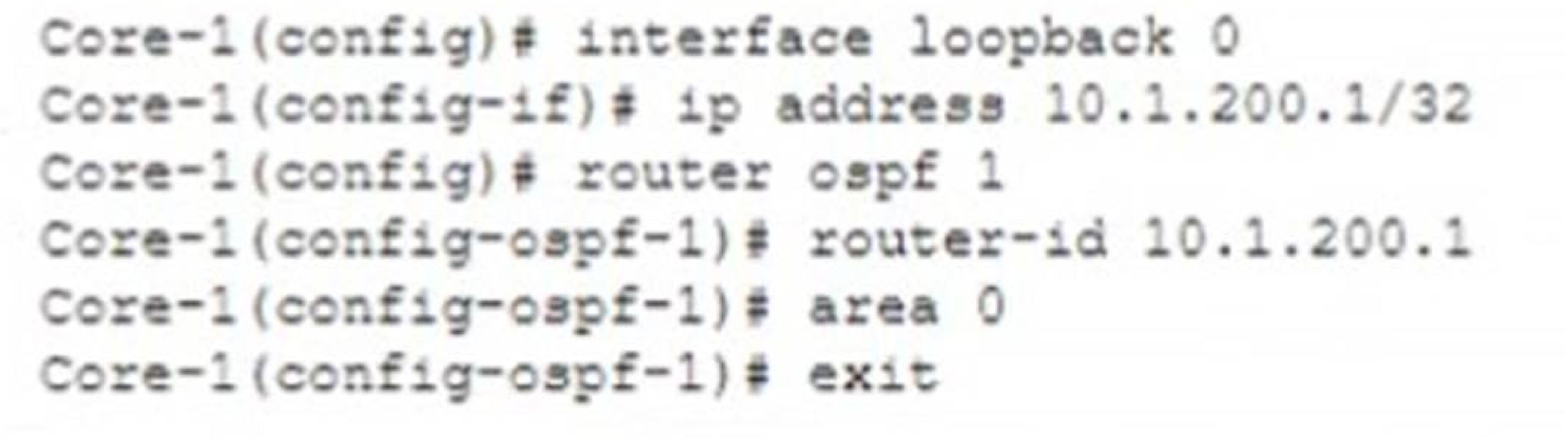
Exam Questions HPE6-A85

Aruba Certified Campus Access Associate Exam

https://www.2passeasy.com/dumps/HPE6-A85/

NEW QUESTION 1

Review the configuration below.



```
Core-1(config)# interface loopback 0
Core-1(config-if)# ip address 10.1.200.1/32
Core-1(config)# router ospf 1
Core-1(config-ospf-1)# router-id 10.1.200.1
Core-1(config-ospf-1)# area 0
Core-1(config-ospf-1)# exit
```

Why would you configure OSPF to use the IP address 10.1.200.1 as the router ID?

A. The IP address associated with the loopback interface is non-routable and preventsloops
B. The loopback interface state is dependent on the management interface state and reduces routing updates.
C. The IP address associated with the loopback interface is routable and prevents loops
D. The loopback interface state Is independent of any physical interface and reduces routing updates.

Answer: D

Explanation:

The reason why you would configure OSPF Open Shortest Path First (OSPF) is a link-state routing protocol that dynamically calculates the best routes for data transmission within an IP network. OSPF uses a hierarchical structure that divides a network into areas and assigns each router an identifier called router ID (RID). OSPF uses hello packets to discover neighbors and exchange routing information. OSPF uses Dijkstra??s algorithm to compute the shortest path tree (SPT) based on link costs and build a routing table based on SPT. OSPF supports multiple equal-cost paths, load balancing, authentication, and various network types such as broadcast, point-to-point, point-to- multipoint, non-broadcast multi-access (NBMA), etc. OSPF is defined in RFC 2328 for IPv4 and RFC 5340 for IPv6. to use the IP address IP address Internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing. There are two versions of IP addresses: IPv4 and IPv6. IPv4 addresses are 32 bits long and written in dotted-decimal notation, such as 192.168.1.1. IPv6 addresses are 128 bits long and written in hexadecimal notation, such as 2001:db8::1. IP addresses can be either static (fixed) or dynamic (assigned by a DHCP server). 10.1.200.1 as the router ID Router ID (RID) Router ID (RID) is a unique identifier assigned to each router in a routing domain or protocol. RIDs are used by routing protocols such as OSPF, IS-IS, EIGRP, BGP, etc., to identify neighbors, exchange routing information, elect designated routers (DRs), etc. RIDs are usually derived from one of the IP addresses configured on the router??s interfaces or loopbacks, or manually specified by network administrators. RIDs must be unique within a routing domain or protocol instance. is that the loopback interface state Loopback interface Loopback interface is a virtual interface on a router that does not correspond to any physical port or connection. Loopback interfaces are used for various purposes such as testing network connectivity, providing stable router IDs for routing protocols, providing management access to routers, etc. Loopback interfaces have some advantages over physical interfaces such as being always up unless administratively shut down, being independent of any hardware failures or link failures, being able to assign any IP address regardless of subnetting constraints, etc. Loopback interfaces are usually numbered from zero (e.g., loopback0) upwards on routers. Loopback interfaces can also be created on PCs or servers for testing or configuration purposes using special IP addresses reserved for loopback testing (e.g., 127.x.x.x for IPv4 or ::1 for IPv6). Loopback interfaces are also known as virtual interfaces or dummy interfaces . Loopback interface state Loopback interface state refers to whether a loopback interface is up or down on a router . A loopback interface state can be either administratively controlled (by using commands such as no shutdown or shutdown) or automatically determined by routing protocols (by using commands such as passive-interface or ip ospf network point-to-point). A loopback interface state affects how routing protocols use the IP address assigned to the loopback interface for neighbor discovery , router ID selection , route advertisement , etc . A loopback interface state can also affect how other devices can access or ping the loopback interface . A loopback interface state can be checked by using commands such as show ip interfacebrief or show ip ospf neighbor . is independent of any physical interface and reduces routing updates.

The loopback interface state is independent of any physical interface because it does not depend on any hardware or link status. This means that the loopback interface state will always be up unless it is manually shut down by an administrator. This also means that the loopback interface state will not change due to any physical failures or link failures that may affect other interfaces on the router.

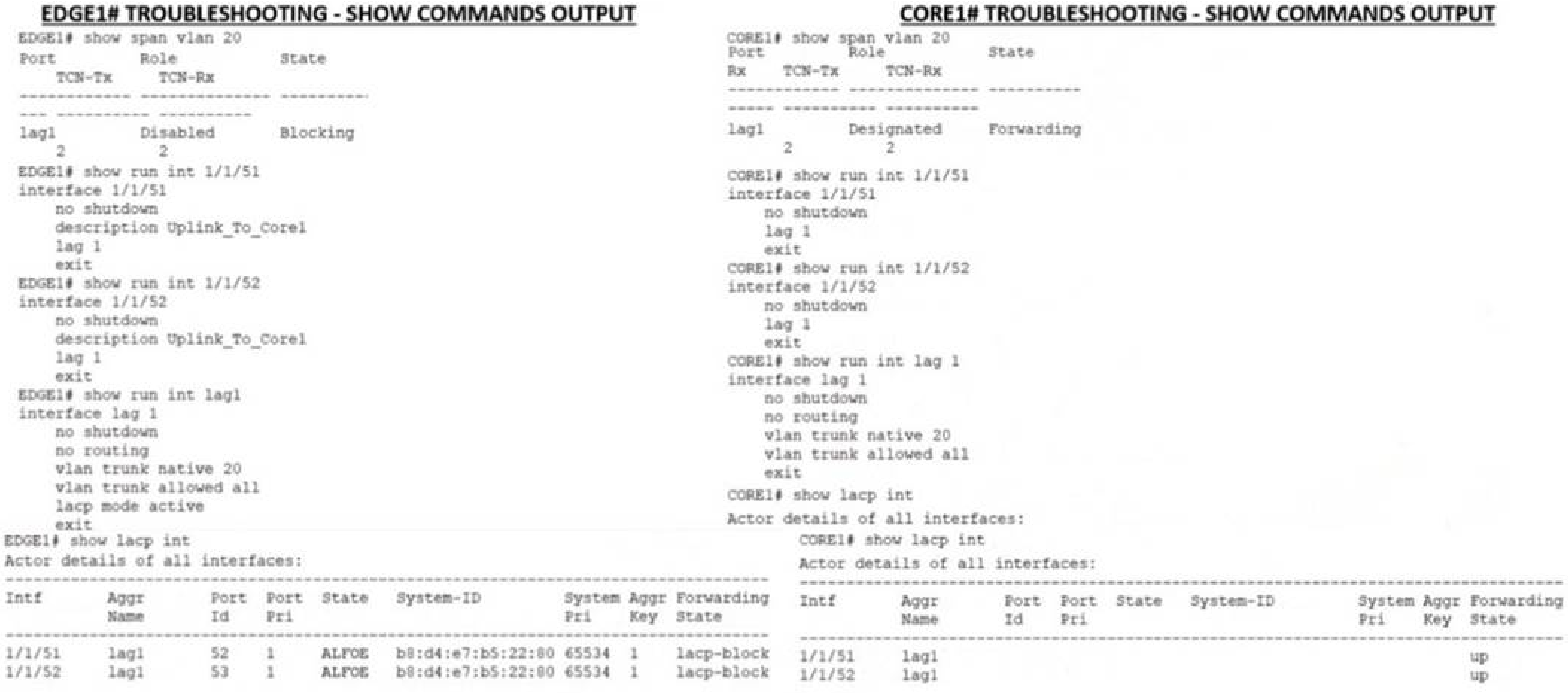
The loopback interface state reduces routing updates because it provides a stable router ID for OSPF that does not change due to any physical failures or link failures that may affect other interfaces on the router. This means that OSPF will not have to re-elect DRs Designated Routers (DRs) Designated Routers (DRs) are routers that are elected by OSPF routers in a broadcast or non-broadcast multi-access (NBMA) network to act as leaders and coordinators of OSPF operations in that network. DRs are responsible for generating link-state advertisements (LSAs) for the entire network segment, maintaining adjacencies with all other routers in the segment, and exchanging routing information with other DRs in different segments through backup designated routers (BDRs). DRs are elected based on their router priority values and router IDs . The highest priority router becomes the DR and the second highest priority router becomes the BDR . If there is a tie in priority values , then the highest router ID wins . DRs can be manually configured by setting the router priority value to 0 (which means ineligible) or 255 (which means always eligible) on specific interfaces . DRs can also be influenced by using commands such as ip ospf priority , ip ospf dr-delay , ip ospf network point-to-multipoint , etc . DRs can be verified by using commands such as show ip ospf neighbor , show ip ospf interface , show ip ospf database , etc . , recalculate SPT Shortest Path Tree (SPT) Shortest Path Tree (SPT) is a data structure that represents the shortest paths from a source node to all other nodes in a graph or network . SPT is used by link-state routing protocols such as OSPF and IS-IS to compute optimal routes based on link costs . SPT is built using Dijkstra??s algorithm , which starts from the source node and iteratively adds nodes with the lowest cost paths to the tree until all nodes are included . SPT can be represented by a set of pointers from each node to its parent node in the tree , or by a set of next-hop addresses from each node to its destination node in the network . SPT can be updated by adding or removing nodes or links , or by changing link costs . SPT can be verified by using commands such as show ip route , show ip ospf database , show clns route , show clns database , etc . , or send LSAs Link- State Advertisements (LSAs) Link-State Advertisements (LSAs) are packets that contain information about the state and cost of links in a network segment . LSAs are generated and flooded by link-state routing protocols such as OSPF and IS-IS to exchange routing information with other routers in the same area or level . LSAs are used to build link-state databases (LSDBs) on each router , which store the complete topology of the network segment . LSAs are also used to compute shortest path trees (SPTs) on each router , which determine the optimal routes to all destinations in the network . LSAs have different types depending on their origin and scope , such as router LSAs , network LSAs , summary LSAs , external LSAs , etc . LSAs have different formats depending ontheir type and protocol version , but they usually contain fields such as LSA header , LSA type , LSA length , LSA age , LSA sequence number , LSA checksum , LSA body , etc . LSAs can be verified by using commands such as show ip ospf database , show clns database , debug ip ospf hello , debug clns hello , etc . due to changes in router IDs.

The other options are not reasons because:

? The IP address associated with the loopback interface is non-routable and prevents loops: This option is false because the IP address associated with the

loopback interface is routable and does not prevent loops. The IP address associated with the loopback interface can be any valid IP address that belongs to an existing subnet or a new subnet created specifically for loopbacks. The IP address associated with the loopback interface does not prevent loops because loops are caused by misconfigurations or failures in routing protocols or devices, not by IP addresses.
? The loopback interface state is dependent on the management interface state and reduces routing updates: This option is false because
the loopback interface state is independent of any physical interface state, including the management interface state Management interface Management interface is an interface on a device that provides access to management functions such as configuration, monitoring, troubleshooting, etc . Management interfaces can be physical ports such as console ports, Ethernet ports, USB ports, etc., or virtual ports such as Telnet sessions, SSH sessions, web sessions, etc . Management interfaces can use different protocols such as CLI Command-Line Interface (CLI) Command-Line Interface (CLI) is an interactive text- based user interface that allows users to communicate with devices using commands typed on a keyboard . CLI is one of the methods for accessing management functions on devices such as routers, switches, firewalls, servers, etc . CLI can use different protocols such as console port serial communication protocol Serial communication protocol Serial communication protocol is a method of transmitting data between devices using serial ports and cables . Serial communication protocol uses binary signals that represent bits (0s and 1s) and sends them one after another over a single wire . Serial communication protocol has advantages such as simplicity, low cost, long

NEW QUESTION 2
You put in a few show commands on switches EDGE1 and CORE1 to attempt to gather information to troubleshoot the issue Use the show command output images to determine the reason for the EDGE1 uplink being down



EDGE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT

```
EDGE1# show span vlan 20
Port          Role            State
    TCN-Tx      TCN-Rx
------------ -------------- ----------
--- ---------- ----------
lag1          Disabled        Blocking
    2           2
EDGE1# show run int 1/1/51
interface 1/1/51
    no shutdown
    description Uplink_To_Core1
    lag 1
    exit
EDGE1# show run int 1/1/52
interface 1/1/52
    no shutdown
    description Uplink_To_Core1
    lag 1
    exit
EDGE1# show run int lag1
interface lag 1
    no shutdown
    no routing
    vlan trunk native 20
    vlan trunk allowed all
    lacp mode active
    exit
EDGE1# show lacp int
Actor details of all interfaces:
----------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID          System Aggr Forwarding
           Name       Id    Pri                              Pri    Key  State
----------------------------------------------------------------------------------
1/1/51     lag1       52    1     ALFOE   b8:d4:e7:b5:22:80 65534  1    lacp-block
1/1/52     lag1       53    1     ALFOE   b8:d4:e7:b5:22:80 65534  1    lacp-block
```

CORE1# TROUBLESHOOTING - SHOW COMMANDS OUTPUT

```
CORE1# show span vlan 20
Port          Role            State
Rx    TCN-Tx     TCN-Rx
------------ -------------- ----------
----- ---------- ----------
lag1          Designated      Forwarding
      2          2
CORE1# show run int 1/1/51
interface 1/1/51
    no shutdown
    lag 1
    exit
CORE1# show run int 1/1/52
interface 1/1/52
    no shutdown
    lag 1
    exit
CORE1# show run int lag 1
interface lag 1
    no shutdown
    no routing
    vlan trunk native 20
    vlan trunk allowed all
    exit
CORE1# show lacp int
Actor details of all interfaces:
        CORE1# show lacp int
        Actor details of all interfaces:
        ----------------------------------------------------------------------------------
        Intf       Aggr       Port  Port  State   System-ID          System Aggr Forwarding
                   Name       Id    Pri                              Pri    Key  State
        ----------------------------------------------------------------------------------
        1/1/51     lag1                                                          up
        1/1/52     lag1                                                          up
```

A. The physical interfaces are not members of the correct LAG.
B. Spanning-Tree block state is preventing the Core uplink from having connectivity to the edge
C. The Core is connected to the incorrect physical interlaces
D. LACP is not configured on the Core uplink

Answer: D

Explanation:
LACP is a protocol that allows multiple physical links to be aggregated into a single logical link for increased bandwidth and redundancy. LACP must be configured on both ends of the link for it to work properly. In this case, EDGE1 has LACP configured on its uplink port-channel 1, but CORE1 does not have LACP configured on its corresponding port-channel 1. This causes a mismatch and prevents the link from coming up.
References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/lacp.htm

NEW QUESTION 3
Which part of the WPA Key Hierarchy is used to encrypt and/or decrypt data"

A. Pairwise Temporal Key (PTK)
B. Pairwise Master Key (PMK)
C. Key Confirmation Key (KCK)
D. number used once (nonce)

Answer: A

Explanation:
The part of WPA Key Hierarchy that is used to encrypt and/or decrypt data is Pairwise Temporal Key (PTK). PTK is a key that is derived from PMK Pairwise Master Key (PMK) is a key that is derived from PSK Pre-shared Key (PSK) is a key that is shared between two parties before communication begins , ANonce Authenticator Nonce (ANonce) is a random number generated by an authenticator (a device that controls access to network resources, such as an AP) , SNonce Supplicant Nonce (SNonce) is a randomnumber generated by supplicant (a device that wants to access network resources, such as an STA) , AA Authenticator Address (AA) is MAC address of authenticator , SA Supplicant Address (SA) is MAC address of supplicant using Pseudo-Random Function (PRF). PTK consists of four subkeys:
? KCK Key Confirmation Key (KCK) is used for message integrity check
? KEK Key Encryption Key (KEK) is used for encryption key distribution
? TK Temporal Key (TK) is used for data encryption
? MIC Message Integrity Code (MIC) key
The subkey that is specifically used for data encryption is TK Temporal Key (TK). TK is also known as Pairwise Transient Key (PTK). TK changes periodically

during communication based on time or number of packets transmitted.
The other options are not part of WPA Key Hierarchy because:
? PMK: PMK is not part of WPA Key Hierarchy, but rather an input for deriving PTK.
? KCK: KCK is part of WPA Key Hierarchy, but it is not used for data encryption, but rather for message integrity check.
? Nonce: Nonce is not part of WPA Key Hierarchy, but rather an input for deriving PTK.
References: https://en.wikipedia.org/wiki/Wi- Fi_Protected_Access#WPA_key_hierarchy_and_management https://www.cwnp.com/wp-content/uploads/pdf/WPA2.pdf

NEW QUESTION 4
What is an advantage of using Layer 2 MAC authentication?

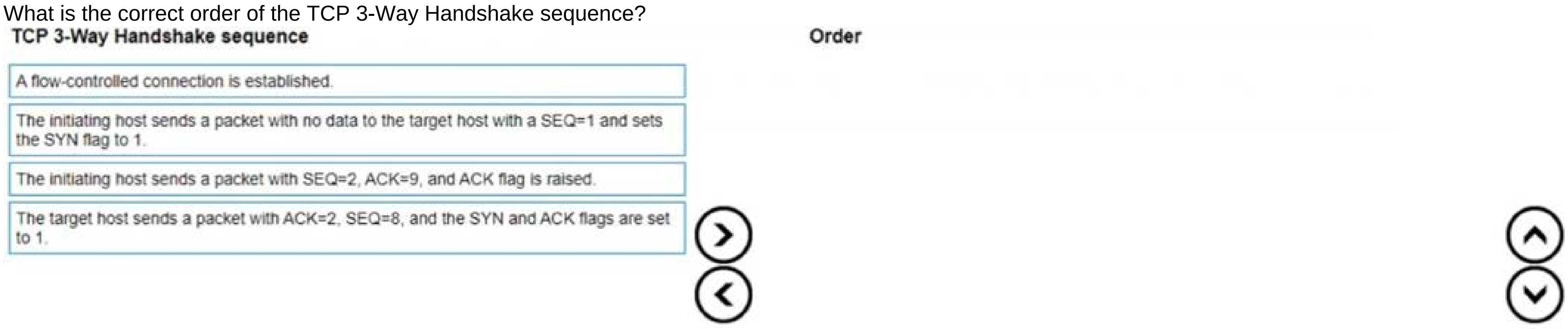
A. it matches user names to MAC address
B. No setup is required on the client
C. MAC allow lists are easily maintained over time
D. MAC identifiers are hard to spoof

Answer: B

Explanation:

Layer 2 MAC authentication is a method of authenticating devices based on their MAC addresses without requiring any client-side configuration or credentials. The switch sends the MAC address of the device to an authentication server such as ClearPass or RADIUS, which checks if the MAC address is authorized to access the network. If yes, the switch grants access to the device based on the assigned role and policies. If no, the switch denies access or redirects the device to a captive portal for further authentication. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/mac-authentication.htm

NEW QUESTION 5
DRAG DROP
What is the correct order of the TCP 3-Way Handshake sequence?



TCP 3-Way Handshake sequence

A flow-controlled connection is established.

The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.

The initiating host sends a packet with SEQ=2, ACK=9, and ACK flag is raised.

The target host sends a packet with ACK=2, SEQ=8, and the SYN and ACK flags are set to 1.

Order

A. Mastered
B. Not Mastered

Answer: A

Explanation:
TCP 3-Way Handshake sequence is:
? Step 1: The initiating host sends a packet with no data to the target host with a SEQ=1 and sets the SYN flag to 1.
? Step 2: The target host responds with a packet with ACK=2, SEQ=8, and the SYN and ACK flags set to 1.
? Step 3: The initiating host sends a packet with SEQ=2, ACK=9, and the ACK flag set to 1.
? Step 4: A normal-controlled connection is established. References: https://en.wikipedia.org/wiki/Transmission_Control_Protocol https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788- 3.html

NEW QUESTION 6
What does a slow amber-flashing Stack-LED indicate?

A. One switch has a stacking failure.
B. A port has a stacking failure Stacking mode Is not selected
C. Stacking mode selected
D. Stacking is synchronizing Please wait

Answer: C

Explanation:
A slow amber-flashing Stack-LED indicates that stacking mode is selected on the switch. This means that the switch is ready to join a stack or form a new stack if no other switches are present. References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/1-overview/stacking-leds.htm

NEW QUESTION 7
You have been asked to onboard a new Aruba 6300M in a customer deployment You are working remotely rather than on-site You have a colleague installing the switch The colleague has provided you with a remote console session to configure the edge switch You have been asked to configure a link aggregation going back to the cores using interfaces 1/1/51 and 1/1/52 The Senior Engineer of the project has asked you to configure the switch and 1Q uplink with these guidelines
* 1. Add VLAN 20 to the local VLAN database with name Mgmt
* 2. Add L3 SVI on VLAN 20 for Management using address 10 in the 10.1.1 0/24 subnet 3. Add LAG 1 using LACP mode active for the uplink
* 4 use vlan 20 as the native vlan on the LAG 5. Make sure the interfaces are all ON. Which configuration script will achieve the task?

A. Edge1# conf t vlan 20 name Mgmt interface vlan 20 ip address 10.1.1.10/24 no shut interface lag 1 shut vlan access 20 lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut
B. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1.1 10/24 no shut interface 1/1/51.1/1/52 shut vlan trunk native 20 vlan trunk allowed all lag 1 lacpmode active interface 1/1/51.1/1/52 no shut
C. Edgel# conf t vlan 20 name Mgmt interface vlan 20 ip address 10 1 1 10/24 no shut interface lag 1 shut vlan trunk native 20 vlan trunk allowed all lacp mode active Int 1/1/51.1/1/52 shut no routing lag 1 interface lag 1 no shut interface 1/1/51.1/1/52 no shut
D. conf t vlan 20 name Mgmt ip address 10 1 1.10/24 no shut interface lag 1 shut vlan trunk native 1 vlan trunk allowed all lacp mode active int 1/1/51.1/1/52 shut no routing interface lag 1 no shut interface 1/1/51.1/1/52 no shut

Answer: C

Explanation:
This configuration script will achieve the task as it follows the guidelines given by the Senior Engineer. It creates VLAN 20 with name Mgmt, adds L3 SVI on VLAN 20 with IP address 10.1.1.10/24, creates LAG 1 with LACP mode active for the uplink, uses VLAN 20 as the native VLAN on the LAG, and ensures that the interfaces are all ON. References:https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6790/GUID-8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

NEW QUESTION 8
What is the recommended VSF topology? (Select two.)

A. Star
B. Daisy chain plus MAD
C. Full mesh
D. Full mesh plus MAD
E. Ring

Answer: BE

Explanation:
Only: Daisy chain plus MAD and ring are the recommended VSF topologies for Aruba switches. They provide high availability and redundancy for the VSF stack. MAD (Multiple Active Detection) is a mechanism to detect and resolve split-brain scenarios in a VSF stack.
References:https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200- 6790/GUID-D6EF042E-EEEF-49F7-B67E-4CAC41CCB24D.html

NEW QUESTION 9
What is the ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack?

A. Aruba CX 6400
B. Aruba CX 6200
C. Aruba CX 6300
D. Aruba CX 6000

Answer: B

Explanation:
The ideal Aruba access switch for a cost-effective connection to 200-380 clients, printers and APs per distribution rack is the Aruba CX 6200. This switch series is a cloud- manageable, stackable access switch series that is ideal for enterprise branch offices and campus networks, as well as SMBs. The CX 6200 series offers the following benefits:
? Enterprise-class connectivity: The CX 6200 series supports ACLs, robust QoS,
and common protocols such as static and Access OSPF routing.
? Power and speed for users and IoT: The CX 6200 series provides built-in 1/10GbE uplinks and 30W to 60W of Class 4 to Class 6 PoE for powering devices such as APs and cameras.
? Scalable growth made simple: The CX 6200 series supports Aruba Virtual Switching Framework (VSF) that allows you to quickly grow your network to eight members in a single stack using high-performance built-in 10G SFP ports.
? Management flexibility: The CX 6200 series supports a choice of management, including cloud-based and on-prem Central, CLI, switch Web GUI and programmability with AOS-CX operating system, and REST APIs.
The other options are not ideal because:
? Aruba CX 6400: This switch series is a high-availability modular switch series that is ideal for versatile edge access to data center deployments. It offers more performance, scalability, and modularity than the CX 6200 series, but it is also more expensive and complex to deploy and manage. It may not be cost-effective for connecting 200-380 clients per distribution rack.
? Aruba CX 6300: This switch series is a layer 3 stackable access and aggregation switch series that offers Smart Rate and High Power PoE. It offers more features and performance than the CX 6200 series, but it is also more expensive and may not be necessary for connecting 200-380 clients per distribution rack.
? Aruba CX 6000: This switch series is a layer 2 access switch series that offers PoE. It offers less features and performance than the CX 6200 series, and it does not support VSF stacking or routing protocols. It may not be sufficient for connecting 200-380 clients per distribution rack.
References: https://www.arubanetworks.com/products/switches/access/ https://www.arubanetworks.com/products/switches/access/6200-series/ https://www.arubanetworks.com/products/switches/access/6400-series/ https://www.arubanetworks.com/products/switches/access/6300-series/ https://www.arubanetworks.com/products/switches/access/6000-series/

NEW QUESTION 10
You are in a meeting with a customer where you are asked to explain the network redundancy feature Multiple Spanning Tree (MSTP). What is the correct statement for this feature?

A. MSTP configuration ID revision by default as current MSTP root priority
B. MSTP configuration ID name by default using switch IMC address
C. MSTP configuration ID name by default using switch serial number
D. MSTP configuration ID revision by default as switch serial number

Answer: B

Explanation:
MSTP Multiple Spanning Tree Protocol. MSTP is an IEEE standard protocol for preventing loops in a network with multiple VLANs. MSTP allows multiple VLANs

to be mapped to a reduced number of spanning-tree instances. configuration ID consists of two parameters: name and revision. The name is a 32-byte ASCII string that identifies the MSTP region, which is a group of switches that share the same configuration ID and VLAN- to-instance mapping. The revision is a 16-bit number that indicates the version of the configuration ID. By default, the MSTP configuration ID name is set to the switch IMC address, which is a unique identifier derived from the MAC address Media Access Control address. MAC address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. of the switch.
References:https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/ar ubaos-solutions/mstp/mstp.htm

NEW QUESTION 10
What is the correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1?

A. ip-route 10.2.10.0/24 172.16.1.1
B. ip route 10.2.10.0.255.255.255.0 172.16.1.1 description aruba
C. ip route 10.2.10.0/24.172.16.11
D. ip route-static 10.2 10.0.255.255.255.0 172.16.1.1

Answer: A

Explanation:
The correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1 is ip-route 10.2.10.0/24 172.16.1.1 . This command specifies the destination network address (10.2.10.0) and prefix length (/24) and the next-hop address
(172.16.1 .1) for reaching that network from the switch. The other commands are either incorrect syntax or incorrect parameters for adding a static route.
References:https://www.arubanetworks.com/techdocs/AOS- CX_10_04/NOSCG/Content/cx-noscg/ip-routing/static-routes.htm

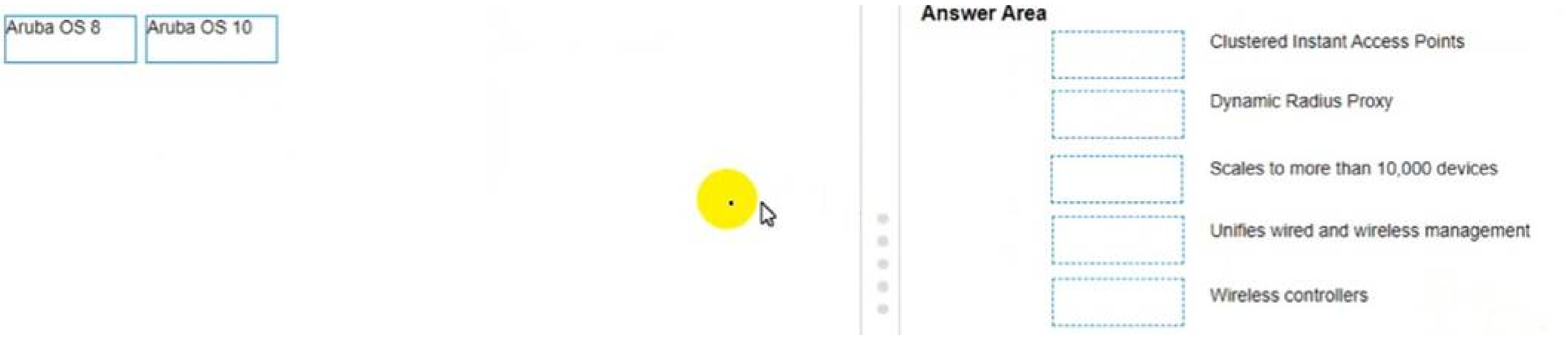
NEW QUESTION 15
What are the main characteristics of the 6 GHz band?

A. Less RF signal is absorb by objects in a 6 GHz WLAN.
B. In North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the 5 GHz band.
C. The 6 GHz band is fully backward compatible with the existing bands.
D. Low Power Devices are allowed for indoor and outdoor usage.

Answer: B

Explanation:
The main characteristic of the 6 GHz band that is true among the given options is that in North America, the 6 GHz band offers more 80 MHz channels than there are 40 MHz channels in the 5 GHz band. This characteristic provides more spectrum availability, less interference, and higher throughput for wireless devices that support Wi-Fi 6E Wi-Fi Enhanced (Wi-Fi 6E) is an extension of Wi-Fi 6 (802.11ax) standard that operates in the newly available unlicensed frequency spectrum around 6 GHz in addition to existing bands below it. Some facts about this characteristic are:
? In North America, there are up to seven non-overlapping channels available in
each of three channel widths (20 MHz, 40 MHz, and 80 MHz) in the entire unlicensed portion of the new spectrum (5925–7125 MHz). This means there are up to 21 non-overlapping channels available for Wi-Fi devices in total.
? In comparison, in North America, there are only nine non-overlapping channels
available in each of two channel widths (20 MHz and 40 MHz) in the entire unlicensed portion of the existing spectrum below it (2400–2483 MHz and 5150–5825 MHz). This means there are only up to nine non-overlapping channels available for Wi-Fi devices in total.
? Therefore, in North America, there are more than twice as many non-overlapping
channels available in each channel width in the new spectrum than in the existing spectrum below it.
? Specifically, there are more than twice as many non-overlapping channels
available at 80 MHz width (seven) than at 40 MHz width (three) in the existing spectrum below it.
The other options are not true because:
? Less RF signal is absorbed by objects in a 6 GHz WLAN: This option is false because higher frequency signals tend to be more absorbed by objects than lower frequency signals due to higher attenuation Attenuation is a general term that refers to any reduction in signal strength during transmission over distance or through an object or medium . Therefore, RF signals in a 6 GHz WLAN would be more absorbed by objects than RF signals in a lower frequency WLAN.
? The 6 GHz band is fully backward compatible with existing bands: This option is false because Wi-Fi devices need to support Wi-Fi 6E standard to operate in the new spectrum around 6 GHz . Existing Wi-Fi devices that do not support Wi-Fi 6Estandard cannot use this spectrum and can only operate in existing bands below it.
? Low Power Devices are allowed for indoor and outdoor usage: This option is false because Low Power Indoor Devices (LPI) are only allowed for indoor usage under certain power limits and registration requirements . Outdoor usage of LPI devices is prohibited by regulatory authorities such as FCC Federal Communications Commission (FCC) is an independent agency of United States government that regulates communications by radio, television, wire, satellite, and cable across United States . However, outdoor usage of Very Low Power Devices (VLP) may be allowed under certain power limits and without registration requirements.
References: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6e https://www.wi-fi.org/file/wi- fi-alliance-spectrum-needs-study
https://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi- fi/prod_white_paper0900aecd807395a9.html
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068- power-levels.html https://www.wi-fi.org/file/wi-fi-alliance-unlicensed-spectrum-in-the-us

NEW QUESTION 20
DRAG DROP
Match the feature to the Aruba OS version (Matches may be used more than once.)



Aruba OS 8 Aruba OS 10

Answer Area

Clustered Instant Access Points

Dynamic Radius Proxy

Scales to more than 10,000 devices

Unifies wired and wireless management

Wireless controllers

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Features: 1) Clustered Instant Access Points Aruba OS version: a) Aruba OS 8
Features: 2) Dynamic Radius Proxy Aruba OS version: a) Aruba OS 8
Features: 3) Scales to more than 10,000 devices Aruba OS version: b) Aruba OS 10 Features: 4) Unifies wired and wireless management Aruba OS version: a) Aruba OS 8 Features: 5) Wireless controllers Aruba OS version: a) Aruba OS 8
ArubaOS is the operating system for all Aruba Mobility Controllers (MCs) and controller- managed wireless access points (APs). ArubaOS 8 delivers unified wired and wireless access, seamless roaming, enterprise grade security, and a highly available network with the required reliability to support high density environments1. Some of the features of
ArubaOS 8 are:
? Clustered Instant Access Points: This feature allows multiple Instant APs to form a cluster and share configuration and state information. This enables seamless roaming, load balancing, and fast failover for clients2.
? Dynamic Radius Proxy: This feature allows an MC to act as a proxy for RADIUS authentication requests from clients or APs. This simplifies the configuration and management of RADIUS servers and reduces the network traffic between MCs and RADIUS servers3.
? Wireless controllers: Aruba wireless controllers are devices that centrally manage and control the wireless network. They provide functions such as AP provisioning, configuration, security, policy enforcement, and network optimization.
ArubaOS 10 is the next-generation operating system that works with Aruba Central, a cloud-based network management platform. ArubaOS 10 delivers greater scalability, security, and AI-powered optimization across large campuses, branches, and remote work environments. Some of the features of ArubaOS 10 are:
? Scales to more than 10,000 devices: ArubaOS 10 can support up to 10,000
devices per cluster, which is ten times more than ArubaOS 8. This enables customers to scale their networks without compromising performance or reliability.
? Unifies wired and wireless management: ArubaOS 10 provides a single platform
for managing both wired and wireless devices across the network. Customers can use Aruba Central to configure, monitor, troubleshoot, and update their devices from anywhere.
Both ArubaOS 8 and ArubaOS 10 share some common features, such as:
? Unifies wired and wireless management: Both operating systems provide unified wired and wireless access for customers who use Aruba switches and APs. Customers can use a single interface to manage their entire network infrastructure1 . References: 1 https://www.arubanetworks.com/resource/arubaos-8-fundamental-
guide/ 2 https://www.arubanetworks.com/techdocs/Instant_86_WebHelp/Content/i nstant-ug/iap-maintenance/cluster.htm 3 https://www.arubanetworks.com/techdocs/ArubaOS_86 _Web_Help/Content/arubaos-solutions/1-overview/dynamic-radius-proxy.htm https://www.arubanetworks.com/products/networking/controllers/ https://www.arubanetworks.com/products/network-management- operations/arubaos/ https://blogs.arubanetworks.com/solutions/making-the-switch/ https://www.arubanetworks.com/products/network-management-operations/aruba- central/

NEW QUESTION 24
After having configured the edge switch uplink as requested your colleague says that they have failed to ping the core You ask your colleague to verify the connection is plugged in and the switch is powered on They confirm that both are correct You attempt to ping the core switch and confirm that the ping is failing. Knowing the nature of this deployment, what commands might you use to troubleshoot this issued

A. Ping 10.11 1 - ping the core to attempt to verify connectivity Show trunk - to verify if the LAG interface was correctly added to the switch Show spanning tree - to check for spanning-tree blocked states Show port-access clients interface all - to view any port- access blocking states or failed authentication attempts on all interfaces Show run interface vlan20 - to double check the layer 3 svi configuration is correct for l_3 connectivity Show lldp neighors - to verify whether you are able to see the Core as an L2 neighbor to verify if the correct links are plugged in to the correct ports
B. diagnostic diag cable-diag 1/1/51 diag cable-diag 1/1/52 - to view diagnostic information for the physical link to get a status on any interruptions to Layer 1 connectivity, show ip route - to verify that the default gateway is present in the routing table show ip ospf - to check whether there is a layer 3 routing protocol enabled show ip dns - to view whether there is a valid dns source
C. Ping 10.1.1.1 - ping the core to attempt to verify connectivity show lacp agg - to verify which link aggregations are currently configured using which physical ports show lacp int - to verify the LACP status and whether any links are blocking in your topology show lldp neighbors - to verify whether you are able to see the Core as an L2 neighbor to verify if the correct links are plugged in to the correct ports show run interface 1/1/51.1/1/52-to ensure the physical interfaces are no-shut and members of the lag show run interface lag 1 - to ensure the correct vlan trunking configuration is applied to the logical interface show run int vlan 20 - to ensure you have the L3 SVI no shut and configured in the correct subnet
D. Show run - to view the running configuration of the switch Show run | begin 20 "vlan 20"- to ensure VLAN 20 was correctly added to the database show run | begin 20 'interface vlan 20' - to view the L3 SVI configuration Show run interface 1/1/51.1/1/52 - to ensure the physical interfaces are no shut and were added as members of LAG 1 Show run int lag 1 - to verify LACP mode active was configured to eliminate LACP blocking states

Answer: C

Explanation:
These commands might help troubleshoot this issue as they check various aspects of the connectivity between the edge switch and the core switch, such as Layer 3 reachability, Layer 2 adjacency, LACP configuration and status, VLAN trunking configuration, and interface status.
References:https://www.arubanetworks.com/techdocs/AOS-CX_10_04/CLI/GUID- 8F0E7E8B-0F4B-4A3C-AE7F-0F1B5A7F9C5D.html

NEW QUESTION 28

……