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

1. Which type of network topology is most often found within a data center?

   A. Point-to-Multipoint
   B. Spine-Leaf
   C. Three-Tier
   D. Collapsed Core

Answer: B
Explanation: Data centers commonly use a Spine-Leaf design, where a leaf switch connects to multiple spine switches, such that the leaf switch can reach any other leaf switch by transiting a single spine switch. A Point-to-Multipoint design is commonly found in older wide area networks using Frame Relay or ATM. A Three-Tier architecture is commonly found in enterprise networks and consists of the Access, Building Distribution, and Core layers. A Collapsed Core design is commonly found in small to medium sized networks, where the Building Distribution and Core layers found in an enterprise network design are consolidated into a "collapsed core."

2. What is the role of an Active Virtual Gateway (AVG)?

   A. An AVG responds to ARP queries with the MAC address of the Master gateway.
   B. An AVG responds to different ARP queries with the MAC addresses of AVFs.
   C. An AVG responds to different ARP queries with the MAC address of the Backup gateway.
   D. An AVG responds to ARP queries with the MAC address of the Standby gateway.

Answer: B
Explanation: An Active Virtual Gateway (AVG) is a type of gateway used by Gateway Load Balancing Protocol (GLBP). GLBP is unique among the First Hop Redundancy Protocols (FHRPs) in that instead of having a single gateway service all traffic from a subnet, it load balances the traffic across as many as four Active Virtual Forwarders (AVFs). An AVG accomplishes this by responding to ARP queries (for a default gateway's virtual IP address) with different MAC addresses (i.e. the MAC addresses of the AVFs in a GLBP group).

3. Which type of wireless deployment access points are used in a large enterprise environment where centralized management is needed?

   A. Autonomous
   B. Lightweight
   C. Controller-less
   D. CAPWAP

Answer: B
Explanation: Lightweight access points require a centralized wireless LAN controller (WLC), which is used to manage all of the access points from a single location. This is also referred to as a controller-based deployment model, where the WLC can be a physical or a virtual device. No management or configuration is necessary on the individual access point.

4. You need to update your wireless network design to accommodate a higher client density. Which two of the following would be reasonable approaches? (Select 2)

   A. Increase the number of APs
   B. Increase Tx power of APs
   C. Use Wi-Fi 6E (if supported by clients)
   D. Decrease the number of APs

Answer: A and **C**
Explanation: Client density is a measure of clients in a wireless coverage area. To support more clients within an area (i.e., a higher client density), you could add the number of APs deployed within an area.

However, overlapping channels can be more of a challenge with tightly packed APs. Therefore, the transmit (i.e., Tx) power of the APs might be reduced to minimize interference with another AP using the same channel. Also, if supported by the clients, Wi-Fi 6E supports a higher client density, because it uses the 6 GHz band, which was not used by previous Wi-Fi standards.

5. Which type of network is created when using SD-WAN to create a virtual infrastructure?

   A. Backhaul Network
   B. Wide Area Network
   C. Underlay Network
   D. Overlay Network

Answer: D
Explanation: SD-WAN solutions create a virtual overlay network built on top of the actual, physical infrastructure. This physical infrastructure is referred to as an underlay network.

Examples of other well-known overlay network technologies include Voice over IP (VoIP) and Virtual Private Networks (VPNs). Creating an overlay network with SD-WAN provides transport independence, meaning that the physical underlay network can be any combination of transport protocols such as LTE, serial, wireless, MPLS, and more. SD-WAN creates a single overlay fabric that will intelligently direct traffic regardless of the underlying infrastructure.

6. Which plane of operation within the Cisco SD-Access fabric leverages Virtual Extensible LAN (VXLAN) tunneling?

   A. Control Plane
   B. Data Plane
   C. Management Plane
   D. Orchestration Plane

Answer: B
Explanation: The SD-Access data plane uses Virtual Extensible LAN (VXLAN) tunneling to create the virtual SD-Access overlay network. This is UDP-based communication, meaning any device with a valid IP address has the ability for receive and forward the information. The VXLAN encapsulation allows for the creation of multiple virtual networks within the overlay, where separate policies can be applied and enforced.

7. Which QoS mechanism is most appropriate for giving priority treatment to voice or video packets?

   A. cRTP
   B. WRED
   C. CB-WFQ
   D. LLQ

Answer: D
Explanation: Low Latency Queuing (LLQ) is an extension of Class Based Weighted Fair Queuing (CB-WFQ) that adds a priority queue. Voice and/or video packets are commonly placed in LLQ's priority queue in order to be sent ahead of other packet types. RTP Header Compression (cRTP) can reduce the size of the combined L2 and L3 headers of voice and video packets to 2 or 4 Bytes (2 Bytes without a UDP checksum, or 4 Bytes with a UDP checksum). However, while cRTP helps conserve bandwidth, it doesn't give priority treatment to RTP traffic. Weighted Random Early Detection (WRED) is a congestion avoidance mechanism, but it cannot be enabled for a priority queue. It can only be enabled on a queue for which CB-WFQ or Class Based Shaping has been configured. Class Based Weighted Fair Queuing (CB-WFQ) is a queuing mechanism that can assign minimum bandwidth guarantees to queues. However, CB-WFQ doesn't offer a priority queue.

8. How many access categories does Wi-Fi Multimedia (WMM) have?

   A. 4
   B. 8
   C. 16
   D. 64

Answer: A
Explanation: Wi-Fi Multimedia (WMM) maps 8 IEEE 802.1P markings into 4 WMM access categories: AC_BK (Background), AC_BE (Best Effort), AC_VI (Video), and AC_VO (Voice).

9. Which switching mechanism is the default method in most modern Cisco IOS devices?

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

Answer: B
Explanation: Cisco Express Forwarding (CEF) is the preferred method for modern IOS switching and is the default method on most modern Cisco devices. CEF stores information in a route cache for optimized lookup and efficient packet handling. This is much less processor-intensive than older mechanisms, reserving CPU power for critical operations such as encryption and QoS.

10. Which switch structure stores IP routing-related information, and is also referred to as the Cisco Express Forwarding (CEF) table?

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

Answer: C
Explanation: The Forwarding Information Base (FIB) table - CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

11. Identify the virtualization technology that includes a specific application a user wants to run, the support files for that applications, but not the operating system on top of which the application runs.

    A. Virtual Data Path
    B. Virtual Switch
    C. Virtual Server
    D. Container

Answer: D
Explanation: A container contains an application and its support files. The underlying operating system can support multiple containers containing applications need that operating system. A virtual server contains an operating system. A virtual data path is a technology that influences data flow, such as creating a tunnel between two sites. A virtual switch runs on a hypervisor and can logically interconnect virtual devices (e.g. virtual servers or virtual routers) also running on that hypervisor, in addition to logically connecting to a physical server's network interface card (NIC).

12. What statement is true of the global routing table in an VRF configuration (by default)?

    A. The global routing table is a combination of the routes found in the routing tables of each VRF instance.
    B. The global routing table does not contain routes seen in the routing table of any VRF instance.
    C. A VRF configuration disables the global routing table, and instead uses the routing table of each VRF instance.
    D. By default, routes appearing in a router's global routing table are "leaked" into the routing table of each VRF instance. However, routes in a VRF instance's routing table are not leaked into the global routing table.

Answer: B
Explanation: Even though "leaking" can be configured to allow a router's global routing table and a VRF instance's routing table to exchange routes, by default, the global routing table doesn't not see routes from nor exchange routes with a VRF instance's routing table.

13. When setting up encryption in an IPsec tunnel configuration, which of the following is NOT an available option?

    A. sha
    B. des
    C. aes
    D. 3des

Answer: A
Explanation: When setting up an IPsec tunnel, common configuration options for encryption are DES, 3DES, and AES, with AES typically being the most preferred option and DES being the least preferred option. However, Secure Hash Algorithm (SHA) is used for authentication rather than encryption.

14. What component of a LISP architecture identifies the IP address of a router responsible for forwarding traffic to devices within a LISP location?

    A. Endpoint ID (EID)
    B. Routing Locator (RLOC)
    C. Map Resolver (MR)
    D. Map Server (MS)

Answer: B
Explanation: Location/ID Separation Protocol (LISP) uses two identifiers for a network endpoint. First, the Routing Locator (RLOC) is the IP address of a router that can forward traffic to devices within a LISP location. Second, the Endpoint ID (EID) identifies the endpoint within a LISP location. The way a source RLOC knows how to reach a specific endpoint at a remote location is by querying a Map Resolver (MR), which returns the destination RLOC for the requested EID. The MR learned the destination RLOC for the EID from a Map Server (MS), with which the destination RLOC registered the EID.

15. Switches SW1 and SW2 are directly connected with a Gigabit Ethernet connection. Which of the following Dynamic Trunk Protocol (DTP) mode combinations will FAIL to bring up a trunk between the switches?

    A. SW1: Dynamic Desirable – SW2: Dynamic Auto
    B. SW1: Trunk – SW2: Dynamic Auto
    C. SW1: Dynamic Auto – SW2: Dynamic Auto
    D. SW1: Trunk – SW2: Dynamic Desirable

Answer: C

Explanation: DTP modes of Trunk and Dynamic Desirable both initiate the formation of a trunk by sending DTP frames. The mode of Dynamic Auto will setup a trunk if it receives a DTP frame, but it doesn't initiate trunk formation. Also, Access mode prevents a trunk from being formed. As a result, the only two mode combinations that would fail to bring up a trunk are: (1) one side set to Access (regardless of the other side's mode) and (2) both sides set to Dynamic Auto.

16. An EtherChannel's load-balancing algorithm is to set "dst-mac," and the EtherChannel contains eight ports. What information determines the specific link in an EtherChannel used to send a specific packet?

    A. The last 2 bits of the destination MAC address
    B. The last 3 bits of the destination MAC address
    C. The last 4 bits of the destination MAC address
    D. The last 8 bits of the destination MAC address

Answer: B
Explanation: The "dst-mac" load-balancing algorithm uses a packet's destination MAC address to select the physical connection in an EtherChannel bundle that is used to send a packet. The number of bits in the destination MAC address used to make the path selection decision is determined by the number of links in the EtherChannel. If there were only two links, the last bit in the destination MAC address would be used, because a single bit could represent two values (i.e. 0 or 1). Similarly, the last two bits in a destination MAC address would be used if the EtherChannel had four physical links (because two bits can be arranged in four different ways), and the last three bits in a destination MAC address would be used if the EtherChannel had eight physical links.

17. Which Spanning Tree Protocol (STP) variant allows different collections of VLANs to share different Spanning Tree instances, resulting in an optimal Spanning Tree topology for each VLAN without the overhead of having a Spanning Tree instance for each VLAN?

    A. CST
    B. PVST+
    C. MSTP
    D. Rapid PVST+

Answer: C
Explanation: Common Spanning Tree (CST) uses a single Spanning Tree topology for all VLANs, which could result a suboptimal tree for some VLANs. Per-VLAN Spanning Tree Protocol Plus (PVST+) and Rapid PVST+ give each VLAN its own Spanning Tree instance. While this results in each VLAN having an optimal tree, it can require a switch to maintain many Spanning Tree instances. Multiple Spanning Trees Protocol (MSTP), which is sometimes written as MST, recognizes that a specific Spanning Tree instance might be optimal for multiple VLANs.

Therefore, rather than having each of those VLANs run their own identical instances of Spanning Tree, a single instance can be created. That instance is then joined by all VLANs whose optimal spanning tree is defined by that instance.

18. Which of the following features creates a Rapid PVST+ Edge Port?

    A. PortFast
    B. UplinkFast
    C. BackboneFast
    D. BPDUGuard

Answer: A
Explanation: The PortFast feature causes a switch port to go active when an end station is connected, without waiting through any STP delays. In Rapid PVST+ terminology, a Point-to-Point interface (i.e. a full duplex switch port) enabled with the PortFast feature is called an Edge Port.

19. Identify the STP protection feature that causes a port to go into a Root Inconsistent state if it receives a superior BPDU.

    A. PortFast
    B. BPDU Guard
    C. UplinkFast
    D. Root Guard

Answer: D
Explanation: PortFast is a Spanning Tree Protocol (STP) feature that causes a previously empty port to bypass the Listening and Learning states of STP when a device is attached, causing the port to immediately transition into the Forwarding state. This feature is often appropriate on client-facing ports.

The BPDU Guard feature is often enabled on a port already configured for PortFast. If that port receives a Bridge Protocol Data Unit (BPDU) then it transitions into an Error Disabled (specifically, “err-disabled”) state.

The UplinkFast feature is a legacy Cisco enhancement to STP. Specifically, the UplinkFast feature sped up STP convergence, in some cases, when there was an STP topology change.

The Root Guard feature can be enabled on a port that should never become a switch’s Root Port. If a superior BPDU (i.e., a BPDU advertising a lower Bridge ID (BID) that the Root Bridge) is seen off a port enabled for Root Guard, that port transitions into a Root Inconsistent state. This can help prevent an attacker from introducing a switch to a network and causing their rogue switch to be elected as a Root Bridge.

20. What parameter exchanged in VTP advertisements determines how authoritative a VTP update is?

    A. Configuration Register
    B. Metric
    C. Distance
    D. Configuration Revision Number

Answer: D
Explanation: A switch configured for VTP uses the Configuration Revision Number of a VTP advertisement to determine whether or not a received VTP advertisement is more authoritative than the switch's local VLAN database.

21. Identify the IPv4 multicast address used to communicate just with OSPF Designated Routers (DRs) and Backup Designated Routers (BDRs).

    A. 224.0.0.10
    B. 224.0.0.5
    C. 224.0.0.9
    D. 224.0.0.6

Answer: D
Explanation: 224.0.0.10 is the IPv4 multicast group used to communicate with EIGRP routers. 224.0.0.5 is used to communicate with all OSPF routers. 224.0.0.9 is used to communicate with RIPv2 routers. 224.0.0.6 is used to communicate with OSFP DR and BDR routers.

22. What OSPF configuration option prevents a router interface from sending OSPF Hello messages, while still participating in an OSPF process?

    A. Stub Area
    B. NSSA
    C. Passive Interface
    D. Totally Stubby Area

Answer: C
Explanation: A Passive Interface is an interface that participates in an OSPF routing process without sending Hello messages. This type of interface might be appropriate for an interface connecting out to endpoints but no other OSPF-speaking routers. Having such an interface be a Passive Interface would allow that network be advertised by OSPF to neighboring routers

without sending unnecessary Hello messages and also prevent a malicious user from adding an OSPF-speaking router to that interface's network and forming an unwanted OSPF adjacency.

23. OSPF can perform route summarization on an ASBR or on an ABR. What command is used to summarize routes on an ASBR?

    A. summary-address
    B. route-map
    C. area range
    D. area stub

Answer: A
Explanation: OSPF route summarization can be performed on an Autonomous System Boundary Router (ASBR) as routes are being redistributed into OSPF from another autonomous system. This is accomplished using the "summary-address" command. Additionally, OSPF can perform route summarization on an Area Border Router (ABR) as routes are being advertised from one OSPF area into another OSPF area. This is accomplished using the "area range" command.

24. What command would you enter to create an OSPF routing process numbered "1" for OSPFv3 using an Address Families configuration?

    A. ipv6 router ospf 1
    B. ipv6 router ospfv3 1
    C. router ospfv3 1
    D. router ipv6 ospf 1

Answer: C
Explanation: Using the traditional configuration approach for OSPFv3, you create an OSPFv3 routing process numbered "1" using the "ipv6 router ospf 1" command. However, with the Address Families approach to OSPFv3 configuration, you instead use the "router ospfv3 1" command. The Address Families configuration approach to OSPFv3 allows you to configure routing for both IPv4 and IPv6 under a single hierarchical configuration.

25. Select the correct order of path selection criteria considered by BGP.

    A. Weight, Local Preference, Origin Type, AS Path Length, Originate MED, Paths, Router ID
    B. Router ID, Weight, Local Preference, Originate, AS Path Length, Origin Type, MED, Paths
    C. Local Preference, Weight, Originate, AS Path Length, Origin Type, MED, Paths, Router ID
    D. Weight, Local Preference, Originate, AS Path Length, Origin Type, MED, Paths, Router ID

Answer: D

Explanation: The correct order of BGP path selection criteria is: Weight, Local Preference, Originate, AS Path Length, Origin Type, MED, Paths, and Router ID. A memory aid for remembering this order is the acrostic: “We Love Oranges AS Oranges Mean Pure Refreshment.” The main challenge with this memory aid is correctly ordering the “Originate” and “Origin Type” criteria, because they both begin with a “O.”

26. Which configuration is often used to influence outbound path selection on a BGP router with two or more neighbors in different autonomous systems?

    A. Assigning a higher Local Preference value to routes coming in from a preferred neighbor
    B. Assigning a lower Local Preference value to routes coming in from a preferred neighbor
    C. Assigning a shorter AS Path value to routes coming in from a preferred neighbor
    D. Assigning a longer AS Path value to routes coming in from a preferred neighbor

Answer: A
Explanation: The Local Preference path selection parameter is commonly used for influencing outbound path selection decisions, with higher values being preferred. The AS Path attribute is commonly used for influencing inbound path selection decisions, with shorter AS Paths being preferred.

27. If you’re configuring Multiprotocol BGP, where IPv4 routes are advertised over an IPv4 session and IPv6 routes are advertised over an IPv6 session, what step must be manually configured for an IPv6 neighbor that is automatically configured for an IP4 neighbor?

    A. The “ebpg-multihop” value must be specified.
    B. The remote AS of a neighbor must be configured in IPv6 address family configuration mode.
    C. A route-map must be configured to advertise the IPv6 next-hop address.
    D. The IPv6 neighbor needs to be activated.

Answer: D
Explanation: When configuring Multiprotocol BGP, neighbors are specified under router configuration mode. Then, under router-address-family configuration mode, the neighbors need to be activated. Interestingly, the “neighbor [neighbor_ip_address] activate” command is automatically entered for the IPv4 address family but must be manually configured for the IPv6 address family.

28. Which lightweight access point special purpose mode is used to delegate the AP to solely perform various background operations, such as location-based services and rogue device detection?

A. FlexConnect Mode
B. Sniffer Mode
C. SE-Connect Mode
D. Monitor Mode

Answer: D
Explanation: Monitor mode is a special purpose mode to which we can assign a Cisco lightweight access point. When operation in this mode, the access point does not provide any network access to users. The operation is dedicated to performing various background operations, such as intrusion detection service (IDS) monitoring, rogue access point detection, and location-based services, among other things.

29. During which lightweight access point operation state does the device poll the wireless LAN controller (WLC) for information such as QoS rules, SSIDs, and security parameters?

A. WLC Join State
B. Image Download State
C. Config Download State
D. WLC Discovery State

Answer: C
Explanation: During the Config Download State, the access point will poll the WLC for configuration information. This includes QoS rules, SSIDs, and security parameters, among other things. Once all of the necessary configurations are known and applied, the lightweight access point moves into the Run State, where it is fully operational and providing clients with network access.

30. In a Network Address Translation (NAT) configuration, a client inside of a network has its private IP address of 10.1.1.12 translated into a publicly routable IP address of 192.0.2.10. What is the 192.0.2.10 IP address referred to in this scenario?

A. Inside Local Address
B. Inside Global Address
C. Outside Local Address
D. Outside Global Address

Answer: B
Explanation: In this scenario, the 192.0.2.10 IP address is referred to an Inside Global Address, because the IP address is Globally routable and refers to a device on the Inside of the network. Also, in this scenario, the 10.1.1.12 IP address is referred to an Inside Local Address, because it’s a Locally routable address and refers to a device on the Inside of the network.

31. When configuring Dynamic NAT, what is the “pool” parameter used to specify?

A. The range of ephemeral port numbers into which outgoing connections are dynamically assigned
B. The range of Inside Local addresses to be mapped to Inside Global addresses
C. The range of Inside Global addresses into which Inside Local addresses are mapped
D. The range of Outside Global addresses into which Inside Local addresses are mapped

Answer: C
Explanation: When configuring Dynamic NAT, an Access Control List (ACL) is typically used to identify the Inside Local addresses to be mapped to Inside Global addresses. However, a “pool” parameter is used to define a range of Inside Global addresses into which the Inside Local addresses are mapped.

32. What port number is used by Network Time Protocol (NTP)?

A. TCP port 443
B. UDP port 69
C. UDP port 123
D. TCP port 25

Answer: C
Explanation: TCP port 443 is used by HTTPS. UDP port 69 is used by TFTP. UDP port 123 is used by NTP, and TCP port 25 is used by SMTP.

33. Which of the following is true of VRRP but not true of HSRP?

A. VRRP has a default Hello time of 3 seconds.
B. VRRP has Preemption disabled by default.
C. VRRP is Cisco-proprietary.
D. VRRP can used an interface’s IP address as a Virtual IP address.

Answer: D
Explanation: HSRP has a default Hello time of 3 seconds. However, instead of a Hello time, VRRP uses a Master Advertisement Interval, which defaults to 1 second. Also, HSRP has Preemption disabled by default, while VRRP has Preemption enabled by default. While HSRP is Cisco-proprietary, VRRP is an industry standard First Hop Redundancy Protocol (FHRP). Finally, while HSRP cannot use a Virtual IP address that is already assigned to an interface, VRRP can.

34. What command is used to require a router to use NTP authentication?

A. ntp secure
B. ntp authentication
C. ntp authenticate
D. ntp peer-authentication

Answer: C
Explanation: The “ntp authenticate” command is used to require a router to use NTP authentication. The “ntp authentication-key [key_number] md5 [key_string]” command is used to define an authentication key, and the “ntp trusted-key [key_number]” command is used to identify which key is trusted.

35. Which of the following is true of an End-to-End Transparent Clock in a topology using Precision Time Protocol (PTP)?

A. It sends pDelay_Request messages in response to Sync messages.
B. It forwards PTP packets without calculating a Residence Time.
C. It has the ability to connect to multiple VLANs in multiple PTP domains.
D. It forwards received Sync messages.

Answer: D
Explanation: Transparent Clocks used in PTP configurations can connect to a single VLAN in a single PTP domain. They also measure the time it takes a PTP packet to move from a switch’s ingress port to a switch’s egress port. That delay is called the Residence Time.

There are two types of Transparent Clocks: (1) End-to-End and (2) Peer-to-Peer. While a Peer-to-Peer Transparent clock responds to Sync messages with pDelay_Request messages, to calculate the path delay for each clock hop, an End-to-End Transparent Clock transparently forwards the original Sync message from a Grandmaster clock towards its destination.

36. Which extended traceroute option allows us to trace a network route that is more than 30 hops away from the device we are using?

A. probe
B. timeout
C. numeric
D. ttl

Answer: D
Explanation: By using the “ttl” keyword at the end of a traceroute command, we can specify the TTL value that should be used during the trace. By default, Cisco IOS TTL values are set to a

maximum of 30 hops. If we need to trace further than this, we can manually set the TTL value up to a maximum of 255 hops. For example, if network 10.10.10.10 needs to be traced up to 40 hops, we would use the command “traceroute 10.10.10.10 ttl 40” from an EXEC prompt.

37. Which well-known port is used by an SNMP manager as default for polling SNMP agent devices in the network?

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

Answer: D
Explanation: By default, SNMP managers use UDP communication over port 161 in order to poll SNMP agent devices in the network. These polls are remote queries that are used to gather information about the hardware and software states of the devices.

38. When configuring an SNMP manager in Cisco IOS, which command keyword option will ensure that we are using both authentication and encryption with SNMP version 3 (SNMPv3)?

    A. auth
    B. nopriv
    C. priv
    D. encrypt

Answer: C
Explanation: SNMP version 3 (SNMPv3) provides both authentication and encryption features. This is the most recent and preferred version of SNMP, which introduced enhanced security. Within SNMPv3 there are three security levels in IOS; “auth,” “no priv,” and “priv.” Using the “priv” keyword will ensure that we take advantage of both the authentication and encryption features in SNMPv3.

39. Which Cisco IOS command would be used to point Syslog message collection to a server with the IP address 10.1.1.5?

    A. logging manager 10.1.1.5
    B. logging host 10.1.1.5
    C. logging server 10.1.1.5
    D. logging external 10.1.1.5

Answer: B

Explanation: Using an external server to collect Syslog message is a best practice in an enterprise environment. In order to point a Cisco IOS device to a Syslog server for message collection, we use the command “logging host” followed by the server’s IP address.

40. Which version of NetFlow added a dynamic data format for use with templates?

    A. NetFlow v5
    B. NetFlow v8
    C. NetFlow v9
    D. NetFlow v10

Answer: C

Explanation: NetFlow version 9 is the most recent version of the protocol, adding better security and analysis features as well as the ability to accurately report on multicast traffic. The format is dynamic, meaning that the format can change. Templates are used to inform the NetFlow collector about the format in which the collected data is being represented so that correct interpretation can happen.

41. Which type of Switched Port Analyzer (SPAN) configuration uses Generic Routing Encapsulation (GRE) for traffic capture?

    A. SPAN
    B. ERSPAN
    C. RSPAN
    D. GRESPAN

Answer: B

Explanation: Encapsulated Remote SPAN (ERSPAN) is a Cisco-proprietary version of SPAN. This is similar to RSPAN, but rather than using Layer 2 switching as RSPAN does, ERSPAN uses Layer 3 routing to send traffic to a centralized server using Generic Routing Encapsulation (GRE).

42. When configuring Remote SPAN (RSPAN), which command option designates a selected VLAN to specifically be used for SPAN traffic delivery to a remote network?

    A. remote-span
    B. vlan remote
    C. vlan-rspan
    D. remote-span vlan

Answer: A

Explanation: While under VLAN configuration mode, the command “remote-span” will designate the selected VLAN to be used as the delivery VLAN for RSPAN traffic. A VLAN that has been designated as an RSPAN VLAN is trunked to other switches in order to transport session traffic to another network. This VLAN cannot be assigned to any access ports.

43. Which piece of an IP Service Level Agreement (SLA) configuration is an optional component?

    A. IP SLA Source
    B. IP SLA Collector
    C. IP SLA Responder
    D. IP SLA Listener

Answer: C
Explanation: An IP Service Level Agreement (SLA) configuration requires an IP SLA source in order to generate packets which are sent out to destination devices. Responses from the devices would include timestamps with other metrics about the device. Optionally, a remote Cisco router can be configured as an IP SLA responder in order to provide more advanced response metrics. Certain IP SLA operations require a responder, while others do not.

44. When configuring an advanced IP SLA configuration, which general command configures a Cisco IOS Router to be an IP SLA responder?

    A. ip sla listen
    B. ip sla remote
    C. ip sla probe
    D. ip sla responder

Answer: D
Explanation: The command “ip sla responder” is used to configure a Cisco IOS router as an IP SLA responder. This command is followed by the type of probe to which it will be responding, and a port number. For example, to configure a router as a responder to TCP connect probes over port 5000, the complete command would be “ip sla responder tcp-connect port 5000.”

45. What configuration structure does PBR use to match traffic and specify behavior for that traffic?

    A. policy-map
    B. route-map
    C. class-map
    D. access-class

Answer: B
Explanation: A policy-map and class-map are used for quality of service (QoS). An access-class is used to limit incoming connections to a router's management plane. However, a route-map can match traffic and dictate how that matched traffic should be treated, and it's a route-map that's used by Policy Based Routing (PBR).

46. When configuring Cisco Embedded Event Manager (EEM) using applets within the CLI, which command keyword defines a condition that we want to take action against?

    A. identity
    B. event
    C. resource
    D. object

Answer: B
Explanation: After creating and naming an applet within the Cisco IOS CLI, the keyword "event" is used to identify a condition that we want to take action against. This event is what will trigger our applet to action. For example, if we used "event syslog" followed by a specific Syslog message that we want to monitor for, any time that message was populated in the logging buffer, the applet would be triggered, and our configured action would be performed.

47. Which Cisco IOS access level provides access to commands at the read-only level?

    A. Level 0
    B. Level 5
    C. Level 1
    D. Level 15

Answer: C
Explanation: Cisco IOS privilege level 1 is also referred to as the user level, or user EXEC mode. From this mode, you have access to read-only information about the router, such as interface status and routing table information, but you do not have the ability to make any changes to the running configuration file.

48. Which of the following is considered to be a standard numbered access control list (ACL)?

    A. 100
    B. 1300
    C. 199
    D. 2000

Answer: B

Explanation: Standard numbered access control lists (ACLs) fall within the range of 1-99. There is also an extended range in case you need additional standard numbered ACLs, which fall within the range of 1300-1999.

49. Which type of access control list (ACL) should be placed as close to the source as possible?

    A. Standard ACL
    B. Extended ACL
    C. Source ACL
    D. Destination ACL

Answer: B

Explanation: Extended ACLs have the ability to filter between protocol types and can match traffic based on both source and destination IP addressing. Because of the ability to see IP addressing in this way, a best practice recommendation is to place extended ACLs as close to the source as possible in order to stop traffic early on. This ensures that unwanted traffic doesn't take up network bandwidth unnecessarily. The opposite is true of standard ACLs, which are recommended to be placed as close to the destination as possible.

50. Which native extensible authentication protocol (EAP) type uses certificates for mutual authentication?

    A. EAP-TLS
    B. EAP-MD5
    C. EAP-SSL
    D. EAP-MSCHAPv2

Answer: A

Explanation: EAP-TLS is one of the most commonly used native EAP types. This is considered to be one of the most secure EAP types and is one of the original authentication methods defined by the IEEE 802.1X standard. This requires a certificate authority in order to use X.509 certificates for mutual authentication between the client and server.

51. Which encryption standard is leveraged by WPA2 and WPA3 for more advanced encryption and protection?

A. SSL
B. TKIP
C. AES
D. SHA

Answer: C
Explanation: TKIP and AES are two encryption standards leveraged by WPA for securing a wireless network. The temporal key integrity protocol (TKIP) is the original standard used by WPA, combining a key string and SSID in order to generate unique encryption keys. Due to this being susceptible to attacks, WPA2 and WPA3 moved to advanced encryption standard (AES) for improved encryption capabilities with a more advanced algorithm.

52. Which secure domain found in Cisco's cyber threat defense framework deals with the internal and external security policies, such as HIPAA regulations?

A. Security Intel
B. Segmentation
C. Compliance
D. Threat Defense

Answer: C
Explanation: The Compliance domain addresses both internal and external security policies. Examples of these include standard regulations such as HIPAA, SOX, and PCI. This would also include any internal policies that are specific to your network.

53. Which mechanism is used by Cisco Identity Services Engine (ISE) to assign security tags for access policy enforcement?

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

Answer: A
Explanation: Cisco TrustSec is used by Cisco ISE to assign a security group tag (SGT) to each device at the egress point of a TrustSec capable device. Based on the SGT tag, certain access policies will be enforced elsewhere in the infrastructure. SGTs can be used by routers, switches, and firewalls on Cisco TrustSec capable devices in order to make forwarding decisions.

54. Which piece of the Network Access Control (NAC) architecture receives extensible authentication protocol (EAP) packets and translates those into RADIUS packets?

A. Supplicant
B. Translator
C. Authentication Server
D. Authenticator

Answer: D
Explanation: The Authenticator is the piece of the Network Access Control (NAC) architecture that controls access to the network based on a client's authentication status. This is commonly a switch or wireless LAN controller. The Authenticator receives EAP packets from the client, where Supplicant software is installed in order to send identity credentials to the Authenticator. These are translated into RADIUS packets and forwarded to the Authentication Server in order to validate the client identity.

55. Northbound Interfaces (NBIs) are what type of Application Programing Interfaces (APIs)?

A. YANG
B. OpenFlow
C. REST
D. JSON

Answer: C
Explanation: Northbound Interfaces are Representational State Transfer (REST) APIs, which use HTTP verbs to communicate with an SDN controller. YANG is a type of data modeling. OpenFlow is an example of a Southbound Interface (SBI), and JSON is a type of data formatting.

56. Which of the following best describe the "Object" JSON data structure?

A. An unordered set of name/value pairs enclosed in straight brackets
B. An unordered set of name/value pairs enclosed in curly brackets
C. An ordered set of name/value pairs enclosed in straight brackets
D. An ordered set of name/value pairs enclosed in curly brackets

Answer: B
Explanation: A JSON Object is an unordered set of name/value pairs enclosed in curly brackets. A JSON Array is an ordered set of comma-separated values enclosed in straight brackets.

57. You install Python version 3.8.1 on an operating system that already has Python version 2.7 installed. What command do you issue at the command prompt to run Python version 3.8.1?

    A. python
    B. python3.8.1
    C. python3.8
    D. python 3

Answer: C
Explanation: If you issue the "python" command, it will run the preinstalled version of 2.7. Issuing the command "python3.8.1" will not work, because you're specifying the version too many levels deep. However, issuing the command "python3.8" will run Python version 3.8.1 in this case. Also, the command "python3" would have worked, but not "python 3," because there is a space before the "3."

58. What utility comes bundled with Python to give you an interface to the Interactive Interpreter and uses straight quotes (instead of open and close quotes) along with color coding of commands, all of which help you better enter Python commands?

    A. Bash
    B. vi
    C. Emacs
    D. IDLE

Answer: D
Explanation: IDLE (Interactive DeveLopment Environment) is a utility that comes with Python and serves as an excellent interface to Python's Interactive Interpreter, as compared to an operating system's command prompt. Bash is a UNIX shell, while both vi and Emacs are UNIX editors.

59. You have a Python list named "inventory" and wish to display the last value in the list. What Python command could you use?

    A. print(inventory[-1])
    B. print(inventory.end)
    C. print(inventory[0])
    D. print[inventory.end]

Answer: A
Explanation: A Python List is an ordered list of comma-separated values enclosed in straight brackets. You can print a specific value from a list using the command print(name[x]), where

“name” is the name of the list variable, and x is an integer identifying the position of the value in the list. The numbering of the values starts at 0. Therefore, in this example, to print the first value in the list, you could use a command of print(inventory[0]). However, you can print the last value in a list with the command print(inventory[-1]). Similarly, you can print the next to last value in a list with the command print(inventory[-2]).

60. Which of the following best describes a Python Dictionary?

   A. An ordered set of name/value pairs enclosed in straight brackets
   B. An unordered set of name/value pairs enclosed in straight brackets
   C. An ordered set of name/value pairs enclosed in curly brackets
   D. An unordered set of name/value pairs enclosed in curly brackets

Answer: D
Explanation: While a Python List is an ordered set of values enclosed in straight brackets, a Python Dictionary is an unordered set of name/value pairs enclosed in curly brackets.

61. You’re writing a Python script and wish to ask the user the name of the SSID in a wireless network, and you want to assign their response to a variable of ssid. Which command can you use?

   A. ssid=input(“What is the name of the SSID? “)
   B. input=ssid(“What is the name of the SSID? “)
   C. ssid=input[“What is the name of the SSID? “]
   D. ssid=input(What is the name of the SSID?)

Answer: A
Explanation: You can use the “input” function to get input from a user running a program. Since “input” is a function, the prompt is enclosed in parenthesis, not straight brackets. Also, since the prompt is a string, it’s enclosed in quotes. Therefore, the command ssid=input(“What is the name of the SSID? “) will prompt the user with the string of “What is the name of the SSID? “ The user’s response will then be stored in the variable of ssid.

62. NETCONF supports what type of data formatting?

   A. XML
   B. JSON
   C. HTTP
   D. HTTPS

Answer: A

Explanation: While RESTCONF supports either XML of JSON data formatting, NETCONF only supports XML data formatting.

63. Which Chef orchestration component pulls configuration information from the central Chef server?

    A. Request Agent
    B. Pull Drone
    C. Workstation
    D. Client Node

Answer: D
Explanation: The Chef Client Nodes are what we call any network components that are being managed by a centralized Chef Server. Each node will have a Chef Client installed that is used to pull the configuration information from the Chef Server. This includes storage devices, containers, physical hardware, and virtual hardware.

64. Which Puppet orchestration component is prepared for Puppet Agents, containing configuration changes that need to take place on a node?

    A. Fact
    B. Catalog
    C. XML Tag
    D. YANG Status

Answer: B
Explanation: The central Puppet server is called a Puppet Master. The Puppet Master received information about the Puppet Agents (or client nodes) referred to as Facts. These Facts are used to compare the current state of each node to the desired configuration state. The Puppet Master then prepares a Catalog containing configuration change and makes the Catalog available to the Puppet Agent.

65. 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.

66. 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.

67. 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.

68. 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 400 range indicate some sort of client-side error. A 401 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.