CCNP ENCOR v8 Certification Practice Exam Answers

itexamanswers.net/ccnp-encor-v8-certification-practice-exam-answers.html

January 4, 2021

CCNPv8 ENCOR (Version 8.0) – CCNP ENCOR Certification Practice Exam

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which two statements are true about NTP servers in an enterprise network? (Choose two.)

- **NTP servers at stratum 1 are directly connected to an authoritative time source.**
- All NTP servers synchronize directly to a stratum 1 time source.
- NTP servers control the mean time between failures (MTBF) for key network devices.
- There can only be one NTP server on an enterprise network.
- **NTP servers ensure an accurate time stamp on logging and debugging information.**

Explanation: Network Time Protocol (NTP) is used to synchronize the time across all devices on the network to make sure accurate timestamping on devices for managing, securing and troubleshooting. NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum 1 devices are directly connected to the authoritative time sources.

2. The command ntp server 10.1.1.1 is issued on a router. What impact does this command have?

- identifies the server on which to store backup configurations
- determines which server to send system log files to
- ensures that all logging will have a time stamp associated with it
- **synchronizes the system clock with the time source with IP address 10.1.1.1**

Explanation: The ntp server ip-address global configuration command configures the NTP server for IOS devices.

3. A network engineer has to decide between a Layer 2 Access Layer (STP-based) and a Layer 3 Access Layer (Routed access) campus design option. Which statement must be considered for a decision to be made?

- The STP based option does not require FHRP, whereas the Routed access option does.
- **The Routed access option offers easier troubleshooting than the STP-based option.**
- The STP based access option supports spanning VLANs across multiple access switches, whereas the Routed access option does not.
- The Routed access option is the best cost-effective solution.

Explanation: The Routed access design has a number of advantages over the STP-based design:

No FHRP required – no need for FHRP protocols such as HSRP and VRRP.
No STP required – since there are no L2 links to block, this design removes the need for STP.
Easier troubleshooting – It offers common end-to-end troubleshooting tools (such as ping and traceroute).
The Routed access is an excellent design for many environments, but it has the same limitation as the STP-based design, in which it does not support spanning VLANs across multiple access switches. Additionally, it might not be the most cost-effective solution because access layer switches with Layer 3 routing capability might cost more than Layer 2 switches do.

4. Which three functions are performed at the distribution layer of the hierarchical network model? (Choose three.)

- **isolates network problems to prevent them from affecting the core layer**
- **provides a connection point for separate local networks**
- **forwards traffic that is destined for other networks**
- allows end users to access the local network
- transports large amounts of data between different geographic sites
- forwards traffic to other hosts on the same logical network

Explanation: The primary function of the distribution layer is to aggregate access layer switches in a given building or campus. The distribution layer provides a boundary between the Layer 2 domain of the access layer and the Layer 3 domain of the core. On the Layer 2 side, it creates a boundary for Spanning Tree Protocol (STP), limiting propagation of Layer 2 faults. On the Layer 3 side, it provides a logical point to summarize IP routing information when it enters the core Layer. The summarization reduces IP route tables for easier troubleshooting and reduces protocol overhead for faster recovery from failures.

5. Which SD-Access feature uses telemetry to enable proactive prediction of network-related and security-related risks.

- policy enforcement
- **network assurance and analytics**
- network virtualization
- network automation

Explanation: Through the use of telemetry, the network assurance and analytics feature of SD-Access improves the performance of the network through proactive prediction of network-related and security-related risks.

6. Which function is provided by the Cisco SD-Access Architecture management layer?

- It delivers data packets to and from the network devices participating in SD-Access.
- It interconnects all of the network devices, forming a fabric of interconnected nodes.
- **It presents all information to the user on a centralized dashboard.**
- It provides all of the management subsystems for the management layer.

Explanation: The management layer of the Cisco SD-Access Architecture abstracts all the complexities and dependencies of the other layers and provides the user with GUI tools and workflows to manage and operate the Cisco DNA network.

7. Which SD-WAN solution architecture component authenticates the vSmart controllers and SD-WAN routers and facilitates their ability to join the network?

- vManage Network Management System
- vAnalytics
- **vBond orchestrator**
- vSmart controller

Explanation: The Cisco SD-WAN solution has four main components:
The vManage Network Management System (NMS) is the single pane of glass for managing the SD-WAN solution.
The vSmart controller acts as the brains of the solution.
The SD-WAN routers serve vEdge and cEdge routers.
The vBond orchestrator authenticates and orchestrates connectivity between SD-WAN routers and vSmart controllers.

8. What two factors are used to achieve end-to-end QoS in the DiffServ model? (Choose two.)

- **DSCP**
- **PHB**
- PCP

- DEI
- VLAN ID

Explanation: IIn order to deliver end-to-end QoS, DiffServ architecture has two major components, packet marking using the IPv4 ToS byte and PHBs. The Differentiated Services (DS) field uses 6 bits to classify packets. DSCP uses the leftmost six bits from the ToS byte in the IPv4 header to specify class of service for each IP packet to form the DiffServ (DS) field. With 6 bits, DSCP has up to 64 DSCP values (0 to 63) that are assigned to various classes of traffic. These selective values are called per-hop behaviors (PHB) and determine how packets are treated at each hop along the path from the source to the destination.

9. What QoS category level is recommended as the best to be configured on a Cisco WLC for VoIP traffic?

- gold
- bronze
- silver
- **platinum**

Explanation: VoIP traffic is extremely sensitive to delay, and the QoS category to be set for this type of traffic on a Cisco WLC is platinum.

10. What are the two main components of Cisco Express Forwarding (CEF)? (Choose two.)

- **adjacency tables**
- routing tables
- MAC-address tables
- **forwarding information base (FIB)**
- ARP tables

Explanation: The forwarding information base (FIB) and adjacency tables are the main components of CEF. The FIB is similar to a routing table, but neither the routing table, nor the ARP table, nor the MAC-address table is part of CEF.

11. What is used to pre-populate the adjacency table on Cisco devices that use CEF to process packets?

- **the ARP table**
- the routing table
- the FIB
- the DSP

Explanation: CEF uses the FIB and adjacency table to make fast forwarding decisions without control plane processing. The adjacency table is pre-populated by the ARP table and the FIB is pre-populated by the routing table.

12. Which technology is part of the Cisco ENFV and provides centralized and consistent network policies across enterprise branch offices?

- Cisco ENCS
- Cisco UCS
- **Cisco DNA center**
- Cisco ISE

Explanation: Cisco DNA Center is a main component of the Cisco NFV solution that provides centralized consistent policies across enterprise branch offices.

13. What is an I/O technology that allows multiple VNFs to share the same pNIC?

- PCI Passthrough
- Open vSwitch
- **SR-IOV**
- OVS-DPDK

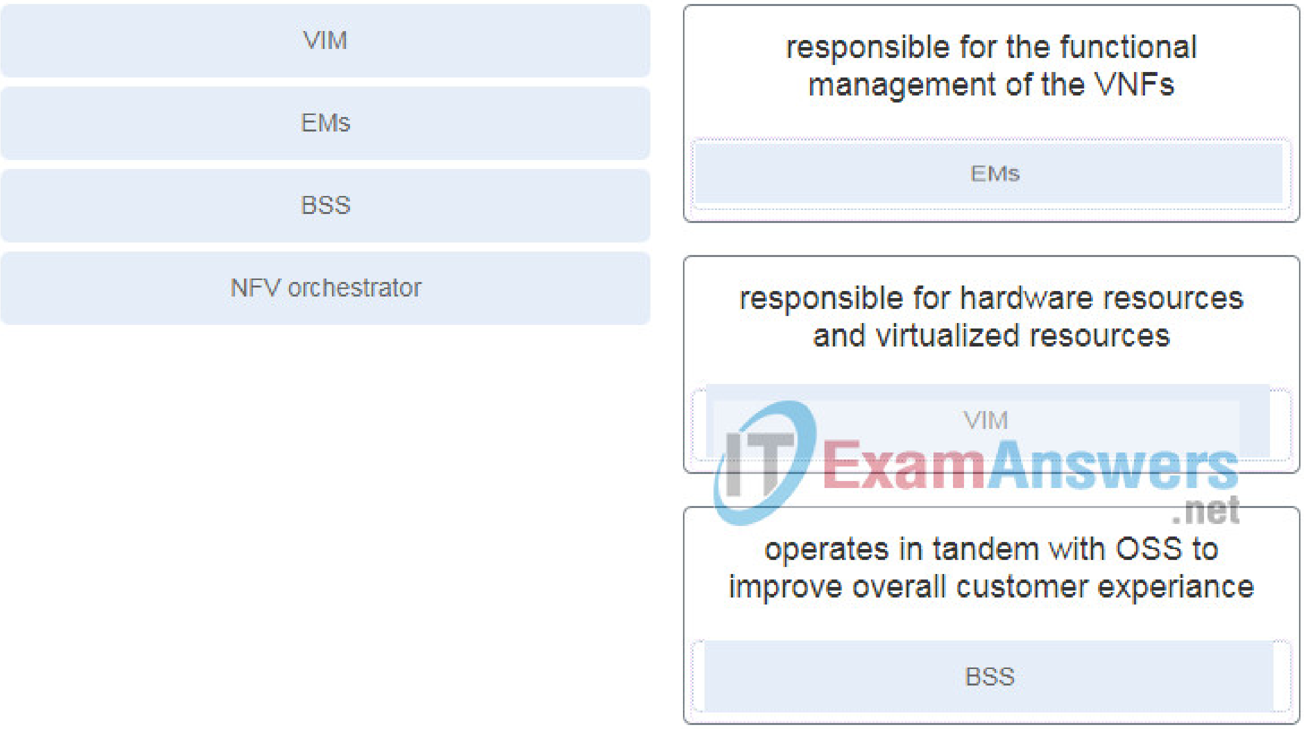
Explanation: SR-IOV is an enhancement to PCI passthrough that allows multiple VNFs to share the same pNIC.

14. Which two are functions of LISP? (Choose two.)

- **It is an overlay tunneling technology.**
- It performs load balancing of SD-WAN routers across vSmart controllers.
- **It is an architecture created to address routing scalability problems.**
- It provides a permanent control plane connection over a DTLS tunnel.
- It authenticates vSmart controllers and SD-WAN routers.

Explanation: Locator/Identifier Separation Protocol (LISP) is used by Internet providers, data centers, branch networks, and campus networks to address routing scalability problems and provide an overlay tunneling technology. LIST separates IP addresses into endpoint identifiers (EID) and routing locators (RLOCs) so endpoints can roam from site to site with only the RLOC changing. An egress tunnel router (ETR), ingress tunnel router (ITR), proxy ETR, proxy ITR, or xTR, a device that is both an ETR and an ITR, are used to connect LISP and non-LISP sites in a variety of ways.

15. Match the VNF role with its description. (Not all options are used.)



VIM

EMs

BSS

NFV orchestrator

responsible for the functional management of the VNFs

EMs

responsible for hardware resources and virtualized resources

VIM

operates in tandem with OSS to improve overall customer experiance

BSS

- **EMS** : responsible for the functional management of the VNFs
- **VIM** : responsible for hardware resources and virtualized resources
- **BSS** : operates in tandem with OSS to improve overall customer experiance

Explanation: Virtual Network Function (VNF) is a software version of a network function that runs on the hypervisor as a VM.
Virtualized Infrastructure Manager (VIM) is responsible for controlling NFVI hardware resources and virtualized resources.
Element Managers (EMs) are responsible for the functional management of the VMs.
NFV orchestrator is responsible for creating, maintaining and tearing down VNF services.
Business Support System (BSS) works in tandem with OSS (platform typically operated by service providers) to improve overall customer experience.

16. Which vitualization component allows communication between VMs within a virtual server?

- container engine
- **vSwitch**
- pNIC
- hypervisor

Explanation: In a virtualized server the vSwitch is connected to external networks through physical NICs (pNICs) and to VMs through virtual NICs (vNICs).

17. A teacher is explaining the concept of virtual switch (vSwitch) to students in a classroom. What explanation accurately describe a vSwitch?

- A vSwitch is a software-based Layer 3 switch that operates like a physical switch.
- Multiple vSwitches can be created under a virtualized server, allowing network traffic to flow directly from one vSwitch to another within the same host.
- A vSwitch is a cluster of switches forming a virtual switching system (VSS).
- **A vSwitch enables VMs to communicate with external physical networks through physical nework interface cards.**

Explanation: A virtual switch (vSwitch) is a software-based Layer 2 switch that operates like a physical Ethernet switch. A vSwitch enables VMs to communicate with each other within a virtualized server and with external physical networks through the physical network interface cards (pNICs.) Multiple vSwitches can be created under a virtualized server, but network traffic cannot flow directly from one vSwitch to another vSwitch within the same host, and the vSwitches cannot share the same pNIC.

18. What are two characteristics of virtual routing that are different from traditional routing? (Choose two.)

- **VRF allows for overlapping IP address ranges.**
- VRF requires the use of the BGP routing protocol.
- VRF requires creating subinterfaces if VRF is to be enabled.
- **Each VRF instance has its own routing table.**
- VRF takes advantages of Layer 2 technologies such as spanning tree.

Explanation: Virtual routing and forwarding (VRF) is a Layer 3 technology used to create separate virtual routers on a physical router. Each VRF instance has associated router interface(s) or subinterface(s), routing table, and forwarding table. Overlapping and even duplicate IP addresses can be used when using VRF because VRF creates segmentation between the interfaces, IP addresses, and routing tables.

19. What is a key difference between a virtual machine and a virtualized container?

- A virtual machine starts much faster than a virtualized container does.
- A virtual machine uses physical memory to run and a virtualized container uses virtualized memory.
- A virtual machine requires a type 1 hypervisor and a virtualized container requires a type 2 hypervisor.
- **A virtual machine contains its own OS and a virtualized container does not.**

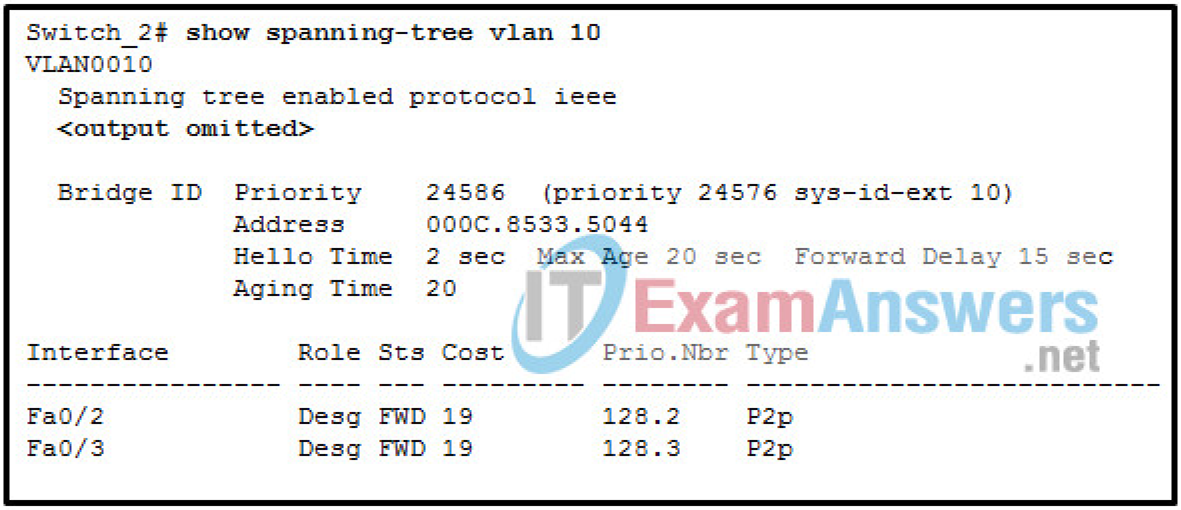
Explanation: A virtual machine (VM) is a software emulation of a physical server with an operating system. A container is an isolated environment where containerized applications run. Containers all share the same OS while remaining isolated from each other. They all use virtualized memory managed by the hypervisor. Because a container does not have a guest OS, it relies on the host operating system to provide underlying services. It typically takes a few seconds to start.

20. A network engineer wants to increase the overall efficiency and cost-effectiveness of a server by maximizing the use of available resources through virtualization. The engineer is considering VMs or containers. What is the difference between these two types of virtualization?

- **VMs take minutes to start, whereas containers take seconds to start.**
- VMs do not include a guest OS, whereas containers do.
- VMs require a type 1 hypervisor directly on the system hardware, whereas containers require a type 2 hypervisor.
- VMs share the same operating system, whereas each container requires a dedicated operating system.

Explanation: Each VM on a server has an dedicated OS and all containers on a server share the host OS while remaining isolated from each other. A VM contains a guest OS. Containers do not contain one, so they are lightweight (small in size). When a VM starts, the guest OS needs to load first, and once it is operational, the application in the VM can then start and run. This whole process may take minutes. When a container starts, it leverages the kernel of the host OS, which is already running, and it typically takes a few seconds to start.

21. Refer to the exhibit. A network administrator is verifying the bridge ID and the status of this switch in the STP election. Which statement is correct based on the command output?



```
Switch_2# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  <output omitted>

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     000C.8533.5044
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

- The bridge priority of Switch_2 has been lowered to a predefined value to become the backup root bridge.
- **The bridge priority of Switch_2 has been lowered to a predefined value to become the root bridge.**

- The STP instance on Switch_2 is using the default STP priority and the election is based on Switch_2 MAC address.
- The STP instance on Switch_2 is failing due to no ports being blocked and all switches believing they are the root.

Explanation: The priority value 24576 is a predefined value that is implemented by the command spanning-tree vlan 10 root primary . This command configures Switch_2 to become the root switch. A root switch will have all forwarding interfaces and no root ports.

22. Which three describe characteristics of a virtual machine? (Choose three.)

- it is an isolated environment for applications
- **it includes a guest OS**
- it shares the underlying resources of the host OS
- it leverages the kernel of the host OS for quick starts
- **it is a virtualized physical server**
- **it requires a hypervisor**

Explanation: A virtual machine is a software emulation of a physical server including a CPU, memory, network interface, and operating system. The hypervisor is virtualization software that performs hardware abstraction. It allows multiple VMs to run concurrently in the virtual environment.

23. What is a characteristic of the PortFast feature?

- PortFast enables a Cisco Catalyst switch to move a port into blocking state when an attached workstation link comes up.
- **A trunk port can be configured with PortFast if it connects to a hypervisor host.**
- PortFast can only be used for STP host ports.
- PortFast prevents alternative ports from becoming designated ports.

Explanation: One of the major benefits of the STP PortFast feature is that the access ports bypass the earlier 802.1D STP states (learning and listening) and forward traffic immediately. PortFast can be enabled on trunk links, but only with ports that are connecting to a single host, such as a server with only one NIC that is running a hypervisor with VMs on different VLANs.

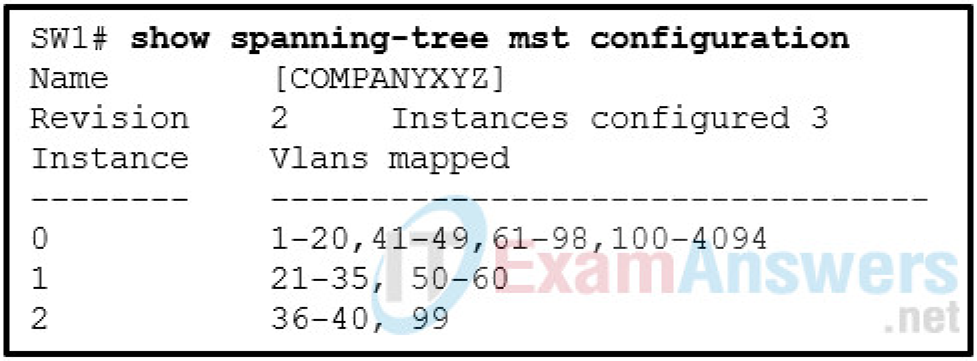
24. Which three spanning tree protocols are industry standards? (Choose three.)

- PVST+
- **MSTP**
- Rapid PVST+

- **STP**
- MST
- **RSTP**

Explanation: STP is the 802.1D standard. RSTP is the 802.1W standard. MSTP is the 802.1S standard. MST, PVST+, and Rapid PVST+ are Cisco proprietary.

25. Refer to the exhibit. A network administrator issues the show spanning-tree mst configuration command to verify the MST configuration. How many VLANs are assigned to IST?

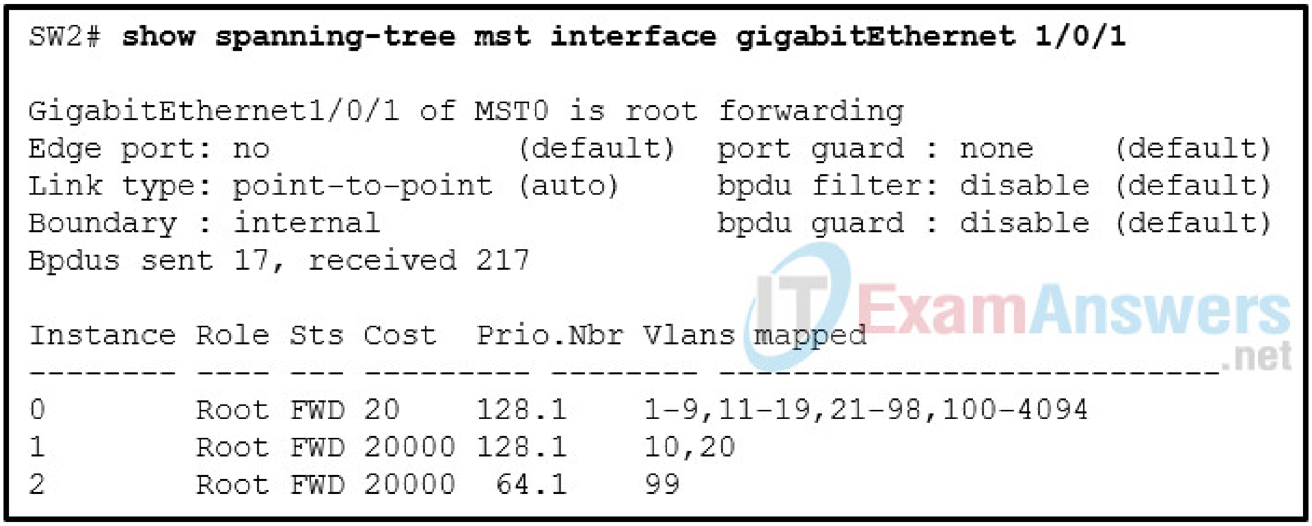


```
SW1# show spanning-tree mst configuration
Name          [COMPANYXYZ]
Revision      2     Instances configured 3
Instance      Vlans mapped
--------      ----------------------------------
0             1-20,41-49,61-98,100-4094
1             21-35, 50-60
2             36-40, 99
```

- 4060
- **4062**
- 4064
- 4094

Explanation: By default, all VLANs are assigned to IST before VLANs are assigned to other instances. In the configuration shown, IST contains all VLANs except for the 32 VLANs assigned to instances 1 and 2, which is 4062 VLANs.

26. Refer to the exhibit. A network administrator is verifying the MST configuration on the switch SW2 with the command:



```
SW2# show spanning-tree mst interface gigabitEthernet 1/0/1

GigabitEthernet1/0/1 of MST0 is root forwarding
Edge port: no              (default)  port guard : none    (default)
Link type: point-to-point  (auto)     bpdu filter: disable (default)
Boundary : internal                   bpdu guard : disable (default)
Bpdus sent 17, received 217

Instance Role Sts Cost  Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- ---------------------------
0        Root FWD 20    128.1    1-9,11-19,21-98,100-4094
1        Root FWD 20000 128.1    10,20
2        Root FWD 20000  64.1    99
```

```
SW2# show spanning-tree mst interface gigabitEthernet 1/0/1
```

Which three conclusions can be drawn based on the output? (Choose three.)

- **The priority value of the gigbitEthernet 1/0/1 port is adjusted for the instance 2.**
- **The gigbitEthernet 1/0/1 port does not connect to another switch that is out of the region.**
- The gigbitEthernet 1/0/1 port connects to the internet through a WAN connection.
- **The cost value of the gigbitEthernet 1/0/1 port is adjusted for IST.**
- SW2 does not support the BPDU guard feature.
- SW2 does not support the BPDU filter feature.

Explanation: Based on the output, three conclusions can be drawn:
The interface gigbitEthernet 1/0/1 port is not an Edge port. It is inside the region.
The cost value on the interface gigbitEthernet 1/0/1 port is adjusted to 20 from 20000 for instance 0.
The priority value on the interface gigbitEthernet 1/0/1 port is adjusted to 64 from 128 for instance 2.

27. What are two drawbacks to turning spanning tree off and having multiple paths through the Layer 2 switch network? (Choose two.)

- Port security shuts down all of the ports that have attached devices.
- **Broadcast frames are transmitted indefinitely.**
- **The MAC address table becomes unstable.**
- Port security becomes unstable.
- The switch acts like a hub.

Explanation: Spanning tree should never be disabled. Without it, the MAC address table becomes unstable, broadcast storms can render network clients and the switches unusable, and multiple copies of unicast frames can be delivered to the end devices.

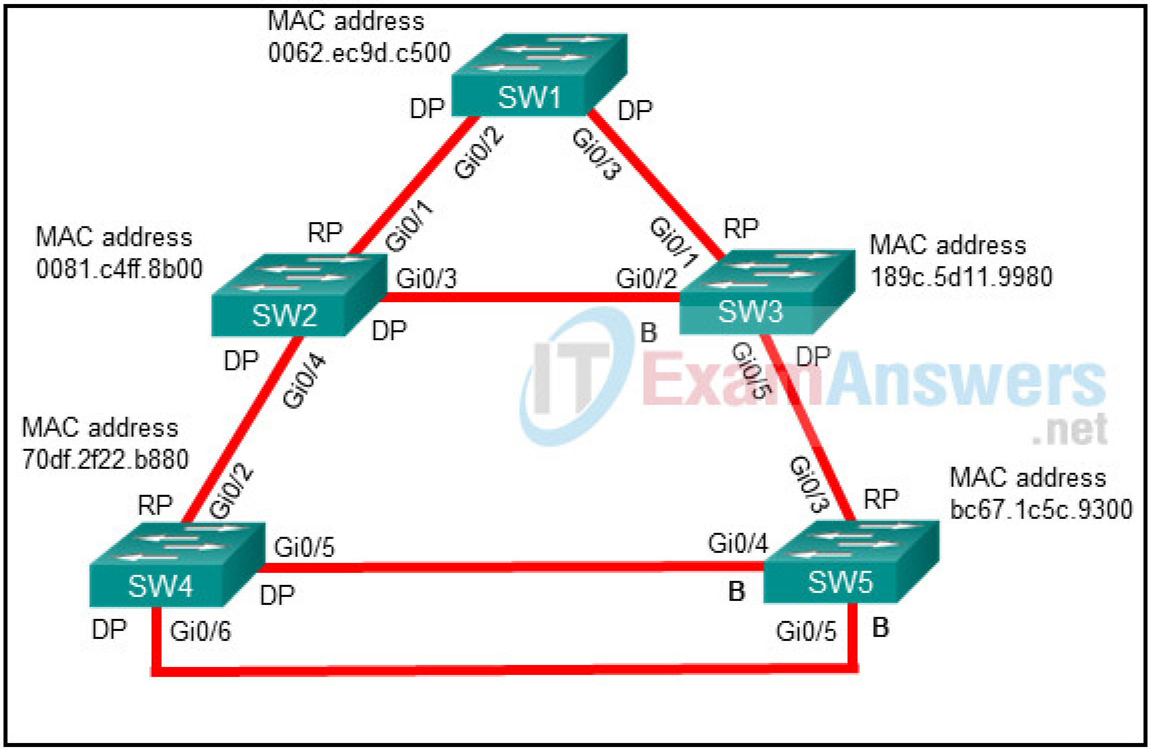
28. Network users complain that the network is running very slowly. Upon investigation, a network technician discovers 100% link utilization on all the network devices. Also, numerous syslog messages are being generated that note continuous MAC address relearning. What is the most likely cause of the problem?

- The routing protocol has been misconfigured and a routing loop is evident.
- **A Layer 2 STP looping condition is present.**
- The dynamic routing protocol has not yet converged the network.
- An incorrect encapsulation has been configured on one of the trunks that connect a Layer 2 device to a Layer 3 device within the affected segment.

- Keepalives are expected but do not arrive.

Explanation: High CPU consumption and low free memory space are common symptoms of a Layer 2 forwarding loop. In Layer 2 forwarding loops, besides constantly consuming switch bandwidth, the CPU spikes as well. As the packet is received on a different interface, the switch must move the MAC address from one interface to the next. The network throughput is impacted drastically, users will probably notice a slow-down on their network applications, and the switches might crash because of an exhausted CPU and low memory resources.

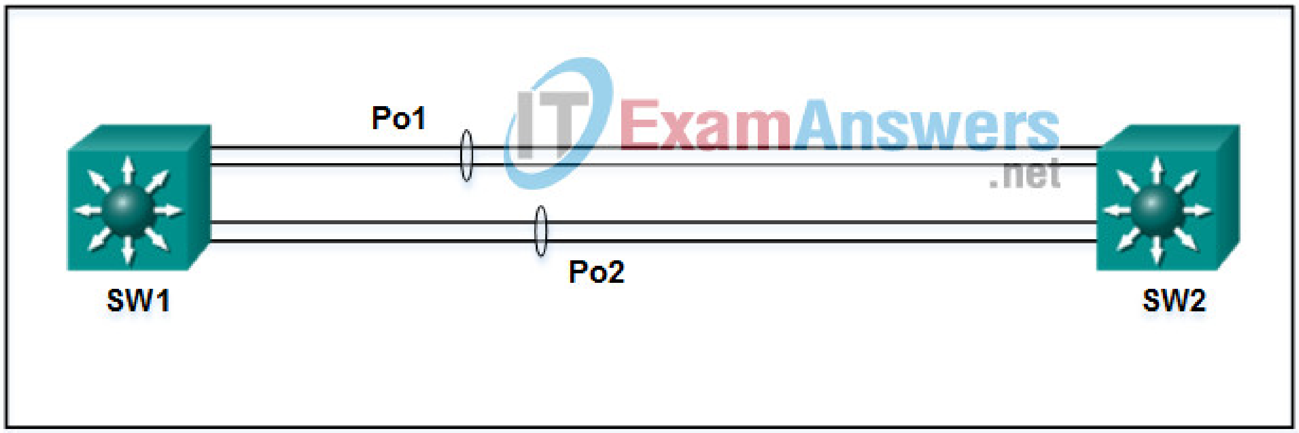
29. Refer to the exhibit. SW1 is the root bridge and SW2 is the backup root bridge. An administrator wants to prevent SW4 and SW5 from ever becoming root bridges, but still allow SW2 to maintain connectivity to SW1 via SW3 if the link connecting SW1 to SW2 fails. On which two ports in this topology should the administrator configure root guard to accomplish this? (Choose two.)



- SW5 Gi0/3 port toward SW3
- **SW2 Gi0/4 port toward SW4**
- **SW3 Gi0/5 port toward SW5**
- SW4 Gi0/6 port toward SW5
- SW4 Gi0/2 port toward SW2

Explanation: Root guard is an STP feature that is enabled on a port-by-port basis. It prevents a configured port from becoming a root port. Root guard prevents a downstream switch from becoming a root bridge in a topology. Root guard is placed on designated ports toward other switches that should never become root bridges. In order to prevent SW4 and SW5 from becoming root bridges, root guard has to be placed on SW2 Gi0/4 port toward SW4 and on SW3 Gi0/5 port toward SW5.

30. Refer to the exhibit. A network administrator has connected two switches together using EtherChannel technology. If STP is running, what will be the end result?



- The resulting loop will create a broadcast storm.
- The switches will load balance and utilize both EtherChannels to forward packets.
- Both port channels will shutdown.
- **STP will block one of the redundant links.**

Explanation: Cisco switches support two protocols for negotiating a channel between two switches: LACP and PAgP. PAgP is Cisco-proprietary. In the topology shown, the switches are connected to each other using redundant links. By default, STP is enabled on switch devices. STP will block redundant links to prevent loops.

31. A new switch is to be added to an existing network in a remote office. The network administrator does not want the technicians in the remote office to be able to add new VLANs to the switch, but the switch should receive VLAN updates from the VTP domain. Which two steps must be performed to configure VTP on the new switch to meet these conditions? (Choose two.)

- Enable VTP pruning.
- Configure all ports of both switches to access mode.
- **Configure the existing VTP domain name on the new switch.**
- **Configure the new switch as a VTP client.**
- Configure an IP address on the new switch.

Explanation: Before the switch is put in the correct VTP domain and in client mode, the switch must be connected to any other switch in the VTP domain through a trunk in order to receive/transmit VTP information.

32. An OSPF router is forming an adjacency with a neighbor and sends the neighbor an OSPF DBD packet describing the contents of its link-state database. During which OSPF neighbor state does the router send the packet?

- **exchange**
- 2-Way
- attempt
- loading

Explanation: In the exchange OSPF neighbor state, two routers exchange link states using DBD packets that summarize their link-state databases.

33. Which IPv6 address is used by OSPFv3 DR and BDR routers for sending link-state updates?

- FF02::2
- **FF02::5**
- FF02::6
- FF02::9

Explanation: OSPFv3 DR/BDR routers send link-state updates and link acknowledgments to the AllSPFRouter IPv6 multicast address of FF02::5.

34. A network administrator is configuring the MST instance priority with the command spanning-tree mst 0 prioritypriority. Which two numbers can be used for the priority argument? (Choose two.)

- 2048
- **4096**
- 6144
- **12288**
- 18432

Explanation: In MST operation, the instance priority is a value between 0 and 61,440, in increments of 4096.

35. A network administrator is configuring MST on switch SW1 with the commands:

```
SW1(config)# spanning-tree mode mst
SW1(config)# spanning-tree mst 12 root primary
```

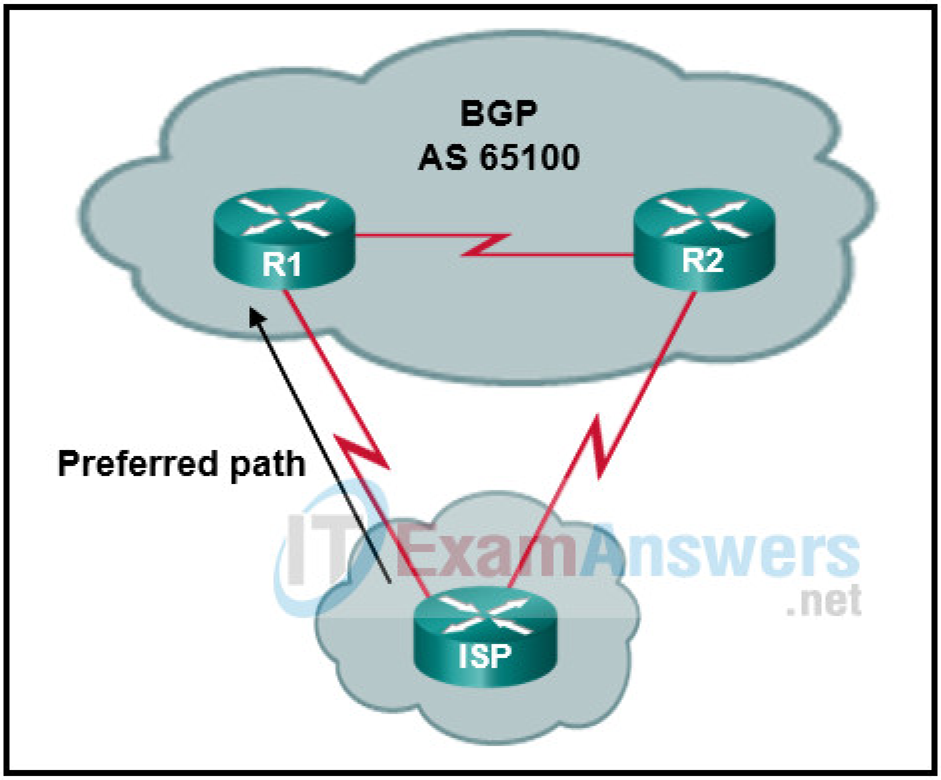
What is the effect after the command is entered?

- The bridge priority on switch SW1 is set to 32768 for MST instance 12.

- The bridge priority on switch SW1 is set to 28672 for MST instance 12.
- The bridge priority on switch SW1 is set to 20480 for MST instance 12.
- **The bridge priority on switch SW1 is set to 24576 for MST instance 12.**

Explanation: In MST configuration, an MST instance priority can be defined in one of two methods:
spanning-tree mst instance-number priority priority , where the priority is a value between 0 and 61,440, in increments of 4096
spanning-tree mst instance-number root { primary | secondary }[diameter diameter], where the primary keyword sets the priority to 24,576, and the secondary keyword sets the priority to 28,672

36. Refer to the exhibit. A network administrator in autonomous system 65100 has set up a dual-homed BGP connection with an ISP. The administrator would like to ensure that all traffic from the ISP enters the autonomous system through the router R1. Which BGP attribute can the administrator configure on routers R1 and R2 to accomplish this?



- next-hop
- weight
- aggregate
- **multiple-exit discriminator**
- local preference

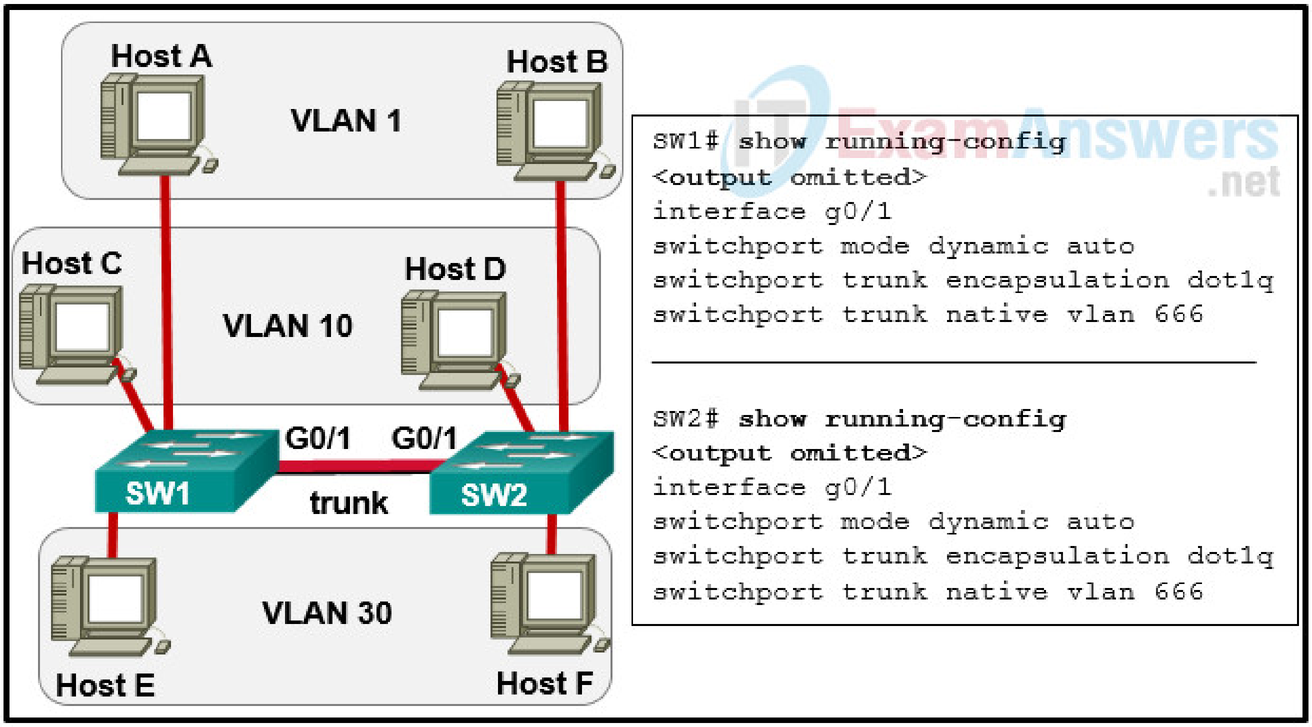
Explanation: The multiple-exit discriminator (MED) is a nontransitive BGP attribute for best-path determination. MED uses a 32-bit value (0 to 4,294,967,295) called a metric. The purpose of MED is to influence traffic flows inbound from a different AS. A lower MED is preferred over a higher MED.

37. A technician is configuring the channel on a wireless router to either 1, 6, or 11. What is the purpose of adjusting the channel?

- **to avoid interference from nearby wireless devices**
- to disable broadcasting of the SSID
- to enable different 802.11 standards
- to provide stronger security modes

Explanation: Channels 1, 6, and 11 are selected because they are 5 channels apart. thus minimizing the interference with adjacent channels. A channel frequency can interfere with channels on either side of the main frequency. All wireless devices need to be used on nonadjacent channels.

38. Refer to the exhibit. The network administrator configures both switches as displayed. However, host C is unable to ping host D and host E is unable to ping host F. What action should the administrator take to enable this communication?



```
SW1# show running-config
<output omitted>
interface g0/1
switchport mode dynamic auto
switchport trunk encapsulation dot1q
switchport trunk native vlan 666
```

```
SW2# show running-config
<output omitted>
interface g0/1
switchport mode dynamic auto
switchport trunk encapsulation dot1q
switchport trunk native vlan 666
```

- **Configure either trunk port in the dynamic desirable mode.**
- Add the switchport nonegotiate command to the configuration of SW2.
- Remove the native VLAN from the trunk.

- Associate hosts A and B with VLAN 10 instead of VLAN 1.
- Include a router in the topology.

Explanation: If one trunk port is in auto DTP negotiation mode, a trunk will be formed if the adjacent switch port is placed in trunk or dynamic desirable mode.

39. What is a function of IGMP snooping?

- updating static MAC entries on ports that should receive multicast traffic from certain sources or groups
- **learning and maintaining multicast group memberships**
- restricting multicast packets for IP multicast groups that have downstream receivers
- updating receiver applications to filter out unwanted traffic

Explanation: IGMP snooping reduces multicast flooding on a LAN segment by learning and maintaining multicast group memberships at the Layer 2 level.

40. Which OSPF packet type contains a summary of the link state database and is sent by an OSPF router as it forms an adjacency with a neighboring OSPF router?

- hello
- link-state ack
- link-state update
- **database description**

Explanation: After hello packets are exchanged, an OSPF router sends a database description packet summarizing its link-state database to its neighbors.

41. An administrator is configuring a pre-shared key for a WLAN environment. The administrator wants to protect the WLAN against any man-in-the-middle attacks occurring during the four-way handshake between the client and the AP. Which WPA3-Personal method will provide the best security?

- Diffie-Hellman method
- not authenticating against a server
- RSA key
- **SAE method**

Explanation: WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) method to strengthen the key exchange between the clients and AP.

42. Which OSPF network type includes the DR/BDR field in OSPF Hello packets and uses a 10 seconds hello and 40 seconds dead interval timer?

- point-to-point
- point-to-multipoint
- **broadcast**
- nonbroadcast

Explanation: The broadcast network type is the default for OSPF Ethernet links and includes the DR/BDR field in hellp packets and uses a 10 seconds hello and 40 seconds dead interval.

43. What are two advantages of using multiple OSPF areas? (Choose two.)

- They allow for unequal cost load balancing.
- **The link-state database is a more manageable size.**
- **They permit configuration of route summarization.**
- DR/BDR elections are not required.
- All areas share an identical link-state database.

Explanation: There are several key advantages to using multiarea vs single area OSPF:
Shortest path first (SPF) tree calculations are contained within an area when a link flaps.
The LSDB is more manageable.
Summarization of route information can occur.

44. Which LSA type is sent by an OSPF DR to advertise attached multiaccess network segments?

- **type 2**
- type 3
- type 4
- type 5

Explanation: An OSPF DR advertises attached multiaccess network segments with the type 2 network LSA.

45. What are two characteristics of OSPF type 3 LSAs? (Choose two.)

- They are originated by DRs and BDRs.
- **They are originated by ABRs.**
- They advertise specific networks that are external to the OSPF process
- **They advertise network prefixes from other areas.**
- They are contained within the originating area.

Explanation: Type 3 LSAs are originated by ABRs to advertise networks learned from other areas.

46. A company is deploying a wireless network using lightweight APs. What is an advantage of Layer 2 roaming compared with Layer 3 roaming when wireless clients roam around the campus?

- **The process of Layer 2 roaming is faster.**
- A wireless client can keep the same IP address.
- The roaming does not involve a WLC.
- DHCP service is not required.

Explanation: Both Layer 2 and Layer 3 roams are intercontroller roaming. In intercontroller roaming, a client roams from one AP to another AP that is bound to a different WLC. If both APs are configured with the same VLAN and IP address subnet, the client has made a Layer 2 intercontroller roam and it stays on the same VLAN and subnet. The process of Layer 2 roaming is faster than Layer 3 roaming (usually less than 20 ms). Both Layer 2 roaming and Layer 3 roaming allow the client to keep the same IP address.

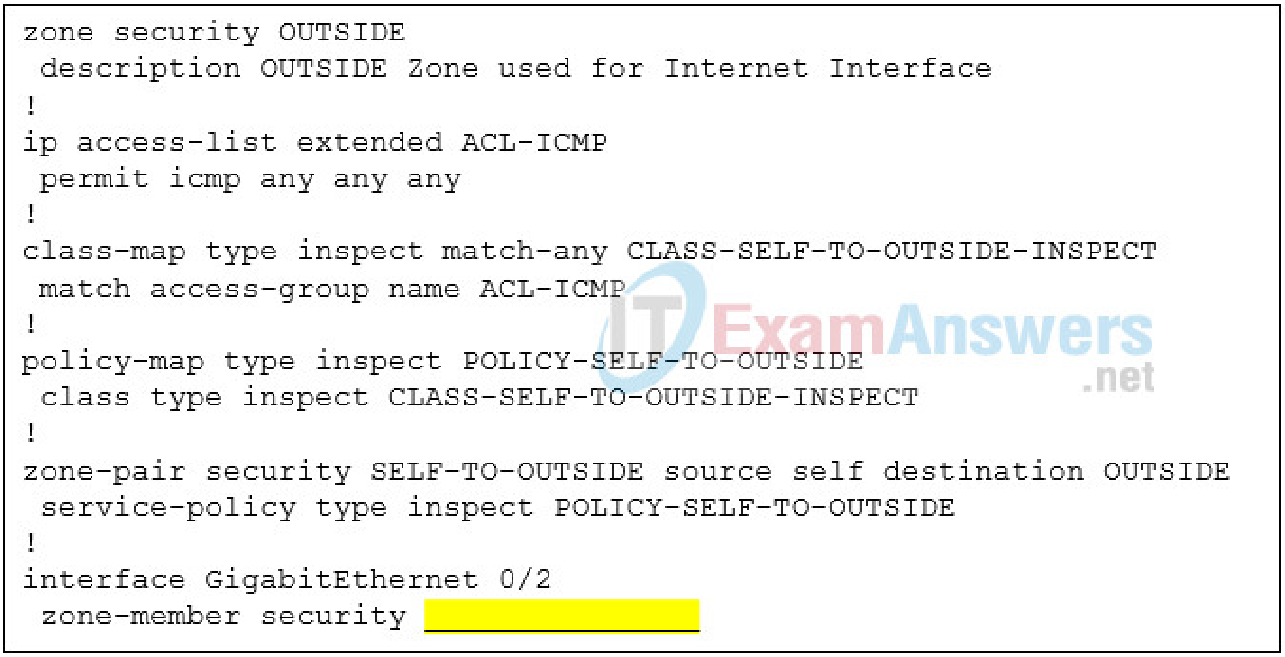
47. How is ERSPAN used for troubleshooting?

- to capture network traffic on a remote switch and send a copy of it to the local switch through Layer 2 toward a local port attached to a traffic analyzer
- to capture network traffic on a switch port and send it to a VLAN
- **to capture network traffic on a remote device and send it to the local system through Layer 3 toward a local port attached to a traffic analyzer**
- to capture local network traffic on a switch and send a copy of it to a local port attached to a traffic analyzer

Explanation: Catalyst switches provide the Switched Port Analyzer (SPAN), which makes it possible to capture packets by using the following techniques:

- Local Switched Port Analyzer. Local network traffic is captured on a switch and a copy of it is sent to a local port attached to a traffic analyzer.
- Remote Switched Port Analyzer (RSPAN). Network traffic is captured on a remote switch and a copy of it is sent to the local switch through Layer 2 (switching) toward a local port attached to a traffic analyzer.
- Encapsulated Remote Switched Port Analyzer (ERSPAN). Network traffic is captured on a remote device and it is sent to the local system through Layer 3 (routing) toward a local port attached to a traffic analyzer.

48. Refer to the exhibit. Which zone-member security command keyword will complete the ZBFW configuration when applied to the GigabitEthernet 0/2 interface?



```
zone security OUTSIDE
 description OUTSIDE Zone used for Internet Interface
!
ip access-list extended ACL-ICMP
 permit icmp any any any
!
class-map type inspect match-any CLASS-SELF-TO-OUTSIDE-INSPECT
 match access-group name ACL-ICMP
!
policy-map type inspect POLICY-SELF-TO-OUTSIDE
 class type inspect CLASS-SELF-TO-OUTSIDE-INSPECT
!
zone-pair security SELF-TO-OUTSIDE source self destination OUTSIDE
 service-policy type inspect POLICY-SELF-TO-OUTSIDE
!
interface GigabitEthernet 0/2
 zone-member security ______________
```

- POLICY-SELF-TO-OUTSIDE
- CLASS-SELF-TO-OUTSIDE-INSPECT
- ACL-ICMP
- **OUTSIDE**

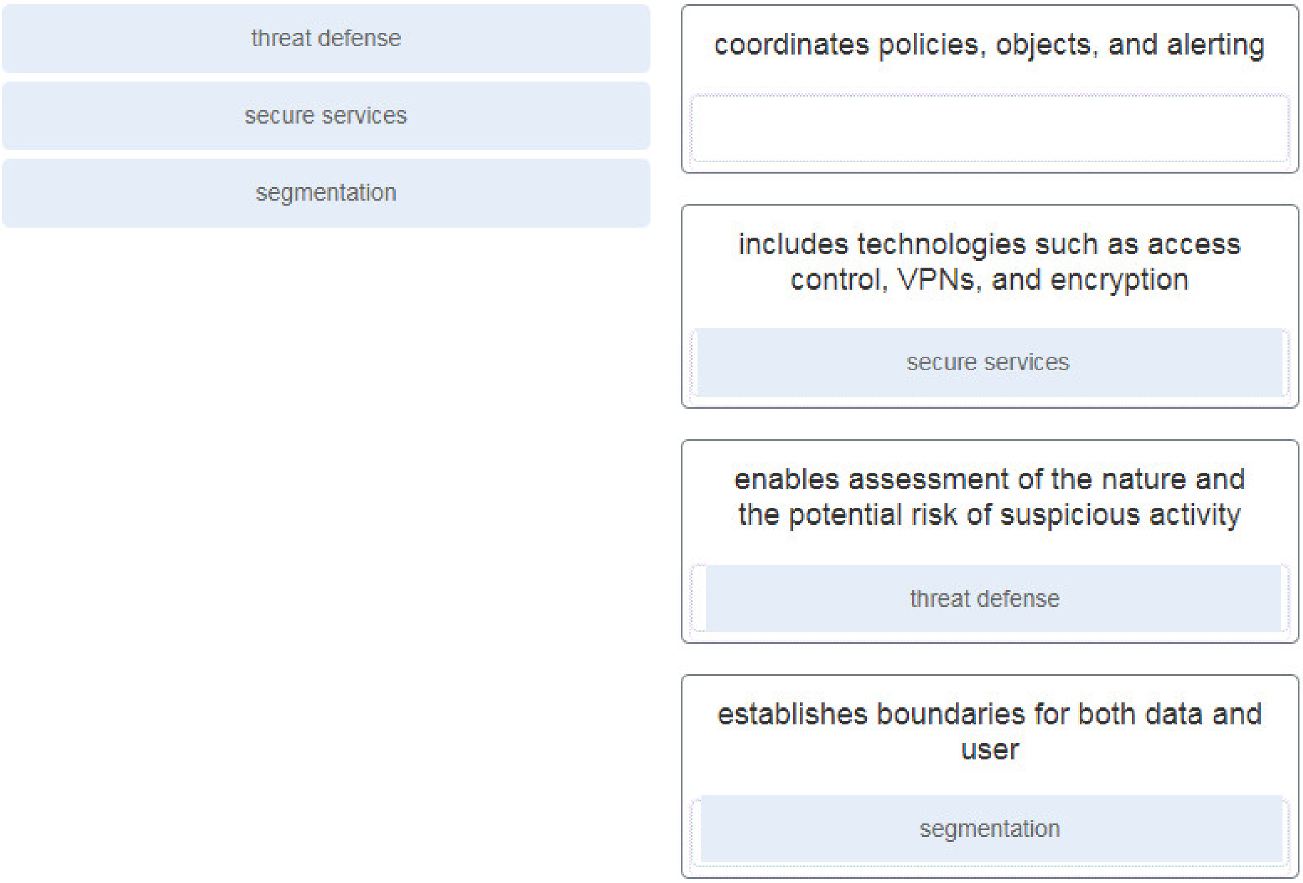
Explanation: To complete the ZBFW configuration the zone-member security OUTSIDE command must be issued to GigabitEthernet 0/2.

49. What is a limitation of PACLs?

- **They do not support outbound filtering.**
- They support only extended ACLs.
- They can filter only Layer 2 traffic.
- They support only numbered ACLs.

Explanation: PACLs have some limitations and restrictions. PACLs do not support filtering of outbound traffic on an interface, and they do not support ACLs to filter IPv6 traffic.

50. Match the Cisco SAFE security concepts with the description. (Not all options are used.)



threat defense

secure services

segmentation

coordinates policies, objects, and alerting

includes technologies such as access control, VPNs, and encryption

secure services

enables assessment of the nature and the potential risk of suspicious activity

threat defense

establishes boundaries for both data and user

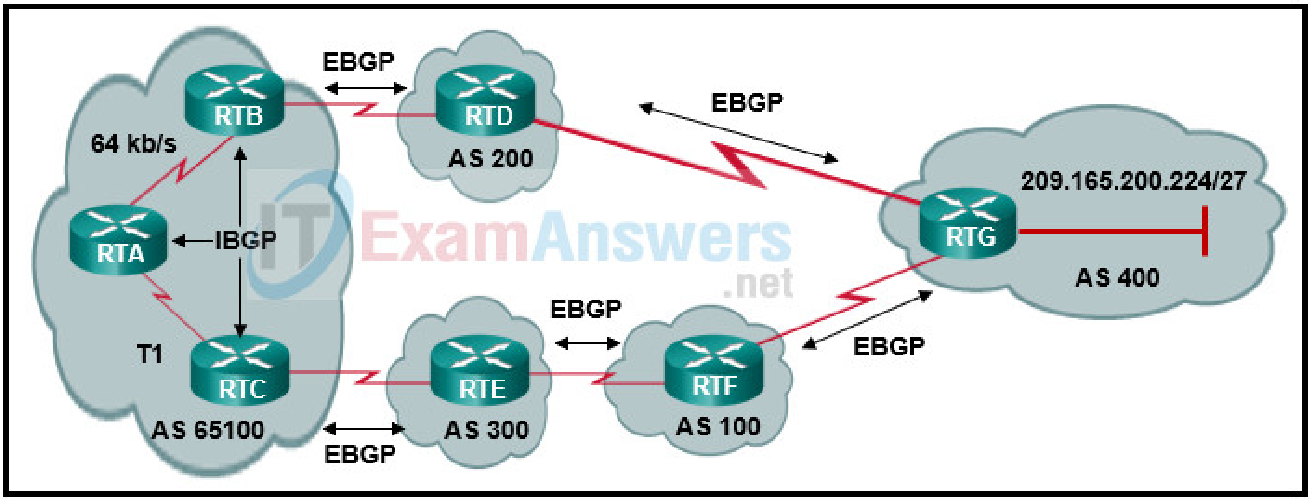
segmentation

51. An organization is deploying a network access security policy for end point devices to access the campus network. The IT department has configured multiple network access control mechanisms, such as 802.1x, WebAuth, and MAB. WebAuth and MAB are configured as fallbacks to 802.1x. What is the authentication process when an employee brings a laptop and connects to a switch on the network?

- The switch will initiate authentication by WebAuth protocol. If it fails, the switch will try 802.1x next, then MAB.
- The switch will initiate authentication by 802.1x protocol. If it fails, the switch will try WebAuth next, then MAB.
- **The switch will initiate authentication by 802.1x protocol. If it fails, the switch will try MAB next, then WebAuth.**
- The switch will initiate authentication by MAB protocol. If it fails, the switch will try 802.1x next, then WebAuth.

Explanation: When an organization deploys network access control, MAB and WebAuth can be used as a fallback authentication mechanism for 802.1x. If both MAB and WebAuth are configured as fallbacks for 802.1x, when 802.1x times out, a switch first attempts to authenticate through MAB, and if it fails, the switch attempts to authenticate with WebAuth.

52. Refer to the exhibit. BGP sessions are established between all routers. RTC receives route updates for network 209.165.200.224/27 from autonomous system 300 with the weight attribute set to 3000. RTB also learns about network 209.165.200.224/27 from autonomous system 200 with a weight of 2000. Which router will be used by RTA as a next hop to reach this network?



- RTC because of the T1 link
- RTB because of the slow 64 kbps link
- **RTB because of the shortest AS_Path**
- RTC because of the highest weight
- RTC because of the longest AS_Path
- RTB because of the lowest weight

Explanation: The BGP best-path algorithm uses attributes for the best-path selection. The top 5 attributes, ranked in order of consideration, are the following:
1. Weight.
2. Local preference.
3. Local originated (network statement, redistribution, or aggregation).
4. AIGP.
5. Shortest AS_Path.

BGP weight is a Cisco-defined attribute and is a 16-bit value assigned locally on the router; it is not advertised to other routers. Thus, the weight attributes as specified in RTD and RTE have no effect in RTA for determining the best outbound path. Assuming that the attributes in ranks 2 to 4 are not specified, the shortest AS_Path attribute is used to choose the outbound path when two paths are available.

53. A company plans to deploy the Postman application as a tool to manage network devices. Which two security related best practices should be considered? (Choose two.)

- An SSH connection should be used to connect to the Postman application.
- **User accesses must be authenticated to make API calls.**
- **A dedicated instance for development should be used to ensure that device configurations are valid.**
- AAA service should be deployed for user authorization.
- ACLs should be used to verify and filter different types of RUSTFul API calls.

Explanation: RESTful APIs are software interfaces into an application or a controller. For security considerations, access to APIs should require authentication such that an API is considered just like any other device to which a user needs to authenticate to gain access to utilize the APIs. A developer who is authenticated has access to making changes using the API, changes that can affect that application. It is best practice to use a dedicated development instance of the application to test change codes to avoid accidental impact to a production environment.

54. Which tool can be used to identify wireless RF signal strength and interference?

- WLAN controller
- packet analyzer
- packet sniffer
- **spectrum analyzer**

Explanation: Spectrum analyzers are designed to detect and measure RF energy that is present in those frequency ranges at 2.4 GHz and 5 GHz. A spectrum analyzer takes RF radio information, whether it is from wireless access points or other equipment using the free ISM band, and puts it into a visible display format.

55. When JSON data format is being used, what characters are used to hold objects?

- **double braces { }**
- double brackets [ ]
- double quotations ” “
- double colons : :

Explanation: A JavaScript Object Notation (JSON) object is a key-value data format that is typically rendered in curly braces { }.

56. What is a characteristic of PIM dense mode?

- It relies on a unicast routing protocol to perform Reverse Path Check.
- **It is not recommended for production environments.**
- Prunes are sent out on all RPF interfaces.

- Prunes are not sent out of non-RPF interfaces.

Explanation: Because Pim dense mode uses more bandwidth during its periodic flood and prune behavior, it is not recommended for production environments.

57. Which automation tool is agentless and uses playbooks to deploy configuration changes or retrieve information from hosts within a network?

- **Ansible**
- Puppet
- SaltStack
- Chef

Explanation: Ansible is an agentless automation tool that uses playbooks to deploy configuration changes or retrieve information from hosts. The Ansible playbook is a structured set of instructions used to enforce configuration and deployment steps or to retrieve information from hosts.

58. A network administrator is configuring the MST instance priority with the command spanning-tree mst 0 priority priority . Which two numbers can be used for the priority argument? (Choose two.)

- 2048
- **4096**
- 6144
- **12288**
- 18432

Explanation: In MST operation, the instance priority is a value between 0 and 61,440, in increments of 4096.

59. What is a requirement to configure a trunking EtherChannel between two switches?

- The participating interfaces must be on the same module on a switch.
- **The allowed range of VLANs must be the same on both switches.**
- The participating interfaces must be assigned the same VLAN number on both switches.
- The participating interfaces must be physically contiguous on a switch.

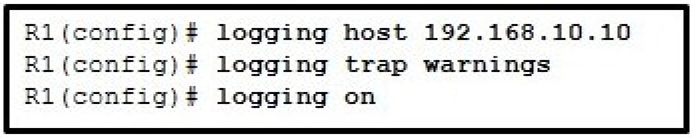
Explanation: To enable a trunking EtherChannel successfully, the range of VLANs allowed on all the interfaces must match; otherwise, the EtherChannel cannot be formed. The interfaces involved in an EtherChannel do not have to be physically contiguous, or on the same module. Because the EtherChannel is a trunking one, participating interfaces are configured as trunk mode, not access mode.

60. Which three packet types are exchanged between EIGRP neighbors? (Choose three.)

- LSU
- database descriptor
- link-state ACK
- **hello**
- **query**
- **request**

Explanation: There are five EIGRP packet types exchanged between EIGRP routers:
Hello
Request
Update
Query
Reply

61. Refer to the exhibit. Which two statements describe the results of entering these commands? (Choose two.)

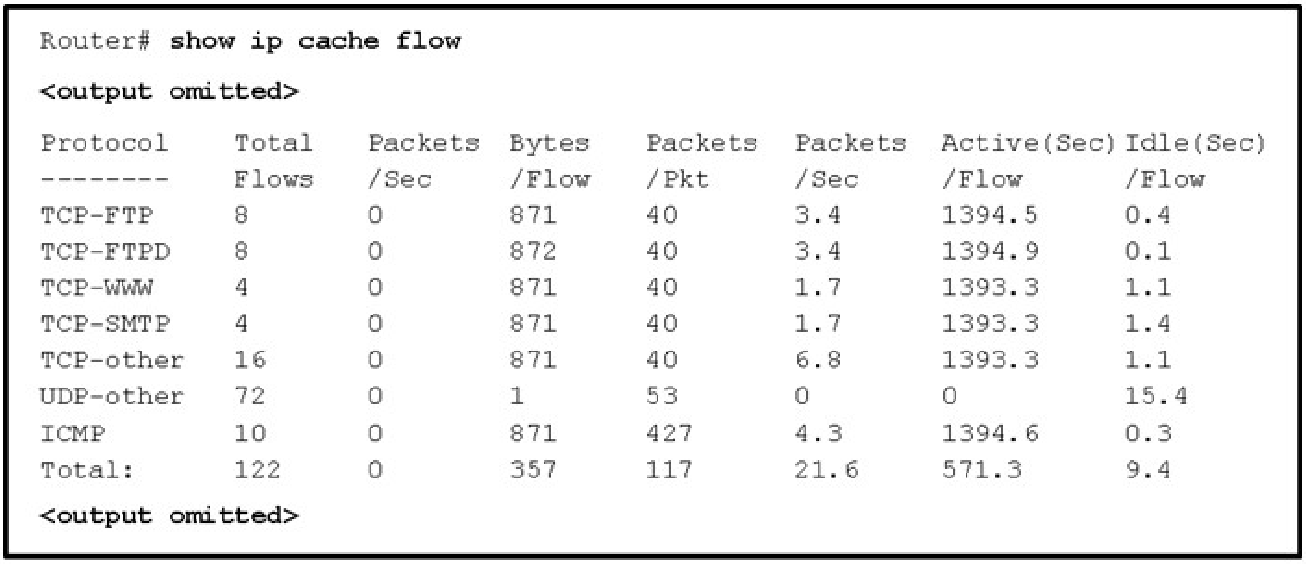


```
R1(config)# logging host 192.168.10.10
R1(config)# logging trap warnings
R1(config)# logging on
```

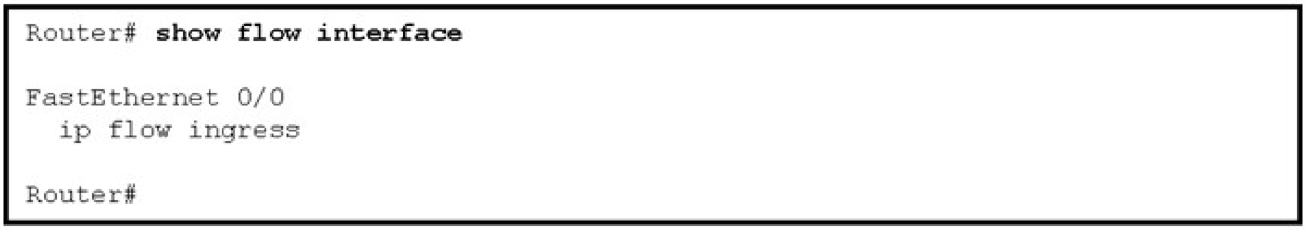
- **R1 will send system messages of levels 0 (emergencies) to level 4 (warnings) to a server.**
- **The syslog server has the IPv4 address 192.168.10.10.**
- R1 will not send critical system messages to the server until the command debug all is entered.
- R1 will reset all the warnings to clear the log.
- R1 will output the system messages to the local RAM.

Explanation: System messages of levels 0 (emergencies) through 4 (warnings) are sent to the syslog server at 192.168.10.10.

62. Refer to the exhibit. The total number of packet flows is not consistent with what is expected by the network administrator. The results show only half of the flows that are typically captured for the interface. Pings between the router and the collector are successful. What is the reason for the unexpected results?



```
Router# show ip cache flow

<output omitted>

Protocol    Total    Packets  Bytes   Packets  Packets  Active(Sec) Idle(Sec)
--------    Flows    /Sec     /Flow   /Pkt     /Sec     /Flow       /Flow
TCP-FTP     8        0        871     40       3.4      1394.5      0.4
TCP-FTPD    8        0        872     40       3.4      1394.9      0.1
TCP-WWW     4        0        871     40       1.7      1393.3      1.1
TCP-SMTP    4        0        871     40       1.7      1393.3      1.4
TCP-other   16       0        871     40       6.8      1393.3      1.1
UDP-other   72       0        1       53       0        0           15.4
ICMP        10       0        871     427      4.3      1394.6      0.3
Total:      122      0        357     117      21.6     571.3       9.4

<output omitted>
```

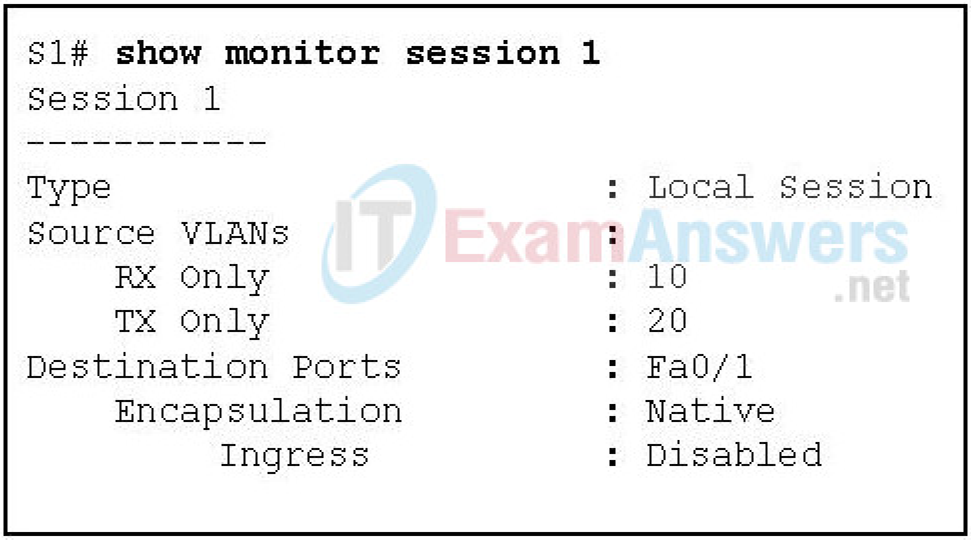


```
Router# show flow interface

FastEthernet 0/0
  ip flow ingress

Router#
```

- Interface Fa0/0 is not configured as the source of the packets sent to the collector.
- The interface is shutdown.
- The Netflow collector IP address and UDP port number are not configured on the router.
- **The router is not configured to monitor outgoing packets on the interface.**

Explanation: NetFlow flows are unidirectional. One user connection exists as two flows. The flow in each direction must be captured. This is done by using both the ip flow ingress and ip flow egress command on the interface.

63. Refer to the exhibit. Based on the output generated by the show monitor session 1 command, how will SPAN operate on the switch?



```
S1# show monitor session 1
Session 1
-----------
Type                      : Local Session
Source VLANs              :
    RX Only               : 10
    TX Only               : 20
Destination Ports         : Fa0/1
    Encapsulation         : Native
         Ingress          : Disabled
```

- All traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- **All traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.**

Explanation: The show monitor session command is used to verify how SPAN is configured (what ports are involved in the traffic mirroring).

64. Which two statements describe items to be considered in configuring NetFlow? (Choose two.)

- **NetFlow consumes additional memory.**
- Netflow requires UDP port 514 for notification messages.
- NetFlow can only be used if all devices on the network support it.
- Netflow requires both management and agent software.
- **Netflow can only be used in a unidirectional flow.**

Explanation: NetFlow consumes additional memory to accommodate the data stored in cache. The collector must have adequate RAM and hard disk space to support NetFlow. Two individual flows exist for each user connection. All devices are not required to support NetFlow. Data can be collected from devices that do support it.

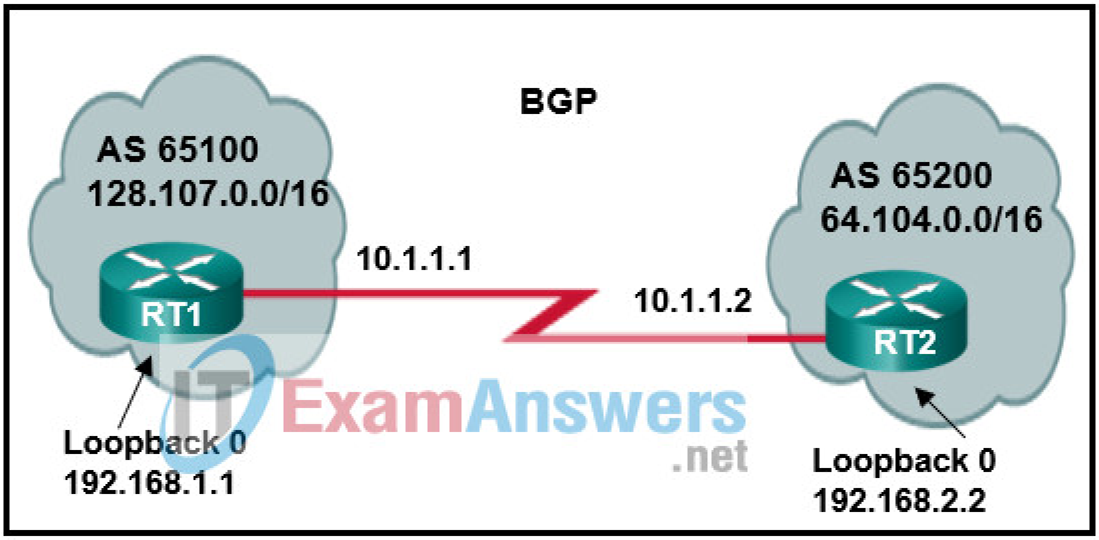
65. Which three statements describe SPAN and RSPAN? (Choose three.)

- SPAN can send a copy of traffic to a port on another switch.

- **SPAN can be configured to send a copy of traffic to a destination port on the same switch.**
- RSPAN is required to copy traffic on a source VLAN to a destination port on the same switch.
- **RSPAN can be used to forward traffic to reach an IPS that is analyzing traffic for malicious behavior.**
- RSPAN is required for syslog and SNMP implementation.
- **SPAN can copy traffic on a source port or source VLAN to a destination port on the same switch.**

Explanation: The Switched Port Analyzer (SPAN) feature on Cisco switches is a type of port mirroring that sends copies of the frame entering a source port (or VLAN), out another port on the same switch. Typically the destination port is attached with a packet sniffer or IPS device. Remote SPAN (RSPAN) allows source and destination ports to be in different switches.

66. Refer to the exhibit. A network administrator is configuring BGP on the router RT1. Which command set will allow RT1 to establish a neighbor relationship with RT2?



RT1(config)# router bgp 65100
RT1(config-router)# network 128.107.0.0 mask 255.255.0.0
RT1(config-router)# neighbor 10.1.1.1 remote-as 65200

RT1(config)# router bgp 65100
RT1(config-router)# network 128.107.0.0 mask 255.255.0.0
RT1(config-router)# neighbor 192.168.2.2 remote-as 65200

RT1(config)# router bgp 65100
RT1(config-router)# network 128.107.0.0 mask 255.255.0.0
RT1(config-router)# neighbor 10.1.1.2 remote-as 65200

RT1(config)# router bgp 65200
RT1(config-router)# network 64.104.0.0 mask 255.255.0.0
RT1(config-router)# neighbor 10.1.1.2 remote-as 65100

Explanation: The basic BGP configuration steps include the following:
Initialize the BGP routing process with the global command router bgp as-number .
Identify the IP address and autonomous system number associated with a BGP neighbor by the BGP router configuration command neighbor ip-address remote-as as-number .
Identify the specific network prefixes to be installed into the BGP table with the network statements.

67. A large shopping mall is planning to deploy a wireless network for customers. The network will use a lightweight AP topology. The network designers are considering the roaming by wireless clients. Which statement describes a difference between Layer 2 roaming and Layer 3 roaming?

- **Layer 2 roaming occurs between two APs configured with the same VLAN and IP subnet, whereas Layer 3 roaming occurs between two APs configured with different VLANs and IP subnets.**
- Layer 2 roaming does not require the client to contact a DHCP server, whereas Layer 3 roaming requires the client to contact a DHCP server.
- Layer 2 roaming does not require communicating to a WLC through CAPWAP, whereas Layer 3 roaming does.
- Layer 2 roaming occurs between two APs that are bound to the same WLC, whereas Layer 3 roaming occurs between two APs that are bound to different WLCs.

Explanation: Both Layer 2 and Layer 3 roams are intercontroller roaming. In intercontroller roaming, a client roams from one AP to another AP that is bound to a different WLC. An AP communicates to the bounding WLC through a CAPWAP tunnel. If the two APs involved in an intercontroller roaming are configured with the same VLAN and IP subnet, Layer 2 roaming occurs. If they are configured with different VLANs and IP subnets, a Layer 3 roaming occurs.

68. Which two types of probes can be configured to monitor traffic by IP SLA within a network environment? (Choose two.)

- **voice quality scores**
- website upload time
- SNMP traps
- **packet loss**

- syslog messages

Explanation: IP SLA is a tool that allows for the continuous monitoring of various aspects of the network. Different types of probes can be configured to monitor traffic within a network environment:

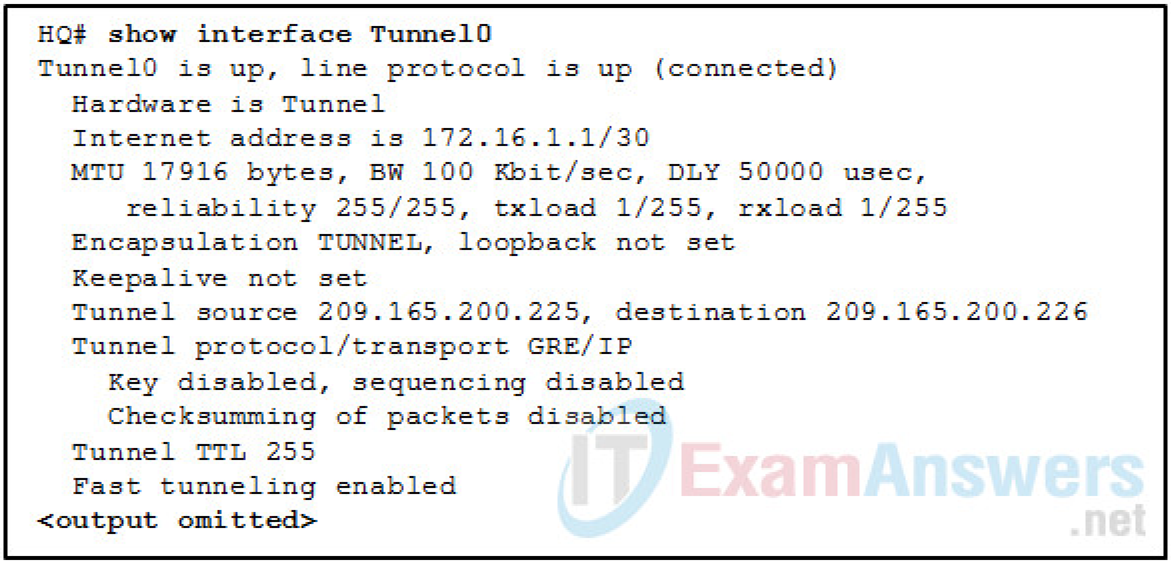
Delay
Jitter (directional)
Packet loss (directional)
Packet sequencing (packet ordering)
Path (per hop)
Connectivity (directional)
Server or website download time
Voice quality scores

69. What is the function of the Diffie-Hellman algorithm within the IPsec framework?

- provides strong data encryption
- guarantees message integrity
- **allows peers to exchange shared keys**
- provides authentication

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. DH (Diffie-Hellman) is an algorithm used for key exchange. DH is a public key exchange method that allows two IPsec peers to establish a shared secret key over an insecure channel.

70. Refer to the exhibit. Which IP address would be configured on the tunnel interface of the destination router?



```
HQ# show interface Tunnel0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.1.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.200.225, destination 209.165.200.226
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
<output omitted>
```

- 209.165.200.226
- 172.16.1.1
- **172.16.1.2**
- 209.165.200.225

Explanation: The IP address that is assigned to the tunnel interface on the local router is 172.16.1.1 with a prefix mask of /30. The only other address, 172.16.1.2, would be the destination tunnel interface IP address. Although 209.165.200.226 is listed as a destination address in the output, this is the address of the physical interface at the destination, not the tunnel interface.

71. What is the purpose of the generic routing encapsulation tunneling protocol?

- to provide fixed flow-control mechanisms with IP tunneling between remote sites
- to support basic unencrypted IP tunneling using multivendor routers between remote sites
- **to manage the transportation of IP multicast and multiprotocol traffic between remote sites**
- to provide packet level encryption of IP traffic between remote sites

Explanation: The GRE tunneling protocol is Cisco proprietary and does not include any flow-control mechanisms by default. GRE does not support encryption and is used to manage the transportation of IP multicast and multiprotocol traffic.

72. Which three services are critical functions of the IPsec service? (Choose three.)

- accounting
- **data integrity**
- speed
- **authentication**
- authorization
- **confidentiality**

Explanation: The acronym CIA provides three critical functions of the IPsec service: confidentiality, integrity, and authentication. Speed, accounting, and authorization are possible factors within the IPsec service but are not critical.

73. Which three functions are provided by the syslog logging service? (Choose three.)

- **gathering logging information**
- authenticating and encrypting data sent over the network

- retaining captured messages on the router when a router is rebooted
- **specifying where captured information is stored**
- **distinguishing between information to be captured and information to be ignored**
- setting the size of the logging buffer

Explanation: Syslog operations include gathering information, selecting which type of information to capture, and directing the captured information to a storage location. The logging service stores messages in a logging buffer that is time-limited, and cannot retain the information when a router is rebooted. Syslog does not authenticate or encrypt messages.

74. What are two operational characteristics of the ZBFW default zone? (Choose two.)

- By default, interfaces in this zone are permitted to communicate with interfaces of other security zones.
- **It includes interfaces that are not members of other security zones.**
- **It is a system-built zone.**
- It includes all IP addresses on a router.
- All traffic to and from this zone is permitted by default.

Explanation: The default zone is a system-level zone. If an interface is not configured as part of another security zone, it is placed in the default zone automatically.

75. Which password type uses a Cisco proprietary Vigenere cypher encryption algorithm and is considered easy to crack?

- type 5
- **type 7**
- type 8
- type 9

Explanation: Type 7 passwords are considered insecure. They are encrypted with a weak Vigenere cypher that is easily deciphered in seconds.

76. Which threat protection capability is provided by Cisco ESA?

- web filtering
- cloud access security
- **spam protection**
- Layer 4 traffic monitoring

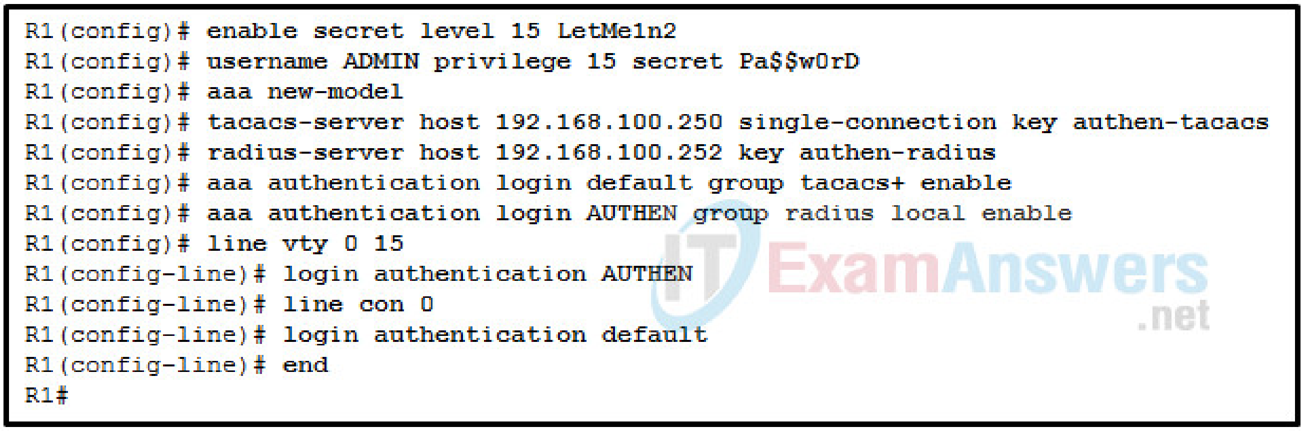
Explanation: Email is a top attack vector for security breaches. Cisco ESA includes many threat protection capabilities for email such as spam protection, forged email detection, and Cisco advanced phishing protection.

77. Which industry standard provides for port-based network access control?

- 802.1Q
- RADIUS
- LISP
- **802.1x**

Explanation: 802.1x is an industry standard for providing port-based network access control. It provides a mechanism to authenticate devices onto local-area networks and WLANs.

78. Refer to the exhibit. A network administrator configures AAA authentication on R1. When the administrator tests the configuration by telneting to R1 and no ACS servers can be contacted, which password should the administrator use in order to login successfully?



```
R1(config)# enable secret level 15 LetMe1n2
R1(config)# username ADMIN privilege 15 secret Pa$$w0rD
R1(config)# aaa new-model
R1(config)# tacacs-server host 192.168.100.250 single-connection key authen-tacacs
R1(config)# radius-server host 192.168.100.252 key authen-radius
R1(config)# aaa authentication login default group tacacs+ enable
R1(config)# aaa authentication login AUTHEN group radius local enable
R1(config)# line vty 0 15
R1(config-line)# login authentication AUTHEN
R1(config-line)# line con 0
R1(config-line)# login authentication default
R1(config-line)# end
R1#
```

- authen-radius
- LetMe1n2
- **Pa$$w0rD**
- authen-tacacs

Explanation: The authentication for Telnet connections is defined by AAA method list AUTHEN. The AUTHEN list defines that the first authentication method is through an ACS server using the RADIUS protocol (or RADIUS server). If the RADIUS server cannot be contacted, the second authentication method is to use the local user database. In this scenario, the local user database is used with a username of ADMIN and a password of Pa$$w0rD.

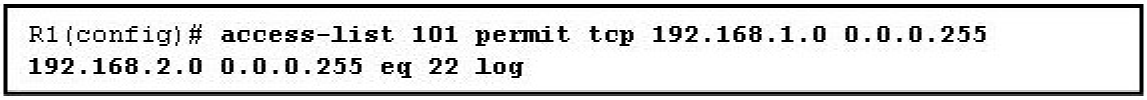
79. What is the one major difference between local AAA authentication and using the login local command when configuring device access authentication?

- The login local command requires the administrator to manually configure the usernames and passwords, but local AAA authentication does not.

- Local AAA authentication allows more than one user account to be configured, but login local does not.
- **Local AAA authentication provides a way to configure backup methods of authentication, but login local does not.**
- The login local command uses local usernames and passwords stored on the router, but local AAA authentication does not.

Explanation: Local AAA authentication works very similar to the login local command, except that it allows you to specify backup authentication methods as well. Both methods require that local usernames and passwords be manually configured on the router.

80. Refer to the exhibit. The ACL statement is the only one explicitly configured on the router. Based on this information, which two conclusions can be drawn regarding remote access network connections? (Choose two.)



```
R1(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255 eq 22 log
```

- SSH connections from the 192.168.2.0/24 network to the 192.168.1.0/24 network are allowed.
- **SSH connections from the 192.168.1.0/24 network to the 192.168.2.0/24 network are allowed.**
- Telnet connections from the 192.168.2.0/24 network to the 192.168.1.0/24 network are allowed.
- SSH connections from the 192.168.1.0/24 network to the 192.168.2.0/24 network are blocked.
- **Telnet connections from the 192.168.1.0/24 network to the 192.168.2.0/24 network are blocked.**
- Telnet connections from the 192.168.1.0/24 network to the 192.168.2.0/24 network are allowed.

Explanation: The extended access list in the exhibit is permitting SSH (TCP port 22) traffic that is sourced from the 192.168.1.0/24 network and traveling to the 192.168.2.0/24 network. The packets meeting this criteria are logged to the local logging buffer (the default), a syslog server, or both depending on how the router is configured for syslog settings. All other traffic is denied because of the implicit deny at the end of every ACL.

81. Consider the configured access list.

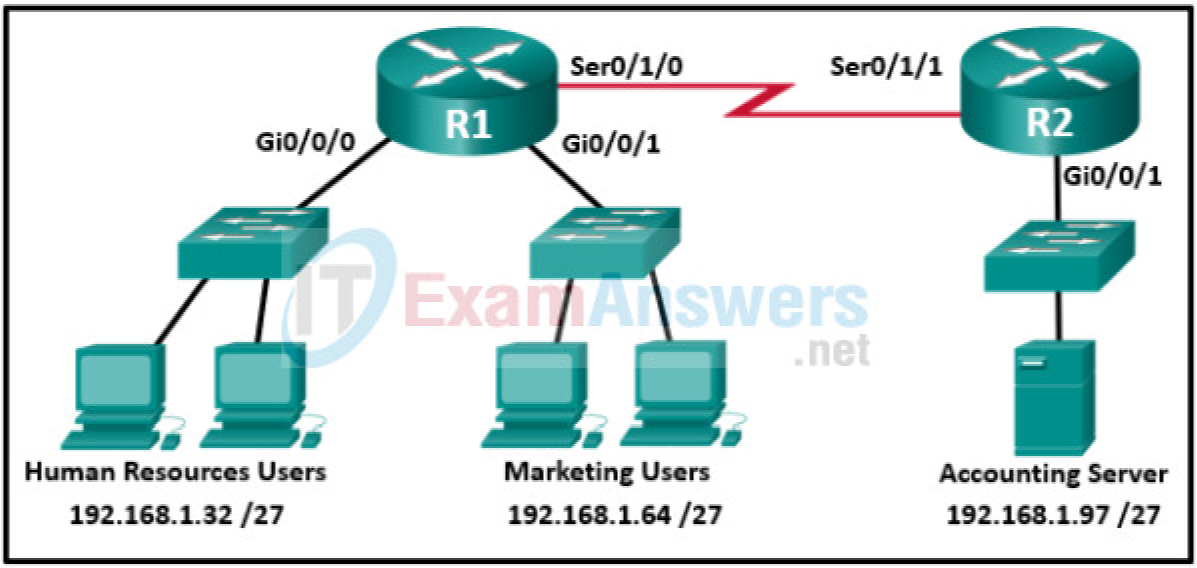
```
R1# show access-lists
extended IP access list 100
deny tcp host 10.1.1.2 host 10.1.1.1 eq telnet
deny tcp host 10.1.2.2 host 10.1.2.1 eq telnet
permit ip any any (15 matches)
```

What are two characteristics of this access list? (Choose two.)

- The 10.1.2.1 device is not allowed to telnet to the 10.1.2.2 device.
- **The access list has been applied to an interface.**
- Any device can telnet to the 10.1.2.1 device.
- A network administrator would not be able to tell if the access list has been applied to an interface or not.
- Only the 10.1.1.2 device can telnet to the router that has the 10.1.1.1 IP address assigned.
- **Any device on the 10.1.1.0/24 network (except the 10.1.1.2 device) can telnet to the router that has the IP address 10.1.1.1 assigned.**

Explanation: The access list stops Telnet traffic from the 10.1.1.2 device to the 10.1.1.1 device. It also stops Telnet traffic from 10.1.2.2 device to 10.1.2.1. All other TCP/IP-based transmissions are allowed. The access list is working because there have been 15 matches on the last ACE.

82. Refer to the exhibit. An extended access list has been created to prevent human resource users from gaining access to the accounting server. All other network traffic is to be permitted. When following the ACL configuration guidelines, on which router, interface, and direction should the access list be applied?

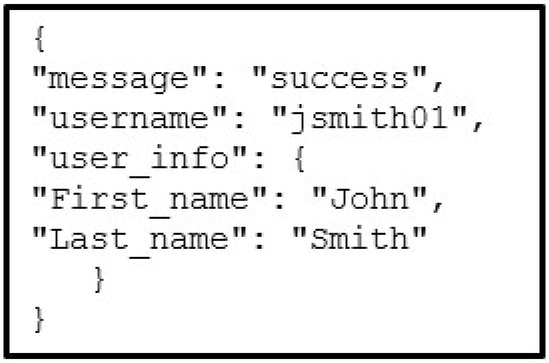


- router R1, interface S0/1/0, outbound
- router R2, interface Gi0/0/1, outbound
- router R2, interface Gi0/0/1, inbound
- **router R1, interface Gi0/0/0, inbound**
- router R2, interface S0/1/1, inbound
- router R1, interface Gi0/0/0, outbound

Explanation: The ACL configuration guidelines recommend placing extended access control lists as close to the source of network traffic as possible and placing standard access control lists as close to the destination of network traffic as possible.

83. Refer to the exhibit. Which data format is used to represent the data for network automation applications?

- XML
- YAML
- HTML
- **JSON**



```
{
"message": "success",
"username": "jsmith01",
"user_info": {
"First_name": "John",
"Last_name": "Smith"
   }
}
```

Explanation: The common data formats that are used in many applications including network automation and programmability are as follows:
JavaScript Object Notation (JSON) – In JSON, the data known as an object is one or more key/value pairs enclosed in braces { }. Keys must be strings within double quotation marks ” “. Keys and values are separated by a colon.
eXtensible Markup Language (XML) – In XML, the data is enclosed within a related set of tags data.
YAML Ain’t Markup Language (YAML) – In YAML, the data known as an object is one or more key value pairs. Key value pairs are separated by a colon without the use of quotation marks. YAML uses indentation to define its structure, without the use of brackets or commas.

84. Which Python function is used for console output?

- for
- from
- **print**
- return

Explanation: The print command is used for console output. The command for is used for repetition logic , from is used for module importing, and return is a function definition.

85. What are two characteristics of the Python programming language? (Choose two.)

- It only runs in the interactive mode.
- It requires a compiler to be installed.
- **The code is easy to read.**
- **It runs without conversion to machine-language.**
- It uses the & symbol to indicate that the interactive mode is ready to accept commands.

Explanation: A compiled computer language is a computer language that compiles its programs into a set of machine-language instructions, whereas an interpreted programming language allows for an interpretation of the instructions directly without first compiling them into machine language.

86. What term is used to describe the files that contain Python definitions and statements?

- function
- file
- **module**
- script

Explanation: A module is a file containing Python definitions and statements.

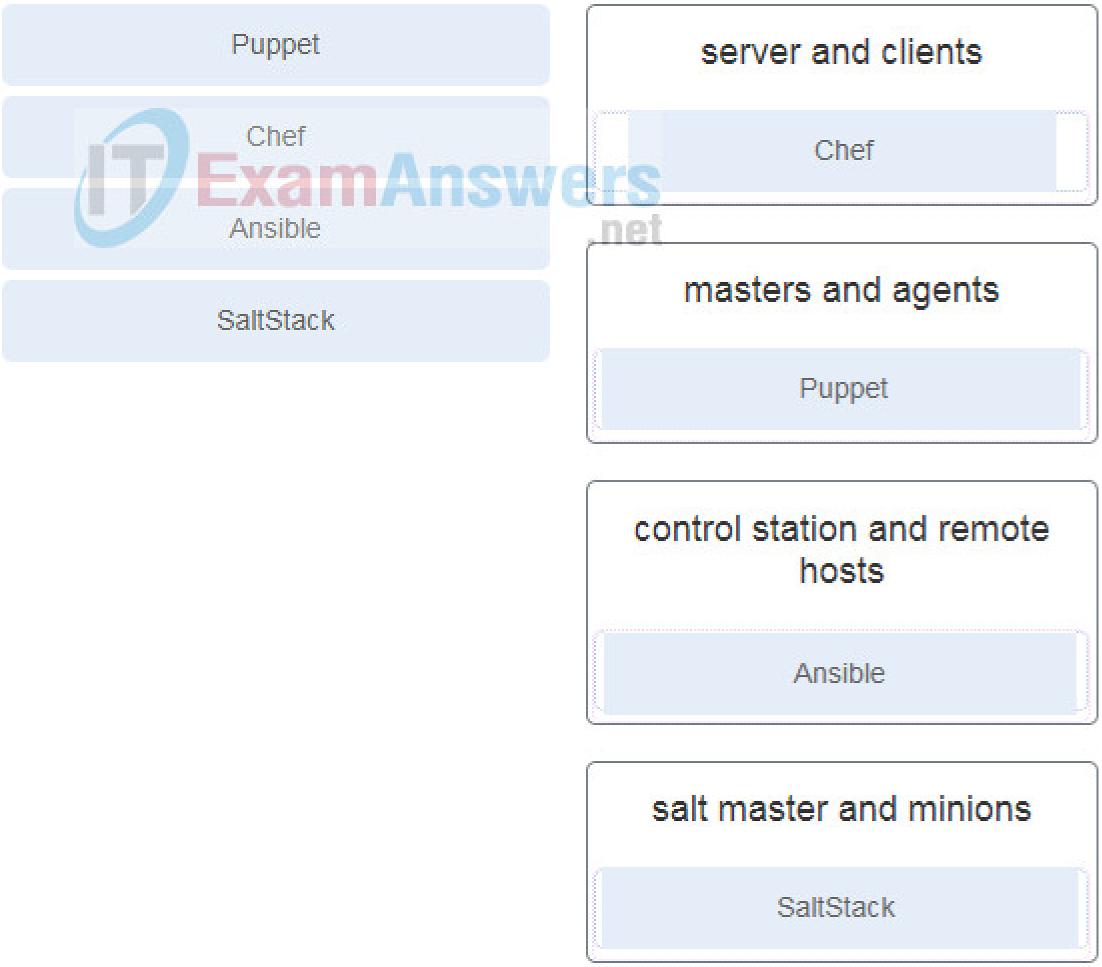
87. Which characteristic is common to both Chef and Puppet?

- Both function in a peer-to-peer model.
- Both use the push model for configuration management.
- **Both have free open source versions.**
- Both are Cisco proprietary.

Explanation: Chef and Puppet have several similarities, to include:

Both have free open source versions available.
Both have paid enterprise versions available.
Both manage code that needs to be updated and stored.
Both manage devices or nodes to be configured.
Both leverage a pull model.
Both function as a client/server model.

88. Question as presented: Match the automation tool to the architecture components.



Puppet

Chef

Ansible

SaltStack

server and clients: Chef

masters and agents: Puppet

control station and remote hosts: Ansible

salt master and minions: SaltStack

- server and clients
- masters and agents
- control station and remote hosts
- salt master and minions

89. Which data format is expected by Cisco DNA Center for all incoming data from the REST API?

- YAML
- HTTP
- **JSON**
- XML

Explanation: The Cisco DNA Center controller expects all incoming data from the REST API to be in JSON format.

90. Which three orchestration tools require agent software on client machines to be managed? (Choose three.)

- **Chef**

- Ansible
- EEM
- Puppet Bolt
- **SaltStack**
- **Puppet**

Explanation: There are several available agent based configuration and automation tools, including Puppet, Chef, and SaltStack. Ansible, Puppet Bolt, and EEM are agentless tools.

91. Which three are components of puppet modules? (Choose three.)

- **files**
- recipes
- **manifests**
- pillars
- playbooks
- **templates**

Explanation: Puppet is a configuration management and automation tool that uses modules to support the configuration of most devices that can be configured manually. Puppet modules contain three components: Manifests, templates, and files.

92. What are the key difference between a type 1 hypervisor and a type 2 hypervisor?

- A type 1 hypervisor runs on specialized systems and a type 2 hypervisor runs on desktop computers.
- **A type 1 hypervisor runs directly on the system hardware and a type 2 hypervisor requieres a host OS to run.**
- A type 1 hypervisor supports all server OS virtualization and a type 2 hypervisor supports Linux and Mac virtualization.
- A type 1 hypervisor supports server virtualization and a type 2 hypervisor supports workstation virtualization.

93. A network administrator issues the show bgp ipv4 unicast summary command to verify BGP session after basic BGP configuration is completed. Which three pieces of information are found in the BGP session summary? (Chose three.)

- **the number of exchanged prefixes with a neighbor**
- **the BGP router ID of peers**
- the routes that are redistributed into BGP
- the peer synchronization configuration
- **the AS number of the peer**

- the IGP that is configured on the BGP peer

94. A network administrator uses the spanning-tree portfast bpduguard default global configuration command to enable BPDU guard on switch. However, BPDU guard is not activated on all access ports. What is the couse of the issue?

- BPDU guard needs to be activated on the interface configuration command mode.
- **PortFast is not configured on all access ports.**
- Access ports configured with root guard cannot be configured with BPDU GURAD.
- Access ports belong to different VLANs.

Explanation: BPDU guard can be enabled globally on all PortFast-enabled ports by using the spanning-tree portfast bpduguard default global configuration command. If PortFast is not configured, then BPDU guard is not activated.

95. What is the key difference between a type 1 hypervisor and a type 2 hypervisor?

- A type 1 hypervisor supports all server OS virtualization and a type 2 hypervisor supports Linux and Mac virtualization.
- **A type 1 hypervisor runs directly on the system hardware and a type 2 hypervisor requires a host OS to run.**
- A type 1 hypervisor runs on specialized systems and a type 2 hypervisor runs on desktop computers.
- A type 1 hypervisor supports server virtualizations and a type 2 hypervisor only supports workstation virtualization.

Explanation: There are two types of hypervisors:

- Type 1 – This type of hypervisor runs directly on the system hardware.
- Type 2 – This type of hypervisor requires a host OS to run.

Both types of hypervisors can run on regular computer systems and support multiple OS virtualizations.

96. A network administrator issues the show bgp ipv4 unicast summary command to verify the BGP session after basic BGP configuration is completed. Which three pieces of information are found in the BGP session summary? (Choose three.)

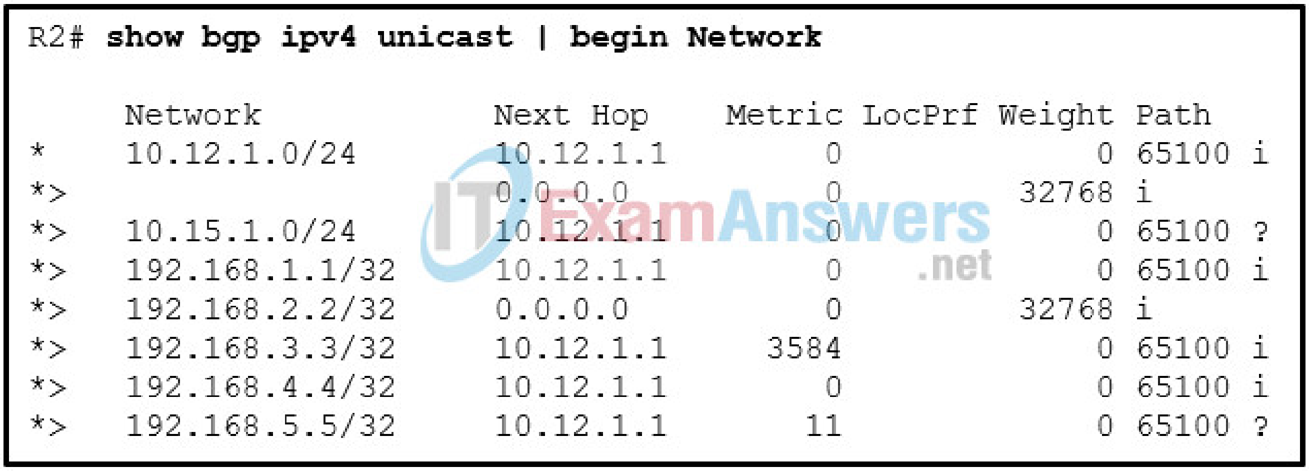
- the routes that are redistributed into BGP
- the IGP that is configured on the BGP peer
- **the number of exchanged prefixes with a neighbor**
- **the AS number of the peer**
- the peer synchronization configuration

- **the BGP router ID of the peers**

Explanation: The BGP session summary report includes information as follows:

- **Neighbor** – the IP address of the BGP peer
- **V** – the BGP version spoken by the BGP peer
- **AS** – the autonomous system number of the BGP peer
- **MsgRcvd** – the count of messages received from the BGP peer
- **MsgSent** – the count of messages sent to the BGP peer
- **TblVer** – the last version of the BGP database sent to the peer
- **InQ** – the number of messages queued to be processed by the peer
- **OutQ** – the number of messages queued to be sent to the peer
- **Up/Down** – the length of time the BGP session is established or the current status if the session is not in an established state
- **State/PfxRcd** – the current state of the BGP peer or the number of prefixes received from the peer

97. Refer to the exhibit. A network administrator issues the show bgp ipv4 unicast | begin Network command to check the routes in the BGP table. What does the symbol ? at the end of a route indicate?



```
R2# show bgp ipv4 unicast | begin Network

     Network             Next Hop    Metric LocPrf Weight Path
*    10.12.1.0/24        10.12.1.1        0             0 65100 i
*>                       0.0.0.0          0         32768 i
*>   10.15.1.0/24        10.12.1.1        0             0 65100 ?
*>   192.168.1.1/32      10.12.1.1        0             0 65100 i
*>   192.168.2.2/32      0.0.0.0          0         32768 i
*>   192.168.3.3/32      10.12.1.1     3584             0 65100 i
*>   192.168.4.4/32      10.12.1.1        0             0 65100 i
*>   192.168.5.5/32      10.12.1.1       11             0 65100 ?
```

- The route is learned through a static route.
- The route is originated from a connected network to the router.
- **The route is redistributed into BGP.**
- The route is the best route for the network prefix

Explanation: The origin is a well-known mandatory BGP path attribute used in the BGP best-path algorithm. A value of i represents an IGP, e indicates EGP, and ? indicates a route that was redistributed into BGP.

98. Which two OSPFv3 LSA types are used to advertise IPv6 prefixes to neighbors? (Choose two.)

- LSA type 4 – interarea router
- LSA type 5 – AS-external
- LSA type 7 – NSSA
- **LSA type 8 – link-local LSA**
- **LSA type 9 – intra-area prefix LSA**

Explanation: Two new LSA types are added to OSPFv3, type 8, link-local LSA, and type 9, intra-area prefix LSA. These two LSAs advertise unicast prefixes and prevent the need for OSPF calculations when interface addresses are added or changed.