ACMP 5.0 Study Guide

Overview

ACMP exam questions cover the topics listed below. The questions include key concepts, networking and topology design, GUI and CLI interpretation, GUI and CLI troubleshooting and interpretation of CLI configuration file segments.

1 - Product Knowledge
2 - Firewall Roles and Policies
3 - Operations
4 - Planning and Design
5 - IDS
6 - Troubleshooting
7 - Applications and Solutions

Topic Details

1. Product Knowledge
    a. Mobility Controllers Models
        i. Understand the limits of user scaling for different controller models.
        ii. Understand the limits of AP scaling for different controller models.
        iii. Understand the limits of Remote AP scaling for different controller models.
        iv. Power supplies offered for various models.
        v. Chassis based controller modules.
        vi. Power-over-Ethernet support.
    b. AP models
        i. Indoor AP models.
        ii. Outdoor AP models.
        iii. Models supporting internal and external antennas.
        iv. Antenna types offered as external antennas.
        v. Models supporting Power-over-Ethernet support.
        vi. 802.11a/b/g/n support by model.
    c. Licensing
        i. Understand the 5.0 licensing model for all controllers
        ii. Be able to articulate the features and functions of the Aruba software licenses.
        iii. Be able to articulate the features and functions included in the base ArubaOS.

2. Firewall Roles and Policies
    a. Policy Design
        i. Function of firewall design.
        ii. Interpretation and troubleshooting of firewall rule policy.
        iii. Application of firewall policy to user roles.
        iv. Application of firewall policy to interfaces.
        v. Be able to articulate the difference between a stateful firewall and an access control list (ACL).
        vi. Describe an Ethertype ACL.
    b. Roles
        i. Describe the function of built-in roles.

ii. Describe the use and creation of user created roles.
iii. Understand role derivation.

c. Aliases
i. Describe the function and use of aliases.
ii. Understand the built in aliases.

d. NAT
i. Describe the function of source NAT.
ii. Describe the function of destination NAT.
iii. Understand the use of NAT for captive portal authentication.
iv. Describe VLAN based NAT functionality.

e. Interpret example policy

3. Operations
a. Authentication
i. 802.1X
ii. Pre-Shared Keys
iii. Open system
iv. Captive portal with credentials
v. Captive portal with guest logon

b. Configuration Wizards
i. Configuration of the controller using the Controller Wizard
ii. VLAN and IP address configuration
iii. Port configuration
iv. Network time configuration
v. Controller role configuration
vi. License configuration
vii. LAN configuration
viii. WLAN configuration for employee SSIDs
ix. WLAN configuration for guest SSIDs
x. RADIUS server configuration
xi. 802.1X authentication configuration
xii. Captive portal configuration and customization

c. Management
i. Software upgrades on the controllers and APs
ii. Interface layout
iii. AP management
iv. License management
v. Configuration screens
vi. Monitoring screens
vii. Security screens

d. Power over Ethernet
i. Power provided
ii. Standards
iii. Transmission distances

e. Roaming
i. Layer 2 roaming
ii. Layer 3 roaming
iii. Mobility domains

iv. HAT table configuration

f. RF management and ARM
   i. ARM channel and power selection
   ii. ARM self healing
   iii. ARM band steering
   iv. ARM Spectrum load balancing
   v. ARM Airtime fairness
   vi. ARM rate shaping
   vii. Client aware ARM scanning

g. Master/local
   i. Differences between a local controller and a master controller
   ii. What is configured on the local
   iii. What is configured on the master

h. Centralized Auth and Encryption
   i. Centralized encryption
   ii. Encryption methods
   iii. Layer 2 Wi-Fi frame termination
   iv. RAIDUS authentication
   v. Fail through servers
   vi. Fall through servers
   vii. Machine authentication
   viii. Per-SSID captive portal

i. AP Provisioning and Configuration
   i. Static provisioning
   ii. Dynamic provisioning
   iii. CLI configuration
   iv. Web interface configuration
   v. Group selection
   vi. Antenna provisioning
   vii. Serial configuration

j. User/Server Derivation Rules
   i. User derivation rules
   ii. Server derivation rules
   iii. Rule based role derivation

k. Profiles
   i. Profile concept
   ii. Profile hierarchy
   iii. Profile reuse

l. Controller configuration methods
   i. SNMP configuration
   ii. Syslog configuration
   iii. VLANs & VLAN trunking
   iv. IP addressing
   v. Use of the loopback interface
   vi. Spanning tree
   vii. VRRP

4. Planning and Design

a. Networking
    i. Layer 2 networks
    ii. Layer 3 networks
    iii. Routing
b. Self-healing
    i. AP deployment design
    ii. ARM functionality
c. L2 model traffic flow
d. L3 model traffic flow
e. VPN
    i. Site-to-Site VPN
    ii. Client server VPN
f. Captive portal
    i. Authentication types
    ii. Authentication sources
    iii. Provisioning capabilities
    iv. Internal DB functionality
    v. Guest provisioning role
g. RF plan
    i. Don't care areas
    ii. Don't deploy areas
    iii. Floor plan image import
    iv. Plan selection criteria
    v. Live heat maps
    vi. Selecting the right AP and connection speed
h. Master/local
    i. Where to place controllers
    ii. Direct and indirect connection of APs
    iii. L2 vs. L3 controller operation
    iv. Controller communication considerations
i. Switch redundancy
    i. Local redundancy
    ii. Master redundancy
j. Mobility
    i. L2 Mobility
    ii. L3 Mobility
k. Wired Access Control
    i. Wired Authentication
    ii. VLAN & Firewall port policies
l. Controller discovery

5. IDS
    a. Rogue & Interfering APs
        i. Detection
        ii. Classification
        iii. Containment
    b. IDS
        i. Configuration

        ii. Reporting
6. Troubleshooting
    a. Client Connectivity
        i. User connection
        ii. AP status
    b. Aruba platform
        i. L2 connectivity
        ii. L3 connectivity
        iii. Licensing
        iv. AP counts
        v. Firewall policy
        vi. Role derivation
        vii. Master/local connectivity
        viii. AP connectivity
        ix. DHCP
        x. Controller IP
    c. Infrastructure
        i. Intervening ACLs
        ii. DHCP
        iii. PoE
7. Applications and Solutions
    a. RAP
        i. Configuration
        ii. Licensing
        iii. Operation modes
        iv. Forwarding modes
        v. Maintenance
        vi. Zero Touch provisioning
    b. Mesh
        i. Mesh topology
        ii. Configuration
        iii. Licensing
        iv. Remote Mesh portal
    c. VIA
        i. Configuration
        ii. Licensing
    d. Location
        i. Locating a client
        ii. AP design for location
        iii. Location functionality

Sample Questions

1. Which access point models support concurrent operations in both the “b/g” band as well as the “a” band? (Choose all the correct answers.)

A. AP-60

B. AP-61

C. AP-65

D. AP-85

E. AP-125

2. Which statement is true about the Content Security License?

a) Applied to the master controller
b) Applied to all the controllers in the network
c) It is based on number of users
d) It is based on number of AP’s

3. When a user first associates to the WLAN, what role are they given?

A. the guest role

B. the stateful role

C. the initial role in the server group profile

D. the initial role in the AAA profile

4. Which tunnel protocol is used between controllers to support L2 mobility in an Aruba environment?

A. Basic IP

B. GRE

C. IPinIP

D. Mobile IP

E. None of the above

5. Which of the statements below are TRUE regarding ARM’s Spectrum Load Balancing feature? (Choose all the correct answers)

A. Available only on 5GHz radios

B. Disabled by default

C. Balances client load across available channels/APs

D. Enabled by default

6. Which types of information are necessary for the RF planner to calculate the number of APs needed? (Choose all the correct answers.)

A. protocol required (802.11a/b/g/n)

B. desired data rate

C. building wall composition and density

D. AP types

E. location and frequency of interfering devices

7. For controller redundancy to work, to which IP address should the Aruba AP terminate its GRE tunnel?

A. VRRP IP address

B. management IP of an Aruba controller

C. management IP of the backup Aruba controller

D. HSRP IP address

8. (group8) #show ap active

Active AP Table

Name	Group	IP Address	11g Clients	11g Ch/EIRP/MaxEIRP	11a Clients	11a Ch/EIRP/MaxEIRP
AP1	building1	10.1.80.150	0	AM	0	AP:HT:149+/19/19
AP2	building1	10.1.80.151	0	AM	0	AM

A user has called technical support because they cannot see any of their APs in building one. You perform the "show" command as illustrated above.

What can you conclude about these two APs from this output?

A. the GRE for the APs terminate on two different controllers: 10.1.80.150 and 10.1.80.151

B. the system will not function because there is no building1 group defined

C. the building1 APs are configured to not accept any user connections

D. the user needs to configure his client to use the b/g band

E. the user needs to configure his client to use the a band

9. A client device associates with an SSID provisioned with 802.1X authentication. The client is set for PEAP authentication. EAP termination (AAA Fastconnect) is disabled on the controller. But the client continuously cycles through the authentication process. Which of the following could cause this? Choose all that apply.

A. The client is provisioned with the wrong EAP type.

B. The client has an expired or revoked server certificate.

C. The DHCP server is not enabled.

D. The VLAN is missing for the SSID.

E. The controller does not support PEAP in this mode.

10. A Remote AP provisioned with an SSID in the operational mode "*always*" has which one of the following characteristics?

A. The RAP must obtain its configuration from the controller each time it boots.
B. The operational mode applies to tunnel and split-tunnel forwarding SSID.
C. The operational mode applies to a Bridge forwarding SSID.
D. The RAP does not support this mode.
E. The SSID only appears if the AP does not see the controller.

11. What is the purpose of Mesh Clusters?

A. To separate Mesh points and Mesh Portals
B. To make sure that mesh points and portals with the same VAPs are not in the same cluster
C. To create a group of mesh points and mesh portals that create mesh links with each other using the same 802.11 connection settings
D. To cluster mesh APs of the same model together