TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **PW0-200**

Title : Certified wireless security professional(cwsp)

Version : DEMO

1. Given: John Smith often telecommutes from a coffee shop near his home. The coffee shop has an 802.11g access point with a captive portal for authentication.

At this hotspot, John is susceptible to what types of WLAN attacks?

A. UDP port redirection

B. Wi-Fi phishing

C. Peer-to-peer

D. 802.11 reverse ARP

E. Eavesdropping/packet reassembly

F. Happy AP

Answer: BCE

2. Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

A. Provide wireless network access to users through specific access points, based on their 802.11e priority level.

B. Allow access to specific files and applications based on the user's IP subnet.

C. Allow specific user groups more bandwidth than others.

D. Allow simultaneous support of multiple EAP types on a single access point.

Answer: C

3. RFC 3748 specifies that the EAP-response/identity frame must comply with what criteria?

A. The EAP-response/identity frame must contain the user identity.

B. When TLS-tunneling mode is active, the EAP-response frame must have a blank user identity.

C. The EAP-response/identity frame must not contain a null identity value.

D. The user identity value must be hashed prior to insertion into the EAP-response identity frame.

Answer: C

4. What option specifies how the 802.11i Group Handshake differs from the 4-Way Handshake?

A. The Group Handshake has four messages like the 4-Way Handshake, except when it is performed after a reauthentication when it exhibits only three messages.

B. The Group Handshake is a 4-Way Handshake, but does not contain EAPoL Key frames.

C. The Group Handshake requires 6 exchanges, including the TCP 3-Way handshake traffic.

D. The Group Handshake has only two messages instead of four.

E. The Group Temporal Key (GTK) is always part of the Group Handshake, but never part of the 4-Way Handshake.

Answer: D

5. Once strong authentication and encryption mechanisms are implemented and tested in a WLAN, what options are needed to maintain a secure WLAN?

A. VPN

B. Internet firewall

C. WIPS

D. Personal firewalls

E. LDAP

Answer: CD

6. What protocols allow an administrator to securely transfer a new operating system image to a WLAN switch/controller?

A. SNMPv2c

B. HTTPS

C. SCP

D. TFTP

E. FTP

Answer: BC

7. Given: You manage a wireless network that services 100 wireless users. Your facility requires 7 access points, and you have installed an 802.11i-compliant implementation of 802.1X/LEAP (TKIP) as an authentication and encryption solution.

In this configuration, the wireless network is susceptible to what type of attack?

A. Man-in-the-middle

B. Password dictionary

C. Layer 3 peer-to-peer

D. WEP cracking

E. Session hijacking

F. Eavesdropping

Answer: B

8. Given: Most of today's lightweight (thin) access points support 802.3af and can be placed anywhere in the network infrastructure instead of directly connected to a WLAN switch/controller port. A lightweight access point can make what logical connection to its controller?

A. LLC port connection

B. GRE tunnel

C. RSVP protocol connection

D. HTTPS tunnel

E. Mobile IP connection

Answer: B

9. Given: ABC Company wants to install an 802.11g WLAN that supports fast roaming for 802.11b IP phones. A requirement is the ability to troubleshoot reassociations that are delayed or dropped during roaming. What is the most cost-effective system ABC Company can implement to meet the troubleshooting requirement?

A. WLAN protocol analyzer software on laptop computers

B. WLAN switch with integrated WIPS

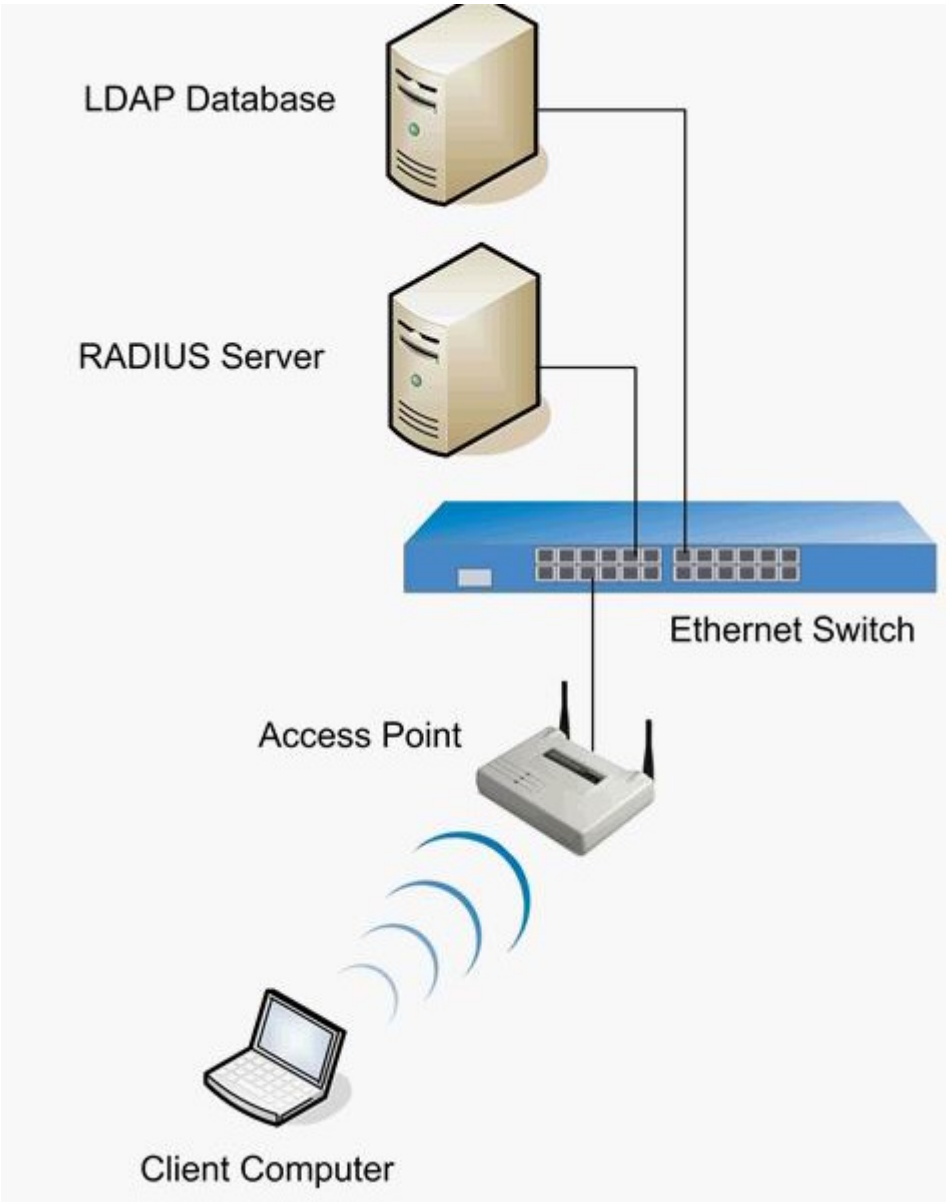
C. WLAN switch with dual lightweight 802.11a/b/g radios

D. Autonomous (thick) access points with a WIDS overlay system

E. Hybrid WLAN switch with integrated RF planning tool

Answer: B

10. Given: This network diagram implements an 802.1X/EAP-based wireless security solution. What device functions as the EAP Authenticator?



A. LDAP database

B. Client computer

C. Access point

D. RADIUS server

E. Ethernet switch

Answer: C

11. For WIPS to describe the location of a rogue WLAN device, what requirement must be part of the WIPS installation?

A. The predictive site survey results must be imported into the WIPS.

B. A GPS system must be installed including the coordinates of the building's corners.

C. All authorized AP radios must be placed in RF monitor mode so that the WIPS knows where the authorized APs are in relation to the WIPS sensors.

D. A graphical floor plan diagram must be imported into the WIPS.

Answer: D

12. Given: XYZ Company has recently installed a WLAN switch and RADIUS server and needs to move authenticated wireless users from various departments onto their designated network segments. How should this be accomplished?

A. The RADIUS server coordinates with an authenticated DHCP server.

B. Manually map each wireless user's MAC address to a VLAN number in the Ethernet switch.

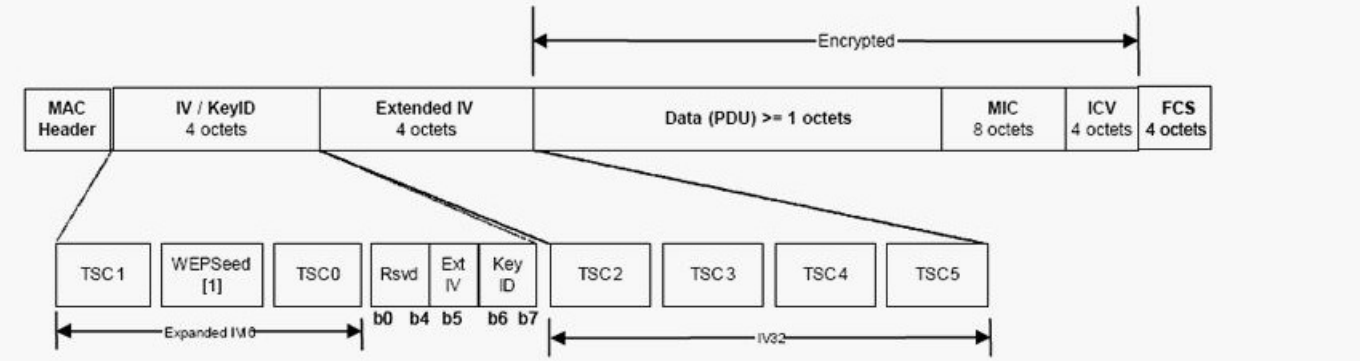
C. Implement multiple 802.1Q VLANs in both the WLAN and Ethernet switches.

D. RADIUS will send a return list attribute with the GRE tunnel number to the WLAN switch.

E. The WLAN user must contact the network administrator at step 4 of the 802.1X/EAP authentication process to receive a network number.

Answer: C

13. Given: The Wi-Fi Alliance implemented TKIP as an upgrade to WEP as part of WPA. The illustration shows an expanded TKIP MPDU. What features were included in TKIP to enhance the security of WEP?



A. FCS

B. ICV

C. MIC

D. Extended IV

E. Encrypted PDU

Answer: CD

14. Given: A new access point is connected to an authorized network segment and is detected by a WIPS. What does the WIPS apply to the new access point?

A. Default security policy

B. FIPS values

C. Site survey template

D. User property profile

E. Updated firmware

F. SNMP MIB

Answer: A

15. Given: Your company has just completed installation of a WLAN switch/controller with 10 lightweight (thin) access points. The Chief Security Officer has specified 802.11i compliant PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication and encryption scheme. Where must the x.509 server certificate reside in this network?

A. Supplicant devices

B. LDAP server

C. RADIUS server

D. WLAN switch/controller

E. Lightweight access points

Answer: AC

16. What wireless authentication technologies build a TLS-encrypted tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server?

A. MS-CHAPv2

B. EAP-FAST

C. LEAP

D. PEAPv1/EAP-GTC

E. EAP-MD5

F. EAP-TTLS

Answer: DF

17. How does a wireless network management system (WNMS) discover WLAN usernames?

A. The WNMS finds the MAC address of the wireless client device in the authentication database and parses the username from the entry.

B. The WNMS polls access points using SNMP.

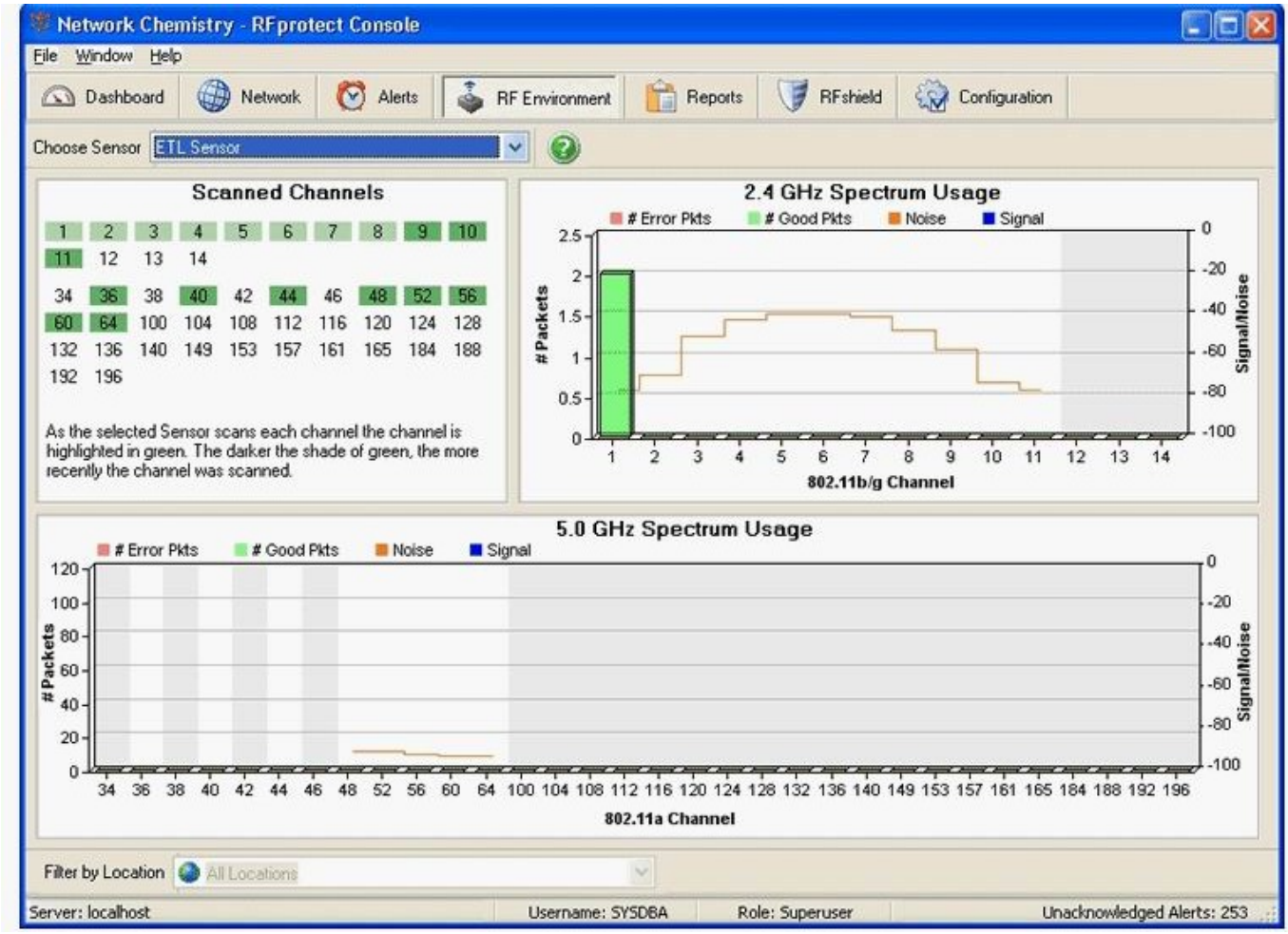
C. The client device sends the username to the WNMS on port 113 (ident service) after successful authentication.

D. The RADIUS server sends the username to the WNMS after the wireless device successfully authenticates.

E. The WNMS captures the username by sniffing the wireless network during the authentication process.

Answer: B

18. What is illustrated by this Wireless Intrusion Prevention System (WIPS)?



A. 802.11a access points on channels 34, 38, 42, and 46

B. Wideband RF jamming attack

C. Only channels 9, 10, and 11 are enabled on the access point

D. An access point on channel 6

E. Use of channels 12-14 is not allowed

Answer: B

19. Given: A university is installing a WLAN switch/controller and one thousand 802.11a/g lightweight access points. In this environment, how should the WLAN switch/controller connect to the Ethernet network?

A. The WLAN switch/controller should connect between every Layer 3 distribution Ethernet switch and every Layer 2 access Ethernet switch by having one port in each VLAN.

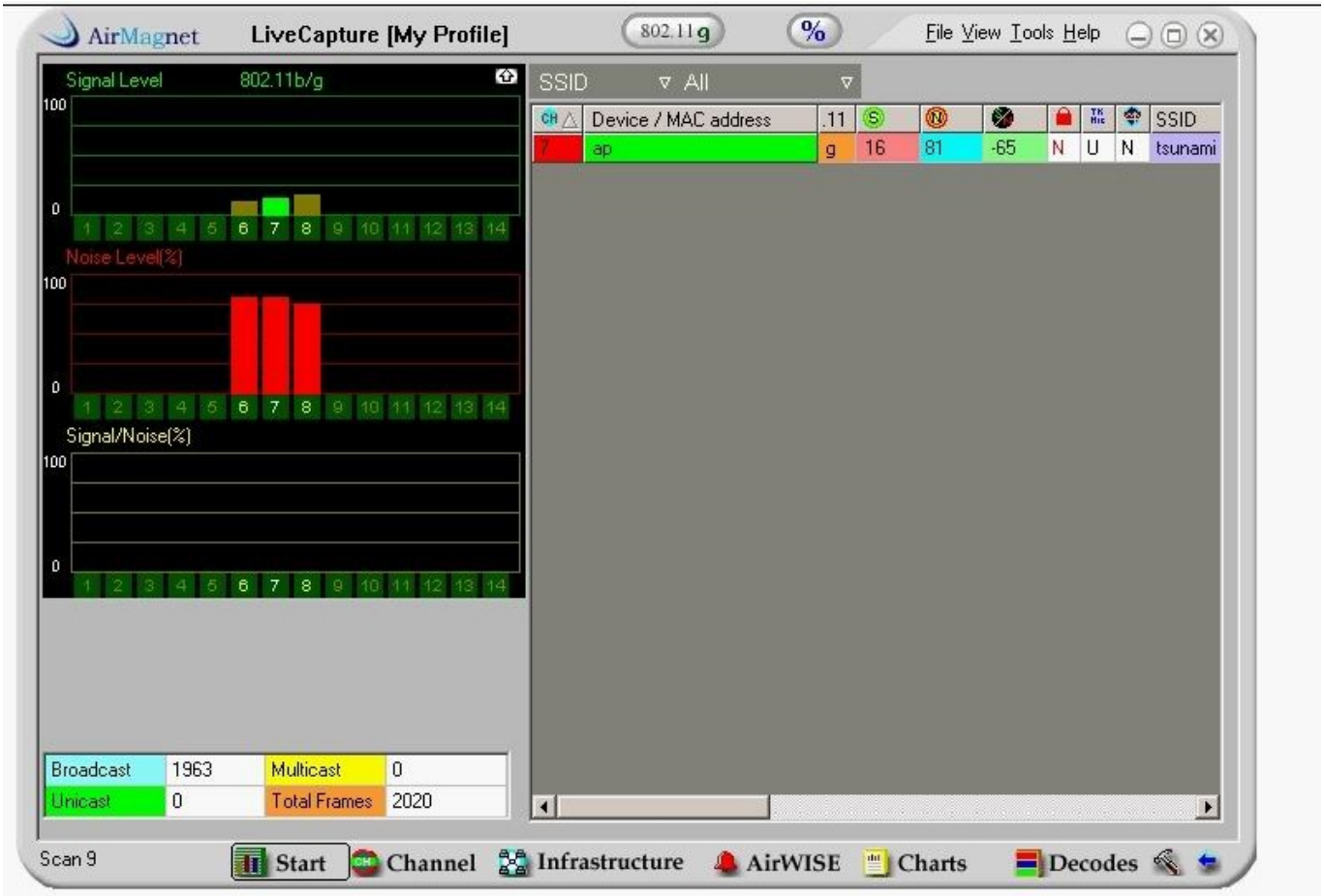
B. The WLAN switch/controller should connect to the core Layer 3 switch via a gigabit (or faster) Ethernet segment.

C. The WLAN switch/controller should be connected between the Layer 3 core Ethernet switch/controller and the corporate Internet firewall using a 100 Mbps connection.

D. The WLAN switch/controller should connect to a Layer 3 distribution switch in a wireless VLAN using a gigabit (or faster) connection.

Answer: B

20. What type of WLAN attack is illustrated on the 802.11 protocol analyzer screenshot?



A. Man-in-the-middle

B. Frame injection

C. RF jamming

D. Authentication flood

E. Hijacking

Answer: C