Type text to search here...

Home > New ENCOR Questions- Part 6

New ENCOR Questions- Part 6

April 11th, 2021 in New ENCOR Questions Go to comments

Premium Member: You can practice these questions first via these links:
+ Question 1 to 22
+ Question 23 to end

Question 1

An engineer must create an EEM applet that sends a syslog message in the event a change happens in the network due to trouble with an OSPF process. Which action should the engineer use?

A. action 1 syslog msg "OSPF ROUTING ERROR"
B. action 1 syslog send "OSPF ROUTING ERROR"
C. action 1 syslog pattern "OSPF ROUTING ERROR"
D. action 1 syslog write "OSPF ROUTING ERROR"

Answer: A

Question 2

Refer to the exhibit.

```
ip nat pool Internet 10.10.10.1 10.10.10.100 netmask 255.255.255.0
ip nat inside source route-map Users pool Internet
!
ip access-list standard Users
 10 permit 192.168.1.0 0.0.0.255
!
route-map Users permit 10
 match ip address Users
```

Which action completes the configuration to achieve a dynamic continuous mapped NAT for all users?

A. Increase the NAT pool size to support 254 usable addresses
B. Reconfigure the pool to use the 192.168.1.0 address range
C. Configure a match-host type NAT pool
D. Configure a one-to-one type NAT pool

Answer: A

Question 3

A customer has 20 stores located throughout a city. Each store has a single Cisco AP managed by a central WLC. The customer wants to gather analytics for users in each store. Which technique supports these requirements?

A. hyperlocation
B. angle of arrival
C. presence
D. trilateration

Answer: C

Explanation

We only have one AP in each store so we can only user “Presence”, which is the most basic form of location tracking.

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKEWN-2012.pdf

Question 4

What is a characteristic of a WLC that is in master controller mode?

A. The master controller is responsible for load balancing all connecting clients to other controllers.
B. Configuration on the master controller is executed on all wireless LAN controllers.
C. All wireless LAN controllers are managed by the master controller.
D. All new APs that join the WLAN are assigned to the master controller.

Answer: D

Explanation

When should I use the master controller mode on a WLC?
– When there is a master controller enabled, all newly added access points with no primary, secondary, or tertiary controllers assigned associate with the master controller on the same subnet.

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html

Question 5

A customer has a pair of Cisco 5520 WLCs set up in an SSO cluster to manage all APs. Guest traffic is anchored to a Cisco 3504 WLC located in a DM2. Which action is needed to ensure that the EoIP tunnel remains in an UP state in the event of failover on the SSO cluster?

A. Configure back-to-back connectivity on the RP ports
B. Use the mobility MAC when the mobility peer is configured
C. Enable default gateway reachability check
D. Use the same mobility domain on all WLCs

Answer: B

Explanation

In order to keep the mobility network stable without any manual intervention and in the event of failure or switchover, the back-and-forth concept of Mobility MAC has been introduced.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/High_Availability_DG.html

Question 6

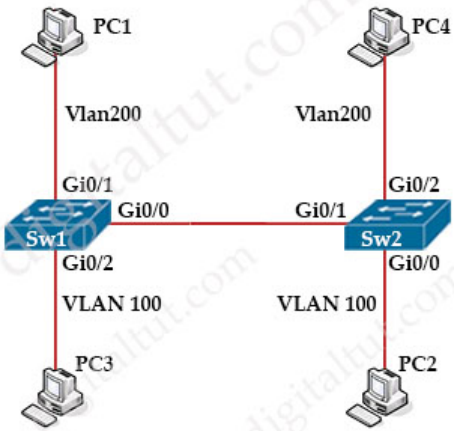
In a Cisco DNA Center Plug and Play environment, why would a device be labeled unclaimed?

A. The device has not been assigned a workflow.
B. The device could not be added to the fabric.
C. The device had an error and could not be provisioned.
D. The device is from a third-party vendor.

Answer: A

Question 7

Refer to the exhibit.




```
SW1#show interfaces gigabitethernet0/0 switchport
Name:Gi0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrtive Native VLAN tagging: enabled
Voice VLAN: none
---output omitted---

SW2#show interfaces gigabitethernet0/1 switchport
Name:Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (NATIVE)
Administrtive Native VLAN tagging: enabled
Voice VLAN: none
---output omitted---
```

The connection between SW1 and SW2 is not operational. Which two actions resolve the issue? (Choose two)

A. configure switchport mode access on SW2
B. configure switchport nonegotiate on SW2
C. configure switchport mode trunk on SW2
D. configure switchport mode dynamic desirable on SW2
E. configure no switchport nonegotiate on SW1

Answer: D E

Explanation

From the outputs (line: “Administrative Mode: dynamic auto”) we notice that both interfaces were configured with “dynamic auto” mode so they cannot form a trunking link. We need to change one of them to “dynamic desirable” mode to activate the trunk -> Answer D is correct.

Another problem is SW1 was set to “nonegotiate” (from the line: “Negotiation of Trunking: Off”) which prevents DTP negotiation packets from being sent out the interface. We need to re-enable with the “no switchport nonegotiate” command -> Answer E is correct.

For your reference, the table below lists trunking condition:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Question 8

Refer to the exhibit.

```
R1#show access-list 100
Extended IP access list 100
 10 deny ip any any
 20 permit ip 192.168.0.0 0.0.255.255 any
 30 permit ip any 192.168.0.0 0.0.255.255
```

Option A R1(config)#no access-list 100 deny ip any any	**Option B** R1(config)#ip access-list extended 100 R1(config-ext-nacl)#5 permit ip any any
Option C R1(config)#ip access-list extended 100 R1(config-ext-nacl)#no 10	**Option D** R1(config)#no access-list 100 seq 10 R1(config-ext-nacl)#access-list 100 seq 40 deny ip any any

Extended access-list 100 is configured on interface GigabitEthernet0/0 in an inbound direction, but it does not have the expected behavior of allowing only packets to or from 192.168.0.0/16. Which command set properly configures the access list?

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation

The first ACL statement of “10 deny ip any any” will match and drop all traffic so we have to remove this statement.

Question 9

How do cloud deployments differ from on-prem deployments?

A. Cloud deployments require longer implementation times than on-premises deployments
B. Cloud deployments are more customizable than on-premises deployments.
C. Cloud deployments have lower upfront costs than on-premises deployments.
D. Cloud deployments require less frequent upgrades than on-premises deployments.

Answer: C

Question 10

Refer to the exhibit.

```
#!/usr/bin/env python
import json
import sys

test_json="""
{
  "type: "Cisco ASR 1001-x Router",
  "lastUpdateTime": 144393848493,
  "macAddress": "00:c8:8b:e3:24:22",
  "serialNumber": "FXS1932Q1SE"
}
"""
print(json.load(test_json))
```

```
Output
$ python printjson.py
Traceback (most recent call last):
File "question_3.py", line 15, in <module>
Print(json.load(test_json))
File
"/System/Library/Framework/Python.framework/Versions/2.7/lib/python2.7/json/_init_ py",
 line 286 in load return loads (fp.read(),
AttributeError: str' object has no attribute 'read'
```

An engineer runs the sample code, and the terminal returns this output. Which change to the sample code corrects this issue?

A. Change the JSON method from load() to loads().
B. Enclose null in the test_json string in double quotes
C. Use a single set of double quotes and condense test_json to a single line
D. Call the read() method explicitly on the test_json string

Answer: A

Explanation

An example of json.loads() is shown below:

```
C:\WINDOWS\system32>python
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC v.1914 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import json
>>> json_string = """
...
... {
...  "ins_api": {
...   "type": "cli_show",
...   "version":"1.0",
...   "sid":"eoc",
...   "outputs":{
...    "output":{
...     "input":"show version",
...     "msg":"Success",
...     "code":"200",
...     "body":{
...      "bios_ver_str":"07.61",
...      "kickstart_ver_str":"7.0(3)I7(4)",
...      "bios_cmpl_time":"04/08/2017",
...      "kick_file_name":"bootflash:///nxos.7.0.3.I7.4.bin",
...      "kick_cmpl_time":"6/14/1970 09:49:04",
...      "chassis_id": "Nexus9000 93180YC-EX chassis",
...      "cpu_name": "Intel(R) Xeon(R) CPU @1.80GHz",
...      "memory": 24633488,
...      "mem_type":"kB",
...      "rr_usecs":134703,
...      "rr_ctime":"Mon Jun 10 12:34:46 2019",
...      "rr_reason": "Reset Requested by CLI command reload",
...      "rr_sys_ver":"7.0(3)I7(4)",
...      "rr_service":"",
...      "manufacturer": "Cisco Systems, Inc",
...      "TABLE_package_list": {
...       "ROW_package_list": {
...        "package_id": {}
...       }
...      }
...     }
...    }
...   }
...  }
... }
...
... """
>>> response = json.loads(json_string)
>>>
>>> print(response['ins_api']['outputs']['output']['body']['kickstart_ver_str'])
7.0(3)I7(4)
>>>
```

Note: Triple quotes (“””) in Python allows strings to span multiple lines, including verbatim NEWLINEs, TABs, and any other special characters.

Question 11

Refer to the exhibit.

```
Switch2#
02:23:22: %PM-4-ERR_DISABLE: channel-misconfig error
detected on Fa0/23, putting Fa0/23 in err-disable state
02:23:22: %PM-4-ERR_DISABLE: channel-misconfig error
detected on Fa0/24, putting Fa0/24 in err-disable state
Switch2#

Switch1# show etherchannel summary
--output omitted--

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------
1      Po2(SD)         LACP      Fa1/0/23(D)

Switch2# show etherchannel summary
--output omitted--

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------
1      Po1(SD)         -         Fa0/23(D) Fa0/24(D)
```

An engineer is configuring an EtherChannel between Switch1 and Switch2 and notices the console message on Switch2. Based on the output, which action resolves this issue?

A. Configure the same port channel interface number on both switches
B. Configure less member ports on Switch2
C. Configure more member ports on Switch1
D. Configure the same EtherChannel protocol on both switches

Answer: D

Explanation

In this case, we are using your EtherChannel without a negotiation protocol on Switch2. As a result, if the opposite switch is not configured for EtherChannel operation on the respective ports either, there is a danger of a switching loop. The EtherChannel Misconfiguration Guard tries to prevent that loop from occurring by disabling all the ports bundled in the EtherChannel.

Question 12

An engineer is concerned with the deployment of a new application that is sensitive to inter-packet delay variance. Which command configures the router to be the destination of jitter measurements?

A. Router(config)# ip sla responder udp-connect 172.29.139.134 5000
B. Router(config)# ip sla responder tcp-connect 172.29.139.134 5000
C. Router(config)# ip sla responder udp-echo 172.29.139.134 5000
D. Router(config)# ip sla responder tcp-echo 172.29.139.134 5000

Answer: C

Explanation

Cisco IOS IP SLA Responder is a Cisco IOS Software component whose functionality is to respond to Cisco IOS IP SLA request packets. The IP SLA source sends control packets before the operation starts to establish a connection to the responder. Once the control packet is acknowledged, test packets are sent to the responder. **The responder inserts a time-stamp when it receives a packet** and factors out the destination processing time **and adds time-stamps to the sent packets**. This feature allows the calculation of unidirectional packet loss, latency, and jitter measurements with the kind of accuracy that is not possible with ping or other dedicated probe testing.

Reference: https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb52.html

UDP Jitter measures the delay, delay variation (jitter), corruption, misordering and packet loss by generating periodic UDP traffic. This operation always requires IP SLA responder.

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKNMS-3043.pdf

The command to enable UDP Jitter Operation is "**ip sla responder udp-echo** {*destination-ip-address*} [*destination-port*]

Question 13

Which resource is able to be shared among virtual machines deployed on the same physical server?

A. VM configuration file
B. operating system
C. disk
D. applications

Answer: C

Question 14

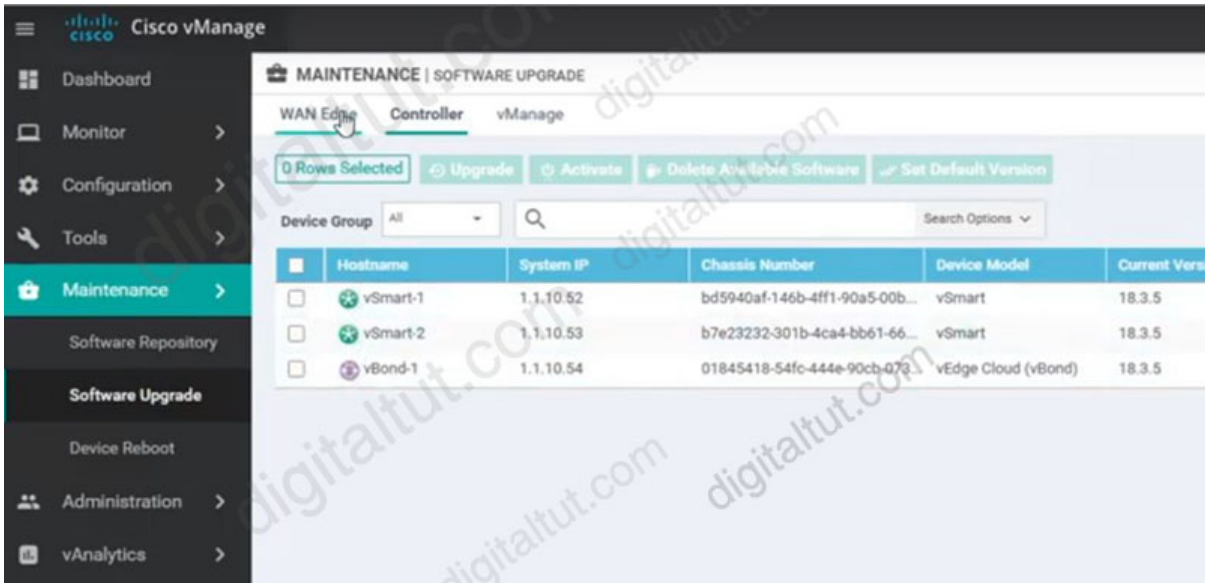
Which function is handled by vManage in the Cisco SD-WAN fabric?

A. Establishes IPsec tunnels with nodes
B. Distributes policies that govern data forwarding
C. Performs remote software upgrades for WAN Edge, vSmart and vBond
D. Establishes BFD sessions to test liveliness of links and nodes

Answer: C

Explanation

We can remote upgrades WAN Edge, vSmart and vBond in vManage.



Question 15

Refer to the exhibit.

```
switch1(config)# interface GigabitEthernet 1/1
switch1(config-if)# switchport mode trunk
switch1(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-90
switch1(config)# exit
switch1(config)# monitor session 1 source vlan 10
switch1(config)# monitor session 1 destination remote vlan 70

switch2(config)# interface GigabitEthernet 1/1
switch2(config-if)# switchport mode trunk
switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,80-90
switch2(config)# exit
switch2(config)# monitor session 2 source remote vlan 70
switch2(config)# monitor session 2 destination interface GigabitEthernet1/1
```

A network administrator configured RSPAN to troubleshoot an issue between switch1 and switch2. The switches are connected using interface GigabitEthernet 1/1. An external packet capture device is connected to switch2 interface GigabitEthernet1/2. Which two commands must be added to complete this configuration? (Choose two)

Option A switch1(config)# interface GigabitEthernet 1/1 switch1(config-if)# switchport mode access switch1(config-if)# switchport access vlan 10 switch2(config)# interface GigabitEthernet 1/1 switch2(config-if)# switchport mode access switch2(config-if)# switchport access vlan 10	**Option B** switch2(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70-80
Option C switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/1	**Option D** switch2(config)# monitor session 2 destination vlan 10
Option E switch2(config)# monitor session 1 source remote vlan 70 switch2(config)# monitor session 1 destination interface GigabitEthernet1/2	

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Answer: B E

Explanation

Switch2 is not allowing VLAN 70 which is used on Switch1 for RSPAN so we must allow it -> Option B is correct (although it would not allow VLAN 81 to 90 to go through).

“An external packet capture device is connected to switch2 interface GigabitEthernet1/2” so we must configure Gi1/2 as the destination port.

For your information, this is how to configure Remote SPAN (RSPAN) feature on two switches. Traffic on FastEthernet0/1 of Switch 1 will be sent to Fa0/10 of Switch2 via VLAN 40.

+ Configure on both switches
Switch1,2(config)#vlan 40
Switch1,2(config-vlan)#remote-span
+ Configure on Switch1
Switch1(config)# monitor session 1 source interface FastEthernet 0/1
Switch1(config)# monitor session 1 destination remote vlan 40
+ Configure on Switch2
Switch2(config)#monitor session 5 source remote vlan 40
Switch2(config)# monitor session 5 destination interface FastEthernet 0/10

Question 16

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. Which action completes the configuration?

A. action 4.0 syslog command “show process cpu sorted | append flash:high-cpu-file”
B. action 4.0 publish-event “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 cli command “show process cpu sorted | append flash:high-cpu-file”

Answer: D

Question 17

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"][2]["description"]
u'my description'
```

Which Python code snippet prints the descriptions of disabled interfaces only?

Option A

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

Option B

```
for interface in netconf_data["GigabitEthernet"]:
    if interface["disabled"] != 'true':
        print(interface["description"])
```

Option C

```
for interface in netconf_data["GigabitEthernet"]:
    if interface["enabled"] != 'true':
        print(interface["description"])
```

Option D

```
for interface in netconf_data["GigabitEthernet"]:
    if interface["enabled"] != 'false':
        print(interface["description"])
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation

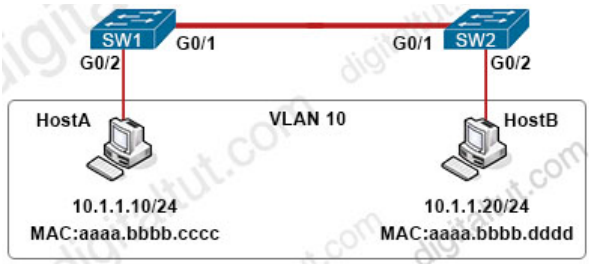
We need a “if” condition here to find out disabled interfaces so Option A is not correct.

From the exhibit, we learn that the “netconf_data” array only has “enabled” element. It does not have “disabled” element so Option B is not correct.

If “enabled” element is not “true” (interface[“enabled”] != ‘true’) then it is a disable interface -> Option C is correct.

Question 18

Refer to the exhibit.



An engineer must deny HTTP traffic from host A to host B while allowing all other communication between the hosts. Which command set accomplishes this task?

Option A SW1(config)# ip access-list extended DENY-HTTP SW1(config-ext-nacl)#deny tcp host 10.1.1.10 host 10.1.1.20 eq www SW1(config)# ip access-list extended MATCH_ALL SW1(config-ext-nacl)#permit ip any any SW1(config)# vlan access-map HOST-A-B 10 SW1(config-access-map)# match ip address DENY-HTTP SW1(config-access-map)# action drop	**Option B** SW1(config)# ip access-list extended DENY-HTTP SW1(config-ext-nacl)#permit tcp host 10.1.1.10 host 10.1.1.20 eq www SW1(config)# ip access-list extended MATCH_ALL SW1(config-ext-nacl)# permit ip any any SW1(config)# vlan access-map HOST-A-B 10 SW1(config-access-map)# match ip address DENY-HTTP SW1(config-access-map)# action drop SW1(config)# vlan access-map HOST-A-B 20 SW1(config-access-map)# match ip address MATCH_ALL SW1(config-access-map)# action forward SW1(config)# vlan filter HOST-A-B vlan 10
Option C SW1(config)# mac access-list extended HOST-A-B SW1(config-ext-mac)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd SW1(config)# ip access-list extended DENY-HTTP SW1(config-ext-nacl)#permit tcp host 10.1.1.10 host 10.1.1.20 eq www SW1(config)# vlan access-map DROP-MAC 10 SW1(config-access-map)# match mac address HOST-A-B SW1(config-access-map)# action forward SW1(config)# vlan access-map HOST-A-B 20 SW1(config-access-map)# match ip address DENY-HTTP SW1(config-access-map)# action drop SW1(config)# vlan filter HOST-A-B vlan 10	**Option D** SW1(config)# mac access-list extended HOST-A-B SW1(config-ext-nacl)# permit host aaaa.bbbb.cccc aaaa.bbbb.dddd SW1(config)# ip access-list extended DENY-HTTP SW1(config-ext-nacl)#deny tcp host 10.1.1.10 host 10.1.1.20 eq www SW1(config)#vlan access-map DROP-MAC 10 SW1(config-access-map)# match mac address HOST-A-B SW1(config-access-map)# action drop SW1(config)# vlan access-map HOST-A-B 20 SW1(config-access-map)# match ip address DENY-HTTP SW1(config-access-map)# action drop

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Explanation

In this case we need to configure a VLAN access-map to deny HTTP traffic and apply it to VLAN 10. To do it, first create an access-list, by which interesting traffic will be matched. The principle of VLAN access-map config is similar to the route-map principle.

After this we'll create a vlan access-map, which has two main parameters: action and match.
Match: by this parameter the interesting traffic is matched and here RACL or MAC ACL can be applied as well.
Action: what to do with matched traffic. Two main parameters exist: Drop and Forward. In case of Drop, matched traffic will be dropped, and in case of forward, matched traffic will be allowed.

A good reference and example can be found at https://www.networkstraining.com/vlan-access-map-example-configuration/

Question 19

Which of the following statements regarding BFD are correct? (Choose two)

A. BFD is supported by OSPF, EIGRP, BGP, and IS-IS.
B. BFD detects link failures in less than one second.
C. BFD can bypass a failed peer without relying on a routing protocol.
D. BFD creates one session per routing protocol per interface.
E. BFD is supported only on physical interfaces.
F. BFD consumes more CPU resources than routing protocol timers do.

Answer: A B

Question 20

What is an advantage of using BFD?

A. It local link failure at layer 1 and updates routing table
B. It detects local link failure at layer 3 and updates routing protocols
C. It has sub-second failure detection for layer 1 and layer 3 problems.
D. It has sub-second failure detection for layer 1 and layer 2 problems.

Answer: C

Question 21

An engineer measures the Wi-Fi coverage at a customer site. The RSSI values are recorded as follows:

Location A: -72 dBm
Location B: -75 dBm
Location C: -85 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 signal strength at location B is 10 dB better than location C
E. The RF signal strength at location C is 10 times stronger than location B

Answer: A C

Explanation

Understanding Signal Strength

The most accurate way to express it is with milliwatts (mW), but you end up with tons of decimal places due to WiFi's super-low transmit power, making it difficult to read. For example, -40 dBm is 0.0001 mW, and the zeros just get more intense the more the signal strength drops.

Ultimately, the easiest and most consistent way to express signal strength is with dBm, which stands for decibels relative to a milliwatt.

You can convert between mW and dBm using the following formulas:

$P(dBm) = 10 \cdot \log_{10}(P(mW))$
For example, a power of 2.5 mW in dBm is:
$dBm = 10\log 2.5 = 3.979$

dBm is that we're working in negatives. -30 is a higher (stronger) signal than -80.

Signal Strength	Rating		Required for

Signal Strength	Rating		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWiFi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

3 dB of gain = **+3 dB = doubles signal strength** (Let's say, the base is P. So 10*log10(P/P)= 0 dB and 10*log10(2P/P) = 10*log10(2) = 3dB -> double signal)
3 dB of loss = **-3 dB = halves signal strength strength** (10*log(½) = -3.0103)
10 dB of loss = **-10 dB = 10 times less** signal strength (0.1 mW = -10 dBm, 0.01 mW = -20 dBm, etc.)
10 dB of gain = **+10 dB = 10 times more** signal strength (0.00001 mW = -50 dBm, 0.0001 mW = -40 dBm, etc.)

Reference: https://www.metageek.com/training/resources/wifi-signal-strength-basics.html

Simple rule of thumb:
When working with power, 3 dB means double (twice) the factor and 10 dB means 10-fold.

Question 22

Which three resources must the hypervisor make available to the virtual machines? (Choose three)

A. memory
B. IP address
C. processor
D. bandwidth
E. secure access
F. storage

Answer: A C F

========== New Questions (added on 16th-Apr-2021) ==========

Question 23

Which unit is used to express the signal-to-noise ratio?

A. dBm
B. dB
C. amp
D. mW

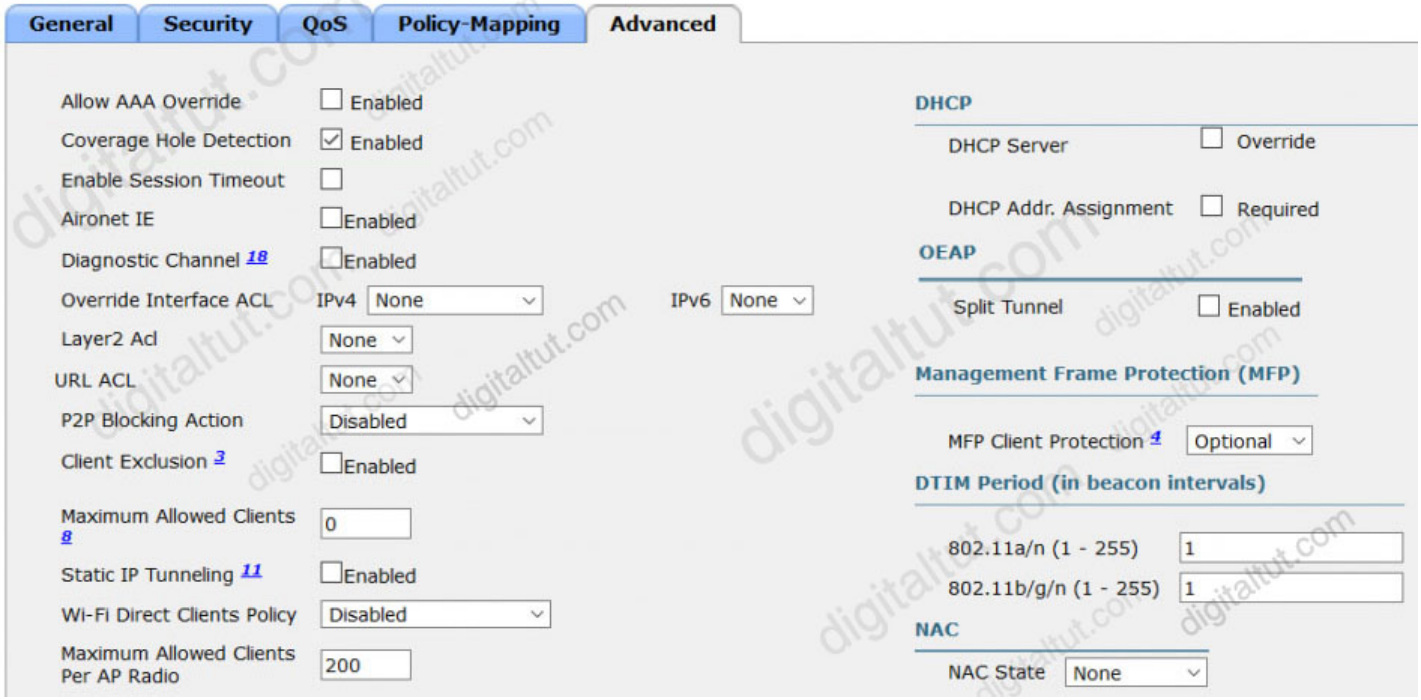
Answer: B

Explanation

Signal-to-noise ratio (SNR or S/N) is the ratio of signal power to the noise power, and its unit of expression is typically decibels (dB).

Question 24

Refer to the exhibit.



An engineer is investigating why guest users are able to access other guest devices when the users are connected to the customer guest WLAN. What action resolves this issue?

A. implement P2P blocking
B. implement MFP client protection
C. implement split tunneling
D. implement Wi-Fi direct policy

Answer: A

Question 25

Which function does a fabric AP perform in a Cisco SD-Access deployment?

A. It manages wireless clients' membership information in the fabric
B. It connects wireless clients to the fabric.
C. It updates wireless clients' locations in the fabric
D. It configures security policies down to wireless clients in the fabric

Answer: B

Question 26

Which design principle should be followed in a Cisco SD-Access wireless network deployment?

A. The WLC is part of the fabric overlay
B. The WLC is part of the fabric underlay
C. The WLC is connected outside of the fabric
D. The access point is connected outside of the fabric

Answer: A

Comments

1. MariaMashABabko
   April 11th, 2021

   Thanks Digital!