- **Vendor:** Cisco
- **Exam Code:** 350-401
- **Exam Name:** Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
- **New Updated Questions from Braindump2go (Updated in August/2020)**

QUESTION 72
Which two operations are valid for RESTCONF? (Choose two.)

A. HEAD
B. REMOVE
C. PULL
D. PATCH
E. ADD
F. PUSH

Answer: AD
Explanation:
RESTCONF operations include OPTIONS, HEAD, GET, POST, PATCH, DELETE.

QUESTION 73
What is a benefit of deploying an on-premises infrastructure versus a cloud infrastructure deployment?

A. faster deployment times because additional infrastructure does not need to be purchased
B. lower latency between systems that are physically located near each other
C. less power and cooling resources needed to run infrastructure on-premises
D. ability to quickly increase compute power without the need to install additional hardware

Answer: B
Explanation:
The difference between on-premise and cloud is essentially where this hardware and software resides. On-premise means that a company keeps all of this IT environment onsite either managed by themselves or a third-party. Cloud means that it is housed offsite with someone else responsible for monitoring and maintaining it.

QUESTION 74
How does Cisco Trustsec enable more access controls for dynamic networking environments and data centers?

A. uses flexible NetFlow
B. assigns a VLAN to the endpoint
C. classifies traffic bused an the contextual identity of the endpoint rather than its IP address
D. classifies traffic based on advanced application recognition

Answer: C
Explanation:

The Cisco TrustSec solution simplifies the provisioning and management of network access control through the use of software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not IP address, enabling policy change without net-work redesign.
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2016/User-to-DC_Access_Control_Using_TrustSec_Deployment_April2016.pdf

QUESTION 75
Which method does the enable secret password option use to encrypt device passwords?

A. AES
B. CHAP
C. PAP
D. MD5

Answer: D

QUESTION 76
Refer to the exhibit. Which privilege level is assigned to VTY users?

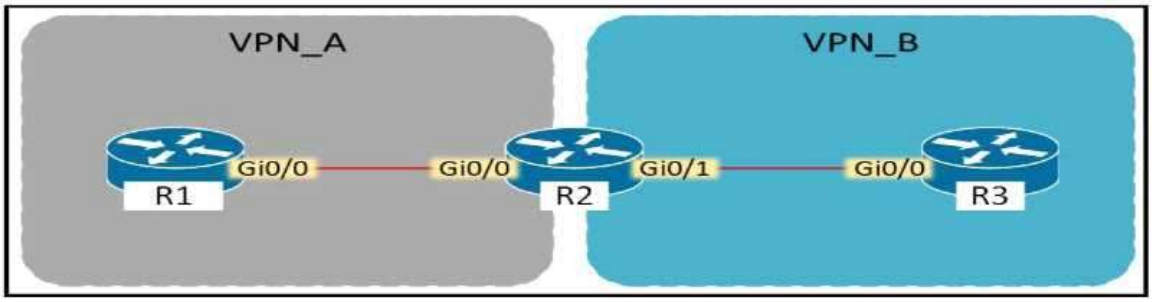
```
R1# sh run | begin line con
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password 7 045802150C2E
 login
line vty 5 15
 password 7 045802150C2E
 login
!
end

R1# sh run | include aaa | enable
no aaa new-model
R1#
```

A. 1
B. 7
C. 13
D. 15

Answer: A
Explanation:
Lines (CON, AUX, VTY) default to level 1 privileges.

QUESTION 77
Refer to the exhibit. Assuming that R is a CE router, which VRF is assigned to Gi0/0 on R1?



A. VRF VPN_B
B. Default
C. Management VRF
D. VRF VPN_A

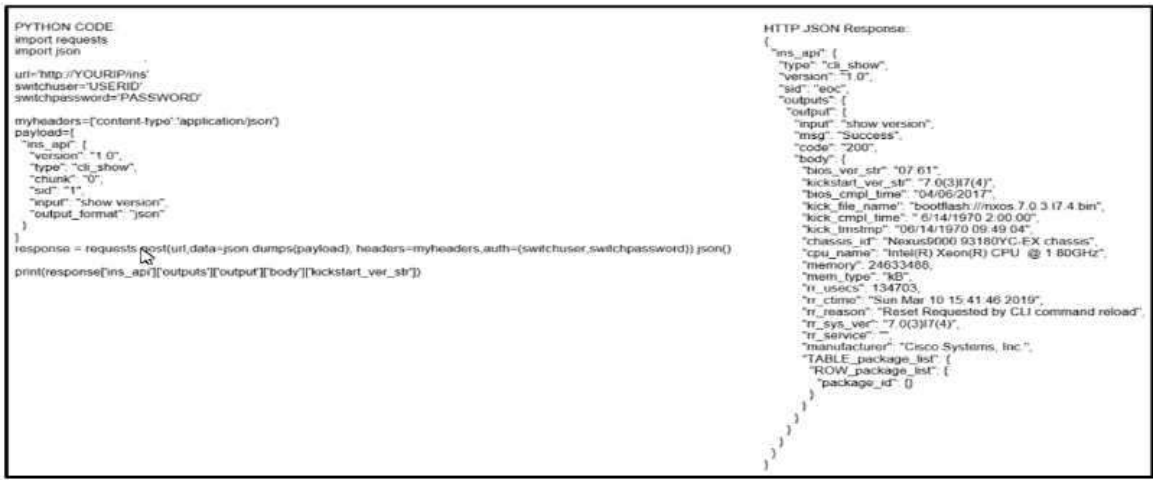
Answer: D

QUESTION 78
Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

A. MACsec
B. IPsec
C. SSL
D. Cisco Trustsec

Answer: A
Explanation:
MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.
A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a MKA peer) using the current session key.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html
Note: Cisco Trustsec is the solution which includes MACsec.

QUESTION 79
Refer to the exhibit. Which HTTP JSON response does the python code output give?



A. NameError: name 'json' is not defined
B. KeyError 'kickstart_ver_str'
C. 7.61
D. 7.0(3)I7(4)

Answer: D
Explanation:
+ If you want to run the full code in this question in Python (with a real HTTP JSON response), you must first install "requests" package before "import requests".
+ The error "NameError: name 'json' is not defined" is only shown if we forgot the line "import json" in Python code -> Answer A is not correct.
+ We only see the "KeyError" message if we try to print out an unknown attribute (key).

QUESTION 80
Which two statements about EIGRP load balancing are true? (Choose two.)

A. EIGRP supports 6 unequal-cost paths.
B. A path can be used for load balancing only if it is a feasible successor.
C. EIGRP supports unequal-cost paths by default.
D. Any path in the EIGRP topology table can be used for unequal-cost load balancing.
E. Cisco Express Forwarding is required to load-balance across interfaces.

Answer: AB
Explanation:
EIGRP provides a mechanism to load balance over unequal cost paths (or called unequal cost load balancing) through the "variance" command. In other words, EIGRP will install all paths with metric < variance * best_metric into the local routing table, provided that it meets the feasibility condition to prevent routing loop. The path that meets this requirement is called a feasible successor. If a path is not a feasible successor, it is not used in load balancing.
Note: The feasibility condition states that, the Advertised Distance (AD) of a route must be lower than the feasible distance of the current successor route.

QUESTION 81
Which statement about LISP encapsulation in an EIGRP OTP implementation is true?

A. OTP uses LISP encapsulation for dynamic multipoint tunneling.
B. OTP maintains the LISP control plane.
C. OTP uses LISP encapsulation to obtain routes from neighbors.
D. LISP learns the next hop.

Answer: B

Explanation:
The EIGRP Over the Top solution can be used to ensure connectivity between disparate EIGRP sites. This feature uses EIGRP on the control plane and Locator ID Separation Protocol (LISP) encapsulation on the data plane to route traffic across the underlying WAN architecture. EIGRP is used to distribute routes between customer edge (CE) devices within the network, and the traffic forwarded across the WAN architecture is LISP encapsulated.
EIGRP OTP only uses LISP for the data plane, EIGRP is still used for the control plane. Therefore we cannot say OTP uses LISP encapsulation for dynamic multipoint tunneling as this requires encapsulating both data and control plane traffic -> Answer A is not correct.
In OTP, EIGRP serves as the replacement for LISP control plane protocols (therefore EIGRP will learn the next hop, not LISP -> Answer D is not correct). Instead of doing dynamic EID-to-RLOC mappings in native LISP-mapping services, EIGRP routers running OTP over a service provider cloud create targeted sessions, use the IP addresses provided by the service provider as RLOCs, and exchange routes as EIDs.

QUESTION 82
Which EIGRP feature allows the use of leak maps?

A. offset-list
B. neighbor
C. address-family
D. stub

Answer: D
Explanation:
If we configured an EIGRP stub router so that it only advertises connected and summary routes. But we also want to have an exception to this rule then we can configure a leak-map. For example:

```
R4(config-if)#router eigrp 1
R4(config-router)#eigrp stub
R4(config)#ip access-list standard R4_L0opback0
R4(config-std-nacl)#permit host 4.4.4.4
R4(config)#route-map R4_L0opback0_LEAKMAP
R4(config-route-map)#match ip address R4_L0opback0
R4(config)#router eigrp 1
R4(config-router)#eigrp stub leak-map R4_L0opback0_LEAKMAP
```

As we can see the leak-map feature goes long with ‘eigrp stub’ command.

QUESTION 83
Which statements are used for error handling in Python?

A. try/catch
B. try/except
C. block/rescue
D. catch/release

Answer: B
Explanation:
The words “try” and “except” are Python keywords and are used to catch exceptions. For example:

```
try:
 print 1/0
except ZeroDivisionError:
 print "Error! We cannot divide by zero!!!"
```