APPENDIX D

Answers Appendix

Chapter 10

1. **B.** In this case, only RRM is lost. Clients may still roam within the FlexConnect group while in standalone mode, and only central authentication will be lost. Local authentication is still possible if it has been configured.
2. **C.** Because the application includes only wireless data applications, and because 10 APs are in use, the minimal bandwidth requirement is 128Kbps, and a minimum of 300 ms latency between the FlexConnect APs and the controller.
3. **C.** The missing step is to configured the WLAN for local switching. Without doing this from the WLAN configuration, all WLANs will be centrally switched.
4. **D.** FlexConnect groups are required to cache the keys locally, thus allowing fast roaming between APs.
5. **B, D.** CAPWAP message aggregation should be turned on to improve the performance of the CAPWAP control messages, and local authentication will use a local RADIUS server instead of relying on the central RADIUS server located over the WAN.
6. **C.** An ACL is required to identify which centrally switched traffic should have access to the local LAN. Answer A is incorrect because this changes the behavior of the centrally switched WLAN to be locally switched. Answer B is incorrect because NAT/PAT is automatically enabled by the split tunneling feature. Answer D is incorrect because split tunneling may be configured at either the AP or the FlexConnect group level.
7. **B.** Smart AP image upgrades will still function without a predefined master, but the master will be automatically selected based on the lowest MAC address from the APs in the FlexConnect group.
8. **B.** Office Extend APs use DTLS to secure communications between the AP and controller.
9. **A.** For an AP to be put into OEAP mode, it must first be converted to FlexConnect mode.