Cisco CCNP Enterprise ENCOR 350-401 PassFast

Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR 350-401)

Todd Lammle
CCNP Enterprise Expert Trainer

TL TODD LAMMLE

Implementing Cisco Enterprise Network Core Technologies v1.0 (350-401)

Book Update Version 1.0

This book will dive into the latest practice questions needed before you take the Cisco CCNP exam 350-401

Table of Contents

Chapter 1: Architecture

The objectives covered in this chapter:

15% 1.0 Architecture

- ***1.1 Explain the different design principles used in an enterprise network***
  - ***1.1.a Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning***
  - ***1.1.b High availability techniques such as redundancy, FHRP, and SSO***
- ***1.2 Analyze design principles of a WLAN deployment***
  - ***1.2.a Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)***
  - ***1.2.b Location services in a WLAN design***
- ***1.3 Differentiate between on-premises and cloud infrastructure deployments***
- ***1.4 Explain the working principles of the Cisco SD-WAN solution***
  - ***1.4.a SD-WAN control and data planes elements***
  - ***1.4.b Traditional WAN and SD-WAN solutions***
- ***1.5 Explain the working principles of the Cisco SD-Access solution***
  - ***1.5.a SD-Access control and data planes elements***
  - ***1.5.b Traditional campus interoperating with SD-Access***
- ***1.6 Describe concepts of wired and wireless QoS***

1.6.a QoS components

1.6.b QoS policy

1.7 Differentiate hardware and software switching mechanisms

1.7.a Process and CEF

1.7.b MAC address table and TCAM

1. What is the full-duplex bandwidth capacity of a Cisco Nexus 7000 Series switch with 18 slots (2 Supervisor Engine Slots and 16 I/O Slots), given that the inter-slot switching capacity is 550 Gbps?
A. 8800 Gbps
B. 9350 Gbps
C. 18.7 Tbps
D. 19.8 Tbps

2. 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

3. 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

4. Which QoS mechanism is most appropriate for giving priority treatment to voice or video packets?
A. cRTP
B. WRED
C. CB-WFQ
D. LLQ

5. How many access categories does Wi-Fi Multimedia (WMM) have?
A. 4
B. 8
C. 16
D. 64

6. 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

7. 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

8. 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

9. 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.

10. 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

11. 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

12. 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

13. Which memory architecture is used on all Catalyst switch models to perform Layer 2 switching?
A. CAM
B. TCAM
C. FIB
D. RIB

14. Which entity within the Control Plane Policing (CoPP) solution allows for traffic filtering and rate limiting?
A. ACL
B. QoS
C. MQC
D. SNMP

15. 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

Chapter 1: Answers

1. What is the full-duplex bandwidth capacity of a Cisco Nexus 7000 Series switch with 18 slots (2 Supervisor Engine Slots and 16 I/O Slots), given that the inter-slot switching capacity is 550 Gbps?

C. 18.7 Tbps

To calculate a switch's bandwidth capacity (not factoring in full-duplex communication), use the formula:
Switch BW Capacity = (Inter-slot Switching Capacity * Number of I/O Slots) + [(Number of SE Modules * Inter-slot Switching Capacity) / 2]

Note that the inter-slot switching capacity of a supervisor engine (SE) is half that of an I/O module, hence the division by 2 at the end of the formula.
Switch BW Capacity = (550 Gbps * 16) + [(2 * 550 Gbps) / 2]
Switch BW Capacity = (8800 Gbps) + 550 Gbps
Switch BW Capacity = 9350 Gbps

To factor in full-duplex communication, we multiply by 2.
Full Duplex Switch BW Capacity = (9350 Gbps) * 2
Full Duplex Switch BW Capacity = 18.7 Tbps
A. 8800 Gbps
B. 9350 Gbps
D. 19.8 Tbps

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

D. Overlay Network

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.

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

B. Data Plane

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.

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

D. LLQ

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.

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

A. 4

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).

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

B. Cisco Express Forwarding

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.

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

D. RIB

The Routing Information Base (RIB) is the location where all information related to IP routing is stored. This is not specific to any particular routing protocol, but is used by all protocols such as OSPF, BPG, and so on. Learned routes are inserted into the RIB, including dynamic, static, and directly connected routes. If a route becomes unreachable it will eventually be removed from the RIB, based on the timers in use with the protocol related to the route.
A. CAM
B. TCAM
C. FIB

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

D. Management and Orchestration Plane

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.

9. 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.

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.

10. 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

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.

11. 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?

D. Fabric Control Plane Node

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.

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

B. Create the "class-default" Class Map

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.

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

A. CAM

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.

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

C. MQC

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.

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

D. Management and Orchestration Plane

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.

Chapter 2: Virtualization

The objectives covered in this chapter:

10% 2.0 Virtualization

2.1 Describe device virtualization technologies

2.1.a Hypervisor type 1 and 2

2.1.b Virtual machine

2.1.c Virtual switching

2.2 Configure and verify data path virtualization technologies

2.2.a VRF

2.2.b GRE and IPsec tunneling

2.3 Describe network virtualization concepts

2.3.a LISP

2.3.b VXLAN

1. 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.

2. 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

3. 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

4. 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.

5. What is the term used to refer to a broadcast domain within a VXLAN network?
A. VLAN
B. VEM
C. VNI
D. VTEP

Chapter 2: Answers

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

B. An AVG responds to different ARP queries with the MAC addresses of AVFs.

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).

2. 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.

D. Container

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).

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

B. Type 2

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.

4. 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")?

D. Each virtual NIC within a virtual machine has a unique MAC address.

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.

5. What is the term used to refer to a broadcast domain within a VXLAN

network?

C. VNI

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.

Chapter 3: Infrastructure

The objectives covered in this chapter:

30% 3.0 Infrastructure

3.1 Layer 2

3.1.a Troubleshoot static and dynamic 802.1q trunking protocols

3.1.b Troubleshoot static and dynamic EtherChannels

3.1.c Configure and verify common Spanning Tree Protocols (RSTP and MST)

3.2 Layer 3

3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link

state, load balancing, path selection, path operations, metrics)

3.2.b Configure and verify simple OSPF

environments, including multiple normal

areas, summarization, and filtering (neighbor adjacency, point-to-point and

broadcast network types, and passive interface)

3.2.c Configure and verify eBGP between directly connected neighbors (best path

selection algorithm and neighbor relationships)

3.3 Wireless

3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise,

band and channels, and wireless client devices capabilities

3.3.b Describe AP modes and antenna types

3.3.c Describe access point discovery and join process (discovery algorithms, WLC

selection process)

3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming

3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues

3.4 IP Services

3.4.a Describe Network Time Protocol (NTP)

3.4.b Configure and verify NAT/PAT

3.4.c Configure first hop redundancy protocols, such as HSRP and VRRP

3.4.d Describe multicast protocols, such as PIM

and IGMP v2/v3

1. 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

2. 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.

3. 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)

4. 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

5. 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

6. 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+

7. Which of the following features creates a Rapid PVST+ Edge Port?
A. PortFast
B. UplinkFast
C. BackboneFast
D. BPDUGuard

8. 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

9. What is the default Priority value used by HSRP?
A. 3
B. 10
C. 100
D. 255

10. An IPv6 multicast address always begins with which Hexadecimal digits?
A. FF
B. FE80
C. F001
D. EE

11. What parameter exchanged in VTP advertisements determines how authoritative a VTP update is?
A. Configuration Register
B. Metric
C. Distance
D. Configuration Revision Number

12. 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

13. 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

14. 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

15. 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

16. 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

17. 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.

18. 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.

19. 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

20. 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

21. 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

22. 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.

23. 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

24. 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.

25. 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

26. 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

27. 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)

28. 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

29. 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

30. 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

31. 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

32. 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.

33. Which if the following is NOT a Rapid PVST+ port state?
A. Discarding
B. Listening
C. Learning
D. Forwarding

34. 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.

35. 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

36. 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.

37. 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

38. 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.

39. 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.

40. 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.

41. 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).

42. 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

43. 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

44. 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

45. 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

Chapter 3: Answers

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

B. Lightweight

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.

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

B. The global routing table does not contain routes seen in the routing table of any VRF instance.

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.

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

B. Routing Locator (RLOC)

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.

4. 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?

C. SW1: Dynamic Auto – SW2: Dynamic Auto

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.

5. 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?

B. The last 3 bits of the destination MAC address.

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.

6. 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?

C. MSTP

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.

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

A. PortFast

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.

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

D. overload

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.”

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

C. 100

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.

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

A. FF

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.

11. What parameter exchanged in VTP advertisements determines how

authoritative a VTP update is?

D. Configuration Revision Number

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.

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

D. 224.0.0.6

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.

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

C. Passive Interface

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.

14. 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

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.

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

C. router ospfv3 1

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.

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

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

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.”

17. 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.

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.

18. 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?

D. The IPv6 neighbor needs to be activated.

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.

19. 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?

D. Monitor Mode

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.

20. 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?

C. Config Download State

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.

21. 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?

B. Inside Global Address

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.

22. When configuring Dynamic NAT, what is the "pool" parameter used to specify?

C. The range of Inside Global addresses into which Inside Local addresses are mapped.

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.

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

C. UDP port 123

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.

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

D. VRRP can used an interface's IP address as a Virtual IP address.

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.

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

C. ntp authenticate

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.

26. 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

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.

27. 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?

D. Nonstop Forwarding (NSF)

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.

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

C. RSS

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.

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

C. Process Switching

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.

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

D. Native VLAN

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.

31. 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?

D. SW1: Auto – SW2: Desirable

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.

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

B. MST0

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.

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

B. Listening

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.

34. 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.

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.

35. What metric components does EIGRP use by default?

B. Bandwidth and Delay

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.

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

B. HDLC

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.

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

D. Distribute List

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.

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

C. ipv6 unicast-routing

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.

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

B. A neighbor's IP address must be statically configured.

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.

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

C. When configuring an iBGP neighbor, the "neighbor" command uses the "local-as" parameter instead of the "remote-as" parameter.

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.

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

B. You need to apply a route map to your IPv6 neighbor specifying the next-hop IPv6 address.

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.

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

B. Cycle

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.

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

A. Dipole Antenna

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.

44. 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?

B. Layer 3

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.

45. 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?

B. Router(config-if)# ip nat inside

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.

Chapter 4: Network Assurance

The objectives covered in this chapter:

10% 4.0 Network Assurance

4.1 Diagnose network problems using tools such as debugs, conditional debugs, trace route, ping, SNMP, and syslog

4.2 Configure and verify device monitoring using syslog for remote logging

Cisco Systems, Inc. This document is Cisco Page

4.3 Configure and verify NetFlow and Flexible NetFlow

4.4 Configure and verify SPAN/RSPAN/ERSPAN

4.5 Configure and verify IPSLA

4.6 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management

4.7 Configure and verify NETCONF and RESTCONF

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

2. 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

3. 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

4. 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

5. 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

6. Which type of Switched Port Analyzer (SPAN) configuration uses Generic

Routing Encapsulation (GRE) for traffic capture?
A. SPAN
B. ERSPAN
C. RSPAN
D. GRESPAN

7. 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

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. 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

17. By default, which type of traffic does SPAN monitor in Cisco IOS?
A. Received
B. Transmitted
C. Transmitted and Received
D. Local

18. 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

19. 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

20. What HTTP verb is used by REST create (not update) a new configuration?
A. GET
B. PUT
C. PATCH
D. POST

21. 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.

Chapter 4: Answers

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

B. Spine-Leaf

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

D. UDP 161

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.

3. 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)?

C. priv

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.

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

B. logging host 10.1.1.5

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.

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

C. NetFlow v9

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.

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

B. ERSPAN

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).

7. 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

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.

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

C. IP SLA Responder

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.

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

D. ip sla responder

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.”

10. 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?

B. event

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.

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

B. no debug all

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.

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

A. ping

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.

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

B. UDP 162

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.

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

A. Level 0

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.

15. 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

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.

16. 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?

D. flow record HELPDESK

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.

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

C. Transmitted and Received

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.

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

C. no shutdown

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.

19. 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

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).

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

D. POST

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.

21. The “5 Nines of Availability” refers to what?

A. Limiting a network’s downtime to no more than 5 minutes per year.

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.

Chapter 5: Security

The objectives covered in this chapter:

20% 5.0 Security

5.1 Configure and verify device access control

5.1.a Lines and password protection

5.1.b Authentication and authorization using AAA

5.2 Configure and verify infrastructure security features

5.2.a ACLs

5.2.b CoPP

5.3 Describe REST API security

5.4 Configure and verify wireless security features

5.4.a EAP

5.4.b WebAuth

5.4.c PSK

5.5 Describe the components of network security design

5.5.a Threat defense

5.5.b Endpoint security

5.5.c Next-generation firewall

5.5.d TrustSec, MACsec

5.5.e Network access control with 802.1X, MAB,

and WebAuth

1. 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

2. Which of the following is considered to be a standard numbered access control list (ACL)?
A. 100
B. 1300
C. 199
D. 2000

3. 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

4. Which Cisco line type is used for controlling inbound Telnet connections?
A. CTY
B. AUX
C. VTY
D. CDP

5. Which native extensible authentication protocol (EAP) type uses certificates for mutual authentication?
A. EAP-TLS
B. EAP-MD5
C. EAP-SSL
D. EAP-MSCHAPv2

6. Which encryption standard is leveraged by WPA2 and WPA3 for more advanced encryption and protection?
A. SSL

B. TKIP
C. AES
D. SHA

7. 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

8. 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

9. 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

10. Northbound Interfaces (NBIs) are what type of Application Programing Interfaces (APIs)?
A. YANG
B. OpenFlow
C. REST
D. JSON

11. 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

12. 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

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

14. Which AAA protocol used for external server deployments encrypts only the password field of the communication?
A. RADIUS
B. TACACS+
C. SNMP
D. Telnet

15. 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

16. 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

17. 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

18. 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

19. 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

20. 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

21. 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

Chapter 5: Answers

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

A. sha

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.

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

B. 1300

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.

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

B. Extended ACL

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.

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

C. VTY

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.

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

A. EAP-TLS

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.

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

C. AES

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.

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

C. Compliance

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.

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

B. MACsec

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.

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

D. Authenticator

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.

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

C. REST

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.

11. 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

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.

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

C. 400

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.

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

C. An ISAKMP tunnel

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

A. RADIUS

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.

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

D. Extended ACLs

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.

16. 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)?

C. Central WebAuth

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.

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

D. Cisco Smart Install

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.

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

A. Zero-touch deployment

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.

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

A. MACsec

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.

20. 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)?

C. 90 seconds

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.

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

D. 401

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.

Chapter 6: Automation

The objectives covered in this chapter:

15% 6.0 Automation

6.1 Interpret basic Python components and scripts

6.2 Construct valid JSON encoded file

6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG

6.4 Describe APIs for Cisco DNA Center and vManage

6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF

6.6 Construct EEM applet to automate configuration, troubleshooting, or data collection

6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

1. 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.

2. 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

3. 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

4. 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]

5. Which section of the Cisco DNA Center management dashboard contains troubleshooting tools for the network?
A. Design
B. Assurance
C. Policy
D. Provision

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

7. 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?)

8. NETCONF supports what type of data formatting?
A. XML
B. JSON
C. HTTP
D. HTTPS

9. Which Chef orchestration component pulls configuration information from the central Chef server?
A. Request Agent
B. Pull Drone
C. Workstation
D. Client Node

10. 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

11. Which section of the Cisco DNA Center management dashboard contains troubleshooting tools for the network?
A. Design
B. Assurance
C. Policy
D. Provision

12. 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

13. Which XML component gives more detail about an element and must appear in quotes?
A. Attribute
B. Comment
C. Declaration
D. Tag

14. Identify the YANG Data Modeling element that represents an attribute of something being modeled.
A. Container
B. List
C. Leaf
D. Type

15. Identify the data type of the following: True.
A. String
B. Floating Point
C. Boolean
D. Integer

16. 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)

17. 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

18. 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

19. 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”)

20. Which component of the Ansible orchestration tool is written in YAML for execution on managed devices?
A. Inventory
B. Playbook
C. Recipe
D. API

21. 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

22. 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

Chapter 6: Answers

1. Which of the following best describe the “Object” JSON data structure?

B. An unordered set of name/value pairs enclosed in curly brackets.

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.

2. 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?

C. python3.8

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."

3. 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?

D. IDLE

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.

4. 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])

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]).

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

B. Assurance

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.

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

D. An unordered set of name/value pairs enclosed in curly brackets.

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.

7. 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? ")

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.

8. NETCONF supports what type of data formatting?

A. XML

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

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

D. Client Node

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.

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

B. Catalog

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.

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

B. Assurance

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.

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

D. Applets

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.

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

A. Attribute

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.

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

C. Leaf

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.

15. Identify the data type of the following: True.

C. Boolean

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.

16. 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?

C. x=str(x)

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.

17. 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?

B. elif

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.

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

C. FOR and WHILE

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.

19. 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?

D. file=open(“vlans.txt”,”a”)

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.

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

B. Playbook

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.

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

C. Grains

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.

22. 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

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.