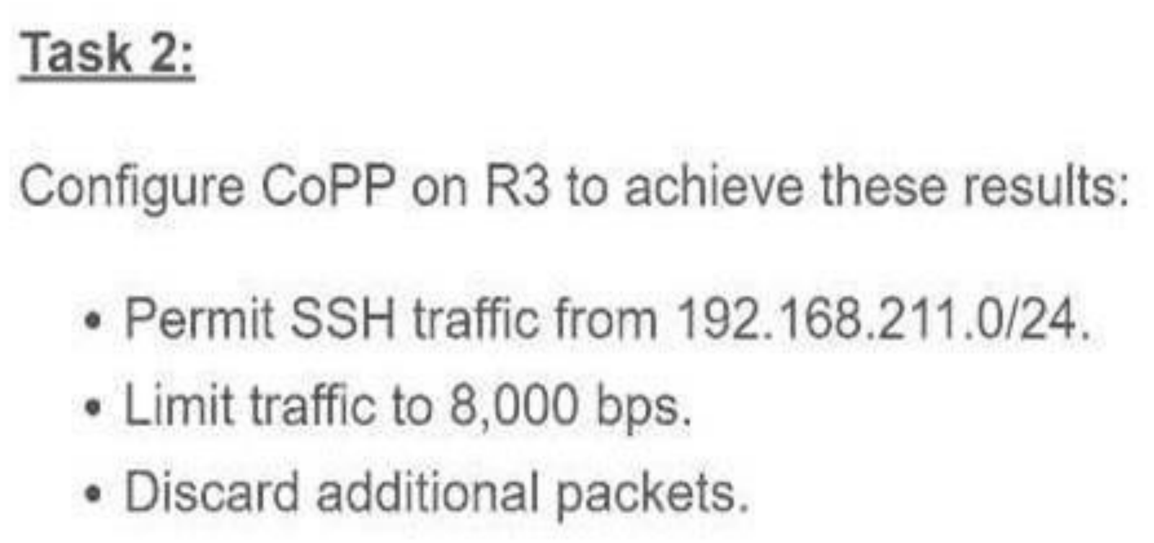
Modify the existing ACL on R2 so that EIGRP routes are received from R1 and R3.

- The modification should only allow EIGRP routes to pass.
- Do not remove any configuration from R2 to achieve this task.

Task 2:

Configure CoPP on R3 to achieve these results:

- Permit SSH traffic from 192.168.211.0/24.
- Limit traffic to 8,000 bps.



Task 2:

Configure CoPP on R3 to achieve these results:

- Permit SSH traffic from 192.168.211.0/24.
- Limit traffic to 8,000 bps.
- Discard additional packets.

Answer:

See the explanation below

Explanation:

below Explanation: Task 1: Modify ACL on R2 to Receive EIGRP Routes The objective is to modify an existing Access Control List (ACL) on router R2 to permit EIGRP routing updates from routers R1 and R3. The existing configuration is likely using a distribute-list to filter incoming routes, and this list needs to be updated. A distribute-list applied inbound uses a standard ACL to filter routes based on the IP address of the advertising router. R1's advertising interface IP: 192.168.213.1. R3's advertising interface IP: 192.168.213.3 Correct Configuration Commands for R2: The specific name or number of the "existing ACL" is not provided. Assuming it is a named ACL called EIGRPFILTER, the modification would be as follows. First, one would enter configuration mode. Cisco CLI R2# configure terminal Next, enter the configuration mode for the existing standard IP access list. Cisco CLI R2(config)# ip access-list standard EIGRPFILTER The instruction "Modify the existing ACL" and "Do not remove any configuration" implies adding new permit statements to the ACL. These commands will allow routes advertised from R1 and R3. Cisco CLI R2(config-std-nacl)# permit host 192.168.213.1 R2(config-std-nacl)# permit host 192.168.213.3 Explanation: These commands modify the specified standard ACL to explicitly permit routing updates sourced from the IP addresses of R1 and R3. When this ACL is applied to an inbound distribute-list within the EIGRP routing process on R2, it will cause R2 to accept EIGRP advertisements originating from those two routers. Any updates from other sources would be denied by the implicit deny any at the end of the ACL. Task 2: Configure CoPP on R3: The objective is to configure Control Plane Policing (CoPP) on R3 to rate-limit SSH traffic from the 192.168.211.0/24 network to 8,000 bps and discard any excess traffic. This is accomplished using the Modular QoS CLI (MQC) framework. Correct Configuration Commands for R3: 1. Create an extended ACL to identify the specific traffic (SSH from the source network). Cisco CLI R3# configure terminal R3(config)# ip access-list extended SSHTRAFFICACL R3(config-ext-nacl)# permit tcp 192.168.211.0 0.0.0.255 any eq 22 2. Create a class-map to classify traffic matching the ACL. Cisco CLI R3(config)# class-map COPPSSHCLASS R3(config-cmap)# match access-group name SSHTRAFFICACL 3. Create a policy-map to define the policing action (rate limit and discard). Cisco CLI R3(config)# policy-map COPPPOLICY R3(config-pmap)# class COPPSSHCLASS R3(config-pmap-c)# police 8000 conform-action transmit exceed-action drop 4. Apply the policy-map to the control plane. Cisco CLI R3(config)# control-plane R3(config-cp)# service-policy input COPPPOLICY Explanation: This configuration protects the router's central processor. The ACL first defines the traffic of interest: TCP port 22 (SSH) from the 192.168.211.0/24 subnet. The class-map then uses this ACL to classify incoming packets. The policy-map applies a policing rule to this class, allowing traffic up to 8,000 bps (conform- action transmit) and dropping anything above that rate (exceed-action drop). Finally, the service-policy input command under the control-plane configuration applies this entire policy to all traffic destined for the router's control plane.

References:

1. Task 1 (EIGRP Distribute-List):
o Source: Cisco, "IP Routing: EIGRP Configuration Guide"
o Details: The section on "How to Filter Routes with a Distribute List"
explains the use of standard ACLs with the distribute-list command
to filter updates based on the advertising router's address.
o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/iprouteeigrp/configuration/15-mt/ire-15-mt-book/ire-filter-
routes.html
2. Task 2 (Control Plane Policing - CoPP):
o Source: Cisco, "Control Plane Policing Configuration Guide"
o Details: This guide details the MQC framework for implementing
CoPP, including the creation of ACLs, class-map, policy-map with
the police action, and application via the control-plane command.
o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/secdatacopp/configuration/15-mt/sec-data-copp-15-mt-
book/sec-copp-understand-config.html

Question: 2

A customer requires their wireless data traffic to egress at the switch port of the access point. Which access point mode supports this?

A. Bridge

B. Sniffer

C. FlexConnect

D. Monitor

Answer:

C

Explanation:

FlexConnect is a Cisco wireless solution designed for branch offices and remote deployments. An AP in FlexConnect mode can switch client data traffic locally. When a Wireless LAN (WLAN) is configured for local switching, the AP breaks out the data traffic directly onto the local wired network through its switch port. This prevents data from having to traverse the WAN link back to a central Wireless LAN Controller (WLC), which is ideal for accessing local resources and conserving WAN bandwidth. Control and management traffic, however, is still typically sent back to the central WLC.

Why Incorrect Options are Wrong:

A. Bridge: This mode, also known as mesh networking, is used to wirelessly link two or more network segments. Its primary function is to provide a wireless backbone connection, not to define the egress point for local client traffic in the manner described. B. Sniffer: An AP in sniffer mode is dedicated to capturing all 802.11 wireless frames on a specific channel for troubleshooting and analysis using tools like Wireshark. It does not provide network access to clients or forward their data traffic. D. Monitor: A monitor mode AP is a dedicated security sensor. It scans wireless channels to detect rogue access points, rogue clients, and intrusion attempts. It does not serve clients and therefore does not handle their data egress.

References:

1. Cisco, FlexConnect Deployment Guide.
o Reference: In the "FlexConnect Modes of Operation" section, it states: "When the FlexConnect access point is connected to the controller, it can send traffic to the controller or switch it locally... In the locally switched mode, the data packets from the client are switched locally at the access point and are not sent to the controller."

o URL:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/85/config-guide/bcg85/flexconnect.html

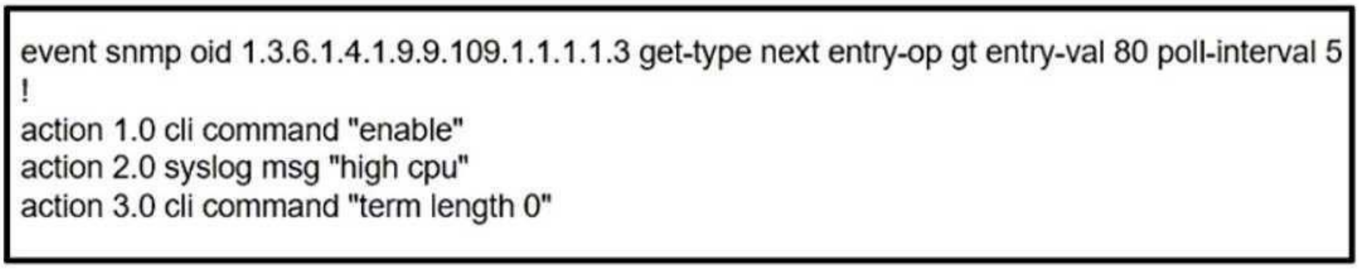
2. Cisco, Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x.

o Reference: Chapter: "Configuring Access Points," Section: "AP Modes." This guide details the different AP modes. For FlexConnect, it describes its ability to decide whether to switch traffic locally or send it to the controller. It describes Monitor mode for radio resource management and rogue detection, Bridge (Mesh) mode for point-to-point and point-to-multipoint bridging, and Sniffer mode for traffic analysis.

o URL:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/176/config-guide/bwl176cg/access
points.html

Question: 3

Refer to the exhibit.



```
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3 get-type next entry-op gt entry-val 80 poll-interval 5
!
action 1.0 cli command "enable"
action 2.0 syslog msg "high cpu"
action 3.0 cli command "term length 0"
```

An engineer must create a script that appends the output of the show process cpu sorted command to a file.

A. action 4.0 syslog command "show process cpu sorted append flash:high- cpu-file"

B. action 4.0 cli command "show process cpu sorted append flash:high-cpu- file"

C. action 4.0 ens-event "show process cpu sorted append flash:high-cpu- file"

D. action 4.0 publish-event "show process cpu sorted append flash:high- cpu-file"

Answer:

B

Explanation:

The question requires adding a command to a Cisco Embedded Event Manager (EEM) applet that executes a CLI command and appends its output to a file. The correct EEM action to execute any CLI command is cli command. The syntax show process cpu sorted append flash:high-cpu-file is the standard Cisco IOS method for taking the output of a show command and appending it to a file located in flash memory. Therefore, combining the EEM action with the IOS command gives the correct answer.

Why Incorrect Options are Wrong:

A. action 4.0 syslog command "...": This is incorrect. The syslog action is used to generate a syslog message (e.g., syslog msg "message text"). It does not have a command keyword and cannot execute CLI commands. C. action 4.0 ens-event "...": This is not a valid EEM action. The Event Notification System (ENS) is related to how EEM publishes events, but ens-event is not a keyword used to execute a CLI command within an applet action. D. action 4.0 publish-event "...": This action is used to publish an EEM event, which can be used to trigger another EEM applet. It does not execute a CLI command to capture output.

References:

1. Cisco Systems, "Embedded Event Manager (EEM) Configuration Guide, Cisco IOS Release 15M&T": This guide details the available EEM actions. It explicitly lists cli command as the action to execute a CLI command.

o Source: Cisco Official Documentation

o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/eem/configuration/15-mt/eem-15-mt-book/eem-policy-cli.html

o Specifics: See the "EEM Action CLI" section, which provides the syntax action label cli command "command".

2. Cisco Systems, "Cisco IOS Configuration Fundamentals Command Reference": This document describes I/O redirection using the pipe () character.

o Source: Cisco Official Documentation

o URL: https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cfbook/cfs1.html#wp1019253

o Specifics: The section "Using the Pipe Character" explains that append url appends the output of a command to a file at the specified URL (e.g., flash:filename).

Question: 4

What is the recommended minimum SNR for data applications on wireless networks?

A. 15

B. 20

C. 25

D. 10

Answer:

C

Explanation:

An SNR (Signal-to-Noise Ratio) of 25 dB is widely recommended as the minimum threshold for reliable performance of data applications over wireless networks. While basic connectivity might be possible at lower values, an SNR below 25 dB typically results in lower data rates, increased retransmissions, and a poor user experience. This value ensures that the received signal is sufficiently stronger than the background noise to support the higher Modulation and Coding Schemes (MCS) required for modern data-intensive applications.

Why Incorrect Options are Wrong:

A. 15 dB: An SNR of 15 dB is generally considered poor and would only support the lowest data rates with significant performance issues and instability. It is not a recommended minimum for reliable data services. B. 20 dB: While some sources may consider 20 dB as a bare minimum for a low-grade data connection, it is not the standard recommendation for designing a reliable network capable of handling typical business or personal data applications. D. 10 dB: This SNR level is very low and would result in an unstable and practically unusable connection for any standard data application. The error rate would be extremely high.

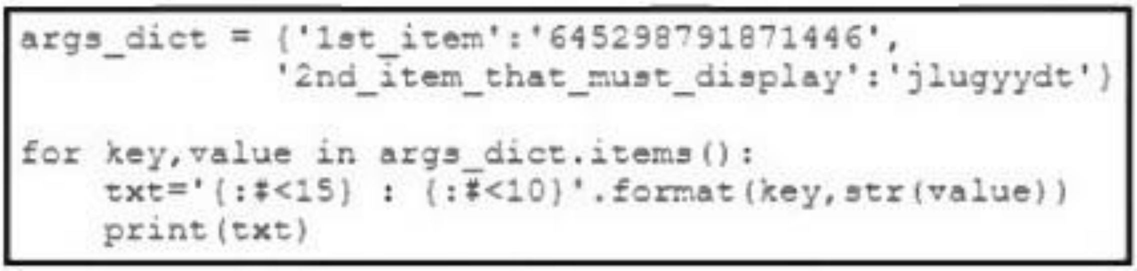
References:

1. Cisco Systems: The High Density Wi-Fi Design and Deployment Guide
explicitly states its design recommendation.
o Source: Cisco, "High Density Wi-Fi Design and Deployment Guide"
o Reference: In the "Design Recommendations" section, it is stated,
"A minimum SNR of 25 dB is recommended for data clients."
o URL:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/
8-5/bhighdensitywi-fidesignanddeploymentguide.html
2. HPE Aruba: Aruba's official documentation for validated reference designs
uses 25 dB as a key threshold for quality voice and data services.

o Source: Hewlett Packard Enterprise (Aruba), "Outdoor Wi-Fi 6 (802.11ax) Validated Reference Design Guide"
o Reference: Section 3.1, "RF Network Design," specifies that for optimal performance, "the SNR should be 25 dB or greater."
o URL: https://www.arubanetworks.com/assets/vrd/DGOutdoor-WiFi6.pdf
3. University Courseware (Carnegie Mellon University): Academic course material on wireless network design reinforces this industry standard.
o Source: Carnegie Mellon University, "Wireless Network Design" Course Material
o Reference: Lecture notes on WLAN Site Surveying and Design often present a table where an SNR of 25-39 dB is categorized as "Excellent" and required for high throughput data. An SNR of 20-24 dB is often labeled merely "Good."
o URL: General concepts are taught in courses like 14-840 at CMU's Information Networking Institute; specific public-facing lecture notes reflect these values.

Question: 5

Refer to the exhibit.



```
args_dict = {'1st_item':'645298791871446',
             '2nd_item_that_must_display':'jlugyydt'}

for key,value in args_dict.items():
    txt='{:#<15} : {:#<10}'.format(key,str(value))
    print(txt)
```

What is the output of this code?

A. 1stitem#######: 6452987918 2nditemthatm: jlugyydt##

B. 1stitem#######: 8791871446 atmustdisplay: jlugyydt

C. 1stitem#######: 645298791871446 2nditemthatmustdisplay: jlugyydt##

D. 645298791871446 ##jlugyydt

Answer:

C

Explanation:

The Python code iterates through a dictionary and prints each key-value pair using specific string formatting. The format string ':#15 : #10' dictates the output's appearance. The format specifier ":fillalignwidth" works as follows: • fill: The character to use for padding, which is # in this case. • align: The alignment of the text. specifies left-alignment. • width: The minimum width of the field. If the content is longer than the specified width, the field expands to fit the content; it does not truncate the string. Execution Analysis: 1. First Loop ('1stitem', '645298791871446'): o key: '1stitem' has 8 characters. The width is 15. It will be left- aligned and padded with 7 # characters: 1stitem#######. o value: '645298791871446' has 15 characters, which is longer than the minimum width of 10. The field expands to fit the entire string, so it prints 645298791871446. 2. Second Loop ('2nditemthatmustdisplay', 'jlugyydt'): o key: '2nditemthatmustdisplay' has 28 characters, which is longer than the minimum width of 15. The field expands to fit the entire key. o value: 'jlugyydt' has 8 characters. The width is 10. It will be left- aligned and padded with 2 # characters: jlugyydt##. This sequence of operations produces the output shown in option C.

Why Incorrect Options are Wrong:

A: This option is incorrect because it truncates the strings that are longer than the specified width. The width specifier sets a minimum size and does not cause truncation. B: This option is incorrect as it displays an entirely wrong value for the first key and an incorrect, truncated key for the second line. It also omits the required padding for the second value. D: This option is incorrect because it completely disregards the specified formatting structure, omitting the keys and the separating colon, and misplacing the padding.

References:

1. Python Software Foundation. (2025). Python 3.13.3 documentation, "string - Common string operations". This document details the str.format() method and its syntax.
o URL: https://docs.python.org/3/library/string.html#format-stringsyntax
2. Python Software Foundation. (2025). Python 3.13.3 documentation, "Format Specification Mini-Language". This section explicitly defines the width component.
o URL: https://docs.python.org/3/library/string.html#formatspec
o Reference: The documentation states: "The width is a decimal integer defining the minimum total field width. If not specified, then the field width will be determined by the content." This confirms that content longer than the width is not truncated.

Question: 6

Which unit of measure is used to measure wireless RF SNR?

A. mw

B. dbm

C. db

D. dBi

Answer:

C

Explanation:

The Signal-to-Noise Ratio (SNR) is a comparison between the power of a desired signal and the power of background noise. As it is a ratio of two power values (e.g., Psignal / Pnoise), the original units of power (like milliwatts) cancel out, making the ratio itself a dimensionless quantity. This dimensionless ratio is then expressed on a logarithmic scale using decibels (dB) for convenience in representing a wide range of values. Therefore, dB is the correct unit of measure for SNR.

Why Incorrect Options are Wrong:

A. mw: Milliwatts (mW) is a unit of absolute power. It can be used to measure the strength of the signal or the noise floor individually, but not their ratio. B. dbm: This is a unit of absolute power level, where the power is referenced to one milliwatt (0 dBm = 1 mW). It is commonly used to measure Received Signal Strength Indicator (RSSI), not a ratio like SNR. D. dBi: This unit measures the gain of an antenna relative to a theoretical isotropic antenna. It quantifies antenna performance (directivity), not the quality of a received signal versus noise.

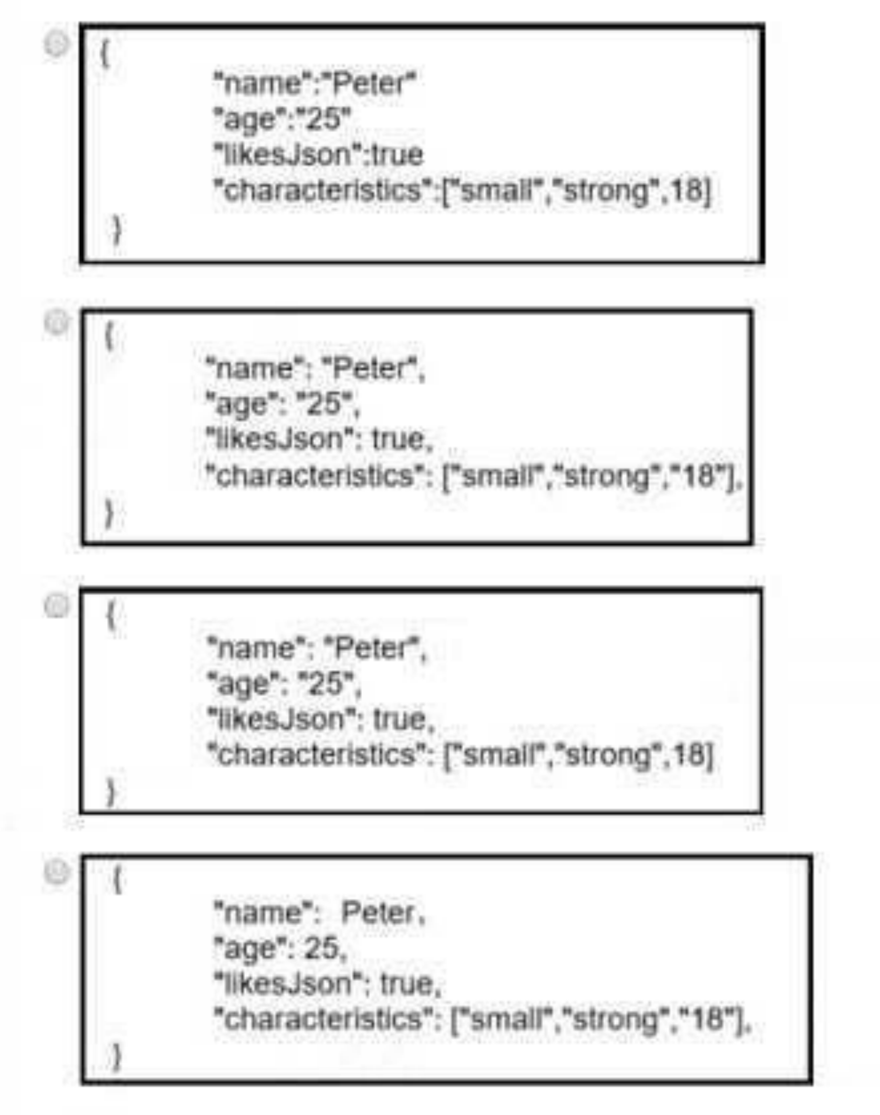
References:

1. Cisco, "Site Survey Guidelines for WLAN Deployment". This document states under the "Signal-to-Noise Ratio (SNR)" section, "SNR is measured in decibels (dB)."
o URL: https://www.cisco.com/c/en/us/support/docs/wireless/5508wireless-controller/116057-site-survey-guidelines-wlan-00.html#anc13
o Reference: Section: "Signal-to-Noise Ratio (SNR)".
2. IEEE Std 802.11-2020, "IEEE Standard for Information Technology...Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." Throughout the standard, receiver sensitivity requirements are specified in terms of a minimum required SNR expressed

in dB for different data rates.
o URL: https://ieeexplore.ieee.org/document/9363693
o Reference: Clause 19 (e.g., Table 19-21- Receiver minimum
sensitivity performance for EHT Preamble), specifies SNR in dB.
3. MIT OpenCourseWare, "6.450 Principles of Digital Communications I, Fall
2006." Lecture notes define SNR and its expression in decibels.
o URL:
https://ocw.mit.edu/courses/6-450-principles-of-digitalcommunications-i-fall-2006/resources/lec5/
o Reference: Lecture 5 Notes, Page 7, defines SNR as PS/N0 and its
decibel equivalent.

Question: 7

Which data is properly formatted with JSON?



○
```
{
        "name":"Peter"
        "age":"25"
        "likesJson":true
        "characteristics":["small","strong",18]
}
```

○
```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

○
```
{
        "name": "Peter",
        "age": "25",
        "likesJson": true,
        "characteristics": ["small","strong",18]
}
```

○
```
{
        "name":  Peter,
        "age": 25,
        "likesJson": true,
        "characteristics": ["small","strong","18"],
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer:

C

Explanation:

This option represents a correctly formatted JSON (JavaScript Object Notation) object. According to the IETF standard RFC 8259, a JSON object consists of key- value pairs. Keys must be strings enclosed in double quotes (e.g., "name"). Values can be a string, number, boolean, array, or another object. Each key- value pair is separated by a colon, and the pairs are separated from each other by commas. Option C correctly follows all these syntax rules without any extra or missing punctuation.

Why Incorrect Options are Wrong:

A: This option is incorrect because it is missing the required commas between the key-value pairs. The JSON standard requires a comma to separate each pair within an object. B: This option is incorrect because it includes a trailing comma after the last key-value pair. While some JavaScript interpreters might tolerate this, the official JSON grammar defined in RFC 8259 does not permit a comma after the final element in an object. D: This option is incorrect for two reasons. First, the string value Peter is not enclosed in double quotes, which is mandatory for all string values in JSON. Second, there is an extraneous period (.) after the closing bracket of the array, which is an invalid character in this context.

References:

1. Internet Engineering Task Force (IETF). RFC 8259: The JavaScript Object Notation (JSON) Data Interchange Format.

o URL: https://www.rfc-editor.org/rfc/rfc8259.html
o Details:

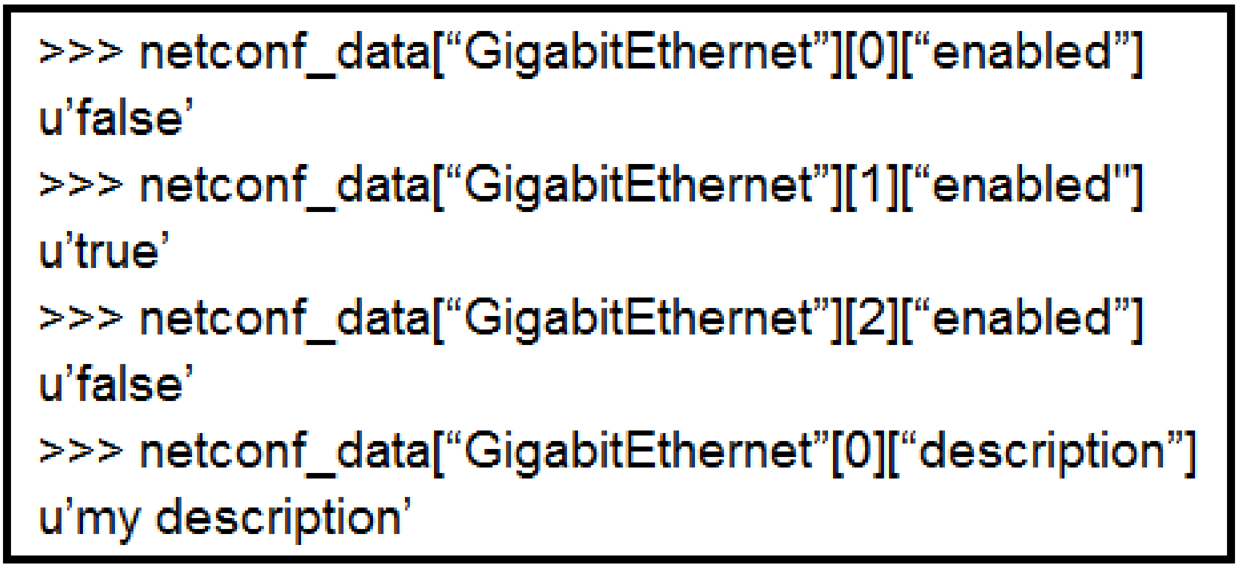
Section 2.2 (Objects): Defines the structure of a JSON object, stating, "A single comma separates a value from a following name." The grammar shown does not allow a trailing comma. This invalidates option B. It also confirms the need for commas between pairs, invalidating option A.

Section 7 (Strings): Defines the string data type, stating, "A JSON string begins and ends with quotation marks." This invalidates option D, where the value Peter is not quoted.
2. json.org. Introducing JSON.
o URL: https://www.json.org/json-en.html
o Details: The syntax diagrams on the official JSON website, maintained by its creator, visually confirm the required structure. The diagram for an object shows that pairs are separated by commas, but no comma follows the last pair. The diagram for a

string clearly shows the requirement for double quotes.

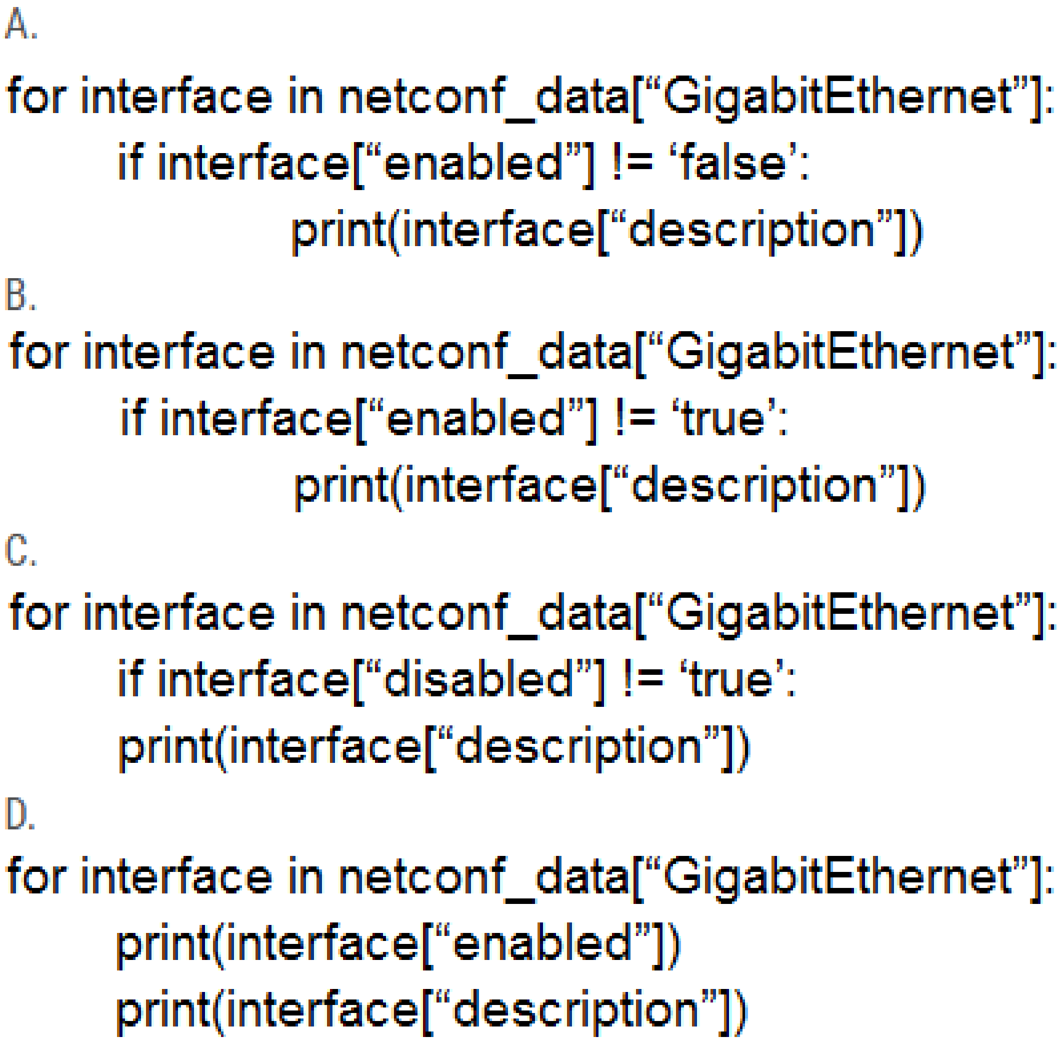
Question: 8

Refer to the exhibit.



```
>>> netconf_data[“GigabitEthernet”][0][“enabled”]
u’false’
>>> netconf_data[“GigabitEthernet”][1][“enabled”]
u’true’
>>> netconf_data[“GigabitEthernet”][2][“enabled”]
u’false’
>>> netconf_data[“GigabitEthernet”[0][“description”]
u’my description’
```

Which python code snippet prints the descriptions of disabled interface only?



A.

```
for interface in netconf_data[“GigabitEthernet”]:
        if interface[“enabled”] != ‘false’:
                print(interface[“description”])
```

B.

```
for interface in netconf_data[“GigabitEthernet”]:
        if interface[“enabled”] != ‘true’:
                print(interface[“description”])
```

C.

```
for interface in netconf_data[“GigabitEthernet”]:
        if interface[“disabled”] != ‘true’:
        print(interface[“description”])
```

D.

```
for interface in netconf_data[“GigabitEthernet”]:
        print(interface[“enabled”])
        print(interface[“description”])
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer:

B

Explanation:

The goal is to print the description for network interfaces that are disabled. According to the provided data exhibit, a disabled interface is represented by the key-value pair "enabled": 'false'. The Python code in option B correctly accomplishes this task. It iterates through each interface dictionary within the netconfdata"GigabitEthernet" list. For each interface, the if statement if interface"enabled" != 'true': evaluates whether the value of the "enabled" key is not equal to the string 'true'. This condition is met when the value is 'false', correctly identifying disabled interfaces. For those interfaces, it then prints the value of the "description" key.

Why Incorrect Options are Wrong:

A: This option checks if interface"enabled" is not equal to 'false' (!= 'false'). This logic is flawed because it would select interfaces that are enabled ('true') and print their descriptions, which is the opposite of the requirement. C: This code attempts to access a key named "disabled". Based on the provided data structure, this key does not exist; the correct key is "enabled". This would result in a KeyError when the program is run. D: This snippet iterates through all the interfaces and prints the "enabled" status and the "description" for every interface without any conditional filtering. It does not isolate and print descriptions for only the disabled interfaces.

References:

1. Python Software Foundation. "The for statement". The Python Tutorial.
This official documentation describes how for loops iterate over items of
any sequence, such as the list of dictionaries in the exhibit.
o URL: https://docs.python.org/3/tutorial/controlflow.html#forstatements
2. Python Software Foundation. "Mapping Types - dict". The Python
Standard Library. This source details how to access values in a dictionary
using a key, as seen with interface"enabled".
o URL: https://docs.python.org/3/library/stdtypes.html#mappingtypes-dict
3. Guttag,
J. V. (2016). Introduction to Computation and Programming Using
Python: With Application to Understanding Data. MIT Press. Chapter 3
discusses objects in Python, including dictionaries, and Chapter 4 covers
control flow, including conditional statements (if) and iteration. This
textbook affirms the fundamental logic used in the correct option.

Question: 9

An engineer must configure a new 6 Ghz only SSID on a cisco catalyst 9800 series WLC, with these requirements: Provide 802.11ax data rates for supported devices All users authenticate using a certificate Which wireless layer 2 security mode meets the requirements?

A. WPA2 Enterprise

B. WPA3 Personal

C. WPA2 Personal

D. WPA3 Enterprise

Answer:

D

Explanation:

The question requires a wireless security configuration for a 6 GHz only SSID that uses certificates for user authentication. 1. 6 GHz Band Requirement: Operation in the 6 GHz band (Wi-Fi 6E) mandates the use of WPA3 security. The Wi-Fi Alliance requires WPA3 for network access in the 6 GHz spectrum to ensure a higher, baseline level of security. This requirement immediately disqualifies options A (WPA2 Enterprise) and C (WPA2 Personal). 2. Certificate Authentication Requirement: The need for users to authenticate using a certificate points directly to an Enterprise security mode, which utilizes the IEEE 802.1X standard for authentication. This framework supports various Extensible Authentication Protocol (EAP) types, including EAP-TLS, which is used for certificate-based authentication. "Personal" modes rely on a pre-shared key (PSK) or Simultaneous Authentication of Equals (SAE), not individual user certificates. Therefore, WPA3 Enterprise is the only option that fulfills both the mandatory WPA3 security for the 6 GHz band and the certificate-based authentication requirement.

Why Incorrect Options are Wrong:

A. WPA2 Enterprise: While it supports certificate-based authentication via 802.1X, WPA2 does not meet the mandatory security requirement for operating a Wi-Fi network in the 6 GHz band. B. WPA3 Personal: This option uses SAE (Simultaneous Authentication of Equals) for password-based authentication. It does not support 802.1X or certificate-based authentication, failing to meet a key requirement of the scenario. C. WPA2 Personal: This option uses a pre-shared key (PSK) and does not support certificate-based authentication. Furthermore, like WPA2 Enterprise, it is not permitted for use in the 6 GHz band.

References:

1. Cisco Systems, "Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper":

o This document explicitly states the security requirement for the 6 GHz band. "The other significant change is that in the 6 GHz band, WPA3 is mandatory. Open authentication is also allowed for guest access, using Opportunistic Wireless Encryption (OWE)."

o URL: https://www.cisco.com/c/en/us/products/collateral/wireless/whitepaper-c11-744315.html

o Reference: See the "Security in the 6 GHz band" section.

2. Cisco Systems, "Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x":

o This guide details the configuration of Layer 2 security on Cisco WLCs. It shows that WPA3 is a configurable policy and that "WPA3 + 802.1x" (WPA3 Enterprise) is the option for using an AAA server and EAP methods for authentication.

o URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/176/config-guide/bwl176cg/mwpa3configguide.html

o Reference: Section "Configuring WPA3 Policy (GUI)".

3. Wi-Fi Alliance, "Wi-Fi CERTIFIED 6TM Release 2 adds new features for advanced Wi-Fi applications" (2022):

o This official press release from the body that certifies Wi-Fi standards reinforces the security foundation for 6 GHz. It mentions that Wi-Fi 6E, the industry name for Wi-Fi in 6 GHz, operates with a mandatory security level of WPA3.

o URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-certified-6release-2-adds-new-features-for-advanced-wi-fi-applications

o Reference: The document discusses how Wi-Fi 6E builds upon a foundation of WPA3 security.

Question: 10

An engineer measures the Wi-Fi coverage at a customer site. The RSSI values are recorded as follows: • LocationA -72dBm • Location B:-75 dBm • Location C; -65 dBm • Location D -80 dBm Which two statements does the engineer use to explain these values to the customer? (Choose two.)

A. The signal strength at location C is too weak to support web surfing

B. Location D has the strongest RF signal strength.

C. The RF signal strength at location B is 50% weaker than location A.

D. The RF signal strength at location C is 10 times stronger than location B

E. The signal strength at location B is 10 dB better than location C

Answer:

C, D

Explanation:

The question requires an understanding of how Wi-Fi signal strength is measured in decibels relative to one milliwatt (dBm). The dBm scale is logarithmic, not linear. Two key rules apply here: 1. The Rule of 3s: A change of 3 dB represents a doubling (for +3 dB) or halving (for -3 dB) of the signal power. 2. The Rule of 10s: A change of 10 dB represents a tenfold increase (for +10 dB) or decrease (for -10 dB) in signal power. Based on these rules: Correct Answer C: Location A is -72 dBm and Location B is -75 dBm. The difference is -3 dB, which means the signal power at Location B is half, or 50% weaker than, the signal power at Location A. • Correct Answer D: Location C is -65 dBm and Location B is -75 dBm. The difference is +10 dB, meaning the signal at Location C is ten times stronger than the signal at Location B.

Why Incorrect Options are Wrong:

A. The signal strength at location C is too weak to support web surfing. o This is incorrect. A signal of -65 dBm is considered good to excellent and is more than sufficient for basic web surfing and even for high-demand applications like voice and video streaming. A signal of -70 dBm is generally considered the minimum for reliable packet delivery. B. Location D has the strongest RF signal strength. o This is incorrect. On the dBm scale, values closer to 0 are stronger. Location C (-65 dBm) has the strongest signal, while Location D (-80 dBm) has the weakest signal. E. The signal strength at location B is 10 dB better than location C. o This is incorrect. "Better" means a stronger signal. Location C (-65 dBm) is stronger than Location B (-75 dBm). Therefore, the signal at Location C is 10 dB better than Location B, not the other way around.

References:

1. Cisco Systems, Inc. (2014). Radio Frequency (RF) Math. Cisco Press. In the section "The Power of dB," it states, "+3 dB = 2x Power," "-3 dB = 1/2x Power," "+10 dB = 10x Power," and "-10 dB = 1/10x Power."

o URL: https://www.cisco.com/c/en/us/support/docs/wireless/wirelesslan-wlan/21427-rf-math.html

o Section: "The Power of dB"

2. Cisco Meraki Documentation. 802.11 Wireless Signal Strength and Data Rates. This guide explains that an RSSI of -65 dBm is considered "Good" and suitable for "High-performance applications." It lists -70 dBm as acceptable for "Email and web."

o URL: https://documentation.meraki.com/MR/WiFiBasicsandBestPractices/802.11WirelessSignalStrength
andDataRates

o Section: "Received Signal Strength Indicator (RSSI)" table.

3. Massachusetts Institute of Technology (MIT) OpenCourseWare. (2011). 6.450 Principles of Digital Communications I, Lecture 2. The lecture notes discuss signal-to-noise ratio and the use of decibels for representing power ratios, illustrating the logarithmic nature of the scale.

o URL: https://ocw.mit.edu/courses/6-450-principles-of-digitalcommunications-i-fall-2006/resources/lecture-2-snr-capacity-and-
modulation/

o Reference: Discussion on decibels (dB) as a power ratio.

Question: 11

Which NGFW mode block flows crossing the firewall?

A. Passive

B. Tap

C. Inline tap

D. Inline

Answer:

D

Explanation:

An NGFW must be deployed inline to block traffic flows. In this mode, the firewall sits directly in the path of the network traffic, functioning like a "bump in the wire." This allows it to actively inspect all passing packets and enforce security policies by dropping or rejecting malicious or unauthorized traffic in real-time. Deployments that are not inline can only monitor and alert on traffic, not prevent it from reaching its destination.

Why Incorrect Options are Wrong:

A. Passive & B. Tap: These are functionally similar out-of-band modes. The NGFW connects to a switch's SPAN (Switched Port Analyzer) or a network TAP port, receiving a copy of the traffic. Since the firewall is not in the actual data path, it can only monitor, log, and generate alerts; it cannot block the live traffic flow. According to Palo Alto Networks documentation, "because the traffic is not running through the firewall when in tap mode it cannot take any action on the traffic, such as blocking." C. Inline tap: This is a specific mode, for example in Cisco Firepower, where the device is physically inline, but it inspects a copy of the traffic rather than the live flow. As a result, it can alert on threats but cannot drop them, behaving more like a passive device. While it can sometimes send TCP resets to disrupt sessions, the fundamental and universally recognized mode for actively blocking flows is the standard Inline mode.

References:

1. Palo Alto Networks, "Tap Interfaces," PAN-OS Networking
Administrator's Guide. States that in tap mode, the firewall "cannot take
any action on the traffic, such as blocking traffic with threats."
o URL: https://docs.paloaltonetworks.com/pan-os/11-0/pan-osnetworking-admin/configure-interfaces/tap-interfaces
2. Cisco, "Cisco Firepower Deployment Modes," RAYKA-CO. Explains that in
inline mode, the device is "physically inserted into the path, so all traffic is
forwarded through the Firepower IPS device." It contrasts this with passive

and inline tap modes, where "it is not possible to drop intrusions and they will be just alerted."

o URL: https://rayka-co.com/lesson/cisco-firepower-deploymentmodes/

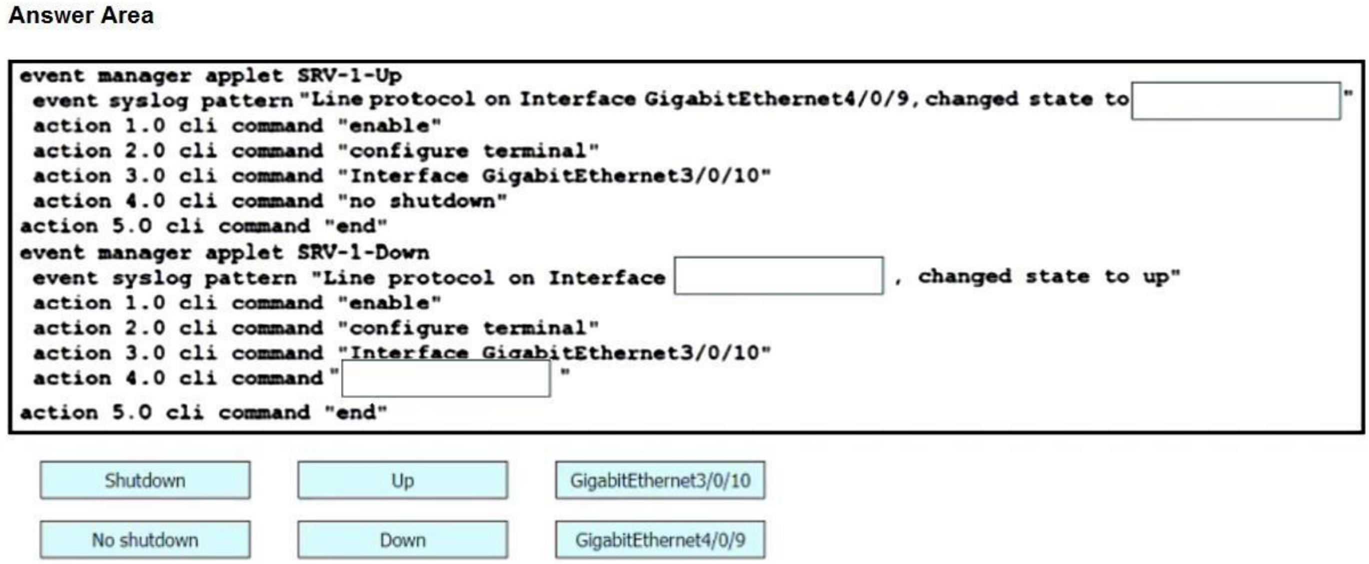
o Section: "Cisco Firepower Deployment Mode: IPS-only Inline Mode" & "Cisco Firepower Deployment Mode: IPS-only Inline Tap Mode"

3. Garland Technology, "What's Your Palo Alto NGFW Deployment Plan?," Blog. Clarifies the core requirement for blocking: "your Palo Alto Networks NGFW needs to be inline in order to block and prevent suspicious behavior."

o URL: https://www.garlandtechnology.com/blog/whats-your-palo-altongfw-deployment-plan

Question: 12

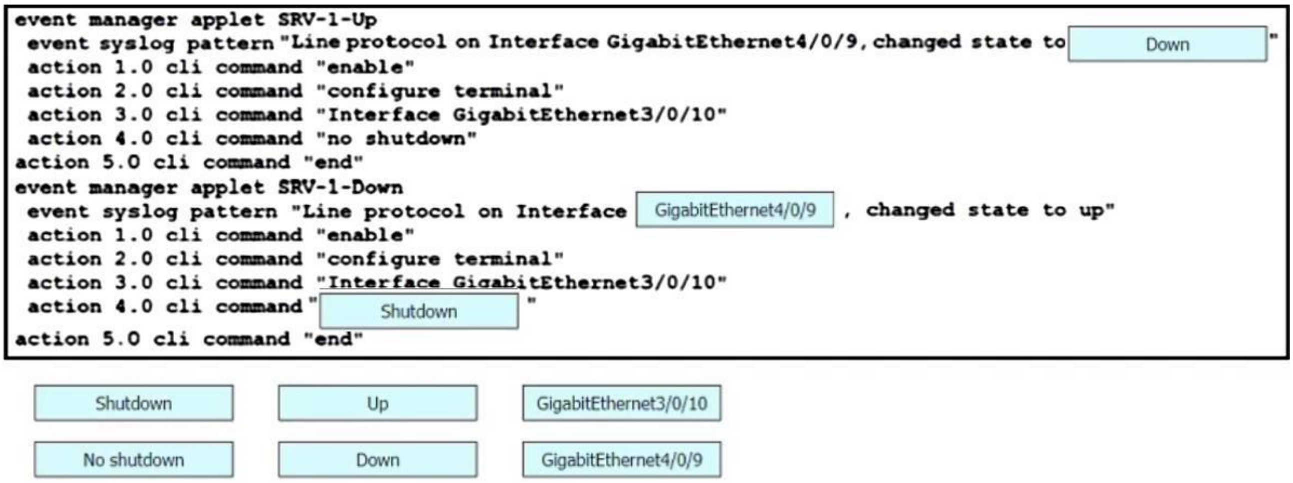
Drag and drop the snippets onto the blanks within the code to construct a script that brings up the failover Ethernet port if the primary port goes down and also shuts down the failover port when the primary returns to service. Not all options are used.



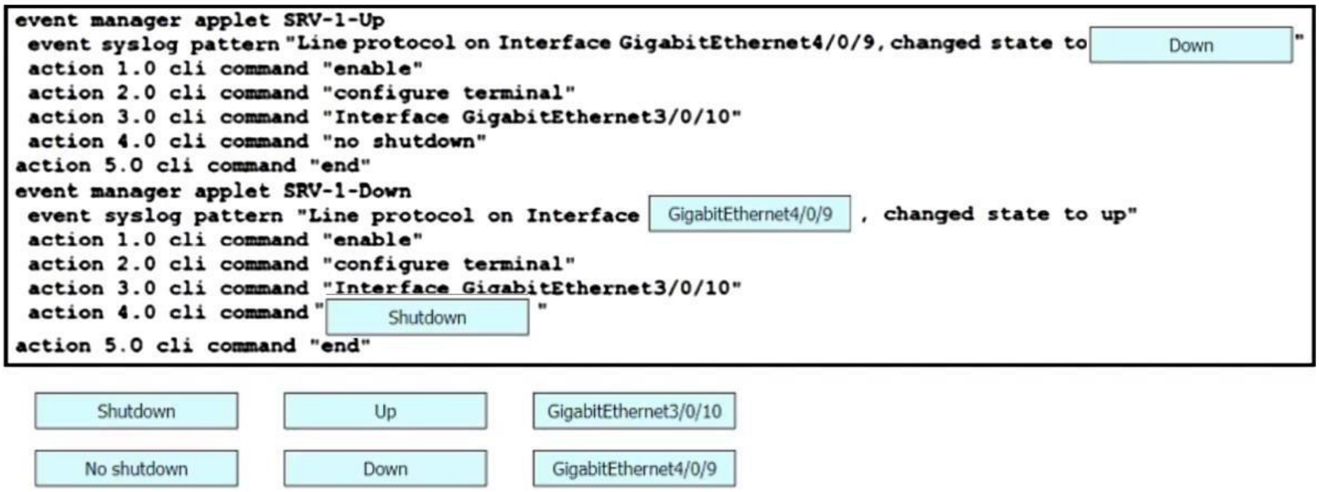
Answer Area

```
event manager applet SRV-1-Up
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to "
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
 event syslog pattern "Line protocol on Interface  , changed state to up"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command " "
action 5.0 cli command "end"
```

Answer:



```
event manager applet SRV-1-Up
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to Down"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9 , changed state to up"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "Shutdown "
action 5.0 cli command "end"
```



```
event manager applet SRV-1-Up
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9, changed state to Down "
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command "no shutdown"
action 5.0 cli command "end"
event manager applet SRV-1-Down
 event syslog pattern "Line protocol on Interface GigabitEthernet4/0/9 , changed state to up"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "Interface GigabitEthernet3/0/10"
 action 4.0 cli command " Shutdown "
action 5.0 cli command "end"
```

Explanation:

The logic hinges on interpreting the applet names (SRV-1-Up, SRV-1-Down) as referring to the action they perform on the backup link, not the event that triggers them. 1. SRV-1-Up Applet: o Action: The script for this applet is fixed to execute the no shutdown command on the backup interface (GigabitEthernet3/0/10). This action brings the backup link up. o Trigger: The action of bringing the backup link up is required when the primary link (GigabitEthernet4/0/9) goes down. o Conclusion: Therefore, the first blank must be filled with Down. 2. SRV-1-Down Applet: o Action: This applet's purpose must be the opposite: to take the backup link down. This requires the Shutdown command. o Conclusion: The third blank (the command) must be Shutdown. o Trigger: The backup link should be shut down when the primary link returns to service- that is, when it comes up. The trigger is correctly configured to detect a changed state to up. This trigger must monitor the primary interface. o Conclusion: The second blank (the interface) must be GigabitEthernet4/0/9.

References:

1. Cisco IOS Embedded Event Manager Configuration Guide: This guide
details the syntax and usage of EEM applets, including the event syslog
pattern trigger. It confirms that the pattern must match a specific syslog
message to trigger the defined actions.
o Source: Cisco, "Embedded Event Manager Configuration Guide,
Cisco IOS XE Gibraltar 16.12.x"
o URL:
https://www.cisco.com/c/en/us/td/docs/iosxml/ios/eem/configuration/16-12/eem-16-12-book.pdf
o Reference: See the chapter "Writing EEM Policies" and the section
on "Event 'syslog'".
2. Cisco EEM Scripting Examples: Cisco documentation and community

forums frequently show examples of using EEM for interface failover.
These examples consistently demonstrate a two-applet approach: one to react to the primary interface going down and another to react to it coming back up.

o Source: Cisco, "EEM Script to shut down backup interface when Primary comes up"

o URL: https://community.cisco.com/t5/network-management/eemscript-to-shut-down-backup-interface-when-primary-comes-up/td-p/2718105

o Reference: This Cisco Community discussion provides a script that validates the required logic: triggering on the primary interface's state changes (up/down) to modify the backup interface's state (shutdown/no shutdown).

Question: 13

Which two conditions occur when the primary route processor fails on a switch that is using dual route processors with stateful switchover? (Choose two.)

A. Data forwarding is stopped until the routing protocols reconverge after the switchover.

B. The standby route processor initialization is started when the primary router processor fails.

C. The standby route processor is fully initialed and state information is maintained.

D. User sessions are immediately recreated on the new active route processor.

E. Data forwarding can continue along known paths until routing protocol information is restored.

Answer:

C, E

Explanation:

Stateful Switchover (SSO) is a high-availability feature that synchronizes critical state information (like configuration and interface states) between a primary and a standby Route Processor (RP). This ensures the standby RP is fully initialized and ready to take over immediately if the primary fails, which directly aligns with option C. When paired with Nonstop Forwarding (NSF) or Graceful Restart, SSO allows the data plane to continue forwarding traffic along existing, known paths using the synchronized Forwarding Information Base (FIB). Meanwhile, the newly active RP rebuilds control plane information, such as routing protocol adjacencies, without interrupting packet flow. This process is accurately described in option E.

Why Incorrect Options are Wrong:

A. Data forwarding is stopped until the routing protocols reconverge after the switchover. This is incorrect. The primary purpose of SSO combined with NSF is specifically to prevent an interruption in data forwarding while the control plane reconverges. B. The standby route processor initialization is started when the primary router processor fails. This is incorrect. In an SSO-enabled system, the standby RP is kept in a "hot standby" state, meaning it is already fully booted, initialized, and synchronized before a failure occurs. D. User sessions are immediately recreated on the new active route processor. This is incorrect. The term "recreated" implies a loss of session state and a new beginning. SSO is designed to maintain sessions seamlessly by synchronizing their state information to the standby processor beforehand.

References:

1. Cisco Systems, "Stateful Switchover (SSO)" (Configuration Guide):
This document describes the core functionality of SSO. It states, "SSO
provides a higher level of availability...by synchronizing the network state

information between a primary and a standby Route Processor (RP)... This
synchronization allows the standby RP to take over immediately if the
primary RP fails." This validates option C.

o Source: Cisco IOS High Availability Configuration Guide

o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/ha/configuration/15-mt/ha-15-mt-book/ha-stateful-switchover.html (Refer to the "Stateful Switchover" and "Benefits of
SSO" sections).

2. Cisco Systems, "NSF/SSO--High Availability" (White Paper): This
paper clarifies the relationship between SSO and NSF. It explains that NSF
works with SSO to "continue forwarding data packets...while the routing
protocols on the redundant route processor converge." It further notes, "the
forwarding of data packets is not affected by the switchover." This directly
supports option E and refutes option A.

o Source: Cisco White Paper

o URL: https://www.cisco.com/c/en/us/support/docs/ios-nx-ossoftware/nonstop-forwarding-nsf/13627-nsfsso.html (Refer to the
"NSF Operation" section).

Question: 14

Which language can be used to model configuration and state data?

A. JSON

B. XML

C. XDR

D. YANG

Answer:

D

Explanation:

YANG (Yet Another Next Generation) is a data modeling language specifically designed to model the configuration and state data of network devices. It provides a standardized way to define the structure, constraints, and semantics of this data, which can then be manipulated by network management protocols like NETCONF and RESTCONF.

Why Incorrect Options are Wrong:

A. JSON: JSON (JavaScript Object Notation) is a lightweight data- interchange format. While data modeled by YANG can be represented in JSON, JSON itself is not the language used for creating the underlying model or schema. B. XML: XML (eXtensible Markup Language) is a markup language for encoding documents and data. Similar to JSON, it is a format used to carry the configuration data (e.g., in NETCONF operations), not the specialized language for modeling it. C. XDR: XDR (External Data Representation) is a standard for data serialization, primarily used in Remote Procedure Call (RPC) systems to exchange data between different computer architectures. It is not a language for modeling network configuration state.

References:

1. IETF RFC 7950: The YANG 1.1 Data Modeling Language.
o Quote/Paraphrase: The abstract explicitly states, "YANG is a data
modeling language used to model configuration data, state data,
Remote Procedure Calls (RPCs), and notifications for network
management protocols."
o Location: Abstract, Page 1.
o URL: https://www.rfc-editor.org/rfc/rfc7950.html
2. Cisco Systems, Inc.: YANG Data Modeling.
o Quote/Paraphrase: "YANG is a data modeling language that is
used to model the configuration and state of a network device."
o Location: "YANG Data Modeling" section.

o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/yang/configuration/16-8/ios-16-8-yang-cfg/yang-data-modeling.html

3. IETF RFC 8259: The JavaScript Object Notation (JSON) Data Interchange Format.

o Quote/Paraphrase: This document defines JSON's role as a "data interchange format," distinguishing it from a modeling language.

o Location: Abstract, Page 1.

o URL: https://www.rfc-editor.org/rfc/rfc8259.html

4. IETF RFC 4506: XDR: External Data Representation Standard.

o Quote/Paraphrase: This document defines XDR's purpose for "the description and encoding of data," primarily for RPCs, which is a different use case than modeling network configuration.

o Location: Abstract, Page 4.

o URL: https://www.rfc-editor.org/rfc/rfc4506.html

Question: 15

Which features does Cisco EDR use to provide threat detection and response protection?

A. containment, threat intelligence, and machine learning

B. firewalling and intrusion prevention

C. container-based agents

D. cloud analysts and endpoint firewall controls

Answer:

A

Explanation:

Cisco's Endpoint Detection and Response (EDR) solution, now known as Cisco Secure Endpoint, integrates multiple advanced capabilities to protect endpoints. Its core functionality relies on a combination of machine learning and behavioral analytics to detect unknown threats, leveraging threat intelligence from Cisco Talos for comprehensive threat awareness. A critical response feature is the ability to contain or isolate a compromised endpoint, preventing the threat from spreading across the network while allowing for further investigation. These three elements machine learning, threat intelligence, and containment are fundamental to its detection and response framework.

Why Incorrect Options are Wrong:

B. firewalling and intrusion prevention: These terms primarily describe network security functions, characteristic of Next-Generation Firewalls (NGFW) and Intrusion Prevention Systems (IPS), not the core features of an endpoint-centric EDR solution. C. container-based agents: This describes a potential deployment architecture for the agent, not a core security feature for threat detection or response. The agent's capabilities, not how it's packaged, are the key features. D. cloud analysts and endpoint firewall controls: "Cloud analysts" refers to a managed service (MDR) that uses the EDR tool, not a feature of the tool itself. While endpoint firewall control can be part of a larger security suite, it is not a defining feature of EDR's advanced detection and response cycle.

References:

1. Cisco, "Cisco Secure Endpoint Data Sheet": This document explicitly
details the product's features. It mentions "Advanced Endpoint Detection
and Response," "Machine Learning," "Cisco Talos threat intelligence," and
"Host Isolation" (containment).
o Source URL:
https://www.cisco.com/c/en/us/products/collateral/security/amp-forendpoints/datasheet-c78-745509.html

o Specific Sections: See sections "Advanced Endpoint Detection and Response" and the features table which lists "Machine learning analysis" and "Isolate an endpoint".

2. Cisco, "What Is Endpoint Detection and Response (EDR)?": This page defines EDR and highlights its key components, including threat hunting, behavioral protection, and response capabilities like isolation. It reinforces the concepts of advanced analysis (machine learning) and the use of threat intelligence.

o Source URL:
https://www.cisco.com/c/en/us/products/security/endpointsecurity/what-is-endpoint-detection-and-response-edr.html

o Specific Sections: See paragraphs under "How does EDR work?" and "Key capabilities of an EDR solution."

Question: 16

What does the LAP send when multiple WLCs respond to the CISCO-CAPWAP-CONTROLLER.localdomain hostname during the CAPWAP discovery and join process?

A. broadcast discover request

B. join request to all the WLCs

C. unicast discovery request to each WLC

D. Unicast discovery request to the first WLS that resolves the domain name

Answer:

C

Explanation:

When a Lightweight Access Point (AP) boots up, it initiates a discovery process to find a Wireless LAN Controller (WLC). One of the methods used is DNS resolution. The AP will attempt to resolve the hostname CISCO-CAPWAP- CONTROLLER.localdomain. If the DNS server returns one or more IP addresses for this hostname, the AP will send a unicast CAPWAP Discovery Request message to each IP address it receives. It does not stop after the first one, nor does it immediately send a join request. A broadcast request is a different step in the discovery process and is not a response to a successful DNS lookup.

Why Incorrect Options are Wrong:

A. broadcast discover request: A broadcast discovery is a separate method sent to the local subnet (255.255.255.255). It is not initiated as a result of a successful DNS resolution for a specific controller hostname. B. join request to all the WLCs: An AP sends a Join Request only after it has received a Discovery Response from a WLC and has selected a controller to join. The initial contact after DNS resolution is a Discovery Request. D. Unicast discovery request to the first WLS that resolves the domain name: This is incorrect because the AP will send a discovery request to all IP addresses returned by the DNS server for the controller hostname, not just the first one, to ensure it discovers all available controllers.

References:

1. Cisco, "Wireless LAN Controller (WLC) Discovery and Join Process,"
Document ID: 107606.
o This document outlines the AP discovery process. In the "WLC
Discovery on a Layer 3 Network" section, step 4 explicitly states:
"The APs can discover controllers through your domain name
server (DNS)... The AP sends a unicast CAPWAP discovery request

to every address."

o URL: https://www.cisco.com/c/en/us/support/docs/wireless/4400series-wireless-lan-controllers/107606-wlc-lap.html (Under the section "WLC Discovery on a Layer 3 Network")

2. Cisco, "Deploying the Cisco 5760 Wireless LAN Controller," Release 3.6E.

o In the "Information About AP-Controller Communication" chapter, the section "How the Access Point Finds the Controller" details the DNS discovery method: "If the DNS returns a list of controller IP addresses, the access point sends a unicast discovery request to each controller on the list."

o URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/5760/software/release/36e/configurationguide/bcg36e/bcg36echapter0101111.html (Under the section "How the Access Point Finds the Controller")

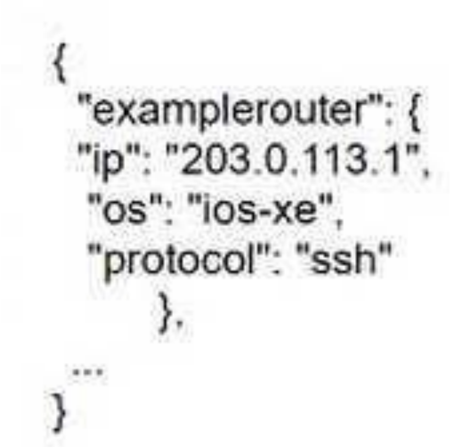
3. Cisco, "Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)," Document ID: 70333.

o This guide reinforces the discovery steps. The "LAP States" section explains that discovery precedes the join state. The "DNS Discovery" part clarifies that the AP resolves CISCO-CAPWAP-CONTROLLER.localdomain and sends discovery messages to the resulting IP addresses.

o URL: https://www.cisco.com/c/en/us/support/docs/wireless/wirelesslan-controller-wlc/70333-lap-registration.html (Under the section "DNS Discovery")

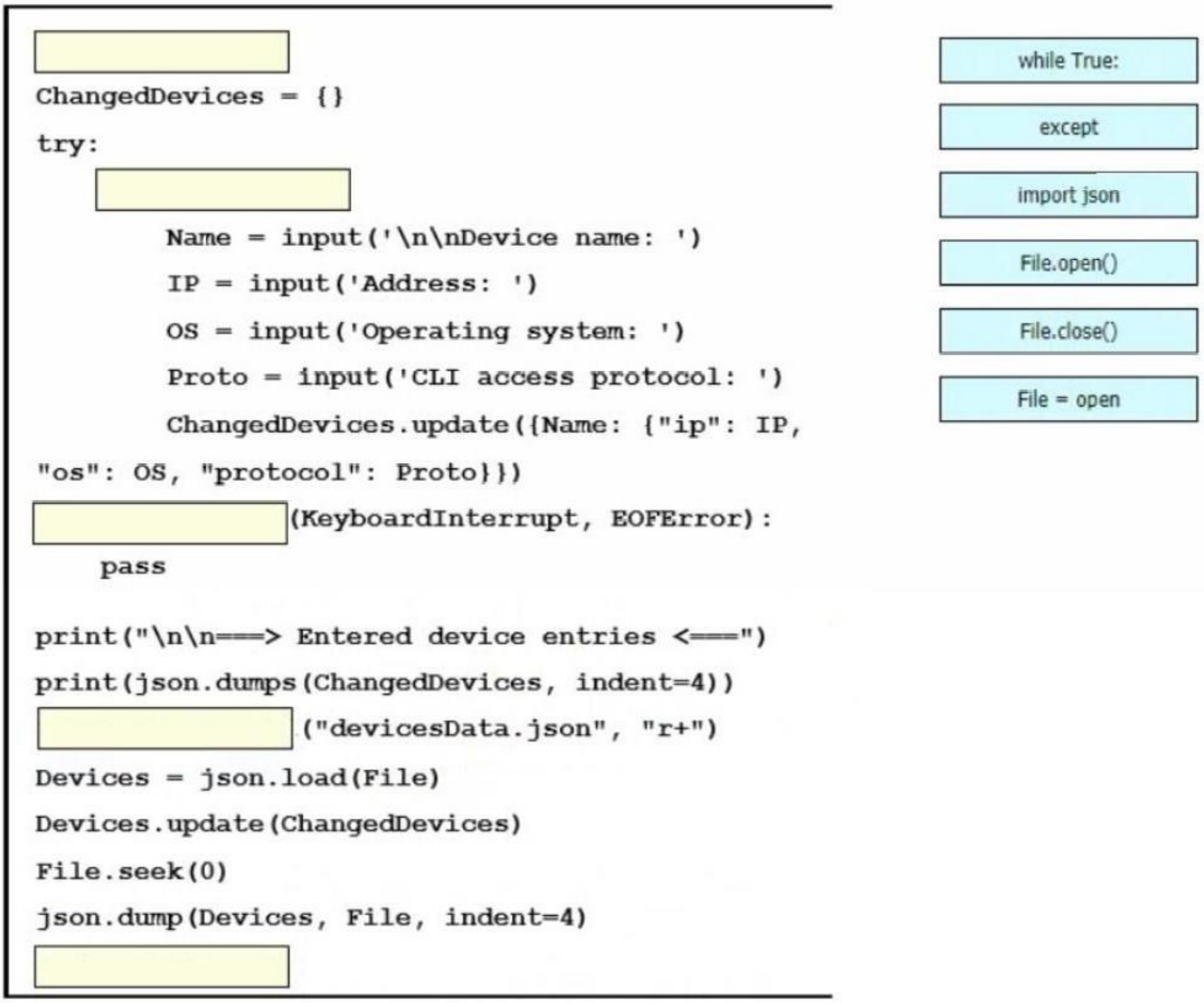
Question: 17

DRAG DROP An engineer must create a script to append and modify device entries in a JSON-formatted file. The script must work as follows: Until interrupted from the keyboard, the script reads in the hostname of a device, its management IP address, operating system type, and CLI remote access protocol. After being interrupted, the script displays the entered entries and adds them to the JSON-formatted file, replacing existing entries whose hostname matches. The contents of the JSON-formatted file are as follows



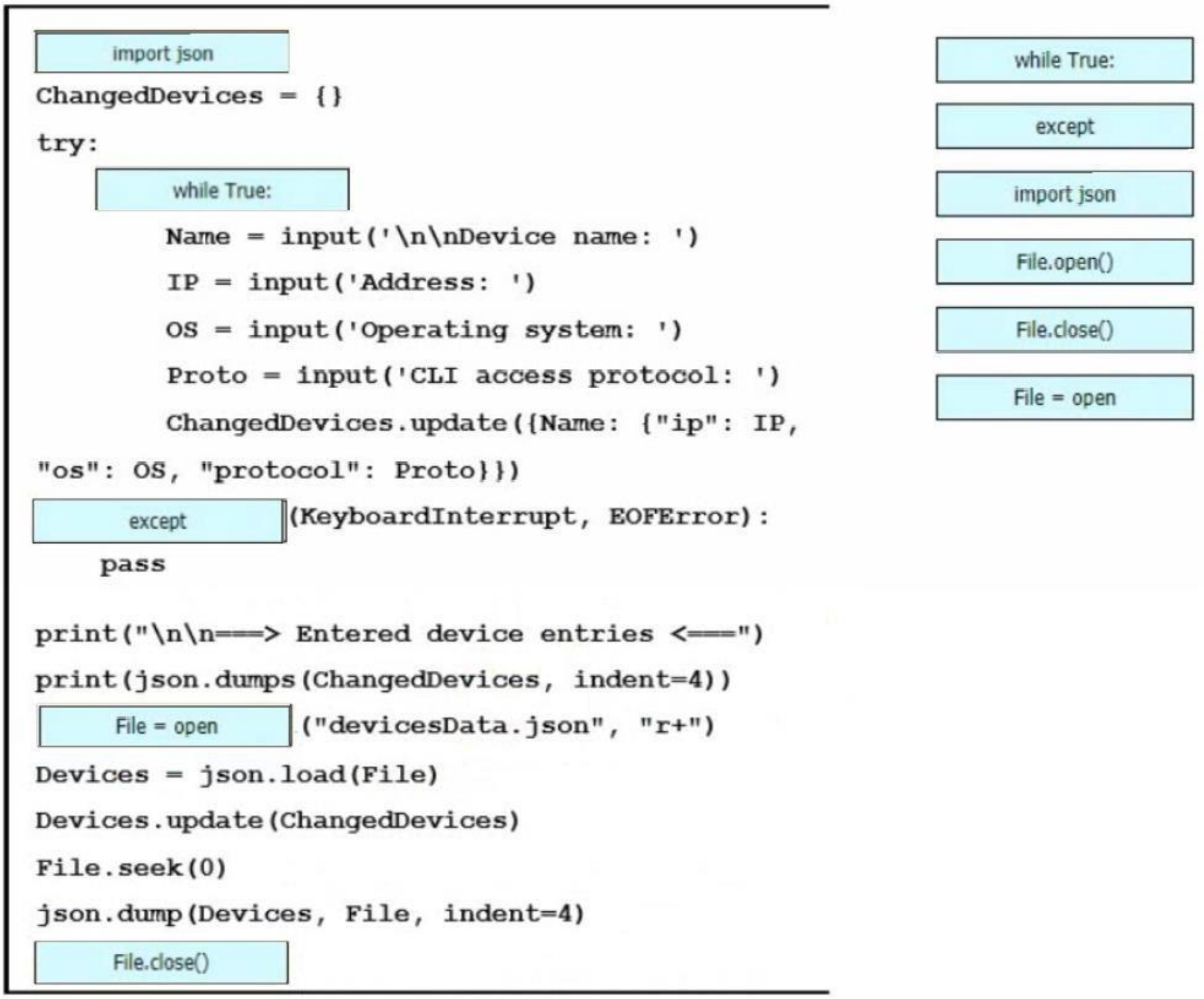
```
{
  "examplerouter": {
  "ip": "203.0.113.1",
   "os": "ios-xe",
   "protocol": "ssh"
        },
   ...
}
```

Drag and drop the statements onto the blanks within the code to complete the script. Not all options are used.

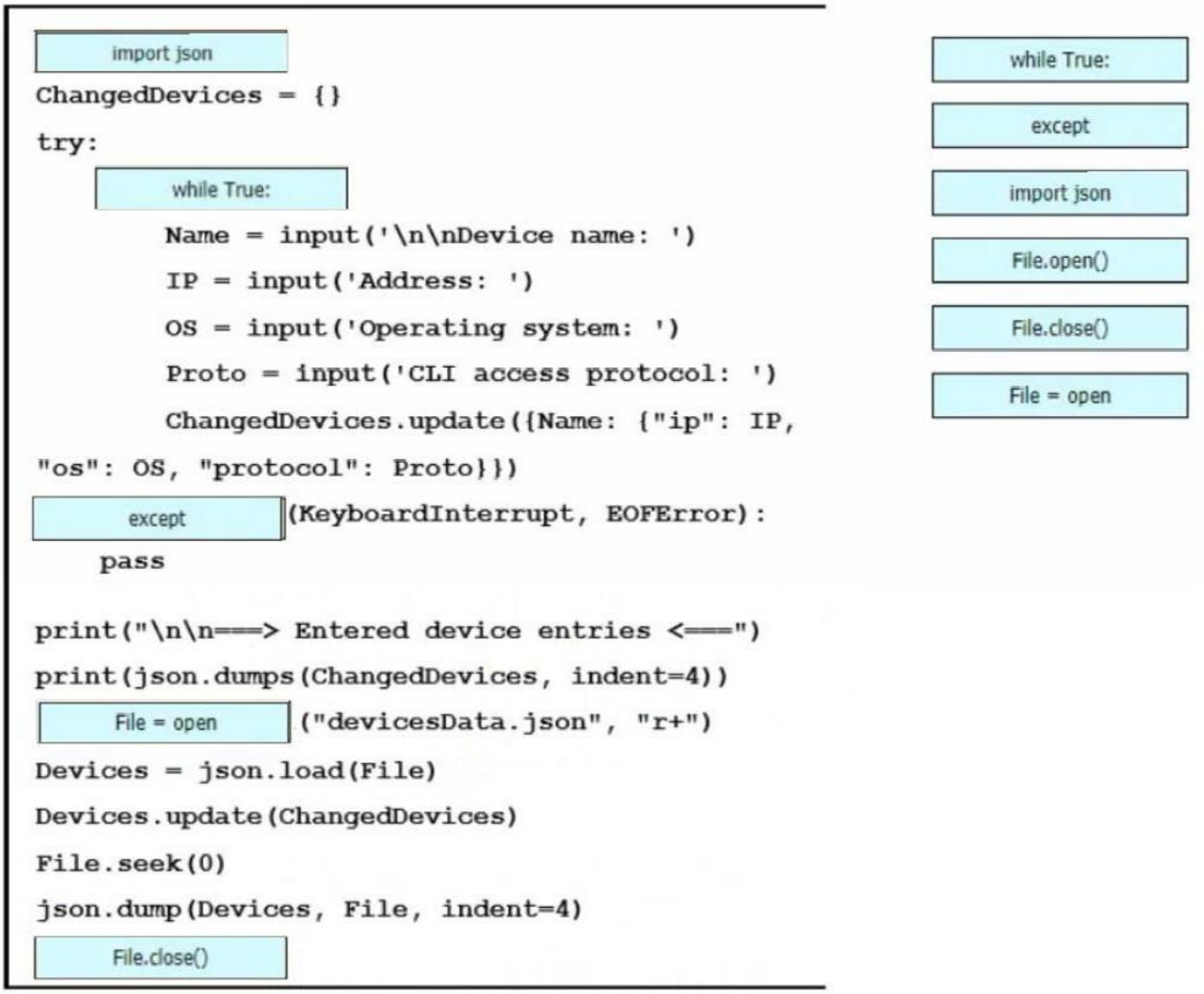


```

ChangedDevices = {}
try:

        Name = input('\n\nDevice name: ')
        IP = input('Address: ')
        OS = input('Operating system: ')
        Proto = input('CLI access protocol: ')
        ChangedDevices.update({Name: {"ip": IP,
"os": OS, "protocol": Proto}})
               (KeyboardInterrupt, EOFError):
    pass

print("\n\n===> Entered device entries <===")
print(json.dumps(ChangedDevices, indent=4))
                ("devicesData.json", "r+")
Devices = json.load(File)
Devices.update(ChangedDevices)
File.seek(0)
json.dump(Devices, File, indent=4)

```

Answer:



```
import json
ChangedDevices = {}
try:
    while True:
        Name = input('\n\nDevice name: ')
        IP = input('Address: ')
        OS = input('Operating system: ')
        Proto = input('CLI access protocol: ')
        ChangedDevices.update({Name: {"ip": IP,
"os": OS, "protocol": Proto}})
except (KeyboardInterrupt, EOFError):
    pass

print("\n\n==> Entered device entries <==")
print(json.dumps(ChangedDevices, indent=4))
File = open ("devicesData.json", "r+")
Devices = json.load(File)
Devices.update(ChangedDevices)
File.seek(0)
json.dump(Devices, File, indent=4)
File.close()
```



```
import json
ChangedDevices = {}
try:
    while True:
        Name = input('\n\nDevice name: ')
        IP = input('Address: ')
        OS = input('Operating system: ')
        Proto = input('CLI access protocol: ')
        ChangedDevices.update({Name: {"ip": IP,
"os": OS, "protocol": Proto}})
except (KeyboardInterrupt, EOFError):
    pass

print("\n\n===> Entered device entries <===")
print(json.dumps(ChangedDevices, indent=4))
File = open ("devicesData.json", "r+")
Devices = json.load(File)
Devices.update(ChangedDevices)
File.seek(0)
json.dump(Devices, File, indent=4)
File.close()
```

while True:

except

import json

File.open()

File.close()

File = open

Explanation:

The objective is to complete a Python script that reads device data from a user and updates a JSON file. The provided code snippets correctly fill the blanks to achieve the required functionality based on standard Python syntax and library usage. • import json: This statement is placed at the top to import the necessary json module. This module provides the json.load() and json.dump() functions used later in the script to parse and write JSON data. • while True:: This creates an infinite loop, satisfying the requirement that the script should continue to read user input "Until interrupted from the keyboard." except: This keyword is required to begin the exception handling block. It catches the KeyboardInterrupt (e.g., from pressing Ctrl+C) or EOFError (e.g., from pressing Ctrl+D), which is the designated signal to stop gathering input. File = open: This statement correctly opens the specified file, devicesData.json, in "r+" mode (read and write) and assigns the file object to the variable File. This is necessary to both read the existing device data and write the updated data back. File.close(): This statement is placed at the end to close the file. It is a crucial best practice to release the file resource after all operations are complete, ensuring data integrity and preventing resource leaks.

References:

1. Python json Module Documentation: The official documentation details the functions json.load() for reading from a JSON file and json.dump() for writing to one.

o Source: Python Software Foundation, Python 3.12.3 documentation.

o URL: https://docs.python.org/3/library/json.html (See sections 19.2.1. Basic Usage)

2. Python Control Flow Statements: The while statement and try...except compound statements are fundamental control flow structures in Python. The documentation specifies their syntax and usage.

o Source: Python Software Foundation, Python 3.12.3 documentation.

o URL: https://docs.python.org/3/tutorial/controlflow.html#morecontrol-flow-tools (for loops) and https://docs.python.org/3/tutorial/errors.html#handling-exceptions (for try...except).

3. Python File I/O: The official tutorial explains the use of the open() function for file access, the different modes like "r+", and the importance of the .close() method.

o Source: Python Software Foundation, Python 3.12.3 documentation.

o URL: https://docs.python.org/3/tutorial/inputoutput.html#readingand-writing-files (See section 7.2).

Question: 18

Which solution simplifies management of secure access to network resources?

A. TrustSec to logically group internal user environments and assign policies

B. ISE to automate network access control leveraging RADIUS AV pairs

C. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs

D. 802 1AE to secure communication in the network domain

Answer:

A

Explanation:

The question asks for a solution that simplifies the management of secure network access. Cisco TrustSec is the most precise answer because it is an architecture specifically designed to achieve this simplification. TrustSec decouples network access from IP addresses by classifying endpoints into logical groups (roles) and assigning them Security Group Tags (SGTs). Policies are then defined based on these role-based SGTs (e.g., "Doctors can access Patient Records"), which is significantly simpler to manage than creating and maintaining thousands of IP-based Access Control Lists (ACLs). This logical grouping is the core mechanism of simplification.

Why Incorrect Options are Wrong:

B. ISE to automate network access control leveraging RADIUS AV pairs This is incorrect because while the Cisco Identity Services Engine (ISE) is the central policy engine that implements the TrustSec architecture, TrustSec is the actual framework that provides the simplification through logical grouping. This option describes the tool, whereas option A describes the architectural solution that achieves the goal. C. RFC 3580-based solution to enable authenticated access leveraging RADIUS and AV pairs This is incorrect as RFC 3580 is a standard that provides guidelines for using RADIUS with IEEE 802.1X. It is a foundational protocol specification, not a comprehensive solution designed to simplify policy management across an enterprise. D. 802 1AE to secure communication in the network domain This is incorrect because IEEE 802.1AE, also known as MACsec, is a standard for Layer 2 data encryption. It ensures data confidentiality and integrity on a wired network but does not provide a framework for simplifying user and device access policy management.

References:

1. Cisco Systems, "Cisco TrustSec Solution Design Guide": "Cisco
TrustSec technology provides a new paradigm for secure networking,
simplifying the provisioning and management of network access...
The goal of the Cisco TrustSec solution is to assign a Security Group Tag

(SGT) to a user/device... This simplifies policy management by reducing the number of access control entries."
o Source URL:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec/2-1/TS2-1DG/tsd2-1overview.html
o Section: "Cisco TrustSec Solution Overview"
2. Cisco Systems, "TrustSec Security Group Tagging Design and Implementation Guide": "The goal of the TrustSec solution is to assign a Security Group Tag (SGT) to a user/device when it connects to the network... This SGT is then used as a source and destination in the access policies... This simplifies policy management by reducing the number of access control entries that would have been required if using IP addresses."
o Source URL:
https://www.cisco.com/c/en/us/support/docs/security/trustsec/116132-config-sgt-00.html
o Section: "Introduction"
3. IETF, RFC 3580, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines": This document describes the use of RADIUS in conjunction with IEEE 802.1X authenticators, focusing on protocol attributes and behavior. It is a technical specification, not a management solution.

o Source URL: https://datatracker.ietf.org/doc/html/rfc3580
o Section: Abstract
4. IEEE Standards Association, "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security": This standard specifies the provision of connectionless user data confidentiality, data integrity, and data origin authenticity. Its focus is on Layer 2 encryption.
o Source URL: https://standards.ieee.org/ieee/802.1AE/3439/
o Identifier: IEEE Std 802.1AETM -2006

Question: 19

In which forms can Cisco Catalyst SD-WAN routers be deployed at the perimeter of a site to provide SD-WAN services?

A. virtualized instances

B. hardware, software, cloud, and virtualized instances

C. hardware, virtualized. and cloud instances

D. hardware and virtualized instances

Answer:

C

Explanation:

Cisco Catalyst SD-WAN routers, which function as the data plane or "WAN Edge" devices in the architecture, can be deployed in multiple form factors to fit various site requirements. These include hardware appliances for physical locations like branches and data centers, virtualized instances that can run on standard hypervisors or enterprise network virtualization platforms, and as instances within public cloud infrastructures like AWS, Azure, and Google Cloud to extend the SD-WAN fabric to cloud workloads. This flexibility allows for a consistent SD-WAN policy and architecture across a hybrid environment of physical, virtual, and cloud-based resources.

Why Incorrect Options are Wrong:

A. virtualized instances: This option is incorrect because it is incomplete. It omits the very common hardware appliance and cloud deployment models. B. hardware, software, cloud, and virtualized instances: This option is less precise than C. In this context, a "virtualized instance" is the "software" form factor. The term "virtualized" is more specific to the deployment model, distinguishing it from a physical appliance. Including both is redundant. D. hardware and virtualized instances: This option is incorrect because it is incomplete. It fails to include the crucial capability of deploying SD- WAN routers directly within public cloud environments, a key feature known as Cloud OnRamp.

References:

1. Cisco Catalyst 8000V Edge Software Data Sheet: This document explicitly states that the Catalyst 8000V is a "virtual-form-factor router" that can be deployed in "virtual and cloud environments." It lists supported hypervisors (VMware ESXi, KVM) for on-premises virtualization and public clouds (Amazon EC2, Microsoft Azure, Google Cloud Platform) as deployment locations.
o Source: Cisco, "Cisco Catalyst 8000V Edge Software Data Sheet"

o URL:
https://www.cisco.com/c/en/us/products/collateral/routers/catalyst8000v-edge-software/nb-06-cat8000v-edge-sw-data-sheet-ctp-
en.html (Refer to "Product overview" and "Benefits" sections).

2. Cisco SD-WAN Solution Overview: This document describes the "endpoint flexibility" of the solution, covering physical platforms for branches, aggregation sites, and virtual platforms. It explicitly mentions extending the SD-WAN fabric to "data centers, branches, campuses, colocation facilities, and clouds."

o Source: Cisco, "Cisco SD-WAN Solution Overview"

o URL: https://fe5e0932bbdbee188a67ade54de1bba9a4fe61c120942a09245b.ssl.cf1.rackcdn.com/nb-06-
sd-wan-sol-overview-cte-en.pdf (Refer to Page 4, "Endpoint flexibility" and Figure 8, "Cisco SD-WAN portfolio").

3. Cisco SD-WAN Cloud OnRamp for IaaS White Paper: This paper details the process of extending the enterprise WAN to public clouds by deploying virtual SD-WAN routers within the cloud provider's infrastructure. It confirms the "cloud" deployment model for edge devices.

o Source: Cisco, "Cisco SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) White Paper"

o URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprisenetworks/sd-wan/white-paper-c11-743126.html (Refer to the "Introduction" and "Solution" sections).

Question: 20

Which feature is needed to maintain the IP address of a client when an inter- controller Layer 3 roam is performed between two WLCs that are using different mobility groups?

A. interface groups

B. RF groups

C. AAA override

D. auto anchor

Answer:

D

Explanation:

Auto anchor, also known as Mobility Anchor, is the feature specifically designed to ensure a wireless client maintains its original IP address when performing a Layer 3 roam between controllers, particularly when they are in different mobility groups. When a client roams to a new "foreign" controller, the foreign controller establishes an Ethernet-over-IP (EoIP) tunnel back to the client's original "anchor" controller. All of the client's traffic is sent through this tunnel to the anchor, from which it enters the wired network. This makes the client's physical location transparent and preserves its IP address, ensuring seamless session continuity.

Why Incorrect Options are Wrong:

A. interface groups: This feature is used on a single WLC to load-balance clients across a group of VLANs (interfaces). It does not provide the tunneling mechanism required for maintaining an IP address during an inter-controller roam. B. RF groups: This feature, also known as an RF domain, is used for coordinating Radio Resource Management (RRM) algorithms among a group of controllers. It manages radio settings like channel and power, and is unrelated to client IP address management during roaming. C. AAA override: This allows a RADIUS server to dynamically assign specific attributes, such as a VLAN ID, to a client upon authentication. It does not provide a mechanism to maintain that client's IP address when it roams to a different controller and subnet.

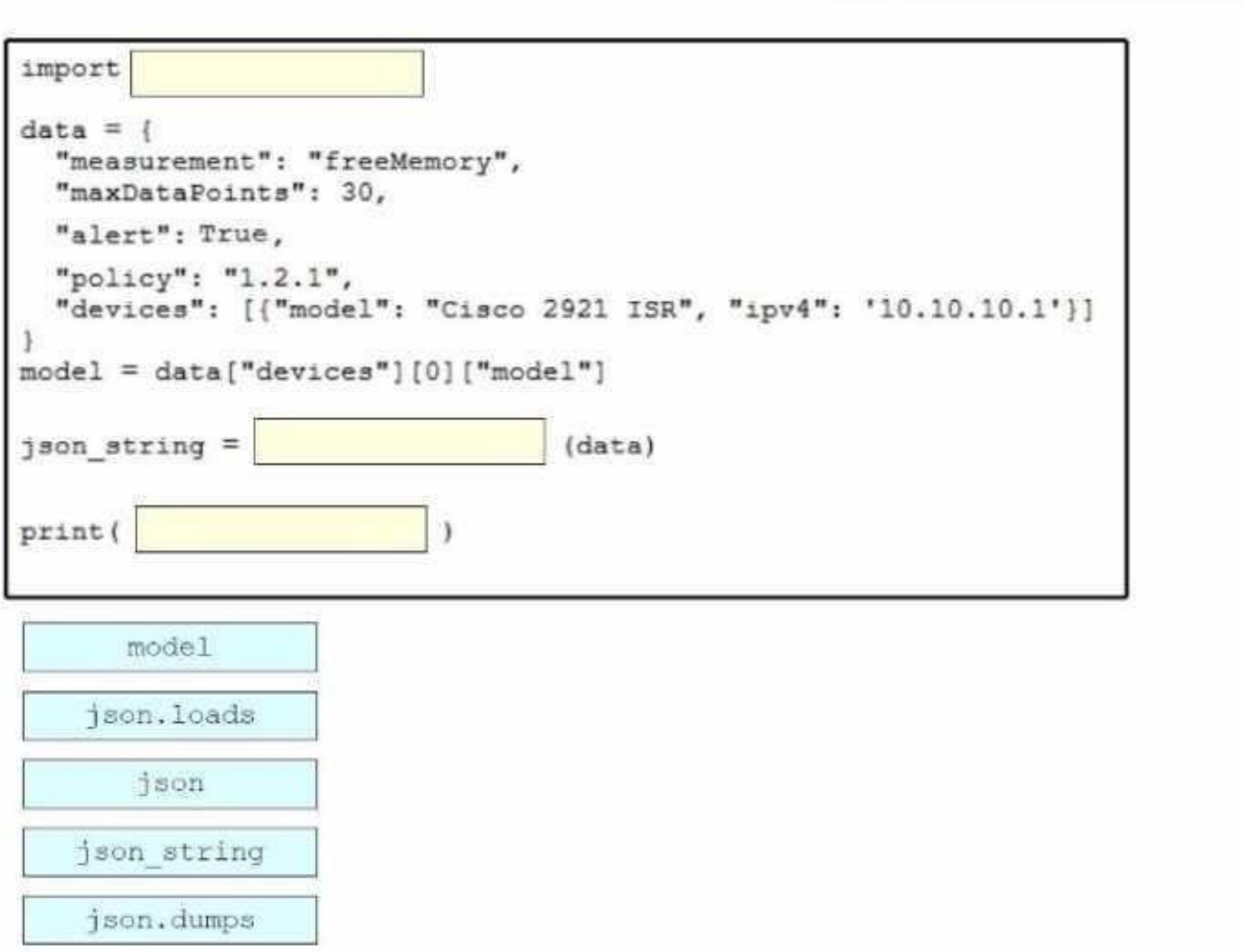
References:

1. Cisco, "Enterprise Mobility 8.5 Design Guide"
o Details: In the "Mobility Architecture" chapter, the "Mobility Anchor" section states: "Mobility anchoring, also known as guest tunneling, is a feature where a controller is designated as the anchor point for a particular WLAN... All client traffic is tunneled from the foreign controller to the anchor controller over a Layer 3 tunnel (Ethernet-

over-IP). This allows a client to maintain its IP address when
roaming between controllers." It also notes this is useful for roaming
between different mobility groups.
o URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/85/Enterprise-Mobility-8-5-Design-Guide/EnterpriseMobility8-5DeploymentGuide/ch3mobilityarch.html#Ref518882092
2. Cisco, "Wireless Controller Configuration Guide, Release 8.10"
o Details: In the "Configuring Mobility Groups" chapter, the section
"Information About Mobility Anchor" explains: "In a mobility anchor
setup, a client can roam to any controller in the mobility list, but its
point of presence on the wired network is always the anchor
controller... This feature is also referred to as 'guest tunneling' or
'auto anchoring'."
o URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/810/config-guide/bcg810/configuringmobilitygroups.html#ID347

Question: 21

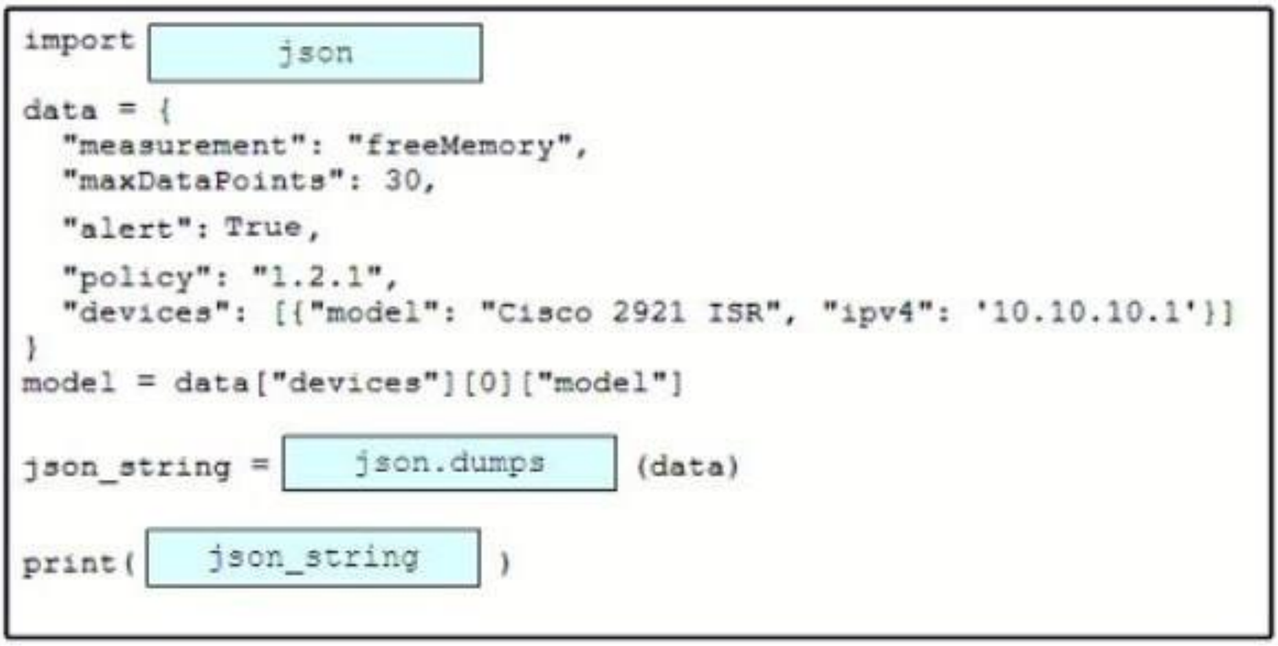
Drag and drop the code snippets from the bottom onto the blanks in the Python script to convert a Python object into a JSON string. Not all options are used.



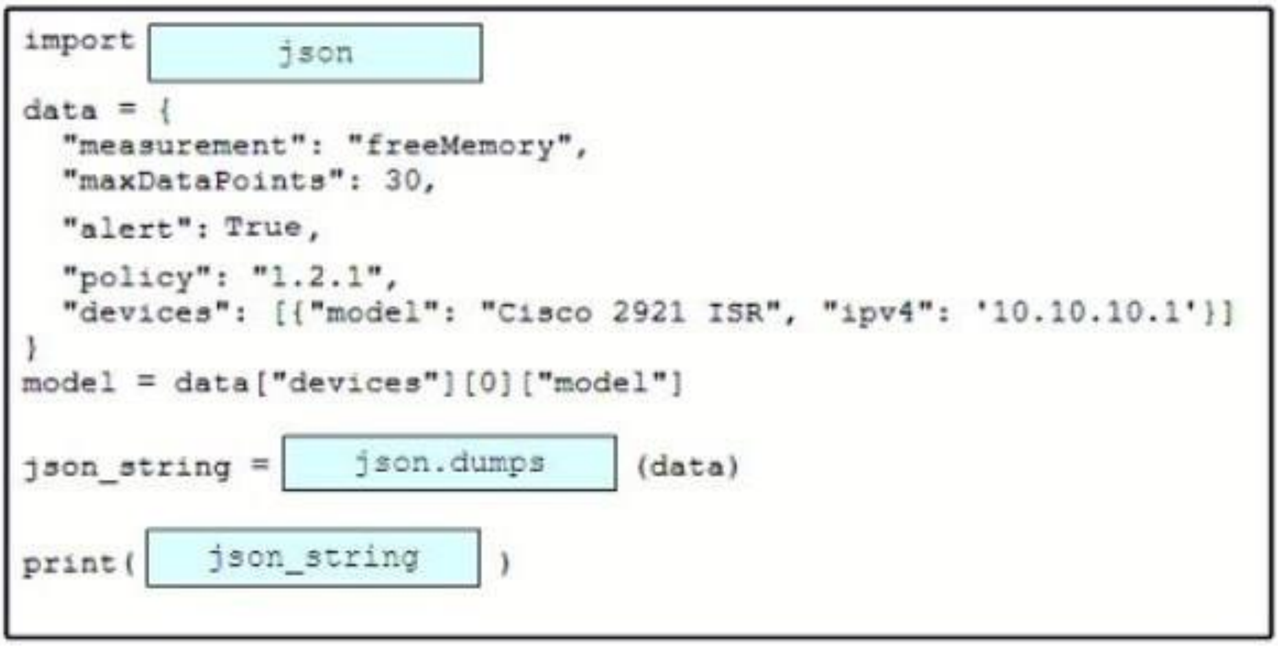
```
import

data = {
   "measurement": "freeMemory",
   "maxDataPoints": 30,
   "alert": True,
   "policy": "1.2.1",
   "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string =                 (data)

print(                 )
```

```
model
json.loads
json
json_string
json.dumps
```

Answer:



```
import json
data = {
  "measurement": "freeMemory",
  "maxDataPoints": 30,
  "alert": True,
  "policy": "1.2.1",
  "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string = json.dumps (data)

print( json_string )
```



```
import json
data = {
  "measurement": "freeMemory",
  "maxDataPoints": 30,
  "alert": True,
  "policy": "1.2.1",
  "devices": [{"model": "Cisco 2921 ISR", "ipv4": '10.10.10.1'}]
}
model = data["devices"][0]["model"]

json_string = json.dumps (data)

print( json_string )
```

Explanation:

The Python script requires three parts to correctly serialize a Python dictionary into a JSON formatted string and print it. 1. import json: The first blank requires importing Python's built-in json module, which provides the necessary tools for working with JSON data. 2. jsonstring = json.dumps(data): The second blank uses the json.dumps() function to perform the conversion. This function takes a Python object (the data dictionary) and returns it as a JSON formatted string. This string is then assigned to the jsonstring variable. 3. print(jsonstring): The third blank prints the value of the jsonstring variable, which now holds the JSON representation of the original Python object.

References:

Python Software Foundation. (2025). json - JSON encoder and
decoder. Python 3.13.3 documentation. This official documentation states,
"To use this module, import json" and describes the json.dumps() function
as the method to "serialize obj to a JSON formatted str".
o URL: https://docs.python.org/3/library/json.html#basic-usage
Guttag,
J. V. (2016). Lecture 10: Files. 6.0001 Introduction to Computer
Science and Programming in Python, Fall 2016. Massachusetts Institute of
Technology: MIT OpenCourseWare. The principles of handling different
data formats like JSON are covered in university-level computer science
introductions.
o URL: https://ocw.mit.edu/courses/6-0001-introduction-to-computerscience-and-programming-in-python-fall-2016/resources/lecture-10-
files/

Question: 22

What is one benefit of adopting a data modeling language?

A. deploying machine-friendly codes to manage a high number of devices

B. augmenting the use of management protocols like SNMP for status subscriptions

C. augmenting management process using vendor centric actions around models

D. refactoring vendor and platform specific configurations with widely compatible configurations

Answer:

D

Explanation:

A primary benefit of a data modeling language, such as YANG, is to create a standardized, vendor-neutral definition for the configuration and state data of network devices. This allows for the abstraction of device management away from proprietary, vendor-specific command-line interfaces (CLIs) or APIs. By using these common models, organizations can create configurations and automation workflows that are "widely compatible" across different hardware platforms and vendors, effectively refactoring what would otherwise be platform-specific code. This approach simplifies network automation and management at scale.

Why Incorrect Options are Wrong:

A: This is imprecise. The data model itself is a definition, not a "machine- friendly code" that is deployed. It defines the structure for management protocols to use, enabling machine-to-machine communication for management, but the core benefit is the standardization it provides. B: This is misleading. While data models describe device status, modern management protocols that use them (like NETCONF and RESTCONF) are often positioned as more capable alternatives to SNMP for configuration, not merely as augmentations for its subscription features. C: This is incorrect. The fundamental purpose of adopting a standardized data modeling language is to move away from vendor-centric models and operations toward a common, interoperable framework, thereby reducing vendor lock-in.

References:

1. IETF RFC 7950: The YANG 1.1 Data Modeling Language:
o Quote/Concept: "YANG is a data modeling language used to model configuration data, state data, Remote Procedure Calls (RPCs), and notifications for network management protocols... This allows a clean separation between the data models and the management protocols..."
o Location: Abstract, Page 4.

o URL: https://www.rfc-editor.org/rfc/rfc7950.html

2. Cisco IOS XE Programmability Configuration Guide:

o Quote/Concept: "YANG is a standards-based, data modeling language that is used to model the configuration and operational state of a network device. The use of a standards-based model provides a vendor-neutral way of programming a network device and helps in managing a multivendor network."

o Location: Chapter: "YANG Data Models".

o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/prog/configuration/1612/b1612progconfigguide/yangd
atamodels.html

3. IETF RFC 8340: YANG Tree Diagrams:

o Quote/Concept: "A YANG data model defines a hierarchy of data that can be used for configuration, to report operational state, and for invoking operations on network devices... The YANG language... is protocol independent." This independence is key to creating compatible configurations across different platforms.

o Location: Section 1: Introduction, Paragraph 1.

o URL: https://www.rfc-editor.org/rfc/rfc8340.html

Question: 23

What occurs during a Layer 2 inter-controller roam?

A. A new security context is applied for each controller to which the client is associated, but the IP address remains the same.

B. The client must be associated to a new controller where a new IP address and security context are applied.

C. The client retains the same IP address and security context.

D. The client is marked as foreign in the database of each new controller to which it is connected.

Answer:

C

Explanation:

During a Layer 2 inter-controller roam, the primary goal is to maintain a seamless connection for the client device. This is achieved by ensuring the client retains its original IP address, as the roam occurs within the same subnet (Layer 2 domain). Furthermore, to avoid disrupting the session and forcing a full re-authentication, the client's security context (which includes security keys and authentication status) is transferred from the original "anchor" controller to the new "foreign" controller. This allows the client to continue communicating securely without interruption.

Why Incorrect Options are Wrong:

A. A new security context is applied for each controller to which the client is associated, but the IP address remains the same. This is incorrect because applying a new security context would require a full re- authentication, which seamless roaming protocols (like 802.11r) are designed to avoid. The existing context is transferred, not replaced. B. The client must be associated to a new controller where a new IP address and security context are applied. This is incorrect as it describes a Layer 3 roam. A defining characteristic of a Layer 2 roam is that the client keeps the same IP address. D. The client is marked as foreign in the database of each new controller to which it is connected. While it is true that the new controller is termed the "foreign" controller and maintains a "foreign" entry for the client, this is an architectural detail of how the roam is managed. Option C more accurately and completely describes the primary outcome and experience for the client's session, which is the core of the roaming event itself.

References:

1. Cisco, Enterprise Mobility 8.5 Design Guide. This guide details the mobility architecture. It states, "In the case of inter-controller L2 roam, the client maintains its IP address... The WLCs exchange mobility messages and the client database entry is moved from the anchor WLC to the foreign

WLC. This includes the security context of the client."
o Source: Cisco, "Enterprise Mobility 8.5 Design Guide", Chapter: Mobility Architecture. (A specific URL is difficult as these guides are updated, but the concept is fundamental in all versions of the Cisco Wireless LAN Controller Design Guides). A representative document is available at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/85/Enterprise-Mobility-8-5-Design-Guide/EnterpriseMobility8-5DeploymentGuide.html, see the "Inter-Controller Roaming" section.

2. IEEE Std 802.11TM -2020, IEEE Standard for Information Technology-Telecommunications and information exchange between systems Local and metropolitan area networks- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. The mechanisms for Fast BSS Transition (FT), defined in section 12.5, are designed to allow a station (client) to quickly transition between access points while maintaining security and connectivity. This involves transferring security key information, thus preserving the security context.
o Source: IEEE Std 802.11TM -2020, DOI:

10.1109/IEEESTD.2021.9363693, Section 12.5 "Fast BSS transition".

Question: 24

A wireless network engineer must configure a WPA2+WPA3 policy with the Personal security type. Which action meets this requirement?

A. Configure the GCMP256 encryption cipher.

B. Configure the CCMP128 encryption cipher.

C. Configure the GCMP128 encryption cipher.

D. Configure the CCMP256 encryption cipher.

Answer:

B

Explanation:

Configuring a wireless network for WPA2+WPA3 transition mode (also called mixed mode) requires enabling cipher suites that are compatible with both WPA2 and WPA3 clients. According to the IEEE 802.11-2020 standard and Wi- Fi Alliance specifications, CCMP-128 (Counter Mode Cipher Block Chaining Message Authentication Code Protocol with a 128-bit key) is the mandatory cipher for WPA2-Personal. For WPA3-Personal, CCMP-128 is also a mandatory baseline cipher, even though stronger optional ciphers exist. Therefore, to ensure that both WPA2 and WPA3 clients can connect to the same SSID, the network must be configured to use CCMP-128. This allows WPA2 clients to connect using PSK and WPA3 clients to connect using SAE, both leveraging the common CCMP-128 cipher.

Why Incorrect Options are Wrong:

A. Configure the GCMP256 encryption cipher: GCMP-256 is an optional, stronger cipher for WPA3 and is not supported by WPA2 clients. Configuring only this would prevent WPA2 clients from connecting, defeating the purpose of a mixed-mode policy. C. Configure the GCMP128 encryption cipher: GCMP-128 is defined as an optional cipher suite for use with WPA3, particularly for management frames, but it is not the standard data encryption cipher for WPA2. Relying on it would not guarantee compatibility. D. Configure the CCMP256 encryption cipher: This cipher suite does not exist within the context of the IEEE 802.11 standard for WPA2 or WPA3 security. The standard specifies CCMP with a 128-bit key (CCMP- 128) and GCMP with a 256-bit key (GCMP-256).

References:

1. Wi-Fi Alliance, "Wi-Fi CERTIFIED WPA3TM Specification," Version 3.1,
January 2023.
o Section 3.2.1 (Cipher Suites): This section specifies that for
WPA3-Personal, the mandatory cipher suite is CCMP-128. It also

lists GCMP-256 as optional. For a mixed WPA2-WPA3 mode, the AP must support the mandatory cipher suites for both security protocols.

o URL: https://www.wi-fi.org/file/wi-fi-certified-wpa3-specification-v3-1

2. IEEE Standard for Information Technology- Telecommunications and information exchange between systems Local and metropolitan area networks- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11TM -2020.

o Section 12.7.2 (Cipher suites): This section details the valid cipher suites. It defines "CCMP-128" for use in Robust Security Network Associations (RSNAs), which is the foundation for WPA2 and WPA3. The standard mandates CCMP-128 for RSN-capable stations.

o DOI: https://doi.org/10.1109/IEEESTD.2021.9363693

3. Cisco, "WPA3 Deployment Guide," December 19, 2022.

o Section: WPA3 Transition Mode (WPA3-Personal): The guide explicitly states, "The WPA3 transition mode enables a graceful migration from WPA2 to WPA3... The AP broadcasts a single SSID that both WPA2 and WPA3 capable clients can use to connect. The mandatory cipher for WPA2 is AES/CCMP128... WPA3 also mandates the use of AES/CCMP128 cipher."

o URL:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/173/config-guide/bcg98001731book/wpa3deploymentguide.html

Question: 25

Which feature allows HSRP to failover from the active route processor to the standby route processor without loss of data or path change?

A. preemption

B. IP SLA tracking

C. stateful switchover

D. HSRP tracking

Answer:

C

Explanation:

Stateful Switchover (SSO) is the correct feature that allows for a seamless transition between a failed active route processor (RP) and a standby RP within the same chassis. SSO synchronizes critical state information (e.g., protocol states, session data) between the two RPs. If the active RP fails, the standby RP can take over immediately without losing data or requiring network protocols like HSRP to reconverge. This maintains the forwarding path and makes the switchover transparent to adjacent network devices.

Why Incorrect Options are Wrong:

A. Preemption: This is an HSRP setting that allows a router with a higher priority to forcibly take over the active role from a currently active router with a lower priority. It does not relate to the failover between route processors within a single device. B. IP SLA tracking: This mechanism is used to monitor the reachability of a specific IP address or path. It can trigger an HSRP failover to a different router if the tracked object becomes unavailable, but it is not the mechanism for an intra-chassis RP failover. D. HSRP tracking: This feature monitors the state of a router's interface. If the tracked interface goes down, the router's HSRP priority is reduced, potentially causing a failover to a separate standby router. This is distinct from an internal RP switchover.

References:

1. Cisco Systems, Inc., "High Availability Configuration Guide, Cisco IOS XE
Bengaluru 17.6.x (Catalyst 9500 Switches)." This guide defines SSO as
the feature that monitors the active RP and switches to the standby RP
upon a fault. It explicitly states, "SSO, in conjunction with NSF (Nonstop
Forwarding), ensures that data traffic is not interrupted during a
switchover."
o Source: Cisco High Availability Configuration Guide
o Section: "Stateful Switchover (SSO)"

2. Cisco Systems, Inc., "IP Application Services Configuration Guide, Cisco IOS Release 15M&T." This document details HSRP features. It describes preemption and tracking as mechanisms that influence which router in an HSRP group becomes active, differentiating them from intra-chassis redundancy.
o Source: Cisco IP Application Services Configuration Guide
o Sections: "HSRP Preemption" and "HSRP Interface Tracking".

Question: 26

What is a characteristic of Layer 3 roaming?

A. Clients must obtain a new IP address when they roam between APs.

B. It provides seamless roaming between APs that are connected to different Layer 3 networks and different mobility groups.

C. It is only supported on controllers that run SSO.

D. It provides seamless client roaming between APs in different Layer 3 networks but within the same mobility group.

Answer:

D

Explanation:

Layer 3 roaming is specifically designed to allow a wireless client to move between Access Points (APs) that are managed by different controllers and are on different IP subnets, without losing its original IP address. This process is managed within a pre-configured mobility group (also known as a mobility domain). The controllers within this group share client security and session context, allowing the new (foreign) controller to tunnel the client's traffic back to the original (anchor) controller. This ensures session persistence for the client.

Why Incorrect Options are Wrong:

A. Clients must obtain a new IP address when they roam between APs. This is incorrect. The primary goal of Layer 3 roaming is to preserve the client's original IP address to prevent the disruption of applications and sessions. The tunneling mechanism makes the subnet change transparent to the client device. B. It provides seamless roaming between APs that are connected to different Layer 3 networks and different mobility groups. This is incorrect. Standard Layer 3 roaming operates within a single mobility group. Roaming between different mobility groups is a more complex process, often called inter-mobility group roaming, and is not the defining characteristic of standard Layer 3 roaming. C. It is only supported on controllers that run SSO. This is incorrect. Stateful Switchover (SSO) is a high-availability feature that provides controller redundancy. Layer 3 roaming is a mobility function that can operate independently of SSO. A single controller can support Layer 3 roaming between APs on different subnets connected to it.

References:

1. Cisco, Enterprise Mobility 8.5 Design Guide. "A mobility group is a group of controllers that have established a dynamic and trusted relationship with each other, which allows them to share context and state about clients, and to forward data traffic on behalf of clients that are

roaming between APs that are associated to different controllers... When a client roams between APs that are joined to different controllers, and the client WLAN is on different VLANs/subnets, the client traffic is tunneled between the two controllers... This process is transparent to the wireless client, and the client maintains its original IP address."

o Source URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/85/Enterprise-Mobility-8-5-Design-Guide/EnterpriseMobility8-5DeploymentGuide/ch3mobilityarchitecture.html(https://www.google.com/search?q=https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/EnterpriseMobility8-5DeploymentGuide/ch3mobilityarchitecture.html)

o Reference Section: Chapter: Mobility Architecture, "Inter-Controller Roaming- Layer 3" section.

2. Cisco, Mobility Fundamentals - WLC. "Layer 3 roaming occurs when a client moves between two WLCs that are in the same mobility group, but the WLCs are on different subnets. The client maintains its original IP address and the traffic is tunneled from the foreign WLC to the anchor WLC."

o Source URL: https://www.cisco.com/c/en/us/support/docs/wirelessmobility/wireless-lan-wlan/80921-mobility-fundamentals-wlc.html

o Reference Section: Introduction and diagrams illustrating Layer 3 roaming.

Question: 27

An engineer must create an EEM script to enable OSPF debugging in the event the OSPF neighborship goes down. Which script must the engineer apply?

A. event manager applet ENABLEOSPFDEBUG event syslog pattern "%OSPF-5-ADJCHG: Process 6, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN" action 1.0 cli command "enable" action 2.0 cli command "debug ip ospf event" action 3.0 cli command "debug ip ospf adj" action 4.0 syslog priority informational msg "ENABLEOSPFDEBUG"

B. event manager applet ENABLEOSPFDEBUG event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL" action 1.0 cli command "debug ip ospf event" action 2.0 cli command "debug ip ospf adj" action 3.0 syslog priority informational msg "ENABLEOSPFDEBUG"

C. event manager applet ENABLEOSPFDEBUG event syslog pattern "%OSPF-1-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from FULL to DOWN" action 1.0 cli command "debug ip ospf event" action 2.0 cli command "debug ip ospf adj" action 3.0 syslog priority informational msg "ENABLEOSPFDEBUG"

D. event manager applet ENABLEOSPFDEBUG event syslog pattern "%OSPF-5-ADJCHG: Process 5, Nbr 1.1.1.1 on Serial0/0 from LOADING to FULL" action 1.0 cli command "enable" action 2.0 cli command "debug ip ospf event" action 3.0 cli command "debug ip ospf adj" action 4.0 syslog priority informational msg "ENABLEOSPFDEBUG"

Answer:

A

Explanation:

The objective is to create a Cisco Embedded Event Manager (EEM) applet that activates OSPF debugging commands when a neighborship transitions to the DOWN state. The core of this functionality lies in the event syslog pattern command, which must precisely match the syslog message generated by the router for this specific event. According to Cisco's official documentation, the system message for an OSPFv2 adjacency change is %OSPF-5-ADJCHG. The script must trigger on the state change from FULL to DOWN. Therefore, the only pattern that correctly identifies the required trigger is "%OSPF-5-ADJCHG: ... from FULL to DOWN". Option A is the only choice that uses this exact, correct pattern. While the action 1.0 cli command "enable" is technically redundant as EEM applets execute in privileged EXEC mode by default, the trigger itself is correct, making it the only functional option for the stated goal.

Why Incorrect Options are Wrong:

B. This option is incorrect because the syslog pattern from LOADING to FULL triggers when an OSPF neighbor comes up and establishes a full adjacency, which is the opposite of the required scenario. C. This option uses an incorrect severity level in its pattern (%OSPF-1- ADJCHG). The standard, default severity level for this message is 5 (Notification), not 1 (Alerts). The pattern would fail to match the router's generated message. D. This option is incorrect for the same reason as B; the trigger pattern from LOADING to FULL monitors for a neighbor coming up, not going down. The inclusion of the redundant enable command does not fix the fundamental logic error in the trigger.

References:

Cisco Systems, Inc. (2023). Cisco IOS XE Amsterdam 17.3.x System
Message Guide. This guide documents the format and severity of system
messages. For OSPF, it specifies:
o Message: %OSPF-5-ADJCHG: Process dec, Nbr ip-addr on
chars from chars to chars, chars
o Explanation: "An OSPF neighbor has changed state... The severity
level is 5 (notification)."
o URL:
https://www.cisco.com/c/en/us/td/docs/iosxml/ios/iprouteospf/message/iro-msgs/os-ir-msgs.html
(Refer to
the %OSPF-5-ADJCHG section).
Cisco Systems, Inc. (2019). Embedded Event Manager Configuration
Guide, Cisco IOS XE Release 3S. This guide explains the configuration
and operation of EEM.
o Reference: It notes that EEM applet CLI actions are executed in
privileged EXEC mode by default.
o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/eem/configuration/xe-3s/eem-xe-3s-book/eem-overview.html
(See the "Benefits of Using Embedded Event Manager" section).

Question: 28

A wireless administrator must create a new web authentication corporate SSID that will be using ISE as the external RADIUS server. The guest VLAN must be specified after the authentication completes. Which action must be performed to allow the ISE server to specify the guest VLAN?

A. Set RADIUS Profiling.

B. Set AAA Policy name.

C. Enable Network Access Control State.

D. Enable AAA Override.

Answer:

D

Explanation:

The core of the question is how to allow an external RADIUS server (ISE) to dynamically assign a VLAN to a wireless user after authentication. The specific feature on a Cisco Wireless LAN Controller (WLC) that enables this is AAA Override. When this feature is enabled for a specific WLAN, the WLC will accept and apply RADIUS attributes sent by ISE, such as the VLAN ID, effectively overriding the default VLAN configured on the WLC for that SSID. This is a fundamental mechanism for dynamic, policy-based network access control in centralized authentication scenarios like the one described.

Why Incorrect Options are Wrong:

A. Set RADIUS Profiling: RADIUS Profiling is a feature within ISE used to identify and classify the type of device connecting (e.g., iPhone, Windows laptop). While this information can be used as a condition within an ISE policy, it does not enable the WLC to accept the VLAN assignment from ISE. B. Set AAA Policy name: This is a superficial configuration step. Naming a policy is for administrative identification and organization; it does not enable the functional capability for the WLC to accept dynamic RADIUS attributes. C. Enable Network Access Control State: This is too generic. "Network Access Control" (NAC) describes the overall security approach. It is not a specific, actionable configuration setting on the WLC that permits the RADIUS server to override the VLAN. The precise feature name is "AAA Override."

References:

1. Cisco, Central Web Authentication on the WLC and ISE Configuration Example: This official Cisco configuration guide, in a nearly identical scenario, explicitly states the requirement. In Step 1: Configure the WLAN, under the "Advanced" tab settings, the guide directs the administrator to: "check the Allow AAA Override check box." This confirms it is the direct

action needed.

o Source: Cisco Official Documentation

o URL: https://www.cisco.com/c/en/us/support/docs/security/identityservices-engine/115732-central-web-auth-wlc-ise-config-00.html

(See Step 1, WLAN Configuration section)

2. Cisco, Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Cupertino 17.9.x: The official controller documentation defines the feature's purpose. "AAA override enables you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server."

o Source: Cisco Official Vendor Documentation

o URL:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/179/config-guide/bwl179cg/maaaoverride.html (See the

"Information About AAA Override" section)

3. Cisco, Identity Services Engine Administrator Guide, Release 3.1: The ISE documentation clarifies its role in sending attributes that require the override setting on the network access device (NAD), such as the WLC. Authorization profiles in ISE are configured to send attributes like Tunnel-Private-Group-ID (for VLAN), which the NAD will only apply if configured to do so.

o Source: Cisco Official Vendor Documentation

o URL: https://www.cisco.com/c/en/us/td/docs/security/ise/31/adminguide/biseadminguide31/bISEadmin31policy.htm

l (See the chapter on "Manage Policies and Rules," specifically sections discussing authorization profiles and results).

Question: 29

What is a benefit of MACsec in a multilayered LAN network design?

A. There is no requirement to run IEEE 802.1X when MACsec is enabled on a switch port.

B. Layer 2 trunk links between switches can be secured.

C. Application flows between hosts on the LAN to remote destinations can be encrypted.

D. Layer 3 links between switches can be secured.

Answer:

B

Explanation:

MACsec (IEEE 802.1AE) is a Layer 2 security protocol that provides confidentiality, integrity, and data origin authenticity on a hop-by-hop basis for Ethernet frames. A primary and direct benefit of this protocol is securing the links between network devices. In a multilayered LAN, the trunk links between switches are critical pathways that carry traffic for multiple VLANs. Applying MACsec to these Layer 2 trunk links encrypts all data traversing them, protecting against threats like passive wiretapping, man-in-the-middle attacks, and content manipulation for all traffic on that link.

Why Incorrect Options are Wrong:

A. There is no requirement to run IEEE 802.1X when MACsec is enabled on a switch port. This is incorrect. While MACsec can be configured with static keys, the standard and most secure method for key exchange is the MACsec Key Agreement (MKA) protocol. MKA typically uses the 802.1X/EAP framework as its control plane for authentication and key distribution. Therefore, 802.1X is often a prerequisite for a dynamic and scalable MACsec deployment. C. Application flows between hosts on the LAN to remote destinations can be encrypted. This is incorrect. MACsec provides security on a single link or hop (hop-by-hop). It does not provide end-to- end encryption for an entire communication path from a LAN host to a remote destination across the internet or a WAN. That function is performed by higher-layer protocols like TLS or IPsec. D. Layer 3 links between switches can be secured. This is incorrect because MACsec is explicitly a Layer 2 protocol (IEEE 802.1AE). It operates on Ethernet frames. While these frames carry Layer 3 packets (like IP), the security mechanism itself is applied at Layer 2. The protocol designed for securing links at Layer 3 is IPsec.

References:

1. Cisco Systems, "MACsec and MACsec Key Agreement (MKA) Configuration Guide": This guide states, "MACsec, defined in 802.1AE, is an IEEE standard that provides data confidentiality, data integrity, and data origin authenticity... MACsec is a Layer 2 hop-to-hop encryption that

encrypts the entire data, except for the source and destination MAC addresses of an Ethernet packet." It also clarifies the common use for "Switch-to-switch security using MACsec with a pre-shared key".

o Source URL:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-9/configurationguide/sec/b179sec9600cg/macsecandmacseckeyagreementmka.html (See "Information About MACsec and MACsec Key Agreement (MKA)" section).

2. IEEE 802.1AE-2018 Standard, "Media Access Control (MAC) Security": The official standard defines MACsec as providing security services for MAC clients. The entire standard is focused on securing the connectionless data service provided by the MAC layer.

o Source URL: https://doi.org/10.1109/IEEESTD.2018.8585421 (See Section 1 "Overview").

3. Juniper Networks, "Understanding Media Access Control Security (MACsec)": This documentation specifies, "MACsec is a Layer 2 feature... It secures all traffic on a point-to-point Ethernet link between two MACsec-capable devices...". This highlights its application on L2 links, such as trunks. It also explains the relationship with 802.1X for key management.

o Source URL:
https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/macsec-overview.html (See the "Overview" and "MACsec in a VLAN Environment" sections).

Question: 30

Which character formatting is required for DHCP Option 43 to function with current AP models?

A. ASCII

B. Hex

C. Base64

D. MD5

Answer:

B

Explanation:

DHCP Option 43 is designated for vendor-specific information. It allows vendors like Cisco, Aruba, and others to provide custom data to their devices, such as the IP address of a Wireless LAN Controller (WLC) for an Access Point (AP). The DHCP standard itself (RFC 2132) defines Option 43 as an opaque field- a sequence of bytes. In practice, when network administrators configure a DHCP server to deliver this option, they must enter this byte sequence as a hexadecimal string. For instance, to direct a Cisco AP to a controller at IP 10.0.0.1, the value is not entered as ASCII text but as a hex string like f1040a000001. This string encodes vendor-specific sub-options, lengths, and values.

Why Incorrect Options are Wrong:

A. ASCII: This is incorrect. The data required is a structured byte stream, not a simple text string. While an IP address can be represented in ASCII, Option 43 requires a specific binary format that is entered in hex. C. Base64: This is incorrect. Base64 is an encoding scheme to represent binary data in ASCII strings, often used in other contexts like email attachments. However, the standard and universally documented method for configuring Option 43 on network infrastructure is hexadecimal. D. MD5: This is incorrect. MD5 is a cryptographic hash function used to verify data integrity. It is a one-way hash and is not used for encoding configuration data like an IP address for an AP to use.

References:

1. Cisco Wireless Controller Configuration Guide: This official Cisco documentation explicitly shows the configuration of DHCP Option 43 using hexadecimal values. It details how to construct the hex string based on the controller's IP address.
o Source: Cisco, "Cisco Wireless Controller Configuration Guide,
Release 8.5"
o Reference: Chapter: "Configuring DHCP Option 43"

o URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/85/config-guide/bcg85/deploying thewlan.html#ID1316 (Note: The
specific section shows the hex value f104c0a80a05 as an example
for the IP 192.168.10.5).
2. Aruba (an HPE company) Documentation: Aruba's official
documentation also specifies using a hexadecimal string for configuring
DHCP Option 43 to direct APs to an Aruba Mobility Conductor.
o Source: Aruba Networks, "Configuring DHCP Option 43 on a
Windows DHCP Server"
o Reference: The guide instructs entering the value as a "string value
in hexadecimal."
o URL:
https://www.arubanetworks.com/techdocs/ArubaOS87WebHelp/
Content/arubaos-solutions/dhcp-options/conf-dhcp-opt-43-wind.htm
3. IETF RFC 2132: This RFC defines the DHCP options. It specifies Option
43 as "Vendor Specific Information," where the data is a sequence of
encapsulated vendor-specific options. The representation of this binary
data in configuration is left to the implementation, which is standardized in
practice as hex.
o Source: IETF, "RFC 2132: DHCP Options and BOOTP Vendor
Extensions"

o Reference: Section 8.4, "Vendor Specific Information"
o URL: https://datatracker.ietf.org/doc/html/rfc2132#section-8.4

Question: 31

Which two components are needed when a Cisco SD-Access fabric is designed? (Choose two.)

A. Cisco Catalyst Center (formerly DNA Center) application

B. Firepower Threat Defense

C. Identity Service Engine

D. Cisco Data Center Network Manager

E. Cisco Prime Infrastructure

Answer:

A, C

Explanation:

A Cisco SD-Access fabric design fundamentally relies on two key components for its operation: a controller for automation and a policy engine for identity and access control. Cisco Catalyst Center (which was formerly known as DNA Center) serves as the centralized network controller. It provides a single pane of glass for design, provisioning, policy application, and network assurance. The Identity Services Engine (ISE) is the required policy engine. It integrates with Catalyst Center to provide dynamic and secure access control, handling user/device authentication and authorization, and enforcing micro-segmentation policies using Scalable Group Tags (SGTs).

Why Incorrect Options are Wrong:

B. Firepower Threat Defense: This is a next-generation firewall. While it can be integrated into an SD-Access fabric for advanced security and threat inspection at the fabric edge, it is not a mandatory component for the core fabric functionality. D. Cisco Data Center Network Manager: DCNM is the management platform specifically for Cisco's data center solutions, such as Nexus switches and the Application Centric Infrastructure (ACI) fabric. It is not used for the campus-focused SD-Access solution. E. Cisco Prime Infrastructure: Cisco Prime was a network management platform that predates Catalyst Center. For SD-Access, the automation and assurance capabilities of Cisco Catalyst Center are required, making Prime Infrastructure an incorrect and legacy option for this solution.

References:

1. Cisco Systems, "Cisco SD-Access Solution Design Guide (CVD) - Cisco Catalyst Center 2.3.7.x and Cisco IOS XE 17.12.x." This guide explicitly identifies the core components of the solution.

o Reference: In the "Solution Components" chapter, the document states, "The Cisco SD-Access solution is composed of the following major software and hardware components: Cisco DNA Center (controller) Cisco Identity Services Engine (identity and policy engine)..."

o URL:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sd-access-design-guide-2-3-7.html

2. Cisco Systems, "SD-Access for Distributed Campus Design Guide." This document reinforces the roles of Catalyst Center and ISE.

o Reference: The "Solution Components" section details the roles: "Cisco DNA Center- Centralized management system for the SD-Access solution... The controller for automation, policy, provisioning, and assurance." and "Cisco Identity Services Engine (ISE)- Identity and policy engine for the SD-Access solution."

o URL:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sdadistributed-campus-design-guide.html

3. Cisco Press, "Cisco SD-Access: The Complete Guide to Cisco's Software-Defined Campus." This book provides an in-depth architectural overview.

o Reference: Chapter 2, "Cisco SD-Access Architecture," describes the foundational pillars of the architecture, consistently highlighting Cisco DNA Center as the controller and ISE as the identity/policy platform.

o URL: https://www.ciscopress.com/store/cisco-sd-access-thecomplete-guide-to-ciscos-software-9780136532485

Question: 32

What are two characteristics of Cisco Catalyst SD-WAN? (Choose two.)

A. control plane operates over DTLS/TLS authenticated and secured tunnels

B. time-consuming configuration and maintenance

C. distributed control plane

D. unified data plane and control plane

E. centralized reachability, security, and application policies

Answer:

A, E

Explanation:

Cisco Catalyst SD-WAN architecture is fundamentally based on the principles of Software-Defined Networking (SDN), which involves separating the control, data, and management planes. Option A is correct because secure communication is paramount in the architecture. Control plane connections between the WAN Edge devices and the vSmart controllers are established over authenticated and encrypted DTLS or TLS tunnels. This ensures the integrity and confidentiality of routing and policy information being exchanged throughout the overlay fabric. Option E is correct because a primary benefit of the solution is the centralization of policy and management. Using the vManage platform, administrators can create and enforce comprehensive policies for routing (reachability), security (e.g., firewalling, IPS), and application quality of service (QoS) from a single point. These policies are then distributed to all WAN Edge devices, ensuring consistent enforcement across the entire network.

Why Incorrect Options are Wrong:

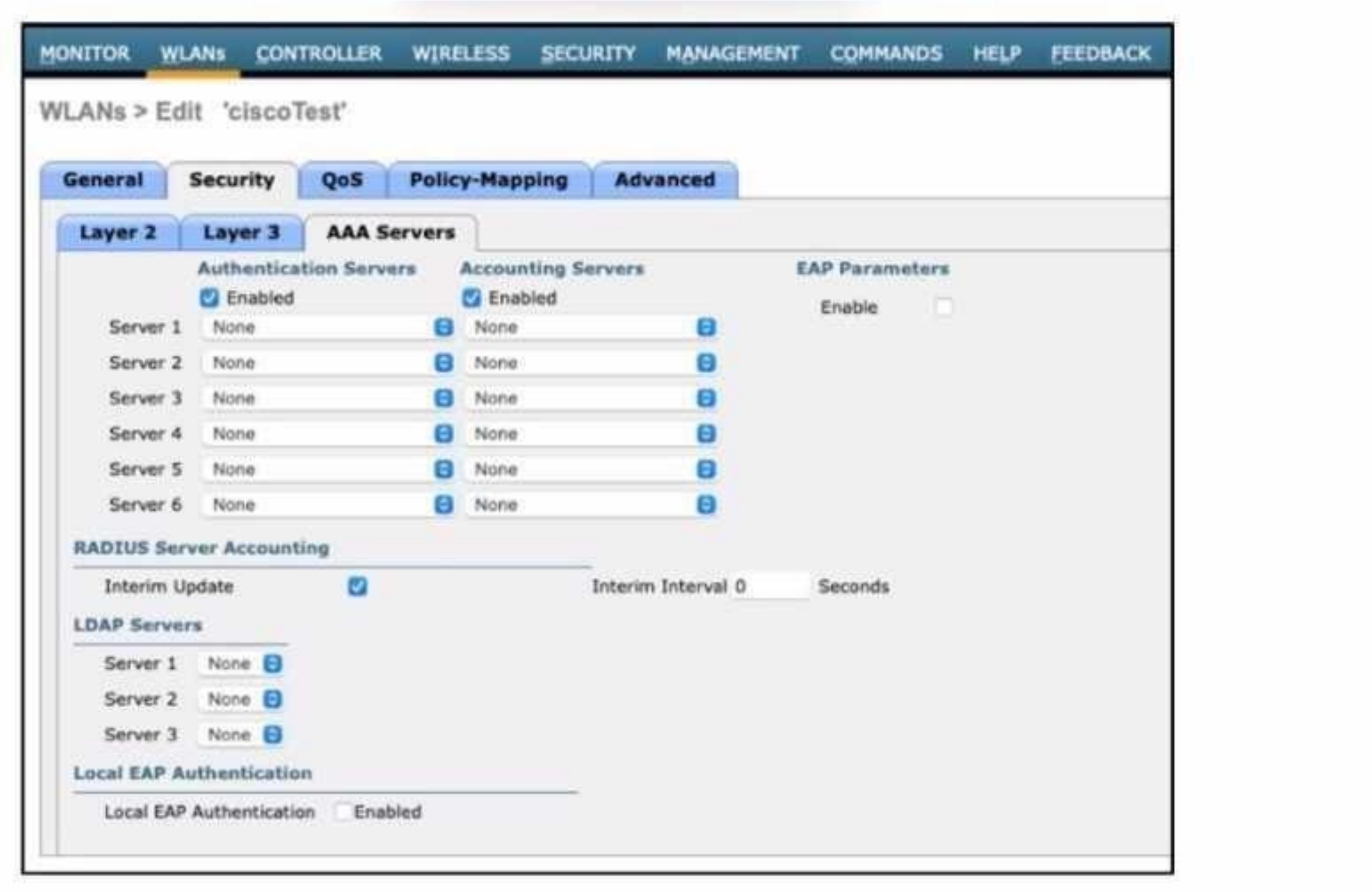
B. time-consuming configuration and maintenance: This is incorrect. A core value proposition of SD-WAN is the simplification and acceleration of WAN deployment and management through centralized control and zero- touch provisioning, reducing the time required for these tasks compared to traditional WANs. C. distributed control plane: This is incorrect. The solution's architecture is defined by a centralized control plane, orchestrated by the vSmart controllers. This is a key differentiator from traditional WANs where the control plane is distributed across every router. D. unified data plane and control plane: This is incorrect. Cisco SD- WAN adheres to the SDN model of separating the control plane from the data plane. The control plane (vSmart) makes decisions, while the data plane (WAN Edge routers) executes them by forwarding packets.

References:

1. Cisco Systems, "Cisco SD-WAN Overlay Network Security" (2023).
o This document states, "The Cisco SD-WAN solution uses a Datagram Transport Layer Security (DTLS) or a Transport Layer Security (TLS) tunnel to provide security and authentication for the control plane that runs between Cisco WAN Edge routers and Cisco vSmart controllers."
o URL:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/overlay-network-security.html
2. Cisco Systems, "Cisco SD-WAN Design Guide" (2022).
o Section: Cisco SD-WAN Architecture and Components: This guide explains the separation of planes and the role of each component. It describes the vSmart Controller as the "central brain of the solution" (centralized control plane) and vManage for "centralized configuration, provisioning, monitoring, and troubleshooting." This supports the correctness of option E and the incorrectness of C and D.
o URL:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/S DWAN/cisco-sdwan-design-guide.html#CiscoSDWANArchitectureandComponents
3. Cisco Systems, "Cisco SD-WAN End-to-End Deployment Guide" (2020).
o Section: Centralized Policies: This guide details how "Centralized policies are provisioned on the vSmart and affect the entire fabric." This directly confirms that policies for reachability and other functions are centralized, validating option E.
o URL:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/17-2/policies-book/centralized-policy.html

Question: 33

Refer to the exhibit.



WLANs > Edit 'ciscoTest'

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable □

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

LDAP Servers

Server 1 None

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication □ Enabled

An engineer must configure a Cisco WLC with WPA2 Enterprise mode and avoid global server lists. Which action is required?

A. Enable EAP parameters.

B. Apply CISCO ISE default settings.

C. Disable the RADIUS server accounting interim update.

D. Select a RADIUS authentication server.

Answer:

D

Explanation:

To configure a WLAN for WPA2-Enterprise, an external authentication server using the RADIUS protocol is required to handle the 802.1X/EAP (Extensible Authentication Protocol) authentication process. The exhibit displays the WLAN-specific 'AAA Servers' configuration tab. This tab is used to override the WLC's global server settings for a particular WLAN. The most critical and mandatory action on this screen to enable WPA2-Enterprise authentication for the 'ciscoTest'

WLAN is to select a configured RADIUS server from the 'Authentication Servers' dropdown list, which is currently set to 'None'. This directly associates the WLAN with the server that will validate user credentials.

Why Incorrect Options are Wrong:

A. Enable EAP parameters: EAP parameters are used for advanced tuning of the EAP protocol, such as setting timeouts or configuring EAP- FAST settings. While related, selecting the authentication server itself is the primary and prerequisite action. B. Apply CISCO ISE default settings: Cisco ISE is a specific type of RADIUS server. The configuration requires selecting any compatible RADIUS server that has been pre-configured on the WLC; it is not limited to Cisco ISE or its default settings. C. Disable the RADIUS server accounting interim update: RADIUS Accounting is a separate function from Authentication. Accounting tracks user session data (e.g., connection time, data usage) after a user has been successfully authenticated. It is not required to enable the authentication process itself.

References:

1. Cisco, "WPA2-Enterprise with RADIUS Server on Cisco WLC Configuration Example": This official configuration example explicitly details the process. In Step 3: Configure the WLAN for WPA2-Enterprise, the guide instructs the user to navigate to the WLANs WLANID Security AAA Servers tab and "Choose the appropriate RADIUS server from the Server 1 drop-down list under Authentication Servers." This directly confirms that selecting the server is the required action.

o URL: https://www.cisco.com/c/en/us/support/docs/wireless/4400series-wireless-lan-controllers/115982-wpa2-ent-wlc-00.html

o Section: Step 3: Configure the WLAN for WPA2-Enterprise.

2. Cisco, "Cisco Wireless LAN Controller Configuration Guide, Release 8.5": This guide explains the purpose of the WLAN-specific AAA server settings. It clarifies that these settings are used to override the global RADIUS server configuration for a specific WLAN. The primary function of this section is to assign the servers that will handle authentication and accounting.

o URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/85/config-guide/bcg85/configuringwlan.html

o Section: "Configuring AAA Servers for a WLAN" (and preceding sections on "Information About AAA Servers on WLANs"). This section states, "You can configure the authentication and accounting servers that are to be used by a particular WLAN. You can also override the global server settings."

Question: 34

Which message type is valid for IGMPv3?

A. leave group

B. hello

C. graft

D. source-specific membership report

Answer:

D

Explanation:

A source-specific membership report is a valid and defining message type in IGMPv3. The primary enhancement of IGMPv3 over its predecessors is the introduction of source filtering. This allows a host to signal to its local router that it wants to receive multicast traffic from a group and only from a specific list of source addresses. This information is carried within an IGMPv3 Membership Report message (Type 0x22), which is fundamentally source- specific in its design and purpose.

Why Incorrect Options are Wrong:

A. leave group: The explicit "Leave Group" message is a feature of IGMPv2. In IGMPv3, leaving a group is handled by sending a new Membership Report that updates the source list for that group (e.g., excluding all sources or changing to an empty include list). B. hello: "Hello" packets are characteristic of routing protocols like OSPF and EIGRP, which use them for neighbor discovery and keepalives. They are not part of the IGMP specification. C. graft: "Graft" messages are used in multicast routing protocols, such as Protocol Independent Multicast - Dense Mode (PIM-DM). A router sends a graft message to rejoin a pruned branch of a multicast distribution tree. IGMP is a host-to-router protocol.

References:

1. IETF RFC 3376: Internet Group Management Protocol, Version 3.
o Quote/Paraphrase: The introduction states, "Version 3 adds support for 'source filtering', that is, the ability for a system to report interest in receiving packets only from specific source addresses...". Section 4.1 specifies the "Version 3 Membership Report" (Type 0x22) as the message that carries this source-specific information.
o Location: Section 1 (Introduction, page 3) and Section 4.1 (IGMP Message Format, page 11).
o URL: https://www.rfc-editor.org/rfc/rfc3376.html

2. Cisco, IP Multicast: IGMP Configuration Guide.
o Quote/Paraphrase: This guide explains that IGMPv3 adds support for source filtering, which allows a client to signal that it wants to receive traffic from only specific sources. This is done via the IGMPv3 Membership Report.
o Location: "IGMP Version 3" section.
o URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/ipmultiigmp/configuration/15-mt/imc-igmp-15-mt-book/imcigmpv3.html
3. Carnegie Mellon University, School of Computer Science, 15-441: Computer Networks, Lecture 19: Multicast.
o Quote/Paraphrase: The lecture slides clearly differentiate the IGMP versions, noting that IGMPv3 supports source-specific join/leave requests, in contrast to IGMPv2's group-specific leave messages.
o Location: Slide 30, "IGMP v3".
o URL: https://www.cs.cmu.edu/srini/15-441/F07/lectures/19multicast.pdf

Question: 35

Which two characteristics apply to Type 1 hypervisors? (Choose two.)

A. They are widely available to license for free.

B. They provide a platform for running bare metal operating systems.

C. They can be used to create and manage virtual storage

D. They are a software layer that runs on top of a virtual server.

E. They provide a platform for running guest operating systems.

Answer:

C, E

Explanation:

A Type 1 hypervisor, also known as a bare-metal hypervisor, runs directly on the host's physical hardware. Its primary role is to create and manage virtual machines (VMs). Each VM operates as a self-contained computer, running its own guest operating system (E). A core function of the hypervisor is to abstract and manage the underlying physical hardware resources, including CPU, memory, and storage. It allocates these resources to the VMs. This includes creating and managing virtual storage (C), such as virtual hard disks, which are presented to the guest operating systems.

Why Incorrect Options are Wrong:

A. They are widely available to license for free. While some Type 1 hypervisors like Xen and KVM are open-source and free, and others like VMware ESXi have free versions with limited features, full-featured enterprise editions typically require paid licenses. Therefore, this is not a universal characteristic. B. They provide a platform for running bare metal operating systems. This is incorrect. A Type 1 hypervisor runs on bare metal hardware itself. It provides a platform for running virtualized or guest operating systems, not bare metal ones. D. They are a software layer that runs on top of a virtual server. This statement inverts the architecture. The hypervisor runs on a physical server and hosts virtual servers; it does not run on top of them.

References:

NIST Special Publication 800-125A (Draft): Defines a hypervisor as a software platform that "provides virtualization of hardware resources (such as CPU, Memory, Network and Storage)" and "enables multiple computing stacks (made of an operating system (OS) and application programs) called Virtual Machines (VMs) to be run on a single physical host." This supports both C and E.

o Source: NIST Computer Security Resource Center, "Draft SP 800-125A Rev. 1, Security Recommendations for Server-based Hypervisor Platforms", Page 7, Lines 130-132.

o URL: https://csrc.nist.gov/CSRC/media/Publications/sp/800125a/rev-1/draft/documents/sp800-125A-r1-draft.pdf

VMware Documentation (via Scale Computing resource): Describes the hypervisor's role: "The hypervisor is the core component of virtualization software, enabling multiple VMs to share a single physical server... Dynamically allocates CPU, memory, and storage to each VM... Guest operating systems... are installed within each VM." This confirms the hypervisor manages storage (C) and runs guest OSs (E).

o Source: Scale Computing, "Virtualization Software: Benefits & Types".

o URL: https://www.scalecomputing.com/resources/virtualizationsoftware-how-it-works-types-and-advantages

Xen Project Documentation: Describes the Xen Project hypervisor as "an open-source type-1 or baremetal hypervisor, which makes it possible to run many instances of an operating system or indeed different operating systems in parallel on a single machine." This directly supports option E. Regarding licensing (A), it notes Xen is "available as open source," but this doesn't apply to all Type 1 hypervisors.

o Source: Xen Project, "Hypervisor".

o URL: https://xenproject.org/projects/hypervisor

IEEE Publication: A 2023 review paper states, "A Type 1 hypervisor runs directly on the host computer's physical hardware and interacts directly with its CPU, memory, and physical storage... A Type 1 hypervisor replaces the host operating system... KVM, Microsoft Hyper-V, and VMware vSphere are examples of a Type 1 hypervisor." This confirms the direct management of hardware, including storage (supporting C).

o Source: JETIR, "A COMPREHENSIVE REVIEW OF THE VIRTUALIZATION AND FACTORS AFFECTING IT.", Volume 10, Issue 4, April 2023, Page 2.

o URL: https://www.jetir.org/papers/JETIR2304110.pdf