ENCOR v1.1 (350-401) Video Training Series
Practice Exam #2

1. Which of the following is an advantage of a Cloud Design versus an On-Premise design?

   A. You don't need to purchase physical servers.
   B. You can better control the user experience.
   C. You can better meet compliance requirements.
   D. You don't need to be concerned with redundancy.

Answer: A
Explanation: With a Cloud Design, you don't need to purchase physical servers. Instead, you can pay the cloud provider for your actual usage of virtual servers they host. However, an On-Premise design usually lets you have better control of the end-user experience and allows you more flexibility in meeting compliance requirements. Also, even though you might have your servers hosted by a cloud provider, you still need to be concerned with redundancy, and perhaps have duplicate servers in the cloud, along with a virtual load-balancer to distribute the load between those servers, while providing redundancy.

2. The "5 Nines of Availability" refers to what?

   A. Limiting a network's downtime to no more than 5 minutes per year
   B. Having 99.9 percent uptime for 99 percent of a network's components
   C. Limiting a network's downtime to no more than 30 seconds per year
   D. Having 99 percent uptime for 99.9 percent of a network's components

Answer: A
Explanation: The "5 Nines of Availability" refers to keeping a network operational 99.999 percent of the time. That translates to approximately 5 minutes of downtime per year. The "6 Nines of Availability" refers to keeping a network operational 99.9999 percent of the time, which translates to approximately 30 seconds of downtime per year.

3. Stateful Switchover (SSO) is often used in conjunction with which feature to prevent packets from being dropped when a router fails over from one of its route processors to another?

   A. Reverse Path Forwarding (RPF)
   B. Embedded Event Manager (EEM)
   C. Multilayer Switching (MLS)
   D. Nonstop Forwarding (NSF)

Answer: D
Explanation: Stateful Switchover (SSO) allows a router with two route processors to fail over from its primary route processor to its backup route processor without dropping routing protocol neighborships with other routers. However, the backup route processor might drop packets while it constructs an IP routing table. To prevent those initial packet drops after the failover, a feature called Nonstop Forwarding (NSF) could be used. NSF allows the IP routing information maintained by Cisco Express Forwarding (CEF) in the primary route processor to remain in memory and be used by the backup route processor. This allows the backup route processor to immediately have IP forwarding information after a failover.

4. Which metric allows WLAN location services to calculate the location of a wireless client within the network?

    A. SNR
    B. RTLS
    C. RSS
    D. SSID

Answer: C
Explanation: The Received Signal Strength (RSS) can be used for enterprise asset tracking within a WLAN. The wireless LAN controller uses the signal strength from all of the access points surrounding a client to determine the exact physical location of a client within the network. This is performed by using three or more surrounding access points to pinpoint this location.

5. Which of the following is NOT a type of Tag used to segment wireless networks?

    A. Policy Tag
    B. Site Tag
    C. QoS Tag
    D. RF Tag

Answer: C
Explanation: On Cisco's newer WLAN controllers, wireless networks can be segmented using Profiles, Tags, and Groups.

A Profile is a collection of settings and parameters about a characteristic of a wireless LAN.

A Tag is a collection of Profiles.

A Group is a collection of one or more APs that share a common set of Tags.

There are three types of Tags: Policy Tag, Site Tag, and RF Tag.

There is no QoS Tag. Instead, QoS settings can be specified in a Policy Profile, which is linked to an SSID in a Policy Tag.

6. Which piece of the Cisco SD-WAN solution resides in the control plane and is thought of as the “brain” of the solution?

   A. vSmart
   B. vManage
   C. vBond
   D. vEdge

Answer: A
Explanation: Cisco vSmart resides within the control plane and is thought of as the “brain” of the Cisco SD-WAN solution. As policies are created within vMangage, vSmart is responsible for enforcing those policies and sharing the policies with other SD-WAN routers and locations in the network. Route information from branch locations are received via the Overlay Management Protocol (OMP), and vSmart will compare the route information to the known polices in order to control traffic.

7. In a typical SD-Access implementation, which type of device would act as a Location ID Separation Protocol (LISP) server for mapping node locations within the network?

   A. Fabric Edge Node
   B. Fabric Intermediate Node
   C. Fabric Border Node
   D. Fabric Control Plane Node

Answer: D
Explanation: In an SD-Access implementation, a Fabric Control Plane Node acts as a LISP server, containing a database used to resolve node locations. LISP is used to create two separate device identity tags; the endpoint identifier (EID) and the routing locator (RLOC). The Fabric Control Plane Node resolves these identity tags using the local LISP database, allowing SD-Access to map the network accurately with node and client locations.

8. Which of the following is NOT one of the Modular QoS Command Line Interface (MQC) configuration steps?

   A. Apply a Policy Map
   B. Create the “class-default” Class Map
   C. Create a Policy Map
   D. Create Class Maps

Answer: B
Explanation: The 3-step MQC process consists of: (1) Creating class maps, (2) Creating a Policy Map, and (3) Applying the Policy Map. However, the “class-default” class map exists by default. You cannot create or delete it.

9. Which mechanism is the slowest method for switching packets, where every packet is inspected by the switch CPU?

   A. Cisco Express Forwarding
   B. Fast Switching
   C. Process Switching
   D. Slow Switching

Answer: C
Explanation: Process Switching is the original method for Cisco IOS switching, where every packet is inspected by the switch CPU. When a packet arrives on the switch, the processor function is interrupted in order to analyze the packet and compare it to the internal routing table for forwarding. The next-hop destination attached to the packet is used to determine the outbound switch interface that should be used for packet delivery. A new Layer 2 frame header is constructed for every single packet, making this a slow method that is not ideal for modern networks.

10. Which memory architecture is used on all Catalyst switch models to perform Layer 2 switching?

    A. CAM
    B. TCAM
    C. FIB
    D. RIB

Answer: A
Explanation: The Content Addressable Memory (CAM) table is the memory architecture used in Cisco Catalyst switches for Layer 2 switching. As data frames arrive on a switchport, the source

MAC addresses for the traffic are recorded in the CAM table. This is used to determine which outgoing switchport should be used for frame delivery.

11. What type of hypervisor runs on top of a traditional operating system (e.g. on top of Microsoft Windows)?

    A. Type 1
    B. Type 2
    C. Type 3
    D. Type 4

Answer: B
Explanation: A Type 1 hypervisor (also known as a "native" or "bare metal" hypervisor) runs directly on a server's hardware. However, a Type 2 hypervisor (also known as a "hosted" hypervisor) runs on top of a traditional operating system. Hypervisors are not categorized as either Type 3 or Type 4.

12. Which of the following is true regarding the operation of a virtual server's virtual network interface card (also known as a "virtual NIC" or "vNIC")?

    A. All virtual NICs share the MAC address of a physical NIC in the physical server.
    B. All virtual NICs share a virtual MAC address.
    C. A virtual NIC can simultaneously connect to multiple virtual switches.
    D. Each virtual NIC within a virtual machine has a unique MAC address.

Answer: D
Explanation: A virtual NIC is software associated with a unique MAC address, which can be used by a VM to send and receive packets. Also, a vNIC (just a like a physical NIC) can only connect to one switchport at a time.

13. An IKE Phase 1 tunnel is also known as what?

    A. An IPsec tunnel
    B. A GRE tunnel
    C. An ISAKMP tunnel
    D. An SA tunnel

Answer: C
Explanation: When an IPsec tunnel is being formed, it goes through two phases. The first phase is the creation of an IKE Phase 1 tunnel. IKE stands for Internet Key Exchange. The second phase is the creation of an IKE Phase 2 tunnel. Another name for the IKE Phase 1 tunnel is an "ISAKMP

tunnel," where ISAKMP stands for Internet Security Association and Key Management Protocol. Another name for the IKE Phase 2 tunnel is an IPsec tunnel. Each of these tunnels has a corresponding security association, referred to as an SA. However, an SA is not a type of tunnel.

14. What is the term used to refer to a broadcast domain within a VXLAN network?

A. VLAN
B. VEM
C. VNI
D. VTEP

Answer: C
Explanation: Virtual Extensible LANs (VXLANs) support over 16 million broadcast domains, thanks to a VXLAN's 24-bit identifier field, as opposed to using VLANs, which support just over 4000 broadcast domains (due to a 12-bit VLAN field). This identifier is called a VXLAN Network Identifier, which is abbreviated as VNI. The device that does the VXLAN encapsulation is called a Virtual Ethernet Module (VEM). Each VEM has (at least) one IP address, and that IP address is assigned to an interface called a VTEP, which stands for VXLAN Tunnel Endpoint. Each VTEP can be associated with one or more VNIs.

15. What term is assigned to an untagged VLAN on an IEEE 802.1Q trunk?

A. Primary VLAN
B. Management VLAN
C. Secondary VLAN
D. Native VLAN

Answer: D
Explanation: VLANs on an IEEE 802.1Q trunk have four Tag Bytes added to each of their frames. One purpose of these Tag Bytes is to identify the VLAN membership of the frames. However, one VLAN, called the Native VLAN, is not tagged. As a result, neighboring switches should agree on the Native VLAN being used on a trunk that is interconnecting to those switches.

16. Switches SW1 and SW2 are directly connected with a Gigabit Ethernet connection. Which of the following Port Aggregation Protocol (PAgP) mode combinations will successfully bring up an EtherChannel between the switches?

A. SW1: Auto – SW2: Auto
B. SW1: On – SW2: Desirable
C. SW1: On – SW2: Auto
D. SW1: Auto – SW2: Desirable

Answer: D
Explanation: A mode of On isn't technically a PAgP or LACP mode. It simply tells the port(s) to be in an EtherChannel, without sending or processing any PAgP or LACP frames. Therefore, if one side is set to On, the other side must also be set to On in order for an EtherChannel to be brought up. The mode of Auto will cause a port to bring join an EtherChannel if it receives PAgP frames from the far end. However, the Auto mode does not initiate the joining of an EtherChannel. As a result, other than both sides being set to the On mode, only two combinations of PAgP settings will cause an EtherChannel to be brought up: (1) both sides set to Desirable or (2) one side set to Desirable and the other side set to Auto.

17. When configuring MSTP, what Spanning Tree instance is used by any VLANs not explicitly assigned an instance?

    A. Those VLANs will not participate in STP.
    B. MST0
    C. MST1
    D. Those VLANs will share the instance assigned to the Native VLAN.

Answer: B
Explanation: In addition to the instances you define in an MSTP configuration, a default instance of MST0 is created. All VLANs not explicitly assigned an MSTP instance are assigned to that MST0 instance.

18. Which if the following is NOT a Rapid PVST+ port state?

    A. Discarding
    B. Listening
    C. Learning
    D. Forwarding

Answer: B
Explanation: Traditional Spanning Tree Protocol (STP) has the following port states: (1) Blocking, (2) Listening, (3) Learning, and (4) Forwarding. However, Rapid PVST+ uses these port states: (1) Discarding, (2) Learning, and (3) Forwarding.

19. What will a Cisco Catalyst switch in VTP Transparent mode do when it receives a VTP advertisement?

    A. The switch will flood the advertisement out all other trunk links, other than the trunk it was received on.
    B. The switch will drop the advertisement.
    C. The switch will send a VTP Reject message back to the sending switch.
    D. The switch will update its VLAN database, based on the advertisement, but the advertisement will not be forwarded.

Answer: A
Explanation: When a switch in VTP Transparent mode receives a VTP update, it will not update its VLAN database. However, it will flood the advertisement out all other trunk links, other than the trunk it was received on.

20. What metric components does EIGRP use by default?

    A. Bandwidth
    B. Bandwidth and Delay
    C. Bandwidth, Delay, and Reliability
    D. Bandwidth, Delay, Reliability, Load, and MTU

Answer: B
Explanation: EIGRP's metric calculation can consider Bandwidth, Delay, Reliability, and Load, with MTU used as a tie breaker if the calculation is the same for two paths. However, the calculation uses K Values to determine how influential the various metric components are in the final metric value. By default, three K Values are set to 0, resulting in only Bandwidth and Delay being used in a default metric calculation.

21. Which of the following router interface encapsulations will, by default, cause an interface to use an OSPF Network Type of Point-to-Point?

    A. Frame-Relay
    B. HDLC
    C. Ethernet
    D. All interfaces use an OSPF Network Type of Broadcast, by default. However, it that be administratively changed.

Answer: B
Explanation: An OSPF Network Type of Point-to-Point is the default OSPF Network Type on a non-Frame Relay serial interface. Therefore, an interface encapsulation type of HDCP or PPP on

a serial interface will result in that interface having a default OSPF Network Type of Point-to-Point. Any type of Ethernet interface has a default OSPF Network Type of Broadcast.

22. What configuration feature can prevent a route known to an OSPF Link State Database from being injected into a router's IP routing table?

    A. Filter List
    B. Redistribution
    C. Access Control List
    D. Distribute List

Answer: D
Explanation: OSPF route filtering can occur in one of three locations: (1) Routes can be filtered at an ASBR as they're about to be redistributed into OSPF, which is accomplished as part of the redistribution configuration. (2) Routes can be filtered at an ABR as they're about to be advertised into a different area, which is accomplished using a Filter List. (3) Routes can be filtered as they're about to be injected into a router's IP routing table from an OSPF Link State Database, which is accomplished using a Distribute List.

23. What LSA type is used by an ASBR in an NSSA to inject routes from another autonomous system into OSPF?

    A. Type 3 LSA
    B. Type 4 LSA
    C. Type 5 LSA
    D. Type 7 LSA

Answer: D
Explanation:
- A Type 3 LSA (i.e., a Summary LSA) is sent from one area to another and is used to advertise a network in the source area.
- A Type 4 LSA (i.e., a Summary ASBR LSA) is created by an ABR to tell members of an area how to reach an ASBR.
- A Type 5 LSA (i.e., an AS External LSA) is created by an ASBR to advertise networks in a different AS.
- A Type 7 LSA (i.e., an NSSA LSA) is sent from an ASBR into an NSSA to advertise networks from a different AS.

24. What command must be entered in Cisco IOS before OSPFv3 can route IPv6 networks?

A. ipv6 cef
B. ipv6 enable
C. ipv6 unicast-routing
D. IPv6 routing is enabled by default.

Answer: C
Explanation: Interestingly, IPv6 routing is not enabled by default in Cisco IOS. Therefore, before routing IPv6 unicast networks, using routing protocols such as RIPng, OSPFv3, or EIGRP for IPv6, you need to enter the "ipv6 unicast-routing" command in global configuration mode. While the "ipv6 cef" command can improve performance, by enabling Cisco Express Forwarding (CEF) for IPv6 routing decisions, it isn't a required command for IPv6 routing.

25. Which of the following is true about BGP neighbor formation?

A. Neighbors are dynamically discovered via multicast Hello messages
B. A neighbor's IP address must be statically configured
C. A UDP session is established between neighbors
D. By default, BGP neighbors can be as many as 255 hops away from one another

Answer: B
Explanation: BGP neighbors must be configured with one another's IP addresses, as opposed to dynamically discovering each other with multicast Hello messages, which are used by EIGRP and OSPF. BGP neighbors form a TCP session between themselves, rather than a UDP session. Also, even though BGP neighbors can be a maximum of 255 hops away from one another (using the "ebgp-multihop" command), by default, BGP neighbors must be adjacent to one another.

26. Identify the statement that is NOT true concerning iBGP connections.

A. By default, a route received from an iBGP neighbor is not advertised to other iBGP neighbors.
B. When a router receives a route from an eBGP neighbor and advertises that route to an iBGP neighbor, the NEXT-HOP attribute is not updated.
C. When configuring an iBGP neighbor, the "neighbor" command uses the "local-as" parameter instead of the "remote-as" parameter.
D. A route reflector is often used within an autonomous system if there is not a full mesh of iBGP neighborships.

Answer: C
Explanation: An iBGP (Internal BGP) neighborship is formed between two routers within an autonomous system (AS). An eBGP (External BGP) neighborship is formed between two routers

in different autonomous systems. When a router receives a route from an eBGP neighbor, it advertises that route to any iBGP neighbors without updating the NEXT-HOP attribute (which can be addressed by configuring the NEXT-HOP-SELF option). Also, when a router receives a route advertisement from an iBGP neighbor, the router does not advertise that route to other iBGP neighbors (which can be addressed using a Route Reflector or by configuring a full mesh of iBGP neighborships). Interestingly, the "neighbor remote-as" command is used to form a neighborship between routers in different autonomous systems as well as between routers in the same autonomous system.

27. When configuring Multiprotocol BGP to advertise IPv6 routes over an IPv4 BGP session, what extra configuration step is needed?

    A. You need to enabled Cisco Express Forwarding (CEF).
    B. You need to apply a route map to your IPv6 neighbor specifying the next-hop IPv6 address.
    C. You need to apply a route map to your IPv6 neighbor specifying the next-hop IPv4 address.
    D. You need to disable Cisco Express Forwarding (CEF).

Answer: B
Explanation: IPv6 routes can be advertised over either an IPv4 or an IPv6 session with Multiprotocol BGP. However, if an IPv4 session is used, the receiving BGP neighbor doesn't learn the IPv6 address of the router sending the IPv6 route advertisement. To overcome this issue, you can configure a route map to add the IPv6 next-hop address to IPv6 route advertisements.

28. What is the term used to refer to one complete up and down motion of an electromagnetic wave?

    A. Frequency
    B. Cycle
    C. Hertz
    D. Wavelength

Answer: B
Explanation: A cycle is defined as one complete up and down motion of an electromagnetic wave. This is used to determine the frequency of an electromagnetic wave by examining the number of cycles that happen over the period of one second, otherwise known as Hertz (Hz). For example, if an electromagnetic wave has four complete up and down motions over the period of one second, this means there are four cycles per second. We would determine that the frequency of this electromagnetic wave would be 4 Hz.

29. Which type of wireless antenna would have a lower gain, creating a less focused path for broad coverage?

    A. Dipole Antenna
    B. Patch Antenna
    C. Yagi Antenna
    D. Dish Antenna

Answer: A
Explanation: A dipole antenna is a type of omnidirectional antenna that is commonly seen on consumer grade wireless devices. Omnidirectional antennas have lower gain and a less focused signal path, created for broad coverage. This is opposed to a directional antenna, which has high gain with a focused path in order to specifically direct the RF signal.

30. A wireless client roams between access points connected to two separate wireless LAN controllers, which do not share a subnet. Which type of intercontroller roam has occurred?

    A. Layer 2
    B. Layer 3
    C. CAPWAP
    D. Intracontroller

Answer: B
Explanation: When a client roams between access points connected to two separate WLCs that do not share a subnet or network, this intercontroller roam is referred to as a Layer 3 roam. Cisco provides seamless Layer 3 roaming through use of an established CAPWAP tunnel between the WLC, allowing the client to keep its original IP address even though it is associated with a different subnet or VLAN.

31. In a Network Address Translation (NAT) configuration, what command is given (and in what configuration mode is it given) to specify that an interface is on the inside of a network?

    A. Router(config)# ip nat inside
    B. Router(config-if)# ip nat inside
    C. Router(config-nat)# nat [interface-id] inside
    D. Router(config-router)# nat [interface-id] inside

Answer: B
Explanation: As part of a NAT configuration, an interface can be identified as an Inside interface using the “ip nat inside” command. That command needs to be issued in interface configuration mode for the interface being identified as an inside interface.

32. What option is added to the end of an “ip nat” command to enable Port Address Translation (PAT)?

A. single
B. ports
C. static
D. overload

Answer: D
Explanation: The “overload” option is specified at the end of an “ip nat” command to enable PAT. In fact, PAT is commonly referred to as “NAT Overloading.”

33. What is the default Priority value used by HSRP?

A. 3
B. 10
C. 100
D. 255

Answer: C
Explanation: HSRP uses a Priority value to elect an Active router. Higher Priority values are preferred. Therefore, an HSRP router can be influenced to become the Active router for an HSRP group by giving it a higher Priority value compared to any other member of the HSRP group. By default, HSRP has a Priority value is 100.

34. An IPv6 multicast address always begins with which Hexadecimal digits?

A. FF
B. FE80
C. F001
D. EE

Answer: A
Explanation: The first 8 Binary bits in an IPv6 multicast address are all 1s, meaning that the first 2 Hexadecimal digits in an IPv6 address are FF. Following those first 8 bits, are 4 Flag bits, 4 Scope bits, and 112 bits identifying the Group ID.

35. Which command is used to turn off all possible debugging in Cisco IOS?

A. no debugging
B. no debug all
C. no debug
D. no enable debug

Answer: B
Explanation: The “no debug all” command is used to stop all debugging features in Cisco IOS. Alternatively, the command “undebug all” can be used to perform the same function.

36. Which variation of the ping command allows for more granular control of the command through built-in IOS prompts?

A. ping
B. ping detail
C. ping extend
D. ping more

Answer: A
Explanation: By entering the “ping” keyword at the EXEC command line level with no IP address attached, a built-in IOS wizard will prompt you for details related to the ping command that you wish to execute. This allows you to control things such as the repeat count, the datagram size, the source address or interface, and more.

37. Which well-known port is used by an SNMP agent device by default to send system information back to the SNMP manager server?

A. TCP 162
B. UDP 162
C. TCP 161
D. UDP 161

Answer: B
Explanation: An SNMP agent is a process running on a monitored device that allows it to respond to information poll requests from an SNMP manager. Unsolicited messages can also be sent out in this manner, known as traps. This information is sent by default as UDP communication over port 162.

38. Which Syslog message code indicates an emergency state where the system is unstable?

A. Level 0
B. Level 1
C. Level 7
D. Level 8

Answer: A
Explanation: Syslog messages have a code ranging from 0-7, where level 7 indicates informational debugging messages and level 0 are the most severe, emergency messages. Level 0 codes indicate an unstable or unusable system with an emergency severity.

39. Which Cisco IOS command would be used to send NetFlow data to a collection server with the IP address 10.1.1.5 over port 9995?

A. ip flow-export destination 10.1.1.5 9995
B. ip flow-export server 10.1.1.5 9995
C. ip flow-export collector 10.1.1.5 9995
D. ip flow-export host 10.1.1.5 9995

Answer: A
Explanation: The command “ip flow-export destination 10.1.1.5 9995” would point a Cisco IOS device to a NetFlow collector at the given IP address, and would send the NetFlow data over port 9995.

40. When using Flexible NetFlow in order to create multiple flow monitors and exporters, which command would allow us to attach the name HELPDESK to a created flow record?

A. flow name HELPDESK
B. flow export HELPDESK
C. flow flexible HELPDESK
D. flow record HELPDESK

Answer: D
Explanation: In order to create a flow record and assign a name to that record, the command “flow record” followed by the desired name is used in Cisco IOS. Once this command is entered, the command line interface is placed in flow record configuration mode, allowing for further configuration options such as attaching a description about what the record was created for.

41. By default, which type of traffic does SPAN monitor in Cisco IOS?

A. Received
B. Transmitted
C. Transmitted and Received
D. Local

Answer: C
Explanation: By default, a Cisco IOS SPAN configuration will monitor both transmitted and received traffic on a selected interface. Other options can be selected during configuration if there are specific needs, using the keywords “rx” (only monitor received traffic) or “tx” (only monitor transmitted traffic). The “both” option is also available, which is the same as the default action that monitors both transmitted and received traffic.

42. After configuring ERSPAN in Cisco IOS, what command is necessary in order to enable the ERSPAN configuration on a selected interface?

A. erspan enable
B. run erspan
C. no shutdown
D. erspan admin enable

Answer: C
Explanation: When creating an ERSPAN session, by default the session is administratively disabled. This is the same state you would find a router interface in before giving the “no shut” command to administratively bring up the interface. While under monitor session configuration mode, the command “no shut” will bring the session into the administratively enabled state.

43. Which command keyword option for IP SLA configuration will allow an administrator to select when an IP SLA source begins transmitting data?

A. start-time
B. begin-sla
C. sla-schedule
D. sla-start

Answer: A
Explanation: The “start-time” keyword allows us to specify a starting time for the IP SLA probe. This can be followed by several options, such as the “after” keyword to start the probe after a specified amount of time. Exact times can also be entered in hours, minutes, and seconds if there is a specific time that the probe should start. Other options include “now” (for immediate probe start) and “random” (to start the probe after a random time interval).

44. Where should Policy Based Routing (PBR) be applied on a router?

A. On a router's egress interface
B. In a router's global configuration mode
C. On a router's ingress interface
D. In a router's router configuration mode

Answer: C
Explanation: Although "Local PBR" can be applied in a router's global configuration mode, PBR is applied on a router's ingress interface.

45. With Cisco Embedded Event Manager (EEM), what is used to create policies by using the command line interface (CLI)?

A. Scripts
B. YANG
C. XML
D. Applets

Answer: D
Explanation: Applets are a more simplified tool for creating EEM policies, as opposed to scripts that are created with an interpreter language. Applets can be used within the Cisco IOS command line interface (CLI) to create EEM policies.

46. Which Cisco line type is used for controlling inbound Telnet connections?

A. CTY
B. AUX
C. VTY
D. CDP

Answer: C
Explanation: VTY lines in Cisco IOS are essentially virtual terminal connections. There is no physical hardware associated with these lines, as they are a function of the IOS software. In the running configuration, these are denoted as "line vty 0 4", where the two numbers at the end are the line numbers. In this example, there are lines 0 through 4, for a total of five available VTY lines. These are used solely for controlling inbound Telnet connections.

47. Which AAA protocol used for external server deployments encrypts only the password field of the communication?

A. RADIUS
B. TACACS+
C. SNMP
D. Telnet

Answer: A
Explanation: The RADIUS protocol is an open standard used with external AAA database deployments. As opposed to the Cisco-proprietary TACACS+ protocol which encrypts the entire payload, RADIUS only encrypts the password field. RADIUS uses UDP ports 1812 and 1813 by default for communication.

48. Which type of access control list (ACL) allows us to match traffic source and destination IP addresses?

A. Expanded ACLs
B. IP ACLs
C. Standard ACLs
D. Extended ACLs

Answer: D
Explanation: Extended access control lists (ACLs) fall within the range of 100-199, with an expanded range of 2000-2699. These have the ability to filter much more granularly than standard ACLs, as they are able to filter specific protocols and match both source and destination IP addresses.

49. Which entity within the Control Plane Policing (CoPP) solution allows for traffic filtering and rate limiting?

A. ACL
B. QoS
C. MQC
D. SNMP

Answer: C
Explanation: Modular QoS CLI (MQC) allows for both filtering and rate-limiting of our network traffic. Within MQC, we have the ability to create and attach a traffic policy to an interface. ACLs are used to identify the traffic itself, against which we want to take action with MQC. Filtering and rate limiting are not performed by the ACL itself, but rather it is only used for traffic identification. The MQC policy is what allows for the filtering and rate-limiting.

50. Identify the component of the EAPOL 4-Way Handshake used to encrypt unicast traffic?

A. GMK
B. MIC
C. ANonce
D. PTK

Answer: D
Explanation: The Groupwise Master Key (GMK) is generated during EAP authentication and is known by both the Supplicant and the Authenticator. The GMK protects multicast and broadcast traffic.

The MIC (Message Integrity Code) is used to confirm a frame has not been modified in transit.

The ANonce is a random number generated by the Authenticator, while the SNonce is a random number generated by the Supplicant.

The PTK (Pairwise Transient Key) encrypts unicast traffic between the Supplicant (i.e., the wireless client) and its Authenticator (i.e., its access point).

51. Which type of web-based authentication (WebAuth) leverages an external AAA server that works as a centralized RADIUS database, such as Cisco Identity Services Engine (ISE)?

A. Local WebAuth
B. Distributed WebAuth
C. Central WebAuth
D. Client-Server WebAuth

Answer: C
Explanation: Central WebAuth redirects network client browsers to a central WebAuth server, which requires the client to login with valid credentials in order to obtain authentication and authorization. This is used in larger deployments that contain a centralized RADIUS database such as Cisco ISE.

52. Which of the following is not a solution used when achieving endpoint hardening?

A. Cisco AMP
B. Cisco Umbrella
C. Cisco AnyConnect

D. Cisco Smart Install

Answer: D
Explanation: Cisco Smart Install is a method for hardening the network, used for zero-touch deployment of new access layer switches. Cisco AMP, Cisco Umbrella, and Cisco AnyConnect are all used specifically for hardening our endpoints.

53. Which of the following is not an advantage of a next generation firewall (NGFW)?

A. Zero-touch deployment
B. Streamlined architecture
C. Deep packet inspection
D. Better throughput rates

Answer: A
Explanation: Next generation firewalls allow for a streamlined architecture by integrating multiple security services into a single appliance, the ability to monitor traffic at OSI layers 2 through 7 with deep packet inspection, and better throughput rates through more robust hardware and streamlined software.

54. Which security standard is considered to be the wired equivalent of WPA2 protection used in wireless networks?

A. MACsec
B. NAC
C. MAB
D. TrustSec

Answer: A
Explanation: MACsec is a Layer 2 protocol that relies on AES to provide confidentiality and integrity, similar to WPA2. However, MACsec operates over a wired Ethernet connection. This is an extension to 802.1X that provides secure key exchange and mutual authentication between MACsec capable devices.

55. By default, how long does it take a Cisco Catalyst switch to consider 802.1X to be timed out before beginning MAC Authentication Bypass (MAB)?

A. 30 seconds
B. 60 seconds
C. 90 seconds
D. 120 seconds

Answer: C
Explanation: MAC Authentication Bypass must wait until 802.1X times out before attempting network access. By default, this value is set to 90 seconds on a Cisco Catalyst switch. It's common for administrators to lower this value in order to overcome client access issues caused by the delay, but it's important to be aware that setting the timer interval too low can result in 802.1X bypass happening unnecessarily.

56. Which XML component gives more detail about an element and must appear in quotes?

A. Attribute
B. Comment
C. Declaration
D. Tag

Answer: A
Explanation: An XML Attribute gives more detail about an element and must appear in quotes. A Comment provides documentation within a file. A Declaration is the optional first line in an XML document that contains version and encoding information. A Tag is a string of text inside the < and > signs.

57. Identify the YANG Data Modeling element that represents an attribute of something being modeled.

A. Container
B. List
C. Leaf
D. Type

Answer: C
Explanation: A Leaf represents an attribute of something being modeled. A Container has Read-Write or Read-Only privileges and contains one or more lists, which represent something (e.g. a router interface) that's being modeled. A Type describes what kind of data (e.g. a string) that can be used to populate a leaf.

58. Identify the data type of the following: True

A. String
B. Floating Point
C. Boolean
D. Integer

Answer: C
Explanation: Since the word True is not in quotes, it's not a String data type. Instead, it's a Boolean data type that states if a condition is True or False.

59. Currently, you have a variable of x assigned an integer value of 4. However, you need to convert your variable of x to a string data type. Which of the following commands could you use?

    A. x=string(x)
    B. x=int("x")
    C. x=str(x)
    D. x=float(x)

Answer: C
Explanation: The str function can convert an integer or floating-point value to a string. The int function can convert a floating-point value to an integer, and the float function can convert an integer to a floating-point value.

60. Python uses the "if" function to do a Boolean evaluation. What Python function can be used with the "if" function to do a secondary Boolean evaluation if the first evaluation (as specified by the "if" function) is False?

    A. else
    B. elif
    C. iff
    D. elseif

Answer: B
Explanation: When using the "if" function in Python to do a Boolean evaluation. If the result of that evaluation is False, you can take a specific action specified by the "else" function, or you can do a secondary Boolean evaluation using the "elif" function.

61. Which if the following identifies two types of Python Loops?

    A. FOR and NEXT
    B. WHILE and IF
    C. FOR and WHILE
    D. INFINITE and IF

Answer: C

Explanation: Two types of Loops that can be used by Python are FOR and WHILE. A FOR loop will loop for as long as there is a value in a List (or an external file). A WHILE loop will loop while a condition is True.

62. In a Python script, you wish to open a file named “vlans.txt” in a mode that will let you write additional VLAN values to the file without overwriting the existing values already in the file. Which command could you use?

    A. file=open(“vlans.txt”,”r”)
    B. file=open(“vlans.txt”,”rw”)
    C. file=open(“vlans.txt”,”w”)
    D. file=open(“vlans.txt”,”a”)

Answer: D
Explanation: The “r” mode opens a file in read-only mode. There is no “rw” mode. The “w” mode opens the file in write mode, which will overwrite any existing values when you write a new value. The “a” mode is the append mode, which will let you add values to a file without overwriting any existing values.

63. What HTTP verb is used by REST create (not update) a new configuration?

    A. GET
    B. PUT
    C. PATCH
    D. POST

Answer: D
Explanation: The POST HTTP verb is used to Create a new entry (e.g. a new configuration), while PUT or PATCH can be used to Update an existing entry. The GET verb, however, only reads information.

64. Which component of the Ansible orchestration tool is written in YAML for execution on managed devices?

    A. Inventory
    B. Playbook
    C. Recipe
    D. API

Answer: B

Explanation: Ansible Playbooks are written in the YAML language, which contain code defining tasks for client execution that can be thought of as to-do lists. They are sets of instructions for the managed devices to perform. Playbooks can also be used to retrieve information from managed devices about their current state.

65. Within the SaltStack orchestration architecture, what is information about managed nodes that is sent back to the central Salt Master referred to as?

    A. Pillars
    B. Cookbooks
    C. Grains
    D. Blocks

Answer: C
Explanation: Grains are the built-in mechanism for determining information about managed nodes. The information included in Grains include network information, operating system version, hardware details, and more. This information is static and is not real-time data.

66. Which type of Application Programming Interface (API) take care of creating and managing sites, as well as retrieving network health information within Cisco DNA Center?

    A. Intent APIs
    B. Integration APIs
    C. Multivendor Support APIs
    D. Event and Notification APIs

Answer: A
Explanation: Intent APIs (also referred to as northbound interfaces) within Cisco DNA Center provide the graphical user interface that allows for site creation and management, network health retrieval, device onboarding and provisioning, policy creation, and troubleshooting. Intent APIs are used to enforce the configurations and settings that we choose in Cisco DNA Center.

67. Which REST API response code is returned when there is a problem with the request syntax that was sent out by the client?

    A. 201
    B. 200
    C. 400
    D. 401

Answer: C
Explanation: API response codes in the 4XX range indicate some sort of client-side error. A 400 BAD REQUEST response code specifically means that there was a problem with the syntax used by the client, and the server was unable to interpret the request.

68. Which section of the Cisco DNA Center management dashboard contains troubleshooting tools for the network?

    A. Design
    B. Assurance
    C. Policy
    D. Provision

Answer: B
Explanation: The Assurance section in Cisco DNA Center provides tools for network monitoring and troubleshooting. This includes both reactive tools, as well as proactive and predictive tools by use of A.I. and machine learning. Cisco DNA Center boasts the ability to predict issues before they happen, and also troubleshooting assistance through suggested remediation steps.

69. Within which plane of Cisco's SD-WAN solution is the vManage interface found?

    A. Data Plane
    B. Virtual Administrator Plane
    C. Control Plane
    D. Management and Orchestration Plane

Answer: D
Explanation: The Management and Orchestration Plane is where we find both vBond (the orchestration and provisioning component) and vManage (the graphical user interface). This is where you perform configuration, monitoring, provisioning, and troubleshooting.