New ENCOR Questions – Part 2

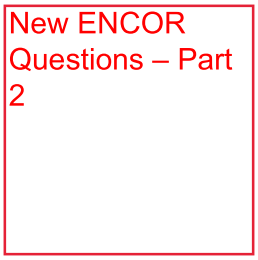
September 17th, 2020 in New ENCOR Questions Go to comments

Premium Member: You can practice these questions via these links first:
+ First 20 questions
+ Question 21 to end

Question 1

Which two LISP infrastructure elements are needed to support LISP to non -LISP internetworking? (Choose two)

A. PETR
B. PITR
C. MR
D. MS
E. ALT



Answer: A C

Question 2

Which statement about dynamic GRE between a headend router and a remote router is true?

A. The headend router learns the IP address of the remote end router statically
B. A GRE tunnel without an IP address has a status of administratively down
C. GRE tunnels can be established when the remote router has a dynamic IP address
D. The remote router initiates the tunnel connection

Answer: D

Question 3

Which two statements about AAA authentication are true? (Choose two)

A. RADIUS authentication queries the router's local username database
B. TACACS+ authentication uses an RSA server to authenticate users
C. Local user names are case-insensitive
D. Local authentication is maintained on the router
E. KRB5 authentication disables user access when an incorrect password is entered

Answer: D E

Question 4

Which action is performed by Link Management Protocol in a Cisco stackwise virtual domain?

A. It discovers the stackwise domain and brings up SVL interfaces
B. It rejects any unidirectional link traffic forwarding
C. It determines if the hardware is compatible to form the stackwise virtual domain
D. It determines which switch becomes active or standby

Answer: B

Explanation

The Link Management Protocol (LMP) performs the following functions:
+ Verifies link integrity by establishing bidirectional traffic forwarding, and rejects any unidirectional links
+ Exchanges periodic hellos to monitor and maintain the health of the links
+ Negotiates the version of StackWise Virtual header between the switches StackWise Virtual link role resolution

Reference: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-stack-wp-cte-en.html

Question 5

Which two actions provide controlled Layer 2 network connectivity between virtual machines running on the same hypervisor? (Choose two)

A. Use a single trunk link to an external Layer2 switch
B. Use a virtual switch provided by the hypervisor
C. Use VXLAN fabric after installing VXLAN tunnelling drivers on the virtual machines
D. Use a single routed link to an external router on stick
E. Use a virtual switch running as a separate virtual machine

Answer: B E

Question 6

How does SSO work with HSRP to minimize network disruptions?

A. It enables HSRP to elect another switch in the group as the active HSRP switch
B. It ensures fast failover in the case of link failure
C. It enables data forwarding along known routes following a switchover, while the routing protocol reconverges
D. It enables HSRP to failover to the standby RP on the same device

Answer: D

Explanation

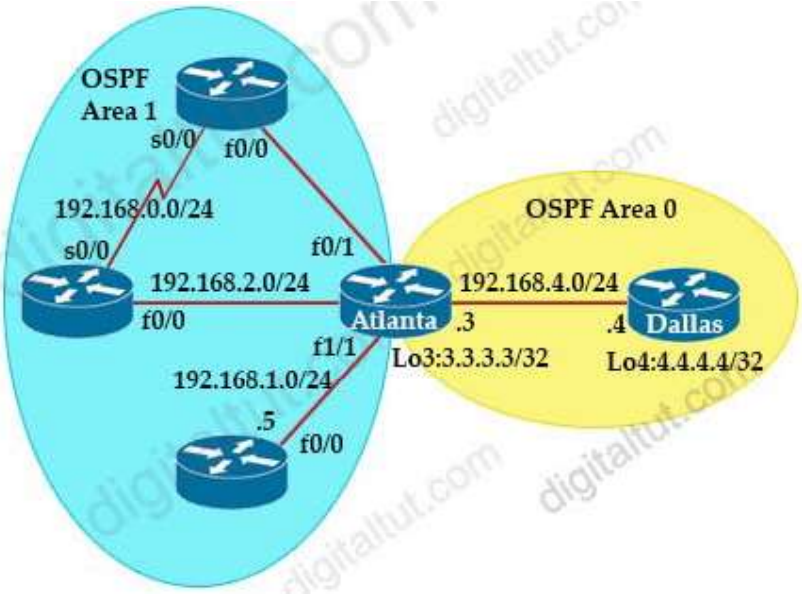
SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/fhp-hsrp-sso.html

Question 7

Refer to the exhibit.




```
Dallas#show ip route ospf
     3.0.0.0/32 i subnetted, 1 subnets
O       3.3.3.3 [110/40001] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.0.0/24 [110/145535] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.1.0/24 [110/80000] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.2.0/24 [110/80000] via 192.168.4.3, 00:33:32, FastEthernet0/0
O IA 192.168.3.0/24 [110/44000] via 192.168.4.3, 00:33:32, FastEthernet0/0
```

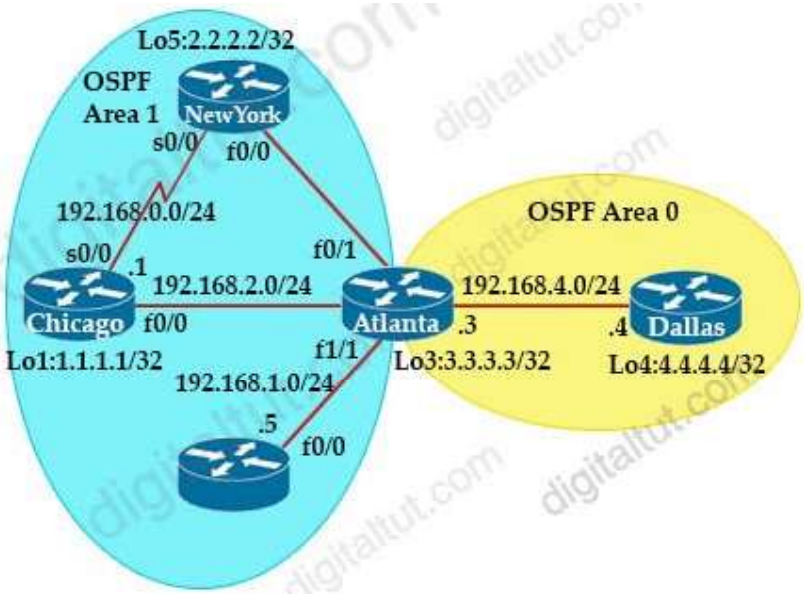
Which command when applied to the Atlanta router reduces type 3 LSA flooding into the backbone area and summarizes the inter-area routes on the Dallas router?

A. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.252.0
B. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.252.0
C. Atlanta(config-route)#area 0 range 192.168.0.0 255.255.248.0
D. Atlanta(config-route)#area 1 range 192.168.0.0 255.255.248.0

Answer: B

Question 8

Refer the exhibit.




```
Chicago#show ip ospf nei

Neighbor ID  Pri   State      Dead Time  Address         Interface
3.3.3.3        1   FULL/BDR   00:00:35   192.168.2.3     FastEthernet0/0
2.2.2.2        0   FULL/ -    00:00:35   192.168.0.2     Serial0/0

Chicago#show ip ospf int bri
Interface  PID Area     IP Address/Mask  Cost   State Nbrs F/C
Fa0/0      1   1        192.168.2.1/24   40444  DR    1/1
Se0/0      1   1        192.168.0.1/24   65535  P2P   1/1
Chicago#
```

Which router is the designated router on the segment 192.168.0.0/24?

A. Router Chicago because it has a lower router ID
B. Router NewYork because it has a higher router ID
C. This segment has no designated router because it is a nonbroadcast network type.
D. This segment has no designated router because it is a p2p network type.

Answer: D

Question 9

An engineer must configure interface GigabitEthernet0/0 for VRRP group 10. When the router has the highest priority in the group, it must assume the master role. Which command set must be added to the initial configuration to accomplish this task?

Initial Configuration

```
interface GigabitEthernet0/0
 description to IDF
 ip address 172.16.13.2 255.255.255.0
```

A.
vrrp 10 ip 172.16.13.254
vrrp 10 preempt

B.
standby 10 ip 172.16.13.254
standby 10 priority 120

C.
vrrp group 10 ip 172.16.13.254 255.255.255.0
vrrp group 10 priority 120

D.
standby 10 ip 172.16.13.254 255.255.255.0
standby 10 preempt

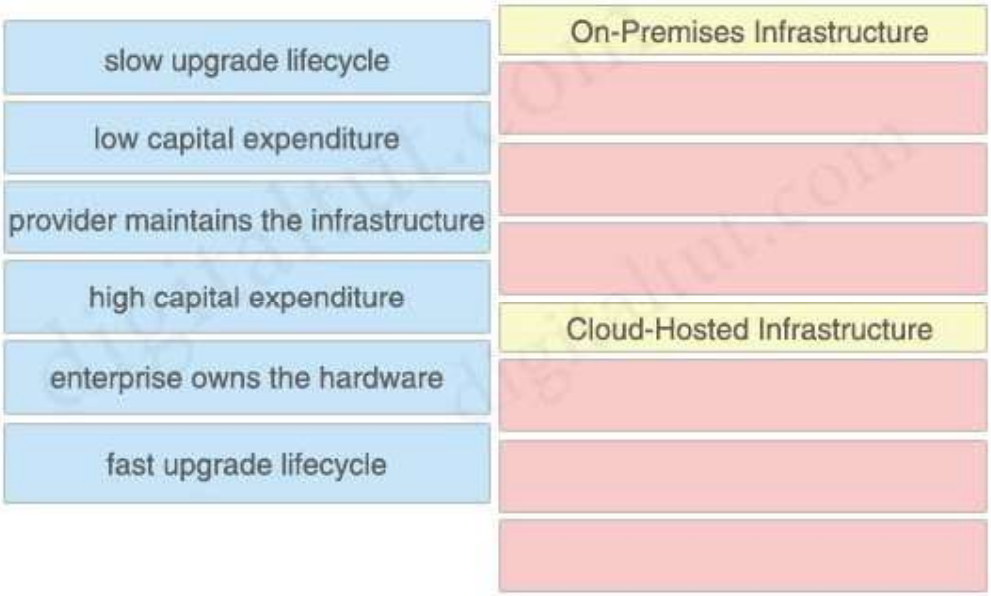
Answer: A

Explanation

In fact, VRRP has the preemption enabled by default so we don't need the "vrrp 10 preempt" command. The default priority is 100 so we don't need to configure it either. But notice that the correct command to configure the virtual IP address for the group is "vrrp 10 ip {*ip-address*}" (not "vrrp group 10 ip …") and this command does not include a subnet mask.

Question 10

Drag and drop the characteristics from the left onto the infrastructure types on the right.



Answer:

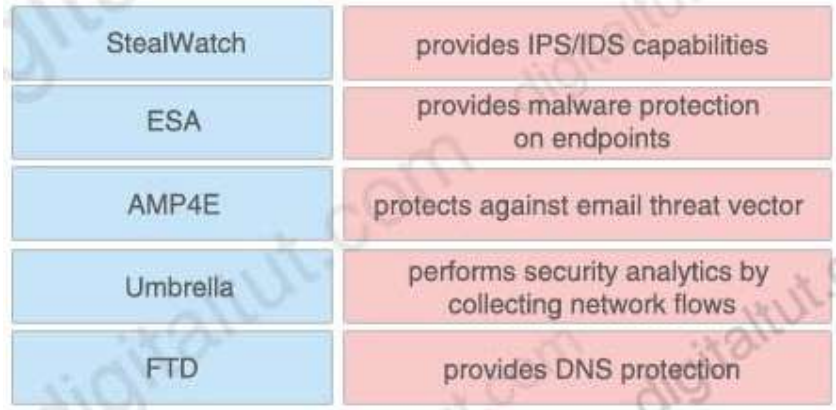
On-Premises Infrastructure:
+ slow upgrade lifecycle
+ high capital expenditure
+ enterprise owns the hardware

Cloud-Hosted Infrastructure:
+ low capital expenditure

+ provider maintains the infrastructure
+ fast upgrade lifecycle

Question 11

Drag and drop the threat defense solutions from the left onto their descriptions on the right.



Answer:

+ StealWatch: performs security analytics by collecting network flows
+ ESA: protects against email threat vector
+ AMP4E: provides malware protection on endpoints
+ Umbrella: provides DNS protection
+ FTD: provides IPS/IDS capabilities

Question 12

Refer to the exhibit. An engineer configures CoPP and enters the show command to verify the implementation. What is the result of the configuration?

```
Router2#show policy-map control-plane

Control Plane
Service-policy input:CISCO
Class-map:CISCO (match-all)
  20 packets, 11280 bytes
  5 minute offerred rate 0 bps, drop rate 0 bps
  Match:access-group 120
  police:
   8000 bps, 1500 limit, 1500 extended limit
   conformed 15 packets, 6210 bytes; action:transmit
   exceeded 5 packets, 5070 bytes; action:drop
   violated 0 packets, 0 bytes; action:drop
   conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
  105325 packets, 11415151 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

A. All traffic will be policed based on access-list 120
B. If traffic exceeds the specified rate, it will be transmitted and remarked

C. Class-default traffic will be dropped
D. ICMP will be denied based on this configuration

Answer: A

Question 13

You are configuring a controller that runs Cisco IOS XE by using the CLI. Which three configuration options are used for 802.11w Protected Management Frames? (Choose three)

A. mandatory
B. association-comeback
C. SA teardown protection
D. saquery-retry-time
E. enable
F. comeback-time

Answer: A B D

Question 14

Which technology is used to provide Layer 2 and Layer 3 logical networks in the Cisco SD-Access architecture?

A. underlay network
B. overlay network
C. VPN routing/forwarding
D. easy virtual network

Answer: B

Explanation

An overlay network creates a logical topology used to virtually connect devices that are built over an arbitrary physical underlay topology.

An overlay network is created on top of the underlay network through virtualization (virtual networks). The data plane traffic and control plane signaling are contained within each virtualized network, maintaining isolation among the networks and an independence from the underlay network.

SD-Access allows for the extension of Layer 2 and Layer 3 connectivity across the overlay through the services provided by through LISP.

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

Question 15

An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

A. by location

B. by role
C. by organization
D. by hostname naming convention

Answer: A

Question 16

Refer to the exhibit.

```
(WLC) >show interface summary
Interface Name                Vlan Id
------------------------      -------
deadnet                       999
users1                        14
users2                        15
users3                        16

(WLC) >show wlan 1
WLAN Identifier . . . . . . . . . . . . . . . . 1
Network Name (SSID) . . . . . . . . . . . . . . wlan1
AAA Policy Override . . . . . . . . . . . . . . Enabled
Interface . . . . . . . . . . . . . . . . . . . deadnet
FlexConnect Local Switching . . . . . . . . . Enabled
FlexConnect Central Association . . . . . . . Disabled
flexconnect Central Dhcp Flag . . . . . . . . Disabled
flexconnect nat-pat Flag . . . . . . . . . . . Disabled
flexconnect DNS Override Flag . . . . . . . . Disabled
flexconnect PPPoE pass-through . . . . . . .  Disabled
flexconnect local-switching IP-source-guar . .Disabled
FlexConnect Vlan based Central Switching . .  Enabled
FlexConnect Local Authentication . . . . . .  Disabled
FlexConnect Learn IP Address . . . . . . . .  Enabled

(WLC) >show ap config general FlexAP1
AP Mode . . . . . . . . . . . . . . . . . . . . FlexConnect
FlexConnect Vlan mode : . . . . . . . . . . . .  Enabled
            Native ID : . . . . . . . . . . . . . . . 1
            WLAN 1 : . . . . . . . . . . . . . . . . .  10 (AP-Specific)
FlexConnect VLAN ACL Mappings
Vlan : . . . . . . . . . . . . . . . . . . . . . 10
            Ingress ACL : . . . . . . . . . . . . . . None
            Egress ACL : . . . . . . . . . . . . . .  None
VLAN with least priority : . . . . . . . . . . . 13
FlexConnect Group . . . . . . . . . . . . . .  flexgroup1
Group VLAN ACL Mappings
Vlan : . . . . . . . . . . . . . . . . . . . . . 11
            Ingress ACL : . . . . . . . . . . . . . . None
            Egress ACL : . . . . . . . . . . . . . .  None
Vlan : . . . . . . . . . . . . . . . . . . . . . 12
```

A wireless client is connecting to FlexAP1 which is currently working standalone mode. The AAA authentication process is returning the following AVPs:

Tunnel-Private-Group-Id(81): 15

Tunnel-Medium-Type(65): IEEE-802(6) Tunnel-Type(64): VLAN(13)

Which three behaviors will the client experience? (Choose three)

A. While the AP is in standalone mode, the client will be placed in VLAN 15.
B. While the AP is in standalone mode, the client will be placed in VLAN 10.
C. When the AP transitions to connected mode, the client will be de-authenticated.
D. While the AP is in standalone mode, the client will be placed in VLAN 13.
E. When the AP is in connected mode, the client will be placed in VLAN 13.
F. When the AP transitions to connected mode, the client will remain associated.
G. When the AP is in connected mode, the client will be placed in VLAN 15.
H. When the AP is in connected mode, the client will be placed in VLAN 10.

Answer: A D E

Question 17

Which three methods does Cisco DNA Center use to discover devices? (Choose three)

A. CDP
B. LLDP
C. SNMP
D. ping
E. NETCONF
F. a specified range of IP addresses

Answer: A B F

Question 18

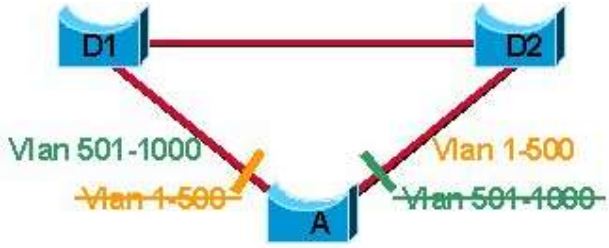
What would be the preferred way to implement a loopless switch network where there are 1500 defined VLANs and it is necessary to load the shared traffic through two main aggregation points based on the VLAN identifier?

A. 802.1D
B. 802.1s
C. 802.1W
D. 802.1AE

Answer: B

Explanation

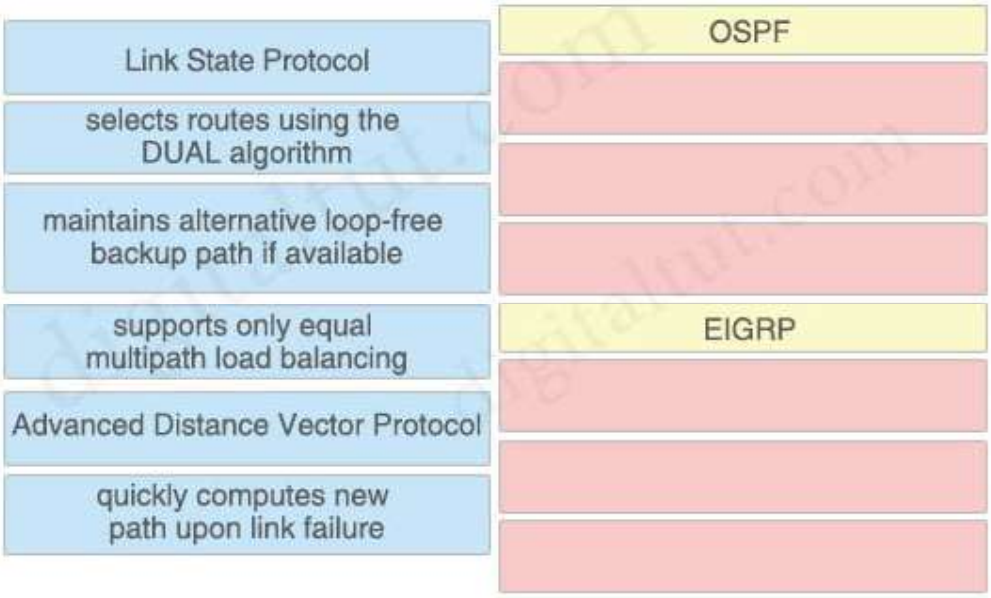
Where to Use MST
This diagram shows a common design that features access Switch A with 1000 VLANs redundantly connected to two distribution Switches, D1 and D2. In this setup, users connect to Switch A, and the network administrator typically seeks to achieve load balancing on the access switch Uplinks based on even or odd VLANs, or any other scheme deemed appropriate.



Reference: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html

Question 19

Drag and drop the characteristics from the left onto the routing protocols they describe on the right.



Answer:

OSPF
+ Link State Protocol
+ supports only equal multipath load balancing
+ quickly computes new path upon link failure

EIGRP
+ selects routes using the DUAL algorithm
+ maintains alternative loop-free backup path if available
+ Advanced Distance Vector Protocol

Explanation

EIGRP maintains alternative loop-free backup via the feasible successors. To qualify as a feasible successor, a router must have an Advertised Distance (AD) less than the Feasible distance (FD) of the current successor route.

Advertised distance (AD): the cost from the neighbor to the destination.
Feasible distance (FD): The sum of the AD plus the cost between the local router and the next-hop router

Question 20

How does the RIB differ from the FIB?

A. The RIB includes many routes to the same destination prefix. The FIB contains only the best route.
B. The FIB maintains network topologies and routing tables. The RIB is a list of routes to particular network destinations.
C. The RIB is used to create network topologies and routing tables. The FIB is a list of routes to particular network destinations.
D. The FIB includes many routes a single destination. The RIB is the best route to a single destination.

Answer: C

Question 21

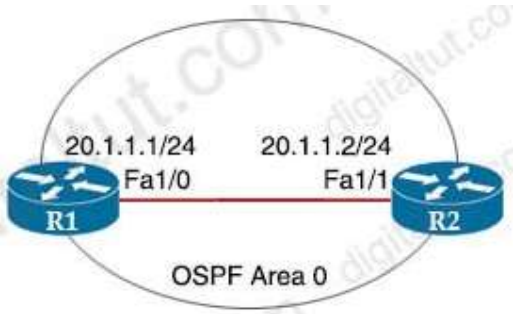
What is the purpose of an RP in PIM?

A. secure the communication channel between the multicast sender and receiver.
B. ensure the shortest path from the multicast source to the receiver.
C. receive IGMP joins from multicast receivers.
D. send join messages toward a multicast source SPT

Answer: C

Question 22

Refer to the exhibit.



Which command must be applied to R2 for an OSPF neighborship to form?

A. network 20.1.1.2 0.0.255.255 area 0
B. network 20.1.1.2 255.255.255.255 area 0
C. network 20.1.1.2 0.0.0.0 area 0
D. network 20.1.1.2 255.255.0.0. area 0

Answer: C

Explanation

The “network 20.0.0.0 0.0.0.255 area 0” command on R2 did not cover the IP address of Fa1/1 interface of R2 so OSPF did not run on this interface. Therefore we have to use the command “network 20.1.1.2 0.0.255.255 area 0” to turn on OSPF on this interface.

Note: The command “network 20.1.1.2 0.0.255.255 area 0” can be used too so this answer is also correct but answer C is the best answer here.

The “network 0.0.0.0 255.255.255.255 area 0” command on R1 will run OSPF on all active interfaces of R1.

Question 23

Which antenna type should be used for a site-to-site wireless connection?

A. Omnidirectional
B. Yagi
C. dipole
D. patch

Answer: B

Question 24

Refer to the exhibit. An engineer is using XML in an application to send information to a RESTCONF-enabled device. After sending the request, the engineer gets this response message and a HTTP response code of 400. What do these responses tell the engineer?

```
<errors xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
  <error>
    <error-message>End-of-file reached in XML
stream</error-message>
    <error-path>/ietf-interfaces:interfaces/interface=Giga
bitEthernet2</error-path>
    <error-tag>malformed-message</error-tag>
    <error-type>application</error-type>
  </error>
</errors>
```

A. POST was used instead of PUT to update
B. The Accept header sent was application/xml
C. The Content-Type header sent was application/xml.
D. JSON body was used

Answer: B

Explanation

Accept and Content-type are both headers sent from a client (a browser) to a service.
Accept header is a way for a client to specify the media type of the response content it is expecting and

Content-type is a way to specify the media type of request being sent from the client to the server.

The response was sent in XML so we can say the Accept header sent was application/xml.

Question 25

Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20? (Choose two)

```
DSW1#show spanning-tree

MST1
  Spanning tree enabled protocol mstp
  Root ID     Priority    32769
              Address     0018.7363.4300
              Cost        2
              Port        13 (FastEthernet1/0/11)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority 32769 (priority 32768 sys-id- ext 1)
              Address     001b.0d8e.e080
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role  Sts    Cost      Prio.Nbr  Type
---------------- ----- -------- --------  ---------- ------------
Fa1/0/7          Desg FWD  2         128.1     P2p Bound (PVST)
Fa1/0/10         Desg FWD  2         128.12    P2p Bound (PVST)
Fa1/0/11         Root FWD  2         128.13    P2p
Fa1/0/12         Altn BLK  2         128.14    P2p

DSW1#show spanning-tree mst

##### MST1    vlans mapped:  10,20
Bridge       address 001b.0d0e.e000 priority  32769 (32768 sysid 1)
Root         address 0018.7363.4300 priority  32769 (32768 sysid 1)
             port    Fa1/0/11       cost      2       (rem hops 19)

------ output omitted ------
```

A. spanning-tree mstp 1 priority 0
B. spanning-tree mst 1 root primary
C. spanning-tree mst vlan 10,20 priority root
D. spanning-tree mst 1 priority 4096
E. spanning-tree mst 1 priority 1
F. spanning-tree mstp vlan 10,20 root primary

Answer: B D

Explanation

From the second command output (show spanning-tree mst) we learn that MST1 includes VLANs 10 & 20. Therefore if we want DSW1 to become root bridge for these VLANs we need to set the MST 1 region to root -> The command “spanning-tree mst 1 root primary” can do the trick. In fact, this command runs a macro and sets the priority lower than the current root.

Also we can see the current root bridge for these VLANs has the priority of 32769 (default value + sysid) so we can set the priority of DSW1 to a specific lower value. But notice that the priority must be a multiple of 4096. Therefore D is a correct answer.

Question 26

Which feature of EIGRP is not supported in OSPF?

A. load balancing of unequal-cost paths
B. load balance over four equal-costs paths
C. uses interface bandwidth to determine best path
D. per-packet load balancing over multiple paths

Answer: A

Question 27

Which two characteristics define the Intent API provided by Cisco DNA Center? (Choose two)

A. northbound API
B. southbound API
C. device-oriented
D. business outcome oriented
E. procedural

Answer: A D

Explanation

The Intent API is a **Northbound REST API** that exposes specific capabilities of the Cisco DNA Center platform.
The Intent API provides policy-based abstraction of **business intent, allowing focus on an outcome** rather than struggling with individual mechanisms steps.

Reference: https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound

Question 28

What is the difference between CEF and process switching?

A. CEF processes packets that are too complex for process switching to manage.
B. CEF is more CPU-intensive than process switching.
C. CEF uses the FIB and the adjacency table to make forwarding decisions, whereas process switching punts each packet.
D. Process switching is faster than CEF.

Answer: C

Explanation

"Punt" is often used to describe the action of moving a packet from the fast path (CEF) to the route processor for handling.

Cisco Express Forwarding (CEF) provides the ability to switch packets through a device in a very quick and efficient way while also keeping the load on the router's processor low. CEF is made up of two different main components: the **Forwarding Information Base** (FIB) and the **Adjacency Table**.

Process switching is the slowest switching methods (compared to fast switching and Cisco Express Forwarding) because it must find a destination in the routing table. Process switching must also construct a new Layer 2 frame header for every packet. With process switching, when a packet comes in, the scheduler calls a process that examines the routing table, determines which interface the packet should be switched to and then switches the packet. The problem is, this happens for the every packet.

Reference: http://www.cisco.com/web/about/security/intelligence/acl-logging.html

Question 29

During deployment, a network engineer notices that voice traffic is not being tagged correctly as it traverses the network. Which COS to DSCP map must be modified to ensure that voice traffic is treated properly?

A. COS of 5 to DSCP 46
B. COS of 7 to DSCP 48
C. COS of 6 to DSCP 46
D. COS of 3 to DSCP of 26

Answer: A

Explanation

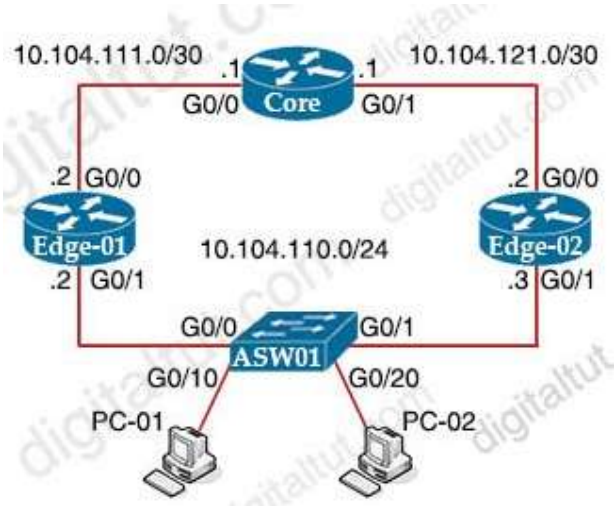
CoS value 5 is commonly used for VOIP and CoS value 5 should be mapped to DSCP 46. DSCP 46 is defined as being for EF (Expedited Forwarding) traffic flows and is the value usually assigned to all interactive voice and video traffic. This is to keep the uniformity from end-to-end that DSCP EF (mostly for VOICE RTP) is mapped to COS 5.

Note:

+ CoS is a L2 marking contained within an 802.1q tag,. The values for CoS are 0 – 7
+ DSCP is a L3 marking and has values 0 – 63
+ The default DSCP-to-CoS mapping for CoS 5 is DSCP 40

Question 30

Refer to the exhibit. Edge-01 is currently operational as the HSRP primary with priority 110. Which command on Edge-02 causes it to take over the forwarding role when Edge-01 is down?



A. standby 10 priority
B. standby 10 timers
C. standby 10 track
D. standby 10 preempt

Answer: D

Explanation

The “preempt” command enables the HSRP router with the highest priority to immediately become the active router.

Question 31

What is a Type 1 hypervisor?

A. runs directly on a physical server and depends on a previously installed operating system
B. runs directly on a physical server and includes its own operating system
C. runs on a virtual server and depends on an already installed operating system
D. run on a virtual server and includes its own operating system

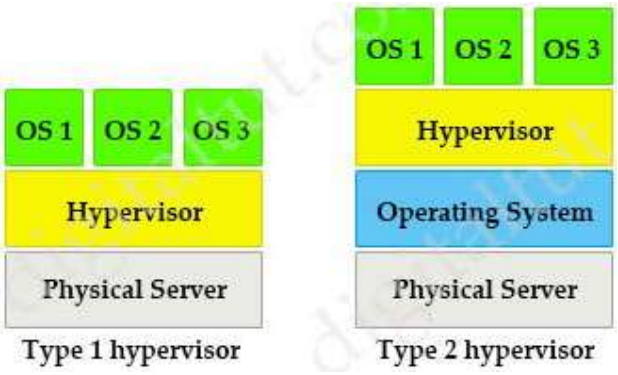
Answer: B

Explanation

There are two types of hypervisors: type 1 and type 2 hypervisor.

In type 1 hypervisor (or native hypervisor), the hypervisor is installed directly on the physical server. Then instances of an operating system (OS) are installed on the hypervisor. Type 1 hypervisor has direct access to the hardware resources. Therefore they are more efficient than hosted architectures. Some examples of type 1 hypervisor are VMware vSphere/ESXi, Oracle VM Server, KVM and Microsoft Hyper-V.

In contrast to type 1 hypervisor, a type 2 hypervisor (or hosted hypervisor) runs on top of an operating system and not the physical hardware directly. A big advantage of Type 2 hypervisors is that management console software is not required. Examples of type 2 hypervisor are VMware Workstation (which can run on Windows, Mac and Linux) or Microsoft Virtual PC (only runs on Windows).



Question 32

An engineer reviews a router's logs and discovers the following entry. What is the event's logging severity level?

```
Router# *Feb 03 11:13:44 334: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
```

A. error
B. notification
C. informational
D. warning

Answer: A

Explanation

Syslog levels are listed below:

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Number "3" in "%LINK-3-UPDOWN" is the severity level of this message so in this case it is "errors".

Question 33

Refer to the exhibit. An engineer attempts to configure a router on a stick to route packets between Clients, Servers, and Printers; however, initial tests show that this configuration is not working. Which command set resolves this issue?

```
interface Vlan10
 ip vrf forwarding Clients
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan20
 ip vrf forwarding Servers
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan30
 ip vrf forwarding Printers
 ip address 10.1.1.1 255.255.255.0
<output omitted>
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.1.0
```

Option A	**Option B**
router eigrp 1 network 10.0.0.0 255.0.0.0 network 172.16.0.0 255.255.0.0 network 192.168.1.0 255.255.0.0	router eigrp 1 network 10.0.0.0 255.255.255.0 network 172.16.0.0 255.255.255.0 network 192.168.1.0 255.255.255.0
Option C	**Option D**
interface Vlan10 no ip vrf forwarding Clients ! interface Vlan20 no ip vrf forwarding Servers ! interface Vlan30 no ip vrf forwarding Printers	interface Vlan10 no ip vrf forwarding Clients ip address 192.168.1.2 255.255.255.0 ! interface Vlan20 no ip vrf forwarding Servers ip address 172.16.1.2 255.255.255.0 ! interface Vlan30 no ip vrf forwarding Printers ip address 10.1.1.2 255.255.255.0

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

Answer: D

Explanation

We must reconfigure the IP address after assigning or removing an interface to a VRF. Otherwise that interface does not have an IP address.

Question 34

How is a data modeling language used?

A. To enable data to be easily structured, grouped validated, and replicated
B. To represent finite and well-defined network elements that cannot be changed

C. To model the flows of unstructured data within the infrastructure
D. To provide human readability to scripting languages

Answer: A

Explanation

Customer needs are fast evolving. Typically, a network center is a heterogenous mix of various devices at multiple layers of the network. Bulk and automatic configurations need to be accomplished. CLI scraping is not flexible and optimal. Re-writing scripts many times, even for small configuration changes is cumbersome. Bulk configuration changes through CLIs are error-prone and may cause system issues. The solution lies in using data models-a programmatic and standards-based way of writing configurations to any network device, replacing the process of manual configuration. Data models are written in a standard, industry-defined language. Although configurations using CLIs are easier (more human-friendly), automating the configuration using data models results in scalability.

Reference: https://www.cisco.com/c/en/us/td/docs/optical/ncs1000/60x/b_Datamodels_cg_ncs1000/b_Datamodels_cg_ncs1000_chapter_00.pdf

Question 35

Refer to the exhibit.

```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line vty 0 4
login authentication authorizationlist
```

What is the effect of the configuration?

A. The device will allow users at 192.168.0.202 to connect to vty lines 0 through 4 using the password ciscotestkey
B. The device will allow only users at 192 168.0.202 to connect to vty lines 0 through 4
C. When users attempt to connect to vty lines 0 through 4, the device will authenticate them against TACACS+ if local authentication fails
D. The device will authenticate all users connecting to vty lines 0 through 4 against TACACS+

Answer: D

Question 36

Refer to the exhibit. R1 is able to ping the R3 fa0/1 interface. Why do the extended pings fail?

```
R1#ping
Protocol [ip]:
Target IP address: 3.3.3.3
Repeat count [5]: 3
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 1.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)

Unreachable from 10.99.69.2, maximum MTU 1492, Received packet has options
Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
<output omitted>
```

A. R2 and R3 do not have an OSPF adjacency
B. R3 is missing a return route to 10.99.69.0/30
C. The maximum packet size accepted by the command is 1476 bytes
D. The DF bit has been set

Answer: D

Explanation

If the DF bit is set, routers cannot fragment packets. From the output below, we learn that the maximum MTU of R2 is 1492 bytes while we sent ping with 1500 bytes. Therefore these ICMP packets were dropped.

Note: Record option displays the address(es) of the hops (up to nine) the packet goes through.

Question 37

Refer to the exhibit. A network engineer configures a GRE tunnel and enters the show interface tunnel command. What does the output confirm about the configuration?

```
Tunnel100 is up, line protocol is up
 Hardware is Tunnel
 Internet address is 192.168.200.1/24
 MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation TUNNEL, loopback not set
 Keepalive set (10 sec), retries 3
 Tunnel source 209.165.202.129 (GigabitEthernet0/1)
  Tunnel Subblocks:
   src-track:
    Tunnel100 source tracking subblock associated with GigabitEthernet0/1
    Set of tunnels with source GigabitEthernet0/1, 1 members (includes iterators),
    on interface <OK>
 Tunnel protocol/transport GRE/IP
  Key disabled, sequencing disabled
  Checksumming of packets disabled
 Tunnel TTL 255, Fast tunneling enabled
 Tunnel transport MTU 1476 bytes
```

A. The keepalive value is modified from the default value.
B. Interface tracking is configured.
C. The tunnel mode is set to the default.
D. The physical interface MTU is 1476 bytes.

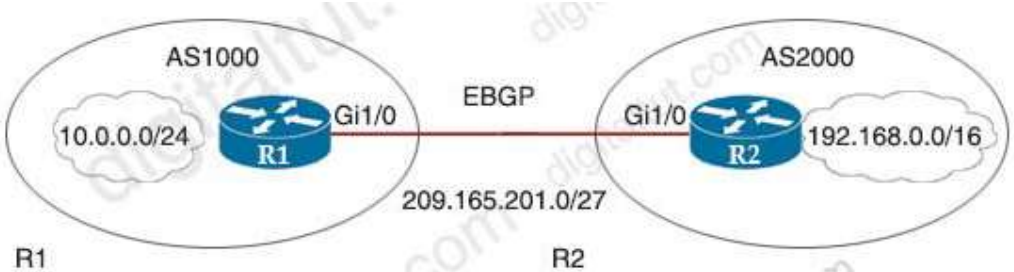
Answer: C

Explanation

From the "Tunnel protocol/transport GRE/IP" line, we can deduce this tunnel is using the default IPv4 Layer-3 tunnel mode. We can return to this default mode with the "tunnel mode gre ip" command.

Question 38

Refer to the exhibit. Which two commands are needed to allow for full reachability between AS 1000 and AS 2000? (Choose two)



R1
```
router bgp 1000
 address-family ipv4 unicast
  neighbor 209.165.201.2 remote-as 2000
  network 10.0.0.0 mask 255.255.255.0
  description Peer Router B
```

R2
```
router bgp 2000
 address-family ipv4 unicast
  neighbor 209.165.201.1 remote-as 1000
  network 10.0.0.0 mask 255.255.255.0
  description Peer Router A
```

A. R2#no network 10.0.0.0 255.255.255.0
B. R1#network 19.168.0.0 mask 255.255.0.0
C. R1#no network 10.0.0.0 255.255.255.0
D. R2#network 209.165.201.0 mask 255.255.192.0
E. R2#network 192.168.0.0 mask 255.255.0.0

Answer: A E

Question 39

Refer to the exhibit.

```
SW1#show monitor session all
Session 1
------------------
Type                  : Remote Destination Session
Source RSPAN VLAN     : 50

Session 2
------------------
Type                  : Local Session
Source Ports          :
        Both          : Fa0/14
  Destination Ports   : Fa0/15
  Encapsulation       : Native
  Ingress             : Disabled
```

An engineer configures monitoring on SW1 and enters the show command to verify operation. What does the output confirm?

A. SPAN session 1 monitors activity on VLAN 50 of a remote switch
B. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
C. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.
D. RSPAN session 1 is incompletely configured for monitoring

Answer: A

Explanation

SW1 has been configured with the following commands:

SW1(config)#monitor session 1 source remote vlan 50
SW1(config)#monitor session 1 destination interface fastethernet 0/14

SW1(config)#monitor session 2 source interface fa0/14
SW1(config)#monitor session 2 destination interface fa0/15

The session 1 on SW1 was configured for Remote SPAN (RSPAN) while session 2 was configured for local SPAN and this configuration was enough. The following configuration will complete RSPAN on the monitored switch:

Switch2(config)# monitor session 1 source interface FastEthernet 0/1
Switch2(config)# monitor session 1 destination remote vlan 50

With this configuration, traffic on FastEthernet0/1 of Switch 2 will be sent to Fa0/14 of SW1 via VLAN 50. Of course we have to configure trunking between two switches and set up “remote-vlan” feature on VLAN 50 on both switches with the following commands:

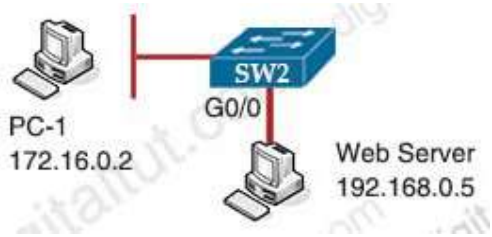
Switch1,2(config)#vlan 50

Switch1,2(config-vlan)#remote-span

Note: By default, both ingress and egress traffic of the source port are copied to the destination port.

Question 40

Refer to the exhibit. PC-1 must access the web server on port 8080. To allow this traffic, which statement must be added to an access control list that is applied on SW2 port G0/0 in the inbound direction?



A. permit host 172.16.0.2 host 192.168.0.5 eq 8080
B. permit host 192.168.0.5 host 172.16.0.2 eq 8080
C. permit host 192.168.0.5 eq 8080 host 172.16.0.2
D. permit host 192.168.0.5 it 8080 host 172.16.0.2

Answer: C

Explanation

The inbound direction of G0/0 of SW2 only filter traffic from Web Server to PC-1 so the source IP address and port is of the Web Server.

Question 41

Refer to the exhibit.

R1	R2
key chain cisco123 key 1 key-string Cisco123!	key chain cisco123 key 1 key-string Cisco123!
Ethernet0/0 - Group 10 State is Active 8 state changes, last state change 00:03:33 Virutal IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a	Ethernet0/0 - Group 10 State is Active 17 state changes, last state change 00:03:33 Virutal IP address is 192.168.0.1 Active virtual MAC address is 0000.0c07.ac0a

An engineer is installing a new pair of routers in a redundant configuration. Which protocol ensures that traffic is not disrupted in the event of a hardware failure?

A. HSRPv2
B. VRRP
C. GLBP
D. HSRPv1

Answer: D

Explanation

The “virtual MAC address” is 0000.0c07.acXX (XX is the hexadecimal group number) so it is using HSRPv1.

Note: HSRP Version 2 uses a new MAC address which ranges from 0000.0C9F.F000 to 0000.0C9F.FFFF.

Question 42

Refer to the exhibit.

```
aaa new-model
aaa authentication login default local-case enable
aaa authentication login ADMIN local-case
username CCNP secret Str0ngP@ssw0rd!
line 0 4
login authentication ADMIN
```

How can you change this configuration so that when user CCNP logs in, the show run command is executed and the session is terminated?

A. Add the autocommand keyword to the aaa authentication command
B. Assign privilege level 15 to the CCNP username
C. Add the access-class keyword to the aaa authentication command
D. Assign privilege level 14 to the CCNP username
E. Add the access-class keyword to the username command
F. Add the autocommand keyword to the username command

Answer: F

Explanation

The “autocommand” causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line. In this specific question, we have to enter this line “username CCNP autocommand show running-config”.

Question 43

Refer to the exhibit. What does the error message relay to the administrator who is trying to configure a Cisco IOS device?

```
<?xml version="1.0" encoding="utf-8"?>
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
```

A. A NETCONF request was made for a data model that does not exist.
B. The device received a valid NETCONF request and serviced it without error.
C. A NETCONF message with valid content based on the YANG data models was made, but the request failed.
D. The NETCONF running datastore is currently locked.

Answer: A

Explanation

Missing Data Model RPC Error Reply Message
If a request is made for a data model that doesn't exist on the Catalyst 3850 or a request is made for a leaf that is not implemented in a data model, the Server (Catalyst 3850) responds with an empty data response. This is expected behavior.

Reference: https://www.cisco.com/c/en/us/support/docs/storage-networking/management/200933-YANG-NETCONF-Configuration-Validation.html

Question 44

In an SD-WAN deployment, which action in the vSmart controller responsible for?

A. handle, maintain, and gather configuration and status for nodes within the SD-WAN fabric
B. onboard vEdge nodes into the SD-WAN fabric
C. gather telemetry data from vEdge routers
D. distribute policies that govern data forwarding performed within the SD-WAN fabric

Answer: D

Explanation

Control plane (vSmart) builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.

Question 45

What does Call Admission Control require the client to send in order to reserve the bandwidth?

A. SIP flow information
B. Wi-Fi multimedia
C. traffic specification
D. VoIP media session awareness

Answer: D

Comments

1. Ban7
   September 17th, 2020

   thanks

2. Hans
   September 17th, 2020

   q1 why not A,B?

   q3 C,D looks correct.

3. Joe
   September 17th, 2020

   Thank you Digital Tut

4. Joe
   September 17th, 2020

   Are there more Qns too coming our way ?

5. AL
   September 17th, 2020

   Thanks for all the effort and work you put in to this site as it very helpful especially the labs and tutorials offered.

6. Joe
   September 18th, 2020

   Fully agree @AL. Keep up the work you guys !!!!!

7. Ban7
   September 18th, 2020

   @Digitaltut, Thanks again for those new questions I am going to give the exam next week, unfortunatly I have a dead line, i hope you guys can release more questions even in small amount just to increase the rating chances to pass the exam. Thank you guys for the good work and for the accurate Job you guys do.

8. Hans
   September 18th, 2020

   Can anyone confirm Q1?
   Which two LISP infrastructure elements are needed to support LISP to non -LISP internetworking? (Choose two)

   Proxy ingress tunnel router (PITR): A PITR is an infrastructure LISP network entity that receives packets from non-LISP sites and encapsulates the packets to LISP sites or natively forwards them to non-LISP sites.

   Proxy egress tunnel router (PETR): A PETR is an infrastructure LISP network entity that de-encapsulates packets from LISP sites to deliver them to non-LISP sites.

   Map server (MS): An MS configures LISP site policy to authenticate when LISP sites try to register to the MS. It also performs the following functions:

   Provides a service interface to the ALT router and injects routes in the ALT BGP when the site registers.

   Receives MAP requests over the ALT router and encapsulates them to registered ETRs.

   Map resolver (MR): The MR performs the following functions:

   Receives MAP requests, which are encapsulated by ITRs.

   Provides a service interface to the ALT router, de-encapsulates MAP requests, and forwards on the ALT topology.