Type text to search here...

Home > New ENCOR Questions – Part 5

New ENCOR Questions – Part 5

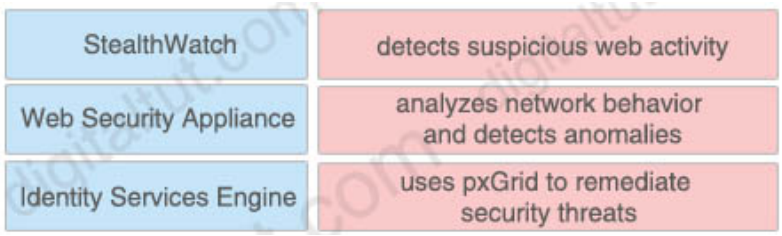
February 24th, 2021 in New ENCOR Questions Go to comments

Note: The New ENCOR Questions Part 1 to Part 3 have been classified into specific topics so we removed them.

Premium Member: You can practice these questions first via these links:
+ Question 1 to 15
+ Question 16 to 38
+ Question 39 to end

Question 1

Drag and drop the solutions that comprise Cisco Cyber Threat Defense from the left onto the objectives they accomplish on the right.



Answer:

+ detects suspicious web activity: Web Security Appliance
+ analyzes network behavior and detects anomalies: StealthWatch
+ uses pxGrid to remediate security threats: Identity Services Engine

Explanation

Cisco ISE collects dynamic contextual data from throughout the network and **uses Cisco pxGrid technology**, a robust context-sharing platform, to share that deeper level of contextual data about connected users and devices with external and internal ecosystem partner solutions. Through the use of a single API, Cisco ISE network and security partners use this data in order to improve their own network access capabilities and accelerate their solutions' capabilities to identify, mitigate, and remediate network threats.

StealWatch: performs security analytics by collecting network flows via NetFlow

Question 2

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

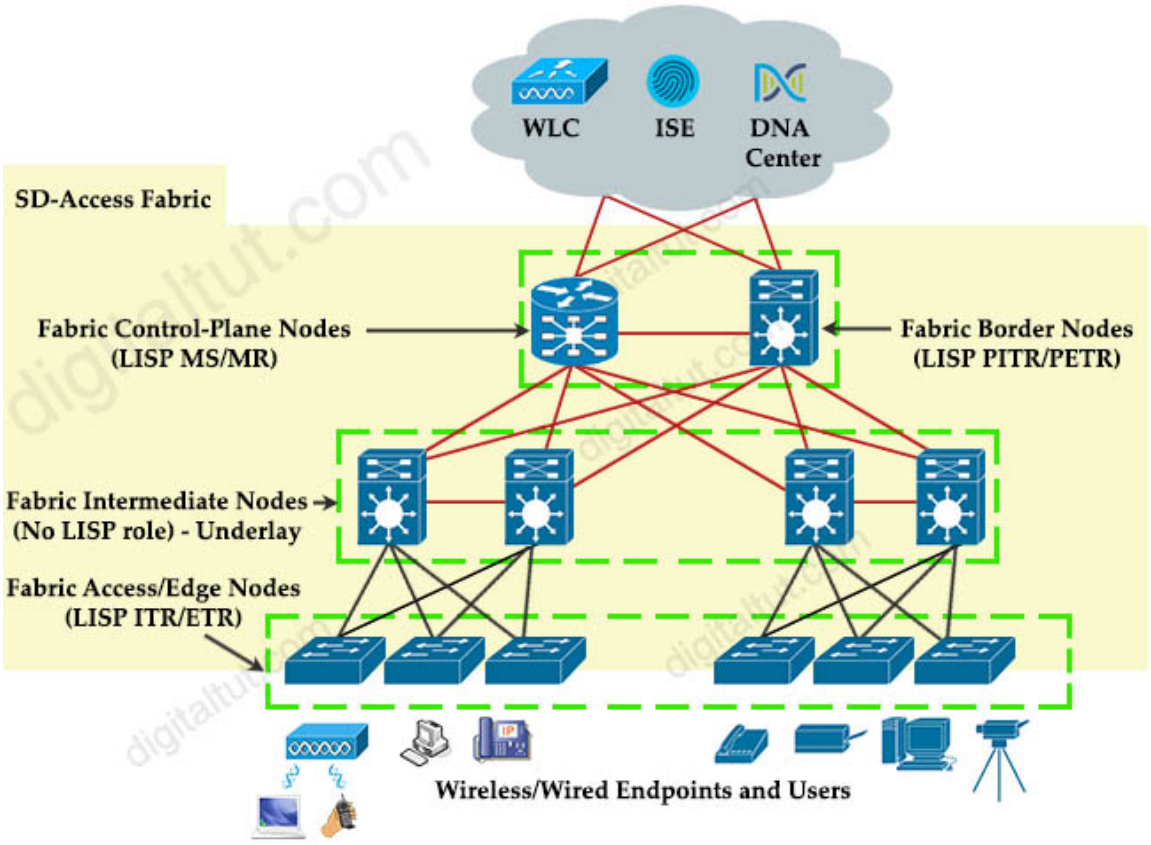
A. Fabric endpoints are connected directly to the border node
B. The border node is required for communication between fabric and nonfabric devices
C. The control plane node has the full RLOC-to-EID mapping database
D. Traffic within the fabric always goes through the control plane node

E. The border node has the full RLOC-to-EID mapping database

Answer: B C

Explanation

There are five basic device roles in the fabric overlay:
+ Control plane node: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
+ Fabric border node: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
+ Fabric edge node: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
+ Fabric WLAN controller (WLC): This fabric device connects APs and wireless endpoints to the SDA fabric.
+ Intermediate nodes: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.



Reference: CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Question 3

Refer to the exhibit.

```
Current configuration: 142 bytes
vrf definition STAFF
!
!
interface GigabitEthernet1
 vrf forwarding STAFF
 no ip address
 negotiation auto
 no mop enabled
```

```
 no mop sysid
end
```

An engineer must assign an IP address of 192.168.1.1/24 to the GigabitEthemet1 interface. Which two commands must be added to the existing configuration to accomplish this task? (Choose two)

A. Router(config-vrf)#address-family ipv6
B. Router(config-if)#ip address 192.168.1.1 255.255.255.0
C. Router(config-vrf)#ip address 192.168.1.1 255.255.255.0
D. Router(config-if)#address-family ipv4
E. Router(config-vrf)#address-family ipv4

Answer: B E

Explanation

In fact we only need to assign IP address to Gi1 with the command “Router(config-if)#ip address 192.168.1.1 255.255.255.0”. The command “Router(config-vrf)#address-family ipv4” is unnecessary unless we have other configurations.

Question 4

What is the data policy in a Cisco SD-WAN deployment?

A. list of ordered statements that define node configurations and authentication used within the SD-WAN overlay
B. Set of statements that defines how data is forwarded based on IP packet information and specific VPNs
C. detailed database mapping several kinds of addresses with their corresponding location
D. group of services tested to guarantee devices and links liveliness within the SD-WAN overlay

Answer: B

Explanation

Data policy operates on the data plane in the Cisco SD-WAN overlay network and affects how data traffic is sent among Cisco SD-WAN devices in the network. The Cisco SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on the devices.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/sda_fabric_troubleshooting/b_cisco_sda_fabric_troubleshooting_guide.html

Question 5

Refer to the exhibit.

```
SW2# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------
1      Po1(SD)         PAgP      Gi0/0(I)   Gi0/1(I)


SW3# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------
1      Po1(SD)         LACP      Gi0/0(I)   Gi0/1(I)
```

Which action resolves the EtherChannel issue between SW2 and SW3?

A. Configure switchport mode trunk on SW2
B. Configure switchport nonegotiate on SW3
C. Configure channel-group 1 mode desirable on both interfaces
D. Configure channel-group 5 mode active on both interfaces

Answer: C

Explanation

From the output we learn that SW2 is running PAgP while Sw3 is running LACP so they cannot form Etherchannel. Therefore we need to configure only LACP (active mode) or PAgP (desirable mode) on both switches. But we have to configure on the existing “channel-group 1”, not group 5.

Question 6

Refer to the exhibit.

```
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 72.16.30.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 72.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled     Shutdown    Topology Name
       0           1       no           no          Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.29, Interface address 172.16.30.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 72.16.11.29/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 72.16.11.29, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled     Shutdown    Topology Name
       0           1       no           no          Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 172.16.11.27, Interface address 172.16.11.27
  Backup Designated router (ID) 172.16.11.30, Interface address 172.16.11.30
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  ! lines omitted for brevity
```

A network engineer configures OSPF and reviews the router configuration. Which interface or interfaces are able to establish OSPF adjacency?

A. GigabitEthemet0/1 and GigabitEthernet0/1.40
B. Gigabit Ethernet0/0 and GigabitEthemet0/1
C. only GigabitEthernet0/0
D. only GigabitEthernet0/1

Answer: C

Explanation

This is the output of command “show ip ospf interface”. From the line “No hellos (Passive interface)”, we learn that interface Gi0/1 was configured passive interface -> It cannot establish OSPF adjacency. Only Gi0/0 established OSPF adjacency.

Note: DROTHER is just a sign of FULL state in OSPF but this router is not a DR or BDR. Therefore DROTHER means interface was established adjacency successfully with the neighbor interface.

Question 7

Refer to the exhibit.

```
TYPE    PROT SYSTEM IP   ID        ID       PRIVATE IP                      PORT
PUBLIC IP                          PORT   LOCAL COLOR     PROXY STATE UPTIME    ID
-------------------------------------------------------------------------------------
----------
vsmart  dtls 0.0.0.0     100       1       192.168.100.80
12346 10.10.20.70                        12446 default           No    up
0:02:24:09   0
vbond   dtls 0.0.0.0     0         0       192.168.100.81
12346 10.10.20.80                        12346 default           -     up
0:02:24:10   0
vmanage dtls 4.4.4.90    100       0       192.168.100.82
12446 10.10.20.90                        12446 default
```

What step resolves the authentication issue?

A. restart the vsmart host
B. target 192.168.100.82 in the URI
C. change the port to 12446
D. use basic authentication

Answer: B

Explanation

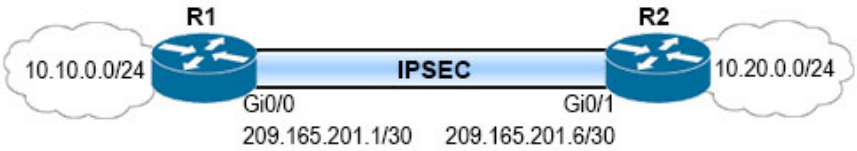
The first figure is the output of the “show control connections” command. From this figure we learned that the vManage IP address is 192.168.100.82 so we need to connect to this IP address (not 192.168.100.80).

Question 8

Refer to the exhibit.

```
access-list 100 permit gre host 209.165.201.1 host 209.165.201.6

crypto isakmp policy 5
 authentication pre-share
 hash sha256
 encryption aes
 group 14

crypto isakmp key D@t@c3nt3r address 209.165.201.6

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
 mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.6
 set transform-set My_Set
 match address 100

interface GigabitEthernet0/0
 description outside_interface
 no switchport
 ip address 209.165.201.1 255.255.255.252
 crypto map MAP

interface Tunnel 100
 ip address 192.168.100.1 255.255.255.0
 ip mtu 1400
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.201.6

ip route 10.20.0.0 255.255.255.0 192.168.100.2 Tunnel100
```

```
access-list 100 permit gre host 209.165.201.6 host 209.165.201.1

crypto isakmp policy 5
 authentication pre-share
 hash sha256
 encryption aes
 group 14

crypto isakmp key D@t@c3nt3r  address 209.165.201.1

crypto ipsec transform-set My_Set esp-aes esp-sha-hmac
 mode transport

crypto map MAP 10 ipsec-isakmp
 set peer 209.165.201.1
 set transform-set My_Set
 match address 100

interface GigabitEthernet0/1
 description outside_interface
 no switchport
 ip address 209.165.201.6 255.255.255.252
 crypto map MAP

interface Tunnel 100
 ip address 192.168.100.2 255.255.255.0
 ip mtu 1400
 tunnel source GigabitEthernet0/0
 tunnel destination 209.165.201.1

ip route 10.10.0.0 255.255.255.0 192.168.100.1 Tunnel100
```



A network engineer must simplify the IPsec configuration by enabling IPsec over GRE using IPsec profiles. Which two configuration changes accomplish this? (Choose two)

A. Apply the crypto map to the tunnel interface and change the tunnel mode to tunnel mode ipsec ipv4
B. Remove all configuration related to crypto map from R1 and R2 and eliminate the ACL 100
C. Remove the crypto map and modify the ACL to allow traffic between 10.10.0.0/24 to 10.20.0.0/24
D. Create an IPsec profile, associate the transform-set, and apply the profile to the tunnel interface

Answer: A D

Question 9

Which encryption hashing algorithm does NTP use for authentication?

A. SSL
B. AES256
C. AES128
D. MD5

Answer: D

Explanation

An example of configuring NTP authentication is shown below:

Router1(config)#ntp authentication-key 2 md5 9tut
Router1(config)#ntp authenticate
Router1(config)#ntp trusted-key 2

Question 10

What is a VPN in a Cisco SD-WAN deployment?

A. virtual channel used to carry control plane information
B. attribute to identify a set of services offered in specific places in the SD-WAN fabric
C. common exchange point between two different services
D. virtualized environment that provides traffic isolation and segmentation in the SD-WAN fabric

Answer: D

Question 11

Drag and drop the characteristic from the left onto the orchestration tools that they describe on the right.

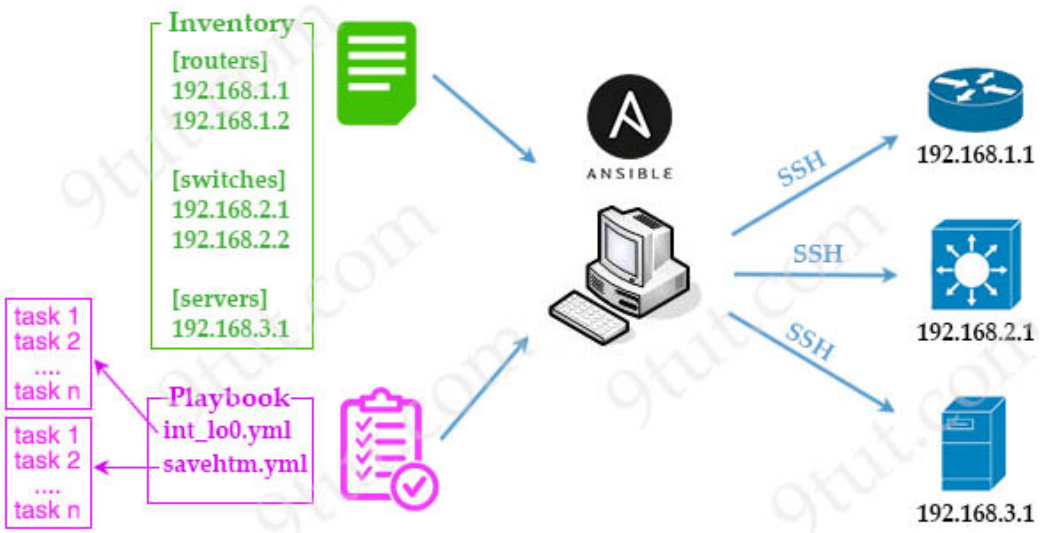
Answer:

Ansible:
+ uses playbooks
+ prodedural

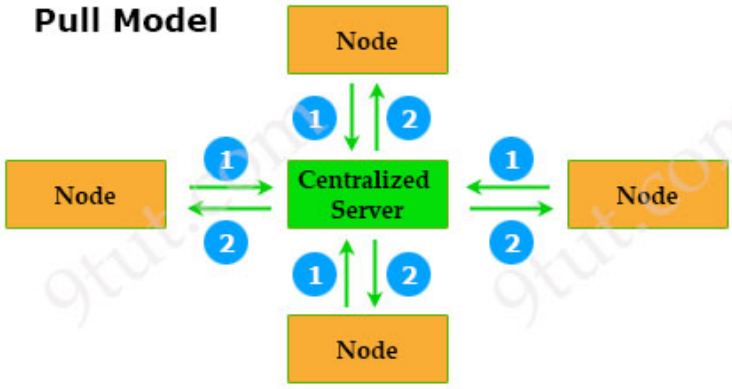
Puppet:
+ uses a pull model
+ declarative

Explanation

In Ansible, **Playbooks** are files that provide actions and logic about what Ansible should do. Ansible playbooks are files that contain tasks to configure hosts. Ansible playbooks are written in YAML format.



Puppet is based on a Pull deployment model, where the nodes check in regularly after every 1800 seconds with the Master to see if anything needs to be updated in the agent. If anything needs to be updated the agent pulls the necessary Puppet codes from the Master and performs required actions.



Chef and Ansible encourage a procedural style where you write code that specifies, step-by-step, how to to achieve some desired end state. Terraform, SaltStack, and Puppet all encourage a more declarative style where you write code that specifies your desired end state, and the IAC tool itself is responsible for figuring out how to achieve that state.

Question 12

Refer to the exhibit.


```
London(config)#interface fa0/1
London(config-if)#switchport trunk encapsulation dot1q
London(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

London(config-if)#end
NewYork#show dtp interface fa0/1
DTP information for FastEthernet0/1:
    TOS/TAS/TNS:            ACCESS/AUTO/ACCESS
    TOT/TAT/TNT:            NATIVE/ISL/NATIVE
```

Communication between London and New York is down. Which command set must be applied to resolve this issue?

Option A	**Option B**
NewYork(config)#int f0/1 NewYork(config)#switchport nonegotiate NewYork(config)#end NewYork#	NewYork(config)#int f0/1 NewYork(config)#switchport trunk encap dot1q NewYork(config)#end NewYork#
Option C	**Option D**
NewYork(config)#int f0/1 NewYork(config)#switchport mode dynamic desirable NewYork(config)#end NewYork#	NewYork(config)#int f0/1 NewYork(config)#switchport mode trunk NewYork(config)#end NewYork#

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

Answer: B

Explanation

From the output line “TOT/TAT/TNT: NATIVE/ISL/NATIVE”, we see interface f0/1 of NewYork router is hard coded ISL which is mismatched with 802.1Q so we have to change trunking encapsulation on NewYork router to 802.1Q.

Note: The TOS/TAS/TNS of “ACCESS/AUTO/ACCESS” shows it is currently operating as an Access Port, in Dynamic Auto mode, and its negotiated to be an Access Port (but it can be negotiated to become a trunk port).

Good reference: https://loopedback.com/2017/08/26/dtp-dynamic-trunking-protocol-the-exam-information-and-a-lot-of-live-cli-output-to-demonstrate-behaviors-of-dtp/

Note:

TOS = Trunk Operational Status
TAS = Trunk Administrative Status
TNS = Trunk Negotiation Status
TOT = Trunk Operational Type
TAT = Trunk Administrative Type
TNT = Trunk Negotiation Type

Question 13

What is an emulated machine that has dedicated compute, memory, and storage resources and a fully installed operating system?

A. host
B. virtual machine
C. container
D. mainframe

Answer: B

Question 14

Which two methods are used to reduce the AP coverage area? (Choose two)

A. Reduce AP transmit power
B. Increase minimum mandatory data rate
C. Reduce channel width from 40 MHz to 20 MHz
D. Enable Fastlane
E. Disable 2.4 GHz and use only 5 GHz

Answer: A B

Explanation

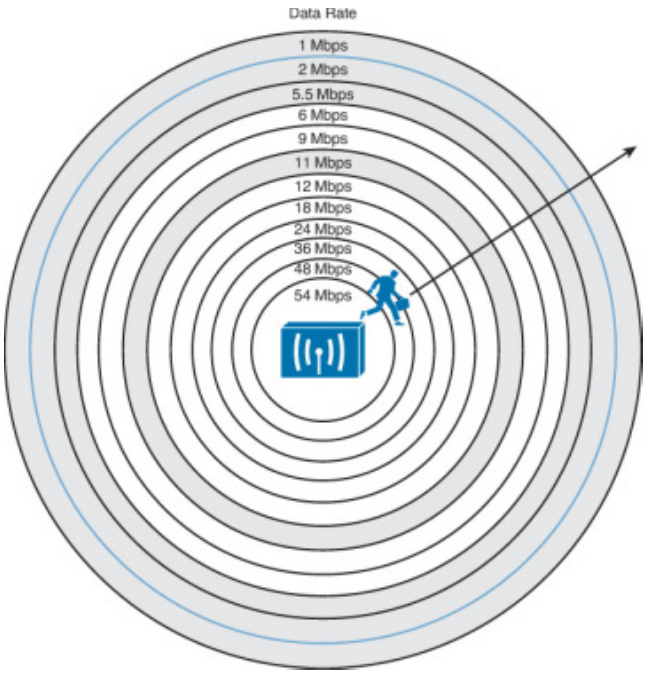
The **transmit power of an AP affects the wireless coverage area** and the maximum achievable signal-to-noise ratio. Proper configuration of transmit power is important for ensuring a wireless network is operating at its highest capacity.

Reference: https://documentation.meraki.com/MR/Radio_Settings/Transmit_Power_and_Antenna_Configuration

AP coverage area or the cell size, according to this Cisco link, there are two ways to reduce the AP coverage area:
+ Tuning Cell Size with Transmit Power
+ Tuning Cell Size with Data Rates

Setting the transmit power level is a simplistic approach to defining the cell size, but that is not the only variable involved. The cell size of an AP is actually a compromise between its transmit power and the data rates that it offers.

To design a wireless LAN for best performance, you would most likely need to **disable some of the lower data rates**. For example, you could disable the 1, 2, and 5.5 Mbps rates to force clients to use higher rates and better modulation and coding schemes. That would improve throughput for individual clients and would also benefit the BSS as a whole by eliminating the slower rates that use more time on a channel.



-> Therefore increasing minimum mandatory data rate would reduce coverage area but enhance performance.

Question 15

Which data is properly formatted with JSON?

Option A
{
"name": "Peter"
"age": "25"
"likesJson": true
"characteristics": ["small","strong",18]
}
	Option B
	{
	"name": Peter,
	"age": 25,
	"likesJson": true,
	"characteristics": ["small","strong","18"],
	}

Option C
{
"name": "Peter",
"age": "25",
"likesJson": true,
"characteristics": ["small","strong",18],
}
	Option D
	{
	"name": "Peter",
	"age": "25",
	"likesJson": true,
	"characteristics": ["small","strong",18]
	}

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

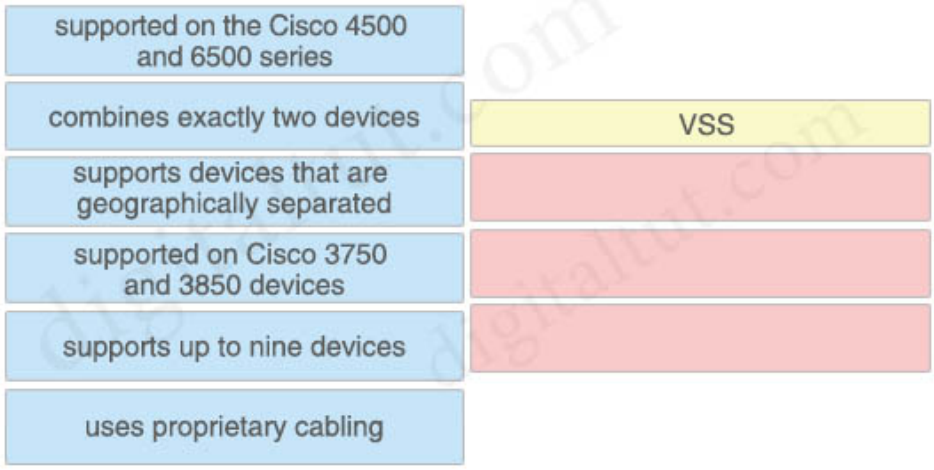
Answer: D

Explanation

Option A is missing commas.
Option B is missing one comma behind “age”:25 and the trailing comma needs to be removed.
Option C needs to remove the trailing comma.

Question 16

Drag and drop the descriptions of the VSS technology from the left to the right. Not all options are used.



Answer:

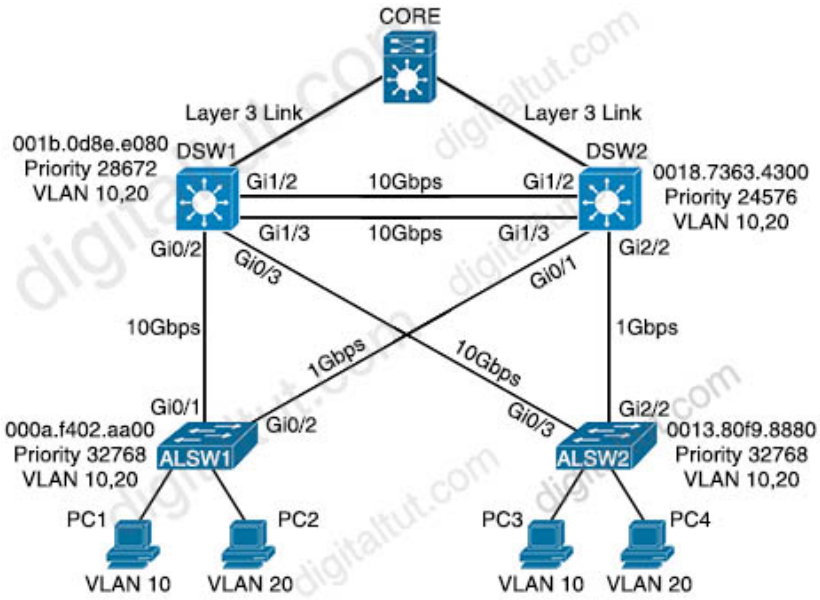
VSS:
+ supported on the Cisco 4500 and 6500 series
+ combines exactly two devices
+ supports devices that are geographically separated

Explanation

The following characteristics are correct for StackWise (but not VSS):
+ can be connected in up to 9 devices
+ is supported only on line 3750 and (2960/3650/3850/3750+)
+ uses proprietary cable for connection

Question 17

Refer to the exhibit.



All switches are configured with the default port priority value. Which two commands ensure that traffic from PC1 is forwarded over Gi1/3 trunk port between DWS1 and DSW2? (Choose two)

A. DWS1(config-if)#spanning-tree port-priority 0
B. DSW2(config-if)#spanning-tree port-priority 16
C. DSW1(config-if)#interface gi1/3
D. DSW2(config-if)#interface gi1/3
E. DSW2(config-if)#spanning-tree port-priority 128

Answer: B D

Explanation

In this topology, DSW2 is the root bridge because of lowest Bridge Priority (24576) so all of its ports are in forwarding state. DSW1 needs to block one of its ports to DSW2 to avoid a bridging loop between the two switches. Unfortunately, DSW blocked port Gi1/3. But how does DSW1 select its blocked port? Well, the answer is based on the BPDUs it receives from DSW2. A BPDU is superior than another if it has:
1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

These four parameters are examined in order. In this specific case, all the BPDUs sent by DSW2 have the same Root Bridge ID, the same path cost to the Root and the same Sending Bridge ID. The only parameter left to select the best one is the Sending Port ID (Port ID = port priority + port index). And the port index of Gi1/2 is lower than the port index of Gi1/3 so the link between two Gi1/2 interfaces has been chosen as the primary link.

Therefore we must change the port priority to change the primary link. The lower numerical value of port priority, the higher priority that port has. In other words, we must change the port-priority on Gi1/3 of DSW2 (not on Gi1/3 of DSW1) to a lower value than that of Gi1/2 (the default port-priority value is 128).

Question 18

In a three-tier hierarchical campus network design, which action is a design best-practice for the core layer?

A. provide QoS prioritization services such as marking, queueing, and classification for critical network traffic
B. provide advanced network security features such as 802. IX, DHCP snooping, VACLs, and port security
C. provide redundant Layer 3 point-to-point links between the core devices for more predictable and faster convergence
D. provide redundant aggregation for access layer devices and first-hop redundancy protocols such as VRRP

Answer: C

Explanation

The core should be highly available and redundant. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

Considerations at the core layer include
– Providing high-speed switching (i.e., fast transport)
– Providing reliability and fault tolerance
– Scaling by using faster, and not more, equipment
– Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes

Reference: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Question 19

Which two network problems indicate a need to implement QoS in a campus network? (Choose two)

A. port flapping
B. misrouted network packets
C. excess jitter
D. bandwidth-related packet loss
E. duplicate IP addresses

Answer: C D

Question 20

In a Cisco SD-Access solution, what is the role of the Identity Services Engine?

A. It provides GUI management and abstraction via apps that share context.
B. It is leveraged for dynamic endpoint to group mapping and policy definition.
C. It is used to analyze endpoint to app flows and monitor fabric status.
D. It manages the LISP EID database.

Answer: B

Explanation

DNA Controller – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context
Identity Services – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
Analytics Engine – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status

Reference: https://www.cisco.com/c/dam/global/da_dk/assets/training/seminaria-materials/Software_Defined_Access_2017.pdf

Question 21

A customer has completed the installation of a Wi-Fi 6 greenfield deployment at their new campus. They want to leverage Wi-Fi 6 enhanced speeds on the trusted employee WLAN. To configure the employee WLAN, which two Layer 2 security policies should be used? (Choose two)

A. WPA (AES)
B. WPA2 (AES) + WEP
C. 802.1X
D. OPEN

Answer: C D

Explanation

Wi-Fi 6 (IEEE 802.11ax)

In greenfield we don’t need to use any security policy to reduce the wasting time of encryption/decryption.

Wi-Fi 6 does not support WPA with AES while WPA2 (AES) would slow down the connection -> Only 802.1X is the best

choice left.

Question 22

Which outcome is achieved with this Python code?

```
client.connect (ip, port=22,username=usr,password=pswd)
stdin,stdout,stderr = client.exec_command('show ip bgp 192.168.10100 bestpath\n')
print(stdout)
```

A. displays the output of the show command in a formatted way
B. connects to a Cisco device using SSH and exports the routing table information
C. connects to a Cisco device using Telnet and exports the routing table information
D. connects to a Cisco device using SSH and exports the BGP table for the prefix

Answer: D

Question 23

What is YANG used for?

A. scraping data via CLI
B. providing a transport for network configuration data between client and server
C. processing SNMP read-only polls
D. describing data models

Answer: D

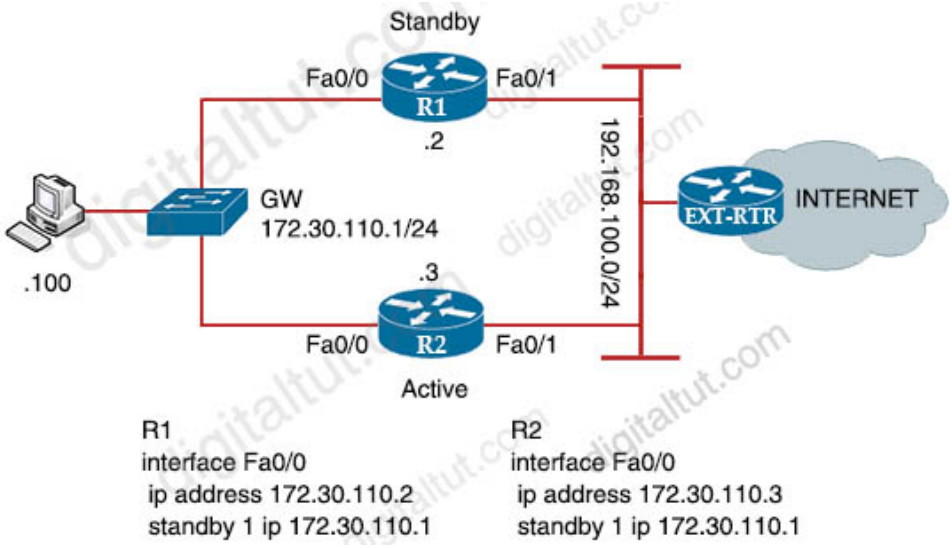
Explanation

YANG is used to model each protocol based on RFC 6020.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book/yang-netconf.html

Question 24

Refer to the exhibit.



Which configuration change ensures that R1 is the active gateway whenever it is in a functional state for the 172.30.110.0/24 network?

Option A R1 standby 1 preempt R2 standby 1 priority 90	**Option B** R1 standby 1 preempt R2 standby 1 priority 100
Option C R2 standby 1 priority 100 standby 1 preempt	**Option D** R2 standby 1 priority 110 standby 1 preempt

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

Answer: A

Explanation

By default, HSRP does not have preemption enabled so we have to enable it on R1 so that R1 can take the active role of R2. We also need to lower the priority of R2 (to 90) than that of R1 (the default HSRP priority is 100) so that R1 can take the active role.

Question 25

Refer to the exhibit.

Person#1: First Name is Johnny Last Name is Table Hobbies are: • Running • Video games Person#2 First Name is Billy Last Name is Smith Hobbies are: • Napping • Reading

Which JSON syntax is derived from this data?

Option A {‘Person’: [{‘First Name’: ‘Johnny’, ‘Last Name’: ‘Table’, ‘Hobbies’: [‘Running’, ‘Video games’]}, {‘First Name’: ‘Billy’, ‘Last Name’: ‘Smith’, ‘Hobbies’: [‘Napping’, ‘Reading’]}]}	**Option B** {[{‘First Name’: ‘Johnny’, ‘Last Name’: ‘Table’, ‘Hobbies’: ‘Running’,’Hobbies’: ‘Video games’}, {‘First Name’: ‘Billy’, ‘Last Name’: ‘Smith’, ‘Hobbies’: ‘Napping’, ‘Hobbies’: Reading’}]}
Option C {‘Person’: [{‘First Name’:’Johnny’, ‘Last Name’: ‘Table’, ‘Hobbies’: ‘Running’, ‘Video games’}, {‘First Name’: ‘Billy’, ‘Last Name’: ‘Smith’, ‘Hobbies’: ‘Napping’, ‘Reading’}]}	**Option D** {[{‘First Name’: ‘Johnny’, ‘Last Name’: ‘Table’, ‘Hobbies’: [‘Running’, ‘Video games’]}, {‘First Name’: ‘Billy’, ‘Last Name’: ‘Smith’, ‘Hobbies’: [‘Napping’,’Reading’]}]}

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

Answer: A

Explanation

Option B and Option D are not correct because the first square bracket in "{[{" should not be there.

Option C "Hobbies" should be an array, not "'Hobbies': 'Running', 'Video games'"

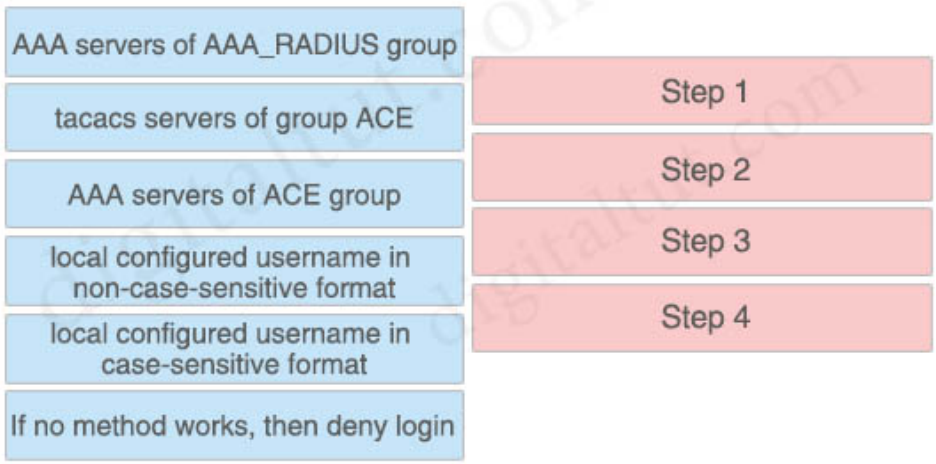
Option A is correct and we also format it in a more comprehensive way below:

```
{
   "Person":[
      {
         "First Name":"Johnny",
         "Last Name":"Table",
         "Hobbies":[
            "Running",
            "Video games"
         ]
      },
      {
         "First Name":"Billy",
         "Last Name":"Smith",
         "Hobbies":[
            "Napping",
            "Reading"
         ]
      }
   ]
}
```

Question 26

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

```
R1#sh run | i aaa
aaa new-model
aaa authentication login default group ACE group AAA_RADIUS local-case
aaa session-id common
R1#
```



Answer:

Step 1: AAA servers of ACE group
Step 2: AAA servers of AAA_RADIUS group
Step 3: local configured username in case-sensitive format
Step 4: If no method works, then deny login

Explanation

The "aaa authentication login default group ACE group AAA_RADIUS local-case" command is broken down as follows:

+ The '**aaa authentication**' part is simply saying we want to configure authentication settings.
+ The '**login**' is stating that we want to prompt for a username/password when a connection is made to the device.
+ The '**default**' means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don't need to configure anything else under tty, vty and aux lines. If we don't use this keyword then we have to specify which line(s) we want to apply the authentication feature.
+ The '**group ACE group AAA_RADIUS**" means all users are authenticated using group ACE (the first method). If the credentials are not found on this group, then the group AAA_RADIUS is used (the second method).
+ The '**local-case**' option uses case-sensitive local usernames.

Question 27

Refer to the exhibit.

```
Vlan503 - Group 1
  State is Active
    1 state change, last state change 32w6d
  Virtual IP address is 10.0.3.241
  Active virtual MAC address is 0000.0c07 ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.064 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl503-1" (default)
```

Which two facts does the device output confirm? (Choose two)

A. The device is using the default HSRP hello timer
B. The standby device is configured with the default HSRP priority
C. The device's HSRP group uses the virtual IP address 10.0.3.242
D. The device is configured with the default HSRP priority
E. The device sends unicast messages to its peers

Answer: A B

Explanation

From the output above, we see the local router is the active HSRP router with priority 110 while the default priority is 100 -> Answer D is not correct.

From the line "Standby router is 10.0.3.242, priority 100", we learn that standby router is configured with default priority -> Answer B is correct.

HSRP default hello and hold timers are 3 seconds and 10 seconds, respectively so answer A is correct.

Question 28

Based on the output below, which Python code shows the value of the “upTime” key?

```
{
“response”: [{
“family”: “Routers”,
“type”: “Cisco ASR 1001-X Router”,
“errorCode”: null,
“location”: null,
“macAddress”: “00:c8:8b:80:bb:00”,
“hostname”: “asr1001-x.abc.inc”,
“role”: “BORDER ROUTER”,
“lastUpdateTime”: 1577391299537,
“serialNumber”: “FXS1932Q1SE”,
“softwareVersion”: “16.3.2”,
“locationName”: null,
“upTime”: “49 days, 13:43:44:13”,
“lastUpdated”: “2019-12-22 16:35:21”
}]
}
```

Option A json_data = response.json() print(json_data[response][0][upTime])	**Option B** json_data = response_json() print(json_data[‘response’][‘family’][‘upTime’])
Option C json_data = response.json() print(json_data[‘response’][0][‘upTime’])	**Option D** json_data = json.loads(response.text) print(json_data[‘response’][‘family’][‘upTime’])

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

Answer: C

Explanation

You can test this question in Python and see the output below:

```
C:\Users\PC>python
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018,
Type "help", "copyright", "credits" or "licen
>>> import json
>>> json_string = """
... {
... "response": [{
... "family": "Routers",
... "type": "Cisco ASR 1001-X Router",
... "errorCode": null,
... "location": null,
... "macAddress": "00:c8:8b:80:bb:00",
... "hostname": "asr1001-x.abc.inc",
... "role": "BORDER ROUTER",
... "lastUpdateTime": 1577391299537,
... "serialNumber": "FXS1932Q1SE",
... "softwareVersion": "16.3.2",
... "locationName": null,
... "upTime": "49 days, 13:43:44:13",
... "lastUpdated": "2019-12-22 16:35:21"
... }]
... }
... """
...
>>> json_data = json.loads(json_string)
>>> print(json_data['response'][0]['upTime'])
49 days, 13:43:44:13
>>>
```

Note: We need to call the first element “[0]” in “json_data[‘response’][0][‘upTime’])” command because “response” is an array with only one element.

Question 29

Which two actions, when applied in the LAN network segment, will facilitate Layer 3 CAPWAP discovery for lightweight AP? (Choose two)

A. Utilize DHCP option 17
B. Utilize DHCP option 43
C. Configure WLC IP address on LAN switch
D. Enable port security on the switch port
E. Configure an ip helper-address on the router interface

Answer: B E

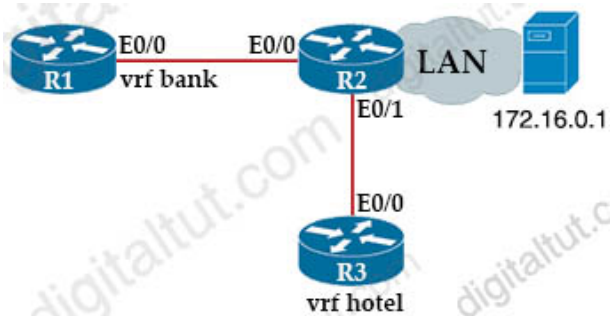
Explanation

In a Cisco Unified Wireless network, the LAPs must first discover and join a WLC before they can service wireless clients. However, this presents a question: how did the LAPs find the management IP address of the controller when it is on a different subnet?
If you do not tell the LAP where the controller is **via DHCP option 43**, DNS resolution of “Cisco-capwap-controller.local_domain”, or statically configure it, the LAP does not know where in the network to find the management interface of the controller.

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/119286-lap-notjoin-wlc-tshoot.html

Question 30

Refer to the exhibit.



R2:

```
vrf definition hotel
 address-family ipv4
 exit-address-family

vrf definition bank
 address-family ipv4
 exit-address-family

interface Ethernet0/0
 vrf forwarding bank
 ip address 172.16.0.4 255.255.0.0

interface Ethernet0/1
 vrf forwarding hotel
 ip address 172.1.0.5 255.255.0.0

router ospf 42 vrf bank
 router-id 1.1.1.1
 network 172.16.0.0 0.0.255.255 area 0

router ospf 43 vrf hotel
 router-id 3.3.3.3
 network 172.16.0.0 0.0.255.255 area 0
```

R1:

```
vrf definition bank
!
 address-family ipv4
 exit-address-family
```

Which configuration must be applied to R1 to enable R1 to reach the server at 172.16.0.1?

Option A interface Ethernet0/0 ip address 172.16.0.7 255.255.0.0 ! router ospf 44 vrf hotel network 172.16.0.0 0.0.255.255	**Option B** interface Ethernet0/0 vrf forwarding bank ip address 172.16.0.7 255.255.0.0 ! router ospf 44 vrf bank network 172.16.0.0 0.0.255.255 area 0
Option C interface Ethernet0/0 vrf forwarding hotel ip address 172.16.0.7 255.255.0.0 ! router ospf 44 vrf hotel network 172.16.0.0 0.0.255.255 area 0	**Option D** interface Ethernet0/0 ip address 172.16.0.7 255.255.0.0 ! router ospf 44 vrf bank network 172.16.0.0 255.255.0.0

A. Option A

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

Answer: B

Question 31

The following system log message is presented after a network administrator configures a GRE tunnel:

```
%TUN-RECURDOWN: Interface Tunnel 0 temporarily disabled due to recursive routing.
```

Why is Tunnel 0 disabled?

A. Because the tunnel cannot reach its tunnel destination
B. Because the best path to the tunnel destination is through the tunnel itself
C. Because dynamic routing is not enabled
D. Because the router cannot recursively identify its egress forwarding interface

Answer: B

Explanation

The **%TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing error** message means that the generic routing encapsulation (GRE) tunnel router has discovered a recursive routing problem. This condition is usually due to one of these causes:
+ A misconfiguration that causes the router to try to route to the tunnel destination address using the tunnel interface itself (recursive routing)
+ A temporary instability caused by route flapping elsewhere in the network

Reference: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/22327-gre-flap.html

========== New Questions (added on 9th-Mar-2020) ==========

Question 32

What is provided by the Stealthwatch component of the Cisco Cyber Threat Defense solution?

A. real-time threat management to stop DDoS attacks to the core and access networks
B. real-time awareness of users, devices and traffic on the network
C. malware control
D. dynamic threat control for web traffic

Answer: B

Explanation

Cisco Stealthwatch is a comprehensive, network telemetry-based, security monitoring and analytics solution that streamlines incident response through behavioral analysis; detecting denial of service attacks, anomalous behaviour, malicious activity and insider threats. Based on a scalable enterprise architecture, Stealthwatch provides near real-time situational awareness of all users and devices on the network.

Reference: https://www.endace.com/cisco-stealthwatch-solution-brief.pdf

Note: Although answer A seems to be correct but in fact, Stealthwatch does not provide real-time protection for DDoS attack. It just helps detect DDoS attack only.

Stealthwatch aggregates observed network activity and performs behavioral and policy driven analytics against what it sees in order to surface problematic activities. While we don't position our self as a DDOS solution, we're going to leverage our analytical capabilities to identify a DDoS attack against an internal host using the WebUI.

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2016/pdf/LTRSEC-8421-LG.pdf

Question 33

How does Protocol Independent Multicast function?

A. It uses unicast routing information to perform the multicast forwarding function.
B. It uses the multicast routing table to perform the multicast forwarding function.
C. In sparse mode it establishes neighbor adjacencies and sends hello messages at 5-second intervals.
D. It uses broadcast routing information to perform the multicast forwarding function.

Answer: A

Explanation

Although PIM is called a multicast routing protocol, **it actually uses the unicast routing table** to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16/imc-pim-xe-16-book/imc-tech-oview.html

Question 34

Under which network conditions is an outbound QoS policy that is applied on a router WAN interface most beneficial?

A. under all network conditions
B. under network convergence conditions
C. under interface saturation conditions
D. under traffic classification and marking conditions

Answer: C

Question 35

Which technology does VXLAN use to provide segmentation for Layer 2 and Layer 3 traffic?

A. bridge domain
B. VLAN
C. VRF
D. VNI

Answer: D

Explanation

VXLAN has a 24-bit VXLAN network identifier (VNI), which allows for up to 16 million (= 2^{24}) VXLAN segments to coexist within the same infrastructure. This surely solve the small number of traditional VLANs.

Question 36

A company has an existing Cisco 5520 HA cluster using SSO. An engineer deploys a new single Cisco Catalyst 9800 WLC to test new features. The engineer successfully configures a mobility tunnel between the 5520 cluster and 9800 WLC. Clients connected to the corporate WLAN roam seamlessly between access points on the 5520 and 9800 WLC. After a failure on the primary 5520 WLC, all WLAN services remain functional; however clients cannot roam between the 5520 and 9800 controllers without dropping their connection. Which feature must be configured to remedy the issue?

A. mobility MAC on the 5520 cluster
B. mobility MAC on the 9800 WLC
C. new mobility on the 5520 cluster
D. new mobility on the 9800 WLC

Answer: B

Question 37

What are two methods of ensuring that the multicast RPF check passes without changing the unicast routing table? (Choose two)

A. disabling BGP routing protocol
B. implementing static mroutes
C. disabling the interface of the router back to the multicast source
D. implementing MBGP
E. implementing OSPF routing protocol

Answer: B D

Question 38

What is the result when an active route processor fails in a design that combines NSF with SSO?

A. An NSF-aware device immediately updates the standby route processor RIB without churning the network
B. The standby route processor temporarily forwards packets until route convergence is complete
C. An NSF-capable device immediately updates the standby route processor RIB without churning the network
D. The standby route processor immediately takes control and forwards packets along known routes

Answer: B

========== New Questions (added on 28th-Mar-2021) ==========

Question 39

What is a benefit of a virtual machine when compared with a physical server?

A. Deploying a virtual machine is technically less complex than deploying a physical server.
B. Virtual machines increase server processing performance.
C. The CPU and RAM resources on a virtual machine cannot be affected by other virtual machines.
D. Multiple virtual servers can be deployed on the same physical server without having to buy additional hardware.

Answer: D

Question 40

What is the wireless received signal strength indicator?

A. The value of how strong the wireless signal is leaving the antenna using transmit power, cable loss, and antenna gain
B. The value given to the strength of the wireless signal received compared to the noise level
C. The value of how much wireless signal is lost over a defined amount of distance
D. The value of how strong a wireless signal is receded, measured in dBm

Answer: D

Explanation

RSSI, or "Received Signal Strength Indicator," is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection.

This value is measured in decibels (dBm) from 0 (zero) to -120 (minus 120). The closer to 0 (zero) the stronger the signal is which means it's better, typically voice networks require a -65db or better signal level while a data network needs -80db or better.

Question 41

Which controller is capable of acting as a STUN server during the onboarding process of Edge devices?

A. vManage
B. vSmart
C. vBond
D. PNP server

Answer: C

Explanation

An additional vBond is deployed on the Internet and acts as a STUN server for WAN Edge devices with Internet access and redirects them to the private controller IP addresses.

Reference: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Note: Session Traversal Utilities for NAT (STUN) is a standardized set of methods, including a network protocol, for traversal of network address translator (NAT) gateways in applications of real-time voice, video, messaging, and other interactive communications.

Question 42

What is the process for moving a virtual machine from one host machine to another with no downtime?

A. live migration
B. disaster recovery
C. high availability
D. multisite replication

Answer: A

Explanation

Live migration refers to the process of moving a running virtual machine or application between different physical machines without disconnecting the client or application. Memory, storage, and network connectivity of the virtual machine

are transferred from the original guest machine to the destination. An example of live migration tool is VMware vSphere vMotion.

Question 43

What are two features of NetFlow flow monitoring? (Choose two)

A. Can track ingress and egress information
B. Include the flow record and the flow importer
C. Copies all ingress flow information to an interface
D. Does not required packet sampling on interfaces
E. Can be used to track multicast, MPLS, or bridged traffic

Answer: A E

Explanation

The following are restrictions for Flexible NetFlow:
+ Traditional NetFlow (TNF) accounting is not supported.
+ Flexible NetFlow v5 export format is not supported, only NetFlow v9 export format is supported.
+ **Both ingress and egress NetFlow accounting is supported.**
+ Microflow policing feature shares the NetFlow hardware resource with FNF.
+ Only one flow monitor per interface and per direction is supported.

Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_011010.html

When configuring NetFlow, follow these guidelines and restrictions:

+ Except in PFC3A mode, NetFlow supports **bridged IP traffic**. PFC3A mode does not support NetFlow bridged IP traffic.
+ NetFlow supports **multicast IP traffic**.

Reference: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/netflow.html

The Flexible NetFlow – MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfg-mpls-netflow.html

Question 44

Which method should an engineer use to deal with a long-standing contention issue between any two VMs on the same host?

A. Adjust the resource reservation limits
B. Reset the host
C. Reset the VM
D. Live migrate the VM to another host

Answer: D

Question 45

What is the recommended MTU size for a Cisco SD-Access Fabric?

A. 4464
B. 9100
C. 1500
D. 17914

Answer: B

Question 46

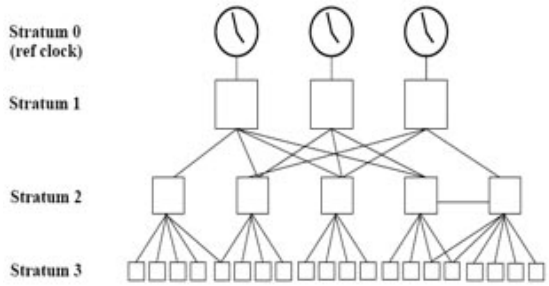
What does the number in an NTP stratum level represent?

A. The number of hops it takes to reach the master time server.
B. The amount of drift between the device clock and true time.
C. The amount of offset between the device clock and true time.
D. The number of hops it takes to reach the authoritative time source.

Answer: D

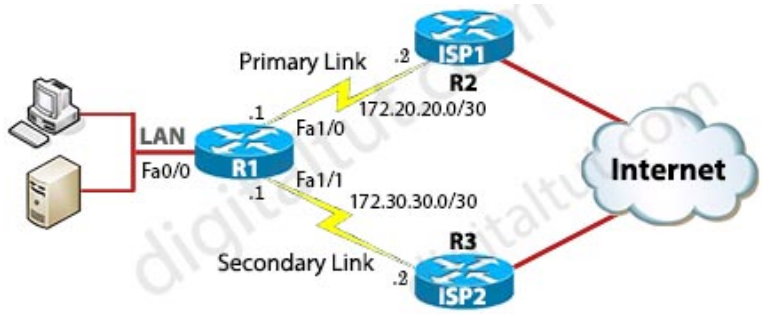
Explanation

NTP uses the concept of a stratum to describe how many hops (routers) away a machine is from an authoritative time source, usually a reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time standard.



Question 47

Refer to the exhibit.




```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 172.20.20.2 source-interface FastEthernet1/0
R1(config-ip-sla-echo)#timeout 5000
```

```
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

After implementing the configuration 172.20.20.2 stops replaying to ICMP echoes, but the default route fails to be removed. What is the reason for this behavior?

A. The source-interface is configured incorrectly.
B. The destination must be 172.30.30.2 for icmp-echo
C. The default route is missing the track feature
D. The threshold value is wrong

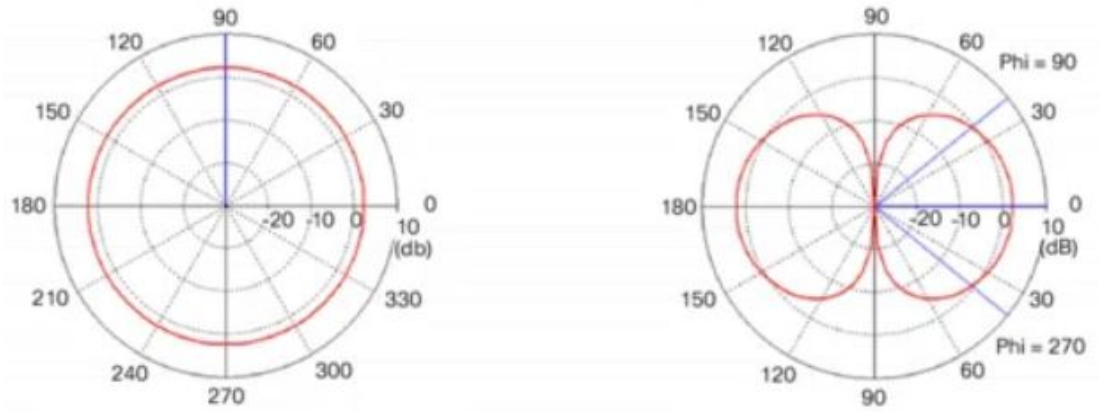
Answer: C

Explanation

The last command should be "R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2 track 10".

Question 48

Refer to the exhibit.



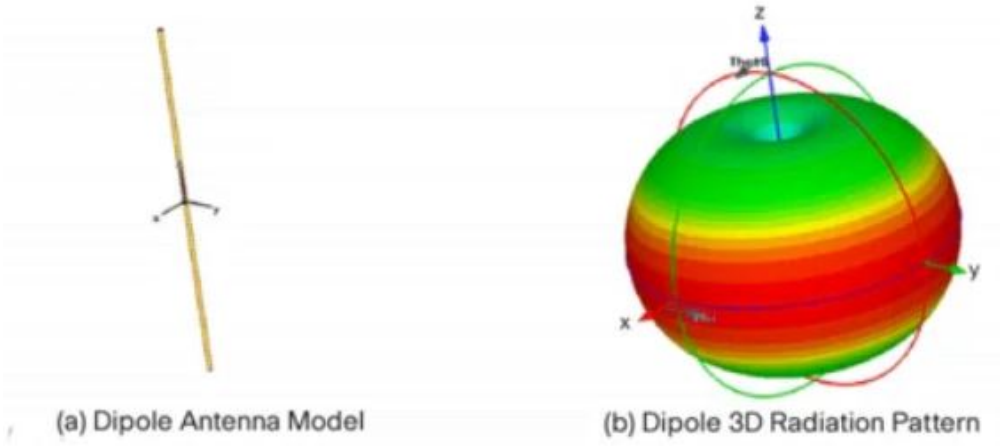
Which type of antenna is show on the radiation patterns?

A. Dipole
B. Yagi
C. Patch
D. Omnidirectional

Answer: A

Explanation

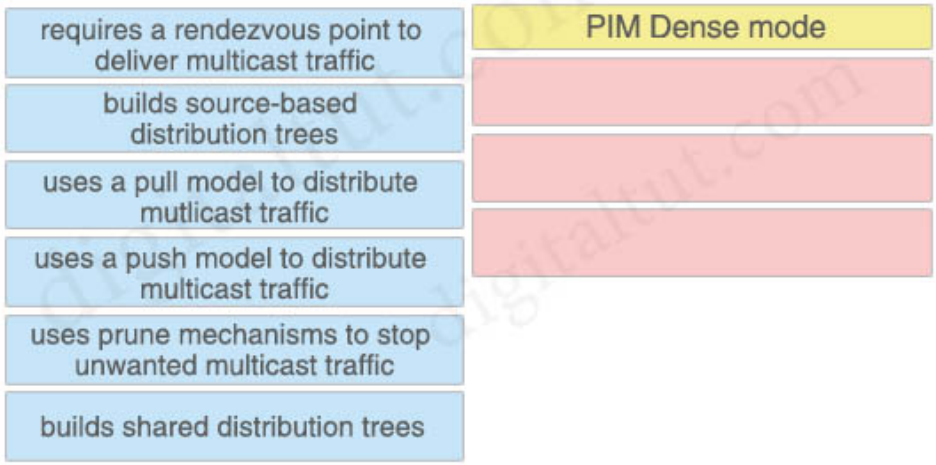
A dipole antenna most commonly refers to a half-wavelength (λ/2) dipole. The physical antenna (not the package that it is in) is constructed of conductive elements whose combined length is about half of a wavelength at its intended frequency of operation. This is a simple antenna that radiates its energy out toward the horizon (perpendicular to the antenna). The patterns shown are those resulting from a perfect dipole formed with two thin wires oriented vertically along the z-axis.



Reference: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html

Question 49

Drag and drop characteristics of PIM dense mode from the left to the right.



Answer:

PIM Dense Mode:
+ builds source-based distribution trees
+ uses a push model to distribute multicast traffic
+ uses prune mechanisms to stop unwanted multicast traffic

Explanation

PIM-DM supports only source trees – that is, (S,G) entries–and cannot be used to build a shared distribution tree.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-16-5/imc-pim-xe-16-5-book/imc-tech-oview.html

PIM dense mode (PIM-DM) uses a **push model** to flood multicast traffic to every corner of the network. This push model is a brute-force method of delivering data to the receivers. This method would be efficient in certain deployments in which there are active receivers on every subnet in the network. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors **prune the unwanted traffic**. This process repeats every 3 minutes.

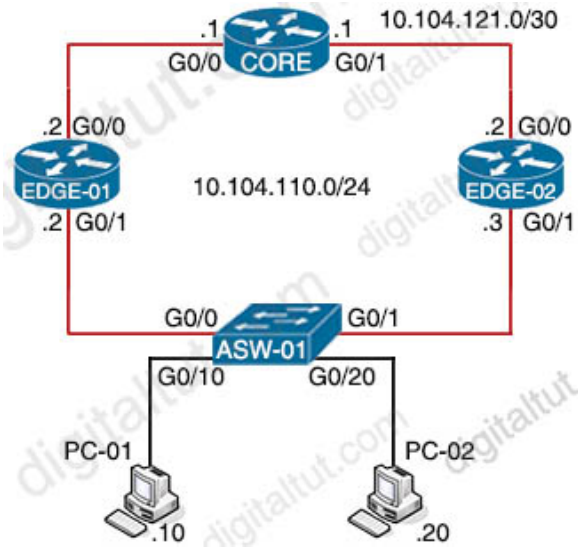
A rendezvous point (RP) is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM).

In PIM dense mode (PIM-DM), multicast traffic is initially flooded to all segments of the network. Routers that have no

downstream neighbors or directly connected receivers prune back the unwanted traffic.

Question 50

Refer to the exhibit.



Edge-01	**Edge-02**
track 10 interface GigabitEthernet0/0 line-protocol ! interface GigabitEthernet0/1 ip address 10.104.110.2 255.255.255.0 vrrp 10 ip 10.104.110.100 vrrp 10 priority 120	interface GigabitEthernet0/1 ip address 10.104.110.3 255.255.255.0 vrrp 10 ip 10.104.110.100

Object tracking has been configured for VRRP enabled routers Edge-01 and Edge-02. Which commands cause Edge-02 to preempt Edge-01 in the event that interface G0/0 goes down on Edge-01?

Option A	**Option B**
Edge-01(config)#interface G0/1 Edge-01(config-if)#vrrp 10 track 10 decrement 10	Edge-02(config)#interface G0/1 Edge-02(config-if)#vrrp 10 track 10 decrement 30
Option C	**Option D**
Edge-02(config)#interface G0/1 Edge-02(config-if)#vrrp 10 track 10 decrement 10	Edge-01(config)#interface G0/1 Edge-01(config-if)#vrrp 10 track 10 decrement 30

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

Answer: D

Question 51

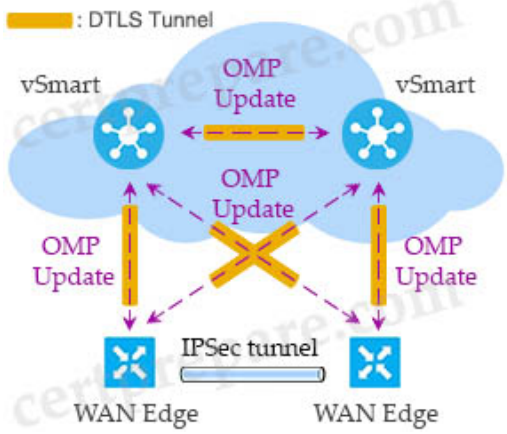
Which protocol is implemented to establish secure control plane adjacencies between Cisco SD-WAN nodes?

A. IKE
B. DTLS
C. IPsec
D. ESP

Answer: B

Explanation

The Cisco SD-WAN control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol.



Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html

Question 52

Refer to the exhibit.

```
flow monitor FLOW-MONITOR-1
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

What is the effect of introducing the sampler feature into the Flexible NetFlow configuration on the router?

A. NetFlow updates to the collector are sent 50% less frequently.
B. Every second IPv4 packet is forwarded to the collector for inspection.
C. CPU and memory utilization are reduced when compared with what is required for full NetFlow.
D. The resolution of sampling data increases, but it requires more performance from the router.

Answer: A

Explanation

The example above shows how to configure and enable deterministic sampling for IPv6 input traffic -> Answer B is not correct.

Answer D is not correct because "1 out-of 2" mode will only sample 1 out of 2 packets, thus the resolution of sampling data will decrease (not increase)

There is three sampling modes:
– deterministic: select each N-th observed flow
– random: select randomly one out of N flows.
– hash: select hash-randomly one out of N flows.

Using 'deterministic' and 'random' sampling will not reduce resource usage caused by the module, because flows are sampled late in exporting process. This will reduces amount of flows which go to the collector, thus, reducing load on the collector -> Answer A is correct.

Reference: https://github.com/aabc/pkt-netflow

CPU is not involved in the process of packet sampling as it is done by the hardware (ASICs) -> Answer C is not correct.

Question 53

When does a stack master lose its role?

A. When the priority value of a stack member is changed to a higher value
B. When a switch with a higher priority is added to the stack
C. When the stack master is reset
D. When a stack member fails

Answer: C

Explanation

A stack master retains its role unless one of these events occurs:
+ The switch stack is reset.*
+ The stack master is removed from the switch stack.
+ **The stack master is reset** or powered off -> Answer C is correct.
+ The stack master fails.
+ The switch stack membership is increased by adding powered-on standalone switches or switch stacks.*

In the events marked by an asterisk (*), the current stack master might be reelected based on the listed factors.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3e/ha_stack_manager/configuration_guide/b_stack_ha_3e_3650_cg/b_hastck_3se_3650_cg_chapter_010.html

Question 54

What is the calculation that is used to measure the radiated power of a signal after it has gone through the radio, antenna cable, and antenna?

A. dBi
B. mW
C. dBm

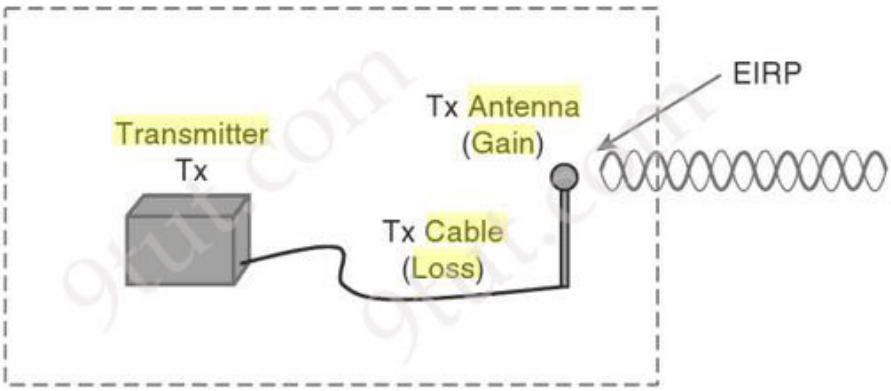
D. EIRP

Answer: D

Explanation

Once you know the complete combination of transmitter power level, the length of cable, and the antenna gain, you can figure out the actual power level that will be radiated from the antenna. This is known as the effective isotropic radiated power (EIRP), measured in dBm.

EIRP is a very important parameter because it is regulated by governmental agencies in most countries. In those cases, a system cannot radiate signals higher than a maximum allowable EIRP. To find the EIRP of a system, simply add the transmitter power level to the antenna gain and subtract the cable loss.



EIRP = Tx Power – Tx Cable + Tx Antenna

Suppose a transmitter is configured for a power level of 10 dBm (10 mW). A cable with 5-dB loss connects the transmitter to an antenna with an 8-dBi gain. The resulting EIRP of the system is 10 dBm – 5 dB + 8 dBi, or 13 dBm.

You might notice that the EIRP is made up of decibel-milliwatt (dBm), dB relative to an isotropic antenna (dBi), and decibel (dB) values. Even though the units appear to be different, you can safely combine them because they are all in the dB “domain”.

Reference: CCNA Wireless 640-722 Official Cert Guide

Comments
Comment pages
« Previous 1 2 3 4003

1. DAgger
   April 5th, 2021

   @digitaltut, yes please lot people saying 10-20 new questions again since the last update. Thank youu!

2. DANY
   April 5th, 2021

   @digitaltut, new questions update?????

3. MariaMashABabko
   April 6th, 2021

   digital?

4. digitaltut