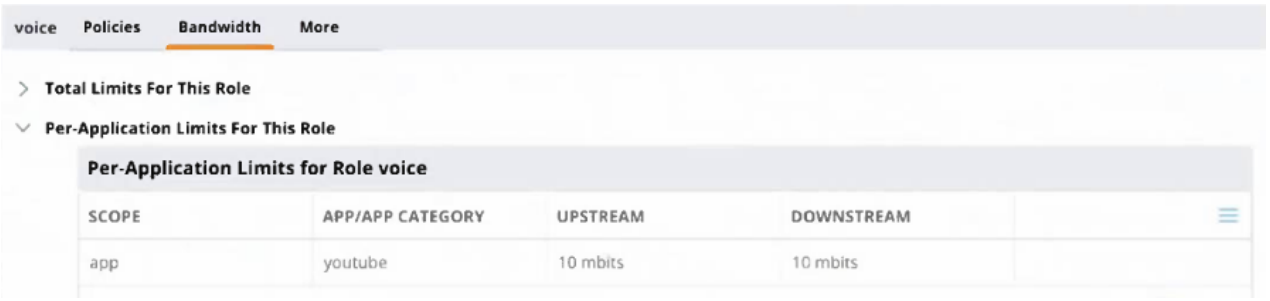
Question #1 *Topic 1*

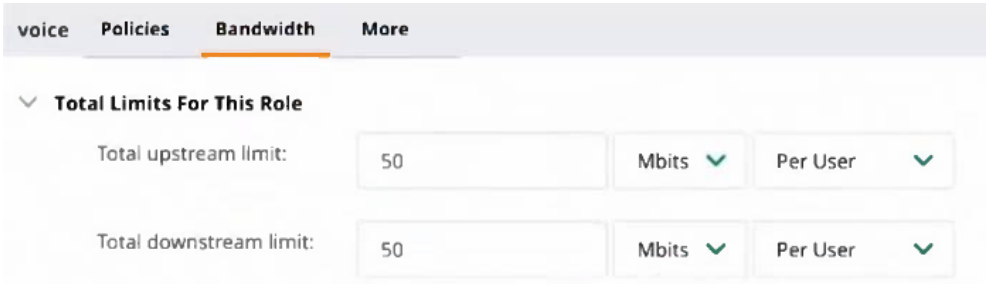
A network administrator accesses HPE Aruba Networking Central and notices that visitors consume too much internet bandwidth, starving employee traffic when accessing an external service. Therefore, the administrator wants to limit wireless bandwidth to 50 Mbps in both directions among all users in the voice role and no more than 10 Mbps in both directions for YouTube traffic. Deep packet inspection, web content classification, and firewall visibility are enabled.

Which configurations are required to accomplish this task? (Choose two.)

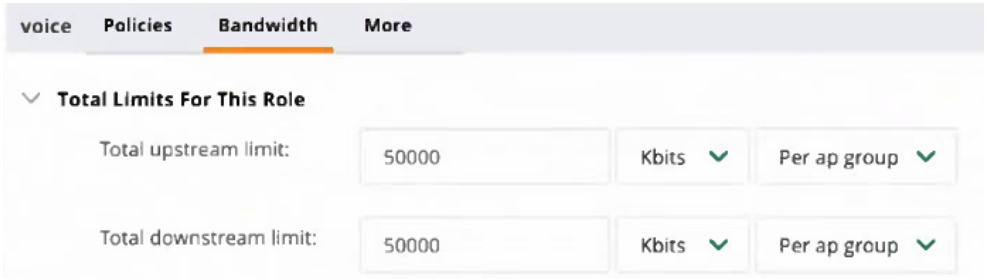
A.



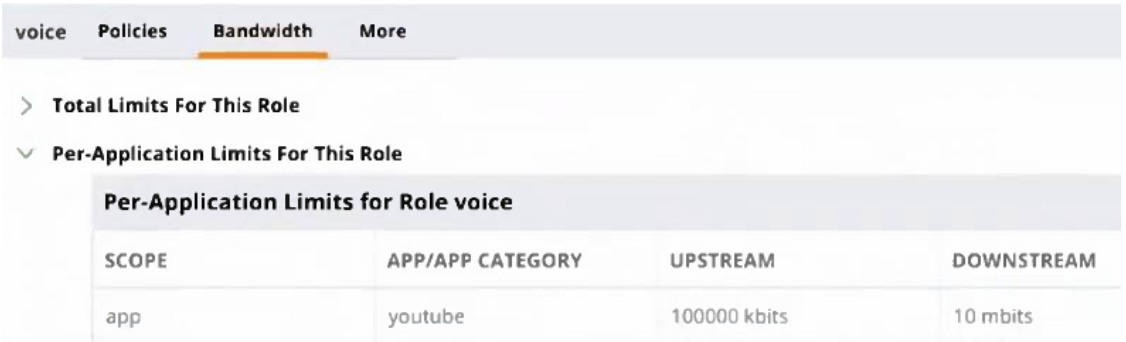
B.



C.



D.



Suggested Answer: *AB*

Community vote distribution

AC (100%)

lowstett 4 months ago

Selected Answer: AC

Question says "Among ALL users", should be C, per AP group not per user.

upvoted 2 times

Question #2 *Topic 1*

You configured a bridged mode SSID with WPA3-Enterprise and EAP-TLS security. When you connect an Active Directory joined client that has valid client certificates, HPE Aruba Networking ClearPass shows the following error:

What is needed to resolve this issue?

A. Modify your ACX-AD authentication source to include the UPN in the search.

B. Recreate the SSID in tunneled mode.

C. Enable authorization in your Authentication Method.

D. Configure ClearPass to trust the client certificate.

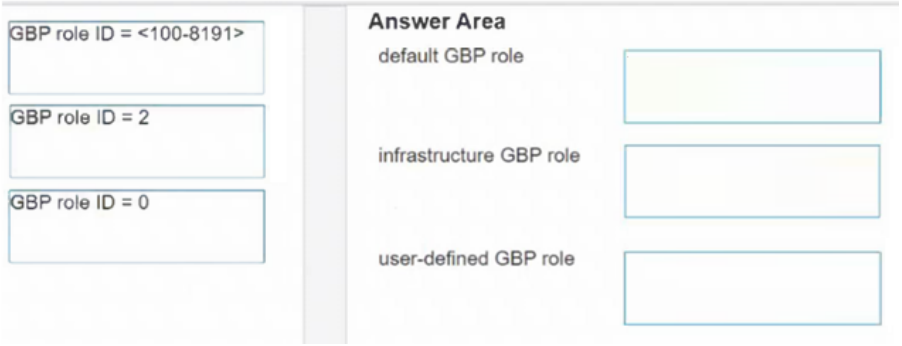
Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

DRAG DROP -

Match each Group Based Policy (GBP) role description to its respective role ID.



Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

A campus topology uses VSX with a collapsed core topology. The customer added redundant SFP+ transceivers and reconfigured their mobility gateways from a single link to an aggregate link. You are asked to verify the CLI output for the link aggregation configuration for one of the mobility gateway cluster members below.

```
interface lag 100 multi-chassis
    no shutdown
    description ArubaGWY_01
    no routing
    vlan trunk native 100
    vlan trunk allowed all
    lacp mode active
    lacp rate fast
```

What is a valid configuration?

A.
```
interface port-channel 0
    description Connected_to_Core
    switchport mode trunk
    trusted vlan 1-4094
!
interface gigabitethernet 0/0/2
    description Core01
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
    lacp group 0 mode active
!
interface gigabitethernet 0/0/3
    description Core02
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
    lacp group 0 mode active
```

B.
```
interface port-channel 0
    description Connected_to_Core
    switchport mode trunk
    trusted
    trusted vlan 100
!
interface gigabitethernet 0/0/2
    description Core01
    lacp group 0 mode active
    lacp timeout short
!
interface gigabitethernet 0/0/3
    description Core02
    lacp group 0 mode active
    lacp timeout short
```

C.
```
interface port-channel 0
    description Connected_to_Core
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
!
interface gigabitethernet 0/0/2
    description Core01
    switchport mode trunk
    switchport trunk native vlan 100
    trusted
    trusted vlan 1-4094
    lacp group 0 mode active
    lacp timeout short
!
interface gigabitethernet 0/0/3
    description Core02
    lacp group 0 mode active
    lacp timeout short
```

Suggested Answer: *A*

Community vote distribution

C (100%)

AlejandroRMontes 3 months, 2 weeks ago

Selected Answer: C

Estoy entre la A y la C pero me inclino más por la opción c (imagen 4) es la válida porque define el LAG (port-channel), configura el LAG como trunk con native VLAN 100 (coincidente con la imagen 1 / requisito), permite el rango de VLANs, y pone los puertos físicos en LACP active (con timeout corto si se desea convergencia más rápida). Todo esto coincide con las prácticas y ejemplos del documento VSX.

upvoted 2 times

Question #5 *Topic 1*

A customer has deployed an AOS-10 mobility gateway cluster consisting of three controllers at a single site. The WLAN is configured to tunnel wireless device traffic to the AOS-10 mobility cluster. The clients are authorized to use WPA2-Personal. An end-user has opened a ticket with the helpdesk stating they cannot connect their client device to the network. There are other devices currently associated with the SSID with no issues.

```
Nov 15 00:47:48.923  station-up *                    c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  -    wpa2 psk aes
Nov 15 00:47:48.923  wpa2-key1   <-                   c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  117
Nov 15 00:47:48.939  wpa2-key2   ->                   c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  123  mic failure
Nov 15 00:47:49.700  rad-acct-start   ->              c8:34:8e:20:50:4b  cc:88:c7:43:23:b1/__gw_172.20.10.102  -  -
Nov 15 00:47:50.421  wpa2-key1   <-                   c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  117
Nov 15 00:47:50.428  wpa2-key2   ->                   c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  123  mic failure
Nov 15 00:47:51.924  wpa2-key1   <-                   c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  117
Nov 15 00:47:51.937  wpa2-key2   ->                   c8:34:8e:20:50:4b  cc:88:c7:43:23:b1                    -  123  mic failure
AP-635#
```

Reviewing the output, what is the issue?

A. Transition mode is not enabled.

B. The client device has an invalid certificate.

C. The client device has an invalid pre-shared key.

D. The RADIUS response from the authentication server is failing.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibits.

```
Central-3-Edge# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.21.10.3

     Network                                                Nexthop          Metric     LocPrf     Weight    Path
-------------------------------------------------------------------------------------------------------------------
Route Distinguisher: 172.21.11.2:200      (L2VNI 200)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]           172.21.11.2      0          100        0         ?
*>i [3]:[0]:[172.21.11.2]                                  172.21.11.2      0          100        0         ?

Route Distinguisher: 172.21.11.2:201      (L2VNI 201)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]           172.21.11.2      0          100        0         ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[10.201.1.102]         172.21.11.2      0          100        0         ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[]                     172.21.11.2      0          100        0         ?
*>i [3]:[0]:[172.21.11.2]                                  172.21.11.2      0          100        0         ?

Route Distinguisher: 172.21.11.3:203      (L2VNI 203)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.203.1.1]           172.21.11.3      0          100        0         ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[10.203.1.100]         172.21.11.3      0          100        0         ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[]                     172.21.11.3      0          100        0         ?
*>  [3]:[0]:[172.21.11.3]                                  172.21.11.3      0          100        0         ?

Route Distinguisher: 172.21.10.1:10010      (L3VNI 10010)
*>i [5]:[0]:[0]:[0]:[0.0.0.0]                              172.21.11.1      0          100        0         ?
*>i [5]:[0]:[0]:[24]:[172.21.111.0]                        172.21.11.1      0          100        0         ?

Route Distinguisher: 172.21.10.2:10010      (L3VNI 10010)
*>i [5]:[0]:[0]:[24]:[10.200.1.0]                          172.21.11.2      0          100        0         ?
*>i [5]:[0]:[0]:[24]:[10.201.1.0]                          172.21.11.2      0          100        0         ?
*>i [5]:[0]:[0]:[32]:[172.21.11.4]                         172.21.11.2      0          100        0         ?

Route Distinguisher: 172.21.10.3:10010      (L3VNI 10010)
*>  [5]:[0]:[0]:[24]:[10.203.1.0]                          172.21.11.3      0          100        0         ?
*>  [5]:[0]:[0]:[32]:[172.21.11.5]                         172.21.11.3      0          100        0         ?
Route Distinguisher: 172.21.11.2:200      (L3VNI 10010)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.200.1.1]           172.21.11.2      0          100        0         ?

Route Distinguisher: 172.21.11.2:201      (L3VNI 10010)
*>i [2]:[0]:[0]:[00:00:00:00:00:01]:[10.201.1.1]           172.21.11.2      0          100        0         ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[10.201.1.102]         172.21.11.2      0          100        0         ?
*>i [2]:[0]:[0]:[20:4c:03:30:67:0c]:[]                     172.21.11.2      0          100        0         ?

Route Distinguisher: 172.21.11.3:203      (L3VNI 10010)
*>  [2]:[0]:[0]:[00:00:00:00:00:01]:[10.203.1.1]           172.21.11.3      0          100        0         ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[10.203.1.100]         172.21.11.3      0          100        0         ?
*>  [2]:[0]:[0]:[20:4c:03:0a:16:20]:[]                     172.21.11.3      0          100        0         ?
Total number of entries 24
```

```
Central-3-Edge# show ip route all-vrfs

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix               Nexthop          Interface     VRF(egress)   Origin/  Distance/    Age
                                                                   Type     Metric
-------------------------------------------------------------------------------------------
0.0.0.0/0            172.21.1.5       vlan501       -               O/E2     [110/25]     06h:47m:36s
172.21.1.0/30        172.21.1.5       vlan501       -               O        [110/200]    06h:47m:36s
172.21.1.4/30        -                vlan501       -               C        [0/0]        -
172.21.1.6/32        -                vlan501       -               L        [0/0]        -
172.21.10.1/32       172.21.1.5       vlan501       -               O        [110/100]    06h:47m:36s
172.21.10.2/32       172.21.1.5       vlan501       -               O        [110/200]    06h:47m:36s
172.21.10.3/32       -                loopback0     -               L        [0/0]        -
172.21.11.1/32       172.21.1.5       vlan501       -               O        [110/100]    06h:47m:36s
172.21.11.2/32       172.21.1.5       vlan501       -               O        [110/200]    06h:47m:36s
172.21.11.3/32       -                loopback1     -               L        [0/0]        -

VRF: overlay_lab

Prefix               Nexthop          Interface     VRF(egress)   Origin/  Distance/    Age
                                                                   Type     Metric
-------------------------------------------------------------------------------------------
0.0.0.0/0            172.21.11.1      -             -               B/EV     [200/0]      06h:47m:30s
10.200.1.0/24        172.21.11.2      -             -               B/EV     [200/0]      00h:06m:54s
10.200.1.1/32        172.21.11.2      -             -               B/EV     [200/0]      00h:06m:54s
10.201.1.0/24        172.21.11.2      -             -               B/EV     [200/0]      05h:15m:03s
10.201.1.1/32        172.21.11.2      -             -               B/EV     [200/0]      05h:15m:03s
10.201.1.102/32      172.21.11.2      -             -               B/EV     [200/0]      05h:14m:09s
10.203.1.0/24        -                vlan203       -               C        [0/0]        -
10.203.1.1/32        -                vlan203       -               L        [0/0]        -
172.21.11.4/32       172.21.11.2      -             -               B/EV     [200/0]      06h:47m:30s
172.21.11.5/32       -                loopback3     -               L        [0/0]        -
172.21.111.0/24      172.21.11.1      -             -               B/EV     [200/0]      06h:47m:30s

Total Route Count : 21
```

Which statement is true given the following CLI output from a CX 6300?

A. There are no active fabric clients on the CX switch with RD 172.16.10.1.

B. A wired client with IP address 10.203.1.100 has a host route that is not being properly advertised.

C. The overlay loopback addresses are advertised in the fabric with 24-bit subnet masks.

D. A wired client with IP address 10.203.1.100 is on a remote CX 6300 in the fabric with loopback IP address 172.21.11.2.

Suggested Answer: *D*

Community vote distribution

B (100%)

LarsBoerdijk 2 months ago

Selected Answer: B

RD 172.16.10.1 is not mentioned in the cli-output

The loopbacks are advertised as /32

10.203.1.100 is mentioned in L2VNI 203 with nexthop 172.21.11.3

There is no such route in the routing table.

10.203.1.100 is not reachable via loopback-ip 172.21.11.2

So the answer must be B

upvoted 1 times

Question #7 *Topic 1*

A customer is evaluating device profiles on a CX 6300 switch. The test device has the following attributes:

MAC address = 81:cd:93:13:ab:31 -

LLDP sys-desc = iotcontroller -

The test device is being assigned to the "iot-dev" role. However, the customer requires the "iot-prod" role be applied.

```
mac-group iot
     seq 10 match mac-oui 81:cd:93
port-access lldp-group iot-lldp
     seq 10 match sys-desc iot
port-access cdp-group iot-cdp
     seq 10 match platform accesspoint

port-access device-profile iot-dev
    associate role iot-dev
    associate lldp-group iot-lldp
port-access device-profile iot-prod
    associate role iot-prod
    associate mac-group iot
port-access device-profile iot-test
    associate role iot-test
    associate cdp-group iot-cdp
```

Given the configuration, what is causing the "iot-dev" role to be applied to the device?

A. An external RADIUS server is unreachable.

B. The device-profile precedence order is not configured.

C. The LLDP system description matches the lldp-group configuration.

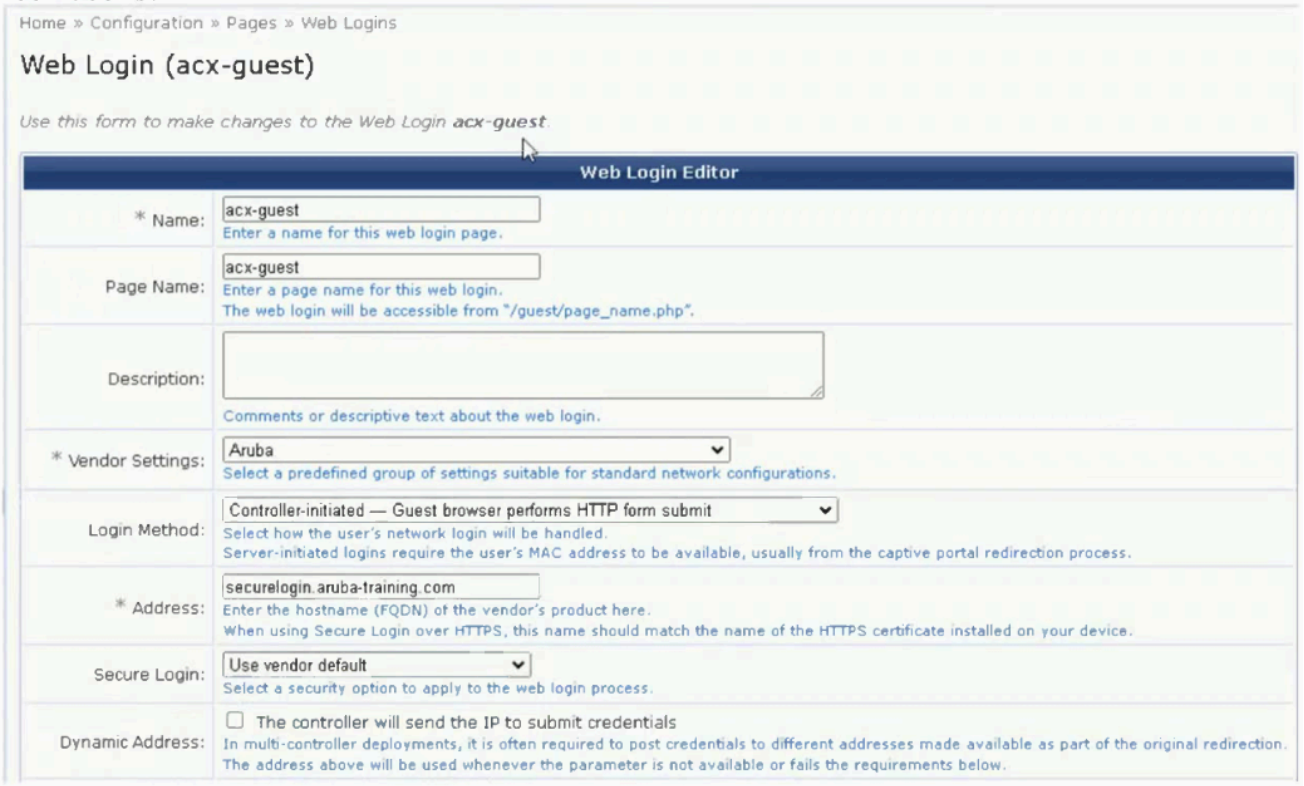
D. The test device does not support CDP

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

A customer reports that their HPE Aruba Networking ClearPass Guest captive portal is not functioning. The page loads but they are unable to browse after pressing connect. They have uploaded a valid and publicly trusted *.aruba-training.com certificate.
Refer to the exhibit.



Which would explain this issue?

A. *.aruba-training.com needs to be entered in the Address field for the ClearPass Guest.

B. HTTPS certificate is not required in ClearPass Guest

C. HTTPS wildcard certificates are not supported.

D. captiveportal-login.aruba-training.com needs to be entered in the Address field for the ClearPass Guest

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Your customer's employees connected to a wired network are complaining about a poor user experience. The customer has HPE Aruba Networking User Experience Insight (UXI) sensors deployed on their premises. These sensors have been running for multiple months. They are testing both the wired network (using the wired interface of each sensor) and the wireless networks. Your customer used the UXI dashboard to find the reason for the poor user experience. To find more details, the customer asked you to check the packet captures that have been downloaded from the sensors using the UXI dashboard.
From the .zip file downloaded from the UXI sensors, you checked the "datagrams" .pcap file, but you were not able to find any issues. How can you explain this?

A. The datagrams captured on the physical Ethernet interface are in a different pcap file

B. The "datagrams" pcap file only contains the successful tests. Failed tests are contained in the "datagrams-failed" pcap file

C. The UXI sensor could not upload the latest test results to the cloud, so the packet capture is outdated

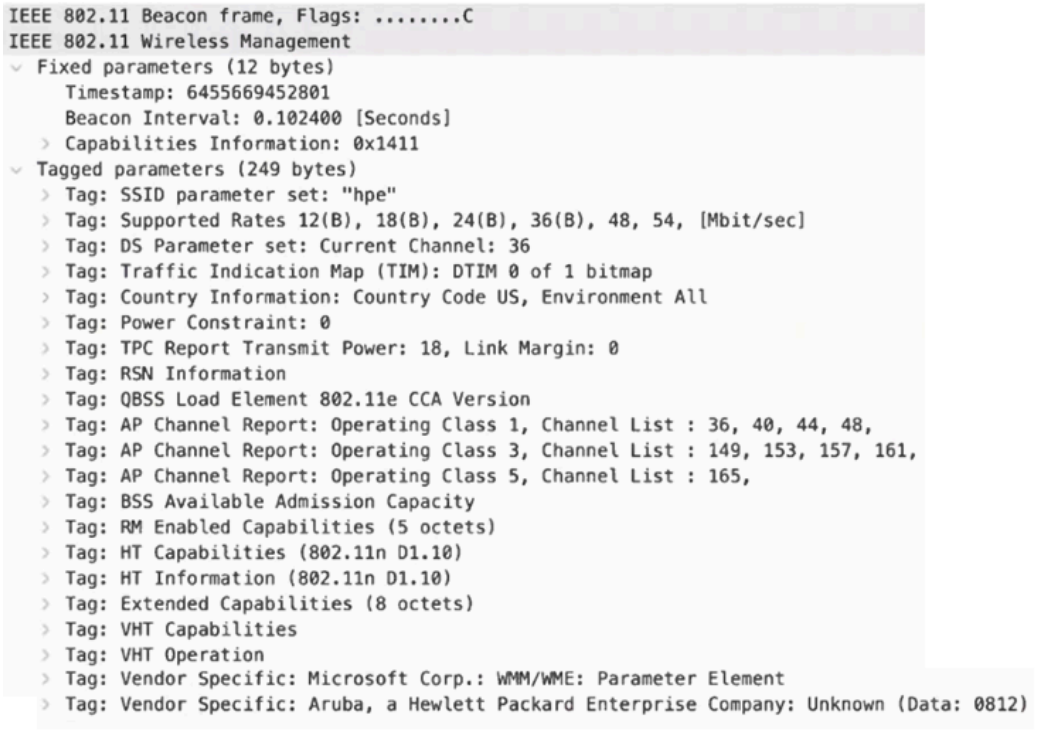
D. The default filters of the packet captures do not allow failed tests to be captured by the sensor.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Refer to the exhibit.



Which statement is true?

A. The SSID supports 802.11ac clients.

B. The SSID supports HR-DSSS data rates.

C. The SSID is supports 6 GHz clients.

D. The SSID supports 802.11ax clients.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

The ACME company has an AOS-CX 6200 VSF switch stack with an uplink over subscription ratio of 9.6.1 They have indicated that their low-priority TCP traffic has been flagged with a DSCP marking coloring them yellow.
Refer to the exhibit.

```
vsf1# show qos dscp-map default
DSCP     code_point local_priority cos color   name
-------- ---------- -------------- --- ------- ----
000000    0         1                  green   CS0
000001    1         1                  green
000010    2         1                  green
000011    3         1                  green
000100    4         1                  green
000101    5         1                  green
000110    6         1                  green
000111    7         1                  green
001000    8         0                  green   CS1
001001    9         0                  green
001010   10         0                  green   AF11
001011   11         0                  green
001100   12         0                  yellow  AF12
001101   13         0                  green
001110   14         0                  yellow  AF13
001111   15         0                  green
010000   16         2                  green   CS2
010001   17         2                  green
010010   18         2                  green   AF21
010011   19         2                  green
010100   20         2                  yellow  AF22
010101   21         2                  green
010110   22         2                  yellow  AF23
010111   23         2                  green
011000   24         3                  green   CS3
011001   25         3                  green
011010   26         3                  green   AF31
011011   27         3                  green
011100   28         3                  yellow  AF32
011101   29         3                  green
011110   30         3                  yellow  AF33
011111   31         3                  green
100000   32         4                  green   CS4
100001   33         4                  green
100010   34         4                  green   AF41
100011   35         4                  green
100100   36         4                  yellow  AF42
100101   37         4                  green
100110   38         4                  yellow  AF43
100111   39         4                  green
101000   40         5                  green   CS5
101001   41         5                  green
101010   42         5                  green
101011   43         5                  green
101100   44         5                  green
101101   45         5                  green
101110   46         5                  green   EF
101111   47         5                  green
110000   48         6                  green   CS6
110001   49         6                  green
110010   50         6                  green
110011   51         6                  green
110100   52         6                  green
110101   53         6                  green
110110   54         6                  green
110111   55         6                  green
111000   56         7                  green   CS7
111001   57         7                  green
111010   58         7                  green
111011   59         7                  green
111100   60         7                  green
111101   61         7                  green
111110   62         7                  green
111111   63         7                  green
```

They are considering adding two more nodes to the stack without adding any additional uplinks due to existing wiring constraints One of their architects has suggested adding the following configuration:

```
vsf1(config)# qos threshold-profile acmethreshold
vsf1(config-threshold)# queue 5 action wred-resp yellow min-threshold 40 percent max-threshold 80 percent
vsf1(config)# int lag 1
vsf1(config-if)# description uplink-to-collapsed-core
vsf1(config-if)# apply qos threshold-profile acmethreshold
```

What would be the impact of applying the acmethreshold profile as shown? (Choose two.)

A. All upper-layer protocol traffic egressing LAG1 will be subject to drop probability

B. All TCP traffic egressing LAG1 will be subject to drop probability

C. VoIP packets egressing any queue on LAG1 will more likely be protected from uplink over-utilization

D. Yellow-flagged TCP traffic egressing LAG1 will be subject to drop probability

E. Only VoIP packets egressing queue 5 on LAG1 will likely be protected from uplink over-utilization

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

You configured a WPA3-SAE with the following MAC Authentication Role Mapping in HPE Aruba Networking Central Cloud Authentication and Policy:

With further default settings, assume a new Android phone is connected to the network. Which role will the client be assigned after connecting for the first time?

A. iot-local

B. client will be rejected network access

C. byod

D. unmatched-device

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Refer to the exhibits.


```
R1(config-if)# show run cur
interface 1/1/1
    no shutdown
    mtu 9100
    ip address 10.255.1.0/31
    ip ospf 1 area 0.0.0.0
    ip ospf cost 100
    exit
```

```
R2(config-if)# show run cur
interface 1/1/1
    no shutdown
    mtu 9100
    ip address 10.255.1.1/31
    ip mtu 9100
    ip ospf 1 area 0.0.0.0
    exit
```

An engineer has applied the above configuration to R1 and R2. However, the router's OSPF adjacency never progresses past the "EXSTART/DR" state as shown below.

```
R2(config)# show ip ospf neighbors
VRF : default                          Process : 1
================================================

Total Number of Neighbors : 1

Neighbor ID      Priority  State            Nbr Address       Interface
-------------------------------------------------------------------------
10.255.1.0       1         EXSTART/DR       10.255.1.0         1/1/1
```

Which configuration action on either router will allow R1 and R2 to progress past the "EXSTART/DR" state?

A. Remove the layer 3 MTU configuration.

B. Ensure the OSPF process is not configured with passive-interface default

C. Change the IP address and mask applied to interface 1/1/1

D. Change R1 and R2 to a network type of point-to-point.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

A customer is evaluating device profiles on a CX 6300 switch. The test device has the following attribute:
MAC address = 81 :cd:93:13:ab:31
The test device needs to be assigned the “iot-prod” role. In addition, the “iot-default” role must be applied for any other device connected to interface 1/1/1.
This is a lab environment with no configuration of any external authentication server for the test.

```
mac-group iot
     seq 10 match mac-oui 81:cd:93

port-access device-profile iot-prod
    enable
    associate role iot-prod
    associate mac-group it
```

Given the configuration example, what is required to meet this testing requirement?

A. Enter the command "port-access device-profile mode block-until-profile-applied" for interface 1/1/1.

B. Enter the command "port-access fallback-role lot-default" for interface 1/1/1

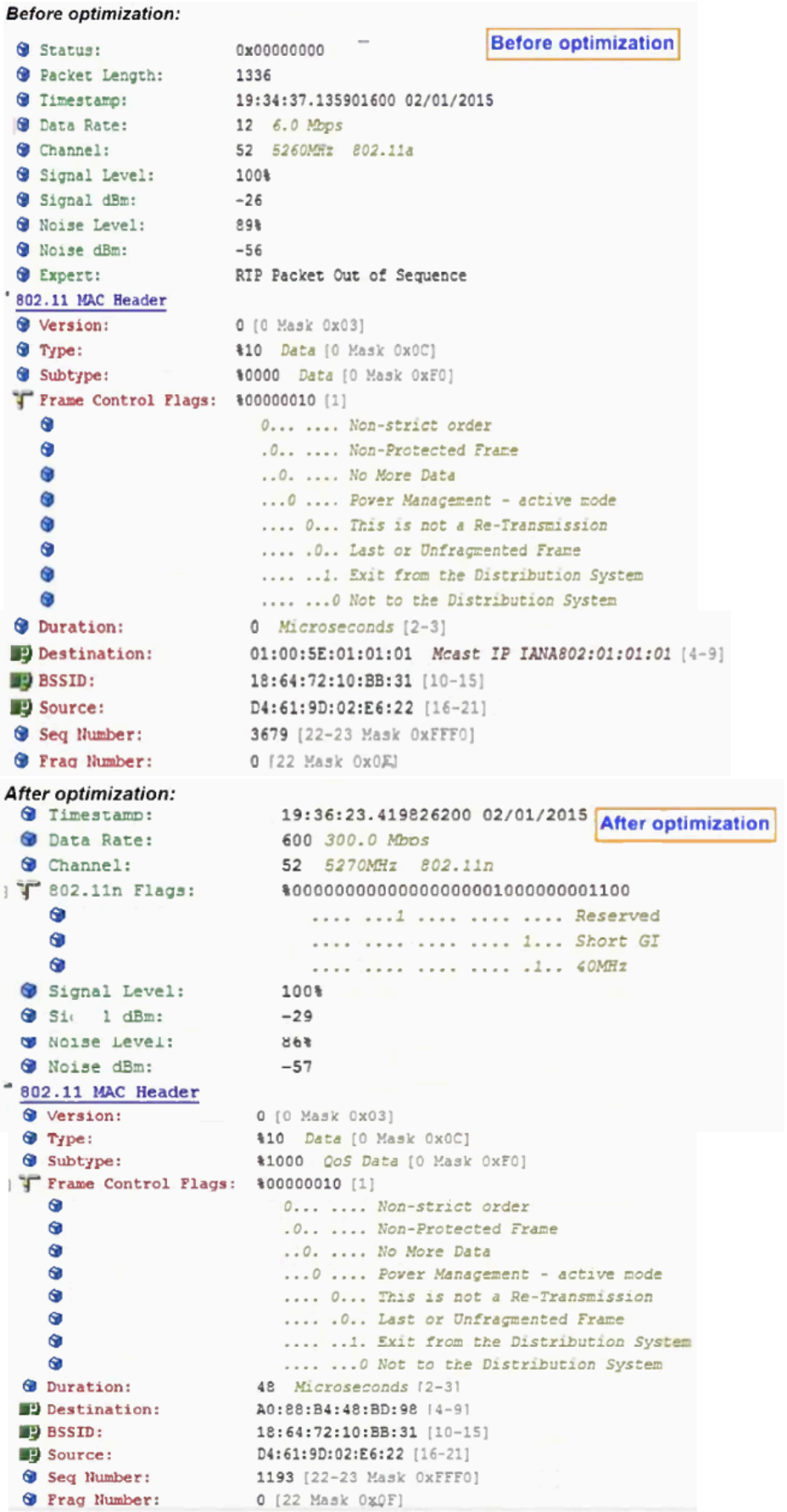
C. Enter the command "port-access onboarding-method precedence" to set device profiles with a higher precedence.

D. Enter the command "port-access onboarding-method precedence" to set device profiles with a lower precedence.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibits.



A network administrator attempts to improve multicast traffic flow and performs some packet captures for validation. What can the network administrator conclude from the results?

A. The data rate increased from 6 Mbps to 300 Mbps because Broadcast Multicast Optimization (BCMCO) was configured.

B. The data rate increased from 6 Mbps to 300 Mbps because Dynamic Multicast Optimization (DMO) was configured.

C. The capture taken after optimization does not show a packet length because Multicast Transmission Optimization was configured.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Refer to the exhibit.

```
AP#show network IoT
Name :IoT
ESSID :IoT
Status :Enabled
Mode :wpa-psk-tkip,wpa2-psk-aes
Band :2.4
Type :employee
Zone :
Termination :Disabled
Passphrase :7e2fdbe07d533847ee5d2fdf7bfdb3d08ef1ac4efc644ea2
Passphrase Size :8
WEP Key :
WEP Key Index :1
Coding :UTF-8
dot11r :Enabled
dot11k :Disabled
dot11v :Enabled
MPSK :Disabled
MPSK-local :Disabled
High Throughput :Enabled
Very High Throughput :Enabled
High Efficiency :Enabled
HE TXBF :Enabled
HE MU-OFDMA :Enabled
HE MU-MIMO :Enabled
HE UL MU-MIMO :Disabled
HE Guard Interval :800ns,1600ns,3200ns
A-beacon-rate :Default
G-beacon-rate :Default
Enable Agile Multiband (MBO) :Disabled
Advertise Cellular Data Capability attribute of MBO :Disabled
Fine Timing Measurement (802.11mc) Responder Mode :Disabled
Dot11k Profile :default
```

Which statement is true?

A. The SSID supports implicit beamforming.

B. The SSID supports sending neighbor reports.

C. The SSID supports RC4 encryption.

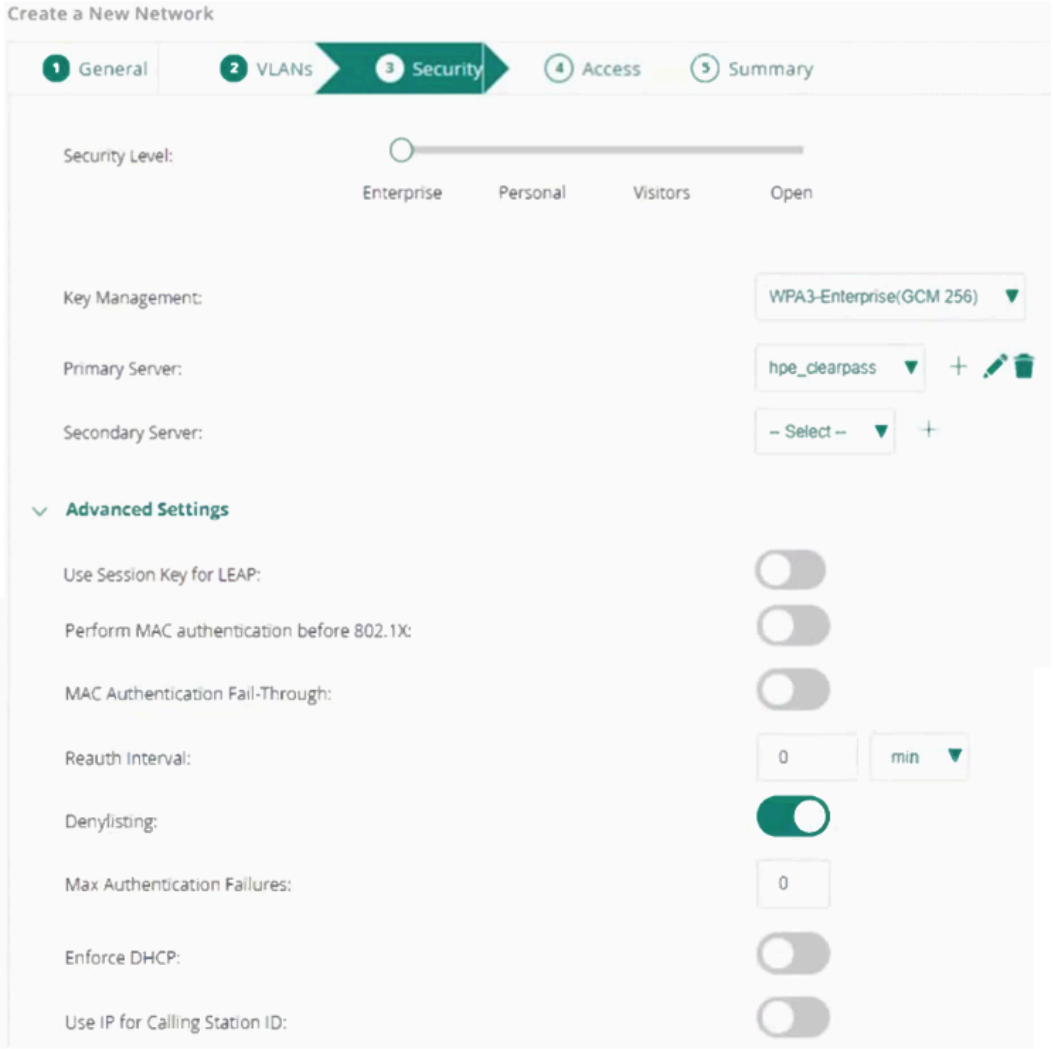
D. The SSID supports 802.11ac clients.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

You created a new SSID with the security settings shown in the exhibit.



Some, but not all, users complain that client devices are unable to connect to this SSID. What is the reason for this?

A. WPA3 Enterprise is not backward compatible with WPA2 Enterprise.

B. The WPA3 Enterprise GCM-256 mode does not support transition mode

C. The primary server's shared key differs from the shared key configured for this server on HPE Aruba Networking Central.

D. MAC authentication after a failed 802.1X authentication is not possible as the option "MAC Authentication Fail-Through" is disabled

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Refer to the CLI output below:

```
(GW1) #show tunneled-node-mgr trace-buf
TNM Trace Buffer
----------------

Nov  9 06:05:11  -->  SW Bootstrap Req     10.10.10.151  8c:85:c1:49:01:40 rsvd-vid=1 sacMode=1 sacIP=0.0.0.0 flags=1 mtu=1500
Nov  9 06:05:11  sos  SW hb tun created    10.10.10.151  tunnel 15.
Nov  9 06:05:11  <--  SW Bootstrap Ack     10.10.10.151  SBY=0.0.0.0
Nov  9 06:05:11  <--  Nodelist to Switch   10.10.10.151  retry=0 seq=1 enabled=1 SBY=10.10.10.101
Nov  9 06:05:11  -->  Nodelist ack         10.10.10.151  seq=1 status=1.
Nov  9 06:06:49  -->  User bootstrap req   10.10.10.151  00:50:56:a5:e8:95 rsvd-vid=1 vlan=40 key=1 role=visitor flags=6 mtu=1500 server=0.0.0.0.
Nov  9 06:06:49  sos  User tunnel created  10.10.10.151  00:50:56:a5:e8:95 dormant=0 tunnel 11.
Nov  9 06:06:49  gsm  Publish tun user     10.10.10.151  00:50:56:a5:e8:95.
Nov  9 06:06:49  <--  User bootstrap ack   10.10.10.151  00:50:56:a5:e8:95 assignedvlan=40 L2=1 S-UAC=10.10.10.101 idx=216 status=1:Success.
```

What statement about the output above is correct?

A. The UBT zone was configured to use a user-defined VRF

B. The port-access role was configured with gateway-role visitor.

C. The downloadable role was configured for gateway-role visitor.

D. The client authenticated using dot1x.

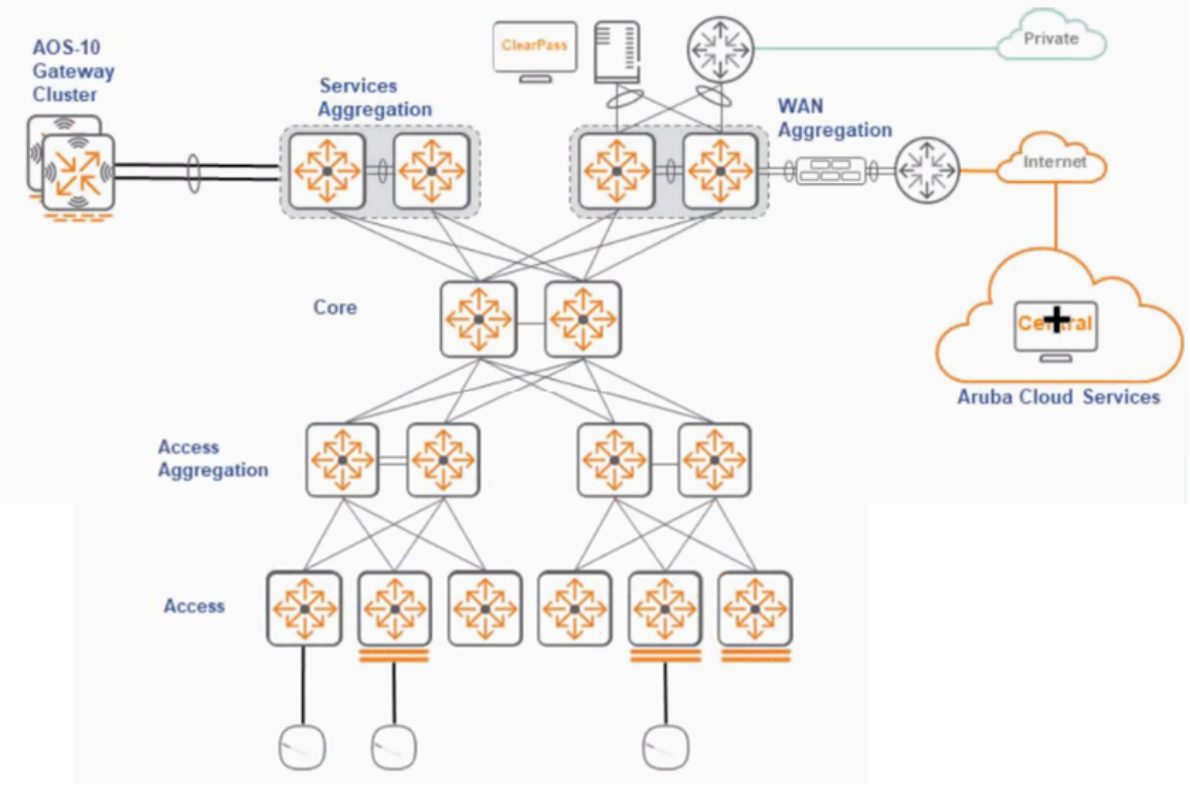
Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

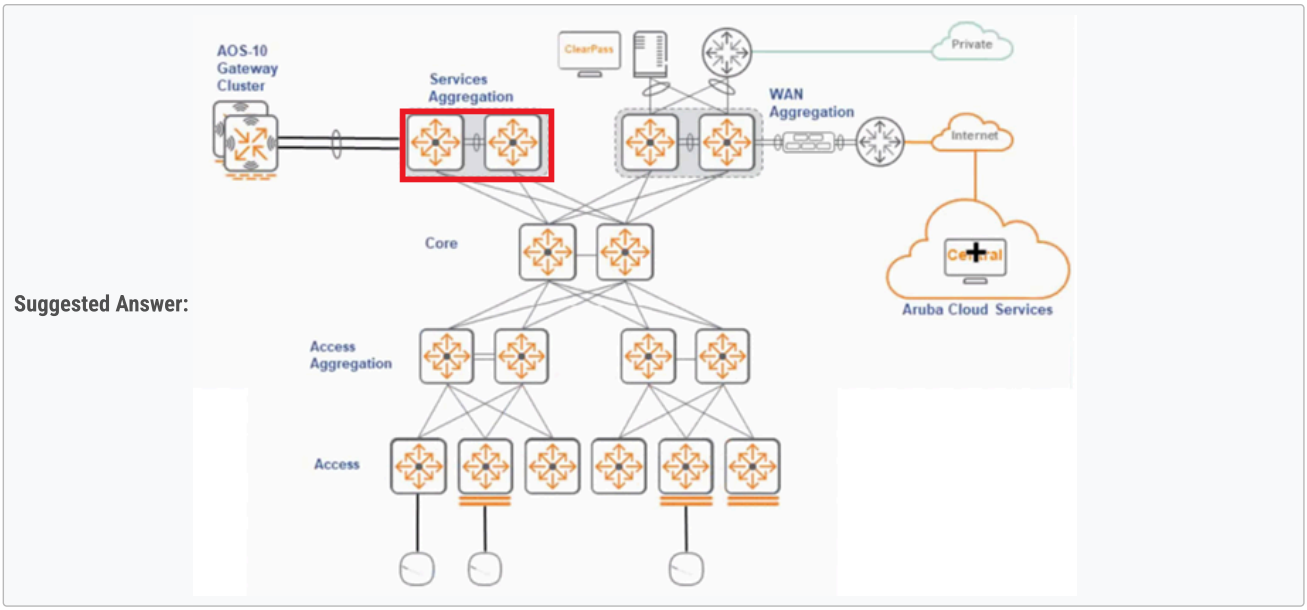
Question #19 *Topic 1*

HOTSPOT -

An administrator is creating a fabric with HPE Aruba Networking Central NetConductor in HPE Aruba Networking Central. Considering an EVPN VXLAN fabric, click on the most appropriate layer to be configured as a Route-Reflector Persona.



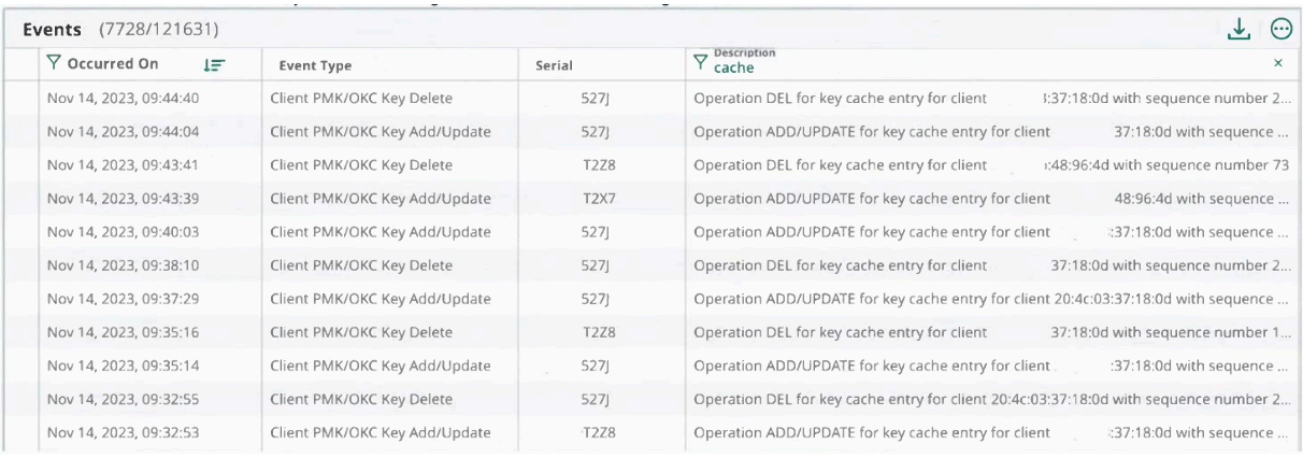
Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

In a WLAN network with a tunneled SSID, you see the following events in HPE Aruba Networking Central:



Events (7728/121631)

Occurred On	Event Type	Serial	Description: cache
Nov 14, 2023, 09:44:40	Client PMK/OKC Key Delete	527J	Operation DEL for key cache entry for client :37:18:0d with sequence number 2...
Nov 14, 2023, 09:44:04	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client 37:18:0d with sequence ...
Nov 14, 2023, 09:43:41	Client PMK/OKC Key Delete	T2Z8	Operation DEL for key cache entry for client :48:96:4d with sequence number 73
Nov 14, 2023, 09:43:39	Client PMK/OKC Key Add/Update	T2X7	Operation ADD/UPDATE for key cache entry for client 48:96:4d with sequence ...
Nov 14, 2023, 09:40:03	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client :37:18:0d with sequence ...
Nov 14, 2023, 09:38:10	Client PMK/OKC Key Delete	527J	Operation DEL for key cache entry for client 37:18:0d with sequence number 2...
Nov 14, 2023, 09:37:29	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client 20:4c:03:37:18:0d with sequence ...
Nov 14, 2023, 09:35:16	Client PMK/OKC Key Delete	T2Z8	Operation DEL for key cache entry for client 37:18:0d with sequence number 1...
Nov 14, 2023, 09:35:14	Client PMK/OKC Key Add/Update	527J	Operation ADD/UPDATE for key cache entry for client :37:18:0d with sequence ...
Nov 14, 2023, 09:32:55	Client PMK/OKC Key Delete	527J	Operation DEL for key cache entry for client 20:4c:03:37:18:0d with sequence number 2...
Nov 14, 2023, 09:32:53	Client PMK/OKC Key Add/Update	T2Z8	Operation ADD/UPDATE for key cache entry for client :37:18:0d with sequence ...

The customer asks you to investigate log messages. What should you tell them?

A. This is normal, expected behavior. No further actions are needed

B. There is a roaming issue. Enable Fast Roaming 802.11r and OKC to resolve the issue.

C. This indicates a client WLAN driver issue for the client with a MAC address ending with 37:18:0d. You should upgrade the client WLAN driver.

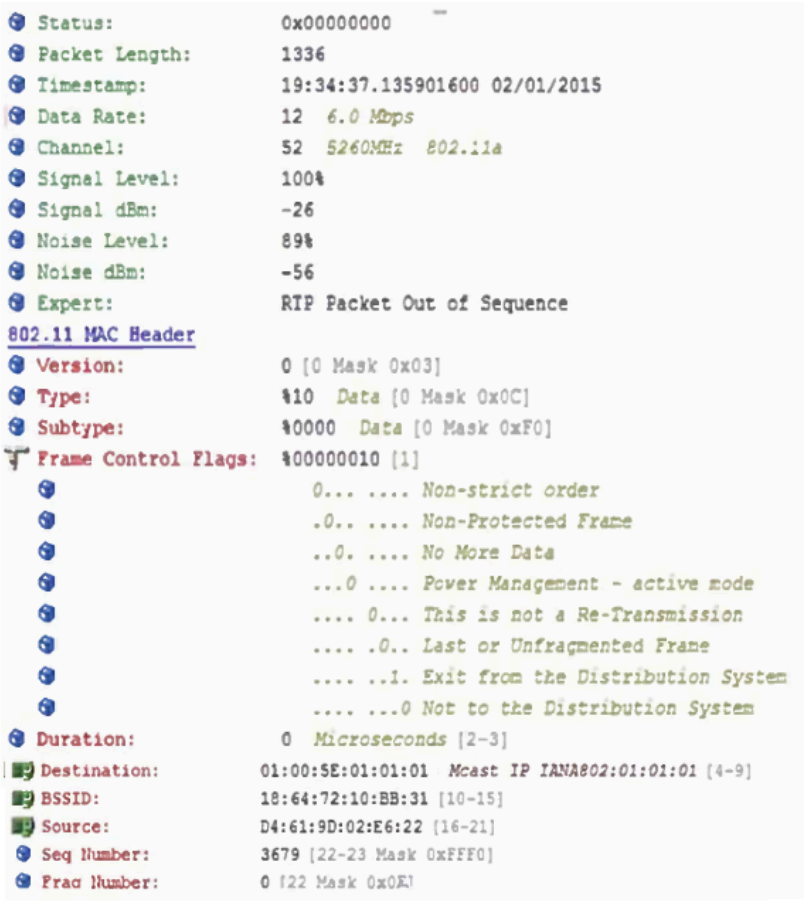
D. This indicates a security issue. The client with a MAC address ending with 37:18:0d is performing a Denial-of-Service attack on your network. You should track down the client and remove it from the network.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Refer to the exhibit.



A university runs its own TV station in the city. The IT department deploys a multimedia server so the TV productions can be sent out to the entire campus over the IP network using multicast-based communications. In order to improve the bandwidth consumption, PIM Sparse Mode and IGMP Snooping features are enabled.

When wireless users join the multicast groups, all users connected to the same WLAN experience poor network performance. However, wired users are not affected in this way. While troubleshooting, the network administrator saves the packet captures shown in the exhibit and concludes that all users, even those not joining the multicast group, receive the same multicast flow at slow speeds.

Which features should the network administrator enable to fix the problem?

A. Dynamic Multicast Optimization and UCC QoS correction

B. UCC QoS correction and Multicast Transmission Optimization

C. Dynamic Multicast Optimization and Multicast Transmission Optimization

D. ARP broadcast conversion into unicast and Multicast Transmission Optimization

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Your customer asked for help to apply an ACL for wireless guest users with the following criteria:

Wi-Fi guests are on VLAN 555 -
allow internet access
only allow access to public DNS servers
deny access to all internal networks except for any DHCP server
These session ACLs are already present in the CLI of the mobility gateway group:

```
ip access-list session dns-acl
    any any svc-dns permit
ip access-list session dhcp-acl
    any any svc-dhcp permit
ip access-list session allowall
    any any any permit
    ipv6 any any any permit
ip access-list session internal-networks
    user network 172.16.0.0 255.240.0.0 any deny
    user network 192.168.0.0 255.255.0.0 any deny
    user network 10.0.0.0 255.0.0.0 any deny
```

You have access to the CLI. Which user role meets all the criteria?

A.
```
user-role "WiFi-guest"
    access-list session dns-acl
    access-list session internal-networks
    access-list session dhcp-acl
    access-list session allowall
    vlan 555
```

B.
```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session internal-networks
    access-list session allowall
    vlan 555
```

C.
```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session internal-networks
    access-list session dns-acl
    vlan 555
```

D.
```
user-role "WiFi-guest"
    access-list session dhcp-acl
    access-list session dns-acl
    access-list session internal-networks
    access-list session allowall
    vlan 555
```

Suggested Answer: *A*

Community vote distribution

B (50%) D (50%)

LarsBoerdijk 2 months ago

Selected Answer: B

Ah crap , after better reading: it is answer B.
first allow dhcp from all sources
then deny all internal subnets
final: allow all (which includes dns ofcourse)
upvoted 1 times

LarsBoerdijk 2 months ago

Selected Answer: D

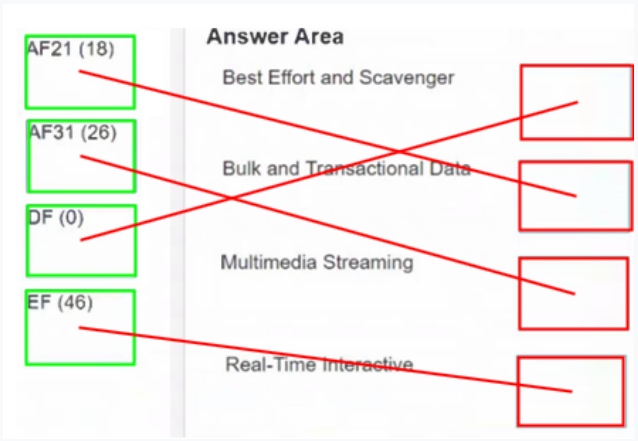
It cannot be A , because due to the order of acls you effectively block dhcp alltogether.
C is close, but does not "allow-all" for internet access
D is probably the best , but does allow for public and private dns servers
upvoted 1 times

Question #23 *Topic 1*

DRAG DROP -

Your customer is requesting a 4-class LAN queuing model for QoS. Following best practices, match the PHB/DSCP values to the application types.

Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

DRAG DROP -

Refer to the exhibit.

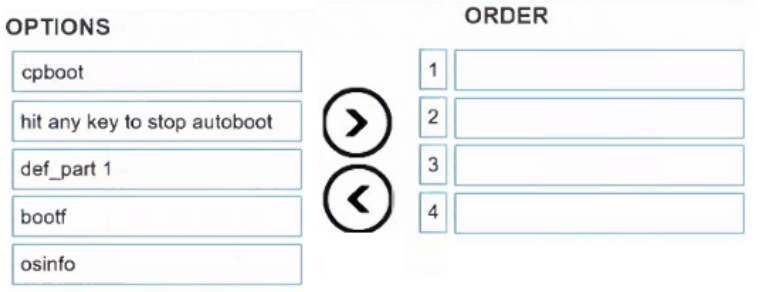
```
USB0:   setting speed to USB_SPEED_HIGH
2 USB Device(s) found
#1 Storage Device(s) found
Partition 0:
    image type: 0
  machine type: ...output omitted
          size: ...output omitted
       version: 10.3.1.0
  build string: ArubaOS version 10.3.1.0 for A70xx ...output omitted
...output omitted
RSA signature verified.
  image verify: PASS
Partition 1:
    image type: 0
  machine type: ...output omitted
          size: ...output omitted
       version: 10.3.1.1
  build string: ArubaOS version 10.3.1.1 for A70xx ...output omitted
 ...output omitted
RSA signature verified.
  image verify: PASS
```

```
cpxload# help
barinit - barinit
cmp     - memory comparing
cp      - memory copy
cpboot  - execute CPBoot
cpld    - cpld  :    read/write CPLD registers
crc16   - compute crc16
ddr     - show ddr registers
ddrinit - ddrinit
ddrrd   - read ddr registers
ddrwr   - write ddr registers
except  - Exception Handler Test
help    - print command description/usage
i2c     - i2c access
loop    - loop cmds
md      - memory display
memecc  - memecc
memsi   - full memory test
mfcr    - mfcr: rd registers
mtcr    - mtcr: write registers
mtest   - memory test
mw      - memory write (fill)
phy     - show ddr phy registers
phyrd   - read ddr phy registers
phywr   - write ddr phy registers
printenv- print environment variables
rd      - rd registers
rw      - write registers
spd     - show ddr3 spd data
tge     - tge cmds
```

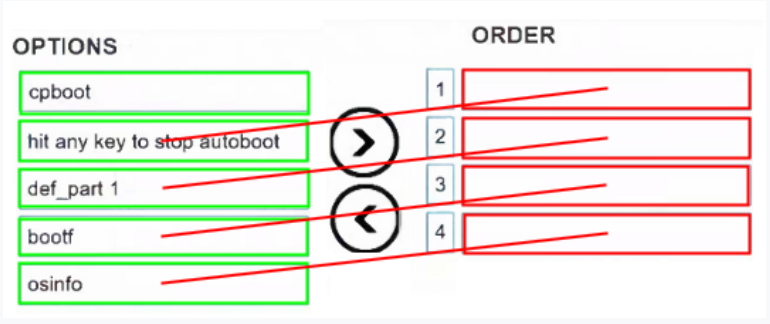
```
cpboot> help
?             - alias for 'help'
bank          - show/set the current bootflash bank (partition).
boot_update   - update bootloader image in boot flash
bootaos       - boot from an AOS image in memory
bootf         - boot from an AOS image from FLASH/External USB
def_part      - set default FLASH boot partition
dhcp          - boot image via network using DHCP/TFTP protocol
dir           - list the files in external USB device (default /)
fltest        - fltest  - test u-boot FLASH driver
format        - format FLASH device
help          - print command description/usage
lock          - Perform flash protection of the selected sectors on boot FLASH
n2xx_vrm      - n2xx_vrm - Show XLP VRM registers and state
osinfo        - osinfo - show the OS image version(s)
part          - write a new DOS partition table to USB Flash
ping          - send ICMP ECHO_REQUEST to network host
printenv      - print environment variables
purgeenv      - restore default environment variables
reset         - perform RESET of the CPU
runelf        - Run from an ELF image in memory
saveenv       - save environment variables to persistent storage
setenv        - set environment variables
tftpboot      - boot image via network using TFTP protocol
upgrade       - upgrade FLASH partition
```

You updated your gateway to the most recent firmware. However, after the firmware was updated, the gateway could no longer connect to HPE Aruba Networking Central. Your corporate ITIL procedures require you to implement your backout plan. You connected a console cable to your gateway and saw the following prompt. cpxload#

In what order, do you need to execute the following commands to return to the previous firmware version?



Suggested Answer:



Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Refer to the exhibit.

```
interface 1/1/7
    description ACCESS_PORT
    no shutdown
    no routing
    vlan access 1
    aaa authentication port-access client-limit 5
    aaa authentication port-access critical-role CRITICAL_AUTH
    aaa authentication port-access critical-voice-role CRITICAL_VOICE
    aaa authentication port-access preauth-role PRE_AUTH
    aaa authentication port-access reject-role REJECT_AUTH
    aaa authentication port-access auth-role DEFAULT_AUTH
    aaa authentication port-access dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
```

Which user role will be assigned when a voice client tries to connect for the first time, but the RADIUS server is unavailable?

A. CRITICAL_VOICE

B. CRITICAL_AUTH

C. PRE_AUTH

D. DEFAULT_AUTH

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 count 27

Warning: user-debug is enabled on one or more specific MAC addresses;
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------

Jun 29 20:56:51  station-up             *  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -      -    wpa2 aes
Jun 29 20:56:51  eap-id-req           <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1      5
Jun 29 20:56:51  eap-start             ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -      -
Jun 29 20:56:51  eap-id-req           <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1      5
Jun 29 20:56:51  eap-id-resp            ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1      7    it
Jun 29 20:56:51  rad-req               ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          42     174  10.1.140.101
Jun 29 20:56:51  eap-id-resp            ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          1      7    it
Jun 29 20:56:51  rad-resp              <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  42     88
Jun 29 20:56:51  eap-req               <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          2      6
Jun 29 20:56:51  eap-resp              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          2      214
Jun 29 20:56:51  rad-req               ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  43     423  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  43     228
Jun 29 20:56:51  eap-req               <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          3      146
Jun 29 20:56:51  eap-resp              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          3      61
Jun 29 20:56:51  rad-req               ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  44     270  10.1.140.101
Jun 29 20:56:51  rad-resp              <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  44     128
Jun 29 20:56:51  eap-req               <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4      46
Jun 29 20:56:51  eap-resp              ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4      46
Jun 29 20:56:51  rad-req               ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  45     255  10.1.140.101
Jun 29 20:56:51  rad-accept            <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0/RADIUS1  45     231
Jun 29 20:56:51  eap-success           <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          4      4
Jun 29 20:56:51  user repkey change     *  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          65535  -    204c0306e790000000170008
Jun 29 20:56:51  macuser repkey change  *  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          65535  -    70:4d:7b:10:9e:c6
Jun 29 20:56:51  wpa2-key1            <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -      117
Jun 29 20:56:51  wpa2-key2             ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -      117
Jun 29 20:56:51  wpa2-key3            <-  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -      151
Jun 29 20:56:51  wpa2-key4             ->  70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0          -      95
```

Which wireless connection phase has just been completed?

A. L3 authentication and encryption

B. MAC Authentication and 4-way handshake

C. 802.11 enhanced open association

D. L2 authentication and encryption

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

You want to configure an MTU of 9198 for a routed lag interface on a CX 6300 switch. Which configuration achieves this?

A.
```
interface lag 11 multi-chassis
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

B.
```
interface lag 11
    no shutdown
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

C.
```
interface lag 11 multi-chassis
    no shutdown
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

D.
```
interface lag 11
    no shutdown
    ip mtu 9198
    ip address 10.1.1.1/24
    lacp mode active
    exit
!
interface 1/1/11
    mtu 9198
    lag 11
    exit
!
interface 1/1/12
    mtu 9198
    lag 11
    exit
```

Suggested Answer: *A*

Community vote distribution

D (100%)

LarsBoerdijk 2 months ago

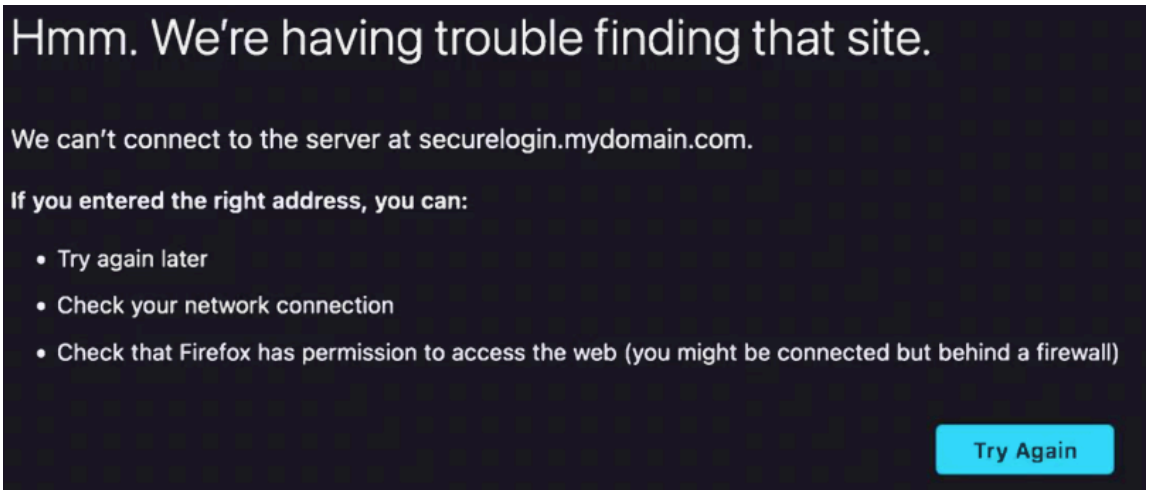
Selected Answer: D

At cannot be answer A, because the 6300 does traditionally not support VSX , only VSF stacking. ANswer A is a multi-chassis lacp : that is only for VSX

upvoted 1 times

Question #28 *Topic 1*

You configured a tunneled SSID with captive portal and an HPE Aruba Networking ClearPass Guest Self Registration workflow. When testing and launching the self-registration workflow, after successful registration, the login action shows the following error:



What is the best solution to resolve this error?

A. You need to be connected to the guest SSID while testing.

B. You need to include the root and intermediate certificates in the captive portal certificate for your access points.

C. You need to change the Login Address in ClearPass to securelogin.arubanetworks com.

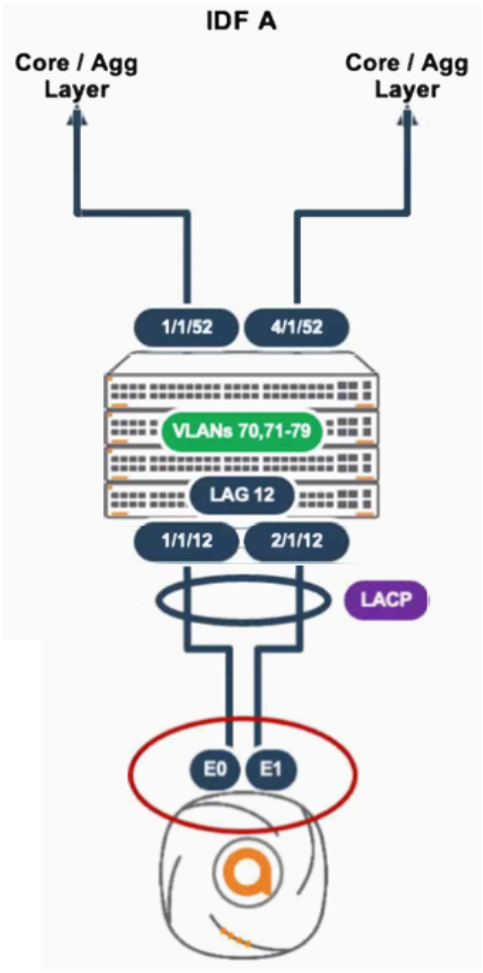
D. You need to include the root and intermediate certificates in the captive portal certificate for your gateway.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

A deployment using AP-635s is connected to a stack of CX 6300s as shown.



The output of the show LACP interfaces shows the following:

```
SW-IDF-A# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
------------------------------------------------------------------------------
1/1/12     lag12      13    1     ALFNCD  88:3a:30:99:ac:40 65534  12   up
2/1/12     lag12      77    1     ALFO    88:3a:30:99:ac:40 65534  12   lacp-block
```

What is causing this issue?

A. e0 is connected to a smart rate interface, and e1 is connected to a non-smart rate interface.

B. The AP is configured with LACP active.

C. Spanning tree and loop protect are enabled on both AP uplink ports.

D. Each AP interface is connected to a routed-only interface on different networks.

Suggested Answer: *D*

Community vote distribution

A (100%)

LarsBoerdijk 2 months ago

Selected Answer: A

Aruba CX switches do not support LACP with different port speeds. All member ports in a Link Aggregation Group (LAG) must have the same speed and duplex settings to be included in the LACP bundle. If a port with a different speed is added, it will not participate in the LAG and the port speed must be manually reconfigured to match the others.