Vendor: Cisco

Exam Code: 350-401

Exam Name: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)

Version: DEMO

QUESTION 1
Which signal strength and noise values meet the minimum SNR for voice networks?

A. signal strength -67 dBm, noise 91 dBm
B. signal strength -69 dBm, noise 94 dBm
C. signal strength -68 dBm, noise 89 dBm
D. signal strength -66 dBm, noise 90 dBm

Answer: B
Explanation:
The recommended minimum SNR for voice applications on wireless networks is 25dB. The noise should be in negative number so if the question says “noise 91 dBm” we should understand: N = -91 dBm.
If your SNR measurements are already in decibel form, then you can subtract the noise quantity from the desired signal: SNR = S – N. This is because when you subtract logarithms, it is the equivalent of dividing normal numbers. Also, the difference in the numbers equals the SNR. In this question, only “signal strength -69 dBm, noise 94 dBm” has SNR = -69 – (-94) = 25dB which is equal to the recommended minimum SNR for voice applications.

QUESTION 2
A system must validate access rights to all its resources and must not rely on a cached permission matrix. If the access level to a given resource is revoked but is not reflected in the permission matrix, the security is violates.
Which term refers to this REST security design principle?

A. economy of mechanism
B. complete mediation
C. separation of privilege
D. least common mechanism

Answer: B
Explanation:
A system should validate access rights to all its resources to ensure that they are allowed and should not rely on the cached permission matrix. If the access level to a given resource is being revoked, but that is not being reflected in the permission matrix, it would be violating security.

QUESTION 3
Drag and Drop Question

Drag and drop the snippets onto the blanks within the code to construct a script that shows all logging that occurred on the appliance from Sunday until 9:00 p.m. Thursday. Not all options are used.

Answer Area

```
event manager applet Logging
  event timer cron name Logging cron-entry "  [          ] "
  action 2.0 cli command "enable"
  action [          ] cli command "show logging | [          ] "
```

1.0 | 0 21 * * 0-4 | redirect ftp://cisco:cisco@192.168.1.1

3.0 | 0 21 * * 1-5 | ftp://cisco:cisco@192.168.1.1

Answer:

Answer Area

```
event manager applet Logging
  event timer cron name Logging cron-entry "  0 21 * * 0-4 "
  action 2.0 cli command "enable"
  action 3.0 cli command "show logging | redirect ftp://cisco:cisco@192.168.1.1 "
```

1.0

0 21 * * 1-5 | ftp://cisco:cisco@192.168.1.1

Explanation:
cron-entry Text string that consists of five fields separated by spaces. The fields represent the times and dates when CRON timer events will be triggered. There are 5 values you can specify:

minute – this controls what minute of the hour the command will fire values between 0 and 59
hour – this controls what hour the command will run – specified in the 24 hour clock format 0-23 (0=midnight)
day-of-month – A number in the range from 1 to 31 that specifies the day of the month when a CRON timer event is triggered.
month – A number in the range from 1 to 12 or the first three letters (not case-sensitive) of the name of the month in which a CRON timer event is triggered.
day-of-week – A number in the range from 0 to 6 (Sunday is 0) or the first three letters (not case-sensitive) of the name of the day when a CRON timer event is triggered.

Examples:
01 * * * * This command is run at one min past every hour
17 8 * * * This command is run daily at 8:17 am
*/1 **** this command runs every minute

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e2.html
This cron runs from Sunday to Thursday -> 0-4

QUESTION 4

On which protocol or technology is the fabric data plane based in Cisco SD-Access fabric?

A. LISP
B. IS-IS
C. Cisco TrustSec
D. VXLAN

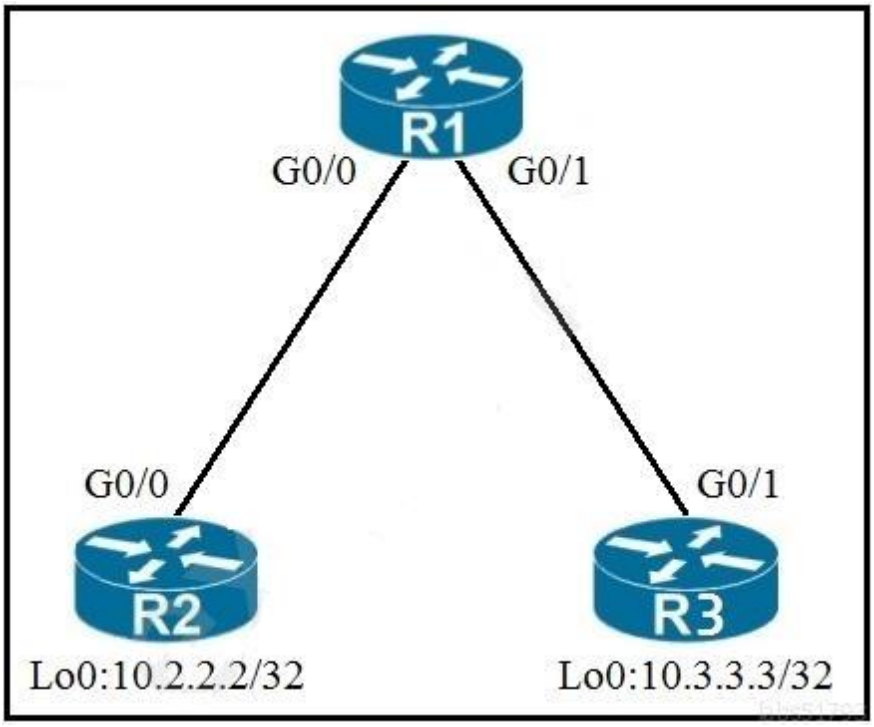
Answer: D
Explanation:
The tunneling technology used for the fabric data plane is based on Virtual Extensible LAN (VXLAN). VXLAN encapsulation is UDP based, meaning that it can be forwarded by any IP-based network (legacy or third party) and creates the overlay network for the SD-Access fabric. Although LISP is the control plane for the SD-Access fabric, it does not use LISP data encapsulation for the data plane; instead, it uses VXLAN encapsulation because it is capable of encapsulating the original Ethernet header to perform MAC-in-IP encapsulation, while LISP does not. Using VXLAN allows the SD-Access fabric to support Layer 2 and Layer 3 virtual topologies (overlays) and the ability to operate over any IP-based network with built-in network segmentation (VRF instance/VN) and built-in group-based policy.

QUESTION 5
Which feature Is used to propagate ARP broadcast, and link-local frames across a Cisco SD-Access fabric to address connectivity needs for silent hosts that require reception of traffic to start communicating?

A. Native Fabric Multicast
B. Layer 2 Flooding
C. SOA Transit
D. Multisite Fabric

Answer: B
Explanation:
Layer2 Flooding
Cisco SD-Access fabric provides many optimizations to improve unicast traffic flow, and to reduce the unnecessary flooding of data such as broadcasts. But, for some traffic and applications, it may be desirable to enable broadcast forwarding within the fabric. By default, this is disabled in the Cisco SD-Access architecture. If broadcast, Link local multicast and Arp flooding is required, it must be specifically enabled on a per-subnet basis using Layer 2 flooding feature.
Layer 2 flooding can be used to forward broadcasts for certain traffic and application types which may require leveraging of Layer 2 connectivity, such as silent hosts, card readers, door locks, etc.

QUESTION 6
Refer to the exhibit. An engineer must deny Telnet traffic from the loopback interface of router R3 to the Loopback interface of router R2 during, the weekend hours. All other traffic between the loopback interfaces of routers R3 and R2 must be allowed at all times Which command set accomplishes this task?



A. R1(config)#**time-range WEEKEND**
R1(config-time-range)#**periodic Friday Sunday 00:00 to 00:00**

R1(config)#**access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND**
R1(config)#**access-list 150 permit ip any any**

R1(config)#**interface G0/1**
R1(config-if)#**ip access-group 150 in**

B. R3(config)#**time-range WEEKEND**
R3(config-time-range)#**periodic Saturday Sunday 00:00 to 23:59**

R3(config)#**access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND**
R3(config)#**access-list 150 permit ip any any time-range WEEKEND**

R3(config)#**interface G0/1**
R3(config-if)#**ip access-group 150 out**

C. R3(config)#**time-range WEEKEND**
R3(config-time-range)#**periodic weekend 00:00 to 23:59**

R3(config)#**access-list 150 permit tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND**
R3(config)#**access-list 150 permit ip any any time-range WEEKEND**

R3(config)#**interface G0/1**
R3(config-if)#**ip access-group 150 out**

D. R1(config)#**time-range WEEKEND**
R1(config-time-range)#**periodic weekend 00:00 to 23:59**

R1(config)#**access-list 150 deny tcp host 10.3.3.3 host 10.2.2.2 eq 23 time-range WEEKEND**
R1(config)#**access-list 150 permit ip any any**

R1(config)#**interface G0/1**
R1(config-if)#**ip access-group 150 in**

Answer: D
Explanation:
We cannot filter traffic that is originated from the local router (R3 in this case) so we can only configure the ACL on R1 or R2. "Weekend hours" means from Saturday morning through Sunday night so we have to configure: "periodic weekend 00:00 to 23:59".
Note: The time is specified in 24-hour time (hh:mm), where the hours range from 0 to 23 and the minutes range from 0 to 59.

QUESTION 7
An engineer must configure a new loopback interface on a router and advertise the interface as a /24 in OSPF. Which command set accomplishes this task?

A. R2(config-router)#network 172.22.2.0 0.0.0.255 area 0
R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf 100 area 0
B. R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf network point-to-point
R2(config-if)#ip ospf 100 area 0
C. R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf network point-to-multipoint
R2(config-if)#router ospf 100
D. R2(config)#interface Loopback0
R2(config-if)#ip address 172.22.2.1 255.255.255.0
R2(config-if)#ip ospf network broadcast
R2(config-if)#ip ospf 100 area 0

Answer: B
Explanation:
Although the configured loopback address is 172.22.2.1/24 but by default OSPF will advertise this route to loopback0 as 172.22.2.1/32 (most specific route to that loopback). In order to override this, we have to change the network type to point-to-point. After this OSPF will advertise the address to loopback as 172.22.2.0/24.

QUESTION 8
A customer transitions a wired environment to a Cisco SD-Access solution. The customer does not want to integrate the wireless network with the fabric. Which wireless deployment approach enables the two systems to coexist and meets the customer requirement?

A. Deploy the APs in autonomous mode
B. Deploy the wireless network over the top of the fabric
C. Deploy a separate network for the wireless environment
D. Implement a Cisco DNA Center to manage the two networks

Answer: B
Explanation:

Customers with a wired network based on SD-Access fabric have two options for integrating wireless access:
+ SD-Access Wireless Architecture
+ Cisco Unified Wireless Network Wireless Over the Top (OTT)
OTT basically involves running traditional wireless on top of a fabric wired network.
Why would you deploy Cisco Unified Wireless Network wireless OTT? There are two primary reasons:
…
2. Another reason for deploying wireless OTT could be that customer doesn't want or cannot migrate to fabric for wireless.
Reference: https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/cisco-dna-center-sd-access-wl-dg.pdf

QUESTION 9
Refer to the exhibit. A network engineer must log in to the router via the console, but the RADIUS servers are not reachable. Which credentials allow console access1?

```
Router# show running-config

! lines omitted for brevity

username cisco password 0 cisco

aaa authentication login group1 group radius line
aaa authentication login group2 group radius local
aaa authentication login group3 group radius none

line con 0
password 0 cisco123
login authentication group1
line aux 0
login authentication group3
line vty 0 4
password 0 test123
login authentication group2
```

A. the username "cisco" and the password "Cisco"
B. no username and only the password "test123"
C. no username and only the password "cisco123"
D. the username "cisco" and the password "cisco123"

Answer: C
Explanation:
We tested with GNS3 and the router only requires password "cisco123" configured under line console to authenticate. So we can deduce the "password" command under line interface is preferred over "login authentication" command.

QUESTION 10
A client device roams between access points located on different floors in an atrium. The access points are Joined to the same controller and configured in local mode. The access points are in different AP groups and have different IP addresses, but the client VLAN in the groups is the same.
Which type of roam occurs?

A. inter-controller
B. inter-subnet
C. intra-VLAN
D. intra-controller

Answer: D
Explanation:
Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. Three popular types of client roaming are:
Intra-Controller Roaming: Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address.
Inter-Controller Roaming: Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active. Inter-Subnet Roaming: Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active.
In three types of client roaming above, only with Inter-Subnet Roaming the controllers are in different subnets.

QUESTION 11
An engineer must configure AAA on a Cisco 9800 WLC for central web authentication.
Which two commands are needed to accomplish this task? (Choose two.)

A. (Cisco Controller) > config wlan aaa-override disable <wlan-id>
B. (Cisco Controller) > config radius acct add 10.10.10.12 1812 SECRET
C. (Cisco Controller) > config wlan aaa-override enable <wlan-id>
D. Device(config-locsvr-da-radius)# client 10.10.10.12 server-key 0 SECRET
E. Device(config)# aaa server radius dynamic-author

Answer: DE
Explanation:
Answer A and answer C are used to enable/disable AAA Override option but it is just optional so they are not the correct answers. AAA Override enables you to apply VLAN tagging, Quality of Service, and Access Control Lists to individual clients based on the returned RADIUS attributes from the AAA server.
According to this Cisco link (under AAA Configuration on 9800 WLCs) section, we need the following commands:

```
# aaa new-model
# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Therefore answer D and answer E are correct.
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213919-configure-802-1x-authentication-on-catal.pdf

QUESTION 12
Refer to the exhibit. A network engineer must configure a password expiry mechanism on the gateway router for all local passwords to expire after 60 days.
What is required to complete this task?

```
username admin privilege 15 password 0 Cisco13579!
aaa new-model
!
aaa authentication login default local
aaa authentication enable default none
!
aaa common-criteria policy Administrators
  min-length 1
  max-length 127
  char-changes 4
  lifetime month 2
!
```

A. The password expiry mechanism is on the AAA server and must be configured there.
B. Add the aaa authentication enable default Administrators command.
C. Add the username admin privilege 15 common-criteria-policy Administrators password 0 Cisco13579! command.
D. No further action Is required. The configuration is complete.

Answer: C
Explanation:
SUMMARY STEPS
Perform this task to create a password security policy and to apply the policy to a specific user profile.

```
enable
configure terminal
aaa new-model
aaa common-criteria policy policy-name
char-changes number
max-length number
min-length number
numeric-count number
special-case number
exit
username username common-criteria-policy policy-name password password
end
```

QUESTION 14
Refer to the exhibit. An engineer must add the SNMP interface table to the NetFlow protocol flow records. Where should the SNMP table option be added?

```
flow record Recorder
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
!
flow exporter Exporter
 destination 192.168.100.22
 transport udp 2055
!
flow monitor Monitor
 exporter Exporter
 record Recorder
!
et-analytics
 ip flow-export destination 192.168.100.22 2055
!
interface gi1
ip flow monitor Monitor input
ip flow monitor Monitor output
et-analytics enable
!
```

A. under the interface
B. under the flow record
C. under the flow monitor
D. under the flow exporter

Answer: D
Explanation:
option interface-table
This command causes the periodic sending of an options table, which will allow the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table
```

https://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html

QUESTION 14
Which two operational models enable an AP to scan one or more wireless channels for rouge access points and at the same time provide wireless services to clients? (Choose two.)

A. Rouge detector
B. Sniffer
C. FlexConnect
D. Local
E. Monitor

Answer: CD
Explanation:
+ In a dense RF environment, where maximum rogue access points are suspected, the chances of detecting rogue access points by a local mode access point and FlexConnect mode access point in channel 157 or channel 161 are less when compared to other channels. To mitigate this problem, we recommend that you use dedicated monitor mode access points.
+ The local and FlexConnect mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

QUESTION 15
What is a consideration when designing a Cisco SD-Access underlay network?

A. End user subnets and endpoints are part of the underlay network.
B. The underlay switches provide endpoint physical connectivity for users.
C. Static routing is a requirement,
D. It must support IPv4 and IPv6 underlay networks

Answer: B
Explanation:
In SD-Access, the underlay switches (edge nodes) support the physical connectivity for users and endpoints. However, end-user subnets and endpoints are not part of the underlay network—they are part of the automated overlay network.
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**