EXAM REFERENCE GUIDE

ARUBA-CERTIFIED MOBILITY PROFESSIONAL (ACMP) 6.4 EXAM GUIDE

The Aruba-Certified Mobility Professional (ACMP) 6.4 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.

- Product Knowledge
- Firewall Roles and Policies
- Operations
- Planning and Design
  - IDS
- Troubleshooting
- Applications and Solutions

Preparation for ACMP includes familiarity with IAW/SWDI 6.4 courseware or its equivalent MBC 6.4. Additionally, review of VRDs will help to reinforce the concepts learned within the courses.

TOPIC DETAILS

Product Knowledge

1. Mobility Controllers Models

    A. Understand the limits of user scaling for different controller models

    B. Understand the limits of AP scaling for different controller models

    C. Understand the limits of Remote AP scaling for different controller models

    D. Power supplies offered for various models

    E. Chassis based controller modules

    F. Power-over-Ethernet support

HELPFUL ACMP TIPS

- Review of VRDs will help to reinforce the concepts learned within the courses.
- An ACMP certified engineer is able to deploy and manage a large-scale, multi-controller network.
- It is assumed that all candidates have completed the Scalable WLAN Design and Implementation (SWDI) course.
- ACMP sets the minimum bar to evaluate your skill level in deploying and managing an Aruba WLAN.
- Building upon ACMA, the ACMP exam covers more complex network settings such as multiple controllers and Layer 3 mobility.

2. AP models

    A. Indoor AP models

    B. Outdoor AP models

    C. Models supporting internal and external antennas

    D. Antenna types offered as external antennas

    E. Models supporting Power-over-Ethernet support

    F. 802.11a/b/g/n/ac support by model

3. Licensing

    A. Understand the 6.4 licensing model for all controllers

    B. Understand Centralized Licensing in AOS 6.4

    C. Be able to articulate the features and functions of the Aruba software licenses

    D. Be able to articulate the features and functions included in the base ArubaOS

Firewall Roles and Policies

1. Policy Design

    A. Function of firewall design

    B. Interpretation and troubleshooting of firewall rule policy

    C. Application of firewall policy to user roles

    D. Application of firewall policy to interfaces

    E. Be able to articulate the difference between a stateful firewall and an access control list (ACL)

    F. Describe an Ethertype ACL

2. Roles

  A. Describe the function of built-in roles

  B. Describe the use and creation of user created roles

  C. Understand role derivation

3. Aliases

  A. Describe the function and use of aliases

  B. Understand the built in aliases

4. NAT

  A. Describe the function of source NAT

  B. Describe the function of destination NAT

  C. Understand the use of NAT for captive portal authentication

  D. Describe VLAN based NAT functionality

5. Interpret example policy

Operations

1. Authentication

  A. 802.1X

  B. Pre-Shared Keys

  C. Open system

  D. Captive portal with credentials

  E. Captive portal with guest logon

2. Configuration of the controller using the WebUI Wizard

  A. VLAN and IP address configuration

  B. Port configuration

  C. Network time configuration

  D. Controller role configuration

  E. License configuration

  F. LAN configuration

  G. WLAN configuration for employee SSIDs

  H. WLAN configuration for guest SSIDs

  I. RADIUS server configuration

  J. 802.1X authentication configuration

  K. Captive portal configuration and customization

3. Management

  A. Software upgrades on the controllers and APs

  B. Interface layout

  C. AP management

  D. License management

  E. Configuration screens

  F. Monitoring screens

  G. Security screens

4. Power over Ethernet

  A. Power provided

  B. Standards

  C. Transmission distances

5. Roaming

  A. Layer 2 roaming

  B. Layer 3 roaming

  C. Mobility domains

  D. HAT table configuration

6. RF management and ARM

  A. ARM channel and power selection

  B. ARM self healing

  C. ARM band steering

  D. ARM Spectrum load balancing

  E. ARM Airtime fairness

  F. ARM rate shaping

  G. ARM ClientMatch

  H. Client aware ARM scanning

  I. Spectrum Monitor provisioning

  J. Spectrum Monitor usage

7. Master/local

  A. Differences between a local controller and a master controller

  B. What is configured on the local

  C. What is configured on the master

8. Centralized Auth and Encryption

   A. Centralized encryption

   B. Encryption methods

   C. Layer 2 Wi-Fi frame termination

   D. RADIUS authentication

   E. Fail through servers

   F. Fall through servers

   G. Machine authentication

   H. Per-SSID captive portal

9. AP Provisioning and Configuration

   A. Static provisioning

   B. Dynamic provisioning

   C. CLI configuration

   D. Web interface configuration

   E. Group selection

   F. Antenna provisioning

   G. Serial configuration

10. User/Server Derivation Rules

   A. User derivation rules

   B. Server derivation rules

   C. Rule based role derivation

11. Profiles

   A. Profile concept

   B. Profile hierarchy

   C. Profile reuse

12. Controller configuration methods

   A. SNMP configuration

   B. Syslog configuration

   C. VLANs & VLAN trunking

   D. IP addressing

   E. Use of the loopback interface

   F. Spanning tree

   G. VRRP

   H. HA redundancy

Planning and Design

1. Networking

   A. Layer 2 networks

   B. Layer 3 networks

   C. Routing

2. Self-healing

   A. AP deployment design

   B. ARM functionality

3. L2 model traffic flow

4. Layer 3 model traffic flow

5. Captive portal

   A. Authentication types

   B. Authentication sources

   C. Provisioning capabilities

   D. Internal DB functionality

   E. Guest provisioning role

6. Master/local

   A. Where to place controllers

   B. Direct and indirect connection of APs

   C. Layer 2 vs. Layer 3 controller operation

   D. Controller communication considerations

7. Controller redundancy

   A. Local redundancy

   B. Master redundancy

8. Mobility

   A. Layer 2 Mobility

   B. Layer 3 Mobility

9. Wired Access Control

   A. Wired Authentication

   B. VLAN & Firewall port policies

10. Controller discovery

RF Protect

1. Rogue & Interfering APs

    A. Detection

    B. Classification

    C. Containment

2. Licensing

Troubleshooting

1. Client Connectivity

    A. User connection

    B. AP status

2. Aruba platform

    A. Layer 2 connectivity

    B. Layer 3 connectivity

    C. Licensing

    D. AP counts

    E. Firewall policy

    F. Role derivation

    G. Master/local connectivity

    H. AP connectivity

    I. DHCP

    J. Controller IP

3. Infrastructure

    A. Intervening ACLs

    B. DHCP

Applications and Solutions

1. RAP

    A. Configuration

    B. Licensing

    C. Operation modes

    D. Forwarding modes

    E. Maintenance

    F. Zero Touch provisioning

2. Mesh

    A. Mesh topology

    B. Configuration

    C. Licensing

    D. Remote Mesh portal

3. Location

    A. Locating a client

    B. AP design for location

    C. Location functionality

SAMPLE QUESTIONS

1. Which dual radio access point models support concurrent operations in the 2.4Ghz band as well as the 5Ghz band? (Choose three)

    A. AP-92

    B. AP-93

    C. AP-105

    D. AP-224

    E. AP-135

2. With CPSec enabled, which tunnel protocol is used between APs and Controllers in an Aruba environment?

    A. EAP

    B. SSH

    C. IPinIP

    D. Mobile IP

    E. IPSec

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

    E. No role

4. Which tunnel protocol is used between controllers to support Layer 2 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 5-GHz radios

   B. Disabled by default

   C. Balances client load across available channels/APs

   D. Enabled by default

   E. Balances mgr frames

6. Which ARM feature aids in steering "sticky clients" to associate to an AP with better 802.11 signal quality?

   A. Co-Channel interference mitigation

   B. Airtime Fairness

   C. ClientMatch

   D. Coordinated access to a single channel

   E. Band Steering

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

   E. DG 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

12. Which of the following licenses can be included in the Centralized licensing pool on the License Server? (Choose three)

A. Factory installed licenses

B. PEFNG licenses

C. Evaluation licenses

D. RFProtect Licenses

E. PEFV license

13. What AP redundancy model between 2 local controllers builds simultaneous tunnels between the AP and both controllers?

A. Fast Failover

B. Configure the locals as remote nodes

C. Use named VLANS

D. LMS and Backup LMS IP

E. AP Redundancy can only be configured between a Master and Local

Answers to odd numbered questions:

1 – C,D,E 3 – D
5 – B,C 7 – A
9 – A,B 11 – C
13 - A