"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

**www.atmicnetworks .com**

Warning: Keep connected with our support team for latest updates

Topic 1, Vulnerabilities, Threats, and Attacks

## Question: 1

Given: John Smith uses a coffee shop's Internet hot-spot (no authentication or encryption) to transfer funds between his checking and savings accounts at his bank's website. The bank's website uses the HTTPS protocol to protect sensitive account information. While John was using the hot-spot, a hacker was able to obtain John's bank account user ID and password and exploit this information.

What likely scenario could have allowed the hacker to obtain John's bank account user ID and password?

A. John's bank is using an expired X.509 certificate on their web server. The certificate is on John's Certificate Revocation List (CRL), causing the user ID and password to be sent unencrypted.
B. John uses the same username and password for banking that he does for email. John used a POP3 email client at the wireless hot-spot to check his email, and the user ID and password were not encrypted.
C. John accessed his corporate network with his IPSec VPN software at the wireless hot-spot. An IPSec VPN only encrypts data, so the user ID and password were sent in clear text. John uses the same username and password for banking that he does for his IPSec VPN software.
D. The bank's web server is using an X.509 certificate that is not signed by a root CA, causing the user ID and password to be sent unencrypted.
E. Before connecting to the bank's website, John's association to the AP was hijacked. The attacker intercepted the HTTPS public encryption key from the bank's web server and has decrypted John's login credentials in near real-time.

**Answer: B**

## Question: 2

What type of WLAN attack is prevented with the use of a per-MPDU TKIP sequence counter (TSC)?

A. Weak-IV
B. Forgery
C. Replay
D. Bit-flipping
E. Session hijacking

**Answer: C**

## Question: 3

What 802.11 WLAN security problem is directly addressed by mutual authentication?

A. Wireless hijacking attacks
B. Weak password policies
C. MAC spoofing
D. Disassociation attacks
E. Offline dictionary attacks

F. Weak Initialization Vectors

**Answer: A**

## Question: 4

ABC Company uses the wireless network for highly sensitive network traffic. For that reason, they intend to protect their network in all possible ways. They are continually researching new network threats and new preventative measures. They are interested in the security benefits of 802.11w, but would like to know its limitations.

What types of wireless attacks are protected by 802.11w? (Choose 2)

A. RF DoS attacks
B. Layer 2 Disassociation attacks
C. Robust management frame replay attacks
D. Social engineering attacks

**Answer: B, C**

## Question: 5

You are configuring seven APs to prevent common security attacks. The APs are to be installed in a small business and to reduce costs, the company decided to install all consumer-grade wireless routers. The wireless routers will connect to a switch, which connects directly to the Internet connection providing 50 Mbps of Internet bandwidth that will be shared among 53 wireless clients and 17 wired clients.

To ensure the wireless network is as secure as possible from common attacks, what security measure can you implement given only the hardware referenced?

A. WPA-Enterprise
B. 802.1X/EAP-PEAP
C. WPA2-Enterprise
D. WPA2-Personal

**Answer: D**

## Question: 6

A WLAN is implemented using WPA-Personal and MAC filtering.

To what common wireless network attacks is this network potentially vulnerable? (Choose 3)

A. Offline dictionary attacks
B. MAC Spoofing
C. ASLEAP
D. DoS

**Answer: A, B, D**

## Question: 7

An attack is under way on the network. The attack is preventing users from accessing resources required for business operations, but the attacker has not gained access to any files or dat a. What kind of attack is described?

A. Man-in-the-middle
B. Hijacking
C. ASLEAP
D. DoS

**Answer: D**

## Question: 8

Given: WLAN attacks are typically conducted by hackers to exploit a specific vulnerability within a network.

What statement correctly pairs the type of WLAN attack with the exploited vulnerability? (Choose 3)

A. Management interface exploit attacks are attacks that use social engineering to gain credentials from managers.
B. Zero-day attacks are always authentication or encryption cracking attacks.
C. RF DoS attacks prevent successful wireless communication on a specific frequency or frequency range.
D. Hijacking attacks interrupt a user's legitimate connection and introduce a new connection with an evil twin AP.
E. Social engineering attacks are performed to collect sensitive information from unsuspecting users
F. Association flood attacks are Layer 3 DoS attacks performed against authenticated client stations

**Answer: C, D, E**

## Question: 9

Given: One of the security risks introduced by WPA2-Personal is an attack conducted by an authorized network user who knows the passphrase. In order to decrypt other users' traffic, the attacker must obtain certain information from the 4-way handshake of the other users.

In addition to knowing the Pairwise Master Key (PMK) and the supplicant's address (SA), what other three inputs must be collected with a protocol analyzer to recreate encryption keys? (Choose 3)

A. Authenticator nonce
B. Supplicant nonce
C. Authenticator address (BSSID)
D. GTKSA
E. Authentication Server nonce

**Answer: A, B, C**

## Question: 10

What is a primary criteria for a network to qualify as a Robust Security Network (RSN)?

A. Token cards must be used for authentication.
B. Dynamic WEP-104 encryption must be enabled.
C. WEP may not be used for encryption.
D. WPA-Personal must be supported for authentication and encryption.
E. WLAN controllers and APs must not support SSHv1.

**Answer: C**

## Question: 11

Given: You are using a Wireless Aggregator utility to combine multiple packet captures. One capture exists for each of channels 1, 6 and 11. What kind of troubleshooting are you likely performing with such a tool?

A. Wireless adapter failure analysis.
B. Interference source location.
C. Fast secure roaming problems.
D. Narrowband DoS attack detection.

**Answer: C**

## Question: 12

Which of the following security attacks cannot be detected by a WIPS solution of any kind? (Choose 2)

A. Rogue APs
B. DoS
C. Eavesdropping
D. Social engineering

**Answer: C, D**

## Question: 13

Given: You have a Windows laptop computer with an integrated, dual-band, Wi-Fi compliant adapter. Your laptop computer has protocol analyzer software installed that is capable of capturing and decoding 802.11ac data.

What statement best describes the likely ability to capture 802.11ac frames for security testing purposes?

A. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the

Radio Tap Header.

B. Integrated 802.11ac adapters are not typically compatible with protocol analyzers in Windows laptops. It is often best to use a USB adapter or carefully select a laptop with an integrated adapter that will work.

C. Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.

D. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.

E. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

**Answer: B**

## Question: 14

In order to acquire credentials of a valid user on a public hot-spot network, what attacks may be conducted? Choose the single completely correct answer.

A. Social engineering and/or eavesdropping

B. RF DoS and/or physical theft

C. MAC denial of service and/or physical theft

D. Authentication cracking and/or RF DoS

E. Code injection and/or XSS

**Answer: A**

## Question: 15

What WLAN client device behavior is exploited by an attacker during a hijacking attack?

A. When the RF signal between a client and an access point is disrupted for more than a few seconds, the client device will attempt to associate to an access point with better signal quality.

B. When the RF signal between a client and an access point is lost, the client will not seek to reassociate with another access point until the 120 second hold down timer has expired.

C. After the initial association and 4-way handshake, client stations and access points do not need to perform another 4-way handshake, even if connectivity is lost.

D. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.

E. Client drivers scan for and connect to access points in the 2.4 GHz band before scanning the 5 GHz band.

**Answer: A**

## Question: 16

What software and hardware tools are used together to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network? (Choose 2)

A. RF jamming device and a wireless radio card

B. A low-gain patch antenna and terminal emulation software

C. A wireless workgroup bridge and a protocol analyzer
D. DHCP server software and access point software
E. MAC spoofing software and MAC DoS software

**Answer: A, D**

## Question: 17

Given: Many computer users connect to the Internet at airports, which often have 802.11n access points with a captive portal for authentication.

While using an airport hot-spot with this security solution, to what type of wireless attack is a user susceptible? (Choose 2)

A. Man-in-the-Middle
B. Wi-Fi phishing
C. Management interface exploits
D. UDP port redirection
E. IGMP snooping

**Answer: A, B**

## Question: 18

Given: During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text.

From a security perspective, why is this significant?

A. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
B. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.
C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
D. The username can be looked up in a dictionary file that lists common username/password combinations.

**Answer: B**

## Question: 19

Given: In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2-Personal.

What statement about the WLAN security of this company is true?

A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
B. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary

attack and the capture of the latest 4-Way Handshake for each client.

C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.

D. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.

E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.

**Answer: B**

## Question: 20

Given: The Aircrack-ng WLAN software tool can capture and transmit modified 802.11 frames over the wireless network. It comes pre-installed on Kali Linux and some other Linux distributions.

What are three uses for such a tool? (Choose 3)

A. Transmitting a deauthentication frame to disconnect a user from the AP.

B. Auditing the configuration and functionality of a WIPS by simulating common attack sequences

C. Probing the RADIUS server and authenticator to expose the RADIUS shared secret

D. Cracking the authentication or encryption processes implemented poorly in some WLANs

**Answer: A, B, D**

## Question: 21

Given: You manage a wireless network that services 200 wireless users. Your facility requires 20 access points, and you have installed an IEEE 802.11-compliant implementation of 802.1X/LEAP with AES-CCMP as an authentication and encryption solution.

In this configuration, the wireless network is initially susceptible to what type of attacks? (Choose 2)

A. Encryption cracking

B. Offline dictionary attacks

C. Layer 3 peer-to-peer

D. Application eavesdropping

E. Session hijacking

F. Layer 1 DoS

**Answer: B, F**

## Question: 22

Given: ABC Corporation is evaluating the security solution for their existing WLAN. Two of their supported solutions include a PPTP VPN and 802.1X/LEAP. They have used PPTP VPNs because of their wide support in server and desktop operating systems. While both PPTP and LEAP adhere to the minimum requirements of the corporate security policy, some individuals have raised concerns about MS-CHAPv2 (and similar)

authentication and the known fact that MS-CHAPv2 has proven vulnerable in improper implementations.

As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication? (Choose 2)

A. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
B. MS-CHAPv2 is subject to offline dictionary attacks.
C. LEAP's use of MS-CHAPv2 is only secure when combined with WEP.
D. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.
E. MS-CHAPv2 uses AES authentication, and is therefore secure.
F. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.

**Answer: B, D**

## Question: 23

You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

A. 802.1X/EAP-TTLS
B. Open 802.11 authentication with IPSec
C. 802.1X/PEAPv0/MS-CHAPv2
D. WPA2-Personal with AES-CCMP
E. EAP-MD5

**Answer: B**

## Question: 24

Given: In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections. XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices.

With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

A. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.
B. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.
C. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the software AP.

D. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.

**Answer: C**

Topic 2, Security Policy

## Question: 25

What elements should be addressed by a WLAN security policy? (Choose 2)

A. Enabling encryption to prevent MAC addresses from being sent in clear text
B. How to prevent non-IT employees from learning about and reading the user security policy
C. End-user training for password selection and acceptable network use
D. The exact passwords to be used for administration interfaces on infrastructure devices
E. Social engineering recognition and mitigation techniques

**Answer: C, E**

## Question: 26

As a part of a large organization's security policy, how should a wireless security professional address the problem of rogue access points?

A. Use a WPA2-Enterprise compliant security solution with strong mutual authentication and encryption for network access of corporate devices.
B. Hide the SSID of all legitimate APs on the network so that intruders cannot copy this parameter on rogue APs.
C. Conduct thorough manual facility scans with spectrum analyzers to detect rogue AP RF signatures.
D. A trained employee should install and configure a WIPS for rogue detection and response measures.
E. Enable port security on Ethernet switch ports with a maximum of only 3 MAC addresses on each port.

**Answer: D**

## Question: 27

In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking?

A. In home networks in which file and printer sharing is enabled
B. At public hot-spots in which many clients use diverse applications
C. In corporate Voice over Wi-Fi networks with push-to-talk multicast capabilities
D. In university environments using multicast video training sourced from professor's laptops

**Answer: B**

## Question: 28

As the primary security engineer for a large corporate network, you have been asked to author a new security

policy for the wireless network. While most client devices support 802.1X authentication, some legacy devices still only support passphrase/PSK-based security methods.

When writing the 802.11 security policy, what password-related items should be addressed?

A. MSCHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.
B. Password complexity should be maximized so that weak WEP IV attacks are prevented.
C. Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK- based authentication.
D. Certificates should always be recommended instead of passwords for 802.11 client authentication.
E. EAP-TLS must be implemented in such scenarios.

**Answer: C**

## Question: 29

Given: ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN.

Before creating the WLAN security policy, what should you ensure you possess?

A. Awareness of the exact vendor devices being installed
B. Management support for the process
C. End-user training manuals for the policies to be created
D. Security policy generation software

**Answer: B**

## Question: 30

What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hot-spots?

A. Require Port Address Translation (PAT) on each laptop.
B. Require secure applications such as POP, HTTP, and SSH.
C. Require VPN software for connectivity to the corporate network.
D. Require WPA2-Enterprise as the minimal WLAN security solution.

**Answer: C**

Topic 3, WLAN Security Design and Architecture

## Question: 31

What is one advantage of using EAP-TTLS instead of EAP-TLS as an authentication mechanism in an 802.11 WLAN?

A. EAP-TTLS sends encrypted supplicant credentials to the authentication server, but EAP-TLS uses

unencrypted user credentials.

B. EAP-TTLS supports client certificates, but EAP-TLS does not.

C. EAP-TTLS does not require an authentication server, but EAP-TLS does.

D. EAP-TTLS does not require the use of a certificate for each STA as authentication credentials, but EAP-TLS does.

**Answer: D**

## Question: 32

What wireless authentication technologies may build a TLS tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)

A. EAP-MD5

B. EAP-TLS

C. LEAP

D. PEAPv0/MSCHAPv2

E. EAP-TTLS

**Answer: B, D, E**

## Question: 33

While performing a manual scan of your environment using a spectrum analyzer on a laptop computer, you notice a signal in the real time FFT view. The signal is characterized by having peak power centered on channel 11 with an approximate width of 20 MHz at its peak. The signal widens to approximately 40 MHz after it has weakened by about 30 dB.

What kind of signal is displayed in the spectrum analyzer?

A. A frequency hopping device is being used as a signal jammer in 5 GHz

B. A low-power wideband RF attack is in progress in 2.4 GHz, causing significant 802.11 interference C. An 802.11g AP operating normally in 2.4 GHz

D. An 802.11a AP operating normally in 5 GHz

**Answer: C**

## Question: 34

You are using a protocol analyzer for random checks of activity on the WLAN. In the process, you notice two different EAP authentication processes. One process (STA1) used seven EAP frames (excluding ACK frames) before the 4-way handshake and the other (STA2) used 11 EAP frames (excluding ACK frames) before the 4-way handshake.

Which statement explains why the frame exchange from one STA required more frames than the frame exchange from another STA when both authentications were successful? (Choose the single most probable answer given a stable WLAN.)

A. STA1 and STA2 are using different cipher suites.
B. STA2 has retransmissions of EAP frames.
C. STA1 is a reassociation and STA2 is an initial association.
D. STA1 is a TSN, and STA2 is an RSN.
E. STA1 and STA2 are using different EAP types.

**Answer: E**

## Question: 35

Given: ABC Corporation's 802.11 WLAN is comprised of a redundant WLAN controller pair (N+1) and 30 access points implemented in 2004. ABC implemented WEP encryption with IPSec VPN technology to secure their wireless communication because it was the strongest security solution available at the time it was implemented. IT management has decided to upgrade the WLAN infrastructure and implement Voice over Wi-Fi and is concerned with security because most Voice over Wi-Fi phones do not support IPSec.

As the wireless network administrator, what new security solution would be best for protecting ABC's data?

A. Migrate corporate data clients to WPA-Enterprise and segment Voice over Wi-Fi phones by assigning them to a different frequency band.
B. Migrate corporate data and Voice over Wi-Fi devices to WPA2-Enterprise with fast secure roaming support, and segment Voice over Wi-Fi data on a separate VLAN.
C. Migrate to a multi-factor security solution to replace IPSec; use WEP with MAC filtering, SSID hiding, stateful packet inspection, and VLAN segmentation.
D. Migrate all 802.11 data devices to WPA-Personal, and implement a secure DHCP server to allocate addresses from a segmented subnet for the Voice over Wi-Fi phones.

**Answer: B**

## Question: 36

Given: The ABC Corporation currently utilizes an enterprise Public Key Infrastructure (PKI) to allow employees to securely access network resources with smart cards. The new wireless network will use WPA2-Enterprise as its primary authentication solution. You have been asked to recommend a Wi-Fi Alliance-tested EAP method.

What solutions will require the least change in how users are currently authenticated and still integrate with their existing PKI?

A. EAP-FAST
B. EAP-TLS
C. PEAPv0/EAP-MSCHAPv2

D. LEAP
E. PEAPv0/EAP-TLS
F. EAP-TTLS/MSCHAPv2

**Answer: B**

## Question: 37

What statement accurately describes the functionality of the IEEE 802.1X standard?

A. Port-based access control with EAP encapsulation over the LAN (EAPoL)
B. Port-based access control with dynamic encryption key management and distribution
C. Port-based access control with support for authenticated-user VLANs only
D. Port-based access control with mandatory support of AES-CCMP encryption
E. Port-based access control, which allows three frame types to traverse the uncontrolled port: EAP, DHCP, and DNS.

**Answer: A**

## Question: 38

In the IEEE 802.11-2012 standard, what is the purpose of the 802.1X Uncontrolled Port?

A. To allow only authentication frames to flow between the Supplicant and Authentication Server
B. To block authentication traffic until the 4-Way Handshake completes
C. To pass general data traffic after the completion of 802.11 authentication and key management
D. To block unencrypted user traffic after a 4-Way Handshake completes

**Answer: A**

## Question: 39

Given: An 802.1X/EAP implementation includes an Active Directory domain controller running Windows Server 2012 and an AP from a major vendor. A Linux server is running RADIUS and it queries the domain controller for user credentials. A Windows client is accessing the network.

What device functions as the EAP Supplicant?

A. Linux server
B. Windows client
C. Access point
D. Windows server
E. An unlisted switch
F. An unlisted WLAN controller

**Answer: B**

## Question: 40

What wireless security protocol provides mutual authentication without using an X.509 certificate?

A. EAP-FAST
B. EAP-MD5
C. EAP-TLS
D. PEAPv0/EAP-MSCHAPv2
E. EAP-TTLS
F. PEAPv1/EAP-GTC

**Answer: A**

## Question: 41

Given: ABC Company has 20 employees and only needs one access point to cover their entire facility. Ten of ABC Company's employees have laptops with radio cards capable of only WPA security. The other ten employees have laptops with radio cards capable of WPA2 security. The network administrator wishes to secure all wireless communications (broadcast and unicast) for each laptop with its strongest supported security mechanism, but does not wish to implement a RADIUS/AAA server due to complexity.

What security implementation will allow the network administrator to achieve this goal?

A. Implement an SSID with WPA2-Personal that allows both AES-CCMP and TKIP clients to connect.
B. Implement an SSID with WPA-Personal that allows both AES-CCMP and TKIP clients to connect.
C. Implement two separate SSIDs on the AP—one for WPA-Personal using TKIP and one for WPA2- Personal using AES-CCMP.
D. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AES-CCMP and unicast traffic using either TKIP or AES-CCMP.

**Answer: C**

## Question: 42

What disadvantage does EAP-TLS have when compared with PEAPv0 EAP/MSCHAPv2 as an 802.11 WLAN security solution?

A. Fast/secure roaming in an 802.11 RSN is significantly longer when EAP-TLS is in use.
B. EAP-TLS does not protect the client's username and password inside an encrypted tunnel.
C. EAP-TLS cannot establish a secure tunnel for internal EAP authentication.
D. EAP-TLS is supported only by Cisco wireless infrastructure and client devices.
E. EAP-TLS requires extensive PKI use to create X.509 certificates for both the server and all clients, which increases administrative overhead.

**Answer: E**

## Question: 43

Given: You are using WEP as an encryption solution. You are using VLANs for network segregation.

Why can you not establish an RSNA?

A. RSNA connections require TKIP or CCMP.
B. RSNA connections require BIP and do not support TKIP, CCMP or WEP.
C. RSNA connections require CCMP and do not support TKIP or WEP.
D. RSNA connections do not work in conjunction with VLANs.

**Answer: A**

## Question: 44

When used as part of a WLAN authentication solution, what is the role of LDAP?

A. A data retrieval protocol used by an authentication service such as RADIUS
B. An IEEE X.500 standard compliant database that participates in the 802.1X port-based access control process
C. A SQL compliant authentication service capable of dynamic key generation and distribution
D. A role-based access control protocol for filtering data to/from authenticated stations.
E. An Authentication Server (AS) that communicates directly with, and provides authentication for, the Supplicant.

**Answer: A**

## Question: 45

When implementing a WPA2-Enterprise security solution, what protocol must the selected RADIUS server support?

A. LWAPP, GRE, or CAPWAP
B. IPSec/ESP
C. EAP
D. CCMP and TKIP
E. LDAP

**Answer: C**

## Question: 46

Given: XYZ Company has recently installed an 802.11ac WLAN. The company needs the ability to control access

to network services, such as file shares, intranet web servers, and Internet access based on an employee's job responsibilities.

What WLAN security solution meets this requirement?

A. An autonomous AP system with MAC filters
B. WPA2-Personal with support for LDAP queries
C. A VPN server with multiple DHCP scopes
D. A WLAN controller with RBAC features
E. A WLAN router with wireless VLAN support

**Answer: D**

## Question: 47

Given: Your network includes a controller-based WLAN architecture with centralized data forwarding. The AP builds an encrypted tunnel to the WLAN controller. The WLAN controller is uplinked to the network via a trunked 1 Gbps Ethernet port supporting all necessary VLANs for management, control, and client traffic.

What processes can be used to force an authenticated WLAN client's data traffic into a specific VLAN as it exits the WLAN controller interface onto the wired uplink? (Choose 3)

A. On the Ethernet switch that connects to the AP, configure the switch port as an access port (not trunking) in the VLAN of supported clients.
B. During 802.1X authentication, RADIUS sends a return list attribute to the WLAN controller assigning the user and all traffic to a specific VLAN.
C. In the WLAN controller's local user database, create a static username-to-VLAN mapping on the WLAN controller to direct data traffic from a specific user to a designated VLAN.
D. Configure the WLAN controller with static SSID-to-VLAN mappings; the user will be assigned to a VLAN according to the SSID being used.

**Answer: B, C, D**

## Question: 48

What is the purpose of the Pairwise Transient Key (PTK) in IEEE 802.11 Authentication and Key Management?

A. The PTK is a type of master key used as an input to the GMK, which is used for encrypting multicast data frames.
B. The PTK contains keys that are used to encrypt unicast data frames that traverse the wireless medium.
C. The PTK is XOR'd with the PSK on the Authentication Server to create the AAA key.
D. The PTK is used to encrypt the Pairwise Master Key (PMK) for distribution to the 802.1X Authenticator prior to the 4-Way Handshake.

**Answer: B**

## Question: 49

Which one of the following describes the correct hierarchy of 802.1X authentication key derivation?

A. The MSK is generated from the 802.1X/EAP authentication. The PMK is derived from the MSK. The PTK is derived from the PMK, and the keys used for actual data encryption are a part of the PTK.

B. If passphrase-based client authentication is used by the EAP type, the PMK is mapped directly from the user's passphrase. The PMK is then used during the 4-way handshake to create data encryption keys.

C. After successful EAP authentication, the RADIUS server generates a PMK. A separate key, the MSK, is derived from the AAA key and is hashed with the PMK to create the PTK and GTK.

D. The PMK is generated from a successful mutual EAP authentication. When mutual authentication is not used, an MSK is created. Either of these two keys may be used to derive the temporal data encryption keys during the 4-way handshake.

**Answer: A**

## Question: 50

What statement is true regarding the nonces (ANonce and SNonce) used in the IEEE 802.11 4 Way Handshake?

A. Both nonces are used by the Supplicant and Authenticator in the derivation of a single PTK.

B. The Supplicant uses the SNonce to derive its unique PTK and the Authenticator uses the ANonce to derive its unique PTK, but the nonces are not shared.

C. Nonces are sent in EAPoL frames to indicate to the receiver that the sending station has installed and validated the encryption keys.

D. The nonces are created by combining the MAC addresses of the Supplicant, Authenticator, and Authentication Server into a mixing algorithm.

**Answer: A**

## Question: 51

When using the 802.1X/EAP framework for authentication in 802.11 WLANs, why is the 802.1X Controlled Port still blocked after the 802.1X/EAP framework has completed successfully?

A. The 802.1X Controlled Port is always blocked, but the Uncontrolled Port opens after the EAP authentication process completes.

B. The 802.1X Controlled Port remains blocked until an IP address is requested and accepted by the Supplicant.

C. The 4-Way Handshake must be performed before the 802.1X Controlled Port changes to the unblocked state.

D. The 802.1X Controlled Port is blocked until Vender Specific Attributes (VSAs) are exchanged inside a RADIUS packet between the Authenticator and Authentication Server.

**Answer: C**

## Question: 52

Given: ABC Company secures their network with WPA2-Personal authentication and AES-CCMP encryption.

What part of the 802.11 frame is always protected from eavesdroppers by this type of security?

A. All MSDU contents
B. All MPDU contents
C. All PPDU contents
D. All PSDU contents

**Answer: A**

## Question: 53

When TKIP is selected as the pairwise cipher suite, what frame types may be protected with data confidentiality? (Choose 2)

A. Robust broadcast management
B. Robust unicast management
C. Control
D. Data
E. ACK
F. QoS Data

**Answer: D, F**

## Question: 54

What statements are true about 802.11-2012 Protected Management Frames? (Choose 2)

A. 802.11w frame protection protects against some Layer 2 denial-of-service (DoS) attacks, but it cannot prevent all types of Layer 2 DoS attacks.
B. When frame protection is in use, the PHY preamble and header as well as the MAC header are encrypted with 256- or 512-bit AES.
C. Authentication, association, and acknowledgment frames are protected if management frame protection is enabled, but deauthentication and disassociation frames are not.
D. Management frame protection protects disassociation and deauthentication frames.

**Answer: A, D**

## Question: 55

Given: AAA is an architectural framework used to provide three separate security components in a network. Listed below are three phrases that each describe one aspect of the AAA framework.

Option-1 — This AAA function is performed first and validates user identify prior to determining the network resources to which they will be granted access.

Option-2 — This function is used for monitoring and auditing purposes and includes the collection of data that identifies what a user has done while connected.

Option-3 — This function is used to designate permissions to a particular user.

What answer correctly pairs the AAA component with the descriptions provided above?

A. Option-1 – Access Control Option-2 – Authorization Option-3 – Accounting

B. Option-1 – Authentication Option-2 – Accounting Option-3 – Association

C. Option-1 – Authorization Option-2 – Access Control Option-3 – Association

D. Option-1 – Authentication Option-2 – Accounting Option-3 – Authorization

**Answer: D**

## Question: 56

What security benefits are provided by endpoint security solution software? (Choose 3)

A. Can prevent connections to networks with security settings that do not conform to company policy

B. Can collect statistics about a user's network use and monitor network threats while they are connected

C. Can restrict client connections to networks with specific SSIDs and encryption types

D. Can be used to monitor for and prevent network attacks by nearby rogue clients or APs

**Answer: A, B, C**

## Question: 57

What drawbacks initially prevented the widespread acceptance and use of Opportunistic Key Caching (OKC)?

A. Sharing cached keys between controllers during inter-controller roaming created vulnerabilities that exposed the keys to attackers.

B. Because OKC is not defined by any standards or certification body, client support was delayed and sporadic early on.

C. Key exchanges during fast roams required processor-intensive cryptography, which was prohibitive for legacy devices supporting only TKIP.

D. The Wi-Fi Alliance continually delayed the creation of a client certification for OKC, even though it was defined by IEEE 802.11r.

**Answer: B**

## Question: 58

Given: When the CCMP cipher suite is used for protection of data frames, 16 bytes of overhead are added to the Layer 2 frame. 8 of these bytes comprise the MIC.

What purpose does the encrypted MIC play in protecting the data frame?

A. The MIC is used as a first layer of validation to ensure that the wireless receiver does not incorrectly process corrupted signals.
B. The MIC provides for a cryptographic integrity check against the data payload to ensure that it matches the original transmitted data.
C. The MIC is a hash computation performed by the receiver against the MAC header to detect replay attacks prior to processing the encrypted payload.
D. The MIC is a random value generated during the 4-way handshake and is used for key mixing to enhance the strength of the derived PTK.

**Answer: B**

## Question: 59

A single AP is configured with three separate WLAN profiles, as follows:
1. SSID: ABCData – BSSID: 00:11:22:00:1F:C3 – VLAN 10 – Security: PEAPv0/EAP-MSCHAPv2 with AES-CCMP – 3 current clients
2. SSID: ABCVoice – BSSID: 00:11:22:00:1F:C4 – VLAN 60 – Security: WPA2-Personal with AES-CCMP – 2 current clients
3. SSID: Guest – BSSID: 00:11:22:00:1F:C5 – VLAN 90 – Security: Open with captive portal authentication – 3 current clients

Three STAs are connected to ABCDat
a. Three STAs are connected to Guest. Two STAs are connected to ABCVoice.

How many unique GTKs and PTKs are currently in place in this scenario?

A. 1 GTK – 8 PTKs
B. 2 GTKs – 5 PTKs
C. 2 GTKs – 8 PTKs
D. 3 GTKs – 8 PTKs

**Answer: B**

## Question: 60

You have an AP implemented that functions only using 802.11-2012 standard methods for the WLAN communications on the RF side and implementing multiple SSIDs and profiles on the management side configured as follows:

1. SSID: Guest – VLAN 90 – Security: Open with captive portal authentication – 2 current clients
2. SSID: ABCData – VLAN 10 – Security: PEAPv0/EAP-MSCHAPv2 with AES-CCMP – 5 current clients
3. SSID: ABCVoice – VLAN 60 – Security: WPA2-Personal – 2 current clients

Two client STAs are connected to ABCData and can access a media server that requires authentication at the Application Layer and is used to stream multicast video streams to the clients.

What client stations possess the keys that are necessary to decrypt the multicast data packets carrying these videos?

A. Only the members of the executive team that are part of the multicast group configured on the media server
B. All clients thatare associated to the AP using the ABCData SSID
C. All clients thatare associated to the AP using any SSID
D. All clients thatare associated to the AP with a shared GTK, which includes ABCData and ABCVoice.

**Answer: B**

## Question: 61

What EAP type supports using MS-CHAPv2, EAP-GTC or EAP-TLS for wireless client authentication?

A. H-REAP
B. EAP-GTC
C. EAP-TTLS
D. PEAP
E. LEAP

**Answer: D**

## Question: 62

Given: You must implement 7 APs for a branch office location in your organization. All APs will be autonomous and provide the same two SSIDs (CORP1879 and Guest).

Because each AP is managed directly through a web-based interface, what must be changed on every AP before enabling the WLANs to ensure proper staging procedures are followed?

A. Fragmentation threshold
B. Administrative password
C. Output power
D. Cell radius

**Answer: B**

## Question: 63

Given: You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet. What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

A. User external antennas.
B. Use internal antennas.
C. Power the APs using PoE.
D. Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.

**Answer: D**

## Question: 64

Given: Fred works primarily from home and public wireless hot-spots rather than commuting to the office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN.

In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

A. Use an IPSec VPN for connectivity to the office network
B. Use only HTTPS when agreeing to acceptable use terms on public networks
C. Use enterprise WIPS on the corporate office network
D. Use WIPS sensor software on the laptop to monitor for risks and attacks
E. Use 802.1X/PEAPv0 to connect to the corporate office network from public hot-spots
F. Use secure protocols, such as FTP, for remote file transfers.

**Answer: A**

## Question: 65

What are the three roles of the 802.1X framework, as defined by the 802.1X standard, that are performed by the client STA, the AP (or WLAN controller), and the RADIUS server? (Choose 3)

A. Enrollee
B. Registrar
C. AAA Server
D. Authentication Server
E. Supplicant
F. Authenticator
G. Control Point

**Answer: D, E, F**

## Question: 66

What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

A. 32-bit ICV (CRC-32) B. Sequence counters C. RC5 stream cipher D. Michael
E. Block cipher support

**Answer: D**

## Question: 67

Which one of the following is a valid reason to avoid the use of EAP-MD5 in production WLANs?

A. It does not support the outer identity.
B. It is not a valid EAP type.
C. It does not support mutual authentication.
D. It does not support a RADIUS server.

**Answer: C**

## Question: 68

Given: Your organization is using EAP as an authentication framework with a specific type that meets the requirements of your corporate policies.

Which one of the following statements is true related to this implementation?

A. The client will be the authenticator in this scenario.
B. The client STAs must use a different, but complementary, EAP type than the AP STAs.
C. The client STAs may communicate over the uncontrolled port in order to authenticate as soon as Open System authentication completes.
D. The client STAs may communicate over the controlled port in order to authenticate as soon as the Open System authentication completes.

**Answer: C**

## Question: 69

Given: A WLAN consultant has just finished installing a WLAN controller with 15 controller-based APs. Two SSIDs with separate VLANs are configured for this network, and both VLANs are configured to use the same RADIUS server. The SSIDs are configured as follows:
SSID Blue - VLAN 10 - Lightweight EAP (LEAP) authentication - CCMP cipher suite
SSID Red - VLAN 20 - PEAPv0/EAP-TLS authentication - TKIP cipher suite
The consultant's computer can successfully authenticate and browse the Internet when using the Blue SSID. The same computer cannot authenticate when using the Red SSID.

What is a possible cause of the problem?

A. The Red VLAN does not use server certificate, but the client requires one.
B. The TKIP cipher suite is not a valid option for PEAPv0 authentication.
C. The client does not have a proper certificate installed for the tunneled authentication within the established TLS tunnel.
D. The consultant does not have a valid Kerberos ID on the Blue VLAN.

**Answer: C**

## Question: 70

Given: Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM.

What device functions as the 802.1X/EAP Authenticator?

A. SRV21
B. WLAN Controller/AP
C. MacBook Pro
D. RADIUS server

**Answer: B**

## Question: 71

When using a tunneled EAP type, such as PEAP, what component is protected inside the TLS tunnel so that it is not sent in clear text across the wireless medium?

A. X.509 certificates
B. User credentials
C. Server credentials
D. RADIUS shared secret

**Answer: B**

## Question: 72

What protocols allow a network administrator to securely manage the configuration of WLAN controllers and access points? (Choose 2)

A. SNMPv1
B. HTTPS
C. Telnet
D. TFTP
E. FTP

F. SSHv2

**Answer: B, F**

## Question: 73

Given: XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization.

What RADIUS features could be used by XYZ to assign the proper network permissions to users during authentication? (Choose 2)

A. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
B. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.
C. RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to-SSID mapping table in the LDAP user database.
D. RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.
E. RADIUS attributes can be used to assign permission levels, such as read-only permission, to users of a particular network resource.

**Answer: B, E**

## Question: 74

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

A. Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.
B. Allow access to specific files and applications based on the user's WMM access category.
C. Provide two or more user groups connected to the same SSID with different levels of network privileges.
D. Allow simultaneous support for multiple EAP types on a single access point.

**Answer: C**

## Question: 75

Given: A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user

authentication.

For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

A. WPA2-Enterprise authentication/encryption
B. Internal RADIUS server
C. WIPS support and integration
D. 802.1Q VLAN trunking
E. SNMPv3 support

**Answer: B**

## Question: 76

Given: ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC's preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources.

What security best practices should be followed in this deployment scenario?

A. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
B. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.
C. RADIUS services should be provided at branch offices so that authentication server and supplicant credentials are not sent over the Internet.
D. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.

**Answer: A**

## Question: 77

Given: ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication.

How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2-Enterprise WLAN security solution?

A. Import all users from the LDAP server into a RADIUS server with an LDAP-to-RADIUS conversion tool.
B. Implement an X.509 compliant Certificate Authority and enable SSL queries on the LDAP server.
C. Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily backups to synchronize the user databases.
D. Implement a RADIUS server and query user authentication requests through the LDAP server.

**Answer: D**

## Question: 78

Given: ABC Company has recently installed a WLAN controller and configured it to support WPA2- Enterprise security. The administrator has configured a security profile on the WLAN controller for each group within the company (Marketing, Sales, and Engineering).

How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller?

A. The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication.
B. The RADIUS server sends a group name return list attribute to the WLAN controller during every successful user authentication.
C. The RADIUS server forwards the request for a group attribute to an LDAP database service, and LDAP sends the group attribute to the WLAN controller.
D. The RADIUS server sends the list of authenticated users and groups to the WLAN controller as part of a 4-Way Handshake prior to user authentication.

**Answer: B**

## Question: 79

Given: ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication. According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection.

What security characteristics and/or components play a role in preventing data decryption? (Choose 2)

A. Multi-factor authentication
B. 4-Way Handshake
C. PLCP Cyclic Redundancy Check (CRC)
D. Encrypted Passphrase Protocol (EPP)
E. Integrity Check Value (ICV)
F. Group Temporal Keys

**Answer: B, F**

## Question: 80

The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?

A. Phase Shift Key (PSK)
B. Group Master Key (GMK)
C. Pairwise Master Key (PMK)
D. Group Temporal Key (GTK)

E. PeerKey (PK)
F. Key Confirmation Key (KCK)

**Answer: C**

## Question: 81

In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce? (Choose 2)

A. They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.
B. The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).
C. They are added together and used as the GMK, from which the GTK is derived.
D. They are input values used in the derivation of the Pairwise Transient Key.
E. They allow the participating STAs to create dynamic keys while avoiding sending unicast encryption keys across the wireless medium.

**Answer: D, E**

## Question: 82

Given: ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES-CCMP to secure their corporate wireless dat
a. They wish to implement a guest WLAN for guest users to have Internet access, but want to implement some security controls. The security requirements for the hot-spot include: Cannot access corporate network resources
Network permissions are limited to Internet access
All stations must be authenticated

What security controls would you suggest? (Choose the single best answer.)

A. Implement separate controllers for the corporate and guest WLANs.
B. Use a WIPS to deauthenticate guest users when their station tries to associate with the corporate WLAN.
C. Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.
D. Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.
E. Force all guest users to use a common VPN protocol to connect.

**Answer: D**

## Question: 83

The IEEE 802.11 standard defined Open System authentication as consisting of two auth frames and two assoc frames. In a WPA2-Enterprise network, what process immediately follows the 802.11 association procedure?

A. Group Key Handshake
B. 802.1X/EAP authentication
C. DHCP Discovery
D. 4-Way Handshake
E. Passphrase-to-PSK mapping
F. RADIUS shared secret lookup

**Answer: B**

## Question: 84

Given: Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAP-compliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server.

Where must the X.509 server certificate and private key be installed in this network?

A. Supplicant devices
B. LDAP server
C. Controller-based APs
D. WLAN controller
E. RADIUS server

**Answer: E**

## Question: 85

Given: You support a coffee shop and have recently installed a free 802.11ac wireless hot-spot for the benefit of your customers. You want to minimize legal risk in the event that the hot-spot is used for illegal Internet activity.

What option specifies the best approach to minimize legal risk at this public hot-spot while maintaining an open venue for customer Internet access?

A. Configure WPA2-Enterprise security on the access point
B. Block TCP port 25 and 80 outbound on the Internet router
C. Require client STAs to have updated firewall and antivirus software
D. Allow only trusted patrons to use the WLAN
E. Use a WIPS to monitor all traffic and deauthenticate malicious stations
F. Implement a captive portal with an acceptable use disclaimer

**Answer: F**

## Question: 86

You are using a utility that takes input and generates random output. For example, you can provide the input of a known word as a secret word and then also provide another known word as salt input. When you process the input it generates a secret code which is a combination of letters and numbers with case sensitivity. For what is the described utility used? (Choose 3)

A. Generating passwords for WLAN infrastructure equipment logins
B. Generating PMKs that can be imported into 802.11 RSN-compatible devices
C. Generating secret keys for RADIUS servers and WLAN infrastructure devices
D. Generating passphrases for WLAN systems secured with WPA2-Personal
E. Generating dynamic session keys used for IPSec VPNs

**Answer: A, C, D**

## Question: 87

Given: Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks.

In this deployment, what risks are still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering features enabled? (Choose 2)

A. Intruders can send spam to the Internet through the guest VLAN.
B. Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.
C. Unauthorized users can perform Internet-based network attacks through the WLAN.
D. Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols (e.g. Telnet, HTTP) are blocked.
E. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

**Answer: A, C**

## Question: 88

While seeking the source of interference on channel 11 in your 802.11n WLAN running within 2.4 GHz, you notice a signal in the spectrum analyzer real time FFT display. The signal is characterized with the greatest strength utilizing only 1-2 megahertz of bandwidth and it does not use significantly more bandwidth until it has weakened by roughly 20 dB. At approximately -70 dB, it spreads across

as much as 35 megahertz of bandwidth.

What kind of signal is described?

A. A high-power, narrowband signal
B. A 2.4 GHz WLAN transmission using transmit beam forming
C. An HT-OFDM access point
D. A frequency hopping wireless device in discovery mode
E. A deauthentication flood from a WIPS blocking an AP
F. A high-power ultra wideband (UWB) Bluetooth transmission

**Answer: A**

## Question: 89

Given: The Marketing department's WLAN users need to reach their file and email server as well as the Internet, but should not have access to any other network resources.

What single WLAN security feature should be implemented to comply with these requirements?

A. Mutual authentication
B. Captive portal
C. Role-based access control
D. Group authentication
E. RADIUS policy accounting

**Answer: C**

## Question: 90

You must support a TSN as you have older wireless equipment that will not support the required processing of AES encryption. Which one of the following technologies will you use on the network so that a TSN can be implemented that would not be required in a network compliant with 802.112012 non-deprecated technologies?

A. WEP
B. RC4
C. CCMP
D. WPA2

**Answer: B**

Topic 4, Security Lifecycle Management

## Question: 91

Given: XYZ Hospital plans to improve the security and performance of their Voice over Wi-Fi implementation and will be upgrading to 802.11n phones with 802.1X/EAP authentication. XYZ would like to support fast secure roaming for the phones and will require the ability to troubleshoot reassociations that are delayed or dropped during inter-channel roaming.

What portable solution would be recommended for XYZ to troubleshoot roaming problems?

A. WIPS sensor software installed on a laptop computer
B. Spectrum analyzer software installed on a laptop computer
C. An autonomous AP mounted on a mobile cart and configured to operate in monitor mode
D. Laptop-based protocol analyzer with multiple 802.11n adapters

**Answer: D**

## Question: 92

Wireless Intrusion Prevention Systems (WIPS) are used for what purposes? (Choose 3)

A. Performance monitoring and troubleshooting
B. Enforcing wireless network security policy
C. Detecting and defending against eavesdropping attacks
D. Security monitoring and notification
E. Preventing physical carrier sense attacks
F. Classifying wired client devices

**Answer: A, B, D**

## Question: 93

For a WIPS system to identify the location of a rogue WLAN device using location patterning (RF fingerprinting), what must be done as part of the WIPS installation?

A. All WIPS sensors must be installed as dual-purpose (AP/sensor) devices.
B. A location chipset (GPS) must be installed with it.
C. At least six antennas must be installed in each sensor.
D. The RF environment must be sampled during an RF calibration process.

**Answer: D**

## Question: 94

Given: A network security auditor is preparing to perform a comprehensive assessment of an 802.11ac network's security.

What task should be performed at the beginning of the audit to maximize the auditor's ability to expose network vulnerabilities?

A. Identify the IP subnet information for each network segment.
B. Identify the manufacturer of the wireless intrusion prevention system.
C. Identify the skill level of the wireless network security administrator(s).
D. Identify the manufacturer of the wireless infrastructure hardware.
E. Identify the wireless security solution(s) currently in use.

**Answer: E**

## Question: 95

Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAP PEAPv0. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS management console for connectivity to ABC's network before it was given to him. The WIPS termination policy includes alarms for rogue stations, roque APs, DoS attacks and unauthorized roaming.

What is a likely reason that Joe cannot connect to the network?

A. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.
B. Joe's integrated 802.11 radio is sending multiple Probe Request frames on each channel.
C. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. The WIPS responded by disabling the APs.
D. Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.

**Answer: A**

## Question: 96

The following numbered items show some of the contents of each of the four frames exchanged during the 4-way handshake:

1. Encrypted GTK sent
2. Confirmation of temporal key installation
3. Anonce sent from authenticator to supplicant
4. Snonce sent from supplicant to authenticator, MIC included

Arrange the frames in the correct sequence beginning with the start of the 4-way handshake.

A. 2, 3, 4, 1
B. 1, 2, 3, 4
C. 4, 3, 1, 2
D. 3, 4, 1, 2

**Answer: D**

## Question: 97

Given: You are the WLAN administrator in your organization and you are required to monitor the network and ensure all active WLANs are providing RSNs. You have a laptop protocol analyzer configured.

In what frame could you see the existence or non-existence of proper RSN configuration parameters for each BSS through the RSN IE?

A. Probe request

B. Beacon
C. RTS
D. CTS
E. Data frames

**Answer: B**

## Question: 98

What attack cannot be detected by a Wireless Intrusion Prevention System (WIPS)?

A. MAC Spoofing
B. Eavesdropping
C. Hot-spotter
D. Soft AP
E. Deauthentication flood
F. EAP flood

**Answer: B**

## Question: 99

What security vulnerabilities may result from a lack of staging, change management, and installation procedures for WLAN infrastructure equipment? (Choose 2)

A. The WLAN system may be open to RF Denial-of-Service attacks
B. WIPS may not classify authorized, rogue, and neighbor APs accurately
C. Authentication cracking of 64-bit Hex WPA-Personal PSK
D. Management interface exploits due to the use of default usernames and passwords for AP management
E. AES-CCMP encryption keys may be decrypted

**Answer: B, D**

## Question: 100

What field in the RSN information element (IE) will indicate whether PSK- or Enterprise-based WPA or WPA2 is in use?

A. AKM Suite List
B. Group Cipher Suite
C. RSN Capabilities
D. Pairwise Cipher Suite List

**Answer: A**

## Question: 101

What preventative measures are performed by a WIPS against intrusions?

A. EAPoL Reject frame flood against a rogue AP
B. Evil twin attack against a rogue AP
C. Deauthentication attack against a classified neighbor AP
D. ASLEAP attack against a rogue AP
E. Uses SNMP to disable the switch port to which rogue APs connect

**Answer: E**

## Question: 102

When monitoring APs within a LAN using a Wireless Network Management System (WNMS), what secure protocol may be used by the WNMS to issue configuration changes to APs?

A. IPSec/ESP
B. TFTP
C. 802.1X/EAP
D. SNMPv3
E. PPTP

**Answer: D**

## Question: 103

Given: WLAN protocol analyzers can read and record many wireless frame parameters.
What parameter is needed to physically locate rogue APs with a protocol analyzer?

A. SSID
B. IP Address
C. BSSID
D. Signal strength
E. RSN IE
F. Noise floor

**Answer: D**

## Question: 104

After completing the installation of a new overlay WIPS for the purpose of rogue detection and security monitoring at your corporate headquarters, what baseline function MUST be performed in order to identify security threats?

A. Authorized PEAP usernames must be added to the WIPS server's user database.
B. WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.
C. Separate security profiles must be defined for network operation in different regulatory domains D. Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.

**Answer: B**

## Question: 105

Given: A WLAN protocol analyzer trace reveals the following sequence of frames (excluding the ACK frames):

1) 802.11 Probe Req and 802.11 Probe Rsp
2) 802.11 Auth and then another 802.11 Auth
3) 802.11 Assoc Req and 802.11 Assoc Rsp
4) EAPOL-KEY
5) EAPOL-KEY
6) EAPOL-KEY
7) EAPOL-KEY

What security mechanism is being used on the WLAN?

A. WEP-128
B. WPA2-Personal
C. EAP-TLS
D. WPA-Enterprise
E. 802.1X/LEAP

**Answer: B**

## Question: 106

You work as the security administrator for your organization. In relation to the WLAN, you are viewing a dashboard that shows security threat, policy compliance and rogue threat charts. What type of system is in view?

A. Wireshark Protocol Analyzer
B. Wireless VPN Management Systems
C. Wireless Intrusion Prevention System
D. Distributed RF Spectrum Analyzer
E. WLAN Emulation System

**Answer: C**

## Question: 107

Given: Mary has just finished troubleshooting an 802.11g network performance problem using a laptop-based WLAN protocol analyzer. The wireless network implements 802.1X/PEAP and the client devices are authenticating properly. When Mary disables the WLAN protocol analyzer, configures her laptop for PEAP authentication, and then tries to connect to the wireless network, she is unsuccessful. Before using the WLAN protocol analyzer, Mary's laptop connected to the network without any problems.

What statement indicates why Mary cannot access the network from her laptop computer?

A. The nearby WIPS sensor categorized Mary's protocol analyzer adapter as a threat and is performing a deauthentication flood against her computer.

B. The PEAP client's certificate was voided when the protocol analysis software assumed control of the wireless adapter.

C. The protocol analyzer's network interface card (NIC) drivers are still loaded and do not support the version of PEAP being used.

D. Mary's supplicant software is using PEAPv0/EAP-MSCHAPv2, and the access point is using PEAPv1/EAP-GTC.

**Answer: C**

## Question: 108

You are implementing a wireless LAN that will be used by point-of-sale (PoS) systems in a retail environment. Thirteen PoS computers will be installed. To what industry requirement should you ensure you adhere?

A. ISA99

B. HIPAA

C. PCI-DSS

D. Directive 8500.01

**Answer: C**

## Question: 109

Given: You view a protocol analyzer capture decode with the following protocol frames listed in the following order (excluding the ACK frames):

1) 802.11 Probe Request and 802.11 Probe Response
2) 802.11 Auth and another 802.11 Auth
3) 802.11 Assoc Req and 802.11 Assoc Rsp
4) EAPOL-Start
5) EAP Request and EAP Response
6) EAP Request and EAP Response

7) EAP Request and EAP Response
8) EAP Request and EAP Response
9) EAP Request and EAP Response
10) EAP Success
19) EAPOL-Key (4 frames in a row)

What are you seeing in the capture file? (Choose 4)

A. WPA2-Enterprise authentication
B. WPA2-Personal authentication
C. 802.11 Open System authentication
D. 802.1X with Dynamic WEP
E. Wi-Fi Protected Setup with PIN
F. Active Scanning
G. 4-Way Handshake

**Answer: A, C, F, G**

## Question: 110

Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Choose 2)

A. Configuration distribution for autonomous APs
B. Wireless vulnerability assessment
C. Application-layer traffic inspection
D. Analysis and reporting of AP CPU utilization
E. Policy enforcement and compliance management

**Answer: B, E**

## Question: 111

ABC Company requires the ability to identify and quickly locate rogue devices. ABC has chosen an overlay WIPS solution with sensors that use dipole antennas to perform this task. Use your knowledge of location tracking techniques to answer the question.

In what ways can this 802.11-based WIPS platform determine the location of rogue laptops or APs? (Choose 3)

A. Time Difference of Arrival (TDoA)
B. Angle of Arrival (AoA)
C. Trilateration of RSSI measurements
D. GPS Positioning
E. RF Fingerprinting

**Answer: A, C, E**

## Question: 112

In an effort to optimize WLAN performance, ABC Company has upgraded their WLAN infrastructure from 802.11a/g to 802.11n. 802.11a/g clients are still supported and are used throughout ABC's facility. ABC has always been highly security conscious, but due to budget limitations, they have not yet updated their overlay WIPS solution to 802.11n or 802.11ac.

Given ABC's deployment strategy, what security risks would not be detected by the 802.11a/g WIPS?

A. Hijacking attack performed by using a rogue 802.11n AP against an 802.11a client
B. Rogue AP operating in Greenfield 40 MHz-only mode
C. 802.11a STA performing a deauthentication attack against 802.11n APs
D. 802.11n client spoofing the MAC address of an authorized 802.11n client

**Answer: B**

## Question: 113

Your organization required compliance reporting and forensics features in relation to the 802.11ac WLAN they have recently installed. These features are not built into the management system provided by the WLAN vendor. The existing WLAN is managed through a centralized management console provided by the AP vendor with distributed APs and multiple WLAN controllers configured through this console.

What kind of system should be installed to provide the required compliance reporting and forensics features?

A. WNMS
B. WIPS overlay
C. WIPS integrated
D. Cloud management platform

**Answer: B**

## Question: 114

You are implementing an 802.11ac WLAN and a WIPS at the same time. You must choose between integrated and overlay WIPS solutions. Which of the following statements is true regarding integrated WIPS solutions?

A. Integrated WIPS always perform better from a client throughput perspective because the same radio that performs the threat scanning also services the clients.
B. Integrated WIPS use special sensors installed alongside the APs to scan for threats.
C. Many integrated WIPS solutions that detect Voice over Wi-Fi traffic will cease scanning altogether to accommodate the latency sensitive client traffic.

D. Integrated WIPS is always more expensive than overlay WIPS.

**Answer: C**

## Question: 115

You have been recently hired as the wireless network administrator for an organization spread across seven locations. They have deployed more than 100 APs, but they have not been managed in either an automated or manual process for more than 18 months. Given this length of time, what is one of the first things you should evaluate from a security perspective?

A. The channel widths configured
B. The channels in use
C. The VLANs in use
D. The firmware revision

**Answer: D**

## Question: 116

ABC Company has deployed a Single Channel Architecture (SCA) solution to help overcome some of the common problems with client roaming. In such a network, all APs are configured with the same channel and BSSID. PEAPv0/EAP-MSCHAPv2 is the only supported authentication mechanism.

As the Voice over Wi-Fi (STA-1) client moves throughout this network, what events are occurring?

A. STA-1 initiates open authentication and 802.11 association with each AP prior to roaming.
B. The WLAN controller is querying the RADIUS server for authentication before the association of STA-1 is moved from one AP to the next.
C. STA-1 controls when and where to roam by using signal and performance metrics in accordance with the chipset drivers and 802.11k.
D. The WLAN controller controls the AP to which STA-1 is associated and transparently moves this association in accordance with the physical location of STA-1.

**Answer: D**

## Question: 117

Select the answer option that arranges the numbered events in the correct time sequence (first to last) for a client associating to a BSS using EAP-PEAPv0/MSCHAPv2.

1. Installation of PTK
2. Initiation of 4-way handshake
3. Open system authentication
4. 802.11 association
5. 802.1X controlled port is opened for data traffic
6. Client validates server certificate
7. AS validates client credentials

A. 3—4—6—7—2—1—5
8. 4—3—5—2—7—6—1
9. 5—3—4—2—6—7—1
10. 6—1—3—4—2—7—5
11. 4—3—2—7—6—1—5
12. 3—4—7—6—5—2—1

**Answer: A**

## Question: 118

Given: You have implemented strong authentication and encryption mechanisms for your enterprise 802.11 WLAN using 802.1X/EAP with AES-CCMP.

For users connecting within the headquarters office, what other security solution will provide continuous monitoring of both clients and APs with 802.11-specific tracking?

A. IPSec VPN client and server software
B. Internet firewall software
C. Wireless intrusion prevention system
D. WLAN endpoint agent software
E. RADIUS proxy server

**Answer: C**

## Question: 119

You must locate non-compliant 802.11 devices. Which one of the following tools will you use and why?

A. A spectrum analyzer, because it can show the energy footprint of a device using WPA differently from a device using WPA2.
B. A spectrum analyzer, because it can decode the PHY preamble of a non-compliant device.
C. A protocol analyzer, because it can be used to view the spectrum energy of non-compliant 802.11 devices, which is always different from compliant devices.
D. A protocol analyzer, because it can be used to report on security settings and regulatory or rule compliance

**Answer: D**